Drsná matematika

Martin Panák, Jan Slovák a „autorský kolektiv“

Projekt netradiční základní učebnice matematiky pro studenty přírodních věd, informatiky, ekonomie apod., přibližující podstatnou část matematiky v rozsahu čtyř semestrálních přednášek.

Text by měl být dokončen a vydán v roce 2013. Práce na učebnici jsou podpořeny projektem Univerzitní výuka matematiky v měnícím se světě (CZ.1.07/2.2.00/15.0203)

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Obsah

Předmluva

Příprava této učebnice byla motivována přednáškami pro informatické obory na Masarykově univerzitě, kde je celý program založen na precizním matematickém přístupu.

Chtěli jsme proto rychle, ale zároveň pořádně, pokrýt zhruba tolik matematických metod, jako je obvyklé u větších kurzů v klasických technických oborech opřených o matematické metody. Zároveň jsme ale nechtěli rezignovat na úplný a matematicky korektní výklad. Chtěli jsme vedle sebe vyložit i obtížnější partie matematiky a spoustu elementárních i obtížnějších konkrétních příkladů, jak s uvedenými postupy ve skutečnosti pracovat. Nechtěli jsme přitom za čtenáře řešit, v jakém pořadí a kolik „teorie“ či „praxe“ pročítat.

Z těchto podnětů vznikl dvousloupcový formát s oddělenými teoretickými úvahami a praktickými postupy, který kopíruje i skutečné rozdělení výkladu na přednáškách na „teoretické přednášky“ a „demonstrovaná cvičení“.

Snažíme se tím vyjít vstříc jak čtenářům, kteří si napřed chtějí procvičit postupy při řešení úloh a teprve pak přemýšlet, proč a jak algoritmy fungují, tak těm druhým, kteří si napřed chtějí dělat jasno o tom proč a jak věci fungují a pak případně zkouší počítat příklady. Zároveň tím snad zbavujeme čtenáře stresu, že by měl přečíst úplně vše. Naopak, měl by mít radost z brouzdání textem a prožitku objevování vlastní cestičky.

Text se přitom v obou svých částech snaží prezentovat standardní výklad matematiky s akcentem na smysl a obsah představovaných matematických metod. Řešené úlohy procvičují základní pojmy, ale zároveň se snažíme dávat co nejlepší příklady užití matematických modelů.

Teoretický text je prezentován dosti kompaktním způsobem, mnoho prostoru je ponecháno pro dořešení podrobností čtenáři. Uváděné příklady se snaží pokrýt celou škálu složitosti, od banálních až po perličky ke skutečnému přemýšlení. Studenti navíc řešili a odevzdávali každý týden zadávané příklady.

Čtenářům bychom rádi pomohli:

- přesně formulovat definice základních pojmů a dokazovat jednoduchá matematická tvrzení,
- vnímat obsah i přibližně formulovaných závislostí, vlastností a výhledů použití matematických nástrojů,
- vstřebat návody na užívání matematických modelů a osvojit si jejich využití.

K těmto ambiciózním cílům nelze dojít lehce a pro většinu lidí to znamená hledat si vlastní cestu s tápáním různými směry (s potřebným překonáváním odporu či nechutě). I proto je celý výklad strukturován tak, aby se pojmy a postupy vždy několikrát vracely s postupně rostoucí složitostí a šíří diskuse.

Jsme si vědomi, že se tento postup může jevit jako chaotický. Domníváme se ale, že dává mnohem lepší šanci na pochopení u těch, kteří vytrvají.

Vstup do matematiky je skoro pro každého obtížný — pokud už „víme“, nechce se nám přemýšlet, pokud „nevíme“, je to ještě horší. Jediný spolehlivý postup pro orientaci v matematice je hledat porozumnění v mnoha pokusech a hledat je při četbě v různých zdrojích. Určitě nepovažujeme tento text za dostatečný jediný zdroj pro každého. Doufáme, že může být dobrým začátkem a případně i dlouhodobým pomocníkem, zvláště pro ty, kdo se k jednotlivým částem budou znovu a znovu vracet.

Pro ulehčení vícekolového přístupu ke čtení je text doprovázen emotivně laděnými ikonkami, které snad nejen oživí obvyklou strohou strukturu matematického textu, ale naznačí čtenáři, kde by složitější text měl být čten pozorněji, ale určitě ne přeskakován, případně kde by bylo možná lépe náročné pasáže přinejmenším napoprvé vůbec nečíst.

Volba jednotlivých ikonek samozřejmě odráží hlavně pocity autorů. Přesto by postupně mohly být dobrým vodítkem pro čtenáře. Velice zhruba řečeno, používáme ikonky varující před pracností/složitostí/náročností, např.

Další označují ne úplně pohodovou zdlouhavost práce a potřebu trpělivosti či nadhledu, jako jsou tyto

A konečně máme také ikonky vyjadřující pohodu nebo radost ze hry, třeba následující

Snažili jsme se sloupce s příklady sepsat tak, aby byly čitelné prakticky víceméně samostatně. Bez ambicí pohrát si s hlubšími důvody, proč uváděné postupy fungují, (nebo s prostým cílem „projít s písemkou“) by mělo skoro stačit probírat se jen příklady. Definice pojmů či popisy jejich vlastností používaných při řešení příkladů jsou v teoretickém sloupci zpravidla vyznačeny, aby o ně bylo možno snadno pohledem zavadit. Souvislost řešených příkladů s paralelně studovanou teorií je přitom spíše volná, snažili jsme ale ulehčit přeskakování „z teorie do praxe a zpět“ co nejvíce.

Obsahově je celá učebnice ovlivněna představou, že pro praktické využití jsou vlastně skoro vždy podstatné metody tzv. diskrétní matematiky, zatímco tzv. spojité modely jsou matematicky dobře uchopitelná přiblížení veskrze diskrétního světa kolem nás. Počítat koneckonců stejně umíme vždy jen s konečně mnoha racionálními čísly naráz. Bez spojité matematiky si lze ale těžko dobře představit koncepty jako konvergence procesu k limitnímu stavu nebo robustnost výpočtu. Bylo by bez ní také obtížné pracovat s odhady chyb při numerických procesech.

Všechna témata a velmi podstatnou část textu jsme v létech 2005 – 2012 ověřovali při výuce studentů informatiky a později i matematiky na Masarykově univerzitě. Paralelně jsme přitom vytvořili také podklady pro praktické semináře matematického modelování a numerických metod. V nich se studenti, věnují skutečnému využití výpočtových nástrojů a modelů.

Závěrem tohoto stručného představení stručně shrneme obsah celé učebnice. Samozřejmě předpokládáme, že si každý čtenář, případně přednášející, vybere témata a jejich pořadí. Pokusíme se proto zároveň vymezit bloky, se kterými lze takto nezávisle zacházet.

Úvodní motivační kapitola se snaží ilustrovat několik

přístupů k matematickému popisu problémů. Začínáme nejjednoduššími funkcemi (základní *kombinatorické vzorce*). Pak naznačujeme jak pracovat se závislostmi zadanými pomocí okamžitých změn (jednoduché *diferenční rovnice*), užití kombinatoriky a množinové algebry diskutujeme prostřednictvím konečné klasické *pravděpodobnosti*. Předvádíme maticový počet pro jednoduché úlohy rovinné geometrie (práce s pojmem *pozice* a *transformace*) a závěrem vše trochu zformalizujeme (*relace, uspořádní, ekvivalence*).

Nenechte se zde uvrhnout do chaotického zmatku rych-

lým střídáním témat — cílem je nashromáždit něco málo netriviálních námětů k přemýšlení a hledání jejich souvislostí i použití, ještě než zabředneme do úrovně problémů a teorií složitějších. Ke všem tématům této úvodní kapitoly se časem vrátíme.

Další dvě kapitoly jsou věnovány základům počtu, který

umožňuje práci s vícerozměrnými daty i grafikou. Jde o postupy tzv. *lineární algebry*, které jsou základem a konečným výpočetním nástrojem pro většinu matematických modelů. Nejprve probíráme jednoduché postupy pro práci s *vektory a maticemi*, třetí kapitola je pak věnována aplikacím maticového počtu v různých lineárních modelech (*systémy lineárních rovnic, lineární procesy, lineární diferenční rovnice, Markovovy procesy, lineární regrese*). Čtvrtá kapitola pak ilustruje použití maticového počtu v geometrických úlohách. Dozvíme se něco málo o *afinní, euklidovské a projektivní geometrii.*

V tomto okamžiku přerušíme diskusi diskrétních mo-

delů a přejdeme ke spojitým. Chceme co nejnázorněji ukázat, že základní ideje, jak s funkcemi pracovat, bývají jednoduché. Stručně řečeno, velmi jednoduché úvahy spojené s popisem okamžitých změn sledovaných veličin umožňují dělat závěry pro jejich celkové chování. Složitosti se pojí skoro výhradně se zvládnutím rozumně velké třídy funkcí, pro které mají naše postupy být použitelné.

Začínáme proto kapitolou, kde diskutujeme jaké funkce potřebujeme pro nelineární modely. Po *polynomech a splajnech* postupně diskutujeme pojmy *spojitosti*, *limity posloupností a funkcí* a *derivace funkcí*, připomeneme všechny základní *elementární funkce* a závěrem se seznámíme s *mocninnými řadami*. Tím je připravena půda pro klasický diferenciální a integrální počet. Ten prezentujeme v kapitole šesté s důrazem na co nejpřímočařejší pochopení souvislostí *limitních procesů*, *integračních procesů* a *aproximací*.

Sedmá kapitola se věnuje náznakům aplikací a snaží se co nejvíce připomínat analogie k postupům jednoduché lineární algebry z minulého semestru. Místo lineárních zobrazení mezi konečně rozměrnými vektorovými prostory tak pracujeme s lineárními operacemi mezi nekonečně rozměrnými vektorovými prostory funkcí, definovanými buď integrálními nebo diferenciálními operátory.

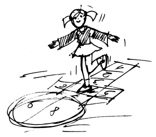
Zatímco studium diferenciální rovnic necháváme na později, zde studujeme nejprve aproximace funkcí s pomocí vzdálenosti definované integrálem (tzv. *Fourierovy řady*). Pak se věnujeme souvislostem s některými integrálními operátory (např. *konvoluce*) a integrálními transformacemi (zejména *Fourirerova transformace*). Po cestě si neodpustíme ilustraci obecného principu, že spojité modely jsou zpravidla ideovým podkladem a zároveň dobrou aproximací pro modely diskrétní. Poslouží nám k tomu stručné nahlédnutí na problematiky tzv. *waweletů* a *diskrétní Fourierovy transformace*.

tady jsem to už hodně odbýval – texty ještě vůbec nejsou :-)

V osmé kapitole pokračujeme v našem stručném nastínění analytických spojitých metod, tentokrát pro modely s mnoha proměnnými. Nejprve rozšíme základní postupy a výsledky týkající se derivací na *funkce více proměnných*, včetně *funkcí zadaných implicitně* a tzv. *vázaných extrémů*. Hned poté rozšíříme teorii integrování o tzv. násobné integrály. Poté se věnujeme stručně modelům opřeným o známou změnu našich objektů, tj. *diferenciálním rovnicím* a malinko naznačíme obdobné problémy *variační*. Závěrem této kapitoly se pak stručně věnujeme numerickým příblížením a odhadům.

stále více se mi líbí představa, že bychom měli jako 9. mít pravděpodobnost a statistiku (Martinův návrh) a pak v grafech, sítích a kódech či šifrách už i s pravděpodobnostmi v aplikacích pracovat. To by do třetího semestru shrnulo zbytek analýzy a právě statistiku, poslední semestr by byl diskretni

Devátá kapitola směřuje zpět do světa diskrétních metod. Zabýváme se v ní základními pojmy poznatky teorie grafů a jejich využitím v praktických problémech (např. prohledávání do šířky a hloubky, *minimální pokrývající kostry*, *toky v sítích*, *hry popisované stromy*). Závěrem uvádíme pár poznámek o vytvořujících funkcích.



Předposlední kapitola se zabývá nejprve obecnými algebraickými strukturami s důrazem na teorii grup. Věnujeme se ale i jiným strukturám a soustředíme se na aplikace, které směřujeme na velmi aktuální oblasti kódování a šifrování.

Poslední jedenáctá kapitola je věnována matematické pravděpododobnosti a statistice. Seznámíme se s pojmy *pravděpodobnostní prostor, hustota pravděpodobnosti, normální rozdělení, střední hodnota, medián, kvantil, rozptyl, příklady diskrétních a spojitých rozdělení* a budeme se náznakem věnovat *statistickému zpracování dat*.

bubák je tady DOČASNĚ kvůli autorovi, nikoliv kvůli složitosti obsahu :-)

POŘÁDNÉ PODĚKOVÁNÍ VŠEM ZÚČASTNĚNÝM, KTEŘÍ NEBUDOU PŘÍMO V AUTORSKÉM KOLEKTIVU, STUDENTŮM APOD.

??. ??. 2013, kolektiv autorů

KAPITOLA 1

Krůčky k matematickým problémům

„hodnota, změna, poloha“
– co to je a jak to uchopit?

Cílem první kapitoly je uvést čtenáře do fascinujícího světa matematického myšlení. Vybíráme si k tomu co nejkonkrétnější příklady modelování reálných situací pomocí abstraktních objektů a souvislostí. Zároveň projdeme několik témat a postupů, ke kterým se postupně budeme vracet a v závěru kapitoly se budeme chvíli věnovat samotnému jazyku matematiky (se kterým budeme jinak zacházet spíše intuitivně).

O co jednodušší jsou východiska a objekty, se kterými zde budeme pracovat, o to složitější je pochopit do důsledku jemnosti použitých nástrojů a postupů. Většinou je možné proniknout k podstatě věcí teprve v jejich souvislostech. Proto je také představujeme hned z několika pohledů zároveň.

Přecházení od tématu k tématu se možná bude zdát jako zmatečné, ale to se jistě postupně spraví při našich návratech k jednotlivým úvahám a pojmům v pozdějších kapitolách.

Název kapitoly lze chápat i jako nabádání k trpělivosti. I nejjednodušší úlohy a úvahy budou snadné jen pro ty, kteří už podobné řešili (a půjde pro ně jen o opakování znalosti ze střední školy). K postupnému poznání a ovládnutí matematického myšlení vede jen pozvolná a spletitá cesta.

Začneme s tím nejjednodušším: obyčejnými čísly.

1. Čísla a funkce

Lidé odjakživa chtějí mít jasno „kolik“ něčeho je, případně „za kolik“ to je, „jak dlouho“ něco trvá apod. Výsledkem takových úvah je většinou nějaké „číslo“. Za číslo přitom považujeme něco, co umíme sčítat a násobit a splňuje to obvyklé zákonitosti, ať už všechny nebo jen některé. Například výsledek sčítání nezávisí na pořadí, v jakém čísla sčítáme, máme k dispozici číslo nula, které přičtením výsledek nezmění, číslo jedna, kterým můžeme násobit, aniž bychom změnili výsledek, apod.

Nejjednodušším příkladem jsou tzv. čísla přirozená, budeme je značit $\mathbb{N} = \{0, 1, 2, 3, \dots\}$. Všimněme si, že jsme mezi přirozená čísla vzali i nulu, jak je obvyklé zvláště v informatice.

Počítat „jedna, dvě, tři, …“ se učí děti už ve školce. O něco později se setkáváme s čísly celými $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ a nakonec si zvykneme na desetinná čísla a víme, co znamená 1.19–násobek ceny díky 19% dani z přidané hodnoty.

1.1 **1.1. Vlastnosti čísel.** Abychom mohli s čísly pracovat

opravdu, musíme se jejich definici a vlastnostem věnovat pořádněji. V matematice se těm základním tvrzením o vlastnostech objektů, jejichž platnost předpokládáme, aniž bychom se zabývali jejich dokazovaním, říká *axiomy*. Vhodná volba axiomů předurčuje jak dosah z nich vycházející teorie, tak její použitelnost v matematických modelech skutečnosti.

Vlastnosti sčítání:

(KG1) $(a+b)+c = a+(b+c)$, pro všechna a, b, c

(KG2) $a+b = b+a$, pro všechna a, b

(KG3) existuje 0 taková, že pro všechna a platí $a+0 = a$

(KG4) pro všechna a existuje b takové, že $a+b = 0$

Vlastnostem (KG1) – (KG4) říkáme vlastnosti *komutativní grupy*. Jsou to po řadě *asociativita*, *komutativita*, *existence neutrálního prvku* (říkáme u sčítání také nulového prvku), *existence inverzního prvku* (říkáme u sčítání také opačného prvku k a a značíme ho $-a$).
Vlastnosti násobení:

(O1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, pro všechny a, b, c

(O2) $a \cdot b = b \cdot a$, pro všechny a, b

(O3)
existuje prvek 1 takový, že pro všechny a platí $1 \cdot a = a$

(O4) $a \cdot (b+c) = a \cdot b + a \cdot c$, pro všechny a, b, c.

Vlastnosti (O1)-(O4) se postupně nazývají *asociativita*, *komutativita*, existence *jednotkového prvku* a *distributivita* sčítání vůči násobení.

Množiny s operacemi $+, \cdot$ a vlastnostmi (KG1)–(KG4), (O1)–(O4) se nazývají *komutativní okruhy*.
Další vlastnosti násobení:

(P) pro každé $a \neq 0$ existuje b takové, že $a \cdot b = 1$.

(OI) je-li $a \cdot b = 0$, potom buď $a = 0$ nebo $b = 0$.

Vlastnost (P) se nazývá existence *inverzního prvku* vzhledem k násobení (tento prvek se pak značí a^{-1}) a vlastnost (OI) říká, že neexistují „dělitelé nuly“.

Vlastnosti skalárů

Uvedli jsme si základní vlastnosti operací sčítání a náso-

bení pro naše počty s čísly, která píšeme jako písmena $a, b, c, \ldots$. Obě tyto operace fungují tak, že vezmeme dvě čísla a, b a aplikací sčítání nebo násobení dostaneme výsledné hodnoty $a+b$ a $a \cdot b$. Vlastnosti těchto operací budeme soustavně využívat, aniž bychom museli přesně vědět, s jakými objekty skutečně pracujeme. Tak se dostaneme k obecným matematickým nástrojům, je však vždy dobré mít představu o typických příkladech.

Celá čísla $\mathbb{Z}$ jsou dobrým příkladem komutativní grupy, přirozená čísla nikoliv, protože nesplňují (KG4) (a případně neobsahují neutrální prvek, pokud někdo nulu do $\mathbb{N}$ nezahrnuje).

Když komutativní okruh navíc splňuje i vlastnost (P), hovoříme o *poli* (často také o *komutativním tělese*).

Poslední uvedená vlastnost (OI) je automaticky splněna, pokud platí (P). Opačně to ovšem neplatí a tak říkáme, že vlastnost (OI) je slabší než (P). Např. okruh celých čísel $\mathbb{Z}$ nesplňuje (P), ale splňuje (OI). Hovoříme v takovém případě o *oboru integrity*.

Všimněme si, že množina všech nenulových prvků v poli společně s operací násobení splňuje (O1), (O2), (O3), (P), a je proto také komutativní grupa. Jen se místo sčítání mluví o násobení. Jako příklad můžeme vzít všechna nenulová reálná čísla.

Prvky nějaké množiny s operacemi $+$ a $\cdot$ splňujícími (ne nutně všechny) výše uvedené vlastnosti (tj. komutativní okruh, obor integrity, pole) budeme nazývat *skaláry*. Budeme pro ně vesměs užívat malá latinská písmena ze začátku nebo konce abecedy.

Všechny vlastnosti (KG1)–(KG4), (O1)–(O4), (P), (OI) z našich úvah je třeba brát jako *axiomatickou definici* příslušných matematických pojmů. Pro naše potřeby bude stačit si průběžně uvědomovat, že při dalších diskusích budeme důsledně používat pouze tyto vlastnosti skalárů a že i naše výsledky proto budou platné pro všechny objekty s těmito vlastnostmi.

V tomto je pravá síla matematických teorií – nejsou platné jen pro konkrétní řešený příklad. Naopak, při rozumné výstavbě mají vždy univerzální použití. Budeme se snažit tento aspekt zdůrazňovat, přestože naše ambice mohou být v rámci daného rozsahu učebnice jen velice skromné.

1.1a

1.2. Existence skalárů. K tomu, aby ale skutečně bylo

možné budovat matematickou teorii, je třeba ověřit, že takové objekty mohou existovat. Pro pořádek si proto budeme postupně ukazovat, jak je možné zkonstruovat základní číselné obory. Pro konstrukci přirozených čísel začneme s předpokladem, že víme, co jsou to množiny.

Prázdnou množinu si označíme $\emptyset$ a definujeme

e1.1

$$0 := \emptyset, \quad n + 1 := n \cup \{n\} \ , \tag{1.1}$$

neboli

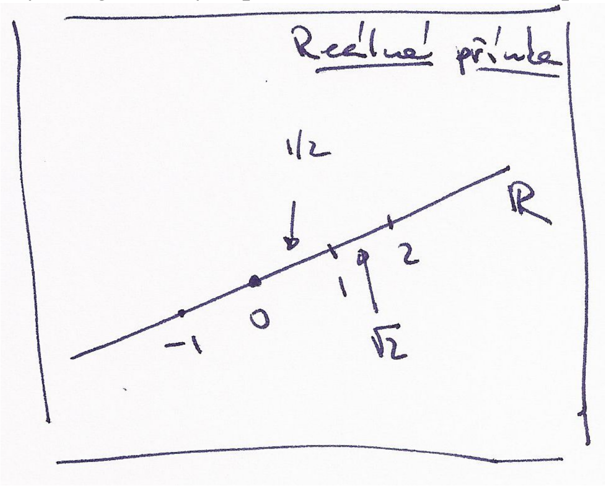
$$0 := \emptyset,\ 1 := \{\emptyset\},\ 2 := \{0, 1\}, \dots, n + 1 := \{0, 1, \dots, n\}.$$

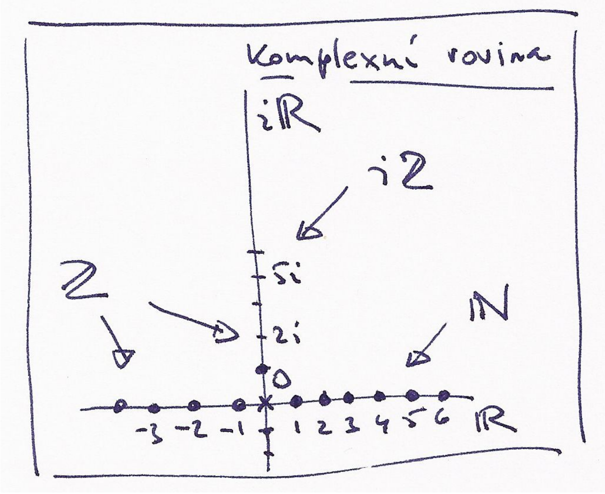
Tímto zápisem říkáme, že pokud už máme definovaná všechna čísla $0, 1, 2, \dots n$, pak číslo $n + 1$ definujeme jako množinu všech předchozích čísel.

Přirozená čísla takto ztotožňujeme s počty prvků konkrétních množin. Číslo n je množina, která má n prvků a dvě přirozená čísla a, b jsou stejná, právě když příslušné množiny mají stejně prvků. V teorii množin se místo slovního spojení „počet prvků množiny“ používá pojem „mohutnost množiny“. Tento pojem má smysl (narozdíl od toho předchozího) i pro nekonečné množiny.

Na první pohled je také vidět obvyklá definice uspořádání přirozených čísel podle velikosti (o číslu a řekneme, že je ostře menší než b tehdy a jen tehdy, když $a \neq b$ a $a \subset b$ jako množina). Dalším formálním krokem by měla být definice sčítání a násobení a důkaz všech základních vlastností přirozených čísel, včetně výše uvedených axiomů komutativního okruhu. Snadno lze např. ukázat, že každá podmnožina v $\mathbb{N}$ má nejmenší prvek a spoustu dalších vlastností o kterých zpravidla už dávno nepřemýšlíme a máme je za samozřejmé.

Nebudeme se tu konstrukcí číselných oborů zabývat podrobně a předpokládáme, že čtenář čísla racionální ($\mathbb{Q}$), reálná ($\mathbb{R}$) a komplexní ($\mathbb{C}$) důvěrně zná. Občas budeme jen připomínat teoretické i praktické souvislosti při dalším výkladu. Podrobně bude konstrukce racionálních čísel z přirozených diskutována v 1.40. Konstrukci reálných čísel bude vhodné zmínit při studiu limitních procesů později a již dříve budeme z různých algebraických pohledů zkoumat čísla komplexní.





Navíc, jak je v matematice obvyklé, budeme místo s čísly manipulovat s písmeny abecedy, případně jinými znaky, ať už jejich hodnota je nebo není předem známá.

1.2 **1.3. Skalární funkce.** Často pracujeme s číselnou hodnotou, která není dána jako konkrétní číslo. Místo

toho něco víme o závislosti naší hodnoty na hodnotách jiných. Formálně píšeme, že hodnota $y = f(x)$ naší „závislé“ proměnné veličiny y je dána „nezávislou“ veličinou x. Přitom můžeme znalost f brát formálně (prostě je to nějaká, blíže nespecifikovaná, závislost) nebo operačně, tj. $f(x)$ je dáno vzorcem poskládaným z (prozatím si představme konečně mnoha) známých operací. Pokud je hodnotou skalár, hovoříme o *skalární funkci*. Každá funkce je definována na nějaké množině, mluvíme o *definičním oboru funkce*, a množina všech hodnot je pak tzv. *obor hodnot funkce*.

Také mohou být ale hodnoty funkce f dány pouze přibližně nebo s jistou pravděpodobností.

Smyslem matematických úvah pak bývá z neformálního popisu závislostí najít explicitní vzorce pro funkce, které je popisují, nebo aspoň explicitní vyjádření pro konkrétní hodnoty závislých proměnných, případně jejich přiblížení. Podle typu úlohy a cíle pracujeme:

- s přesným a konečným výrazem
- s nekonečným výrazem
- s přiblížením neznámé funkce známým odhadem (většinou s vyčíslenou možnou chybou)
- s odhadem hodnot s vyčíslením jejich pravděpodobnosti apod.

Skalární funkcí je např. roční mzda pracovníka nějaké firmy (hodnoty nezávislé veličiny, tj. definiční obor funkce, jsou jednotliví pracovníci x z množiny všech sledovaných pracovníků, $f(x)$ je jejich roční mzda za dané období). Stejně tak můžeme sledovat měsíční mzdu konkrétního pracovníka v čase (nezávislou hodnotou je čas v měsících, závislou příjem v jednom každém měsíci). Jiným příkladem je třeba plocha obrazce v rovině, objem tělesa v prostoru, rychlost konkrétního auta v čase atd. Dovedeme si jistě představit, že ve všech uvedených případech může být hodnota dána nějakou volně popsanou souvislostí nebo naměřena přibližně nebo odhadnuta atd.

1.3 **1.4. Operačně definované funkce.** Funkce můžeme mít

dány výčtem jejich hodnot – např. ve firmě je jen konečně mnoho zaměstnanců a umíme sestavit tabulku s jejich aktuálními měsíčními platy. Častěji ale máme místo hodnot pravidla, jak k hodnotám dojít.

Důležitou skalární funkcí na přirozených číslech je *faktoriál*, který definujeme vztahy

$$f(0) = 1, \ \ f(n) = n \cdot f(n-1)$$

pro $n = 1, 2, \ldots$. Píšeme $f(n) = n!$ a definice zjevně znamená

$$n! = n \cdot (n-1) \cdots 1.$$

Funkce faktoriál

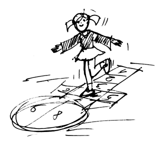
Naše definice funkce faktoriál říká, jak se změní hodnota $f(n)$, když změníme hodnotu n o jedničku. Vzorec pro $n!$ již explicitně říká, kolik to je doopravdy. V tomto případě to není příliš efektivní vzorec, protože se jeho složitost zvětšuje s rostoucím n, lepší ale těžko hledat.

Podívejme se ještě na obyčejné sčítání přirozených čísel jako na operačně definovanou skalární funkci. Definičním oborem je množina všech dvojic (a, b) přirozených čísel. Definujeme $a+b$ jako výsledek procedury, ve které k a několikrát po sobě přičítáme 1. Tak jsme vlastně obecně $a + 1$ definovali v rovnicích (1.1). Při každém přičtení odebereme z b největší prvek a postupujeme tak, dokud není b prázdná (tj. b se postupně zmenšuje o jedničku a v každém kroku nám říká, kolik ještě zbývá přičíst).

Je evidentní, že takto definované sčítání sice je dáno (iterativním) vzorcem, postup ale není vhodný pro praktické počítání. Tak tomu bude v našem výkladu často – teoreticky korektní definice pojmu či operace neznamená, že úkony s nimi spojené jsou efektivně vykonavatelné. Právě k tomu budeme postupně rozvíjet celé teorie, abychom praktické nástroje získávali. Co se týče přirozených čísel, od školky je umíme sčítat zpaměti a rychle (pokud jsou malá), pro větší známe ze základní školy algoritmus písemného sčítání a s velkými si poradí počítače (pokud nejsou příliš velká).

2. Kombinatorické veličiny

Typickým „kombinatorickým“ problémem je napočítat, kolika různými způsoby se může něco stát.



Např. kolika způsoby lze vybrat v samoobsluze dva různé sendviče z dané nabídky? Myslíme si přitom, že jsou všechny sendviče v regálu po dvou různé nebo rozlišujeme jen různé typy sendvičů? Připouštíme pak, že si také můžeme vzít dva stejné? Nepřeberně takových otázek máme u karetních a jiných her.

1.4

1.5. Permutace. Jestliže z množiny n předmětů vytváříme nějaké pořadí jejich prvků, máme pro volbu prvního prvku n možností, další je volen z $n - 1$ možností atd., až nám nakonec zbude jediný poslední prvek. Zjevně tedy je na dané konečné množině S s n prvky právě $n!$ různých pořadí. Procesu uspořádávání prvků množiny S říkáme *permutace* prvků množiny S. Výsledkem permutace je pak vždy nějaké pořadí prvků. Jestliže si předem prvky v S očíslujeme, tj. ztotožníme si S s množinou $S = \{1, \dots, n\}$ n přirozených čísel, pak permutace odpovídají možným pořadím čísel od jedné do n. Máme tedy příklad jednoduché matematické věty a naši předchozí diskusi je možné považovat za její důkaz:

Tvrzení. *Počet $p(n)$ různých pořadí na konečné množině s n prvky je dán známou funkcí faktoriál:*

e1.1a

$$p(n) = n! \tag{1.2}$$

Počet permutací na konečné množině

1.4a **1.6. Kombinace a variace.** Dalším jednoduchým příkladem hodnoty určené vzorcem jsou tzv. *kombinační čísla*, která vyjadřují, kolika způsoby lze vybrat k různých rozlišitelných předmětů z množiny n předmětů. Zjevně máme

$$n(n-1)\cdots(n-k+1)$$

možných výsledků postupného výběru našich k prvků, přitom ale stejnou výslednou k–tici dostaneme v $k!$ různých pořadích. Pokud nám záleží i na pořadí vybrané k-tice prvků, hovoříme o *variaci k–tého stupně*.

Jak jsme si právě ověřili, počet kombinací a variací udávají následující vzorce, které také nejsou pro výpočet moc efektivní při velikých k a n, protože obsahují výrazy pro faktoriály.

Tvrzení. *Pro počet $c(n,k)$ kombinací k-tého stupně z n prvků, kde $0 \le k \le n$, platí*

e1.2 (1.3)
$$c(n,k) = \binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots 1} = \frac{n!}{(n-k)!k!}.$$

Pro počet $v(n,k)$ variací platí

e1.2a (1.4)
$$v(n,k) = n(n-1)\cdots(n-k+1)$$

pro všechny $0 \le k \le n$ (a nula jinak).

Kombinace a variace

Kombinační číslo $\binom{n}{k}$ čteme „n nad k" a nazýváme ho také někdy *binomickým číslem.* Tento název čísla dostala od tzv. *binomického rozvoje*, tj. roznásobení n-té mocniny dvojčlenu. Počítáme-li totiž $(a+b)^n$, bude koeficient u mocniny $a^k b^{n-k}$ pro každé $0 \le k \le n$ roven právě počtu možností, jak vybrat k–tici z n závorek v součinu (ty, kde bereme do výsledku a). Platí proto

e1.3 (1.5)
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

a všimněme si, že pro odvození jsme potřebovali pouze distributivitu, komutativitu a asociativitu násobení a sčítání. Formule (1.5) proto platí v každém komutativním okruhu.

Jako další jednoduchou ukázku, jak vypadá matematický důkaz si odvoďme několik jednoduchých tvrzení o kombinačních číslech. Pro zjednodušení formulací definujme $\binom{n}{k} = 0$, kdykoliv je buď $k < 0$ nebo $k > n$.

1.5 **1.7. Tvrzení.** *Pro všechna přirozená čísla k a n platí*

(1) $\binom{n}{k} = \binom{n}{n-k}$
(2) $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$
(3) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$
(4) $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}.$

DŮKAZ. První tvrzení je zjevné přímo z formule (1.3). Jestliže vyčíslíme pravou stranu z tvrzení (2), dostáváme

$$\begin{aligned}\binom{n}{k}+\binom{n}{k+1}&=\frac{n!}{k!(n-k)!}+\frac{n!}{(k+1)!(n-k-1)!}\\&=\frac{(k+1)n!+(n-k)n!}{(k+1)!(n-k)!}\\&=\frac{(n+1)!}{(k+1)!(n-k)!}\end{aligned}$$

což je ale levá strana tohoto tvrzení.

Tvrzení (3) dokážeme tzv. *matematickou indukcí*. Tento

typ důkazu je vhodný právě pro tvrzení, která říkají, že něco má platit pro všechna přirozená čísla n. Matematická indukce se skládá ze dvou kroků. V prvním se tvrzení dokáže pro $n = 0$ (popřípadě $n = 1$ nebo další hodnoty n). V druhém, tzv. indukčním, kroku předpokládáme, že tvrzení platí pro nějaké n (a všechny předešlé hodnoty), a za pomoci tohoto předpokladu dokážeme, že tvrzení platí i pro $n + 1$. Dohromady z toho pak vyvodíme, že tvrzení platí pro všechna přirozená n.

Tvrzení (3) zjevně platí pro $n = 0$, protože $\binom{0}{0} = 1 = 2^0$. (Stejně tak je přímo vidět i pro $n = 1$.) Předpokládejme, že platí pro nějaké n a spočtěme příslušnou sumu pro $n + 1$ s využitím tvrzení (2) i (3). Dostaneme

$$\begin{aligned}\sum_{k=0}^{n+1}\binom{n+1}{k}&=\sum_{k=0}^{n+1}\left[\binom{n}{k-1}+\binom{n}{k}\right]\\&=\sum_{k=-1}^{n}\binom{n}{k}+\sum_{k=0}^{n+1}\binom{n}{k}=2^n+2^n=2^{n+1}.\end{aligned}$$

Všimněme si, že vzorec (3) udává počet všech podmnožin n–prvkové množiny, neboť $\binom{n}{k}$ je počet všech jejích k–prvkových podmnožin. Všimněme si také, že tvrzení (3) plyne přímo z (1.5) volbou $a = b = 1$.

Tvrzení (4) dokážeme opět matematickou indukcí, podobně jako (3). Zjevně platí pro $n = 0$, čímž je hotov první krok. Indukční předoklad říká, že (4) platí pro nějaké n. Spočtěme nyní příslušnou sumu pro $n + 1$ s využitím tvrzení (2) a indukčního předpokladu. Dostaneme

$$\begin{aligned}\sum_{k=0}^{n+1}k\binom{n+1}{k}&=\sum_{k=0}^{n+1}k\left[\binom{n}{k-1}+\binom{n}{k}\right]\\&=\sum_{k=-1}^{n}(k+1)\binom{n}{k}+\sum_{k=0}^{n+1}k\binom{n}{k}\\&=\sum_{k=0}^{n}\binom{n}{k}+\sum_{k=0}^{n}k\binom{n}{k}+\sum_{k=0}^{n}k\binom{n}{k}\\&=2^n+n2^{n-1}+n2^{n-1}=(n+1)2^n.\end{aligned}$$

Tím je proveden indukční krok, a tvrzení je dokázáno pro všechna přirozená n. □

Druhá vlastnost z našeho tvrzení umožňuje sestavit všechna kombinační čísla do tzv. *Pascalova trojúhelníku*, kde každé číslo obdržíme jako součet dvou bezprostředně nad ním ležících sousedů:

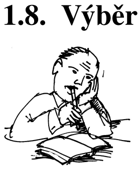
$$
\begin{array}{lccccccccccc}
n=0: & & & & & & 1 & & & & & \\
n=1: & & & & & 1 & & 1 & & & & \\
n=2: & & & & 1 & & 2 & & 1 & & & \\
n=3: & & & 1 & & 3 & & 3 & & 1 & & \\
n=4: & & 1 & & 4 & & 6 & & 4 & & 1 & \\
n=5: & 1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}
$$

Všimněme si, že v jednotlivých řádcích máme právě koeficienty u jednotlivých mocnin z výrazu (1.5), např. poslední uvedený řádek říká

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

1.6

1.8. Výběr s opakováním. Pořadí n prvků, z nichž mezi některými nerozlišujeme, nazýváme *permutace s opakovaním.*



Nechť je mezi n danými prvky p_1 prvků prvního druhu, p_2 prvků druhého druhu, ..., p_k prvků k–tého druhu, $p_1 + p_2 + \cdots + p_k = n$, potom počet pořadí těchto prvků s opakováním budeme značit $P(p_1, \dots, p_k)$.

Podobně jako u permutací a kombinací bez opakování, pro výběr prvního z nich máme n možností, pro další $n-1$ a tak dále, až po poslední, který zbude. Přitom ale za stejná považujeme pořadí nerozlišitelných objektů. Těch je pro každou skupinku o p_i objektech právě $p_i!$, takže zřejmě platí

$$P(p_1, \dots, p_k) = \frac{n!}{p_1! \cdots p_k!}.$$

Permutace s opakováním

Volný výběr k prvků z n možností, včetně pořadí, nazýváme *variace k-tého stupně s opakováním*, jejich počet budeme značit $V(n,k)$. Volný výběr v tomto případě znamená, že předpokládáme, že stále máme pro výběr stejně možností, např. díky tomu, že vybrané prvky před dalším výběrem vracíme nebo třeba házíme pořád stejnou kostkou. Zřejmě platí

$$V(n,k) = n^k.$$

Variace s opakováním

Pokud nás výběr zajímá bez zohlednění pořadí, hovoříme o *kombinacích s opakováním* a pro jejich počet píšeme $C(n,k)$. Zde se na první pohled nezdá tak jednoduché, jak výsledný počet zjistit. Důkaz následující věty je pro matematiku typický – podaří se nám nový problém převést na problém jiný, který jsme už dříve zvládli. V našem případě je to převedení na problém standardních kombinací bez opakování:

Věta. *Počet kombinací s opakováním k-té třídy z n prvků je pro všechny $k \geq 0$ a $n \geq 1$*

$$C(n,k) = \binom{n+k-1}{k}.$$

Kombinace s opakováním

Důkaz. Důkaz je opřen o trik (jednoduchý, jakmile ho pochopíme). Uvedeme dva různé postupy.

Představme si nejprve, že taháme postupně karty z balíku n různých karet a abychom mohli případně některou z nich vytáhnout vícekrát, přidáme si k balíku ještě $k-1$ různých žolíků (alespoň jednou určitě chceme jednu z původních karet). Řekněme, že postupně vytáhneme r původních karet a s žolíků, tj. $r+s=k$. Zdá se, že bychom měli vymyslet postup, jak z těch s žolíků poznat, které karty nám zastupují. Ve skutečnosti nám ale stačí diskuse počtů možností takových voleb.

K tomu můžeme použít matematickou indukci a předpokládat, že dokazovaná věta platí pro menší argumenty než jsou n a k. Skutečně, potřebujeme obsáhnout kombinace s–té třídy s opakováním z pouze r původních karet, což dává $\binom{r+k-r-1}{s} = \binom{k-1}{s}$, což je právě počet kombinací s–tého stupně (bez opakování) ze všech žolíků. Tím je věta dokázána.

Druhý přístup (bez matematické indukce): Na množině

$$S = \{a_1, \dots, a_n\},$$

ze které vybíráme kombinace, si zafixujeme uvedené pořadí prvků a pro naše volby prvků z S si připravíme n přihrádek, do kterých si již předem dáme v námi zvoleném pořadí po právě jednom prvku z S.

Jednotlivé volby $x_i \in S$ přidáváme do přihrádky, která již tento prvek obsahuje. Nyní si uvědomme, že pro rozpoznání původní kombinace nám stačí vědět, kolik je prvků v jednotlivých přihrádkách. Například,

$$a \mid bbb \mid cc \mid d \ \simeq \ * \mid *** \mid ** \mid *,$$

vypovídá o volbě b, b, c z množiny $S = \{a, b, c, d\}$.

V obecném případě výběru k prvků z n možných tedy máme řetězec $n+k$ znaků a počet $C(n,k)$ je roven počtu možných umístění přihrádek | mezi jednotlivé znaky. To odpovídá výběru $n-1$ pozic z $n+k-1$ možných. Protože je

$$\binom{n+k-1}{k} = \binom{n+k-1}{n+k-1-k} = \binom{n+k-1}{n-1},$$

je věta dokázána i podruhé. □

3. Diferenční rovnice

V předchozích odstavcích jsme viděli vzorce, které zadávaly hodnotu skalární funkce definované na přirozených číslech (faktoriál) nebo dvojicích čísel (binomická čísla) pomocí předcházejících hodnot. Zatímco v odstavci 1.5 jsou kombinační čísla definována přímo spočítatelným výrazem, lze rozumět vztahům v 1.8 také tak, že místo hodnoty naší funkce zadáváme její změnu při odpovídající změně nezávislé proměnné.

Takto se skutečně velice často postupuje při matematické formulaci modelů, které popisují reálné systémy v ekonomice, biologii apod. My si tu povšimneme jen několika jednoduchých případů a budeme se k této tématice postupně vracet.

1.7 **1.9. Lineární diferenční rovnice prvního řádu.** Obecnou *diferenční rovnicí prvního řádu* rozumíme výraz

$$f(n+1) = F(n, f(n)),$$

kde F je známá skalární funkce závislá na dvojicích přirozených čísel. Známe–li „počáteční" hodnotu $f(0)$, můžeme spočítat $f(1) = F(0, f(0))$, poté $f(2) = F(1, f(1))$ atd. Tímto postupným způsobem můžeme tedy nakonec spočítat hodnotu $f(n)$ pro libovolné $n \in \mathbb{N}$. Všimněme si, že tato úvaha je podobná konstrukci přirozených čísel z prázdné množiny nebo principu matematické indukce.

Jako příklad může sloužit definiční formule pro faktoriál, tj.

$$(n+1)! = (n+1) \cdot n!$$

Vidíme, že skutečně vztah pro $f(n+1)$ závisí na n i na hodnotě $f(n)$.

Dalším obzvlášť jednoduchým příkladem je $f(n) = C$ pro nějaký pevný skalár C a všechna n a tzv. *lineární diferenční rovnice*

e1.4 (1.6) $$f(n+1) = a \cdot f(n) + b,$$

kde $a \neq 0$, a b jsou známé skaláry.

Takovou diferenční rovnici umíme snadno řešit, je-li $b = 0$. Pak se totiž jedná o dobře známou rekurentní definici geometrické posloupnosti a platí

$$f(1) = af(0), \quad f(2) = af(1) = a^2 f(0) \quad \text{atd.}$$

Máme tedy pro všechna n

$$f(n) = a^n f(0).$$

To je např. vztah pro tzv. Malthusiánský model populačního růstu, který vychází z představy, že za zvolený časový interval vzroste populace s konstantní úměrou a vůči předchozímu stavu.

Dokážeme si obecný výsledek pro rovnice prvního řádu, které se podobají lineárním, ale připouští proměnné koeficienty a a b,

e1.5 (1.7) $$f(n+1) = a_n \cdot f(n) + b_n.$$

Nejdřívě se ale zamysleme, co mohou takové rovnice popisovat.

Lineární diferenční rovnici (1.6) můžeme pěkně interpretovat jako matematický model pro spoření nebo splácení úvěru s pevnou úrokovou mírou a a pevnou splátkou b (tyto dva případy se liší pouze znaménkem u parametru b).

S proměnnými parametry dostáváme obdobný model,

ovšem s proměnlivými jak úroky, tak splátkami. Můžeme si představit třeba n jako počet měsíců, a_n bude vyjadřovat úrokovou míru v měsíci n, b_n příslušnou splátku v měsíci n.

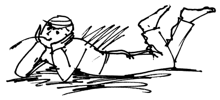
Neděste se zdánlivě složitého sčítání a násobení v následujícím výsledku. Jde o typický příklad technického matematického tvrzení, kdy těžké je „uhodnout“, jak zní. Naopak důkaz je už pak jen docela snadné cvičení na základní vlastnosti skalárů a matematickou indukci. Skutečně zajímavé jsou teprve důsledky, viz 1.11 níže.

Ve formulaci používáme vedle obvyklých znaků pro součet $\sum$ také obdobné znaky pro součin $\prod$. V dalším budeme vždy používat také konvenci, že pokud u součtu je množina uvedených indexů prázdná, pak je součet nula, zatímco u součinu je ve stejném případě výsledek jedna.

1.8 **1.10. Tvrzení.** *Obecné řešení diferenční rovnice (1.7) prvního řádu s počáteční podmínkou $f(0) = y_0$ je dáno vztahem*

e1.6 (1.8) $$f(n) = \left(\prod_{i=0}^{n-1} a_i\right) y_0 + \sum_{j=0}^{n-2}\left(\prod_{i=j+1}^{n-1} a_i\right) b_j + b_{n-1}.$$

Důkaz. Tvrzení dokážeme matematickou indukcí.



Zjevně tvrzení platí pro $n = 1$, kdy se jedná právě o definiční vztah $f(1) = a_0 y_0 + b_0$.

Předpokládáme-li, že tvrzení platí pro nějaké pevně zvolené n, můžeme snadno spočíst:

$$\begin{aligned} f(n+1) &= a_n\left(\left(\prod_{i=0}^{n-1} a_i\right) y_0 + \sum_{j=0}^{n-2}\left(\prod_{i=j+1}^{n-1} a_i\right) b_j + b_{n-1}\right) \\ &\quad + b_n \\ &= \left(\prod_{i=0}^{n} a_i\right) y_0 + \sum_{j=0}^{n-1}\left(\prod_{i=j+1}^{n} a_i\right) b_j + b_n, \end{aligned}$$

jak se přímo vidí roznásobením výrazů. □

Opět si všimněme, že jsme pro důkaz nepotřebovali o použitých skalárech nic víc než vlastnosti komutativního okruhu.

1.9 **1.11. Důsledek.** *Obecné řešení lineární diferenční rovnice (1.6) s $a \neq 1$ a počáteční podmínkou $f(0) = y_0$ je*

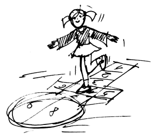
e1.7 (1.9) $$f(n) = a^n y_0 + \frac{1 - a^n}{1 - a} b.$$

Důkaz. Dosazením konstantních hodnot za a_i a b_i do obecného vzorce (1.8) dostáváme

$$f(n) = a^n y_0 + b\left(1 + \sum_{j=0}^{n-2} a^{n-j-1}\right).$$

Pro vyčíslení součtu součinů v druhém sčítanci si je třeba všimnout, že se jedná o výrazy $(1 + a + \cdots + a^{n-1})b$. Součet této geometrické řady spočteme ze vztahu $1 - a^n = (1 - a)(1+a+\cdots+a^{n-1})$ a dostaneme právě požadovaný výsledek. □

Všimněme si, že pro výpočet součtu geometrické řady



jsme potřebovali existenci inverze pro nenulové skaláry. To bychom nad celými čísly neuměli. Poslední výsledek tedy platí pro pole skalárů a můžeme jej bez problému použít pro lineární diferenční rovnice, kde koeficienty a, b a počáteční podmínka $f(0) = y_0$ jsou racionální, reálné nebo komplexní, ale také nad okruhem zbytkových tříd $\mathbb{Z}_k$ s prvočíselným k (zbytkové třídy budeme definovat v odstavci 1.41).

Pozoruhodné je, že ve skutečnosti vzorec (1.9) platí i s celočíselnými koeficienty a počáteční podmínkou. Pak totiž předem víme, že všechny $f(n)$ budou také celočíselné, a celá čísla jsou podmnožinou v číslech racionálních. Musí proto nutně náš vzorec dávat ta správná celočíselná řešení.

tady to asi není šikovné — příklady na zbytkové třídy snad budou v druhém sloupci už dříve, nejlépe by bylo i z tohoto udělat příklad a odtud to přesunout (nebo úplně vypustit)

Při pozornějším pohledu na důkaz je zřejmé, že $1 - a^n$ je vždy dělitelné $1 - a$, takže nás poslední pozorování nemělo překvapit. Nicméně je vidět, že třeba nad skaláry ze $\mathbb{Z}_4$ a třeba $a = 3$ už neuspějeme, protože pak $1 - a = 2$ je dělitelem nuly.

1.11

1.12. Nelineární příklad. Vraťme se na chvíli k rovnici prv-

ního řádu (1.6), kterou jsme použili na velice primitivní model populačního růstu závisející přímo úměrně na okamžité velikosti populace p. Na první pohled je zřejmé, že takový model vede při úměře $a > 1$ k příliš rychlému a hlavně neomezenému růstu.

Realističtější model bude mít takto úměrnou změnu populace $\Delta p(n) = p(n + 1) - p(n)$ jen při malých hodnotách p, tj. $\Delta p/p \sim r > 0$. Pokud tedy budeme chtít nechat růst populaci o 5% za období při malém p, budeme r volit $0,05$. Při určité limitní hodnotě $p = K > 0$ ale naopak už populace neroste a při ještě větších už klesá (třeba protože zdroje pro její obživu jsou omezené, jedinci ve veliké populaci si navzájem překáží apod.).

Předpokládejme, že právě hodnoty $y_n = \Delta p(n)/p(n)$ se v závislosti na $p(n)$ mění lineárně. Graficky si tedy tuto závislost můžeme představit jako přímku v rovině proměnných p a y, která prochází body $[0, r]$ (tj. při $p = 0$ máme $y = r$) a $[K, 0]$ (což dává druhou podmínku, že při $p = K$ se populace nemění). Položíme proto

$$y = -\frac{r}{K} p + r.$$

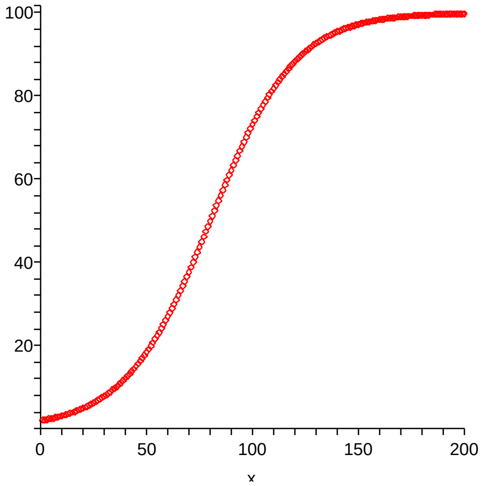
Dosazením y_n za y a $p(n)$ za p dostáváme

$$\frac{p(n + 1) - p(n)}{p(n)} = -\frac{r}{K} p(n) + r,$$

tj. roznásobením dostáváme diferenční rovnici prvního řádu (kde hodnota $p(n)$ vystupuje v první i v druhé mocnině)

e1.7a (1.10) $$p(n+1) = p(n)\big(1 - \frac{r}{K}p(n) + r\big).$$

Zkuste si promyslet nebo vyzkoušet chování tohoto modelu pro různé hodnoty r a K. Na obrázku je průběh hodnot pro parametry $r = 0,05$ (tj. pětiprocentní nárůst v ideálním stavu), $K = 100$ (tj. zdroje limitují hodnotu na 100 jedinců) a $p(0)$ jsou dva jedinci.



Všimněme si, že počáteční přibližně exponenciální růst se skutečně později zlomí a hodnota se postupně blíží kýženému limitu 100 jedinců. Pro p blízké jedné a K daleko větší než r bude pravá strana rovnice (1.10) přibližně $p(n)(1+r)$, tzn. chování je obdobné Malthusiánskému modelu. Naopak při p přibližně K bude pravá strana přibližně $p(n)$. Pro větší počáteční hodnoty p než K budou hodnoty klesat, pro menší než K růst, takže systém bude zpravidla postupně oscilovat kolem hodnoty K.

4. Pravděpodobnost

Teď se podíváme na jiný obvyklý případ skalárních hodnot funkcí – sledované hodnoty často nejsou známy ani explicitně vzorcem, ani implicitně nějakým popisem. Jsou výsledkem nějaké nahodilosti a my se snažíme popsat s jakou *pravděpodobností* nastane ta či ona možnost.

1.12 **1.13. Co je pravděpodobnost?** Jako jednoduchý příklad může sloužit obvyklé házení kostkou se šesti stěnami s označeními

$$1,\ 2,\ 3,\ 4,\ 5,\ 6.$$

Pokud popisujeme matematický model takového házení „poctivou“ kostkou, budeme očekávat a tudíž i předepisovat, že každá ze stran padá stejně často. Slovy to vyjadřujeme „každá předem vybraná stěna padne s pravděpodobností $\frac{1}{6}$“.

Pokud ale si třeba sami nožíkem vyrobíme takovou kostku z kusu dřeva, je jisté, že skutečné relativní četnosti výsledků nebudou stejné. Pak můžeme z velikého počtu pokusů usoudit na relativní četnosti jednotlivých výsledků hodů a tyto ustanovit jako pravděpodobnosti v našem matematickém popisu. Nicméně při sebevětším počtu pokusů nemůžeme vyloučit možnost, že se náhodou povedla velice nepravděpodobná kombinace výsledků a že jsme proto náš matematický model skutečnosti pro naši kostku nevybrali dobře.

V dalším budeme pracovat s abstraktním matematickým popisem pravděpodobnosti v nejjednodušším

přiblížení. To, do jaké míry je takový popis adekvátní pro konkrétní pokusy či jiný problém, je záležitostí mimo samotnou matematiku. To ale neznamená, že by se takovým přemýšlením neměli zabývat matematikové (nejspíše ve spolupráci s jinými experty). Později se vrátíme k pravděpodobnosti coby teorii popisující chování nahodilých procesů nebo i plně determinovaných dějů, kde ovšem neznáme přesně všechny určující parametry.

Matematická statistika pak umožňuje posuzovat, do jaké míry lze očekávat, že vybraný model je ve shodě s realitou, resp. umožňuje určit parametry modelu tak, aby docházelo k co nejlepší shodě s pozorováním a zároveň umí odhadnout míru spolehlivosti zvoleného modelu.

K matematické pravděpodobnosti i statistice ovšem budeme potřebovat dosti rozsáhlý matematický aparát, který budeme mezitím několik semestrů budovat.

Na příkladu naší neumělé kostky si to můžeme představit tak, že v teorii pravděpodobnosti budeme pracovat s parametry p_i pro pravděpodobnost jednotlivých hodnot stran a budeme požadovat pouze aby všechny tyto pravděpodobnosti byly nezáporné a jejich součet byl

$$p_1 + p_2 + p_3 + p_4 + p_5 + p_6 = 1.$$

Při volbě konkrétních hodnot p_i pro konkrétní kostku pak v matematické statistice budeme schopni odhadnout s jakou spolehlivostí tento model naší kostce odpovídá.

Naším skromným cílem je teď pouze naznačit, jak abs-

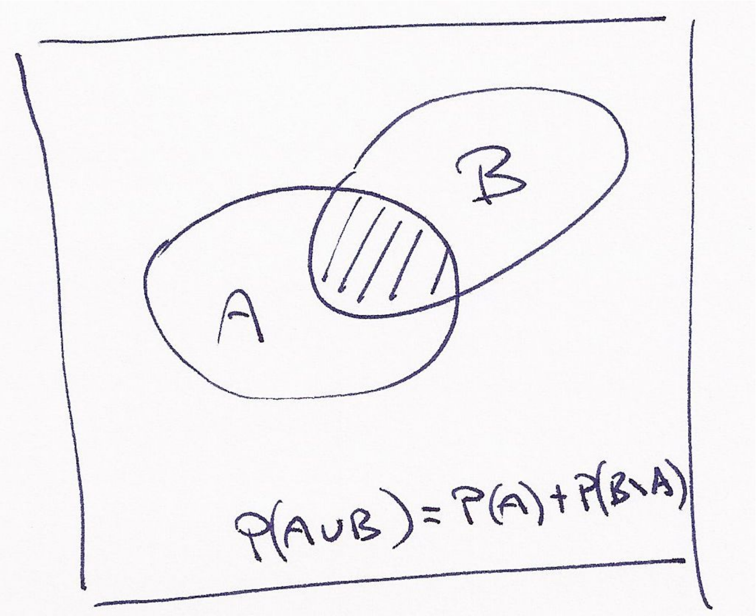
traktně zachytit pravděpodobnostní úvahy ve formalizovaných matematických objektech. Následující odstavce tak budou ve své podstatě pouhými cvičeními v jednoduchých operacích nad množinami a jednoduché kombinatorice (tj. výpočtech počtu možností, jak mohou být splněny dané podmínky kladené na konečné množiny prvků).

1.13

1.14. Náhodné jevy. Budeme pracovat s neprázdnou pevně zvolenou množinou Ω všech možných výsledků, kterou nazýváme *základní prostor*. Pro jednoduchost bude pro nás Ω konečná množina s prvky $\omega_1, \dots, \omega_n$, představujícími jednotlivé *možné výsledky*. Každá podmnožina $A \subset \Omega$ představuje možný *jev*. Systém podmnožin $\mathcal{A}$ základního prostoru se nazývá *jevové pole*, jestliže

- $\Omega \in \mathcal{A}$ (tj. základní prostor, je jevem),
- je-li $A, B \in \mathcal{A}$, pak $A \setminus B \in \mathcal{A}$ (tj. pro každé dva jevy je jevem i jejich množinový rozdíl),

- jsou-li $A, B \in \mathcal{A}$, pak $A \cup B \in \mathcal{A}$ (tj. pro každé dva jevy je jevem i jejich sjednocení).



Zjevně je i komplement $A^c = \Omega \setminus A$ jevu A jevem, který nazýváme *opačný jev* k jevu A. Průnik dvou jevů je opět jevem, protože pro každé dvě podmnožiny $A, B \subset \Omega$ platí

$$A \setminus (\Omega \setminus B) = A \cap B.$$

Slovy se tak dá jevové pole charakterizovat jako systém podmnožin (konečného) základního prostoru uzavřený na průniky, sjednocení a rozdíly. Jednotlivé množiny $A \in \mathcal{A}$ nazýváme *náhodné jevy* (vzhledem k $\mathcal{A}$).

Pro naše házení kostkou je $\Omega = \{1, 2, 3, 4, 5, 6\}$ a jevové pole je tvořeno všemi podmnožinami množiny Ω. Např. náhodný jev $\{1, 3, 5\}$ pak interpretujeme jako „padne liché číslo“.

Něco málo terminologie, která by měla dále připomínat souvislosti s popisem skutečných modelů:

- celý základní prostor Ω se nazývá *jistý jev*, prázdná podmnožina $\emptyset \in \mathcal{A}$ se nazývá *nemožný jev*,
- jednoprvkové podmnožiny $\{\omega\} \subset \Omega$ se nazývají *elementární jevy*,
- *společné nastoupení jevů* A_i, $i \in I$, odpovídá jevu $\cap_{i \in I} A_i$, *nastoupení alespoň jednoho z jevů* A_i, $i \in I$, odpovídá jevu $\cup_{i \in I} A_i$,
- $A, B \in \mathcal{A}$ jsou *neslučitelné jevy*, je-li $A \cap B = \emptyset$,
- jev A má za *důsledek* jev B, když $A \subset B$,

Přestavte si příklady všech uvedených pojmů pro jevový prostor popisující házení kostkou nebo obdobně pro házení mincí!

1.15. Definice. *Pravděpodobnostní prostor* je trojice

$(\Omega, \mathcal{A}, P)$, kde $\mathcal{A}$ je jevové pole podmnožin (konečného) základního prostoru Ω, na kterém je definována skalární funkce $P : \mathcal{A} \to \mathbb{R}$ s následujícími vlastnostmi:

- P je nezáporná, tj. $P(A) \geq 0$ pro všechny jevy A,

- P je aditivní, tj. $P(A \cup B) = P(A) + P(B)$, kdykoliv je $A, B \in \mathcal{A}$ a $A \cap B = \emptyset$,
- pravděpodobnost jistého jevu je 1, tj. $P(\Omega) = 1$.

Funkci P nazýváme *pravděpodobností* na jevovém poli $\mathcal{A}$.

Zjevně je okamžitým důsledkem našich definic řada prostých ale užitečných tvrzení. Např. pro všechny jevy platí

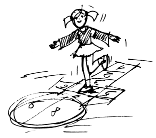
$$P(A^c) = 1 - P(A).$$

Dále můžeme matematickou indukcí snadno rozšířit aditivnost na jakýkoliv konečný počet vzájemně neslučitelných jevů $A_i \subset \Omega$, $i \in I$, tj.

$$P(\cup_{i \in I} A_i) = \sum_{i \in I} P(A_i),$$

kdykoliv $A_i \cap A_j = \emptyset$, pro všechna $i \neq j$, $i, j \in I$.

1.16. Definice. Nechť Ω je konečný základní prostor a nechť



jevové pole $\mathcal{A}$ je právě systém všech podmnožin v Ω. *Klasická pravděpodobnost* je pravděpodobnostní prostor $(\Omega, \mathcal{A}, P)$ s pravděpodobnostní funkcí

$$P : \mathcal{A} \to \mathbb{R}, \quad P(A) = \frac{|A|}{|\Omega|},$$

kde $|A|$ značí počet prvků množiny $A \in \mathcal{A}$.

Zjevně takto zadaná funkce skutečně definuje pravděpodobnost, ověřte si samostatně všechny požadované axiomy.

1.17. Sčítání pravděpodobností. U neslučitelných jevů je

sčítání pravděpodobností pro výskyt alespoň jednoho z nich přímo požadováno v základní definici pravděpodobnosti. Obecně je sčítání pravděpodobností pro výskyty jevů složité. Problém totiž je, že pokud jsou jevy slučitelné, částečně máme v součtu pravděpodobností započteny příznivé výskyty vícekrát.

Nejjednodušší je si nejprve představit situci se dvěma slučitelnými jevy A, B. Uvažme nejprve klasickou pravděpodobnost, kde jde vlastně o počítání prvků v podmnožinách. Pravděpodobnost výskytu alespoň jednoho z nich, tj. pravděpodobnost jejich sjednocení, je dána vztahem

e1.12a
$$P(A \cup B) = P(A) + P(B) - P(A \cap B) \tag{1.11}$$

protože ty prvky, které patří do množiny A i B, jsme nejprve započetli dvakrát a tak je musíme jednou odečíst.

Tentýž výsledek dostaneme i pro obecnou pravděpodobnost P na nějakém jevovém poli. Protože $A \cap B$ a $A \setminus B$ jsou nezávislé jevy,

$$P(A) = P(A \setminus B) + P(A \cap B),$$

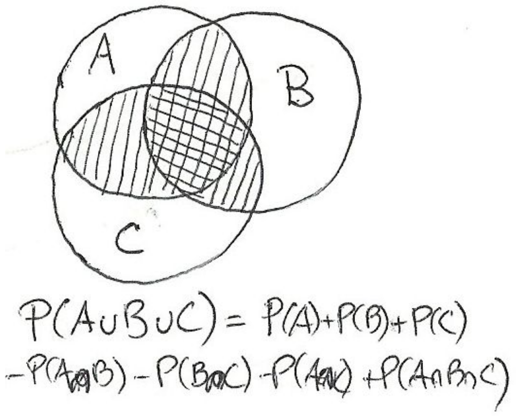
podobně pro B, ale také máme

$$P(A \cup B) = P(A \setminus B) + P(B \setminus A) + P(A \cap B).$$

Dosazením za pravděpodobnosti množinových rozdílů dostáváme opět vztah (1.11).

Následující věta je přímým promítnutím tzv. kombinatorického *principu inkluze a exkluze* do naší konečné pravděpodobnosti a říká, jakým způsobem vícenásobné započítávání výsledků kompenzovat v obecném případě.

Jde patrně o dobrý příklad matematického tvrzení, kde nejtěžší je najít dobrou formulaci a pak se dá říci, že (intuitivně) je tvrzení zřejmé.



Na obrázku je situace znázorněna pro tři množiny A, B, C a pro klasickou pravděpodobnost. Jednoduše šrafované oblasti v prostém součtu máme dvakrát, dvojitě šrafované třikrát. Pak ty jednoduše šrafované jednou odečteme, přitom ty dvojitě šrafované opět třikrát odečteme, proto je tam nakonec ještě jednou započteme.

Obecně, díky aditivní vlastnosti pravděpodobnosti, si můžeme představit, že každý jev rozložíme na elementární (tj. jednobodové) jevy, jakkoliv ve skutečnosti nemusí jednoprvkové podmnožiny do uvažovaného jevového pole patřit. Pak je pravděpodobnost každého jevu dána součtem pravděpodobností jednotlivých elementárních jevů do něj patřících a můžeme při vyjádření pravděpodobnosti nastoupení alespoň jednoho z jevů takto: sečteme všechny pravděpodobnosti výsledků pro všechna A_i zvlášť, pak ovšem musíme odečíst ty, které tam jsou započteny dvakrát (tj. prvky v průnicích dvou). Teď si ovšem dovolujeme odečíst příliš mnoho tam, kde ve skutečnosti byly prvky třikrát, tj. korigujeme přičtením pravděpodobností ze třetího členu, atd.

1.16 **Věta.** *Buďte $A_1, \dots, A_k \in \mathcal{A}$ libovolné jevy na základním prostoru Ω s jevovým polem $\mathcal{A}$. Pak platí*

$$\begin{aligned} P(\cup_{i=1}^k A_i) = &\sum_{i=1}^{k} P(A_i) - \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} P(A_i \cap A_j) \\ &+ \sum_{i=1}^{k-2} \sum_{j=i+1}^{k-1} \sum_{\ell=j+1}^{k} P(A_i \cap A_j \cap A_\ell) \\ &- \cdots \\ &+ (-1)^{k-1} P(A_1 \cap A_2 \cap \cdots \cap A_k). \end{aligned}$$

Důkaz. Aby se výše naznačený postup stal důkazem, je zapotřebí si ujasnit, že skutečně všechny korekce, tak jak jsou popsány, jsou skutečně s koeficienty jedna. Místo toho můžeme snáze dát dohromady formálnější důkaz matematickou indukcí přes počet k jevů, jejichž pravděpodobnosti sčítáme. Zkuste si průběžně porovnávat oba postupy, mělo by to vést k vyjasnění, co to znamená „dokázat“ a co „porozumět“.

Pro $k = 1$ tvrzení zjevně platí, vztah pro $k = 2$ je totožný s rovností (1.11) a tu jsme pro obecné pravděpodobnostní funkce již dokázali také.

Předpokládejme tedy, že věta platí pro všechny počty množin až do pevně zvoleného $k \geq 1$. Nyní můžeme pracovat v indukčním kroku se vztahem pro $k+1$ jevů, když sjednocení prvních k jevů bereme jako A ve vzorci (1.11) výše, zatímco zbývající jev hraje roli B:

$$\begin{aligned} P(\cup_{i=1}^{k+1} A_i) &= P\big((\cup_{i=1}^{k} A_i\big) \cup A_{k+1}) \\ &= \sum_{j=1}^{k} \Bigg((-1)^{j+1} \sum_{1 \leq i_1 < \cdots < i_j \leq k} P(A_{i_1} \cap \cdots \cap A_{i_j}) \Bigg) \\ &\quad + P(A_{k+1}) - P((A_1 \cup \cdots \cup A_k) \cap A_{k+1}). \end{aligned}$$

To už připomíná formuli pro $k + 1$ sčítaných jevů, nicméně nám ve velké sumě chybějí všechny výrazy obsahující A_{k+1} a člen s pravděpodobností současného nastoupení všech jevů. Zato nám však přebývá poslední člen. Tento člen výrazu můžeme nahradit výrazem

$$-P\big((A_1 \cap A_{k+1}) \cup \cdots \cup (A_k \cap A_{k+1})\big)$$

a pro tento výraz opět použít indukční předpoklad, tj. formuli ve větě. Při troše trpělivosti (a dostatečně velkém papíru na rozepsání všech členů) ověříme, že tím právě přidáme všechny dosud chybějící členy. □

1.17

1.18. Princip inkluze a exkluze. Speciálním případem předchozí věty je případ klasické pravděpodobnosti, kdy všechny konečné podmnožniny základního prostoru jsou jevy a všechny elementární jevy mají stejnou pravděpodobnost. Ve vzorci z předchozí věty pak všechny pravděpodobnosti dávají právě počet prvků příslušných podmnožin, až na společný faktor $\frac{1}{n}$, kde n je počet prvků základního prostoru.

Takto můžeme z věty 1.17 vyčíst následující tvrzení pro mohutnosti obecné konečné množiny M a jejích podmnožin $A_1, \dots, A_k$. Jako obvykle píšeme $|M|$ pro počet prvků množiny M.

Samozřejmě pro konečnou množinu M a její podmnožiny platí

$$|M \setminus (\cup_{i=1}^{k} A_i)| = |M| - | \cup_{i=1}^{k} A_i|.$$

Nyní můžeme dosadit z předchozí věty za mohutnost sjednocení na pravé straně a dostáváme tvrzení, kterému se říká *princip inkluze a exkluze.*

$$|M \setminus (\cup_{i=1}^{k} A_i)| =$$
$$= |M| + \sum_{j=1}^{k} \Bigg((-1)^j \sum_{1 \le i_1 < \cdots < i_j \le k} |A_{i_1} \cap \cdots \cap A_{i_j}| \Bigg).$$

Opět je snadné nakreslit si tvrzení pro dvě nebo tři množiny, viz obrázek před větou 1.17.

1.19. Nezávislé jevy. Vraťme se na chvíli k jednoduchému modelu dokonalé hrací kostky. Bude nás zajímat, jak mohou být jevy závislé.

Např. pravděpodobnost, že nastanou zároveň jevy „padne liché číslo" a „padne alespoň trojka", je $\frac{1}{3}$. To je totéž jako $\frac{1}{2} \cdot \frac{2}{3}$, tedy součin pravděpodobností jednotlivých jevů. To odpovídá představě, že můžeme nezávisle testovat obě podmínky a výsledná pravděpodobnost současného splnění bude dána součinem pravděpodobnostní dílčích. Naopak, jestliže budeme uvažovat neslučitelné jevy, jako jsou např. „padne sudé číslo" a „padne liché číslo", bude pravděpodobnost současného výskytu obou nulová, zatímco součin dílčích pravděpodobností nulový není. To odpovídá přestavě, že tyto dva jevy musí být závislé, protože výskyt jednoho z nich ten druhý už vylučuje. Samozřejmě může nastávat slabší závislost, např. jev „padne liché číslo" je důsledkem jevu „padne trojka" a proto také není dána pravděpodobnost společného výskytu těchto dvou jevů pomocí součinu.

Pro pravděpodobnosti P na libovolných jevových polích řekneme že jevy A a B jsou *stochasticky nezávislé* jestliže platí

$$P(A \cap B) = P(A) \cdot P(B).$$

Zkusme ale tutéž hru s kostkou s více jevy, třebas jev A „padne liché číslo", jev B „padne alespoň 3" a jev C „padne nejvýše 3". Pravděpodobnosti jsou $P(A) = \frac{1}{2}$, $P(B) = \frac{2}{3}$, $P(C) = \frac{1}{2}$, $P(A \cap B \cap C) = \frac{1}{6} = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{1}{2}$, ale po dvojicích dostáváme např. $P(A \cap C) = \frac{2}{3} \neq \frac{1}{2} \cdot \frac{1}{2}$.

Obecně tedy definujeme nezávislé jevy takto:

Definice. Uvažme libovolný pravděpodobnostní prostor

$(\Omega, \mathcal{A}, P)$ a v něm k jevů $A_1, \dots, A_k$. Řekneme, že tyto jevy jsou *stochasticky nezávislé* (vzhledem k pravděpodobnosti P), jestliže pro libovolné z nich vybrané jevy $A_{i_1}, \dots, A_{i_\ell}$, $1 \le \ell \le k$ platí

$$P(A_{i_1} \cap \cdots \cap A_{i_\ell}) = P(A_{i_1}) \cdot \ldots \cdot P(A_{i_\ell}).$$

Zjevně je každý podsystém stochasticky nezávislých jevů opět stochasticky nezávislý. Dále si pro dva stochasticky nezávislé jevy A, B spočtěme

$$P(A \cap B^c) = P(A \setminus B) = P(A) - P(A \cap B) =$$
$$= P(A)(1 - P(B)) = P(A)P(B^c).$$

Odtud už snadno dovodíme, že záměnou jednoho nebo více stochasticky nezávislých jevů za jejich opačné jevy obdržíme opět stochasticky nezávislé jevy.

Často je potřebná pravděpodobnost, že nastane alespoň jeden ze stochasticky nezávislých jevů, tzn. hledáme $P(A_1 \cup \cdots \cup A_k)$. Můžeme pak použít elementární vlastnosti množinových operací, tzv. de Morganova pravidla,

$$(\cup_{i\in I} A_i)^c = \cap_{i\in I} A_i^c$$
$$(\cap_{i\in I} A_i)^c = \cup_{i\in I} A_i^c$$

a dostáváme:

e1.14a

$$P(A_1 \cup \cdots \cup A_k) = 1 - P(A_1^c \cap \cdots \cap A_k^c) = \\ = 1 - (1 - P(A_1)) \ldots (1 - P(A_k)). \tag{1.12}$$

1.20. Podmíněná pravděpodobnost. Míru závislosti dvou jevů můžeme přeformulovat s představou, že zkoumáme jeden z nich za podmínky, že druhý nastal. U nezávislých by podmínka neměla mít žádný vliv. Např. „jaká je pravděpodobnost, že při hodu dvěmi kostkami padly dvě pětky, je-li součet hodnot deset?“. Formalizovat takový postup umíme následovně.

Definice. Nechť H je jev s nenulovou pravděpodobností v jevovém poli $\mathcal{A}$ v pravděpodobnostním prostoru $(\Omega, \mathcal{A}, P)$. *Podmíněná pravděpodobnost* $P(A|H)$ jevu $A \in \mathcal{A}$ vzhledem k hypotéze H je definována vztahem

$$P(A|H) = \frac{P(A \cap H)}{P(H)}.$$

Podmíněná pravděpodobnost

Jak je vidět přímo z definice, hypotéza H a jev A jsou skutečně nezávislé tehdy a jen tehdy, je-li $P(A) = P(A|H)$. Přímo z definice také vyplývá tzv. „věta o násobení pravděpodobností“. Máme-li dva jevy A_1, A_2 splňující $P(A_1 \cap A_2) > 0$, potom

$$P(A_1 \cap A_2) = P(A_2)P(A_1|A_2) = P(A_1)P(A_2|A_1).$$

Všechna tato čísla vyjadřují pravděpodobnost toho, že nastanou oba jevy A_1 i A_2, jenom jinými způsoby. Například v posledním případě nejprve sledujeme, zda nastane první jev. Potom za předpokladu, že ten první nastal, sledujeme zda nastane i ten druhý. Podobně, pro tři jevy A_1, A_2, A_3 splňující $P(A_1 \cap A_2 \cap A_3) > 0$, dostaneme

$$P(A_1 \cap A_2 \cap A_3) = P(A_1)P(A_2|A_1)P(A_3|A_1 \cap A_2).$$

Slovy to lze opět popsat tak, že pravděpodobnost výskytu všech tří jevů zároveň můžeme spočítat tak, že se nejprve zabýváme výskytem pouze prvního z nich, potom druhého za předpokladu, že první už nastal a naposledy třetího za předpokladu, že oba předešlé jevy již nastaly.

Máme-li obecný počet k jevů $A_1, \ldots, A_k$ splňujících $P(A_1 \cap \cdots \cap A_k) > 0$, pak věta říká následující:

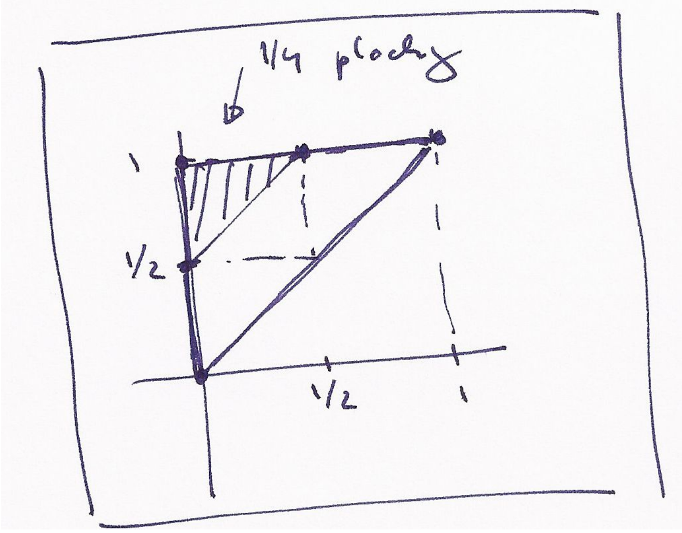
$$P(A_1 \cap \cdots \cap A_k) = P(A_1)P(A_2|A_1) \cdots P(A_k|A_1 \cap \cdots \cap A_{k-1}).$$

Skutečně, dle předpokladu jsou i pravděpodobnosti všech průniků, které jsou brány ve výrazu za hypotézy, nenulové. Pokrácením čitatelů a jmenovatelů získáme i napravo právě pravděpodobnost jevu odpovídajícího průniku všech uvažovaných jevů.

1.21. Geometrická pravděpodobnost. V praktických problémech se často setkáváme s daleko složitějšími modely, kde základní prostor není konečnou množinou. Nemáme momentálně k dispozici ani základní nástroje pro dostatečné zobecnění pojmu pravděpodobnosti, nicméně můžeme uvést alespoň jednoduchou ilustraci.

Uvažme rovinu $\mathbb{R}^2$ dvojic reálných čísel a v ní podmnožinu Ω se známým obsahem vol Ω (symbol „vol" je od anglického „volume", tj. obsah/objem). Příkladem může sloužit třeba jednotkový čtverec. Náhodné jevy budou reprezentovány podmnožinami $A \subset \Omega$ a za jevové pole $\mathcal{A}$ bereme nějaký vhodný systém podmnožin, u kterých umíme určit jejich obsah. Nastoupení nebo nenastoupení jevu je dáno výběrem bodu v Ω, kterým se trefíme nebo netrefíme do množiny reprezentující jev A.

Uvažme jako příklad problém, kdy náhodně vybereme dvě hodnoty $a < b$ v intervalu $[0, 1] \subset \mathbb{R}$. Všechny hodnoty a i b jsou stejně pravděpodobné a otázka zní „jaká je pravděpodobnost, že interval (a, b) bude mít velikost alespoň jedna polovina?". Volba čísel a, b je volbou libovolného bodu $[a, b]$ ve vnitřku trojúhelníku Ω s hraničními vrcholy $[0, 0]$, $[0, 1]$, $[1, 1]$ (viz obrázek).



Úlohu si můžeme představit jako popis problému, kdy se hodně unavený účastník večírku nad ránem pokouší dvěma řezy rozdělit párek na tři díly pro sebe a své dva kamarády. Jaká je pravděpodobnost, že se na někoho dostane aspoň půlka?

Odpověď je docela jednoduchá: Podobně jako u klasické pravděpodobnosti definujeme pravděpodobnostní funkci $P : \mathcal{A} \to \mathbb{R}$ vztahem

$$P(A) = \frac{\operatorname{vol} A}{\operatorname{vol} \Omega},$$

kde A jsou podmnožiny v rovině, které odpovídají námi vybraným jevům.

Potřebujeme tedy znát plochu podmnožiny, která odpovídá bodům s $b \geq a + \frac{1}{2}$, tj. vnitřku trojúhelníku A ohraničeného vrcholy $[0, \frac{1}{2}]$, $[0, 1]$, $[\frac{1}{2}, 1]$. Evidentně dostáváme $P(A) = \frac{1}{4}$.

Zkuste si samostatně odpovědět na otázku „pro jakou požadovanou minimální délku intervalu (a, b) dostaneme pravděpodobnost jedna polovina?“.

1.20a

1.22. Metody Monte Carlo. Jednou z účinných výpočetních metod přibližných hodnot je naopak simulace

známé takovéto pravděpodobnosti pomocí relativní četnosti nastoupení vhodně zvoleného jevu. Např. známá formule pro obsah kruhu o daném poloměru říká, že obsah jednotkového kruhu je roven právě konstantě

$$\pi = 3,1415\ldots,$$

která vyjadřuje poměr obsahu kruhu a druhé mocniny jeho poloměru. (Tady si také povšimněme východiska, které jsme nedokázali – proč by měl být obsah kruhu roven konstantnímu násobku druhé mocniny poloměru? Matematicky to budeme umět ukázat, až zvládneme tzv. integrování. Experimentálně si to ale můžeme ověřit níže uvedeným postupem s různými velikostmi strany čtverce.)

Pokud zvolíme za Ω jednotkový čtverec a za A průnik Ω a jednotkového kruhu se středem v počátku, pak vol $A = \frac{1}{4}\pi$. Máme-li tedy spolehlivý generátor náhodných čísel mezi nulou a jedničkou a počítáme relativní četnosti, jak často bude vzdálenost bodu $[a, b]$ (určeného vygenerovanou dvojicí a, b) od počátku menší než jedna, tj. $a^2 + b^2 < 1$, pak výsledek bude při velkém počtu pokusů s velikou jistotou dobře aproximovat číslo $\frac{1}{4}\pi$.

Numerickým postupům založeným na tomto principu se říká *metody Monte Carlo*.

5. Geometrie v rovině

V posledních odstavcích jsme intuitivně používali ele-

mentární pojmy z geometrie reálné roviny. Teď budeme podrobněji zkoumat, jak se vypořádávat s potřebou popisovat „polohu v rovině“, resp. dávat do souvislostí polohy různých bodů roviny.

Nástrojem k tomu budou opět zobrazení, tentokrát to ale budou velice speciální pravidla přiřazující dvojicím hodnot (x, y) dvojice $(w, z) = F(x, y)$. Zároveň půjde o předzvěst úvah z oblasti matematiky, které se říká *lineární algebra* a kterou se budeme podrobně zabývat v dalších třech kapitolách.

1.23

1.23. Vektorový prostor $\mathbb{R}^2$. Podívejme se na „rovinu“ jakožto na množinu dvojic reálných čísel $(x, y) \in \mathbb{R}^2$. Budeme jim říkat *vektory* v $\mathbb{R}^2$. Pro takové vektory umíme definovat sčítání „po složkách“, tj. pro vektory $u = (x, y)$ a

$v = (x', y')$ klademe

$$u + v = (x + x', y + y').$$

Protože pro jednotlivé složky platí všechny vlastnosti komutativní grupy, evidentně budou tyto vlastnosti platit i pro naše nové sčítání vektorů. Zejména tedy máme tzv. *nulový vektor* $0 = (0, 0)$, jehož přičtením k jakémukoliv vektoru v dostaneme opět vektor v. Záměrně teď používáme tentýž symbol 0 pro vektor i jeho skalární složky — z kontextu je vždy jasné, jakou „nulu“ máme kdy na mysli.

Dále definujeme násobení vektorů a skalárů tak, že pro $a \in \mathbb{R}$ a $v = (x, y) \in \mathbb{R}^2$ klademe

$$a \cdot v = (ax, ay).$$

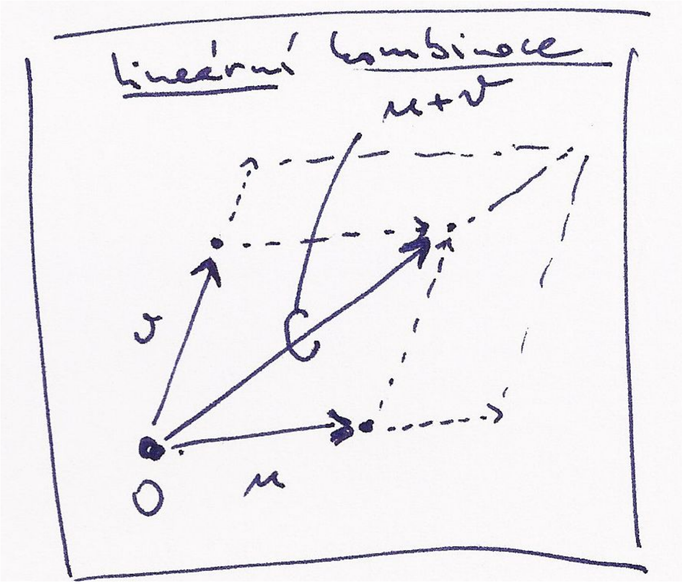
Zpravidla budeme znak $\cdot$ vynechávat a pouhé zřetězení znaků $a\,v$ bude označovat skalární násobek vektoru. Přímo se ověří další vlastnosti pro násobení skaláry a, b a sčítání vektorů u, v, např.

$$a\,(u+v) = a\,u + a\,v, \;\; (a+b)u = a\,u + b\,u, \;\; a(b\,u) = (ab)u,$$

kde opět používáme stejný znak plus pro sčítání vektorů i skalárů.

Tyto operace si můžeme dobře představit, jestliže uvažujeme vektory v jako šipky začínající v počátku $0 = [0, 0]$ a končící v bodě $[x, y]$ v rovině.

Takové šipky pak můžeme přikládat jednu za druhou a to přesně odpovídá sčítání vektorů. Násobení skalárem a pak odpovídá natažení dané šipky na a–násobek.



Nyní můžeme udělat podstatný krok: jestliže si zapamatujeme dva významné vektory $e_1 = (1, 0)$ a $e_2 = (0, 1)$, pak každý jiný vektor dostaneme jako

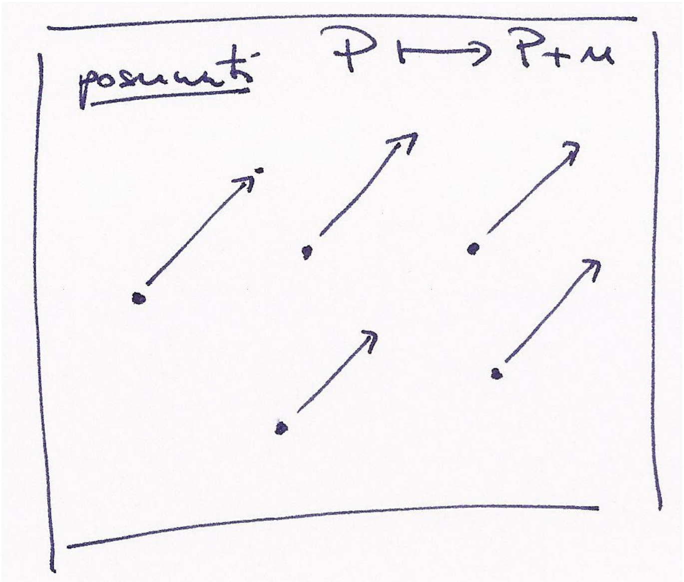
$$u = (x, y) = x\,e_1 + y\,e_2.$$

Výrazu napravo říkáme *lineární kombinace vektorů* e_1 a e_2. Dvojici vektorů $\underline{e} = (e_1, e_2)$ říkáme *báze* vektorového prostoru $\mathbb{R}^2$.

Jestliže si ale vybereme jiné dva vektory u, v, které nejsou jeden násobek druhého, tj. jinou bázi v $\mathbb{R}^2$, budeme moci udělat totéž. Lineární kombinace $w = x\,u + y\,v$ nám pro všechny různé dvojice (x, y) dá právě všechny vektory w v rovině.

Nakonec můžeme nahlížet vektory jako naše šipky v abstraktní poloze, tj. zapomeneme na ztotožnění bodů v rovině s dvojicemi čísel. Jenom budou naše šipky všechny „upoutány" v bodě 0, který je zároveň nulovým vektorem. Zůstanou nám operace sčítání a násobení skaláry a teprve volbou báze e_1, e_2 ztotožníme naši rovinu šipek s $\mathbb{R}^2$.

1.24. Afinní rovina. Když si pevně vyvolíme nějaký vektor $u \in \mathbb{R}^2$, můžeme jej přičítat (tj. coby šipku přikládat) k libovolnému bodu $P = [x, y]$. Máme tak tedy s pevným vektorem definované *posunutí*, které každý bod roviny P zobrazí na $P + u$.

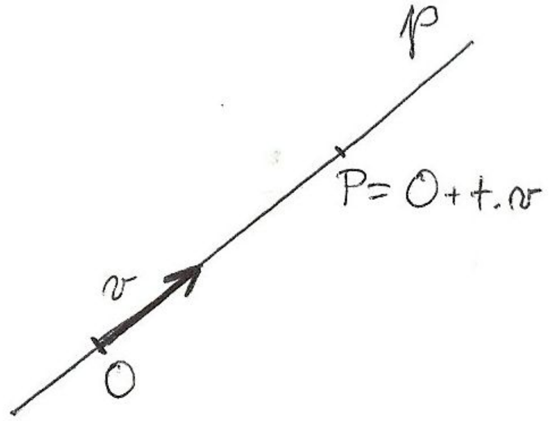


Zkusme teď úplně zapomenout na souřadnice a vnímat celou rovinu jako množinu, na které fungují naše posunutí. Takovou množinu $A = \mathbb{R}^2$ si můžeme představit z pohledu pozorovatele, který sedí v některém pevně zvoleném místě (můžeme mu říkat třeba bod $O = [x_0, y_0] \in \mathbb{R}^2$). Předpokládejme, že ji vnímá jako nekonečnou desku bez jakýchkoliv zvolených měřítek a popisů a jenom ví, co to znamená posunout se o libovolný násobek nějakého vektoru $u \in \mathbb{R}^2$. Takové rovině budeme říkat „afinní rovina".

Aby mohl vidět kolem sebe „dvojice reálných čísel", musí si vybrat nějaký bod E_1, kterému řekne „bod [1, 0]" a jiný bod E_2, kterému začne říkat „bod [0, 1]". Jinými slovy, zvolí si bázi $e_1 = (1, 0)$, $e_2 = (0, 1)$ mezi vektory posunutí. Do všech ostatních se pak dostane tak, že poskočí „a–krát ve směru e_1" a pak „b–krát ve směru e_2" a takovému bodu bude říkat „bod $[a, b]$". Pokud to bude dělat obvyklým způsobem, nebude výsledek záviset na pořadí, tzn. může také napřed jít b–krát ve směru e_2 a pak teprve ve směru e_1.

To, co jsme popsali, se nazývá volba *(afinního) souřadného systému v rovině*, bod O je jeho *počátkem*, a obecně každý bod P roviny je ztotožněn s dvojicí čísel $[a, b]$, kterou také budeme psát jako *posunutí* $P - O$.

Budeme dále pracovat v pevně zvolených souřadnicích, tj. s dvojicemi reálných čísel, ale pro lepší orientaci budeme vektory zapisovat s kulatými závorkami místo hranatých u souřadnic bodů v afinní rovině.



1.24

1.25. Přímky v rovině. Když se náš pozorovatel umí posouvat o libovolný násobek pevného vektoru, pak také ví, co je to *přímka*.

Je to podmnožina $p \subset A$ v rovině taková, že existují bod O a nenulový vektor v takové, že

$$p = \{P \in A;\ P - O = t \cdot v,\ t \in \mathbb{R}\}.$$

Popišme si $P = P(t) \in p$ ve zvolených souřadnicích s volbou $v = (\alpha, \beta)$:

$$x(t) = x_0 + \alpha \cdot t, \quad y(t) = y_0 + \beta \cdot t.$$

Protože vektor $v = (\alpha, \beta)$ je nenulový, musí být aspoň jedno z čísel α, β různé od nuly. Když pro určitost předpokládáme, že třeba $\alpha \neq 0$, pak vyloučíme t z parametrického vyjádření pro x a y a jednoduchým výpočtem dostaneme

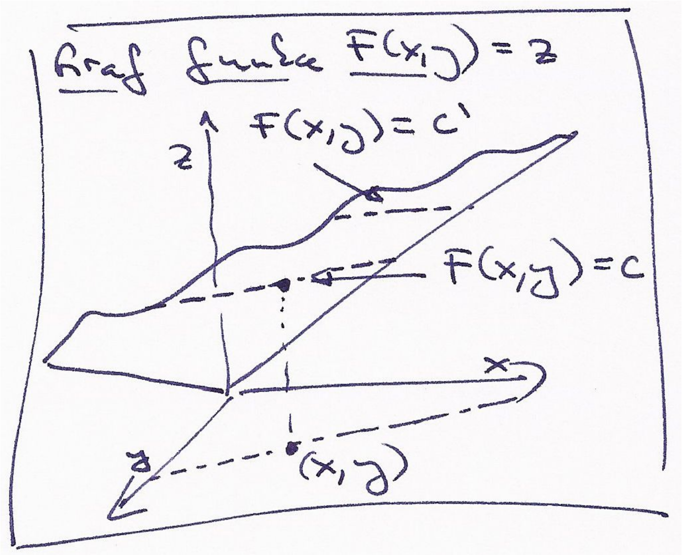
$$-\beta x + \alpha y = -\beta x_0 + \alpha y_0.$$

To je obecná rovnice přímky

e1.12 (1.13) $$ax + by = c,$$

se známým vztahem dvojice čísel $(a, b) = (-\beta, \alpha)$ a směrového vektoru přímky $v = (\alpha, \beta)$

e1.13 (1.14) $$a\alpha + b\beta = 0.$$



Výraz nalevo v rovnici přímky (1.13) můžeme vidět jako

skalární funkci F závislou na bodech v rovině a s hodnotami v $\mathbb{R}$, samu rovnici pak jako požadavek na její hodnotu. Časem uvidíme, že vektor (a, b) je v tomto případě právě směrem, ve kterém F nejrychleji roste. Proto bude směr kolmý na (a, b) právě tím směrem, ve kterém zůstává naše funkce F konstantní. Konstanta c pak určuje, kterou ze všech rovnoběžných přímek rovnice určuje.

Mějme nyní dvě přímky p a q a ptejme se po jejich průniku $p \cap q$. Ten bude popsán jako bod, splňující obě rovnice přímek současně. Pišme je takto

e1.14

$$\begin{aligned} ax + by &= r \\ cx + dy &= s. \end{aligned} \tag{1.15}$$

Opět můžeme levou stranu vnímat jako přiřazení, které každé dvojici souřadnic $[x, y]$ bodů P v rovině přiřadí vektor hodnot dvou skalárních funkcí F_1 a F_2 daných levými stranami jednotlivých rovnic (1.15). Můžeme tedy naše rovnice napsat jako jediný vztah $F(v) = w$, kde F je přiřazení, které vektor v popisující polohu obecného bodu v rovině (v našich souřadnicích) zobrazí na vektor zadaný levou stranou rovnic, a požadujeme, aby se toto zobrazení strefilo do předem zadané hodnoty $w = (r, s)$.

1.25

1.26. Lineární zobrazení a matice. Přiřazení F, se kterými

jsme pracovali při popisu průniku přímek, mají jednu velice podstatnou společnou vlastnost: respektují operace sčítání a násobení s vektory a skaláry, tj. respektují lineární kombinace:

$$F(a \cdot v + b \cdot w) = a \cdot F(v) + b \cdot F(w)$$

pro všechny $a, b \in \mathbb{R}$, $v, w \in \mathbb{R}^2$. Říkáme, že F je *lineární zobrazení* z $\mathbb{R}^2$ do $\mathbb{R}^2$, a píšeme $F : \mathbb{R}^2 \to \mathbb{R}^2$. Slovy lze podmínku také vyjádřit tak, že lineární kombinace vektorů se zobrazuje na tutéž lineární kombinaci jejich obrazů, tj. lineární zobrazení jsou ta zobrazení, která zachovávají lineární kombinace.

Se stejným chováním jsme se setkali i v rovnici (1.13) pro přímku, kde šlo o lineární zobrazení $F : \mathbb{R}^2 \to \mathbb{R}$ a jeho předepsanou hodnotu c. To je také důvodem, proč jsou hodnoty zobrazení $z = F(x, y)$ na obrázku vyobrazeny jako rovina v $\mathbb{R}^3$.

Stručně budeme zapisovat taková zobrazení pomocí tzv. *matic* a jejich násobení. Maticí rozumíme obdélníkové schéma skalárů, např.

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{nebo} \quad v = \begin{pmatrix} x \\ y \end{pmatrix},$$

hovoříme o (čtvercové) matici A a (sloupcovém) vektoru v. Jejich násobení definujeme takto:

$$A \cdot v = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Podobně, můžeme místo vektoru v zprava násobit jinou maticí B stejného rozměru jako je A. Prostě aplikujeme předchozí formule po jednotlivých sloupcích matice B a obrdržíme jako výsledek opět čtvercovou matici.

Neumíme násobit vektor v zprava maticí A protože nám nevychází počty skalárů na řádcích v s počty skalárů ve sloupcích A. Umíme však napsat vektor w do řádku skalárů (tzv. transponovaný vektor) $w^T = (a\ b)$ a ten zprava našimi maticemi A nebo vektory v již násobit umíme.

Snadno ověříme tzv. asociativitu násobení (propočítejte pro obecné matice A, B a vektor v detailně):

$$(A \cdot B) \cdot v = A \cdot (B \cdot v).$$

Místo vektoru v můžeme samozřejmě psát i libovolnou matici C správného rozměru. Stejně snadno je vidět i distributivita

$$A \cdot (B + C) = A \cdot B + A \cdot C,$$

neplatí však komutativita a existují „dělitelé nuly“. Např.

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Zejména vidíme, že násobení vektorů pevnou maticí zadává linerání zobrazení, a naopak, pomocí hodnot lineárního zobrazení F na dvou pevných vektorech báze už dostaneme celé příslušné zobrazení. Body v rovině jsou tedy obecně vzory hodnot lineárních zobrazení F roviny do roviny, přímky jsou obecně vzory hodnot lineárních zobrazení z roviny do reálné přímky $\mathbb{R}$. S maticemi a vektory umíme rovnice pro přímky a body psát

$$w^T \cdot v = \begin{pmatrix} a & b \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = c$$

$$A \cdot v = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} r \\ s \end{pmatrix} = u.$$

Samozřejmě, ve zvláštních situacích tomu tak být nemusí. Tak třeba průnikem dvou stejných přímek je opět sama přímka (a vzorem vhodné hodnoty pro takové lineární zobrazení bude celá přímka), nulové zobrazení má za vzor nuly celou rovinu.

V prvém případě to poznáme tak, že jsou nalevo v rovnicích (1.15) stejné výrazy až na skalární násobek (nebo jinak řečeno, řádky matice A jsou stejné až na skalární násobek). V takovém případě buď nebude v průniku příslušných přímek žádný bod (rovnoběžné různé přímky) nebo tam budou všechny body přímky (stejné přímky). Tuto podmínku může vyjádřit tak, že poměry a/c a b/d musí být stejné, neboli

e1.15 (1.16)
$$ad - bc = 0.$$

Všimněme si, že toto vyjádření už zahrnuje i případy, kdy c nebo d je nulové.

1.25a

1.27. Determinant matice. Výrazu nalevo v (1.16) říkáme *determinant* matice A a píšeme pro něj

$$\det A = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Naši diskusi teď můžeme vyjádřit takto:

Tvrzení. *Determinant je skalární funkce* $\det A$ *definovaná na všech maticích A a rovnice $A \cdot v = u$ je jednoznačně řešitelná, právě když je* $\det A \neq 0$.

Zkuste promyslet, že pro tuto úvahu bylo podstatné, že

pracujeme s polem skalárů. Například nad celými čísly obecně neplatí. Když prostě spočteme řešení rovnic s celočíselnými koeficienty (tj. matice A má pouze celočíselné vstupy), tak toto řešení celočíselné být nemusí.

1.25b

1.28. Afinní zobrazení. Podíváme se, jak maticová symbo-

lika umožňuje pracovat s jednoduchými zobrazeními v afinní rovině. Viděli jsme, že násobením maticí je dáno linerání zobrazení. Posunutí v afinní rovině $\mathbb{R}^2$ o pevný vektor $t = (r, s) \in \mathbb{R}^2$ umíme v maticové formě také snadno zapsat:

$$P = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto P + t = \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} x + r \\ y + s \end{pmatrix}.$$

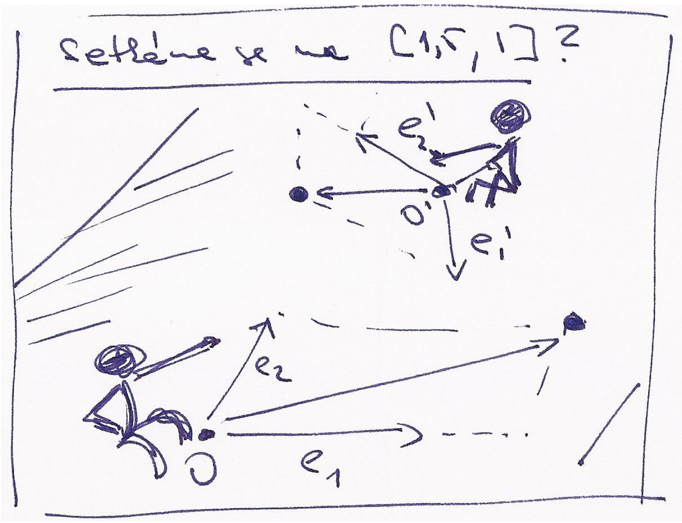
Jestliže k výsledku lineárního zobrazení ještě dovolíme přičíst pevný vektor $t = (r, s)$, pak naše zobrazení bude mít tvar

$$v = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto A \cdot v + t = \begin{pmatrix} ax + by + r \\ cx + dy + s \end{pmatrix}.$$

Takto jsou popsána právě všechna tzv. *afinní zobrazení roviny* do sebe.

Taková zobrazení nám umožní přepočítávání souřad-

nic vzniklých různými volbami počátků a bází směrů pro posunutí. Co se stane, když náš pozorovatel z odstavce 1.23 bude tutéž rovinu shlížet z jiného bodu nebo si aspoň vybere jiné body E_1, E_2? Zkuste si promyslet, že na úrovni souřadnic to skutečně bude právě změna realizovaná pomocí afinního zobrazení. Časem budeme vidět obecné důvody, proč tomu tak je ve všech dimenzích.



1.26

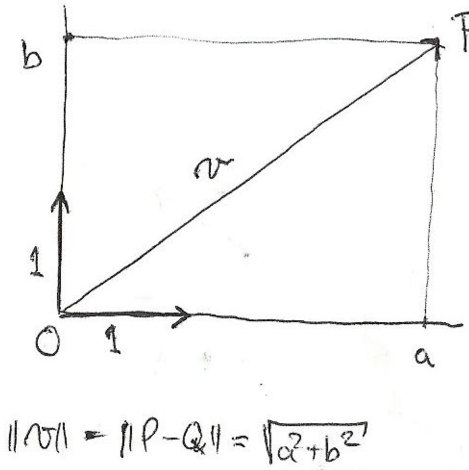
1.29. Euklidovská rovina. Přidejme nyní schopnost našeho pozorovatele vidět vzdálenosti. Např. může věřit obvyklému vzorci pro velikost vektoru $v = (a, b)$

$$\|v\| = \sqrt{a^2 + b^2}$$

v jím zvolených afinních souřadnicích. Okamžitě pak můžeme definovat pojmy jako jsou úhel a otočení v rovině.

Jednoduše si to můžeme představit takto: náš člověk se

rozhodne o nějakých bodech E_1 a E_2, že jsou od něj ve vzdálenosti jedna, a zároveň si řekne, že jsou na sebe kolmé. Vzdálenosti ve směrech souřadných os pak jsou dány příslušným poměrem, obecně používá Euklidovu (nebo Pythagorovu) větu. Odtud vyjde právě výše uvedený vzorec.



Náš pozorovatel roviny může samozřejmě postupovat i jinak. Může použít nějaký standard pro skutečné měření vzdálenosti bodů P a Q v rovině a říci, že to je právě velikost vektoru $Q - P$, který potřebujeme na posunutí z P do Q. Pak si vybere nějaký z vektorů, které skutečně mají velikost 1 a třeba pomocí trojúhelníku o stranách s velikostmi 3, 4 a 5 zkonstruuje kolmý vektor o velikosti jedna a dále pokračuje jako výše.

Euklidovská rovina je afinní rovina s výše zavedeným pojmem vzdálenosti.

1.26a

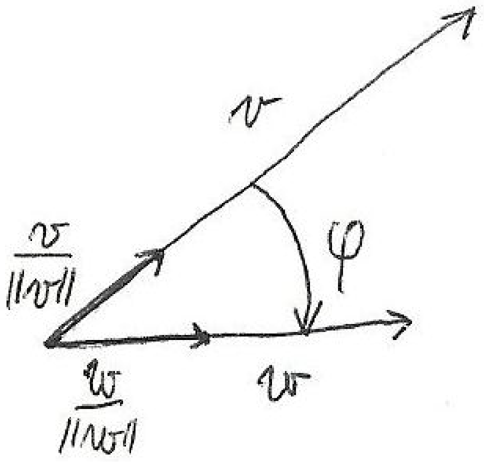
1.30. Úhel vektorů. Jak jsme již používali při diskusi komplexních čísel coby bodů v rovině, tzv. goniometrická funkce $\cos\varphi$ je dána hodnotou reálné první souřadnice jednotkového vektoru, jehož úhel s vektorem $(1, 0)$ je φ.

Zjevně je pak druhá souřadnice takového vektoru dána reálnou hodnotou $0 \le \sin\varphi \le 1$ splňující

$$(\cos\varphi)^2 + (\sin\varphi)^2 = 1.$$

Obecně pak pro dva vektory v a w můžeme jejich úhel popsat pomocí souřadnic $v = (v_x, v_y)$, $w = (w_x, w_y)$ takto:

$$\cos\varphi = \frac{v_x w_x + v_y w_y}{\|v\| \cdot \|w\|}.$$



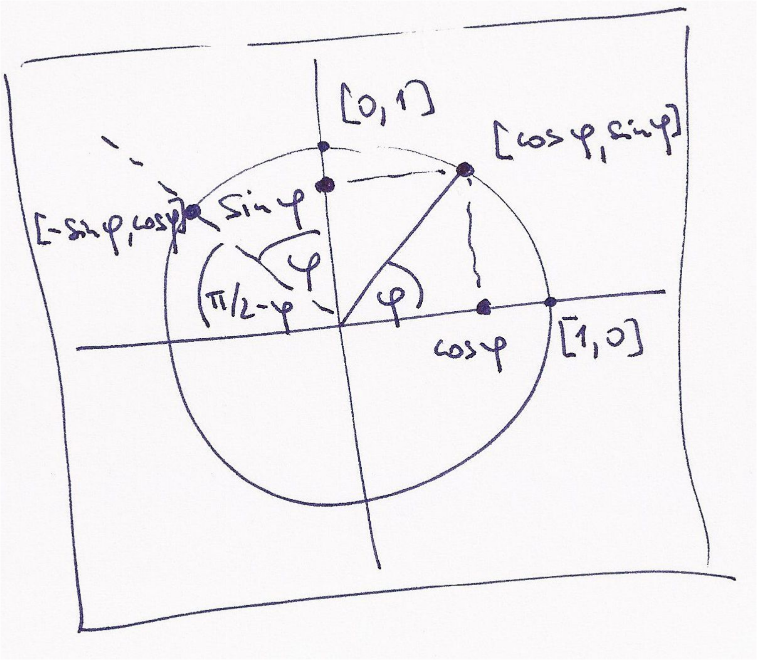
Tento vztah si snadno ověříme, pokud věříme, že otočení roviny kolem počátku nemění úhly. Pak totiž můžeme napřed libovolně zvolené vektory vynásobit vhodnými skaláry tak, abychom dostali vektory velikosti jedna (náš vzorec totiž po násobení vektorů libovolnými skaláry dává pochopitleně neměnné výsledky). Poté můžeme vhodným otočením naší roviny dosáhnout toho, že první z vektorů bude právě prvním bázovým vektorem $(1, 0)$. Potom dává náš vzorec

$$\cos\varphi = \frac{w_x}{\|w\|},$$

což je pouze opakováním definice funkce $\cos\varphi$.

1.26b

1.31. Rotace kolem bodu v rovině. Matici libovolného známého zobrazení $F : \mathbb{R}^2 \to \mathbb{R}^2$ lze vcelku snadno uhádnout: Je-li totiž výsledkem matice se sloupci (a, c) a (b, d), pak první sloupec dostaneme nasobením této matice s prvním vektorem báze $(1, 0)$ a druhý je vyčíslením na druhém vektoru báze $(0, 1)$.



Z obrázku je proto vidět, že pro rotaci o úhel ψ proti směru hodinových ruček jsou v matici sloupce

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\psi \\ \sin\psi \end{pmatrix} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin\psi \\ \cos\psi \end{pmatrix}$$

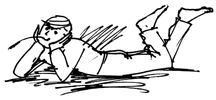
Směr proti směru hodinových ruček označujeme jako *kladný směr rotace*, opačný je pak záporný. Proto dostáváme tvrzení:

Rotace o předem daný úhel ψ v kladném směru kolem počátku souřadnic je dána maticí R_ψ:

$$v = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto R_\psi \cdot v = \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

Matice rotace

Nyní, když už víme, jak vypadá matice otočení v rovině,



můžeme ověřit, že otočení zachovává vzdálenosti a úhly (definované předešlým vzorcem). Označíme-li obraz vektoru v jako

$$v' = \begin{pmatrix} v'_x \\ v'_y \end{pmatrix} = R_\psi \cdot v = \begin{pmatrix} v_x \cos\psi - v_y \sin\psi \\ v_x \sin\psi + v_y \cos\psi \end{pmatrix},$$

a podobně $w' = R_\psi \cdot w$, pak lze snadno přepočítat, že opravdu platí

$$\|v'\| = \|v\|$$

$$v'_x w'_x + v'_y w'_y = v_x w_x + v_y w_y.$$

Předchozí výraz lze pomocí vektorů a matic napsat následovně

$$(R_\psi \cdot w)^T (R_\psi \cdot v) = w^T v.$$

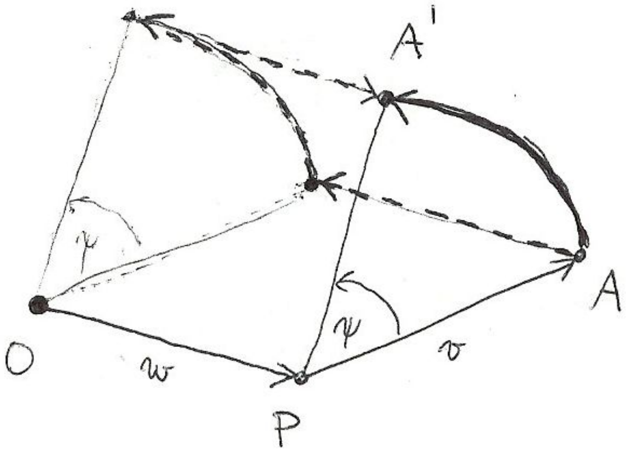
Transponovaný vektor $(R_\psi \cdot w)^T$ je roven $w^T \cdot R_\psi^T$, kde R_ψ^T je tzv. transponovaná matice k matici R_ψ. To je matice, jejíž řádky tvoří sloupce původní matice a sloupce naopak tvoří řádky původní matice. Vidíme tedy, že matice otočení splňují vztah $R_\psi^T \cdot R_\psi = I$, matice I (někdy píšeme prostě 1 a máme tím na mysli jednotku v okruhu matic), je tzv. *jednotková matice*

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

Tím jsme odvodili pozoruhodné tvrzení — matice F s vlastností, že $F \cdot R_\psi = I$ (budeme takové říkat inverzní matice k matici rotace R_ψ) je maticí transponovanou k původní. To je logické, neboť inverzní zobrazení k rotaci o úhel ψ je opět rotace, ale o úhel $-\psi$, tj. inverzní matice R_ψ^T je rovna matici

$$R_{-\psi} = \begin{pmatrix} \cos(-\psi) & -\sin(-\psi) \\ \sin(-\psi) & \cos(-\psi) \end{pmatrix} = \begin{pmatrix} \cos\psi & \sin\psi \\ -\sin\psi & \cos\psi \end{pmatrix}.$$

Pokud bychom chtěli zapsat rotaci kolem jiného bodu $P = O + w$, $P = [w_x, w_y]$, opět pomocí matice, snadno napíšeme potřebný vzorec pomocí posunutí:



Stačí si k tomu uvědomit, že můžeme místo rotace kolem daného bodu P napřed posunout P do našeho počátku, pak provést rotaci a pak udělat opačné posunutí, kterým celou rovinu vrátíme tam, kde měla celou dobu být, viz obrázek. Počítejme tedy

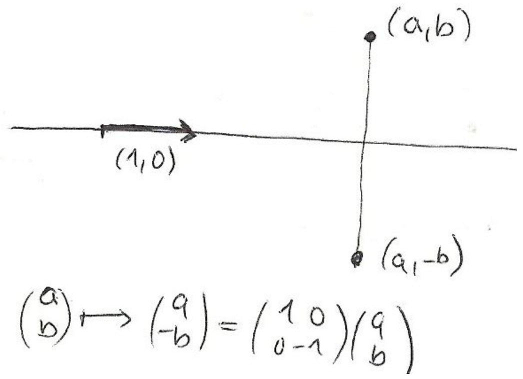
$$\begin{aligned} v = \begin{pmatrix} x \\ y \end{pmatrix} &\mapsto v - w \mapsto R_\psi \cdot (v - w) \\ &\mapsto R_\psi \cdot (v - w) + w \\ &= \begin{pmatrix} \cos\psi(x - w_x) - \sin\psi(y - w_y) + w_x \\ \sin\psi(x - w_x) + \cos\psi(y - w_y)) + w_y \end{pmatrix}. \end{aligned}$$

1.26c

1.32. Zrcadlení. Dalším dobře známým příkladem zobrazení, která zachovávají velikosti, je tzv. *zrcadlení vzhledem k přímce*. Opět nám bude stačit popsat zrcadlení vzhledem k přímkám procházejícím počátkem O a ostatní se z nich odvodí pomocí posunutí, resp. rotací.

Hledejme tedy matici Z_ψ zrcadlení vzhledem k přímce s jednotkovým směrovým vektorem v svírajícím úhel ψ s vektorem $(1, 0)$. Nejprve si uvědomme, že

$$Z_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$



Obecně můžeme každou přímku otočit do směru vektoru $(1, 0)$ a tedy zapsat obecnou matici zrcadlení jako

$$Z_\psi = R_\psi \cdot Z_0 \cdot R_{-\psi},$$

kdy nejprve otočíme maticí $R_{-\psi}$ přímku do „nulové“ polohy, odzrcadlíme maticí Z_0 a vrátíme zpět otočením R_ψ.

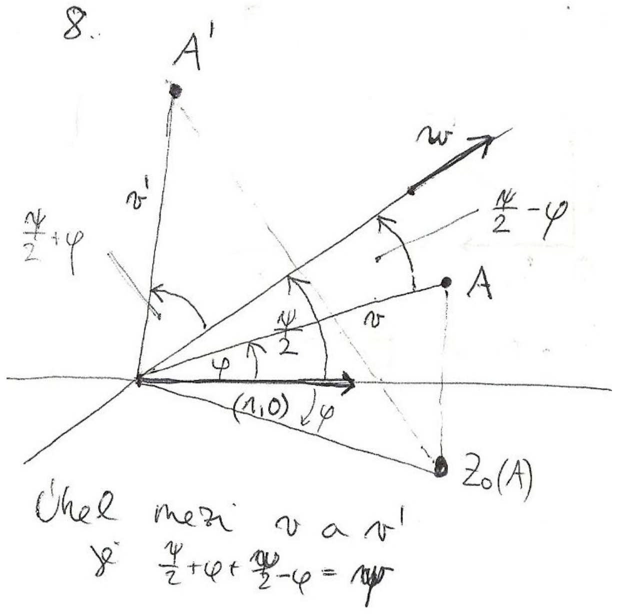
Můžeme proto (díky asociativitě násobení matic) spočíst:

$$\begin{aligned}
Z_\psi &= \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \cos\psi & \sin\psi \\ -\sin\psi & \cos\psi \end{pmatrix} \\
&= \begin{pmatrix} \cos\psi & \sin\psi \\ \sin\psi & -\cos\psi \end{pmatrix} \cdot \begin{pmatrix} \cos\psi & \sin\psi \\ -\sin\psi & \cos\psi \end{pmatrix} \\
&= \begin{pmatrix} \cos^2\psi - \sin^2\psi & 2\sin\psi\cos\psi \\ 2\sin\psi\cos\psi & -(\cos^2\psi - \sin^2\psi) \end{pmatrix} \\
&= \begin{pmatrix} \cos 2\psi & \sin 2\psi \\ \sin 2\psi & -\cos 2\psi \end{pmatrix}.
\end{aligned}$$

Použili jsme přitom obvyklé součtové vzorce pro goniometrické funkce. Povšimněme si také, že $Z_\psi \cdot Z_0$ je dáno:

$$\begin{pmatrix} \cos 2\psi & \sin 2\psi \\ \sin 2\psi & -\cos 2\psi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos 2\psi & -\sin 2\psi \\ \sin 2\psi & \cos 2\psi \end{pmatrix}.$$

Toto pozorování lze zakreslit a zformulovat následovně



Tvrzení. *Otočení o úhel ψ obdržíme následným provedením dvou zrcadlení vzhledem ke směrům, které spolu svírají úhel $\frac{1}{2}\psi$.*

Pokud umíme odůvodnit předchozí tvrzení ryze geometrickou úvahou (zkuste si zahrát na „syntetického geometra“), dokázali jsme právě standardní vzorce pro goniometrické funkce dvojnásobného úhlu.

Hlubší je následující rekapitulace předchozích úvah (skoro si můžeme říci, že už umíme dokázat skutečně zajímavý matematický výsledek):

1.27 **1.33. Věta.** *Lineární zobrazení euklidovské roviny je složeno z jednoho nebo více zrcadlení, právě když je dáno maticí R splňující*

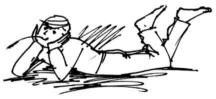
$$R = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad ab + cd = 0, \quad a^2 + c^2 = b^2 + d^2 = 1.$$

To nastane, právě když toto zobrazení zachovává velikosti.

Otočením je takové zobrazení přitom právě tehdy, když je determinant matice R roven jedné, což odpovídá sudému počtu zrcadlení. Při lichém počtu zrcadlení je determinant roven -1.

Zobrazení zachovávající velikosti

Důkaz. Zkusme napřed spočíst, jak může vypadat obecně matice A, když příslušné zobrazení zachovává velikosti. Tj. máme zobrazení



$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Zachování velikosti tedy znamená, že pro všechna x a y je

$$x^2 + y^2 = (ax + by)^2 + (cx + dy)^2 =$$
$$= (a^2 + c^2)x^2 + (b^2 + d^2)y^2 + 2(ab + cd)xy.$$

Protože má tato rovnost platit pro všechna x a y, musí si být rovny koeficienty u jednotlivých mocnin x^2, y^2 a xy na pravé i levé straně. Tím jsme spočetli, že rovnosti kladené na matici R v prvním tvrzení dokazované věty jsou ekvivalentní vlastnosti, že příslušné zobrazení zachovává velikosti.

Díky vztahu $a^2 + c^2 = 1$ můžeme předpokládat, že $a = \cos\varphi$ a $c = \sin\varphi$ pro vhodný úhel φ. Jakmile takto zvolíme první sloupec matice R, až na násobek nám vztah $ab + cd = 0$ určuje i druhý sloupec. Zároveň ale víme, že i velikost vektoru ve druhém sloupci je jedna a dostáváme tedy právě dvě možnosti pro matici R:

$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}, \qquad \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}.$$

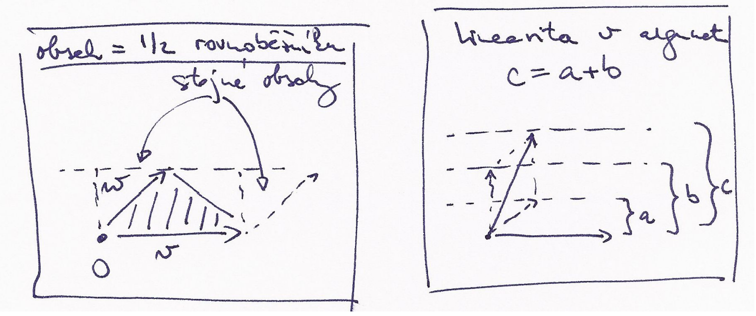
V prvém případě jde o rotaci o úhel φ, ve druhém pak o rotaci složenou se zrcadlením podle první souřadné osy. Jak jsme viděli v předchozím tvrzení 1.31, každá rotace odpovídá dvěma zrcadlením a determinant matice R je v těchto dvou případěch skutečně jedna nebo mínus jedna a rozlišuje je. □

1.28

1.34. Obsah trojúhelníka. Závěrem našeho malého výletu do geometrie se zaměřme na *obsah* rovinných objektů. Budou nám stačit trojúhelníky. Každý trojúhelník je vymezen dvojicí vektorů v a w, které, přiloženy do jednoho z vrcholů P, zadají zbylé dva vrcholy. Chtěli bychom tedy najít vzorec (skalární funkci vol), která dvěma vektorům přiřadí číslo rovné obsahu vol $\Delta(v, w)$ takto definovaného trojúhelníku $\Delta(v, w)$, kde si pro určitost za P volíme počátek a posunutím se obsah stejně nemění.

Ze zadání je vidět, že hledaná hodnota je polovinou plochy rovnoběžníku nataženého na vektory v a w a snadno se spočte (pomocí známého vzorečku: základna krát příslušná výška) nebo prostě vidí z obrázku, že nutně platí

$$\begin{aligned} \operatorname{vol} \Delta(v + v', w) &= \operatorname{vol} \Delta(v, w) + \operatorname{vol} \Delta(v', w) \\ \operatorname{vol} \Delta(av, w) &= a \operatorname{vol} \Delta(v, w). \end{aligned}$$



Nakonec ještě přidáme k našemu zadání požadavek

$$\operatorname{vol} \Delta(v, w) = -\operatorname{vol} \Delta(w, v),$$

který odpovídá představě, že opatříme plochu znaménkem podle toho, v jakém pořadí bereme vektory (tj. jestli se na ni díváme shora nebo zespodu).

Pokud vektory v a w napíšeme do sloupců matice A, pak

$$A = (v, w) \mapsto \det A$$

splňuje všechny tři naše požadavky. Kolik takových zobrazení ale může být? Každý vektor umíme vyjádřit pomocí dvou bázových vektorů $e_1 = (1, 0)$ a $e_2 = (0, 1)$ a díky linearitě je tedy každá možnost pro vol Δ jednoznačně určena už vyčíslením na těchto vektorech. Protože ale pro obsah, stejně jako pro determinant, je zjevně vol $\Delta(e_1, e_1) = \operatorname{vol} \Delta(e_2, e_2) = 0$ (kvůli požadované antisymetrii), je nutně každá taková skalární funkce jednoznačně zadána hodnotou na jediné dvojici argumentů (e_1, e_2). Jsou si tedy všechny možnosti rovny až na skalární násobek. Ten umíme určit požadavkem

$$\operatorname{vol} \Delta(e_1, e_2) = \frac{1}{2},$$

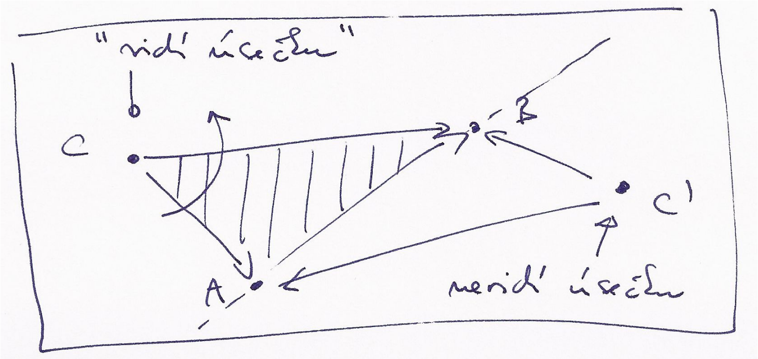
tj. volíme *orientaci* a *měřítko* pomocí volby bázových vektorů a chceme aby jednotkový čtverec měl plochu jedna.

Vidíme tedy, že determinant zadává plochu rovnoběžníku určeného sloupci matice A a plocha trojúhelníku je tedy poloviční.

1.29

1.35. Viditelnost v rovině. Předchozí popis hodnot pro orientovaný obsah nám dává do rukou elegantní nástroj pro určování pozice bodu vůči orientovaným úsečkám. Orientovanou úsečkou rozumíme dva body v rovině $\mathbb{R}^2$ s určeným pořadím. Můžeme si ji představit jako šipku od prvého k druhému bodu. Taková orientovaná úsečka nám rozděluje rovinu na dvě poloroviny, říkejme jim „levou“ a „pravou“. Pro daný bod chceme poznat, jestli je v té levé nebo pravé.

Takové úlohy často potkáváme v počítačové grafice při řešení viditelnosti objektů. Pro zjednodušení si zde jen představme, že úsečku „je vidět“ z bodů nalevo a není vidět z těch napravo.



Máme-li dán nějaký bod C, spočtěme orientovanou plochu příslušného trojúhelníku zadaného vektory $A-C$ a $B-C$. Pokud jsme s bodem C nalevo od úsečky, pak při obvyklé kladné orientaci proti směru hodinových ruček bude vektor $A-C$ dříve než ten druhý a proto výsledná plocha (tj. hodnota determinantu matice jejímiž sloupci jsou tyto dva vektory) bude kladná. Naopak, při opačné poloze bude výsledkem záporná hodnota determinantu a podle záporné hodnoty determinantu zjistíme, že je náš bod od úsečky napravo.

Uvedený jednoduchý postup je skutečně často využíván pro testování polohy při standardních úlohách v 2D grafice.

6. Relace a zobrazení

V této závěrečné části úvodní motivační kapitoly se vrátíme k formálnímu popisu matematických struktur, budeme se je ale průběžně snažit ilustrovat na již známých příkladech. Zároveň můžeme tuto část brát jako cvičení ve formálním přístupu k objektům a konceptům matematiky.

1.30

1.36. Relace mezi množinami. Nejprve potřebujeme definovat *kartézský součin* $A \times B$ dvou množin A a B. Je to množina všech uspořádaných dvojic (a, b) takových, že $a \in A$ a $b \in B$. *Binární relací* mezi množinami A a B pak rozumíme libovolnou podmnožinu R kartézského součinu $A \times B$.

Často píšeme $a \simeq_R b$ pro vyjádření skutečnosti, že $(a, b) \in R$, tj. že body $a \in A$ a $b \in B$ jsou v relaci R.

Definičním oborem relace je podmnožina

$$D \subseteq A, \quad D = \{a \in A; \exists b \in B, (a,b) \in R\}.$$

Slovy vyjádřené, je to množina prvků a z množiny A takových, že existuje prvek b z množiny B tak, že (a,b) patří do relace R. Stručněji, jsou to takové prvky z A, které mají obraz v B. Podobně *oborem hodnot relace* je podmnožina

$$I \subseteq B, \quad I = \{b \in B; \exists a \in A, (a,b) \in R\},$$

to znamená takové prvky v B, které mají vzor v A.

Speciálním případem relace mezi množinami je *zobrazení z množiny A do množiny B*. Je to případ, kdy pro každý prvek definičního oboru relace existuje právě jeden prvek z oboru hodnot, který je s ním v relaci. Nám známým případem zobrazení jsou všechny skalární funkce, kde oborem hodnot zobrazení je množina skalárů, třeba celých nebo reálných čísel. Pro zobrazení zpravidla používáme značení, které jsme také u skalárních funcí zavedli. Píšeme

$$f : D \subseteq A \to I \subseteq B, f(a) = b$$

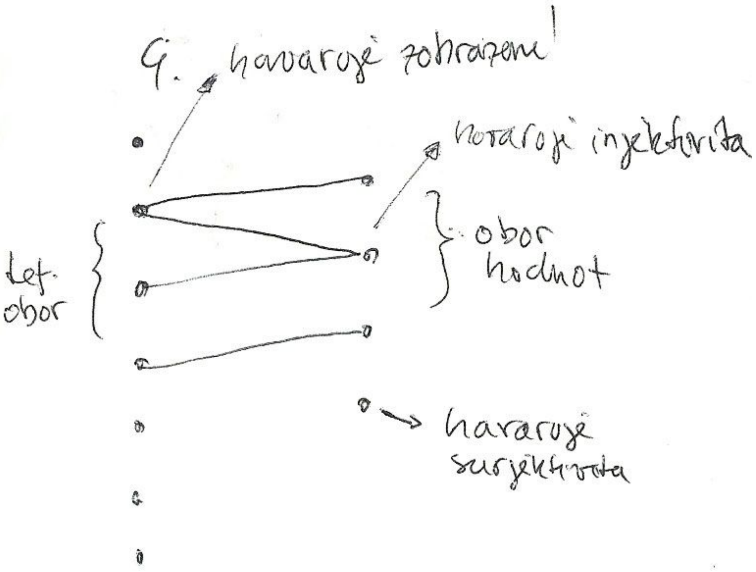
pro vyjádření skutečnosti, že (a,b) patří do relace, a říkáme, že b je hodnotou zobrazení f v bodě a. Dále říkáme, že f je

- zobrazení množiny A *do* množiny B, jestliže je $D = A$,
- zobrazení množiny A *na* množinu B, jestliže je $D = A$ a $I = B$, často také *surjektivní zobrazení*
- prosté (často také *injektivní zobrazení*), jestliže je $D = A$ a pro každé $b \in I$ existuje právě jeden *vzor* $a \in A$, $f(a) = b$.

Vyjádření zobrazení $f : A \to B$ jakožto relace

$$f \subseteq A \times B, \quad f = \{(a, f(a)); a \in A\}$$

známe také pod názvem *graf zobrazení* f.



1.31

1.37. Skládání relací a funkcí. U zobrazení je jasná koncepce, jak se skládají. Máme-li dvě zobrazení $f : A \to B$ a $g : B \to C$, pak jejich *složení* $g \circ f : A \to C$ je definováno

$$(g \circ f)(a) = g(f(a)).$$

Ve značení používaném pro relace totéž můžeme zapsat jako

$$\begin{aligned} f &\subseteq A \times B, & f &= \{(a, f(a)); a \in A\} \\ g &\subseteq B \times C, & g &= \{(b, g(b)); b \in B\} \\ g \circ f &\subseteq A \times C, & g \circ f &= \{(a, g(f(a))); a \in A\}. \end{aligned}$$

Zcela obdobně definujeme *skládání relací*, v předchozích

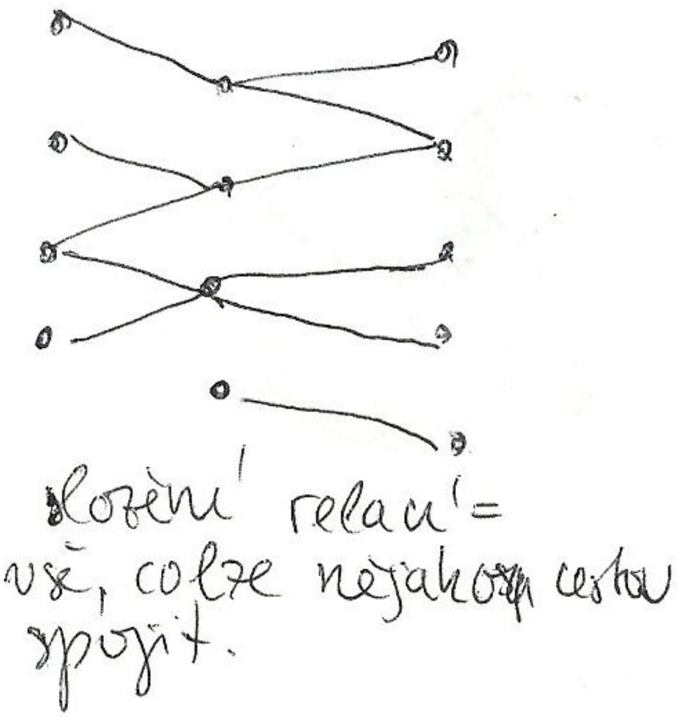
vztazích jen doplníme existenční kvantifikátory, tj. musíme uvažovat všechny „vzory“ a všechny „obrazy“. Uvažme relace $R \subseteq A \times B$, $S \subseteq B \times C$. Potom $S \circ R \subseteq A \times C$,

$$S \circ R = \{(a, c); \exists b \in B, (a, b) \in R, (b, c) \in S\}.$$

Zvláštním případem relace je *identické zobrazení*

$$\mathrm{id}_A = \{(a, a) \in A \times A; a \in A\}$$

na množině A. Je neutrální vzhledem ke skládání s každou relací s definičním oborem nebo oborem hodnot A.



Pro každou relaci $R \subseteq A \times B$ definujeme *inverzní relaci*

$$R^{-1} = \{(b, a); (a, b) \in R\} \subset B \times A.$$

Pozor, u zobrazení, je stejný pojem užíván ve specifičtější situaci. Samozřejmě, že existuje pro každé zobrazení jeho invezní relace, ta však nemusí být zobrazením. Zcela logicky proto hovoříme o existenci inverzního zobrazení, pokud každý prvek $b \in B$ je obrazem pro právě jeden vzor v A. V takovém případě je samozřejmě inverzní zobrazení právě inverzní relací.

Všimněme si, že složením zobrazení a jeho inverzního zobrazení (pokud obě existují) vždy vznikne identické obrazení, u obecných relací tomu tak být nemusí.

1.32

1.38. Relace na množině. V případě $A = B$ hovoříme o relaci na množině A. Říkáme, že relace R je:

- *reflexivní*, pokud $\mathrm{id}_A \subseteq R$, tj. $(a, a) \in R$ pro všechny $a \in A$,
- *symetrická*, pokud $R^{-1} = R$, tj. pokud $(a, b) \in R$, pak i $(b, a) \in R$,
- *antisymetrická*, pokud $R^{-1} \cap R \subseteq \mathrm{id}_A$, tj. pokud $(a, b) \in R$ a zároveň $(b, a) \in R$, pak $a = b$,
- *tranzitivní*, pokud $R \circ R \subseteq R$, tj. pokud z $(a, b) \in R$ a $(b, c) \in R$ vyplývá i $(a, c) \in R$.

Relace se nazývá *ekvivalence*, pokud je současně reflexivní, symetrická i tranzitivní.

Relace se nazývá *uspořádání* jestliže je reflexivní, tranzitivní a antisymetrická. Relaci uspořádání obvykle značíme symbolem $\leq$, tj. skutečnost, že prvek a je v relaci s prvkem b značíme $a \leq b$.

Zde je dobré si uvědomit, že relace $<$, tj. „býti ostře menší než“, mezi reálnými (racionálními, celými, přirozenými) čísly není relace uspořádání, protože není reflexivní.

Dobrým příkladem uspořádání je inkluze. Uvažme množinu 2^A všech podmnožin konečné množiny A (značení je speciálním případem obvyklé notace B^A pro množinu všech zobrazení z A do B; prvky množiny 2^A jsou tedy zobrazení $A \to \{0, 1\}$, které "říkají", zda určitý prvek je či není v dané podmnožině) a na ní relaci $X \subseteq Z$ danou vlastností „být podmnožinou“.

Evidentně jsou splněny všechny tři vlastnosti pro uspořádání: skutečně, je–li $X \subseteq Y$ a zároveň $Y \subseteq X$ musí být nutně množiny X a Y stejné. Je–li $X \subseteq Y \subseteq Z$ je také $X \subseteq Z$ a také reflexivita je zřejmá.

Říkáme, že uspořádání $\leq$ na množině A je *úplné*, když pro každé dva prvky $a, b \in A$ platí, že jsou *srovnatelné*, tj. buď $a \leq b$ nebo $b \leq a$. Všimněme si, že ne všechny dvojice (X, Y) podmnožin v A jsou srovnatelné v tomto smyslu. Přesněji, pokud je v A více než jeden prvek, existují podmnožiny X a Y, kdy není ani $X \subseteq Y$ ani $Y \subseteq X$.

Připomeňme rekurentní definici přirozených čísel $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, kde

$$0 = \emptyset, \quad n + 1 = \{0, 1, 2, \dots, n\}.$$

Na této množině $\mathbb{N}$ definujeme relaci $\leq$ následovně: $m \leq n$, právě když $m \in n$ nebo $m = n$. Evidentně jde o úplné úspořádání. Např. $2 \leq 4$, protože

$$2 = \{\emptyset, \{\emptyset\}\} \in \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} = 4.$$

Jinak řečeno, samotná rekurentní definice zadává vztah $n \leq n+1$ a tranzitivně pak $n \leq k$ pro všechna k, která jsou tímto postupem definována později.

1.33

1.39. Rozklad podle ekvivalence. Každá ekvivalence R na

množině A zadává zároveň *rozklad* množiny A na podmnožiny vzájemně ekvivalentních prvků, tzv. *třídy ekvivalence*. Pro libovolné $a \in A$ uvažujeme třídu (množinu) prvků, které jsou ekvivalentní s prvkem a, tj.

$$R_a = \{b \in A; (a,b) \in R\}.$$

Často budeme psát pro R_a prostě $[a]$, je-li z kontextu zřejmé, o kterou ekvivalenci jde.

Zjevně $R_a = R_b$, právě když $(a,b) \in R$ a každá taková třída ekvivalence je tedy reprezentována kterýmkoliv svým prvkem, tzv. *reprezentantem*. Zároveň $R_a \cap R_b \neq \emptyset$, právě když $R_a = R_b$, tj. třídy ekvivalence jsou po dvou disjunktní. Konečně, $A = \cup_{a \in A} R_a$, tj. celá množina A se skutečně rozloží na jednotlivé třídy.

Můžeme také třídám rozkladu rozumět tak, že třídu $[a]$ vnímáme jako prvek a „až na ekvivalenci".

1.34

1.40. Konstrukce celých a racionálních čísel. Na přiroze-

ných číslech umíme sice sčítat a víme, že přičtením nuly se číslo nezmění. Umíme i definovat odečítání, při něm ale jen někdy existuje výsledek v množině $\mathbb{N}$.

Základní ideou konstrukce celých čísel z přirozených je tedy přidat k nim chybějící rozdíly. To můžeme udělat tak, že místo výsledku odečítání budeme pracovat s uspořádanými dvojicemi čísel, které nám samozřejmě vždy výsledek dobře reprezentují. Zbývá jen dobře definovat, kdy jsou (z hlediska výsledku odečítání) takové dvojice ekvivalentní. Potřebný vztah tedy je:

$$(a,b) \sim (a',b') \iff a-b = a'-b' \iff a+b' = a'+b.$$

Všimněme si, že zatímco výrazy v prostřední rovnosti v přirozených číslech neumíme, výrazy vpravo už ano. Snadno ověříme, že skutečně jde o ekvivalenci a její třídy označíme jako celá čísla $\mathbb{Z}$. Na nich definujeme operaci sčítání (a s ní i odečítání) pomocí reprezentantů. Např.

$$[(a,b)] + [(c,d)] = [(a+c, b+d)],$$

což zjevně nezávisí na výběru reprezentantů.

Lze si přitom vždy volit reprezentanty $(a,0)$ pro kladná čísla a reprezentanty $(0,a)$ pro čísla záporná, se kterými se nám bude patrně počítat nejlépe.

Tento jednoduchý příklad ukazuje, jak důležité je umět nahlížet na třídy ekvivalence jako na celistvý objekt a soustředit se na vlastnosti těchto objektů, nikoliv formální popisy jejich konstrukcí. Ty jsou však důležité k ověření, že takové objekty vůbec existují.

U celých čísel nám už platí všechny vlastnosti skalárů (KG1)–(KG4) a (O1)–(O4), viz odstavce 1.1 a 1.3. Pro násobení je neutrálním prvkem jednička, ale pro všechna čísla a různá od nuly a jedničky neumíme najít číslo a^{-1} s vlastností $a \cdot a^{-1} = 1$, tzn. chybí nám inverzní prvky pro násobení.

Zároveň si povšimněme, že platí vlastnost oboru integrity (OI), viz 1.3, tzn. je-li součin dvou čísel nulový, musí být alespoň jedno z nich nula.

Díky poslední jmenované vlastnosti můžeme zkonstruovat racionální čísla $\mathbb{Q}$ přidáním všech chybějících inverzí zcela obdobným způsobem, jak jsme konstruovali $\mathbb{Z}$ z množiny $\mathbb{N}$. Na množině uspořádaných dvojic (p, q), $q \neq 0$, celých čísel definujeme relaci $\sim$ tak, jak očekáváme, že se mají chovat podíly p/q:

$$(p, q) \sim (p', q') \iff p/q = p'/q' \iff p \cdot q' = p' \cdot q.$$

Opět neumíme očekávané chování v prostřední rovnosti v množině $\mathbb{Z}$ formulovat, nicméně rovnost na pravé straně ano. Zjevně jde o dobře definovanou relaci ekvivalence (ověřte podrobnosti!) a racionální čísla jsou pak její třídy ekvivalence. Když budeme formálně psát p/q místo dvojic (p, q), budeme definovat operace násobení a sčítání právě pomocí formulí, které nám jsou jistě dobře známy.

1.35

1.41. Zbytkové třídy. Jiným dobrým a jednoduchým příkladem jsou tzv. zbytkové třídy celých čísel. Pro pevně zvolené přirozené číslo k definujeme ekvivalenci $\sim_k$ tak, že dvě čísla $a, b \in \mathbb{Z}$ jsou ekvivalentní, jestliže jejich zbytek po dělení číslem k je stejný. Výslednou množinu tříd ekvivalence označujeme $\mathbb{Z}_k$. Nejjednodušší je tato procedura pro $k = 2$. To dostáváme $\mathbb{Z}_2 = \{0, 1\}$, kde nula reprezentuje sudá čísla, zatímco jednička čísla lichá. Opět lze snadno zjistit, že pomocí reprezentantů můžeme koerektně definovat násobení a sčítání na každém $\mathbb{Z}_k$.

Věta. *Zbytkové třídy $\mathbb{Z}_k$ jsou komutativním tělesem skalárů (tj. splňují i vlastnost (P) z odstavce 1.3), právě když je k prvočíslo.*

Pokud k prvočíslem není, obsahuje $\mathbb{Z}$ vždy dělitele nuly, není proto ani obor integrity.

Důkaz. Okamžitě je vidět druhé tvrzení — jestliže $x \cdot y = k$ pro přirozená čísla x, y, pak samozřejmě je výsledek násobení příslušných tříd $[x] \cdot [y]$ nulový.

Naopak, jsou-li x a k nesoudělná, existují podle tzv. Bezoutovy rovnosti, kterou dovodíme později (viz **??**) přirozená čísla a a b splňující

$$a\,x + b\,k = 1,$$

což pro odpovídající třídy ekvivalence dává

$$[a] \cdot [x] + [0] = [a] \cdot [x] = [1]$$

a proto je $[a]$ inverzním prvkem k $[x]$. □

KAPITOLA 2

Elementární lineární algebra

V minulé kapitole jsme se snad rozehřáli s relativně jednoduchými úlohami, k jejichž řešení nebylo potřeba složitých nástrojů. Vystačili jsme si přitom se sčítáním a násobením skalárů. V této a dalších kapitolách se postupně budeme věnovat jednotlivým tématům souvisleji.

Hned tři kapitoly budou věnovány nástrojům pro práci s daty, kdy operace spočívají v obzvlášť jednoduchých úkonech se skaláry, jen je těch skalárů povíce naráz. Hovoříme o „lineárních objektech“ a „lineární algebře“. Jakkoliv to teď může vypadat jako hodně speciální nástroj, uvidíme později, že složitější objekty a závislosti stejně studujeme hlavně pomocí jejich „lineárních přiblížení“.

V této kapitole budeme pracovat přímo s konečnými posloupnostmi skalárů. Takové se objevují v praktických úlohách všude, kde máme objekty popisovány pomocí několika parametrů. Nedělejme si přitom problémy s představou, jak vypadá prostor s více než třemi „souřadnicemi“. Smiřme se se skutečností, že malovat si budeme umět jednu, dvě nebo tři dimenze, ale představovat ty obrázky mohou jakýkoliv jiný počet. A když budeme sledovat jakýkoliv parametr u třeba 500 studentů (např. jejich váhu nebo věk), budou naše data mít hned zrovna 500 položek a budeme s nimi chtít pracovat. Naším cílem bude vytvořit nástroje, které budou dobře fungovat nezávisle na skutečném počtu těchto položek.

Také se neděsme slovních spojení jako pole či okruh skalárů $\mathbb{K}$. Prostě si můžeme představit jakýkoliv konkrétní číselný obor. Okruhy skalárů pak zahrnují i celá čísla $\mathbb{Z}$ a všechny zbytkové třídy, zatímco mezi poli jsou pouze $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ a zbytkové třídy $\mathbb{Z}_k$ s prvočíselným k. Zvláštní je mezi nimi Z_2, kde ze vztahu $x = -x$ nemůžeme usoudit, že $x = 0$, zatímco u všech ostatních číselných oborů tomu tak je.

Většinou se o vektorech hovoří pouze ve spojení s poli skalárů, protože obecná teorie je při existenci neivertibilních nenulových skalárů nesrovnatelně složitější. Jen v prvních dvou částech této kapitoly budeme pracovat s vektory a maticemi v kontextu konečných poslouností skalárů a tam bude zajímavé si i třeba případu celých čísel povšimnout. Bude přitom snad pěkně vidět, jak silné výsledky lze důslednným formálním uvažováním odvodit.

1. Vektory a matice

2.1

2.1. Vektory nad skaláry. Prozatím budeme *vektorem* rozumět uspořádanou n-tici skalárů z $\mathbb{K}$, kde pevně zvolené $n \in \mathbb{N}$ budeme nazývat *dimenzí*.

Skaláry umíme sčítat a násobit. Vektory budeme také sčítat, násobit však vektor budeme umět jen skalárem. To odpovídá představě, kterou jsme již viděli v rovině $\mathbb{R}^2$, kde sčítání odpovídalo skládání vektorů coby šipek vycházejících z počátku a násobení skalárem pak jejich patřičnému natahování.

Násobení vektoru $u = (a_1, \dots, a_n)$ skalárem b tedy definujeme tak, že každý prvek n-tice u vynásobíme stejným skalárem b a také sčítání vektorů definujeme po složkách.. To znamená

$$u + v = (a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$
$$b \cdot u = b \cdot (a_1, \dots, a_n) = (b \cdot a_1, \dots, b \cdot a_n).$$

Základní operace s vektory

Pro sčítání vektorů a násobení vektorů skaláry budeme používat stále stejné symboly jako u skalárů samotných, tj. symboly plus a buď tečku nebo prosté zřetězení znaků.

Konvence zápisu vektorů. Nebudeme, na rozdíl od mnoha jiných učebnic, v textu používat pro vektory žádné speciální značení a ponecháváme na čtenáři, aby udržoval svoji pozornost přemýšlením o kontextu. Pro skaláry ale spíše budeme používat písmena ze začátku abecedy a pro vektory od konce (prostředek nám zůstane na indexy proměných či komponent a také pro sčítací indexy v součtech).

Často budeme požadovat, aby skaláry byly z nějakého pole, viz 1.1, ale v této kapitole budeme vesměs pracovat s operacemi, které tento přepoklad nepotřebují. V literatuře se pak většinou místo o vektorových prostorech hovoří o *modulech nad okruhy*. U obecné teorie se ale v příští kapitole již zcela omezíme na pole skalárů.

Pro sčítání vektorů v $\mathbb{K}^n$ zjevně platí (KG1)–(KG4) s nulovým prvkem

$$0 = (0, \dots, 0) \in \mathbb{K}^n.$$

Schválně zde používáme i pro nulový prvek stejný symbol jako pro nulový prvek skalárů.

Pro všechny vektory $v, w \in \mathbb{K}^n$ a skaláry $a, b \in \mathbb{K}$ platí

(V1) $$a \cdot (v + w) = a \cdot v + a \cdot w$$

(V2) $$(a + b) \cdot v = a \cdot v + b \cdot v$$

(V3) $$a \cdot (b \cdot v) = (a \cdot b) \cdot v$$

(V4) $$1 \cdot v = v$$

Vlastnosti vektorů

Vlastnosti vektorů (V1)–(V4) se pro $\mathbb{K}^n$ snadno ověří pro kterýkoliv okruh skalárů $\mathbb{K}$, protože při ověřování vždy používáme pro jednotlivé souřadnice vektorů pouze vlastnosti skalárů uvedené v 1.1 a 1.3.

Budeme takto pracovat např. s $\mathbb{R}^n$, $\mathbb{Q}^n$, $\mathbb{C}^n$, ale také $\mathbb{Z}^n$, $(\mathbb{Z}_k)^n$, $n = 1, 2, 3, \dots$.

2.2 **2.2. Matice nad skaláry.** O něco složitějším objektem, který budeme při práci s vektory používat, jsou matice.

Maticí typu m/n nad skaláry $\mathbb{K}$ rozumíme obdélníkové schéma

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

kde $a_{ij} \in \mathbb{K}$ pro všechny $1 \le i \le m,\ 1 \le j \le n$. Matici A s prvky a_{ij} značíme také $A = (a_{ij})$.

Vektory $(a_{i1}, a_{i2}, \dots, a_{in}) \in \mathbb{K}^n$ nazýváme (i–té) *řádky matice* A, $i = 1, \dots, m$, vektory $(a_{1j}, a_{2j}, \dots, a_{mj}) \in \mathbb{K}^m$ nazýváme (j–té) *sloupce matice* A, $j = 1, \dots, n$.

Matice nad skaláry

Matici můžeme také chápat jako zobrazení

$$A : \{1, \dots, m\} \times \{1, \dots, n\} \to \mathbb{K},$$

kde $A(i, j) = a_{ij}$. Matice typu $1/n$ nebo $n/1$ jsou vlastně právě vektory v $\mathbb{K}^n$.

I obecné matice lze chápat jako vektory v $\mathbb{K}^{m \cdot n}$, prostě zapomeneme na řádkování. Zejména tedy je definováno sčítání matic a násobení matic skaláry:

$$A + B = (a_{ij} + b_{ij}), \quad a \cdot A = (a \cdot a_{ij})$$

kde $A = (a_{ij})$, $B = (b_{ij})$, $a \in \mathbb{K}$.

Matice $-A = (-a_{ij})$ se nazývá *matice opačná* k matici A a matice

$$0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

se nazývá *nulová matice*. Zapomenutím řádkování tak získáme následující tvrzení, že matice jsou jen specificky zapsané vektory:

Tvrzení. *Předpisy pro $A + B$, $a \cdot A$, $-A$, 0 zadávají na množině všech matic typu m/n operace sčítání a násobení skaláry splňující axiomy (V1)–(V4).*

2.3 **2.3. Matice a rovnice.** Velmi častý nástroj pro popis nějakých matematických modelů jsou systémy lineárních rovnic. Právě matice lze vhodně využít pro jejich zápis.

Uvažme následující systém m rovnic v n proměnných:

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

Posloupnost $x_1, \dots, x_n$ lze chápat jako vektor proměnných, tj. sloupec v matici typu $n/1$, a podobně hodnoty $b_1, \dots, b_n$

můžeme vnímat jako vektor u a to opět jako jediný sloupec v matici typu $n/1$. Systém rovnic lze pak formálně psát ve tvaru $A \cdot x = u$ takto:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

Původní rovnice nyní obdržíme tak, že vždy bereme řádky z A a sčítáme součiny odpovídajících komponent. To znamená, že skutečně jako i-tý prvek výsledného vektoru získáme

$$a_{i1}x_1 + \cdots + a_{in}x_n$$

a zápis $A \cdot x = u$ dává skutečně původní systém lineárních rovnic.

V rovině, tj. pro vektory dimenze 2, jsme už zavedli takovýto počet a viděli jsme, že s ním lze pracovat velice efektivně (viz 1.26). Nyní budeme postupovat obecněji a zavedeme všechny nástroje již známé z roviny pro všechny dimenze n.

2.4

2.4. Součin matic. Násobení matic je definována pouze, když to rozměry sloupců a řádků v maticích dovolí:

Pro libovolnou matici $A = (a_{ij})$ typu m/n nad okruhem skalárů $\mathbb{K}$ a libovolnou matici $B = (b_{jk})$ typu n/q nad $\mathbb{K}$ definujeme jejich součin $C = A \cdot B = (c_{ik})$ jako matici typu m/q s prvky

$$c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}, \text{ pro libovolné } 1 \le i \le m,\ 1 \le k \le q.$$

Součin matic

Například máme

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

2.5

2.5. Čtvercové matice. Je-li v matici stejný počet řádků a sloupců, hovoříme o *čtvercové matici*. Počet řádků a sloupců pak nazýváme také *dimenzí matice*. Matici

$$E = (\delta_{ij}) = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix}$$

se říká *jednotková matice*. Na množině čtvercových matic nad $\mathbb{K}$ dimenze n je součin matic definován pro každé dvě matice, je tam tedy definována operace násobení, jejíž vlastnosti jsou velice podobné jako u skalárů:

Tvrzení. *Na množině všech čtvercových matic dimenze n nad libovolným okruhem skalárů $\mathbb{K}$ je definována operace násobení s následujícími vlastnosti okruhů (viz 1.3):*

(1) Platí asociativita násobení (O1)
(2) jednotková matice $E = (\delta_{ij})$ je jednotkovým prvkem pro násobení dle (O3)
(3) Platí distributivita sčítání a násobení (O4).

Obecně však neplatí axiomy (O2) ani (OI). Čtvercové matice pro $n > 1$ proto netvoří obor integrity, zejména tedy nejsou ani (nekomutativním) tělesem.

Důkaz. Asociativita násobení – (O1): Protože skaláry jsou asociativní, distributivní i komutativní, můžeme pro tři matice $A = (a_{ij})$ typu m/n, $B = (b_{jk})$ typu n/p a $C = (c_{kl})$ typu p/q spočíst

$$A \cdot B = \Big(\sum_j a_{ij}.b_{jk}\Big), \quad B \cdot C = \Big(\sum_k b_{jk}.c_{kl}\Big)$$

$$(A \cdot B) \cdot C = \Big(\sum_k (\sum_j a_{ij}.b_{jk}).c_{kl}\Big) = \Big(\sum_{j,k} a_{ij}.b_{jk}.c_{kl}\Big)$$

$$A \cdot (B \cdot C) = \Big(\sum_j a_{ij}.(\sum_k b_{jk}.c_{kl})\Big) = \Big(\sum_{j,k} a_{ij}.b_{jk}.c_{kl}\Big).$$

Všimněme si, že jsme při výpočtu vycházeli z toho, že je jedno v jakém pořadí uvedené součty a součiny provádíme, tj. využívali jsme podstatně našich vlastností skalárů.

Velmi snadno vidíme, že násobení jednotkovou maticí má skutečně vlastnost jednotkového prvku:

$$A \cdot E = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \\ 0 & 0 & \cdots & 1 \end{pmatrix} = A = E \cdot A$$

Zbývá distributivita násobení a sčítání. Opět díky distributivitě skalárů snadno spočteme pro matice $A = (a_{ij})$ typu m/n, $B = (b_{jk})$ typu n/p, $C = (c_{jk})$ typu n/p, $D = (d_{kl})$ typu p/q

$$\begin{aligned} A \cdot (B + C) &= \Big(\sum_j a_{ij}(b_{jk} + c_{jk})\Big) \\ &= \Big((\sum_j a_{ij}b_{jk}) + (\sum_j a_{ij}c_{jk})\Big) = A \cdot B + A \cdot C \\ (B + C) \cdot D &= \Big(\sum_k (b_{jk} + c_{jk})d_{kl}\Big) \\ &= \Big((\sum_k b_{jk}d_{kl}) + (\sum_k c_{jk}d_{kl})\Big) = B \cdot D + C \cdot D \end{aligned}$$

Jak jsme již viděli v 1.26, dvě matice dimenze 2 nemusí komutovat:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Tím jsme získali zároveň protipříklad na platnost (O2) i (OI). Pro matice typu $1/1$ ovšem oba axiomy samozřejmě platí, protože je mají samy skaláry a pro větší matice získáme protipříklady snadno tak, že právě uvedené matice umístíme do levého horního rohu příslušných čtvercových schémat a doplníme nulami. (Ověřte si sami!) □

V důkazu jsme vlastně pracovali s maticemi obecnějšího typu, dokázali jsme tedy příslušné vlastnosti obecněji:

Důsledek. *Násobení matic je asociativní a distributivní, tj.*

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C$$
$$A \cdot (B + C) = A \cdot B + A \cdot C,$$

kdykoliv jsou všechny uvedené operace definovány. Jednotková matice je neutrálním prvkem pro násobení zleva i zprava.

Asociativita a distributivita násobení matic

2.6

2.6. Inverzní matice. Se skaláry umíme počítat tak, že z rovnosti $a \cdot x = b$ umíme vyjádřit $x = a^{-1} \cdot b$, kdykoliv inverze k a existuje. Podobně bychom to chtěli umět i s maticemi, máme ale problém, jak poznat, zda taková existuje, a jak ji spočítat.

Říkáme, že B je *matice inverzní* k matici A, když

$$A \cdot B = B \cdot A = E.$$

Píšeme pak $B = A^{-1}$ a je samozřejmé, že obě matice musí mít tutéž dimenzi n. Matici, k níž existuje matice inverzní, říkáme *invertibilní matice*.

Pokud A^{-1} a B^{-1} existují, pak existuje i inverze k součinu $A \cdot B$

$$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}.$$

Je totiž, díky právě dokázané asociativitě násobení,

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

Protože s maticemi umíme počítat podobně jako se skaláry, jen mají složitější chování, mohou nám skutečně hodně pomoci s řešením systémů lineárních rovnic: Jestliže vyjádříme soustavu n rovnic pro n neznámých součinem matic

$$A \cdot x = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = u$$

a jestliže existuje matice inverzní k matici A, pak lze násobit zleva A^{-1} a dostaneme

$$A^{-1} \cdot u = A^{-1} \cdot A \cdot x = E \cdot x = x,$$

tj. hledané řešení.

Naopak rozepsáním podmínky $A \cdot A^{-1} = E$ pro neznámé skaláry v hledané matici A^{-1} dostaneme n systémů lineárních rovnic se stejnou maticí na levé straně a různými vektory napravo.

2.7 **2.7. Ekvivalentní úpravy matic.** Zkusme se praktičtěji zorientovat v předchozí úvaze o systémech rovnic a jejich maticích. Samozřejmě nás nalezení inverzní matice stojí jisté úsilí – větší než přímé vyřešení rovnice. Podstatné však je, že pokud máme mnohokrát za sebou řešit systémy se stejnou maticí A ale různými pravými stranami u, pak se nám nalezení A^{-1} opravdu hodně vyplatí.

Z hlediska řešení systémů rovnic $A \cdot x = u$ je jistě přirozené považovat za ekvivalentní matice A a vektory u, které zadávají systémy rovnic se stejným řešením. Zkusme se teď zamyslet nad možnostmi, jak zjednodušovat matici A tak, abychom se k řešení blížili.

Začneme jednoduchými manipulacemi s řádky rovnic, které řešení ovlivňovat nebudou, a stejným způsobem pak můžeme upravovat i vektor napravo. Když se nám u čtvercové matice podaří vlevo dostat systém s jednotkovou maticí, bude napravo řešení původního systému. Pokud při našem postupu nějaké řádky úplně vypadnou (při úpravách se vynulují), bude to také dávat další přímé informace o řešení.

Naše jednoduché úpravy jsou:

- záměna dvou řádků
- vynásobení vybraného řádku nenulovým skalárem
- přičtení řádku k jinému řádku.

Těmto operacím říkáme *řádkové elementární transformace*. Je zjevné, že odpovídající operace na úrovni rovnic v systému skutečně nemohou změnit množinu všech jeho řešení.

Řádkové elementární transformace

Analogicky, *sloupcové elementární transformace* matic jsou

- záměna dvou sloupců
- vynásobení vybraného sloupce nenulovým skalárem
- přičtení sloupce k jinému sloupci,

ty však nezachovávají řešení příslušných rovnic, protože mezi sebou míchají samotné proměnné.

Systematicky můžeme použít elementární řádkové úpravy k postupné eliminaci proměnných. Postup je algoritmický a většinou se mu říká *Gausova eliminace* proměnných.

Tvrzení. *Nenulovou matici nad libovolným okruhem skalárů $\mathbb{K}$ lze konečně mnoha elementárními řádkovými transformacemi převést na tzv. (řádkově) schodovitý tvar:*

- *Je-li $a_{ij} = 0$ a všechny předchozí prvky na i-tém řádku jsou také nulové, potom $a_{kj} = 0$ pro všechna $k \geq i$*
- *je-li $a_{(i-1)j}$ první nenulový prvek na $(i-1)$-ním řádku, pak $a_{ij} = 0$.*

Gaussova eliminace proměnných

Důkaz. Matice v řádkově schodovitém tvaru vypadá takto

$$\begin{pmatrix} 0 & \dots & 0 & a_{1j} & \dots & \dots & \dots & a_{1m} \\ 0 & \dots & 0 & 0 & \dots & a_{2k} & \dots & a_{2m} \\ \vdots & & & & & & & \\ 0 & \dots & \dots & \dots & \dots & 0 & a_{lp} & \dots \\ \vdots & & & & & & & \end{pmatrix}$$

a matice může, ale nemusí, končit několika nulovými řádky. K převodu libovolné matice můžeme použít jednoduchý algoritmus, kterým se postupně, řádek za řádkem, blížíme k výslednému schodovitému tvaru:

(1) Záměnou řádků docílíme, že v prvním řádku bude v prvním nenulovém sloupci nenulový prvek, nechť je to j-tý sloupec.
(2) Pro $i = 2, \dots$, vynásobením prvního řádku prvkem a_{ij}, i-tého řádku prvkem a_{1j} a odečtením vynulujeme prvek a_{ij} na i-tém řádku.
(3) Opakovanou aplikací bodů (1) a (2), vždy pro dosud neupravený zbytek řádků a sloupců v získané matici dospějeme po konečném počtu kroků k požadovanému tvaru.

Algoritmus Gaussovy eliminace

Tím je tvrzení dokázáno □

Uvedený postup je skutečně právě obvyklá eliminace proměnných v systémech lineárních rovnic.

Poznámka. Gaussovu eliminaci jsme sformulovali pro obecné skaláry z nějakého okruhu. Zdá se být přirozené, že ve schodovitém tvaru ještě vynásobením vhodnými skaláry dosáhneme jednotkových koeficientů na výsledné nenulové „diagonále“ nad nulami v matici a dopočítáme řešení. To ale pro obecné skaláry nepůjde, představte si třeba celá čísla $\mathbb{Z}$.

Pro řešení systémů rovnic nemá ale vůbec uvedený postup rozumný smysl, když jsou mezi skaláry dělitelé nuly. Promyslete si pečlivě rozdíl mezi $\mathbb{K} = \mathbb{Z}$, $\mathbb{K} = \mathbb{R}$ a případně $\mathbb{Z}_2$ nebo $\mathbb{Z}_3$.

2.8 **2.8. Poznámka.** V dalším budeme už pracovat jen s polem skalárů P, každý nenulový skalár je tedy invertibilní.

Všimněme si, že elementární řádkové (resp. sloupcové) transformace odpovídají vynásobením zleva (resp. zprava) následujícími maticemi:

(1) Přehození i-tého a j-tého řádku (resp. sloupce)

$$\begin{pmatrix} 1 & 0 & \dots & & & & \\ 0 & \ddots & & & & & \\ \vdots & & 0 & \dots & 1 & & \\ & & \vdots & \ddots & \vdots & & \\ & & 1 & \dots & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

(2) Vynásobení i-tého řádku (resp. sloupce) skalárem a:

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & a & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \leftarrow i \\ \\ \\ \\ \end{matrix}$$

(3) Sečtení i-tého řádku (resp. sloupce) s j-tým:

$$\begin{array}{cc} i \rightarrow & \begin{pmatrix} 1 & 0 & & & & & \\ 0 & \ddots & & & & & \\ & & \ddots & & & & \\ & & & \ddots & & & \\ & & 1 & & \ddots & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \\ & \begin{matrix} & & \uparrow & & & & \\ & & j & & & & \end{matrix} \end{array}$$

Toto prostinké pozorování je ve skutečnosti velice podstatné, protože součin invertibilních matic je invertibilní a všechny elementární transformace jsou nad polem skalárů invertibilní. Pro libovolnou matici A tedy dostaneme násobením vhodnou invertibilní maticí $P = P_k \cdots P_1$ zleva (postupné násobení k maticemi zleva) její ekvivalentní řádkový schodovitý tvar $A' = P \cdot A$.

Jestliže obecně aplikujeme tentýž eliminační postup na sloupce, dostaneme z každé matice B její sloucový schodovitý tvar B' vynásobením vhodnou invertibilní maticí $Q = Q_1 \cdots Q_\ell$. Pokud ale začneme s maticí $B = A'$ v řádkově schodovitém tvaru, eliminuje takový postup pouze všechny dosud nenulové prvky mimo diagonálu matice a závěrem lze ještě i tyto elementárními operacemi změnit na jedničky. Celkem jsme tedy ověřili důležitý výsledek, ke kterému se budeme mnohokrát vracet:

2.9 **2.9. Věta.** *Pro každou matici A typu m/n nad polem skalárů $\mathbb{K}$ existují čtvercové invertibilní matice P dimenze m a Q dimenze n takové, že matice $P \cdot A$ je v řádkově schodovitém* *tvaru a*

$$P \cdot A \cdot Q = \begin{pmatrix} 1 & \dots & 0 & \dots & \dots & \dots & 0 \\ \vdots & \ddots & & & & & \\ 0 & \dots & 1 & 0 & \dots & \dots & 0 \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & \end{pmatrix}.$$

2.10

2.10. Algoritmus pro výpočet inverzní matice. V předchozích úvahách jsme se dostali prakticky k úplnému algoritmu pro výpočet inverzní matice. Během jednoduchého níže uvedeného postupu buď zjistíme, že inverze neexistuje, nebo bude inverze spočtena. I nadále pracujeme nad polem skalárů.

Ekvivalentní řádkové transformace se čtvercovou maticí A dimenze n vedou k matici P' takové, že matice $P' \cdot A$ bude v řádkově schodovitém tvaru. Přitom může (ale nemusí) být jeden nebo více posledních řádků nulových. Jestliže má existovat inverzní matice k A, pak existuje i inverzní matice k $P' \cdot A$. Jestliže však je poslední řádek v $P' \cdot A$ nulový, bude nulový i poslední řádek v $P' \cdot A \cdot B$ pro jakoukoliv matici B dimenze n. Existence takového nulového řádku ve výsledku (řádkové) Gaussovy eliminace tedy vylučuje existenci A^{-1}.

Předpokládejme nyní, že A^{-1} existuje. Podle předchozího, nalezneme řádkově schodovitý tvar bez nulového řádku, tzn. že všechny diagonální prvky v $P' \cdot A$ jsou nenulové. Pak ovšem pokračováním eliminace pomocí řádkových elementárních transformací od pravého dolního rohu zpět a vynormováním diagonálních prvků na jedničky získáme jednotkovou matici E. Jinými slovy, najdeme další invertibilní matici P'' takovou, že pro $P = P'' \cdot P'$ platí $P \cdot A = E$. Výměnou řádkových a sloupcových transformací lze za předpokladu existence A^{-1} stejným postupem najít Q takovou, že $A \cdot Q = E$. Odtud

$$P = P \cdot E = P \cdot (A \cdot Q) = (P \cdot A) \cdot Q = Q.$$

To ale znamená, že jsme nalezli hledanou inverzní matici

$$A^{-1} = P = Q$$

k matici A. Prakticky tedy můžeme postupovat takto:

Vedle sebe napíšeme původní matici A a jednotkovou matici E, matici A upravujeme řádkovými elementárními úpravami nejprve na schodovitý tvar, potom tzv. zpětnou eliminací na diagonální matici a v té násobíme řádky inverzními prvky z $\mathbb{K}$. Tytéž úpravy postupně prováděné s E vedou právě k hledané matici A^{-1}. Pokud tento algoritmus narazí na vynulování celého řádku v původní matici, znamená to, že matice inverzní neexistuje.

Výpočet inverzní matice

2.10a

2.11. Závislost řádků a sloupců a hodnost matice. V předchozích úvahách a počtech s maticemi jsme stále pracovali se sčítáním řádků nebo sloupců coby vektorů, spolu s jejich násobením skaláry. Takové operaci říkáme *lineární* *kombinace*. V abstraktním pojetí se k operacím s vektory vrátíme za chvíli v 2.23, bude ale užitečné pochopit podstatu už nyní. Lineární kombinací řádků (nebo sloupců) matice $A = (a_{ij})$ typu m/n rozumíme výraz $a_1 u_{i_1} + \cdots + a_k u_{i_k}$, kde a_i jsou skaláry, $u_j = (a_{j1}, \dots, a_{jn})$ jsou řádky (nebo $u_j = (a_{1j}, \dots, a_{mj})$ jsou sloupce) matice A.

Jestliže existuje lineární kombinace daných řádků s alespoň jedním nenulovým skalárním koeficientem, jejímž výsledkem je nulový řádek, říkáme, že jsou *lineárně závislé*. V opačném případě, tj. když jedinou možnost jak získat nulový řádek je vynásobení výhradně nulovými skaláry, jsou *lineárně nezávislé*. Obdobně definujeme lineárně závislé a nezávislé sloupce matice.

Předchozí výsledky o Gausově eliminaci můžeme teď intepretovat tak, že počet výsledných nenulových „schodů" v řádkově nebo sloupcově schodovitém tvaru je vždy roven počtu lineárně nezávislých řádků matice, resp. počtu lineárně nezávislých sloupců matice. Označme E_h matici z věty 2.9 s h jedničkami na diagonále a předpokládejme, že dvěma různými postupy dostaneme různá $h' < h$. Pak ovšem podle našeho postupu budou existovat také invertibilní matice P a Q takové, že

$$P \cdot E_{h'} \cdot Q = E_h.$$

V součinu $E_{h'} \cdot Q$ bude více nulových řádků ve spodní části matice, než kolik má být jedniček v E_h a přitom se k nim máme dostat už jen řádkovými transformacemi. Zvýšit počet lineárně nezávislých řádků ale pomocí elementárních řdákových transformací nelze. Proto je počet jedniček v matici $P \cdot A \cdot Q$ ve větě 2.9 nezávislý na volbě našeho postupu eliminace a je roven jak počtu lineárně nezávislých řádků v A, tak počtu lineárně nezávislých sloupců v A. Tomuto číslu říkáme *hodnost matice* a značíme je $h(A)$. Zapamatujme si výsledné tvrzení:

Věta. *Nechť A je matice typu m/n nad polem skalárů $\mathbb{K}$. Matice A má stejný počet $h(A)$ linárně nezávislých řádků a lineárně nezávislých sloupců. Zejména je hodnost vždy nejvýše rovna menšímu z rozměrů matice A.*

Algoristmus pro výpočet inverzních matic také říká, že čtvercová matice A dimenze m má inverzi právě, když je její hodnost rovna počtu řádků m.

2.10b

2.12. Matice jako zobrazení. Zcela stejně, jak jsme s maticemi pracovali v geometrii roviny, viz 1.29, můžeme každou čtvercovou matici A interpretovat jako zobrazení

$$A : \mathbb{K}^n \to \mathbb{K}^n, \quad x \mapsto A \cdot x.$$

Díky distributivnosti násobení matic je zřejmé, jak jsou zobrazovány lineární kombinace vektorů takovými zobrazeními:

$$A \cdot (a\,x + b\,y) = a\,A \cdot x + b\,A \cdot y.$$

Přímo z definice je také vidět (díky asociativnosti násobení matic), že skládání zobrazení odpovídá skládání matic. Invertibilní matice tedy odpovídají bijektivním zobrazením.

Z tohoto pohledu je velice zajímavá věta 2.9. Můžeme ji číst tak, že hodnost matice určuje, jak velký je obraz celého $\mathbb{K}^n$ v tomto zobrazení. Skutečně, je-li $A = P \cdot J \cdot Q$ s maticí J s k jedničkami jako v 2.9, pak invertibilní Q napřed jen bijektivně „zamíchá“ n–rozměrné vektory v $\mathbb{K}^n$, matice J pak „zkopíruje“ prvních k souřadnic a vynuluje $n-k$ zbývajících. Tento „k–rozměrný“ obraz už pak následně násobení invertibilní P nemůže zvětšit. K pojmům dimenze, lineární nezávislost apod. se vrátíme ve třetí části této kapitoly.

2.11

2.13. Matice rotací v $\mathbb{R}^3$. Nyní si jako ilustraci najdeme popis rotací v $\mathbb{R}^3$. Nejprve si napíšeme matice zobrazení rotací o úhel φ postupně kolem os x, y, z v $\mathbb{R}^3$. Při rotaci libovolného bodu kolem dané osy (řekněme x), se příslušná souřadnice daného bodu nemění, v rovině dané dvěma zbylými osami pak již je rotace dána známou maticí typu $2/2$.

Postupně tedy dostáváme následující matice — rotace kolem osy z:

$$\begin{pmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

rotace kolem osy y:

$$\begin{pmatrix} \cos\varphi & 0 & \sin\varphi \\ 0 & 1 & 0 \\ -\sin\varphi & 0 & \cos\varphi \end{pmatrix}$$

rotace kolem osy x:

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

U matice rotace kolem osy y máme jinak znaménko u φ. Chceme totiž, stejně jako u ostatních os rotaci kolem osy y v kladném smyslu, tedy takovou, že pokud se díváme proti směru osy y, tak se svět točí proti směru hodinových ručiček. Při obvyklé orientaci souřadných os jako na obrázku jde tady o rotaci v záporném smyslu v rovině xz (tedy osa z se otáčí směrem k x). Rozmyslete si kladný a záporný smysl rotace podél všech tří os. vlozit obrazek

Díky tomu, že násobení matic odpovídá skládání zbrazení (stejně jako jsme to používali v rovině) můžeme nyní docela snadno napsat matici pro zobrazení rotace kolem libovolné osy procházející počátkem v $\mathbb{R}^3$.

Ukážeme si to na rotaci v kladném smyslu o úhel 60° kolem přímky dané počátkem a vektorem $(1, 1, 0)$ v $\mathbb{R}^3$. Toto otáčení je složením následujících tří zobrazení:

- rotace o 45° v záporném smyslu podle osy z (osa rotace $(1, 1, 0)$ přejde do osy x)
- rotace o 60° v kladném smyslu podle osy x.
- rotace o 45° v kladném smyslu podle osy z (osa x přejde zpět na osu danou vektorem $(1, 1, 0)$).

Matice výsledné rotace tedy bude součinem matic odpovídajících těmto třem zobrazením, přičemž pořadí matic je dáno pořadím provádění jednotlivých zobrazení, prvnímu zobrazení odpovídá v součinu matice nejvíce napravo. Celkem tedy dostáváme pro hledanou matici A vztah:

$$A = \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} \frac{3}{4} & \frac{1}{4} & \frac{\sqrt{6}}{4} \\ \frac{1}{4} & \frac{3}{4} & -\frac{\sqrt{6}}{4} \\ -\frac{\sqrt{6}}{4} & \frac{\sqrt{6}}{4} & \frac{1}{2} \end{pmatrix}$$

2. Determinanty

V páté části první kapitoly jsme viděli, že pro čtvercové matice dimenze 2 nad reálnými čísly existuje skalární funkce det, která matici přiřadí nenulové číslo právě, když existuje její inverze. Neříkali jsme to sice stejnými slovy, ale snadno si to ověříte (viz odstavce počínaje 1.26 a vzorec (1.16)). Determinant byl užitečný i jinak, viz 1.33 a 1.34, kde jsme si volnou úvahou odvodili, že obsah rovnoběžníka by měl být lineárně závislý na každém ze dvou vektorů definujících rovnoběžník a že je užitečné zároveň požadovat změnu znaménka při změně pořadí těchto vektorů. Protože tyto vlastnosti měl, až na pevný skalární násobek, jedině determinant, odvodili jsme, že je obsah dán právě takto. Nyní uvidíme, že podobně lze postupovat v každé konečné dimenzi.

V této části budeme pracovat s libovolnými skaláry $\mathbb{K}$ a maticemi nad těmito skaláry. Naše výsledky o determinantech tedy budou vesměs platit pro všechny komutativní okruhy, zejména tedy třeba pro celočíslené matice.

2.10c

2.14. Definice determinantu. Připomeňme, že bijektivní zobrazení množiny X na sebe se nazývá *permutace množiny* X, viz 1.7. Je-li $X = \{1, 2, \dots, n\}$, lze permutace zapsat pomocí výsledného pořadí ve formě tabulky:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Prvek $x \in X$ se nazývá samodružným bodem permutace σ, je-li $\sigma(x) = x$. Permutace σ taková, že existují právě dva různé prvky $x, y \in X$ s $\sigma(x) = y$ a $\sigma(z) = z$ pro všechna ostatní $z \in X$ se nazývá *transpozice*, značíme ji (x, y). Samozřejmě pro takovou transpozici platí také $\sigma(y) = x$, odtud název.

V dimenzi dva byl vzorec pro determinant jednoduchý – vezmeme všechny možné součiny dvou prvků, po jednom z každého sloupce a řádku matice, opatříme je znaménkem tak, aby při přehození dvou sloupců došlo ke změně celkového znaménka, a výrazy všechny (tj. oba) sečteme:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ \det A = ad - bc.$$

Obecně, uvažujme čtvercové matice $A = (a_{ij})$ dimenze n nad $\mathbb{K}$. Vzorec pro determinant matice A bude také poskládány ze všech možných součinů prvků z jednotlivých řádků a sloupců:

Determinant matice A je skalár $\det A = |A|$ definovaný vztahem

$$|A| = \sum_{\sigma \in \Sigma_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

kde Σ_n je množina všech možných permutací na $\{1, \dots, n\}$ a znaménko sgn pro každou permutaci σ ještě musíme popsat. Každý z výrazů

$$\operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

nazýváme *člen determinantu* $|A|$.

Definice determinantu

V dimenzích 2 a 3 snadno uhádneme i správná znaménka. Součin prvků z diagonály má být s kladným znaménkem a chceme linearitu v každém sloupci a antisymetrii při přehození dvou sloupců nebo řádků.

Pro $n = 2$ je, jak jsme čekali

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = +a_{11}a_{22} - a_{12}a_{21}.$$

Podobně pro $n = 3$

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

$$- a_{11}a_{23}a_{32} + a_{12}a_{23}a_{31} - a_{12}a_{21}a_{33}.$$

Tomuto vzorci se říká *Saarusovo pravidlo.*

Determinanty v dimensi dvě a tři

2.13a

2.15. Parita permutace. Jak tedy najít správná znaménka permutací? Říkáme, že dvojice prvků $a, b \in X = \{1, \dots, n\}$ tvoří *inverzi v permutaci* σ, je-li $a < b$ a $\sigma(a) > \sigma(b)$. Permutace σ se nazývá *sudá* (resp. *lichá*), obsahuje-li sudý (resp. lichý) počet inverzí.

Parita permutace σ je $(-1)^{\text{počet inverzí}}$ a značíme ji $\operatorname{sgn}(\sigma)$. Tolik tedy definice znamének našich členů determintu, chceme ale vědět, jak s paritou počítat. Z následujícího tvrzení o permutacích už je jasně vidět, že Saarusovo pravidlo skutečně počítá determinant v dimenzi 3.

Věta. *Na množině* $X = \{1, 2, \dots, n\}$ *je právě* $n!$ *různých permutací. Tyto lze seřadit do posloupnosti tak, že každé dvě po sobě jdoucí se liší právě jednou transpozicí a každá transpozice mění paritu. Lze při tom začít libovolnou permutací.*

Důkaz. Pro jednoprvkové a dvouprvkové X tvrzení samozřejmě platí. Budeme postupovat indukcí přes dimenzi.

Předpokládejme, že tvrzení platí pro všechny množiny s $n-1$ prvky a uvažme permutaci $\sigma(1)=a_1,\dots,\sigma(n)=a_n$. Podle indukčního předpokladu všechny permutace, které mají na posledním místě a_n, dostaneme z tohoto pořadí postupným prováděním transpozic. Přitom jich bude $(n-1)!$. V posledním z nich prohodíme $\sigma(n)=a_n$ za některý z prvků, který dosud nebyl na posledním místě, a znovu uspořádáme všechny permutace s tímto vybraným prvkem na posledním místě do posloupnosti s požadovanými vlastnostmi. Po n-násobné aplikaci tohoto postupu získáme $n(n-1)=n!$ zaručeně různých permutací, tzn. všechny, právě předepsaným způsobem. Všimněme si, že poslední věta dokazovaného tvrzení se nezdá příliš důležitá pro jeho využití. Je však velice důležitou částí postupu v našem důkazu indukcí přes počet prvků.

Zbývá tvrzení věty o paritách. Uvažme pořadí

$$(a_1,\dots,a_i,a_{i+1},\dots,n),$$

ve kterém je r inverzí. Pak zjevně je v pořadí

$$(a_1,\dots,a_{i+1},a_i\dots,n)$$

buď $r-1$ nebo $r+1$ inverzí. Každou transpozici (a_i,a_j) lze přitom získat postupným provedením $(j-i)+(j-i-1)=2(j-i)-1$ transpozic sousedních prvků. Proto se provedením libovolné transpozice parita permutace změní. Navíc již víme, že všechny permutace lze získat prováděním transpozic. □

Zjistili jsme, že provedení libovolné transpozice změní paritu permutace a že každé pořadí čísel $\{1,2,\dots,n\}$ lze získat postupnými transpozicemi sousedních prvků. Dokázali jsme proto:

Důsledek. *Na každé konečné množině $X=\{1,\dots,n\}$ s n prvky, $n>1$, je právě $\frac{1}{2}n!$ sudých a $\frac{1}{2}n!$ lichých permutací.*

Jestliže složíme dvě permutace za sebou, znamená to provést napřed všechny transpozice tvořící první a pak druhou. Proto pro libovolné permutace $\sigma,\eta : X\to X$ platí

$$\operatorname{sgn}(\sigma\circ\eta)=\operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\eta)$$

a proto také

$$\operatorname{sgn}(\sigma^{-1})=\operatorname{sgn}(\sigma).$$

2.13b

2.16. Rozklad permutace na cykly. Dobrým nástrojem pro praktickou práci s permutacemi je jejich rozklad na tzv. cykly.

Permutace σ na množině $X=\{1,\dots,n\}$ se nazývá *cyklus* délky k, jestliže je možné najít prvky $a_1,\dots,a_k\in X$, $2\le k\le n$ takové, že $\sigma(a_i)=a_{i+1}$, $i=1,\dots,k-1$, zatímco $\sigma(a_k)=a_1$ a ostatní prvky v X jsou pro σ samodružné. Cykly délky dva jsou právě transpozice.

Každá permutace je složením cyklů. Cykly sudé délky mají paritu -1, cykly liché délky mají paritu 1.

Cykly

Poslední tvrzení musíme ještě dokázat. Jestliže definujeme pro danou permutaci σ relaci R tak, že dva prvky x, $y \in X$ jsou v relaci právě když $\sigma^r(x) = y$ pro nějakou iteraci permutace σ, pak zjevně jde o relaci ekvivalence. Protože je X konečná množina, musí pro nějaké ℓ být $\sigma^\ell(x) = x$. Jestliže zvolíme jednu třídu ekvivalence $\{x, \sigma(x), \dots, \sigma^{\ell-1}(x)\} \subset X$ a ostatní prvky definujeme jako samodružné, dostáváme cyklus. Evidentně je pak celá původní permutace X složením všech těchto cyklů a je jedno v jakém pořadí cykly skládáme.

Pro určení parity si nyní stačí povšimnout, že cykly sudé délky lze napsat jako lichý počet transpozic, proto mají paritu -1. Obdobně cyklus liché délky dostaneme ze sudého počtu transpozic a proto mají paritu 1.

2.12

2.17. Jednoduché vlastnosti determinantu. Poznání vlastností permutací a jejich parit z předchozích odstavců nám teď umožní rychle odvodit základní vlastnosti detemrintů.

Pro každou matici $A = (a_{ij})$ typu m/n nad skaláry z $\mathbb{K}$ definujeme *matici transponovanou* k A. Jde o matici $A^T = (a'_{ij})$ s prvky $a'_{ij} = a_{ji}$, která je typu n/m.

Čtvercová matice A s vlastností $A = A^T$ se nazývá *symetrická*. Jestliže platí $A = -A^T$, pak se A nazývá *antisymetrická*.

Věta. *Pro každou čtvercovou matici $A = (a_{ij})$ platí*

(1) $|A^T| = |A|$,
(2) Je-li jeden řádek v A tvořen nulovými prvky z $\mathbb{K}$, pak $|A| = 0$,
(3) Jestliže matice B vznikla z A výměnou dvou řádků, pak $|A| = -|B|$,
(4) Jestliže matice B vznikla z A vynásobením řádku skalárem $a \in \mathbb{K}$, pak $|B| = a\,|A|$,
(5) Jsou-li prvky k-tého řádku v A tvaru $a_{kj} = c_{kj} + b_{kj}$ a všechny ostatní řádky v maticích A, $B = (b_{ij})$, $C = (c_{ij})$ jsou stejné, pak $|A| = |B| + |C|$,
(6) Determinant $|A|$ se nezmění, přičteme-li k libovolnému řádku A lineární kombinaci ostatních řádků.

Jednoduché vlastnosti determinantů

DŮKAZ. (1) Členy determinantů $|A|$ a $|A^T|$ jsou v bijektivní korespondenci. Členu $\operatorname{sgn}(\sigma)a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdots a_{n\sigma(n)}$ přitom v A^T odpovídá člen (na pořadí skalárů v součinu totiž nezáleží)

$$\begin{aligned}\operatorname{sgn}(\sigma)a_{\sigma(1)1} \cdot a_{\sigma(2)2} \cdots a_{\sigma(n)n} &= \\ &= \operatorname{sgn}(\sigma)a_{1\sigma^{-1}(1)} \cdot a_{2\sigma^{-1}(2)} \cdots a_{n\sigma^{-1}(n)},\end{aligned}$$

přičemž musíme ověřit, že je tento člen opatřen správným znaménkem. Parita σ a σ^{-1} je ale stejná, jde tedy opravdu o člen $|A^T|$ a první tvrzení je dokázáno.

(2) Plyne přímo z definice determinantu, protože všechny jeho členy obsahují z každého řádku právě jeden člen, a je-li jeden z řádků nulový, budou tedy všechny nulové.

(3) Ve všech členech $|B|$ dojde ve srovnání s determinantem $|A|$ u permutací k přidání jedné transpozice, znaménko všech členů determinantu tedy bude opačné.

(4) Vyplývá přímo z definice, protože členy determinantu $|B|$ jsou členy $|A|$ vynásobené skalárem a.

(5) V každém členu $|A|$ je právě jeden součinitel z k-tého řádku matice A. Protože platí distributivní zákon pro násobení a sčítání v $\mathbb{K}$, vyplývá tvrzení přímo z definičního vztahu pro determinanty.

(6) Jsou-li v A dva stejné řádky, jsou mezi členy determinantu vždy dva sčítance stejné až na znaménko. Proto je v takovém případě $|A| = 0$. Je tedy podle tvrzení (5) možné přičíst k vybranému řádku libovolný jiný řádek, aniž by se zmněnila hodnota determinantu. Vzhledem k tvrzení (4) lze ale přičíst i skalární násobek libovolného jiného řádku. □

2.13

2.18. Výpočetní důsledky. Podle předchozí věty umíme převést elementárními řádkovými transformacemi každou čtvercovou matici A na řádkově schodovitý tvar, aniž bychom změnili hodnotu jejího determinantu. Jen musíme dávat pozor, abychom vždy k upravovanému řádku pouze přičítali lineární kombinace řádků ostatních.

Je-li matice A v řádkovém schodovitém tvaru, pak v každém členu $|A|$ je alespoň jeden součinitel prvkem pod diagonálou s výjimkou případu, kdy jsou všechny jen na diagonále. Pak je ale jediným nenulovým členem determinantu ten, který odpovídá identické permutaci. Vidíme tedy, že determinant takové matice ve schodovitém tvaru je

$$|A| = a_{11} \cdot a_{22} \cdot \dots \cdot a_{nn}.$$

Předchozí věta tedy poskytuje velice efektivní metodu výpočtu determinantů pomocí Gaussovy eliminační metody, viz 2.7.

Výpočet determinantů eliminací

Všimněme si také hezkého důsledku prvního tvrzení předchozí věty o rovnosti determinantů matice a matice transponované. Zaručuje totiž, že kdykoliv se nám podaří dokázat nějaké tvrzení o determinantech formulované s využitím řádků příslušné matice, pak analogické tvrzení platí i pro sloupce. Např. tedy můžeme okamžitě všechna tvrzení (2)–(6) této věty přeformulovat i pro přičítání lineárních kombinací ostatních sloupců k vybranému.

Dále si všimněme, že vlastnosti (3)–(5) z předchozí věty říkají, že determinant jakožto zobrazení, které n vektorům dimenze n (řádkům nebo sloupcům matice) přiřadí skalár, je antisymetrické zobrazení lineární v každém svém argumentu, přesně jako jsme podle analogie z dimenze 2 požadovali.

2.14

2.19. Další vlastnosti determinantu. Časem uvidíme, že skutečně stejně jako v dimenzi dva je determinant matice roven orientovanému objemu rovnoběžnostěnu určeného jejími sloupci. Uvidíme také, že když uvážíme zobrazení $x \mapsto A \cdot x$

zadané čtvercovou maticí A na $\mathbb{R}^n$, pak můžeme determinant této matice vidět jako vyjádření poměru mezi objemem rovnoběžnostěnů daných vektory $x_1, \dots x_n$ a jejich obrazy $A \cdot x_1, \dots, A \cdot x_n$. Protože skládání zobrazení $x \mapsto A \cdot x \mapsto B \cdot (A \cdot x)$ odpovídá násobení matic, je snad docela pochopitelná tzv. *Cauchyova věta*:

Věta. *Nechť $A = (a_{ij})$, $B = (b_{ij})$ jsou čtvercové matice dimenze n nad okruhem skalárů $\mathbb{K}$. Pak $|A \cdot B| = |A| \cdot |B|$.*

Cauchyova věta

My teď tuto větu odvodíme ryze algebraicky už proto, že předchozí odvolávka na geometrický argument těžko může fungovat pro jakékoliv skaláry. Základním nástrojem je tzv. *rozvoj determinantu* podle jednoho nebo více řádků či sloupců. Budeme potřebovat něco málo technické přípravy. Čtenář, který by snad tolik abstrakce neztrávil může tyto pasáže přeskočit a vstřebat pouze znění Laplaceovy věty a jejich důsledků.

1.14a

2.20. Minory matice. Nechť $A = (a_{ij})$ je matice typu m/n a $1 \le i_1 < \dots < i_k \le m$, $1 \le j_1 < \dots < j_l \le n$ jsou pevně zvolená přirozená čísla. Pak matici

$$M = \begin{pmatrix} a_{i_1 j_1} & a_{i_1 j_2} & \dots & a_{i_1 j_\ell} \\ \vdots & & & \vdots \\ a_{i_k j_1} & a_{i_k j_2} & \dots & a_{i_k j_\ell} \end{pmatrix}$$

typu k/ℓ nazýváme *submaticí matice A* určenou řádky $i_1, \dots, i_k$ a sloupci $j_1, \dots, j_\ell$. Zbývajícími $(m - k)$ řádky a $(n - l)$ sloupci je určena matice M^* typu $(m - k)/(n - \ell)$, která se nazývá *doplňková submatice* k M v A. Při $k = \ell$ je definován $|M|$, který nazýváme *subdeterminant* nebo *minor* řádu k matice A. Je-li $m = n$, pak při $k = \ell$ je i M^* čtvercová a $|M^*|$ se nazývá *doplněk minoru* $|M|$, nebo *doplňkový minor* k submatici M v matici A. Skalár

$$(-1)^{i_1+\dots+i_k+j_1+\dots+j_l} \cdot |M^*|$$

se nazývá *algebraický doplněk* k minoru $|M|$.

Submatice tvořené prvními k řádky a sloupci se nazývají *hlavní submatice*, jejich determinanty *hlavní minory* matice A.

Při speciální volbě $k = \ell = 1$, $m = n$ hovoříme o *algebraickém doplňku A_{ij}* prvku a_{ij} matice A.

Pokud je $|M|$ hlavní minor matice A řádu k, pak přímo z definice determinantu je vidět, že každý z jednotlivých $k!(n - k)!$ sčítanců v součinu $|M|$ s jeho algebraickým doplňkem je členem determinantu $|A|$.

Obecně, uvažme submatici M, tj. čtvercovou matici, určenou řádky $i_1 < i_2 < \dots < i_k$ a sloupci $j_1 < \dots < j_k$. Pak pomocí $(i_1 - 1) + \dots + (i_k - k)$ výměn sousedních řádků a $(j_1 - 1) + \dots + (j_k - k)$ výměn sousedních sloupců v A převedeme tuto submatici M na hlavní submatici a doplňková matice přitom přejde právě na doplňkovou matici. Celá matice A přejde přitom v matici B, pro kterou platí podle 2.17 a definice determinantu $|B| = (-1)^{\alpha}|A|$, kde $\alpha = \sum_{h=1}^{k}(i_h - j_h) - 2(1 + \cdots + k)$. Tím jsme ověřili:

Tvrzení. *Jestliže je A je čtvercová matice dimenze n a $|M|$ je její minor řádu $k < n$, pak součin libovolného členu $|M|$ s libovolným členem jeho algebraického doplňku je členem $|A|$.*

Toto tvrzení už podbízí představu, že by se pomocí takových součinů menších determinantů skutečně mohl determinant matic vyjadřovat. Víme, že $|A|$ obsahuje právě $n!$ různých členů, právě jeden pro každou permutaci. Tyto členy jsou navzájem různé jakožto polynomy v prvcích (neznámé obecné) matice A. Jestliže tedy ukážeme, že navzájem různých výrazů z předchozího tvrzení je právě tolik jako je tomu u determinantu $|A|$, pak dostaneme jejich součtem právě determinant.

Zbývá proto ukázat, že uvažované součiny $|M| \cdot |M^*|$ obsahují právě $n!$ různých členů z $|A|$.

Ze zvolených k řádků lze vybrat $\binom{n}{k}$ minorů M a podle předchozího lematu je každý z $k!(n-k)!$ členů v součinech $|M|$ s jejich algebraickými doplňky členem $|A|$. Přitom pro různé výběry M nemůžeme nikdy obdržet stejné členy a jednotlivé členy v $(-1)^{i_1+\cdots+i_k+j_1+\cdots+j_l} \cdot |M| \cdot |M^*|$ jsou také po dvou různé. Celkem tedy máme právě požadovaný počet $k!(n-k)!\binom{n}{k} = n!$ členů.

Tím jsme bezezbytku dokázali tzv. *Laplaceovu větu*:

Věta. *Nechť $A = (a_{ij})$ je čtvercová matice dimenze n nad libovolným okruhem skalárů a nechť je pevně zvoleno k jejích řádků. Pak $|A|$ je součet všech $\binom{n}{k}$ součinů $(-1)^{i_1+\cdots+i_k+j_1+\cdots+j_l} \cdot |M| \cdot |M^*|$ minorů řádu k vybraných ze zvolených řádků, s jejich algebraickými doplňky.*

Laplaceova věta

Uvedená věta převádí výpočet $|A|$ na výpočet determinantů nižšího stupně. Této metodě výpočtu se říká *Laplaceův rozvoj* podle zvolených řádků či sloupců. Např. rozvoj podle i-tého řádku nebo i-tého sloupce:

$$|A| = \sum_{j=1}^{n} a_{ij}A_{ij} = \sum_{j=1}^{n} a_{ji}A_{ji}$$

kde A_{ij} označuje algebraický doplněk k prvku a_{ij} (tj. k minoru stupně 1).

Při praktickém počítání determinantů bývá výhodné kombinovat Laplaceův rozvoj s přímou metodou přičítání lineárních kombinací řádků či sloupců.

2.21. Důkaz Cauchyovy věty. Důkaz se opírá o trikovou ale elementární aplikaci Laplaceovy věty. Použijeme prostě dvakrát Laplaceův rozvoj na vhodné matice:

Uvažme nejprve matici H dimenze $2n$ (používáme tzv. blokovou symboliku, tj. píšeme matici jakoby složenou ze (sub)matic A, B atd.)

$$H = \begin{pmatrix} A & 0 \\ -E & B \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} & 0 & \dots & 0 \\ -1 & & 0 & b_{11} & \dots & b_{1n} \\ & \ddots & & \vdots & & \vdots \\ 0 & & -1 & b_{n1} & \dots & b_{nn} \end{pmatrix}$$

Laplaceovým rozvojem podle prvních n řádků obdržíme právě $|H| = |A| \cdot |B|$.

Nyní budeme k posledním n sloupcům postupně přičítat lineární kombinace prvních n sloupců tak, abychom obdrželi matici s nulami v pravém dolním rohu. Dostaneme

$$K = \begin{pmatrix} a_{11} & \dots & a_{1n} & c_{11} & \dots & c_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} & c_{n1} & \dots & c_{nn} \\ -1 & & 0 & 0 & \dots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & -1 & 0 & \dots & 0 \end{pmatrix}.$$

Prvky submatice nahoře vpravo přitom musí splňovat

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

neboli jde právě o prvky součinu $A \cdot B$ a $|K| = |H|$. Přitom rozvojem podle posledních n sloupců dostáváme

$$|K| = (-1)^{n+1+\dots+2n}|A \cdot B| = (-1)^{2n\cdot(n+1)} \cdot |A \cdot B| = |A \cdot B|.$$

Tím je Cauchyova věta bezezbytku dokázána.

2.16

2.22. Determinant a inverzní matice. Předpokládejme nejprve, že existuje matice inverzní k matici A, tj. $A \cdot A^{-1} = E$. Protože pro jednotkovou matici platí vždy $|E| = 1$, je pro každou invertibilní matici vždy $|A|$ invertibilní skalár a díky Cauchyově větě platí $|A|^{-1} = |A^{-1}|$.

My však nyní kombinací Laplaceovy věty a Cauchyho věty umíme říci víc.

Pro libovolnou čtvercovou matici $A = (a_{ij})$ dimenze n definujeme matici $A^* = (a^*_{ij})$, kde $a^*_{ij} = A_{ji}$ jsou algebraické doplňky k prvkům a_{ji} v A. Matici A^* nazýváme *algebraicky adjungovaná matice* k matici A.

Věta. *Pro každou čtvercovou matici A nad okruhem skalárů $\mathbb{K}$ platí*

e2.1a (2.1) $$AA^* = A^*A = |A| \cdot E.$$

Zejména tedy

(1) A^{-1} existuje jako matice nad okruhem skalárů $\mathbb{K}$ právě, když $|A|^{-1}$ existuje v $\mathbb{K}$.
(2) Pokud existuje A^{-1}, pak platí $A^{-1} = |A|^{-1} \cdot A^*$.

Vzorec pro inverzní matici

Důkaz. Jak jsme již zmínili, Cauchyova věta ukazuje, že z existence A^{-1} vyplývá invertibilita $|A| \in \mathbb{K}$.

Pro libovolnou čtvercovou matici A spočteme přímým výpočtem $A \cdot A^* = (c_{ij})$, kde

$$c_{ij} = \sum_{k=1}^{n} a_{ik} a^*_{kj} = \sum_{k=1}^{n} a_{ik} A_{jk}.$$

Pokud $i = j$ je to právě Laplaceův rozvoj $|A|$ podle i-tého řádku. Pokud $i \neq j$ jde o rozvoj determinantu matice v níž je i-tý a j-tý řádek stejný a proto je $c_{ij} = 0$. Odtud plyne $A \cdot A^* = |A| \cdot E$ a dokázali jsme rovnost (2.1).

Předpokládejme navíc, že $|A|$ je invertibilní skalár. Jestliže zopakujeme předešlý výpočet pro $A^* \cdot A$, obdržíme $|A|^{-1} A^* \cdot A = E$. Proto náš výpočet skutečně dává inverzní matici A, jak je tvrzeno ve větě. □

3. Vektorové prostory a lineární zobrazení

Vraťme se teď na chvilku k systémům m lineárních rovnic pro n proměnných z 2.3 a předpokládejme navíc, že jde o rovnice tvaru $A \cdot x = 0$, tj.

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Díky vlastnosti distributivity pro násobení matic je zřejmé, že součet dvou řešení $x = (x_1, \dots, x_n)$ a $y = (y_1, \dots, y_n)$ splňuje

$$A \cdot (x + y) = A \cdot x + A \cdot y = 0$$

a je tedy také řešením. Stejně tak zůstává řešením i skalární násobek $a \cdot x$. Množina všech řešení pevně zvoleného systému rovnic je proto uzavřená na sčítání vektorů a násobení vektorů skaláry. To byly základní vlastnosti vektorů dimenze n v $\mathbb{K}^n$, viz 2.1. Teď ale máme vektory v prostoru řešení s n souřadnicemi a „dimenze“ tohoto prostoru určitě nemá být n (pokud matice systému není nulová). Případy dvou rovnic pro dvě neznámé jsme potkali při řešení geometrických problémů v rovině v 1.25 a pro dvě závislé rovnice byl množinou všech řešení „jednorozměrný“ prostor – přímka. U dvou nezávislých rovnic to byl průsečík dvou přímek, tj. „nularozměrný“ prostor.

2.17

2.23. Abstraktní vektorové prostory. Už v 1.12, jsme ale potkali ještě zajímavější příklad prostoru všech řešení homogenní lineární diferenční rovnice (druhého řádu). Opět jsme dvě řešení mohli libovolně kombinovat pomocí sčítání a násobení skaláry a dostali jsme tak všechna možná řešení. Tyto „vektory“ ovšem jsou nekonečné posloupnosti čísel, přestože intuitivně očekáváme, že dimenze celého prostoru řešení by měla být dvě. Potřebujeme proto obecnější definici vektorového prostoru a jeho dimenze:

Vektorovým prostorem V nad polem skalárů $\mathbb{K}$ rozumíme množinu, na které jsou definovány

- operace sčítání splňující axiomy 1.1(KG1)–(KG4),
- násobení skaláry, pro které platí axiomy 2.1(V1)–(V4).

Definice vektorového prostoru

Připomeňme naši jednoduchou konvenci ohledně značení: skaláry budou zpravidla označovány znaky z počátku abecedy, tj. $a, b, c, \dots$, zatímco pro vektory budeme užívat znaky z konce, u, v, w, x, y, z. Přitom ještě navíc většinou x, y, z budou opravdu n-tice skalárů. Pro úplnost výčtu, písmena z prostředka, např. i, j, k, ℓ budou nejčastěji označovat indexy výrazů.

Abychom se trochu pocvičili ve formálním postupu, ověříme jednoduché vlastnosti vektorů, které pro n-tice skalárů byly samozřejmé, nicméně teď je musíme odvodit z axiomů.

Tvrzení. *Nechť V je vektorový prostor nad polem skalárů $\mathbb{K}$, dále uvažme $a, b, a_i \in \mathbb{K}$, vektory $u, v, u_j \in V$. Potom*

(1) $a \cdot u = 0$ *právě když* $a = 0$ *nebo* $u = 0$
(2) $(-1) \cdot u = -u$
(3) $a \cdot (u - v) = a \cdot u - a \cdot v$
(4) $(a - b) \cdot u = a \cdot u - b \cdot u$
(5) $\left(\sum_{i=1}^{n} a_i\right) \cdot \left(\sum_{j=1}^{m} u_j\right) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \cdot u_j$.

Důkaz. Můžeme rozepsat

$$(a + 0) \cdot u \overset{(V2)}{=} a \cdot u + 0 \cdot u = a \cdot u$$

což podle axiomu (KG4) zaručuje $0 \cdot u = 0$. Nyní

$$u + (-1) \cdot u \overset{(V2)}{=} (1 + (-1)) \cdot u = 0 \cdot u = 0$$

a odtud $-u = (-1) \cdot u$. Dále

$$a \cdot (u + (-1) \cdot v) \overset{(V2,V3)}{=} a \cdot u + (-a) \cdot v = a \cdot u - a \cdot v$$

což dokazuje (3). Platí

$$(a - b) \cdot u \overset{(V2,V3)}{=} a \cdot u + (-b) \cdot u = a \cdot u - b \cdot u$$

a tím je ověřeno (4). Vztah (5) plyne indukcí z (V2) a (V1).

Zbývá (1): $a \cdot 0 = a \cdot (u - u) = a \cdot u - a \cdot u = 0$, což spolu s prvním tvrzením tohoto důkazu ukazuje jednu implikaci. K opačné implikaci poprvé potřebujeme axiom pole pro skaláry a axiom (V4) pro vektorové prostory: je-li $p \cdot u = 0$ a $p \neq 0$, pak $u = 1 \cdot u = (p^{-1} \cdot p) \cdot u = p^{-1} \cdot 0 = 0$. □

2.17a **2.24. Lineární (ne)závislost.** V odstavci 2.11 jsme pracovali s tzv. lineárními kombinacemi řádků matice. S obecnými vektory budeme zacházet zcela analogicky:

Výrazy tvaru $a_1 \cdot v_1 + \dots + a_k \cdot v_k$ nazýváme *lineární kombinace* vektorů $v_1, \dots, v_k \in V$. Množina vektorů $M \subset V$ ve vektorovém prostoru V nad $\mathbb{K}$ se nazývá *lineárně nezávislá* jestliže pro každou k-tici vektorů $v_1, \dots, v_k \in M$ a každé skaláry $a_1, \dots, a_k \in \mathbb{K}$ platí:

$$a_1 \cdot v_1 + \dots + a_k \cdot v_k = 0 \quad \Longrightarrow \quad a_1 = a_2 = \dots = a_k = 0.$$

Posloupnost vektorů $v_1, \dots, v_k$ nazveme *lineárně nezávislou* jestliže $v_1, \dots, v_k$ jsou po dvou různé a $\{v_1, \dots, v_k\}$ je lineárně nezávislá.

Množina M vektorů je *lineárně závislá*, jestliže není lineárně nezávislá.

Lineární kombinace a nezávislost

Přímo z definice pak vyplývá, že neprázdná podmnožina M vektorů ve vektorovém prostoru nad polem skalárů $\mathbb{K}$ je závislá právě, když je jeden z jejích vektorů vyjádřitelný jako lineární kombinace ostatních. Skutečně, alespoň jeden koeficient ve výrazu musí být nenulový a protože jsme nad polem skalárů, můžeme jím podělit a vyjádřit tak u něj stojící vektor pomocí ostatních.

Každá podmnožina lineárně nezávislé množiny M je samozřejmě také lineárně nezávislá (požadujeme stejné podmínky na méně vektorů). Stejně snadno vidíme, že $M \subset V$ je lineárně nezávislá právě tehdy, když každá konečná podmnožina v M je lineárně nezávislá.

2.18

2.25. Generátory a podprostory. Podmnožina $M \subset V$ se nazývá *vektorovým podprostorem* jestliže spolu se zúženými operacemi sčítání a násobení skaláry je sama vektorovým prostorem. Tzn. požadujeme

$$\forall a, b \in \mathbb{K},\ \forall v, w \in M,\ a \cdot v + b \cdot w \in M.$$

Rozeberme si hned několik příkladů: Prostor m–tic skalárů $\mathbb{R}^m$ se sčítáním a násobením po složkách je vektorový prostor nad $\mathbb{R}$, ale také vektorový prostor nad $\mathbb{Q}$. Např. pro $m = 2$, jsou vektory $(1, 0), (0, 1) \in \mathbb{R}^2$ lineárně nezávislé, protože z

$$a \cdot (1, 0) + b \cdot (0, 1) = (0, 0)$$

plyne $a = b = 0$. Dále, vektory $(1, 0), (\sqrt{2}, 0) \in \mathbb{R}^2$ jsou lineárně závislé nad $\mathbb{R}$, protože $\sqrt{2} \cdot (1, 0) = (\sqrt{2}, 0)$, ovšem nad $\mathbb{Q}$ jsou lineárně nezávislé! Nad $\mathbb{R}$ tedy tyto dva vektory „generují" jednorozměrný podprostor, zatímco nad $\mathbb{Q}$ je dvourozměrný.

Polynomy stupně nejvýše m tvoří vektorový prostor $\mathbb{R}_m[x]$. Polynomy můžeme chápat jako zobrazení $f : \mathbb{R} \to \mathbb{R}$ a sčítání a násobení skaláry definujeme takto: $(f + g)(x) = f(x) + g(x)$, $(a \cdot f)(x) = a \cdot f(x)$. Polynomy všech stupňů také tvoří vektorový prostor $\mathbb{R}_\infty[x]$ a $\mathbb{R}_m[x] \subset \mathbb{R}_n[x]$ je vektorový podprostor pro všechna $m \le n \le \infty$. Podprostory jsou také např. všechny sudé polynomy nebo liché polynomy, tj. splňující $f(-x) = \pm f(x)$.

Úplně analogicky jako u polynomů můžeme definovat strukturu vektorového prostoru na množině všech zobrazení

$\mathbb{R} \to \mathbb{R}$ nebo všech zobrazení $M \to V$ libovolné pevně zvolené množiny M do vektorového prostoru V.

Protože podmínka v definici podprostoru obsahuje pouze univerzální kvantifikátory, je jistě průnik podprostorů opět podprostor. Snadno to ověříme i přímo: Nechť W_i, $i \in I$, jsou vektorové podprostory ve V, $a, b \in \mathbb{K}$, $u, v \in \cap_{i \in I} W_i$. Pak pro všechny $i \in I$, $a \cdot u + b \cdot v \in W_i$, to ale znamená, že $a \cdot u + b \cdot v \in \cap_{i \in I} W_i$.

Zejména je tedy podprostorem průnik všech podprostorů $W \subset V$, které obsahují předem danou množinu vektorů $M \subset V$. Říkáme, že takto M *generuje* podprostor $\langle M \rangle$, nebo že prvky M jsou *generátory* podprostoru $\langle M \rangle$.

Zformulujme opět několik jednoduchých tvrzení o generování podprostorů:

Tvrzení. *Pro každou podmnožinu $M \subset V$ platí*

(1) $\langle M \rangle = \{a_1 \cdot u_1 + \dots + a_k \cdot u_k;\ k \in \mathbb{N}, a_i \in \mathbb{K}, u_j \in M, j = 1, \dots, k\}$*;*
(2) $M = \langle M \rangle$ *právě když* M *je vektorový podprostor;*
(3) jestliže $N \subset M$ *pak* $\langle N \rangle \subset \langle M \rangle$ *je vektorový podprostor;*
(4) $\langle \emptyset \rangle = \{0\} \subset V$*, triviální podprostor.*

Důkaz. (1) Množina všech lineárních kombinací $a_1 u_1 + \dots + a_k u_k$ na pravé straně (1) je jistě vektorový podprostor a samozřejmě obsahuje M. Naopak, každá z jednotlivých lineárních kombinací nutně musí být v $\langle M \rangle$ a první tvrzení je dokázáno.

Tvrzení (2) vyplývá okamžitě z (1) a z definice vektorového podprostoru a obdobně je z prvního tvrzení zřejmé i tvrzení třetí.

Konečně, nejmenší vektorový podprostor je $\{0\}$, protože prázdnou množinu obsahují všechny podprostory a každý z nich obsahuje 0. □

2.19 **2.26. Součty podprostorů.** Když už máme představu o generátorech a jimi vytvářených podprostorech, měli bychom rozumět i možnostem, jak několik podprostorů může vytvářet celý vektorový prostor V.

Nechť V_i, $i \in I$, jsou podprostory ve V. Pak podprostor generovaný jejich sjednocením, tj. $\langle \cup_{i \in I} V_i \rangle$, nazýváme *součtem podprostorů* V_i. Značíme $\sum_{i \in I} V_i$. Zejména pro $V_1, \dots, V_k \subset V$,

$$V_1 + \dots + V_k = \langle V_1 \cup V_2 \cup \dots \cup V_k \rangle.$$

Součty podprostorů

Vidíme jsme, že každý prvek v uvažovaném součtu podprostorů můžeme vyjádřit jako lineární kombinaci vektorů z podprostorů V_i. Protože však je sčítání vektorů komutativní, lze k sobě poskládat členy patřící do stejného podprostoru a pro konečný součet k podprostorů tak dostáváme

$$V_1 + V_2 + \dots + V_k = \{v_1 + \dots + v_k;\ v_i \in V_i, i = 1, \dots, k\}.$$

Součet $W = V_1 + \dots + V_k \subset V$ se nazývá *přímý součet* podprostorů, jsou-li průniky všech dvojic triviální, tj. $V_i \cap$

$V_j = \{0\}$ pro všechny $i \neq j$. Ukážeme, že v takovém případě lze každý vektor $w \in W$ napsat právě jedním způsobem jako součet

$$w = v_1 + \cdots + v_k,$$

kde $v_i \in V_i$. Skutečně, pokud by tento vektor šlo zároveň vyjádřit, jako $w = v_1' + \cdots + v_k'$, potom

$$0 = w - w = (v_1 - v_1') + \cdots + (v_k - v_k').$$

Pokud bude $v_i - v_i'$ první nenulový člen na pravé straně, pak tento vektor z V_i umíme vyjádřit pomocí vektorů z ostatních podprostorů. To je ale ve sporu s předpokladem, že V_i má se všemi ostatními nulový průnik. Jedinou možností tedy je, že všechny vektory na pravé straně jsou nulové a tedy je rozklad w jednoznačný.

Pro přímé součty podprostorů píšeme

$$W = V_1 \oplus \cdots \oplus V_k = \oplus_{i=1}^k V_i.$$

2.19a

2.27. Báze. Nyní máme vše připravené pochopení minimálních množin generátorů tak, jak jsme to dělali v rovnině $\mathbb{R}^2$.

Podmnožina $M \subset V$ se nazývá *báze vektorového prostoru* V, jestliže $\langle M \rangle = V$ a M je lineárně nezávislá.

Vektorový prostor, který má konečnou bázi nazýváme *konečněrozměrný*, mohutnost báze nazýváme *dimenzí* V.

Nemá-li V konečnou bázi, říkáme, že V je *nekonečněrozměrný*. Píšeme $\dim V = k$, $k \in \mathbb{N}$, případně $k = \infty$.

Báze vektorových prostorů

Všimněme si, že triviální podprostor je generován prázdnou množinou, která je "prázdnou"bazí. Má tedy triviální podprostor dimenzi nulovou.

Bázi k-rozměrného prostoru budeme obvykle zapisovat jako k-tici $\underline{v} = (v_1 \dots, v_k)$ bázových vektorů. Jde tu především o zavedení konvence: U konečněrozměrných podprostorů budeme totiž vždy uvažovat bázi včetně zadaného pořadí prvků i když jsme to takto, striktně vzato, nedefinovali.

Zjevně, je-li $(v_1, \dots, v_n)$ bazí V, je celý prostor V přímým součtem jednorozměrných podprostorů

$$V = \langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle.$$

Okamžitým důsledkem výše odvozené jednoznačnosti rozkladu jakéhokoliv vektoru ve V do komponent v přímém součtu dává jednoznačné vyjádření

$$w = x_1 v_1 + \cdots + x_n v_n$$

a dovoluje nám tedy po volbě báze opět vidět vektory jako n–tici skalárů. K tomuto pohledu se vrátíme v zápětí v odstavci 2.31, jak jen dokončíme diskusi existence bazí a součtů podprostorů v obecné poloze.

2.20

2.28. Věta. *Z libovolné konečné množiny generátorů vektorového prostoru V lze vybrat bázi. Každá báze V má přitom stejný počet prvků.*

Důkaz. První tvrzení ukážeme snadno indukcí přes počet generátorů k.

Jedině nulový podprostor nepotřebuje žádný generátor a tedy umíme vybrat prázdnou bázi. Naopak, nulový vektor vybrat nesmíme (generátory by byly lineárně závislé) a nic jiného už v podprostoru není.

Abychom měli indukční krok přirozenější, probereme ještě přímo případ $k = 1$. Máme $V = \langle\{v\}\rangle$ a $v \neq 0$ protože $\{v\}$ je lineárně nezávislá množina vektorů. Pak je ovšem $\{v\}$ zároveň báze V.

Předpokládejme, že tvrzení platí pro $k = n$, a uvažme $V = \langle v_1, \dots, v_{n+1}\rangle$. Jsou-li $v_1, \dots, v_{n+1}$ lineárně nezávislé, pak tvoří bázi. V opačném případě existuje index i takový, že

$$v_i = a_1 v_1 + \cdots + a_{i-1} v_{i-1} + a_{i+1} v_{i+1} + \cdots + a_{n+1} v_{n+1}.$$

Pak ovšem $V = \langle v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_{n+1}\rangle$ a již umíme vybrat bázi (podle indukčního předpokladu).

Zbývá ověřit, že báze mají vždy stejný počet prvků. Uvažujme bázi $(v_1, \dots, v_n)$ prostoru V a libovolný nenulový vektor

$$u = a_1 v_1 + \cdots + a_n v_n \in V$$

s $a_i \neq 0$ pro jisté i. Pak

$$v_i = \frac{1}{a_i}\big(u - (a_1 v_1 + \cdots + a_{i-1} v_{i-1} + a_{i+1} v_{i+1} + \cdots + a_n v_n)\big)$$

a proto také $\langle u, v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n\rangle = V$. Jistě je to opět báze, protože vektory $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$ byly nezávislé, takže kdyby přidáním u vznikly lineárně závislé vektory, pak by u bylo jejich lineární kombinací, ale to by znamenalo

$$V = \langle v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n\rangle,$$

což není možné. Takže už víme, že pro libovolný nenulový vektor $u \in V$ existuje i, $1 \leq i \leq n$, takové, že $(u, v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n)$ je opět báze V.

Dále budeme místo jednoho vektoru u uvažovat lineárně nezávislou množinu $u_1, \dots, u_k$ a budeme postupně přidávat $u_1, u_2, \dots$, vždy výměnou za vhodné v_i podle předchozího postupu. Je třeba pouze ověřit, že takové v_i vždy bude existovat (tj. že se nebudou vektory u vyměňovat vzájemně). Předpokládejme tedy, že již máme umístěné $u_1, \dots, u_\ell$. Pak $u_{\ell+1}$ se jistě vyjádří jako lineární kombinace těchto vektorů a zbylých v_j. Pokud by pouze koeficienty u $u_1, \dots, u_\ell$ byly nenulové, znamenalo by to, že již samy vektory $u_1, \dots, u_{\ell+1}$ byly lineárně závislé, což je ve sporu s našimi předpoklady.

Pro každé $k \leq n$ tak po k krocích získáme bázi ve které z původní došlo k výměně k vektorů za nové. Pokud by $k > n$, pak již v n-tém kroku obdržíme bázi vybranou z nových vektorů u_i, což znamená, že tyto nemohou být lineárně nezávislé. Zejména tedy není možné, aby dvě báze měly různý počet prvků. □

Ve skutečnosti jsme dokázali silnější tvrzení, tzv. *Steinitzovu větu o výměně*, která říká, že pro každou konečnou bázi $\underline{v}$ a každý systém lineárně nezávislých vektorů ve V umíme najít podmnožinu bázových vektorů v_i, po jejichž záměně za zadané nové vektory opět dostaneme bázi.

2.20a

2.29. Důsledky Steinitzovy věty o výměně. Díky možnosti volně volit a vyměňovat bázové vektory můžeme okamžitě dovodit pěkné (a intuitivně snad také očekávané) vlastnosti bazí vektorových prostorů:

Tvrzení. *(1) Každé dvě báze konečněrozměrného vektorového prostoru mají stejný počet vektorů, tzn. že naše definice dimenze nezávisí na volbě báze.*
(2) Má-li V konečnou bázi, lze každou lineárně nezávislou množinu doplnit do báze.
(3) Báze konečněrozměrných vektorových prostorů jsou právě maximální lineárně nezávislé množiny.
(4) Báze prostoru s konečnou dimenzí jsou právě minimální množiny generátorů.

Malinko složitější, ale nyní snadno zvládnutelná, je situace kolem dimenzí podprostorů a jejich součtů:

Důsledek. *Nechť $W, W_1, W_2 \subset V$ jsou podprostory v prostoru konečné dimenze. Pak platí*
(1) $\dim W \le \dim V$
(2) $V = W$ *právě když* $\dim V = \dim W$
(3) $\dim W_1 + \dim W_2 = \dim(W_1 + W_2) + \dim(W_1 \cap W_2)$.

Důkaz. Zbývá dokázat pouze poslední tvrzení. To je zřejmé, pokud je dimenze jednoho z prostorů nulová. Předpokládejme tedy $\dim W_1 = r \neq 0$, $\dim W_2 = s \neq 0$ a nechť $(w_1 \dots, w_t)$ je báze $W_1 \cap W_2$ (nebo prázdná množina, pokud je průnik triviální).

Podle Steinitzovy věty o výměně lze tuto bázi doplnit na bázi $(w_1, \dots, w_t, u_{t+1} \dots, u_r)$ pro W_1 a bázi $(w_1 \dots, w_t, v_{t+1}, \dots, v_s)$ pro W_2. Vektory

$$w_1, \dots, w_t, u_{t+1}, \dots, u_r, v_{t+1} \dots, v_s$$

jistě generují $W_1 + W_2$. Ukážeme, že jsou přitom lineárně nezávislé. Nechť tedy

$$a_1 w_1 + \dots + a_t w_t + b_{t+1} u_{t+1} + \dots + b_r u_r + c_{t+1} v_{t+1} + \dots + c_s v_s = 0$$

Pak nutně

$$\begin{aligned} &-(c_{t+1} \cdot v_{t+1} + \dots + c_s \cdot v_s) = \\ &= a_1 \cdot w_1 + \dots + a_t \cdot w_t + b_{t+1} \cdot u_{t+1} + \dots + b_r \cdot u_r \end{aligned}$$

musí patřit do $W_2 \cap W_1$. To ale má za následek, že

$$b_{t+1} = \dots = b_r = 0,$$

protože tak jsem doplňovali naše báze. Pak ovšem i

$$a_1 \cdot w_1 + \dots + a_t \cdot w_t + c_{t+1} \cdot v_{t+1} + \dots + c_s \cdot v_s = 0$$

a protože příslušné vektory tvoří bázi W_2, jsou všechny koeficienty nulové.

Tvrzení (3) se nyní ověří přímým počítáním generátorů.

□

2.21 **2.30. Příklady.** (1) $\mathbb{K}^n$ má (jako vektorový prostor nad $\mathbb{K}$) dimenzi n. Bazí je např. n-tice vektorů

$$((1,0,\dots,0),(0,1,\dots,0)\dots,(0,\dots,0,1)).$$

Tuto bázi nazýváme *standardní báze v* $\mathbb{K}^n$. V případě konečného pole skalárů, např. $\mathbb{Z}_k$, má celý vektorový prostor $\mathbb{K}^n$ jen konečný počet prvků. Kolik?

(2) $\mathbb{C}$ jako vektorový prostor nad $\mathbb{R}$ má dimenzi 2, bázi tvoří např. čísla 1 a i.

(3) $\mathbb{K}_m[x]$, tj. prostor polynomů stupně nejvýše m, má dimenzi $m+1$, bazí je např. posloupnost $1, x, x^2, \dots, x^m$. Vektorový prostor všech polynomů $\mathbb{K}[x]$ má dimenzi ∞, umíme však ještě stále najít bázi (i když s nekonečně mnoha prvky): $1, x, x^2, \dots$.

(4) Vektorový prostor $\mathbb{R}$ nad $\mathbb{Q}$ má dimenzi ∞ a nemá spočetnou bázi.

(5) Vektorový prostor všech zobrazení $f : \mathbb{R} \to \mathbb{R}$ má také dimenzi ∞ a nemá spočetnou bázi.

2.22 **2.31. Souřadnice vektorů.** Když je množina $\{v_1, \dots, v_n\} \subset V$ báze, můžeme každý vektor $w \in V$ vyjádřit jako lineární kombinaci $v = a_1v_1 + \dots + a_nv_n$. Předpokládejme, že to uděláme dvěma způsoby:

$$w = a_1v_1 + \dots + a_nv_n = b_1v_1 + \dots + b_nv_n.$$

Potom ale

$$0 = (a_1 - b_1)\cdot v_1 + \dots + (a_n - b_n)\cdot v_n$$

a proto $a_i = b_i$ pro všechna $i = 1, \dots, n$. Lze tedy každý vektor zadat právě jediným způsobem jako lineární kombinaci bázových vektorů. Koeficienty této jediné lineární kombinace vyjadřující daný vektor $w \in V$ ve zvolené bázi $\underline{v} = (v_1, \dots, v_n)$ se nazývají *souřadnice vektoru* w v této bázi.

Kdykoliv budeme mluvit o souřadnicích $(a_1, \dots, a_n)$ vektoru w, které vyjadřujeme jako posloupnost, musíme mít pevně zvolenu i posloupnost bázových vektorů $\underline{v} = (v_1, \dots, v_n)$. Jakkoliv jsme tedy báze zavedli jako minimální množiny generátorů, ve skutečnosti s nimi budeme pracovat jako s posloupnostmi.

Přiřazení, které vektoru $u = a_1v_1 + \dots + a_nv_n$ přiřadí jeho souřadnice v bázi $\underline{v}$, budeme značit stejným symbolem $\underline{v} : V \to \mathbb{K}^n$. Má tyto vlastnosti:

(1) $\underline{v}(u + w) = \underline{v}(u) + \underline{v}(w)$; $\forall u, w \in V$

(2) $\underline{v}(a \cdot u) = a \cdot \underline{v}(u)$; $\forall a \in \mathbb{K}, \forall u \in V$.

Přiřazení souřadnic vektorům

Všimněme si, že operace na levých a pravých stranách těchto rovnic nejsou totožné, naopak, jde o operace na různých vektorových prostorech! Při této příležitosti se také můžeme zamyslet nad obecným případem báze M (možná nekonečněrozměrného) prostoru V. Báze pak nemusí být spočetná, pořád ale ještě můžeme definovat zobrazení $\underline{M} : V \to \mathbb{K}^M$ (tj. souřadnice vektoru jsou zobrazení z M do $\mathbb{K}$).

Uvedené vlastnosti přiřazení souřadnic jsme viděli už dříve u zobrazení, kterým jsme v geometrii roviny říkali lineární (zachovávaly naši lineární strukturu v rovině). Než se budeme věnovat podrobněji závislosti souřadnic na volbě báze, podíváme se obecněji na pojem linearity zobrazení.

2.23

2.32. Lineární zobrazení. Pro zcela obecné vektorové prostory, konečné i nekonečné dimenze, definujeme pojem „linearity“ takto:

Nechť V a W jsou vektorové prostory nad týmž polem skalárů $\mathbb{K}$. Zobrazení $f : V \to W$ se nazývá *lineární zobrazení (homomorfismus)* jestliže platí:

(1) $f(u+v) = f(u) + f(v), \ \forall u, v \in V$
(2) $f(a \cdot u) = a \cdot f(u), \ \forall a \in \mathbb{K}, \ \forall u \in V.$

Definice lineárních zobrazení

Samozřejmě, že jsme taková zobrazení již viděli ve formě násobení matic:

$$\mathbb{K}^n \ni x \mapsto A \cdot x \in \mathbb{K}^m$$

s maticí typu m/n nad $\mathbb{K}$.

Obraz $\operatorname{Im} f := f(V) \subset W$ je vždy vektorový podprostor, protože lineární kombinace obrazů $f(u_i)$ je obrazem lineární kombinace vektorů u_i se stejnými koeficienty.

Stejně tak je vektorovým podprostorem množina všech vektorů $\operatorname{Ker} f := f^{-1}(\{0\}) \subset V$, protože lineární kombinace nulových obrazů bude vždy zase nulovým vektorem. Nazývá se *jádro lineárního zobrazení* f.

Lineární zobrazení, které je bijekcí nazýváme *izomorfismus*.

Podobně jako u abstraktní definice vektorových prostorů, opět je třeba ověřit zdánlivě samozřejmá tvrzení vyplývající z axiomů:

Tvrzení. *Nechť $f : V \to W$ je lineární zobrazení. Pro všechny vektory $u, u_1, \dots, u_k \in V$, $a_1, \dots, a_k \in \mathbb{K}$ platí:*

(1) $f(0) = 0$
(2) $f(-u) = -f(u)$
(3) $f(a_1 \cdot u_1 + \dots + a_k \cdot u_k) = a_1 \cdot f(u_1) + \dots + a_k \cdot f(u_k)$
(4) pro každý vektorový podprostor $V_1 \subset V$ je jeho obraz $f(V_1)$ vektorový podprostor ve W.
(5) Pro každý podprostor $W_1 \subset W$ je množina $f^{-1}(W_1) = \{v \in V;\ f(v) \in W_1\}$ vektorový podprostor ve V.

Důkaz. Počítáme s využitím axiomů a definic a již dokázaných výsledků (dohledejte si případně samostatně!):

$$f(0) = f(u-u) = f((1-1)\cdot u) = 0 \cdot f(u) = 0$$
$$f(-u) = f((-1)\cdot u) = (-1)\cdot f(u) = -f(u).$$

Vlastnost (3) se ověří snadno z definičního vztahu pro dva sčítance indukcí přes počet sčítanců. Z platnosti (3) nyní plyne, že $\langle f(V_1) \rangle = f(V_1)$, je to tedy vektorový podprostor.

Je-li naopak $f(u) \in W_1$ a $f(v) \in W_1$, pak pro libovolné skaláry bude i $f(a\cdot u + b \cdot v) = a \cdot f(u) + b \cdot f(v) \in W_1$. $\square$

2.24

2.33. Jednoduché důsledky.

(1) Složení $g \circ f : V \to Z$ dvou lineárních zobrazení $f : V \to W$ a $g : W \to Z$ je opět lineární zobrazení.
(2) Lineární zobrazení $f : V \to W$ je izomorfismus právě když $\operatorname{Im} f = W$ a $\operatorname{Ker} f = \{0\} \subset V$. Inverzní zobrazení k izomorfismu je opět izomorfismus.
(3) Pro libovolné podprostory $V_1, V_2 \subset V$ a lineární zobrazení $f : V \to W$ platí

$$f(V_1 + V_2) = f(V_1) + f(V_2),$$
$$f(V_1 \cap V_2) \subset f(V_1) \cap f(V_2).$$

(4) Zobrazení „přiřazení souřadnic“ $\underline{u} : V \to \mathbb{K}^n$ dané libovolně zvolenou bází $\underline{u} = (u_1, \dots, u_n)$ vektorového prostoru V je izomorfismus.
(5) Dva konečněrozměrné vektorové prostory jsou izomorfní právě když mají stejnou dimenzi.
(6) Složení dvou izomorfismů je izomorfismus.

Důkaz. Ověření prvního tvrzení je velmi snadné cvičení.

Pro druhé si uvědomme, že je-li f lineární bijekce, pak $w = f^{-1}(au + bv)$ právě, když

$$f(w) = au + bv = f(a \cdot f^{-1}(u) + b \cdot f^{-1}(v)).$$

Je tedy také $w = af^{-1}(u) + bf^{-1}(v)$ a tedy je inverze k lineární bijekci opět lineární zobrazení.

Dále, f je surjektivní právě, když $\operatorname{Im} f = W$ a pokud $\operatorname{Ker} f = \{0\}$, pak $f(u) = f(v)$ zaručuje $f(u - v) = 0$, tj. $u = v$. Je tedy v tom případě f injektivní.

Další tvrzení se dokáže snadno přímo z definic. Najděte si protipříklad, že v dokazované inkluzi opravdu nemusí nastat rovnost! Zbývající body jsou již zřejmé. $\square$

2.25

2.34. Opět souřadnice. Uvažujme libovolné vektorové prostory V a W nad $\mathbb{K}$ s $\dim V = n$, $\dim W = m$ a mějme lineární zobrazení $f : V \to W$. Pro každou volbu bází $\underline{u} = (u_1, \dots, u_n)$ na V, $\underline{v} = (v_1, \dots, v_n)$ na W, máme k dispozici příslušná přiřazení souřadnic a celou situaci několika právě zmíněných zobrazení zachycuje následující diagram:

$$\begin{tikzcd}
V \arrow[r, "f"] \arrow[d, "\underline{u}"', "\simeq"] & W \arrow[d, "\underline{v}", "\simeq"'] \\
\mathbb{K}^n \arrow[r, dotted, "f_{\underline{u},\underline{v}}"] & \mathbb{K}^m
\end{tikzcd}$$

Spodní šipka $f_{\underline{u},\underline{v}}$ je definována zbylými třemi, tj. jako zobrazení jde o složení

$$f_{\underline{u},\underline{v}} = \underline{v} \circ f \circ \underline{u}^{-1}.$$

Přitom je každé lineární zobrazení jednoznačně určeno svými hodnotami na libovolné množině generátorů, zejména tedy na vektorech báze $\underline{u}$. Označme

$$\begin{aligned} f(u_1) &= a_{11} \cdot v_1 + a_{21} \cdot v_2 + \dots + a_{m1}v_m \\ f(u_2) &= a_{12} \cdot v_1 + a_{22} \cdot v_2 + \dots + a_{m2}v_m \\ &\vdots \\ f(u_n) &= a_{1n} \cdot v_1 + a_{2n} \cdot v_2 + \dots + a_{mn}v_m \end{aligned}$$

tj. skaláry a_{ij} tvoří matici A, kde sloupce jsou souřadnice hodnot $f(u_j)$ zobrazení f na bázových vektorech vyjádření v bázi $\underline{v}$ na cílovém prostoru W. Pro obecný vektor $u = x_1u_1 + \dots + x_nu_n \in V$ spočteme (vzpomeňme, že sčítání vektorů je komutativní a distributivní vůči násobení skaláry)

$$\begin{aligned} f(u) &= x_1 f(u_1) + \dots + x_n f(u_n) \\ &= x_1(a_{11}v_1 + \dots + a_{m1}v_m) + \dots + x_n(a_{1n}v_1 + \dots + a_{mn}v_m) \\ &= (x_1a_{11} + \dots + x_na_{1n})v_1 + \dots + (x_1a_{m1} + \dots + x_na_{mn})v_m \end{aligned}$$

Pomocí násobení matic lze nyní velice snadno a přehledně zapsat hodnoty zobrazení $f_{\underline{u},\underline{v}}(w)$ definovaného jednoznačně předchozím diagramem. Připomeňme si, že vektory v $\mathbb{K}^r$ chápeme jako sloupce, tj. matice typu $r/1$

$$f_{\underline{u},\underline{v}}(\underline{u}(w)) = \underline{v}(f(w)) = A \cdot \underline{u}(w).$$

Matici A nazýváme *maticí zobrazení* f v bázích $\underline{u}$, $\underline{v}$.

Naopak, máme-li pevně zvoleny báze na V i W, pak každá volba matice A typu m/n zadává jednoznačně lineární zobrazení $\mathbb{K}^n \to \mathbb{K}^m$ a tedy i zobrazení $f : V \to W$. Máme-li tedy zvoleny báze prostorů V a W, odpovídá každé volbě matice typu m/n právě jedno lineární zobrazení $V \to W$ a ukázali jsme bijekci mezi maticemi příslušného rozměru a lineárními zobrazeními $V \to W$.

2.25a

2.35. Matice přechodu mezi souřadnicemi. Jestliže za V i W zvolíme tentýž prostor, ale s různými bazemi, a za f identické zobrazení, vyjadřuje postup z předchozího odstavce vektory báze $\underline{u}$ v souřadnicích vzhledem k $\underline{v}$. Označme výslednou matici T. Když pak zadáme vektor u

$$u = x_1u_1 + \dots + x_nu_n$$

v souřadnicích vzhledem k $\underline{u}$ a dosadíme za u_i jejich vyjádření pomocí vektorů z $\underline{v}$, obdržíme souřadné vyjádření $\bar{x} = (\bar{x}_1, \dots, \bar{x}_n)$ téhož vektoru v bázi $\underline{v}$. Stačí k tomu přeskládat pořadí sčítanců a vyjádřit skaláry u jednotlivých vektorů báze.

Ve skutečnosti teď děláme totéž, co v předchozím odstavci pro speciální případ identického zobrazení id_V na vektorovém prostoru V. Matice tohoto identického zobrazení je T a tedy nutně musí naznačený přímý výpočet dát $\bar{x} = T \cdot x$. Situace se zobrazena na diagramu:

$$\begin{tikzcd} V \arrow[r, "\mathrm{id}_V"] \arrow[d, "\underline{u}"', "\simeq"] & V \arrow[d, "\underline{v}", "\simeq"'] \\ \mathbb{K}^n \arrow[r, dotted, "T = (\mathrm{id}_V)_{\underline{u},\underline{v}}"] & \mathbb{K}^n \end{tikzcd}$$

Výslednou matici T nazýváme *matice přechodu* od báze $\underline{u}$ vektorového prostoru V k bázi $\underline{v}$ téhož prostoru.

Přímo z definice vyplývá:

Tvrzení. *Matici T přechodu od báze $\underline{u}$ k bázi $\underline{v}$ získáme tak, že souřadnice vektorů báze $\underline{u}$ v bázi $\underline{v}$ napíšeme do sloupců matice T.*

Výpočet matice přechodu

Funkce matice přechodu je taková, že známe-li souřadnice x vektoru v bázi $\underline{u}$, pak jeho souřadnice v bázi $\underline{v}$ se obdrží vynásobením sloupce x maticí přechodu (zleva). Protože inverzní zobrazení k identickému je opět totéž identické zobrazení, je matice přechodu vždy invertibilní a její inverze je právě matice přechodu opačným směrem, tj. od báze $\underline{v}$ k bázi $\underline{u}$.

2.26 **2.36. Více souřadnic.** Nyní si ukážeme, jak se skládají souřadná vyjádření lineárních zobrazení. Uvažme ještě další vektorový prostor Z nad $\mathbb{K}$ dimenze k s bází $\underline{w}$, lineární zobrazení $g : W \to Z$ a označme příslušnou matici $g_{\underline{v},\underline{w}}$.

$$\begin{tikzcd}
V \arrow[r, "f"] \arrow[d, "\underline{u}"', "\simeq"] & W \arrow[r, "g"] \arrow[d, "\simeq"', "\underline{v}"] & Z \arrow[d, "\simeq"', "\underline{w}"] \\
\mathbb{K}^n \arrow[r, dotted, "f_{\underline{u},\underline{v}}"] & \mathbb{K}^m \arrow[r, dotted, "g_{\underline{v},\underline{w}}"] & \mathbb{K}^k
\end{tikzcd}$$

Složení $g \circ f$ na horním řádku odpovídá matici zobrazení $\mathbb{K}^n \to \mathbb{K}^k$ dole a přímo spočteme (píšeme A pro matici f a B pro matici g ve zvolených bazích):

$$\begin{aligned}
g_{\underline{v},\underline{w}} \circ f_{\underline{u},\underline{v}}(x) &= \underline{w} \circ g \circ \underline{v}^{-1} \circ \underline{v} \circ f \circ \underline{u}^{-1} \\
&= B \cdot (A \cdot x) = (B \cdot A) \cdot x = (g \circ f)_{\underline{u},\underline{w}}(x)
\end{aligned}$$

pro všechny $x \in \mathbb{K}^n$. Skládání obrazení tedy odpovídá násobení příslušných matic. Všimněte si také, že isomorfismy odpovídají právě invertibilním maticím.

Stejný postup nám dává odpověď na otázku, jak se změní matice zobrazení, změníme-li báze na definičním oboru i oboru hodnot:

$$\begin{tikzcd}
V \arrow[r, "\mathrm{id}_V"] \arrow[d, "\underline{u}'"', "\simeq"] & V \arrow[r, "f"] \arrow[d, "\underline{u}"', "\simeq"] & W \arrow[r, "\mathrm{id}_W"] \arrow[d, "\simeq"', "\underline{v}"] & W \arrow[d, "\simeq"', "\underline{v}'"] \\
\mathbb{K}^n \arrow[r, dotted, "T"] & \mathbb{K}^n \arrow[r, dotted, "f_{\underline{u},\underline{v}}"] & \mathbb{K}^m \arrow[r, dotted, "S^{-1}"] & \mathbb{K}^m
\end{tikzcd}$$

kde T je matice přechodu od $\underline{u}'$ k $\underline{u}$ a S je matice přechodu od $\underline{v}'$ k $\underline{v}$. Je-li tedy A původní matice zobrazení, bude nová dána jako $A' = S^{-1}AT$.

Ve speciálním případě lineárního zobrazení $f : V \to V$, tj. zobrazení má stejný prostor V jako definiční obor i obor hodnot, vyjadřujeme zpravidla f pomocí jediné báze $\underline{u}$ prostoru V. Pak tedy přechod k nové bázi $\underline{u}'$ s maticí předchodu T od $\underline{u}'$ k $\underline{u}$ bude znamenat změnu matice zobrazení na $A' = T^{-1}AT$.

2.27

2.37. Lineární formy. Obzvlášť jednoduchým a zároveň důležitým případem lineárních zobrazení jsou tzv. *lineární formy*. Jde o lineární zobrazení z vektorového prostoru V nad polem skalárů $\mathbb{K}$ do skalárů $\mathbb{K}$. Jsou-li dány souřadnice na V, je přiřazení jednotlivé i-té souřadnice vektorům právě takovou lineární formou. Přesněji řečeno, pro každou volbu báze $\underline{v} = (v_1, \dots, v_n)$ máme k dispozici lineární formy $v_i^* : V \to \mathbb{K}$ takové, že $v_i^*(v_j) = \delta_j^i$, tj. nula pro různé indexy i a j a jednička pro stejné.

Vektorový prostor všech lineárních forem na V značíme V^* a říkáme mu *duální prostor* vektorovému prostoru V. Předpokládejme nyní, že prostor V má konečnou dimenzi n. Bázi V^* sestavenou z přiřazování jednotlivých souřadnic jako výše nazýváme *duální báze*. Skutečně se jedná o bázi prostoru V^*, protože jsou tyto formy zjevně lineárně nezávislé (prověřte si!) a je-li α libovolná forma, pak platí pro každý vektor $u = x_1v_1 + \dots + x_nv_n$

$$\begin{aligned}\alpha(u) &= x_1\alpha(v_1) + \dots + x_n\alpha(v_n)\\ &= \alpha(v_1)v_1^*(u) + \dots + \alpha(v_n)v_n^*(u)\end{aligned}$$

a je tedy α lineární kombinací forem v_i^*.

Při pevně zvolené bázi $\{1\}$ na jednorozměrném prostoru skalárů $\mathbb{K}$ jsou s každou volbou báze $\underline{v}$ na V lineární formy α ztotožněny s maticemi typu $1/n$, tj. s řádky y. Právě komponenty těchto řádků jsou souřadnicemi obecných lineárních forem v duální bázi $\underline{v}^*$. Vyčíslení takové formy na vektoru je pak dáno vynásobením příslušného řádkového vektoru y se sloupcem souřadnic x vektoru $u \in V$ v bázi $\underline{v}$:

$$\alpha(u) = y \cdot x = y_1x_1 + \dots + y_nx_n.$$

Zejména tedy vidíme, že pro každý konečněrozměrný prostor V je V^* izomorfní prostoru V. Realizace takového izomorfismu je dána např. naší volbou duální báze k zvolené bázi na V.

U nekonečně rozměrného prostoru se věci mají jinak. Např. už nejjednodušší příklad prostoru všech polynomů $\mathbb{K}[x]$ v jedné proměnné je vektorovým prostorem se spočetnou bazí s prvky $v_i = x^i$ a stejně jako výše můžeme definovat lineárně nezávislé formy v_i^*. Jakýkoliv formální nekonečný součet $\sum_{i=0}^{\infty} a_i v_i^*$ je nyní dobře definovanou lineární formou na $\mathbb{K}[x]$, protože bude vyčíslován vždy pouze na konečné lineární kombinaci bázových polynomů x^i, $i = 0, 1, 2, \dots$. Spočetná množina všech v_i^* tedy není bazí. Ve skutečnosti lze ukázat, že tento duální prostor ani spočetnou bázi mít nemůže.

2.27a

2.38. Multilineární formy. Podobně budeme pracovat i se zobrazeními ze součinu k kopií vektorového prostoru V do skalárů, která jsou lineární v každém ze svých k argumentů. Hovoříme o *k–lineárních* formách. Budeme se často setkávat s *bilineárními formami*, tj. případem $\alpha : V \times V \to \mathbb{K}$, kde pro jakékoliv vektory u, v, w, z a skaláry a, b, c a d platí

$$\alpha(au+bv, cw+dz) = ac\,\alpha(u,w) + ad\,\alpha(u,z) \\ + bc\,\alpha(v,w) + bd\,\alpha(v,z).$$

Pokud navíc platí

$$\alpha(u,w) = \alpha(w,u),$$

hovoříme o *symetrické bilineární formě.*

Již v dimenzi 2 jsme zavedli determinant jako bilineární antisymetrickou formu, tj. takovou, kde místo druhé rovnosti výše platí $\alpha(u,w) = -\alpha(w,u)$. Obecně víme z věty 2.17, že je determinant možno nahlížet jako n–lineární antisymetrickou formu.

Jako u lineárních zobrazení je zřejmé, že každá k–lineární forma je úplně určena svými hodnotami na všech k–ticích bázových prvků v pevné bázi. V analogii k lineárním zobrazením tyto hodnoty můžeme vnímat jako k–rozměrné analogie matic. Ukážeme si to v případě $k = 2$, kde půjde doopravdy o matice, jak jsme je zavedli.

Jestliže zvolíme bázi $\underline{u}$ na V a definujeme pro danou bilineární formu α skaláry $a_{ij} = \alpha(u_i, u_j)$, pak zjevně dostaneme pro vektory v, w se souřadnicemi x a y (jakožto sloupce souřadnic)

$$\alpha(v,w) = \sum_{i,j=1}^{n} a_{ij} x_i y_j = y^T \cdot A \cdot x,$$

kde A je matice $A = (a_{ij})$.

Matice bilineární formy

Přímo z definice matice bilinerání formy je vidět, že forma je symetrická nebo antisymetrická právě, když má tutéž vlastnost její matice.

2.28

2.39. Skalární součin a velikost vektorů. V geometrii roviny $\mathbb{R}^2$ jsme již pracovali nejen s bázemi a lineárními zobrazeními, ale také s velikostí vektorů a jejich úhly. Pro zavedení těchto pojmů jsme použili souřadného vyjádření pro velikost $v = (x, y)$:

$$\|v\| = \sqrt{x^2 + y^2},$$

zatímco úhel φ dvou vektorů $v = (x, y)$ a $v' = (x', y')$ byl dán

$$\cos\varphi = \frac{xx' + yy'}{\|v\|\|v'\|}.$$

Povšimněme si, že výraz v čitateli posledního výrazu je lineární v každém ze svých argumentů, značíme jej $\langle v, v'\rangle$ a říkáme mu skalární součin vektorů v a v'. Takto definovaný skalární součin je také symetrický ve svých argumentech a platí

$$\|v\|^2 = \langle v, v\rangle.$$

Zejména platí, že $\|v\| = 0$ právě, když $v = 0$. Z našich úvah je také vidět, že v Euklidovské rovině jsou dva vektory kolmé právě, když je jejich skalární součin nulový.

Analogicky budeme postupovat v obecném případě reálného vektorového prostoru, tj. uvažujeme nyní pouze vektorové prostory nad reálnými skaláry $\mathbb{R}$.

Skalární součin na vektorovém prostoru V nad reálnými čísly je bilineární symetrická forma $\langle\ ,\ \rangle : V \times V \to \mathbb{R}$ taková, že $\langle v, v\rangle \geq 0$ a $\|v\|^2 = \langle v, v\rangle = 0$ pouze při $v = 0$.

Číslu $\|v\|$ říkáme velikost vektoru v.

Vektory v a $w \in V$ se nazývají *ortogonální*, jestliže $\langle v, w\rangle = 0$. Vektor v se nazývá *normovaný*, jestliže $\|v\| = 1$. Báze prostoru V složená z ortogonálních vektorů se nazývá *ortogonální báze*. Jsou-li bázové vektory navíc i normované, je to *ortonormální báze*.

Skalární součin

Pro skalární součin se často používá také obvyklé tečky, tj. $\langle u, v\rangle = u \cdot v$. Z kontextu je pak třeba poznat, zda jde o součin dvou vektorů (tedy výsledkem je skalár) nebo něco jiného (stejně jsme značili součin matic a také někdy součin skalárů).

Jak jsme viděli v minulém odstavci, bilineární formy jsou v souřadnicích dány svojí maticí.

Zvolíme-li si tedy bázi $\underline{u}$, je skalární součin plně určen svými hodnotami na dvojicích bázových vektorů. Označme si tedy

$$s_{ij} = \langle u_i, u_j\rangle.$$

Pak ze symetričnosti skalárního součinu plyne $s_{ij} = s_{ji}$ a z lineárnosti součinu v každém z argumentů dostáváme:

$$\langle \sum_i x_i u_i, \sum_j y_j u_j\rangle = \sum_{i,j} x_i y_j \langle u_i, u_j\rangle = \sum_{i,j} s_{ij} x_i y_j.$$

Pokud je báze ortonormální, je matice S jednotkovou maticí. Tím jsme dokázali následující užitečné tvrzení:

Tvrzení. *Skalární součin je v každé ortonormální bázi dán výrazem*

$$\langle x, y\rangle = x^T \cdot y.$$

V obecné bázi V existuje symetrická matice S taková, že

$$\langle x, y\rangle = x^T \cdot S \cdot y.$$

skalární součin a ortogonální báze

2.33b

2.40. Ortogonální doplňky a projekce. Pro každý pevně zvolený podprostor $W \subset V$ v prostoru se skalárním součinem definujeme jeho *ortogonální doplněk* takto

$$W^\perp = \{u \in V;\ \langle u, v\rangle = 0 \text{ pro všechny } v \in W\}.$$

Přímo z definice je zjevné, že $W^\perp$ je vektorový podprostor. Jestliže $W \subset V$ má bázi $(u_1, \dots, u_k)$ je podmínka pro $W^\perp$ dána jako k homogenních rovnic pro n proměnných. Bude tedy mít $W^\perp$ dimenzi alespoň $n-k$. Zároveň ale $u \in W \cap W^\perp$

znamená $\langle u, u\rangle = 0$ a tedy i $u = 0$ podle definice skalárního součinu. Zřejmě je tedy vždy

$$V = W \oplus W^{\perp}.$$

Lineární zobrazení $f : V \to V$ na libovolném vektorovém prostoru se nazývá *projekce*, jestliže platí

$$f \circ f = f.$$

V takovém případě je pro každý vektor $v \in V$

$$v = f(v) + (v - f(v)) \in \mathrm{Im}(f) + \mathrm{Ker}(f) = V$$

a je-li $v \in \mathrm{Im}(f)$ a $f(v) = 0$, pak je i $v = 0$. Je tedy přechozí součet podprostorů přímý. Říkáme, že f je projekce na podprostor $W = \mathrm{Im}(f)$ podél podprostoru $U = \mathrm{Ker}(f)$. Slovy se dá projekce popsat přirozeně takto: rozložíme daný vektor na komponentu ve W a v U a tu druhou zapomeneme.

Je-li na V navíc skalární součin, říkáme že jde o kolmou projekci, když je jádro kolmé na obraz. Každý podprostor $W \neq V$ tedy definuje *kolmou projekci* na W. Je to projekce na W podél $W^{\perp}$, která je dána pomocí jednoznačného rozkladu každého vektoru u na komponenty $u_W \in W$ a $u_{W^{\perp}} \in W^{\perp}$, tj. lineární zobrazení, které $u_W + u_{W^{\perp}}$ zobrazí na u_W.

2.33a

2.41. Existence ortonormální báze. Povšimněme si, že na každém vektorovém prostoru jistě existují skalární součiny. Prostě si stačí vybrat libovolnou bázi, prohlásit ji za ortonormální a hned jeden dobře definovaný skalární součin máme. V této bázi pak skalární součiny počítáme podle vzorce v Tvrzení 2.39.

Umíme to ale i naopak. Máme-li zadán skalární součin na vektorovém prostoru V, můžeme vcelku jednoduše početně využít vhodných kolmých projekcí a jakoukoliv zvolenou bázi upravit na ortonormální. Jde o tzv. *Grammův–Schmidtův ortogonalizační proces*. Cílem této procedury bude z dané posloupnosti nenulových generátorů $v_1, \dots, v_k$ konečněrozměrného prostoru V vytvořit ortogonální množinu nenulových generátorů pro V.

Tvrzení. *Nechť $(u_1, \dots, u_k)$ je lineárně nezávislá k-tice vektorů prostoru V se skalárním součinem. Pak existuje ortogonální systém vektorů $(v_1, \dots, v_k)$ takový, že $v_i \in \langle u_1, \dots, u_i\rangle$, $i = 1, \dots, k$. Získáme je následující procedurou:*

- *Nezávislost vektorů u_i zaručuje, že $u_1 \neq 0$; zvolíme $v_1 = u_1$.*
- *Máme-li již vektory $v_1, \dots, v_\ell$ potřebných vlastností, zvolíme $v_{\ell+1} = u_{\ell+1} + a_1 v_1 + \dots + a_\ell v_\ell$, kde $a_i = -\frac{\langle u_{\ell+1}, v_i\rangle}{\|v_i\|^2}$.*

Grammova–Schmidtova ortogonalizace

DŮKAZ. Začneme prvním (nenulovým) vektorem v_1 a spočteme kolmou projekci v_2 do

$$\langle v_1\rangle^{\perp} \subset \langle\{v_1, v_2\}\rangle.$$

Výsledek bude nenulový právě, když je v_2 nezávislé na v_1. Ve všech dalších krocích budeme postupovat obdobně.

V ℓ-tém kroku tedy chceme, aby pro $v_{\ell+1} = u_{\ell+1}+a_1v_1+\dots+a_\ell v_\ell$ platilo $\langle v_{\ell+1}, v_i\rangle = 0$, pro všechny $i = 1, \dots, \ell$. Odtud plyne

$$0 = \langle u_{\ell+1} + a_1v_1 + \dots + a_\ell v_\ell, v_i\rangle = \langle u_{\ell+1}, v_i\rangle + a_i\langle v_i, v_i\rangle$$

a je vidět, že vektory s požadovanými vlastnostmi jsou určeny jednoznačně až na násobek. □

Kdykoliv máme ortogonální bázi vektorového prostoru V, stačí vektory vynormovat a získáme bázi ortonormální. Dokázali jsme proto:

Důsledek. *Na každém vektorovém prostoru se skalárním součinem existuje ortonormální báze.*

V ortonormální bázi se obzvlášť snadno spočtou souřadnice a kolmé projekce. Skutečně, mějme ortonormální bázi $(e_1, \dots, e_n)$ prostoru V. Pak každý vektor $v = x_1e_1 + \dots + x_ne_n$ splňuje

$$\langle e_i, v\rangle = \langle e_i, x_1e_1 + \dots + x_ne_n\rangle = x_i$$

a platí tedy vždy

e2.2 (2.2) $$v = \langle e_1, v\rangle e_1 + \dots + \langle e_n, v\rangle e_n.$$

Pokud máme zadán podprostor $W \subset V$ a jeho ortonormální bázi $(e_1, \dots, e_k)$, jde ji jistě doplnit na ortonormální bázi $(e_1, \dots, e_n)$ celého V. Kolmá projekce obecného vektoru $v \in V$ do W pak bude dána vztahem

$$v \mapsto \langle e_1, v\rangle e_1 + \dots + \langle e_n, v\rangle e_k.$$

Pro kolmou projekci nám tedy stačí znát jen ortonormání bázi podprostoru W, na nejž promítáme.

Povšimněme si také, že obecně jsou projekce f na podprostor W podél U a projekce g na U podél W svázány vztahem $g = \mathrm{id}_V - f$. Je tedy u kolmých projekcí na daný podprostor W vždy výhodnější počítat ortonormální bázi toho z dvojice W, $W^\perp$, který má menší dimenzi.

Uvědomme si také, že existence ortonormální báze nám zaručuje, že pro každý prostor V se skalárním součinem existuje lineární zobrazení, které je izomorfismem mezi V a prostorem $\mathbb{R}^n$ se standardním skalárním součinem. Podrobně to bylo ukázáno již ve Tvrzení 2.39, kde jsme ukázali, že hledaným izomorfismem je právě přiřazení souřadnic. Řečeno volnými slovy – v ortonormální bázi se skalární součin pomocí souřadnic počítá stejnou formulí jako standardní skalární součin v $\mathbb{R}^n$.

2.28a

2.42. Úhel dvou vektorů. Určitě očekáváme, že úhel dvou lineárně nezávislých vektorů musí být stejný, když je budeme uvažovat v dvourozměrném podprostoru, který generují, nebo když budou v okolním prostoru větším. Ve své podstatě je proto pojem úhlu dvou vektorů nezávislý na dimenzi okolního prostoru a můžeme převzít definici z roviny, kterou jsme už úspěšně používali:

Úhel φ dvou vektorů v a w ve vektorovém prostoru se skalárním součinem je dán vztahem

$$\cos\varphi = \frac{\langle v, w\rangle}{\|v\|\,\|w\|}.$$

Úhel dvou vektorů

K problematice skalárních součinů a úhlů vektorů se vrátime v dalších kapitolách.

4. Vlastnosti lineárních zobrazení

Podrobnějším rozborem vlastností různých typů lineárních zobrazení se nyní dostaneme k pořádnějšímu pochopení nástrojů, které nám vektorové prostory pro lineární modelování procesů a systémů nabízejí.

2.29 **2.43. Příklady.** Začneme čtyřmi příklady v nejnižší zajímavé dimenzi. Ve standardní bázi roviny $\mathbb{R}^2$ se standardním skalárním součinem uvažujme následující matice zobrazení $f : \mathbb{R}^2 \to \mathbb{R}^2$:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ C = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},\ D = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Matice A zadává kolmou projekci podél podprostoru

$$W \subset \{(0, a);\ a \in \mathbb{R}\} \subset \mathbb{R}^2$$

na podprostor

$$V \subset \{(a, 0);\ a \in \mathbb{R}\} \subset \mathbb{R}^2.$$

Evidentně pro toto zobrazení $f : \mathbb{R}^2 \to \mathbb{R}^2$ platí $f \circ f = f$ a tedy zúžení $f|_V$ daného zobrazení na obor hodnot je identické zobrazení. Jádrem f je právě podprostor W.

Matice B má vlastnost $B^2 = 0$, platí tedy totéž o příslušném zobrazení f. Můžeme si jej představit jako matici derivování polynomů $\mathbb{R}_1[x]$ stupně nejvýše jedna v bázi $(1, x)$.

Matice C zadává zobrazení f, které první vektor báze zvětší a–krát, druhý b–krát. Tady se nám tedy celá rovina rozpadá na dva podprostory, které jsou zobrazením f zachovány a ve kterých jde o pouhou *homotetii*, tj. roztažení skalárním násobkem (první příklad byl speciální případem s $a = 1$, $b = 0$). Např. volba $a = 1$, $b = -1$ odpovídá osové symetrii (zrcadlení) podle osy x, což je totéž jako komplexní konjugace $x + iy \mapsto x - iy$ na dvourozměrném reálném prostoru $\mathbb{R}^2 \simeq \mathbb{C}$ v bázi $(1, i)$. Toto je lineární zobrazení dvourozměrného reálného vektorového prostoru $\mathbb{C}$, nikoliv však jednorozměrného komplexního prostoru $\mathbb{C}$.

Matice D je maticí rotace o pravý úhel ve standardní bázi a na první pohled je vidět, že žádný jednorozměrný podprostor není zobrazením zachováván.

Taková rotace je bijekcí roviny na sebe, proto jistě umíme najít (různé) báze na definičním oboru a oboru hodnot, ve kterých bude jeho maticí jednotková matice E (prostě vezmeme jakoukoliv bázi na definičním oboru a její obraz na oboru hodnot). Neumíme ale v tomto případě totéž s jednou bází na definičním oboru i oboru hodnot.

Zkusme však uvažovat matici D jako matici zobrazení $g : \mathbb{C}^2 \to \mathbb{C}^2$ ve standardní bázi komplexního vektorového prostoru $\mathbb{C}^2$. Pak umíme najít vektory $u = (i, 1)$, $v = (1, i)$, pro které bude platit

$$g(u) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} i \\ 1 \end{pmatrix} = i \cdot u, \ g(v) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ i \end{pmatrix} = -i \cdot v.$$

To ale znamená, že v bázi (u, v) na $\mathbb{C}^2$ má zobrazení g matici

$$K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

a povšimněme si, že tato komplexní analogie k případu matice C má na diagonále prvky $\pm a$, $a = \cos(\frac{1}{2}\pi) + i \sin(\frac{1}{2}\pi)$. Jinými slovy, argument v goniometrickém tvaru tohoto komplexního čísla udává úhel otočení. Navíc, můžeme si označit reálnou a imaginární část vektoru u takto

$$u = x_u + iy_u = \operatorname{Re} u + i \operatorname{Im} u = \begin{pmatrix} 0 \\ 1 \end{pmatrix} + i \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

a zúžení komplexního zobrazení g na reálný vektorový podprostor generovaný vektory x_u a iy_u (tj. násobení komplexní jednotkou i) je právě otočení o úhel $\frac{1}{2}\pi$.

2.30 **2.44. Vlastní čísla a vlastní vektory zobrazení.** Klíčem k popisu zobrazení v předchozích příkladech byly odpovědi na otázku „jaké jsou vektory splňující rovnici $f(u) = a \cdot u$?“ pro nějaké skaláry a. Zvolme tedy pevně lineární zobrazní $f : V \to V$ na vektorovém prostoru dimenze n nad skaláry $\mathbb{K}$. Jestliže si představíme takovou rovnost zapsanou v souřadnicích, tj. s využitím matice zobrazení A v nějakých bazích, jde o výraz

$$A \cdot x - a \cdot x = (A - a \cdot E) \cdot x = 0.$$

Z předchozího víme, že taková soustava rovnic má jediné řešení $x = 0$, pokud je matice $A - aE$ invertibilní. My tedy chceme najít takové hodnoty $a \in \mathbb{K}$, pro které naopak $A - aE$ invertibilní není, a nutnou a dostatečnou podmínkou je (viz Věta 2.22)

e2.1 (2.3) $$\det(A - a \cdot E) = 0.$$

Jestliže považujeme $\lambda = a$ za proměnnou v předchozí skalární rovnici, hledáme ve skutečnosti kořeny polynomu stupně n. Jak jsme viděli v případě matice D výše, kořeny mohou, ale nemusí existovat podle volby pole skalárů $\mathbb{K}$.

Skaláry a vyhovující rovnici $f(u) = a \cdot u$ pro nenulový vektor $u \in V$ nazýváme *vlastní čísla zobrazení* f, příslušné vektory u pak *vlastní vektory zobrazení* f.

Vlastní čísla a vlastní vektory lineárního zobrazení

Z definice vlastních čísel je zřejmé, že jejich výpočet nemůže záviset na volbě báze a tedy matice zobrazení f. Skutečně, jako přímý důsledek trasformačních vlastností z 2.36 a Cauchyovy věty 2.19 pro výpočet determinantu součinu dostáváme jinou volbou souřadnic matici $A' = P^{-1}AP$ s invertibilní maticí P a

$$\begin{aligned}|P^{-1}AP - \lambda E| &= |P^{-1}AP - P^{-1}\lambda EP| \\ &= |P^{-1}(A - \lambda E)P| = |P^{-1})||(A - \lambda E||P|,\end{aligned}$$

protože násobení skalárů je komutativní a $|P^{-1}| = |P|^{-1}$.

Obdobnou terminologii používáme i pro matice. Pro matici A dimenze n nad $\mathbb{K}$ nazýváme polynom $|A - \lambda E| \in \mathbb{K}_n[\lambda]$ *charakteristický polynom matice A*.

Kořeny tohoto polynomu jsou *vlastní hodnoty matice A*. Je-li A matice zobrazení $f : V \to V$ v jisté bázi, pak $|A - \lambda E|$ nazýváme také *charakteristický polynom zobrazení f*.

Charaktersitický polynom matice a obrazení

Protože je charakteristický polynom zobrazení $f : V \to V$ nezávislý na volbě báze V, jsou i jeho koeficienty u jednotlivých mocnin proměnné λ skaláry vyjadřující vlastnosti zobrazení f, tj. nemohou záviset na naší volbě báze. Zejména jako jednoduché cvičení na počítání determinantů vyjádříme koeficienty u nejvyšších a nejnižších mocnin (předpokládáme $\dim V = n$):

$$|A - \lambda \cdot E| = (-1)^n \lambda^n + (-1)^{n-1}(a_{11} + \dots + a_{nn}) \cdot \lambda^{n-1} + \dots + |A| \cdot \lambda^0$$

Součet diagonálních členů matice se nazývá *stopa matice*, značíme ji TrA, *stopa zobrazení* je definována jako stopa jeho matice v libovolné bázi.

2.30a **2.45. Věta.** *Vlastní vektory lineárního zobrazení $f : V \to V$ příslušné různým vlastním hodnotám jsou lineárně nezávislé.*

Důkaz. Nechť $a_1, \dots, a_k$ jsou různé vlastní hodnoty zobrazení f a $u_1, \dots, u_k$ vlastní vektory s těmito vlastními hodnotami. Důkaz provedeme indukcí přes počet lineárně nezávislých vektorů mezi zvolenými. Předpokládejme, že $u_1, \dots, u_\ell$ jsou lineárně nezávislé a $u_{l+1} = \sum_i c_i u_i$ je jejich lineární kombinací. Alespoň $\ell = 1$ lze zvolit, protože vlastní vektory jsou nenulové. Pak ovšem $a_{l+1} \cdot u_{l+1} = \sum_{i=1}^{l} a_{l+1} \cdot c_i \cdot u_i$, tj.

$$f(u_{l+1}) = \sum_{i=1}^{l} a_{l+1} \cdot c_i \cdot u_i = \sum_{i=1}^{l} c_i \cdot f(u_i) = \sum_{i=1}^{l} c_i \cdot a_i \cdot u_i.$$

Odečtením druhého a čtvrtého výrazu v rovnostech dostáváme $0 = \sum_{i=1}^{l}(a_{l+1} - a_i) \cdot c_i \cdot u_i$. Všechny rozdíly vlastních hodnot jsou však nenulové a alespoň jeden koeficient c_i je nenulový. To je spor s předpokládanou nezávislostí $u_1, \dots, u_\ell$, takže i vektor u_{l+1} musí být lineárně nezavislý na předchozích. □

Na právě dokázané tvrzení se můžeme podívat z pohledu rozkladu lineárního zobrazení f na součet nejjednodušších možných zobrazení, které budou vždy představovat projekci na invariantní jednorozměrný podprostor v rozkladu celého prostoru V na přímý součet jednotlivých vlastních podprostorů, následovanou vynásobením příslušným vlastním číslem. Navíc lze tento rozklad na vlastní podprostory snadno spočíst:

Důsledek. *Jestliže existuje n navzájem různých kořenů a_i charakteristického polynomu zobrazení $f : V \to V$, na n–rozměrném prostoru V, pak existuje rozklad V na přímý součet vlastních podprostorů dimenze 1. To znamená, že existuje báze V složená výhradně z vlastních vektorů a v této bázi má f diagonální matici. Tato báze je určená jednoznačně až na pořadí prvků.*

Příslušnou bázi (vyjádřenou v souřadnicích vzhledem k libovolně zvolené bázi V) obdržíme řešením n systémů homogenních lineárních rovnic o n neznámých s maticemi $(A - a_i \cdot E)$, kde A je matice f ve zvolené bázi.

Báze z vlastních vektorů

2.44

2.46. Invariantní podprostory. Každý vlastní vektor v zobrazení $f : V \to V$ generuje podprostor $\langle v \rangle \subset V$, který je zobrazením f zachováván.

Obecněji říkáme, že podprostor $W \subset V$ je *invariantní podprostor* pro zobrazení f, jestliže platí $f(W) \subset W$.

Jestliže je V konečněrozměrný vektorový prostor a vybereme nějakou bázi $(u_1, \dots, u_k)$ podprostoru W, můžeme ji vždy doplnit na bázi $(u_1, \dots, u_k, u_{k+1}, \dots, u_n)$ celého V a v každé takové bázi má naše zobrazení matici A tvaru

e2.3a (2.4)
$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

kde B je čtvercová matice dimenze k, D je čtvercová matice dimenze $n - k$ a C je matice typu $n/(n-k)$. Naopak, jestliže existuje v nějaké bázi matice zobrazení f tvaru (2.4), je $W = \langle u_1, \dots, u_k \rangle$ invariantní podprostor zobrazení f.

Pochopitelně bude v naší matici zobrazení (2.4) submatice C nulová právě tehdy, když bude i podprostor $\langle u_{k+1}, \dots, u_n \rangle$ generovaný doplněnými vektory báze invariantní.

Z tohoto pohledu jsou vlastní podprostory lineárního zobrazení extrémní případy invariantních podsprostorů a zejména v případě existence $n = \dim V$ různých vlastních čísel zobrazení f dostáváme rozklad V na přímý součet n vlastních podprostorů. V příslušné bázi z vlastních vektorů má pak naše zobrazení diagonální tvar s vlastními čísly na diagonále.

2.36

2.47. Ortogonální zobrazení. Podívejme se teď na speciální případ zobrazení $f : V \to W$ mezi prostory se skalárními součiny, která zachovávají velikosti pro všechny vektory $u \in V$.

Lineární zobrazení $f : V \to W$ mezi prostory se skalárním součinem se nazývá *ortogonální zobrazení*, jesltiže pro všechny $u \in V$

$$\langle f(u), f(u) \rangle = \langle u, u \rangle.$$

Definice ortogonálních zobrazení

Z linearity f a ze symetrie skalárního součinu vyplývá pro všechny dvojice vektorů rovnost

$$\langle f(u+v), f(u+v)\rangle = \langle f(u), f(u)\rangle + \langle f(v), f(v)\rangle + 2\langle f(u), f(v)\rangle.$$

Proto všechny ortogonální zobrazení splňují i zdánlivě silnější požadavek, aby

$$\langle f(u), f(v)\rangle = \langle u, v\rangle,$$

pro všechny vektory $u, v \in V$.

V úvodní diskusi o geometrii v rovině jsme ve Větě 1.33 dokázali, že lineární zobrazení $\mathbb{R}^2 \to \mathbb{R}^2$ zachovává velikosti vektorů právě, když jeho matice ve standardní bázi (a ta je ortonormální vzhledem ke standardnímu skalárnímu součinu) splňuje $A^T \cdot A = E$, tj. $A^{-1} = A^T$.

Obecně, ortogonální zobrazení musí vždycky být injektivní, protože podmínka $\langle f(u), f(u)\rangle = 0$ znamená i $\langle u, u\rangle = 0$ a tedy $u = 0$. Je tedy vždy v takovém případě dimenze oboru hodnot alespoň taková, jako je dimenze definičního oboru f. Pak ovšem je dimenze obrazu rovna dimenzi oboru hodnot a bez újmy na obecnost můžeme rovnou předpokládat, že jsou stejné a $f : V \to V$ (pokud by nebyly, doplníme ortonormální bázi na oboru hodnot na bázi cílového prostoru a matice zobrazení bude čtvercovou maticí A doplněnou nulami na potřebnou velikost).

Naše podmínka pro matici ortogonálního zobrazení v ortonormální bázi pak říká pro všechny vektory x a y v prostoru $\mathbb{K}^n$ toto:

$$(A \cdot x)^T \cdot (A \cdot y) = x^T \cdot (A^T \cdot A) \cdot y = x^T \cdot y.$$

Speciálními volbami vektorů standardní báze za x a y dostaneme přímo, že $A^T \cdot A = E$, tedy tentýž výsledek jako v dimenzi dvě. Dokázali jsme tak následující tvrzení:

Věta. *Nechť V je reálný vektorový prostor se skalárním součinem a $f : V \to V$ je lineární zobrazení. Pak f je ortogonální právě, když v některé ortonormální bázi (a pak už všech) má matici A splňující $A^T = A^{-1}$.*

Matice ortogonálních zobrazení

DŮKAZ. Skutečně, jestliže zachovává f velikosti, musí mít uvedenou vlastnost v každé ortonormální bázi. Naopak, předchozí výpočet ukazuje, že vlastnost matice v jedné bázi už zaručuje zachovávání velikostí. □

Maticím splňujícím $A^T = A^{-1}$ se říká *ortogonální matice.*

Důsledkem této věty je také popis všech matic přechodu S mezi ortonormálními bázemi. Každá totiž musí zadávat zobrazení $\mathbb{K}^n \to \mathbb{K}^n$ zachovávající velikosti a splňují tady také právě podmínku $S^{-1} = S^T$. Při přechodu od jedné ortonormální báze ke druhé se tedy matice (ortogonálního) zobrazení mění podle vztahu

2.45 $$A' = S^T AS.$$

2.48. Rozklad ortogonálního zobrazení. Podívejme se nyní podrobněji na vlastní vektory a vlastní čísla ortogonálních zobrazení na vektorovém prostoru V se skalárním součinem. Uvažme pevně zvolené ortogonální zobrazení $f : V \to V$ s maticí A v nějaké ortonormální bázi a zkusme postupovat obdobně jako s maticí rotace D v příkladu 2.43.

Nejprve se ale podívejme obecně na invariantní podprostory ortogonálních zobrazení a jejich ortogonální doplňky. Jestliže pro libovolný podprostor $W \subset V$ a ortogonální zobrazení $f : V \to V$ platí $f(W) \subset W$, pak také platí pro všechny $v \in W^{\perp}$, $w \in W$

$$\langle f(v), w\rangle = \langle f(v), f \circ f^{-1}(w)\rangle = \langle v, f^{-1}(w)\rangle = 0$$

protože i $f^{-1}(w) \in W$. To ale znamená, že také $f(W^{\perp}) \subset W^{\perp}$. Dokázali jsme tedy jednoduché, ale velice důležité tvrzení:

Tvrzení. *Ortogonální doplněk k invariantnímu podprostoru je také invariantní.*

Kdyby byla vlastní čísla ortogonálního zobrazení reálná, zaručovalo by už toto tvrzení, že bude vždy existovat báze V z vlastních vektorů. Skutečně, zúžení f na ortogonální doplněk invariantního podprostoru je opět ortogonální zobrazení, takže můžeme do báze přibírat jeden vlastní vektor za druhým, až dostaneme celý rozklad V. Nicméně většinou nejsou vlastní čísla ortogonálních zobrazení reálná. Musíme si proto pomoci opět výletem do komplexních vektorových prostorů. Sformulujeme rovnou výsledek:

Věta. *Nechť $f : V \to V$ je ortogonální zobrazení na prostoru se skalárním součinem. Pak všechny kořeny charakteristického polynomu f mají velikost jedna a existuje rozklad V na jednorozměrné vlastní podprostory odpovídající vlastním číslům $\lambda = \pm 1$ a dvourozměrné podprostory $P_{\lambda,\bar{\lambda}}$, na kterých působí f rotací o úhel rovný argumentu komplexního čísla λ. Všchny tyto různé podprostory jsou po dvou ortogonální.*

Rozklad ortogonálních zobrazení

Náznak důkazu. Jestliže budeme považovat ortogonální matici A za matici lineárního zobrazení na komplexním prostoru $\mathbb{C}^n$ (která je jen shodou okolností reálná), bude zaručeně existovat právě n (koplexních) kořenů charakteristického polynomu, včetně jejich algebraické násobnosti. Navíc, protože charakteristický polynom zobrazení bude mít výhradně reálné koeficienty, budou tyto kořeny buď reálné, nebo půjde o dvojice komplexně sdružených kořenů λ a $\bar{\lambda}$. Příslušné vlastní vektory v $\mathbb{C}^n$ k takové dvojici komplexně sdružených vlastních čísel budou řešením dvou komplexně sdružených systémů homogenních lineárních rovnic, neboť příslušné matice systémů rovnic jsou celé reálné, až na samotná dosazená vlastní čísla. Evidentně proto budou také řešení těchto systémů komplexně sdružené vektory.

Označme v_λ, stejně jako v případě rotace v 2.43, vlastní vektor příslušný k vlastnímu číslu $\lambda = \alpha + i\beta$, $\beta \neq 0$. Reálný vektorový podprostor P_λ generovaný reálnou a imaginární částí $x_\lambda = \operatorname{re} v_\lambda$, $y_\lambda = \operatorname{im} v_\lambda$ je zjevně invariantní vůči násobení maticí A a dostáváme

$$A \cdot x_\lambda = \alpha x_\lambda - \beta y_\lambda, \ \ A \cdot y_\lambda = \alpha y_\lambda + \beta x_\lambda.$$

To ale neznamená nic jiného, než že zúžení našeho zobrazení na P_λ je dáno složením rotace o argument vlastní honoty λ (úhel arccos $\frac{\alpha}{\sqrt{\alpha^2+\beta^2}}$) s násobením velikostí vlastní hodnoty λ (skalárem $\sqrt{\alpha^2+\beta^2}$). Protože naše zobrazení zachovává velikosti, musí být velikost vlastní hodnoty λ rovna jedné.

Společně s předchozími úvahami jsme tedy dokázali úplný popis všech ortogonálních zobrazení ve větě. □

K důkazu se ještě vrátíme v kapitole třetí, když budeme studovat komplexní rozšíření euklidovských vektorových prostorů, viz 3.23.

Poznámka. Specielně v dimenzi tři musí být alespoň jedno vlastní číslo ± 1, protože je trojka liché číslo. Pak ovšem příslušný vlastní podprostor je osou rotace trojrozměrného prostoru o úhel daný argumentem dalších vlastních čísel. Zkuste si rozmyslet, jak poznat, kterým směrem jde rotace a také, že vlastní číslo -1 znamená ještě dodatečnou symetrii podle roviny kolmé na osu rotace.

K diskusi vlastností matic a lineárních zobrazení se budeme vracet. Před pokračováním obecné teorie si ukážeme několik aplikací, ještě ale uzavřeme naši diskusi obecnou definicí:

2.32 **2.49. Definice.** *Spektrum lineárního zobrazení* $f : V \to V$ (resp. matice) je posloupnost kořenů charakteristického polynomu zobrazení f, včetně násobností. *Algebraickou násobností* vlastní hodnoty rozumíme její násobnost jakožto kořenu charakteristického polynomu, *geometrická násobnost* vlastní hodnoty je dimenze příslušného podprostoru vlastních vektorů.

Spektrálním poloměrem lineárního zobrazení (matice) je největší z absolutní hodnot vlastních čísel.

Spektrum lineárního zobrazení

V této terminologii můžeme naše výsledky o ortogonálních zobrazeních zformulovat tak, že jejich spektra jsou vždy celá podmnožinou jednotkové kružnice v komplexní rovině. To znamená, že v reálné části spektra mohou být pouze hodnoty ± 1, jejichž algebraické a geometrické násobnosti jsou stejné. Komplexní hodnoty spektra pak odpovídají rotacím ve vhodných dvourozměrných podprostorech.

KAPITOLA 3

Linární modely a maticový počet

Máme už vybudován docela slušný balíček nástrojů a tak je na čase, abychom si maticový počet zkusili použít. Na docela jednoduchých úlohách uvidíme, že teorie nám umožňuje kvalitativní i kvantitativní analýzy a někdy i překvapivě snadno vede k výsledkům.

Jakkoliv se může zdát, že předpoklad linearity vztahů mezi veličinami je příliš omezující, v reálných úlohách naopak často právě lineární závislosti buď vystupují přímo nebo je skutečný proces výsledkem iterace mnoha lineárních kroků,

V této kapitole proto neprve zrekapitulujeme nejjednodušší případ, kdy celý proces je popsán jediným lineárním zobrazením. O co méně tady bude nové teorie, tím více snad bude zajímavé, jak takové modely vznikají v různých oblastech využití matematických nástrojů. Poté se vrátíme k tzv. lineárním diferenčním rovnicím, které lze chápat buď jako rekurentně definované funkce nebo také jako specifický případ lineárního interovaného procesu. Právě těm bude věnována část třetí, kde si ukážeme, k jakým kouzlům vede pochopení vlastností vlastních hodnot matic.

Na matice (resp. lineární zobrazení) se také někdy rádi díváme jako na objekty, se kterými bychom rádi pracovali tak, jak to umíme se skaláry. To hodně souvisí i s tak zvanými rozklady matic, které jsou potřebné pro numerické zvládnutí matickového počtu co nejrobustnějším způsobem.

1. Lineární procesy

2.37

3.1. Struktura řešení systému lineárních rovnic. Jednoduché lineární procesy jsou dány lineárními zobrazeními $\varphi : V \to W$ na vektorových prostorech. Jak si jistě umíme představit, vektor $v \in V$ může představovat stav nějakého námi sledovaného systému, zatímco $\varphi(v)$ pak dá výsledek po uskutečněném procesu. Pokud chceme dosáhnout předem daného výsledku $b \in W$ takového jednorázového procesu, řešíme problém

$$\varphi(x) = b$$

pro neznámý vektor x a známý vektor b.

V pevně zvolených souřadnicích pak máme matici A zobrazení φ a souřadné vyjádření vektoru b. Jak jsme si povšimnuli už v úvodu druhé kapitoly, množina všech řešení tzv. *homogenní úlohy*

$$A \cdot x = 0$$

je vektorovým podprostorem.

Pokud je dimenze V konečná, řekněme n, a dimenze obrazu zobrazení φ je k, pak řešením této soustavy pomocí převodu na řádkově schodovitý tvar (viz 2.7) zjistíme, že dimenze podprostoru všech řešení je právě $n-k$. Skutečně, protože sloupce matice zobrazení jsou právě obrazy bázových vektorů, je v matici systému právě k lineárně nezávislých sloupců a tedy i stejný počet lineárně nezávislých řádků. Proto nám zůstane při převodu na řádkový schodovitý tvar právě $n-k$ nulových řádků. Při řešení systému rovnic nám tak zůstane právě $n-k$ volných parametrů a dosazením vždy jednoho z nich s hodnotou jedna a vynulováním ostatních získáme právě $n-k$ lineárně nezávislých řešení. Všechna řešení jsou pak dána právě všemi lineárními kombinacemi těchto $n-k$ řešení. Každé takové $(n-k)$–tici řešení říkáme *fundamentální systém řešení* daného homogenního systému rovnic. Dokázali jsme:

Věta. *Množina všech řešení homogenního systému rovnic*

$$A \cdot x = 0$$

pro n proměnných s maticí A hodnosti k je vektorovým podprostorem v $\mathbb{K}^n$ dimenze $n-k$. Každá báze tohoto podprostoru tvoří fundamentální systém řešení daného homogenního systému.

3.2. Nehomogenní systémy rovnic. Uvažme nyní obecný systém rovnic

$$A \cdot x = b.$$

Znovu si uvědomme, že sloupce matice A jsou ve skutečnosti obrazy vektorů standardní báze v $\mathbb{K}^n$ v lineárním zobrazení φ odpovídajícím matici A. Pokud má existovat řešení, musí být b v obrazu φ a tedy musí být lineární kombinací sloupců v A.

Jestliže tedy rozšíříme matici A o sloupec b, můžeme, ale nemusíme, také zvětšit počet lineárně nezávislých sloupců a tedy i řádků. Pokud se tento počet zvětší, pak b v obrazu není a tedy systém rovnic nemůže mít řešení. Jestliže ale naopak máme stejný počet nezávislých řádků i po přidání sloupce b k matici A, znamená to, že sloupec b musí být lineární kombinací sloupců matice A. Koeficienty takové kombinace jsou právě řešení našeho systému rovnic.

Uvažme nyní dvě pevně zvolená řešení x a y našeho systému a nějaké řešení z systému homogenního se stejnou maticí. Pak zjevně

$$A \cdot (x-y) = b - b = 0$$
$$A \cdot (x+z) = 0 + b = b.$$

Můžeme proto shrnout:

3.3. Věta. *Řešení nehomogenního systému lineárních rovnic $A \cdot x = b$ existuje právě, když přidáním sloupce b k matici A nezvýšíme počet lineárně nezávislých řádků. V takovém případě je prostor všech řešení dán všemy součty jednoho pevně zvoleného partikulárního řešení systému a všech řešení systému homogenního se stejnou maticí.*

3.2a

3.4. ??? …následuje výklad několika modelů založených na systémech rovnic / lineární procesy, může být 4-5 stran …

3.2b

3.5. ??? …

2. Diferenční rovnice

Diferenčními rovnicemi jsme se stručně zabývali již v první kapitole, byť pouze těmi prvního řádu.Nyní si ukážeme obecnou teorii pro lineární rovnice s konstantními koeficienty, která poskytuje nejen velmi praktické nástroje, ale je také pěknou ilustrací pro koncepty vektorových podprostorů a lineárních zobrazení.

3.10 **3.6. Definice.** *Homogenní lineární diferenční rovnice řádu k* je dána výrazem

$$a_0x_n + a_1x_{n-1} + \cdots + a_kx_{n-k} = 0, \quad a_0 \neq 0 \quad a_k \neq 0,$$

kde koeficienty a_i jsou skaláry, které mohou případně i záviset na n.

Říkáme také, že taková rovnost zadává *homogenní lineární rekurenci* řádu k a často zapisujeme hledanou posloupnost jako funkci

$$x_n = f(n) = -\frac{a_1}{a_0} f(n-1) - \cdots - \frac{a_k}{a_0} f(n-k).$$

Řešením této rovnice nazýváme posloupnost skalárů x_i, pro všechna $i \in \mathbb{N}$, případně $i \in \mathbb{Z}$, které vyhovují rovnici s libovolným pevným n.

Homogenní lineární diferenční rovnice řádu k

Libovolným zadáním k po sobě jdoucích hodnot x_i jsou určeny i všechny ostatní hodnoty jednoznačně. Skutečně, pracujeme nad polem skalárů, takže hodnoty a_0 i a_k jsou invertibilní a proto z definičního vztahu lze vždy spočíst hodnotu x_n ze známých ostatních hodnot a stejně tak pro x_{n-k}. Indukcí tedy okamžitě dokážeme, že lze jednoznačně dopočíst všechny hodnoty jak pro kladná tak pro záporná celá n.

Prostor všech nekonečných posloupností x_i je vektorový prostor, kde sčítání i násobení skaláry je dáno po složkách. Přímo z definice je zjevné, že součet dvou řešení homogenní lineární rovnice nebo skalární násobek řešení je opět řešení. Stejně jako u homogenních systémů lineárních tedy vidíme, že množina všech řešení je vektorový podprostor.

Počáteční podmínka na hodnoty řešení je dána jako k–rozměrný vektor v $\mathbb{K}^k$. Součtu počátečních podmínek odpovídá součet příslušných řešení a obdobně se skalárními násobky. Dále si všimněme, že dosazením nul a jedniček do zadávaných počástečních k hodnot snadno získáme k lineárně nezávislých řešení naší rovnice. Jakkoliv jsou tedy zkoumané vektory nekonečné posloupnosti skalárů, samotný prostor všech řešení je konečněrozměrný, předem víme, že jeho dimenze bude rovna řádu rovnice k, a umíme snadno určit bázi všech těchto řešení. Opět hovoříme o *fundamentálním systému řešení* a všechna ostatní řešení jsou právě jejich lineární kombinace.

3.11 **3.7. Řešení homogenních rekurencí s konstantními koeficienty.** Těžko bychom hledali univerzální postup, jak hledat řešení obecných homogenních lineárních diferenčních rovnic, tj. přímo spočítatelný výraz pro obecné řešení x_n.

V praktických modelech ale velice často vystupují rovnice, kde jsou koeficienty konstantní. V tomto případě se daří uhodnout vhodnou formu řešení a skutečně se nám podaří najít k lineárně nezávislých možností. Tím budeme mít problém vyřešený, protože všechny ostatní budou jejich lineární kombinací.

Pro jednoduchost začneme rovnicemi druhého řádu. Takové potkáváme obzvlášť často v praktických problémech, kde se vyskytují vztahy závisející na dvou předchozích hodnotách. Lineární diferenční rovnicí druhého řádu s konstantními koeficienty tedy rozumíme předpis

e1.8 (3.1) $$f(n+2) = a \cdot f(n+1) + b \cdot f(n) + c,$$

kde a, b, c jsou známé skalární koeficienty.

Např. v populačních modelech můžeme zohlednit, že jedinci v populaci dospívají a pořádně se rozmnožují až o dvě období později (tj. přispívají k hodnotě $f(n+2)$ násobkem $b \cdot f(n)$ s kladným $b > 1$), zatímco nedospělí jedinci vysílí a zničí část dospělé populace (tj. koeficient a může být i záporný). Navíc si je třeba někdo pěstuje a průběžně si ujídá konstantní počet $c < 0$.

Speciálním takovým příkladem s $c = 0$ je např. Fibonacciho posloupnost čísel $y_0, y_1, \dots$, kde $y_{n+2} = y_{n+1} + y_n$.

Jestliže při řešení matematického problému nemáme žádný nový nápad, vždy můžeme zkusit, do jaké míry funguje známé řešení podobných úloh. Zkusme proto dosadit do rovnice (3.1) s koeficientem $c = 0$ podobné řešení jako u rovnic lineárních, tj. $f(n) = \lambda^n$ pro nějaké skalární λ. Dosazením dostáváme

$$\lambda^{n+2} - a\lambda^{n+1} - b\lambda^n = \lambda^n(\lambda^2 - a\lambda - b) = 0.$$

Tento vztah bude platit buď pro $\lambda = 0$ nebo při volbě hodnot

$$\lambda_1 = \frac{1}{2}(a + \sqrt{a^2 + 4b}), \quad \lambda_2 = \frac{1}{2}(a - \sqrt{a^2 + 4b}).$$

Zjistili jsme tedy, že skutečně opět taková řešení fungují, jen musíme vhodně zvolit skalár λ. To nám ale nestačí, protože my chceme najít řešení pro jakékoliv počáteční hodnoty $f(0)$ a $f(1)$, a zatím jsme našli jen dvě konkrétní posloupnosti splňující danou rovnici (a nebo dokonce jen jednu, pokud je $\lambda_2 = \lambda_1$).

Jak jsem již dovodili i u zcela obecných lineárních rekurencí, součet dvou řešení $f_1(n)$ a $f_2(n)$ naší rovnice $f(n+2) - a \cdot f(n+1) - b \cdot f(n) = 0$ je zjevně opět řešením téže rovnice a totéž platí pro konstatní násobky řešení. Naše dvě konkrétní řešení proto poskytují daleko obecnější řešení

$$f(n) = C_1\lambda_1^n + C_2\lambda_2^n$$

pro libovolné skaláry C_1 a C_2 a pro jednoznačné vyřešení konkrétní úlohy se zadanými počátečními hodnotami $f(0)$ a $f(1)$ nám zbývá jen najít příslušné konstanty C_1 a C_2. (A také si musíme ujasnit, zda to pro všechny počáteční hodnoty půjde).

3.8. Volba skalárů. Ukažme si, jak to může fungovat alespoň na jednom příkladě. Soustředíme se přitom na problém, že kořeny charakteristického polynomu nevychází obecně ve stejném oboru skalárů, jako jsou koeficienty v rovnici.

e1.9 (3.2)
$$\begin{aligned} y_{n+2} &= y_{n+1} + \frac{1}{2} y_n \\ y_0 &= 2,\, y_1 = 0. \end{aligned}$$

V našem případě je tedy $\lambda_{1,2} = \frac{1}{2}(1 \pm \sqrt{3})$ a zjevně

$$y_0 = C_1 + C_2 = 2$$
$$y_1 = \frac{1}{2} C_1 (1 + \sqrt{3}) + \frac{1}{2} C_2 (1 - \sqrt{3})$$

je splněno pro právě jednu volbu těchto konstant. Přímým výpočtem $C_1 = 1 - \frac{1}{3}\sqrt{3}$, $C_2 = 1 + \frac{1}{3}\sqrt{3}$ a naše úloha má jediné řešení

$$f(n) = (1 - \frac{1}{3}\sqrt{3})\frac{1}{2^n}(1 + \sqrt{3})^n + (1 + \frac{1}{3}\sqrt{3})\frac{1}{2^n}(1 - \sqrt{3})^n$$

.

Všimněme si, že i když nalezená řešení pro rovnice s celočíselnými koeficienty vypadají složitě a jsou vyjádřena pomocí iracionálních (případně komplexních) čísel, o samotném řešení dopředu víme, že je celočíselné též. Bez tohoto „úkroku“ do většího oboru skalárů bychom ovšem obecné řešení napsat neuměli.

S podobnými jevy se budeme potkávat velice často. Obecné řešení nám také umožňuje bez přímého vyčíslování konstant diskutovat kvalitativní chování posloupnosti čísel $f(n)$, tj. zda se budou s rostoucím n blížit k nějaké pevné hodnotě nebo budou oscilovat v nějakém rozsahu nebo utečou do neomezených kladných nebo záporných hodnot.

3.11a

3.9. Obecný případ homogenních rekurencí s konstantními koeficienty. Zkusme nyní stejně jako v případě druhého řádu dosadit volbu $x_n = \lambda^n$ pro nějaký (zatím neznámý) skalár λ do obecné homogenní rovnice z definice 3.6. Dostáváme pro každé n podmínku

$$\lambda^{n-k}(a_0\lambda^k + a_1\lambda^{k-1} \cdots + a_k) = 0$$

což znamená, že buď $\lambda = 0$ nebo je λ kořenem tzv. *charakteristického polynomu* v závorce. Charakteristický polynom ale už není závislý na n.

Předpokládejme, že má charakteristický polynom k různých kořenů $\lambda_1, \dots, \lambda_k$. Můžeme za tímto účelem i rozšířit uvažované pole skalárů, např. $\mathbb{Q}$ na $\mathbb{R}$ nebo $\mathbb{R}$ na $\mathbb{C}$, protože výsledkem výpočtu pak stejně budou řešení, která opět zůstanou v původním poli díky samotné rovnici. Každý z kořenů nám dává jedno možné řešení

$$x_n = (\lambda_i)^n.$$

Abychom byli uspokojeni, potřebujeme k lineárně nezávislých řešení.

K tomu nám postačí ověřit nezávislost dosazením k hodnot pro $n = 0, \dots, k - 1$ pro k možností λ_i. Dostaneme tzv. Vandermondovu matici a je pěkným (ale ne úplně snadným) cvičením spočíst, že pro všechna k a jakékoliv k–tice různých λ_i je determinant takovéto matice nenulový, viz **??**. To ale znamená, že zvolená řešení jsou lineárně nezávislá.

Nalezli jsme tedy fundamentální systém řešení homogenní diferenční rovnice v případě, že všechny kořeny jejího charakteristického polynomu jsou po dvou různé.

Uvažme nyní násobný kořen λ a dosaďme do definiční rovnice předpokládané řešení $x_n = n\lambda^n$. Dostáváme podmínku

$$a_0 n\lambda^n + \dots + a_k(n-k)\lambda^{n-k} = 0.$$

Tuto podmínku je možné přepsat pomocí tzv. derivace polynomu, kterou značíme apostrofem:

$$\lambda(a_0\lambda^n + \dots + a_k\lambda^{n-k})' = 0$$

a hned na začátku kapitoly páté uvidíme, že kořen polynomu f je vícenásobný právě, když je kořenem i jeho derivace f'. Naše podmínka je tedy splněna.

Při vyšší násobnosti ℓ kořenu charakteristického polynomu můžeme postupovat obdobně a využijeme skutečnosti, že ℓ–násobný kořen je kořenem všech derivací polynomu až do $\ell - 1$ včetně. Derivace přitom postupně vypadají takto:

$$\begin{aligned}
f(\lambda) &= a_0\lambda^n + \dots + a_k\lambda^{n-k}\\
f'(\lambda) &= a_0 n\lambda^{n-1} + \dots + a_k(n-k)\lambda^{n-k-1}\\
f''(\lambda) &= a_0 n(n-1)\lambda^{n-2} + \dots + a_k(n-k)(n-k-1)\lambda^{n-k-2}\\
&\;\;\vdots\\
f^{(\ell+1)} &= a_0 n \dots (n-\ell)\lambda^{n-\ell-1} + \dots\\
&\qquad + a_k(n-k)\dots(n-k-\ell)\lambda^{n-k-\ell-1}
\end{aligned}$$

Podívejme se na případ trojnásobného kořenu λ a hledejme řešení ve tvaru $n^2\lambda^n$. Dosazením do definiční podmínky dostaneme rovnost

$$a_0 n^2\lambda^n + \dots + a_k(n-k)^2\lambda^{n-k} = 0.$$

Zjevně je levá strana rovna výrazu $\lambda^2 f''(\lambda) + \lambda f'(\lambda)$ a protože je λ kořenem obou derivací, je podmínka splněna.

Indukcí snadno dokážeme, že i obecnou podmínku pro hledané řešení ve tvaru $x_n = n^\ell\lambda^n$,

$$a_0 n^\ell\lambda^n + \dots a_k(n-k)^\ell\lambda^{n-k} = 0,$$

dostaneme jako vhodnou lineární kombinaci derivací charakteristického polynomu začínající $\lambda^{\ell+1} f^{(\ell+1)} + \frac{1}{2}\lambda^\ell\ell(\ell+1) f^{(\ell)} + \dots$ a dostali jsme se tedy blízko k úplnému důkazu následující:

Věta. *Každá homogenní lineární diferenční rovnice řádu k nad libovolným číselným oborem $\mathbb{K}$ obsaženým v komplexních číslech $\mathbb{K}$ má za množinu všech řešení k–rozměrný vektorový prostor generovaný posloupnostmi $x_n = n^\ell\lambda^n$, kde λ jsou (komplexní) kořeny charakteristického polynomu a mocniny ℓ probíhají všechna přirozená čísla od nuly až do násobnosti příslušného kořenu λ.*

DůKAZ. Výše použité vztahy násobnosti kořenů a derivací uvidíme později, a nebudeme tu dokazovat tvrzení, že každý komplexní polynom má právě tolik kořenů, včetně násobnosti, jaký má stupeň. Zbývá tedy ještě dokázat, že nalezená k–tice řešení je lineárně nezávislá. I v tomto případě lze induktivně dokázat nenulovost příslušného determinantu, jako jsme zmiňovali u toho Vandermondova výše. □

3.12

3.10. Reálné báze řešení reálných diferenčních rovnic. Pro rovnice s reálnými koeficienty povedou reálné počáteční podmínky vždy na reálná řešení. Přesto ale budou příslušná fundamentální řešení z právě odvozené věty často existovat pouze v oboru komplexním.

Zkusme proto najít jiné generátory, se kterými se nám bude pracovat lépe. Potože jsou koeficienty charakteristického polynomu reálné, každý jeho kořen bude buď také reálný nebo musí kořeny vystupovat po dvou komplexně združených.

Jestliže si řešení popíšeme v goniometrickém tvaru jako

$$\lambda^n = |\lambda|^n(\cos n\phi + i \sin n\phi)$$
$$\bar{\lambda}^n = |\lambda|^n(\cos n\phi - i \sin n\phi),$$

okamžitě je vidět, že jejich součtem a rozdílem dostáváme jiná dvě lineárně nezávislá řešení

$$x_n = |\lambda|^n \cos n\phi, \quad y_n = |\lambda|^n \sin n\phi.$$

Difereční rovnice se velmi často vyskytují jako model dynamiky nějakého systému. Pěkným tématem na přemýšlení je proto souvislost absolutních hodnot jednotlivých kořenů a stabilizace řešení, buď všech nebo v závislosti na počátečních podmínkách. Nepůjdeme zde do podrobností, protože teprve v páté kapitole budeme probírat pojem konvergence hodnot k nějaké hodnotě limitní apod., jistě je tu ale prostor pro zajímavé numerické experimenty např. s oscilacemi vhodných populačních nebo ekonomických modelů.

3.13

3.11. Nehomogenní lineární diferenční rovnice. Stejně jako u systémů lineárních rovnic můžeme dostat všechna řešení *nehomogenních lineárních diferenčních rovnic*

$$a_0(n)x_n + a_1(n)x_{n-1} + \cdots + a_k(n)x_{n-k} = b(n),$$

kde koeficienty a_i a b jsou skaláry, které mohou záviset na n, a $a_0(n) \neq, a_k(n) \neq 0$.

Postupujeme tak, že najdeme jedno řešení a přičteme celý vektorový prostor dimenze k řešení odpovídajících systémů homogenních. Skutečně takto dostáváme řešení a protože je rozdíl dvou řešení nehomogenní rovnice zjevně řešením homogenní, dostáváme takto řešení všechna.

U systémů lineárních rovnic se mohlo stát, že nemusel vůbec mít řešení. To u našich diferenčních rovnic možné není. Zato ale bývá nesnadné nalézt to jedno potřebné partikulární řešení nehomogenního systému, pokud je chování skalárních koeficientů v rovnici složité.

Omezíme se tu na jediný případ, kdy příslušný homogenní systém má koeficienty konstantní a $b(n)$ je polynom stupně s.

Řešení pak lze hledat ve tvaru polynomu

$$x_n = \alpha_0 + \alpha_1 n + \cdots + \alpha_s n^s$$

s neznámými koeficienty α_i, $i = 1, \dots, s$. Dosazením do diferenční rovnice a porovnáním koeficientů u jednotlivých mocnin n dostaneme systém $s+1$ rovnic pro $s+1$ proměnných α_i. Pokud má tento systém řešení, našli jsme řešení našeho původního problému. Pokud řešení nemá, může stačit zvětšit stupeň s hledaného polynomu.

Např. rovnice $x_n - x_{n-2} = 2$ nemůže mít konstantní řešení, ale dosazením $x_n = \alpha_0 + \alpha_1 n$ dostáváme řešení $\alpha_1 = 1$ (a koeficient α_0 může být libovolný) a proto je obecné řešení naší rovnice

$$x_n = C_1 + C_2(-1)^n + n.$$

Všimněme si, že skutečně matice příslušného systému rovnic pro polynom nižšího stupně nula je nulová a rovnice $0 \cdot \alpha_0 = 2$ nemá řešení.

doplnit pořádněji diskusi řešitelnosti pomocí variace konstant ...

3.14

3.12. Lineární filtry. Uvažujme nyní nekonečné posloupnosti

$$x = (\dots, x_{-n}, x_{-n+1}, \dots, x_{-1}, x_0, x_1, \dots, x_n, \dots)$$

a budeme, podobně jako u systémů lineárních rovnic, pracovat s operací T, která zobrazí celou posloupnost x na posloupnost $z = Tx$ se členy

$$z_n = a_0 x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k}.$$

S posloupnostmi x můžeme opět pracovat jako s vektory vzhledem ke sčítání i násobení skaláry po složkách. Pouze bude tento velký vektorový prostor nekonečněrozměrný. Naše zobrazení T je zjevně lineárním zobrazením na takovém vektorovém prostoru.

Posloupnosti si představme jako diskrétní hodnoty nějakého signálu, odečítané zpravidla ve velmi krátkých časových jednotkách, operace T pak může být filtrem, který signál zpracovává. Bude nás zajímat, jak odhadnout vlastnosti, které takový „filtr“ bude mít.

Signály jsou velice často ze své podstaty dány součtem několika částí, které jsou samy o sobě víceméně periodické. Z naší definice je ale zřejmé, že periodické posloupnosti x_n, tj. posloupnosti splňující pro nějaké pevné přirozené číslo p

$$x_{n+p} = x_n$$

budou mít i periodické obrazy $z = Tx$

$$\begin{aligned} z_{n+p} &= a_0 x_{n+p} + a_1 x_{n-1+p} + \cdots + a_k x_{n-k+p} \\ &= a_0 x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k} = z_n \end{aligned}$$

se stejnou periodou p.

Pro pevně zvolenou operaci T nás bude zajímat, které vstupní periodické posloupnosti zůstanou přibližně stejné (případně až na násobek) a které budou utlumeny na nulové hodnoty.

V druhém případě tedy hledáme jádro našeho lineárního zobrazení T. To je ale dáno právě homogenní diferenční rovnicí

$$a_0x_n + a_1x_{n-1} + \cdots + a_kx_{n-k} = 0, \quad a_0 \neq 0 \quad a_k \neq 0,$$

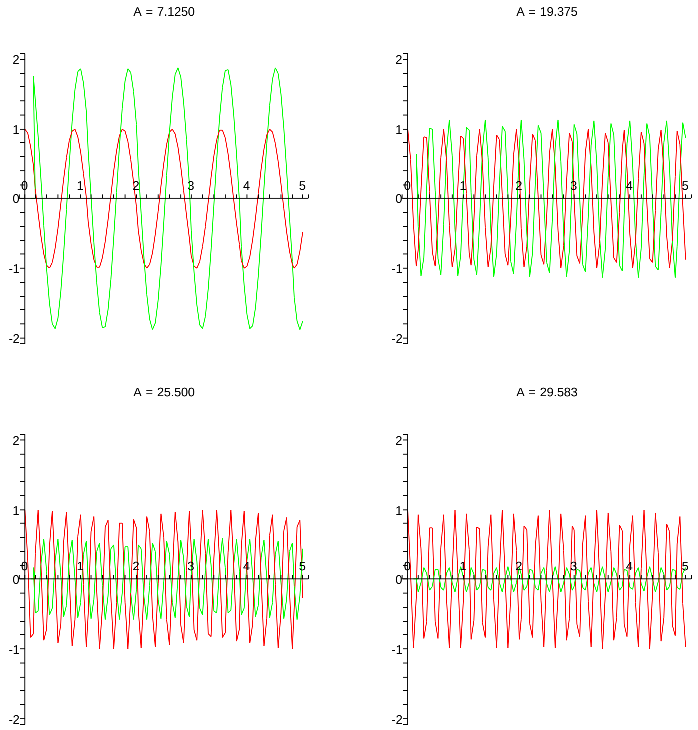
kterou jsme se naučili řešit.

3.15

3.13. Špatný equalizer. Jako příklad uvažujme velmi jednoduchý lineární filtr zadaný rovnicí

$$z_n = (Tx)_n = x_{n+2} + x_n.$$

Výsledky takového zpracování signálu jsou naznačeny na následujících čtyřech obrázcích pro postupně se zvyšující frekvenci periodického signálu $x_n = \cos(\varphi n)$. Červený je původní signál, zelený je výsledek po zpracování filtrem. Nerovnoměrnosti křivek jsou důsledkem nepřesného kreslení, oba signály jsou samozřejmě rovnoměrnými sinusovkami.



Všimněme si, že v oblastech, kde je výsledný signál přibližně stejně silný jako původní, dochází k dramatickému posuvu fáze signálu. Levné equalizery skutečně podobně špatně fungují.

doplnit podrobný výpočet pomocí uvedených nástrojů

3.16

3. Iterované lineární procesy

3.14. Iterované procesy. V praktických modelech se často setkáváme se situací, kdy je vývoj systému v jednom časovém období dán lineárním procesem, zajímáme se ale o chování systému po mnoha iteracích. Často přitom samotný lineární proces zůstává pořád stejný, z pohledu našeho matematického modelu tedy nejde o nic jiného než opakované násobení stavového vektoru stále stejnou maticí.

Zatímco pro řešení systémů lineárních rovnic jsme potřebovali jen minumum znalostí o vlastnostech lineárních zobrazení, k pochopení chování iterovaného systému budeme účelně používat znalosti vlastních čísel, vlastností vlastních vektorů a další strukturní výsledky.

V jistém smyslu se pohybujeme v podobném prostředí jako u lineárních rekurencí a skutečně můžeme náš popis filtrů v minulých odstavcích takto také popsat. Představme si, že pracujeme se zvukem a uchováváme si stavový vektor

$$Y_n = (x_n, \dots, x_{n-k+1})$$

všech hodnot od aktuální až po poslední, kterou ještě v našem lineárních filtru zpracováváme. V jednom (ve vzorkovací frekveci audio signálu mimořádně krátkém) časovém intervalu pak přejdeme ke stavovému vektoru

$$Y_{n+1} = (x_{n+1}, x_n, \dots, x_{n-k+2}),$$

kde první hodnota $x_{n+1} = a_1 x_n + \dots + a_k x_{n-k+1}$ je spočtena jako u homogenních diferenčních rovnic, ostatní si jen posunujeme o jednu pozici a poslední zapomeneme. Příslušná čtvercová matice řádu k, splňující $Y_{n+1} = A \cdot Y_n$, bude vypadat takto:

$$A = \begin{pmatrix} a_1 & a_2 & \dots & a_{k-1} & a_k \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \ddots & 0 & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

Pro takovou jednoduchou matici jsme si odvodili explicitní postup pro úplné řešení otázky, jak vypadá formule pro řešení. Obecně to tak snadno nepůjde ani pro velice podobné systémy. Jedním z typických případů je studium dynamiky populací v různých biologických systémech.

Všimněme si také, že vcelku pochopitelně má matice A za charakteristický polynom právě $p(\lambda) = \lambda^k - a_1\lambda^{k-1} - \dots - a_k$ (snadno dovodíme pomocí rozvoje podle posledního sloupce a rekurencí). To je snadno vysvětlitelné přímo, protože řešení $x_n = \lambda^n$, $\lambda \neq 0$ vlastně nyní znamená, že matice A vynásobením převede vlastní vektor $(\lambda^k, \dots, \lambda)^T$ na jeho λ–násobek. Musí být tedy λ vlastním číslem matice A.

3.17

3.15. Model růstu populací. Představme si, že zkoumáme nějaký systém jednotlivců (pěstovaná zvířata, hmyz, buněčné kultury apod.) rozdělený do m skupin (třeba podle stáří, fází vývoje hmyzu apod.). Stav X_n je tedy dán vektorem

$$X_n = (u_1, \dots, u_m)^T$$

závisejícím na okamžiku t_n, ve kterém systém pozorujeme. Lineární model vývoje takového systému je dán maticí A dimenze n, která zadává změnu vektoru X_n na

$$X_{n+1} = A \cdot X_n$$

při přírůstku času z t_k na t_{k+1}.

Uvažujme jako příklad tzv. *Leslieho model růstu*, ve kterém vystupuje matice

$$A = \begin{pmatrix} f_1 & f_2 & f_3 & \dots & f_{m-1} & f_m \\ \tau_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \tau_2 & 0 & \dots & 0 & 0 \\ 0 & 0 & \tau_3 & \ddots & 0 & 0 \\ \vdots & & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \tau_{m-1} & 0 \end{pmatrix},$$

jejíž parametry jsou svázány s vývojem populace rozdělené do m věkových skupin tak, že f_i označuje relativní plodnost příslušné věkové skupiny (ve sledovaném časovém skoku vznikne z N jedinců v i–té skupině $f_i N$ jedinců nových, tj. ve skupině první), zatímco τ_i je relativní úmrtnost i-té skupiny během jednoho období. Pochopitelně lze použít takový model s libovolným počtem věkových skupin.

Všechny koeficienty jsou tedy nezáporná reálná čísla a čísla τ jsou mezi nulou a jedničkou (a pokud jsou všechna rovna jedné, jde vlastně o lineární rekurenci s konstantními koeficienty). Než se pustíme do obecnější teorie, trochu si pohrajeme s tímto konkrétním modelem.

Přímým výpočtem pomocí Laplaceova rozvoje podle posledního sloupce spočteme charakteristický polynom $p_m(\lambda)$ matice A pro model s m skupinami:

$$p_m(\lambda) = \det(A-\lambda E) = -\lambda p_{m-1}(\lambda)+(-1)^{m-1} f_m \tau_1 \dots \tau_{m-1}.$$

Vcelku snadno dovodíme indukcí, že tento charakteristický polynom má tvar

$$p_m(\lambda) = (-1)^m(\lambda^m - a_1\lambda^{m-1} - \dots - a_{m-1}\lambda - a_m)$$

s vesměs nezápornými koeficienty $a_1, \dots, a_m$, pokud jsou všechny prametry τ_i a f_i kladné. Např. je vždy $a_m = f_m \tau_1 \dots \tau_{m-1}$.

Zkusme kvalitativně odhadnout rozložení kořenů polynomu p_m, detaily budeme umět přesně vysvětlit a ověřit až po absolvování příslušných partií tzv. matematické analýzy v kapitole páté a později. Vyjádříme si

$$p_m(\lambda) = \pm\lambda^m(1 - q(\lambda))$$

kde $q(\lambda) = a_1\lambda^{-1}+\dots+a_m\lambda^{-m}$ je ostře klesající a nezáporná funkce pro $\lambda > 0$. Evidentně bude proto existovat právě jedno kladné λ, pro které bude $q(\lambda) = 1$ a tedy také $p_m(\lambda) = 0$. Jinými slovy, pro každou Leslieho matici existuje právě jedno kladné reálné vlastní číslo.

Pro skutečné Leslieho modely populací bývají všechny koeficienty τ_i i f_j mezi nulou a jedničkou a typicky nastává situace, kdy jediné reálné vlastní číslo λ_1 je větší nebo rovno jedné, zatímco absolutní hodnoty ostatních vlastních čísel jsou ostře menší než jedna.

Jestliže začneme s libovolnýmn stavovým vektorem X, který bude dán jako součet vlastních vektorů

$$X = X_1 + \dots + X_m$$

s vlastními hodnotami λ_i, pak při iteracích dostáváme

$$A^k \cdot X = \lambda_1^k X_1 + \dots \lambda_m^k X_m,$$

takže za předpokladu, že $|\lambda_i| < 1$ pro všechna $i \geq 2$, budou všechny komponenty ve vlastních podprostorech velmi rychle mizet, kromě kompomenty $\lambda_1 X_1^k$. Rozložení populace do věkových skupin se tak budou rychle blížit poměrům komponent vlastního vektoru k dominantnímu vlastnímu číslu λ_1.

Například pro matici (uvědomme si význam jednotlivých koeficientů, jsou převzaty z modelu pro chov ovcí, tj. hodnoty τ zahrnují jak přirozený úhyn tak případné aktivity chovatelů na jatkách)

$$A = \begin{pmatrix} 0 & 0.2 & 0.8 & 0.6 & 0 \\ 0.95 & 0 & 0 & 0 & 0 \\ 0 & 0.8 & 0 & 0 & 0 \\ 0 & 0 & 0.7 & 0 & 0 \\ 0 & 0 & 0 & 0.6 & 0 \end{pmatrix}$$

vyjdou vlastní hodnoty přibližně

$$1.03,\ 0,\ -0.5,\ -0,27 + 0.74i,\ -0.27 - 0.74i$$

s velikostmi 1.03, 0, 0.5, 0.78, 0.78 a vlastní vektor příslušný dominantnímu vlastnímu číslu je přibližně

$$x = (30\ 27\ 21\ 14\ 8).$$

Zvolili jsme rovnou jediný vlastní vektor se součtem souřadnic rovným stu, zadává nám proto přímo výsledné procentní rozložení populace.

Pokud bychom chtěli místo tříprocentního celkového růstu populace setrvalý stav a předsevzali si ujídat více ovce třeba z druhé věkové skupiny, řešili bychom úlohu, o kolik máme změnšit τ_2, aby bylo dominantní vlastní číslo rovno jedné.

3.18

3.16. Matice s nezápornými prvky. Reálné matice, které nemají žádné záporné prvky mají velmi speciální vlastnosti. Zároveň jsou skutečně časté v praktických modelech. Naznačíme proto teď proto tzv. *Perronovu-Frobeniovu teorii*, která se právě takovým maticím věnuje.

Začneme definicí několika pojmů, abychom mohli naše úvahy vůbec formulovat.

tady by se hodilo trochu historie, vlastně jen naznačíme část výsledků Perrona, k Frobeniově obecnější situaci se vůbec nedopracujeme.

Definice. Za *kladnou matici* budeme považovat takovou čtvercovou matici A, jejíž všechny prvky a_{ij} jsou reálné a ostře kladné. *Primitivní matice* je pak taková čtvercová matice A, jejíž nějaká mocnina A^k je kladná.

Kladné a primitivní matice

Připoměňme, že *spektrálním poloměrem matice A* nazýváme maximum absolutních hodnot všech jejích (komplexních) vlastních čísel. Spektrálním poloměrem lineárního zobrazení na (konečněrozměrném) vektorovém prostoru rozumíme spektrální poloměr jeho matice v některé bázi. *Normou* matice $A \in \mathbb{R}^{n^2}$ nebo vektoru $x \in \mathbb{R}^n$ rozumíme součet absolutních hodnot všech jejich prvků. U vektorů x píšeme pro jejich normu $|x|$.

Následující výsledek je mimořádně užitečný a snad i dobře srozumitelný. Jeho důkaz se svou náročností dosti vymyká této učebnici, uvádíme ale alespoň jeho stručný nástin. Pokud by čtenář měl problém s plynulým čtení nástinu důkazu, doporučujeme jej přeskočit.

Věta (Perronova)**.** *Jestliže je A primitivní matice se spektrálním poloměrem $\lambda \in \mathbb{R}$, pak je λ jednoduchým kořenem charakteristického polynomu matice A, který je ostře větší než absolutní hodnota kteréhokoliv jiného vlastního čísla matice A. K vlastnímu číslu λ navíc existuje vlastní vektor x s výhradně kladnými prvky x_i.*

inspirováno materiálem na webu, viz http://www-users.math.umd.edu/~mmb/475/spec.pdf

Náznak důkazu. V důkazu se budeme opírat o intuici elementární geometrie. Částečně budeme použité koncepty upřesňovat už v analytické geometrii ve čtvrté kapitole, některé analytické aspekty budeme studovat podrobněji v kapitolách páté a později, přesné důkazy některých analytických kroků v této učebnici nepodáme vůbec. Snad budou následující úvahy nejen osvětlovat dokazovaný teorém, ale budou také samy o sobě motivací pro naše další studium geometrie i matematické analýzy. Začneme docela srozumitelně znějícím pomocným lemmatem:

Lemma. *Uvažme libovolný mnohostěn P obsahující počátek $0 \in \mathbb{R}^n$. Jestliže nějaká iterace lineárního zobrazení $\psi : \mathbb{R}^n \to \mathbb{R}^n$ zobrazuje P do jeho vnitřku, pak je spektrální poloměr zobrazení ψ ostře menší než jedna.*

Uvažme matici A zobrazení ψ ve standardní bázi. Protože vlastní čísla A^k jsou k–té mocniny vlastních čísel matice A, můžeme rovnou bez újmy na obecnosti předpokládat, že samotné zobrazení ψ již zobrazuje P do vnitřku P. Zjevně tedy nemůže mít ψ žádnout vlastní hodnotu s absolutní hodnotou větší než jedna.

Důkaz dále povedeme sporem. Předpokládejme, že existuje vlastní hodnota λ s $|\lambda| = 1$. Máme tedy dvě možnosti. Buď je $\lambda^k = 1$ pro vhodné k nebo takové k neexistuje.

Obrazem P je uzavřená množina (to znamená, že pokud se body v obrazu budou hromadit k nějakému bodu y v $\mathbb{R}^n$, bude y opět v obrazu) a hranici P tento obraz vůbec neprotíná. Nemůže tedy mít ψ pevný bod na hranici P ani nemůže existovat žádný bod na hranici, ke kterému by se mohly libovolně blížit body v obrazu. První argument vylučuje, že by nějaká mocnina λ byla jedničkou, protože to by takový pevný bod na hranici P jistě existoval. Ve zbývajícím případě jistě existuje dvourozměrný podprostor $W \subset \mathbb{R}^n$, na nějž se ψ zužuje coby rotace o iracionální argument a jistě existuje bod

y v průniku W s hranicí P. Pak by ale byl bod y libovolně přesně přiblížen body z množiny $\psi^n(y)$ při průchodu přes všechny iterace a tedy by musel sám být také v obrazu. Došli jsme tedy ke sporu a lemma je ověřeno.

Nyní se dáme do důkazu Perronovy věty. Naším prvním krokem bude ověření existence vlastního vektoru, který má všechny prvky kladné. Uvažme za tím účelem tzv. standardní simplex

$$S = \{x = (x_1, \dots, x_n)^T,\ |x| = 1, x_i \geq 0, i = 1, \dots, n\}.$$

Protože všechny prvky v matici A jsou nezáporné, obraz $A \cdot x$ bude mít samé nezáporné souřadnice stejně jako x a alespoň jedna z nich bude vždy nenulová. Zobrazení $x \mapsto |A \cdot x|^{-1}(A \cdot x)$ proto zobrazuje S do sebe, Toto zobrazení $S \to S$ splňuje všechny předpoklady tzv. Browerovy věty o pevném bodě a proto existuje vektor $y \in S$ takový, že je tímto zobrazením zobrazen sám na sebe. To ale znamená, že

$$A \cdot y = \lambda\, y, \quad \lambda = |A \cdot y|$$

a našli jsme vlastní vektor, který leží v S. Protože ale má nějaká mocnina A^k podle našeho předpokladu samé kladné prvky a samozřejmě je také $A^k \cdot y = \lambda^k y$, všechny souřadnice vektoru y jsou ostře kladné (tj. leží ve vnitřku S) a $\lambda > 0$.

Abychom dokázali zbytek věty, budeme uvažovat zobrazení zadané maticí A ve výhodnější bázi a navíc ho vynásobíme konstantou λ^{-1}:

$$B = \lambda^{-1}(Y^{-1} \cdot A \cdot Y),$$

kde Y je diagonální matice se souřadnicemi y_i vektoru y na diagonále. Evidentně je B také primitivní matice a navíc je vektor $z = (1, \dots, 1)^T$ jejím vlastním vektorem.

Jestliže nyní dokážeme, že $\mu = 1$ je jednoduchým kořenem charakteristického polynomu matice B a všechny ostatní kořeny mají absolutní hodnotu ostře menší než jedna, bude Perronova věta dokázána.

K tomu se nám teď bude hodit dříve dokázané pomocné lemma. Uvažujme matici B jako matici lineárního zobrazení, které zobrazuje řádkové vektory

$$u = (u_1, \dots, u_n) \mapsto u \cdot B = v,$$

tj. pomocí násobení zprava. Díky tomu, že je $z = (1, \dots, 1)^T$ vlastním vektorem matice B, je součet souřadnic řádkového vektoru v

$$\sum_{i,j=1}^{n} u_i b_{ij} = \sum_{i=1}^{n} u_i = 1,$$

kdykoliv je $u \in S$. Proto toto zobrazení zobrazuje simplex S na sebe a má také jistě v S vlastní (řádkový) vektor w s vlastní hodnotou jedna (pevný bod, opět dle Browerovy věty). Protože nějaká mocnina B^k obsahuje samé ostře pozitivní prvky, je nutně obraz simplexu S v k–té iteraci zobrazení daného B uvnitř S. To už jsme blízko použití našeho lematu, které jsme si pro důkaz připravili.

Budeme i nadále pracovat s řádkovými vektory a označme si P posunutí simplexu S do počátku pomocí vlastního vektoru w, který jsme právě našli, tj. $P = -w + S$. Evidentně je P mnohostěn obsahující počátek a vektorový podprostor $V \subset \mathbb{R}^n$ generovaný P je invariantní vůči násobení maticí B násobením řádkových vektorů zprava. Zúžení našeho zobrazení na P tedy splňuje předpoklady pomocného lemmatu a proto nutně musí být všechny jeho vlastní hodnoty v absolutní hodnotě menší než jedna. Ještě se musíme vypořádat se skutečností, že právě uvažované zobrazení je dáno násobením řádkových vektorů zprava maticí B (zatímco nás původně zajímalo chování zobrazení, daného B pomocí násobení sloupcových vektorů zleva). To je ale ekvivalentní násobení transponovaných sloupcových vektorů transponovanou maticí B obvyklým způsobem zleva. Dokázali jsem tedy vlastně potřebné tvrzení o vlastních číslech pro matici transponovanou k naší matici B. Transponování ale vlastní čísla nemění.

Dimenze prostoru V je přitom $n-1$, takže důkaz věty je ukončen. □

3.19

3.17. Jednoduché důsledky. Následující velice užitečné tvrzení má při znalosti Perronovy věty až překvapivě jednoduchý důkaz a ukazuje, jak silná je vlastnost primitivnosti matice zobrazení.

Důsledek. *Jestliže $A = (a_{ij})$ je primitivní matice a $x \in \mathbb{R}^n$ její vlastní vektor se samými nezápornými souřadnicemi a vlastní hodnotou λ, pak $\lambda > 0$ je spektrální poloměr A. Navíc platí*

$$\min_j \sum_{i=1}^{n} a_{ij} \le \lambda \le \max_j \sum_{i=1}^{n} a_{ij}.$$

Důkaz. Uvažme vlastní vektor x z dokazovaného tvrzení. Protože je A primitivní, můžeme zvolit pevně k tak, aby A^k už měla samé positivní prvky a pak je samozřejmě i $A^k \cdot x = \lambda^k x$ vektor se samými ostře kladnými souřadnicemi. Nutně proto je $\lambda > 0$.

Z Perronovy věty víme, že spektrální poloměr μ je vlastním číslem a zvolme takový vlastní vektor y k μ, že rozdíl $x - y$ má samé kladné souřadnice. Potom nutně pro všechny mocniny n

$$0 < A^n \cdot (x - y) = \lambda^n x - \mu^n y,$$

ale zároveň platí $\lambda \le \mu$. Odtud již vyplývá $\lambda = \mu$.

Zbývá odhad spektrálního poloměru pomocí minima a maxima součtů jednotlivých sloupců matice. Označme je $b_{\min}$ a $b_{\max}$, zvolme za x vektor se součtem souřadnic jedna a počítejme:

$$\sum_{i,j=1}^{n} a_{ij}x_j = \sum_{i=1}^{n} \lambda x_i = \lambda$$

$$\lambda = \sum_{j=1}^{n}\Bigl(\sum_{i=1}^{n} a_{ij}\Bigr)x_j \le \sum_{j=1}^{n} b_{\max}x_j = b_{\max}$$

$$\lambda = \sum_{j=1}^{n}\Bigl(\sum_{i=1}^{n} a_{ij}\Bigr)x_j \ge \sum_{j=1}^{n} b_{\min}x_j = b_{\min}$$

□

Všimněmě si, že např. všechny Leslieho matice z 3.15, kde jsou všechny uvažované koeficienty f_i a τ_j ostře kladné, jsou primitivní a tedy na ně můžeme plně použít právě odvozené výsledky.

Perronova-Frobeniova věta je zobecněním Perronovy věty na obecnější matice, které tu nebudeme uvádět. Další informace lze najít např. v **??**.

3.20

3.18. Markovovy řetězce. Velice častý a zajímavý případ lineárních procesů se samými nezápornými prvky v matici je matematický model systému, který se může nacházet v m různých stavech s různou pravděpodobností. V jistém okamžiku je systém ve stavu i s pravděpodobností x_i a k přechodu z možného stavu i do stavu j dojde s pravděpodobností t_{ij}.

Můžeme tedy proces zapsat takto: V čase n je systém popsán pravděpodobnostním vektorem

$$x_n = (u_1(n), \dots, u_m(n))^T.$$

To znamená, že všechny komponenty vektoru x jsou reálná nezáporná čísla a jejich součet je roven jedné. Komponenty udávají rozdělení pravděpodobnosti jednotlivých možností stavů systému. Rozdělení pravděpodobností pro čas $n+1$ bude dáno vynásobením pravděpodobnostní maticí přechodu $T = (t_{ij})$, tj.

$$x_{n+1} = T \cdot x_n.$$

Protože předpokládáme, že vektor x zachycuje všechny možné stavy a proto s celkovou pravděpodobností jedna přejde opět do některého z nich, budou všechny sloupce matice T tvořeny také pravděpodobnostními vektory. Takovému procesu říkáme (diskrétní) *Markovův proces*.

Všimněme si, že každý pravděpodobnostní vektor x je skutečně Markovovým procesem zobrazen na vektor se součtem souřadnic jedna:

$$\sum_{i,j} t_{ij}x_j = \sum_{j}\Bigl(\sum_{i} t_{ij}\Bigr)x_j = \sum_{j} x_j = 1.$$

Nyní můžeme v plné síle použít Perronovu–Frobeniovu teorii. Protože je součet řádků matice T vždy roven vektoru $(1, \dots, 1)$, je zcela elementárně vidět, že matice $T - E$ je singulární a jednička proto bude zaručeně vlastním číslem matice T.

Pokud je navíc T primitivní matice (tj. např. když jsou všechny prvky nenulové), z Důsledku 3.17 víme, že je jednička jednoduchým kořenem charakteristického polynomu a všechny ostatní mají absolutní hodnotu ostře měnší než jedna.

Věta. *Markovovy procesy s maticí, která nemá žádné nulové prvky nebo jejíž některá mocnina má tuto vlastnost, splňují:*

- *existuje jediný vlastní vektor x_∞ pro vlastní číslo 1, který je pravděpodobnostní*
- *iterace $T^k x_0$ se blíží k vektoru x_∞ pro jakýkoliv počáteční pravděpodobnostní vektor x_0.*

Důkaz. První tvrzení vyplývá přímo z kladnosti souřadnic vlastního vektoru dovozené v Perronově větě.

Pokud jsou algebraické a geometrické násobnosti vlastních čísel matice T stejné, pak druhé tvrzení okamžitě vyplývá z toho, že absolutní hodnoty všech ostatních vlastních čísel musí být ostře menší než jedna. Skutečně, za uvedeného předpoladu na vlastní čísla lze každý počáteční vektor x_0 napsat jako součet vlastních vektorů matice T a při iterovaném působení matice T na počátečním vektoru x_0 všechny komponenty rychle vymizí, kromě té jediné s vlastním číslem 1.

Ve skutečnosti ale i při různé algebraické a geometrické násobnosti vlastních čísel dojdeme ke stejnému závěru pomocí podrobnějšího studia tzv. kořenových podprostorů pro matic T, ke kterým se dostaneme v souvislosti s tzv. Jordanovým
3.21 rozkladem ještě v této kapitole, viz poznámka **??**. □

3.19. Iterace stochastických matic. Matice Markovových procesů, tj. matice jejichž všechny sloupce mají součet svých komponent roven jedné se nazývají *stochastické matice*. Standardní úlohy spojené s Markovovými procesy zahrnují odpovědi na otázky po očekávané střední době přechodu mezi předem určenými stavy systému apod. Momentálně nejsme na řešení těchto úloh připraveni, vrátíme se ale k této tématice později.

vymazat příslib, pokud to nenastane, a nahradit odkazem do literatury

Přeformulujeme předchozí větu do jednoduchého, ale asi docela překvapivého důsledku. Konvergencí k limitní matici v následujcím tvrzení myslíme skutečnost, že když si předem určíme možnou chybu $\epsilon > 0$, tak najdeme hranici na počet iterací k po níž už všechny komponenty uvedené matice se od té limitní budou lišit o méně než ϵ.

Důsledek. *Nechť T je primitivní stochastická matice z Markovova procesu a x_∞ je stochastický vlastní vektor k dominantnímu číslu 1 jako ve větě výše. Pak iterace T^k konvergují k limitní matici T_∞, jejíž všechny sloupce jsou rovny x_∞.*

Nyní se ještě na rozlučku s Markovovými procesy zamyslíme se nad problémem, zda existují pro daný systém stavy, do kterých se má systém tendenci dostat a setrvat v nich. O stavu systému řekneme, že je *přechodový*, jestliže v něm systém setrvává s pravděpodobností ostře menší než jedna. Za *absorbční* označíme stav, ve kterém systém setrvává s pravděpodobností 1, a do kterého se lze dostat s nenulovou pravděpodobností z kteréhokoliv z přechodových stavů. Konečně, Markovův řetězec X_n je *absorpční*, jestliže jsou jeho všechny jeho stavy buď absorpční nebo přechodové.

Je-li v absorpčním Markovově řetězci prvních r stavů systému absorpčních, pro stochastickou matici T systému to znamené, že se rozpadá na „blokově“ horní trojúhelníkový tvar

$$T = \begin{pmatrix} E & R \\ 0 & Q \end{pmatrix}$$

kde E je jednotková matice, jejíž rozměr je dán počtem absorpčních stavů, zatímco R je kladná matice a Q nezáporná. V každém případě iteracemi této matice budeme pořád dostávat stejný blok nulových hodnot v levém dolním bloku a tedy zcela jistě nebude primitivní, např.

$$T^2 = \begin{pmatrix} E & R + R \cdot Q \\ 0 & Q^2 \end{pmatrix}.$$

I o takových maticích lze získat hodně informací pomocí plné Perronovy–Frobeniovy teorie a se znalostí pravděpodobnosti a statistiky také odhadovat střední doby, po kterých se systém dostane do jedhodo z abosrpčních stavů apod.

4. Více maticového počtu

Na vcelku praktických příkladech jsme viděli, že porozumění vnitřní struktuře matic a jejim vlastnostem je silným nástrojem pro konkrétní výpočty nebo analýzy. Ještě více to platí pro efektivitu numerického počítání s maticemi. Proto se budeme zase chvíli věnovat abstraktní teorii.

Budeme přitom zkoumat další speciální typy lineárních zobrazení na vektorových prostorech ale také obecný případ, kdy je struktura zobrazení popsána tzv. Jordanovou větou.

3.30 **3.20. Unitární prostory a zobrazení.** Už jsme si zvykli, že je užitečné pracovat rovnou v číselném oboru komplexních čísel a to i v případě, kdy nás zajímají jen reálné objekty. Navíc v mnohých oblastech jsou komplexní vektorové prostory nutnou součástí úvah. Jasným příkladem je například tzv. kvantové počítání, které se stalo velmi akční oblastí teoretické informatiky, přestože kvantové počítače zatím zkonstruovány ve funkční podobě nebyly.

Proto navážeme na ortogonální zobrazení a matice z konce druhé kapitoly následující definicí:

Definice. *Unitární prostor* je komplexní vektorový prostor V spolu se zobrazením $V \times V \to \mathbb{C}$, $(u, v) \mapsto u \cdot v$, které splňuje pro všechny vektory $u, v, w \in V$ a skaláry $a \in \mathbb{C}$

(1) $u \cdot v = \overline{v \cdot u}$ (zde pruh značí komplexní konjugaci)
(2) $(au) \cdot v = a(u \cdot v)$
(3) $(u + v) \cdot w = u \cdot w + v \cdot w$
(4) je-li $u \neq 0$, pak $u \cdot u > 0$ (zejména je výraz reálný).

Toto zobrazení nazýváme *skalární součin* na V.

Reálné číslo $\sqrt{v \cdot v}$ nazýváme *velikostí vektoru* v a vektor je *normovaný*, jestliže má velikost jedna. Vektory u a v nazýváme *ortogonální*, jestliže je jejich skalární součin nulový, bázi sestavenou z po dvou ortogonálních a normovaných vektorů nazýváme *ortonormální báze* V.

Unitární prostory

Na první pohled jde o rozšíření definice euklidovských vektorových prostorů do komplexního oboru. Nadále budeme také používat alternativní značení $\langle u, v\rangle$ pro sklaární součin vektorů u a v. Zcela stejně jako v reálném oboru také okamžitě z definice vyplývají násludující jednoduché vlastnosti skalárního součinu pro všechny vektory ve V a skaláry v $\mathbb{C}$:

$$u \cdot u \in \mathbb{R}$$
$$u \cdot u = 0 \quad \text{právě tehdy, když} \quad u = 0$$
$$u \cdot (av) = \bar{a}(u \cdot v)$$
$$u \cdot (v + w) = u \cdot v + u \cdot w$$
$$u \cdot 0 = 0 \cdot u = 0$$
$$\Big(\sum_i a_i u_i\Big) \cdot \Big(\sum_j b_j v_j\Big) = \sum_{i,j} a_i \bar{b}_j (u_i \cdot v_j),$$

kde poslední rovnost platí pro všechny konečné lineární kombinace. Podrobné ověření je skutečně jednoduchým cvičením, např. první vztah plyne okamžitě z definiční vlastnosti (1).

Standardním příkladem skalárního součinu na komplexním prostoru $\mathbb{C}^n$ je

$$(x_1, \dots, x_n)^T \cdot (y_1, \dots, x_n)^T = x_1 \bar{y}_1 + \dots + x_n \bar{y}_n.$$

Díky konjugování souřadnic druhého argumentu toto zobrazení splňuje všechny požadované vlastnosti. Prostor $\mathbb{C}^n$ s tímto skalárním součinem budeme nazývat *standardní unitární prostor* v dimenzi n. Maticově můžeme tento skalární součin psát jako $x \cdot y = \bar{y}^T \cdot x$.

Zcela obdobně jako u euklidovských prostorů a ortogonálních zobrazení budou důležitá lineárních zobrazení, která respektují skalární součiny.

Lineární zobrazení $\varphi : V \to W$ mezi unitárními prostory se nazývá *unitární zobrazení*, jestliže pro všechny vektory $u, v \in V$ platí

$$u \cdot v = \varphi(u) \cdot \varphi(v).$$

Unitární isomorfismus je bijektivní unitární zobrazení.

Unitární zobrazení

3.31

3.21. Vlastnosti prostorů se skalárním součinem. Ve stručné diskusi euklidovských prostorů v předchozí kapitole jsme už některé jednoduché vlastnosti prostorů se skalárním součinem odvodili, důkazy v komplexním oboru jsou velmi podobné. V dalším budeme pracovat s reálnými i komplexními prostory zároveň a budeme psát $\mathbb{K}$ pro $\mathbb{R}$ nebo $\mathbb{C}$, v reálném případě je konjugace prostě identické zobrazení (tak jak skutečně zúžení konjugace na reálnou přímku v komplexní rovině je). Stejně jako u reálných prostorů definujeme obecně pro libovolný vektorový podprostor $U \subset V$ v prostoru se skalárním součinem jeho *ortogonální doplněk*

$$U^\perp = \{v \in V;\ u \cdot v = 0 \text{ pro všechny } u \in U\},$$

což je zjevně také vektorový podprostor v V.

Budeme v dalším pracovat prakticky pouze s konečněrozměrnými unitárními nebo euklidovskými prostory. Řada našich výsledků ale má přirozené rozšíření pro tzv. Hilbertovy prostory, což jsou jisté nekonečněrozměrné prostory se skalárním součinem, ke kterým se aspoň stručně vrátíme později.

Tvrzení. *Pro každý konečněrozměrný prostor V dimenze n se skalárním součinem platí:*

(1) Ve V existuje ortonormální báze.
(2) Každý systém nenulových ortogonálních vektorů ve V je lineárně nezávislý a lze jej doplnit do ortogonální báze.
(3) Pro každý systém lineárně nezávislých vektorů $(u_1, \dots, u_k)$ existuje ortonormální báze $(v_1, \dots, v_n)$ taková, že její vektory postupně generují stejné podprostory jako vektory u_j, tzn. $\langle v_1, \dots, v_i \rangle = \langle u_1 \dots, u_i \rangle$, $1 \le i \le k$.
(4) Je-li $(u_1, \dots, u_n)$ ortonormální báze V, pak souřadnice každého vektoru $u \in V$ jsou vyjádřeny vztahem

$$u = (u \cdot u_1)u_1 + \dots + (u \cdot u_n)u_n.$$

(5) V libovolné ortonormální bázi má skalární součin souřadný tvar

$$u \cdot v = x \cdot y = x_1\bar{y}_1 + \dots + x_n\bar{y}_n$$

kde x a y jsou sloupce souřadnic vektorů u a v ve zvolené bázi. Zejména je tedy každý n–rozměrný prostor se skalárním součinem izomorfní standardnímu euklidovskému $\mathbb{R}^n$ nebo unitárnímu $\mathbb{C}^n$.
(6) Ortogonální součet unitárních podprostorů $V_1 + \dots + V_k$ ve V je vždy přímý součet.
(7) Je-li $A \subset V$ libovolná podmnožina, pak $A^\perp \subset V$ je vektorový (tedy i unitární) podprostor a $(A^\perp)^\perp \subset V$ je právě podprostor generovaný A. Navíc platí $V = \langle A \rangle \oplus A^\perp$.
(8) V je ortogonálním součtem n jednorozměrných unitárních podprostorů.

Důkaz. (1),(2),(3): Daný systém vektorů nejprve doplníme do libovolné báze $(u_1, \dots, u_n)$ vektorového prostoru V a spustíme na ni Grammovu–Schmidtovu ortogonalizaci z 2.41. Tak získáme ortogonální bázi s vlastnostmi požadovanými v (3). Přitom ale z algoritmu Grammovy–Schmidtovy ortogonalizace vyplývá, že pokud již původních k vektorů tvořilo ortogonální systém vektorů, pak v průběhu ortogonalizace zůstanou nezměněny. Dokázali jsme tedy zároeveň i (2) a (1).
(4): Je-li $u = a_1u_1 + \dots + a_nu_n$, pak

$$u \cdot u_i = a_1(u_1 \cdot u_i) + \dots + a_n(u_n \cdot u_i) = a_i\|u_i\|^2 = a_i$$

(5): Podobně spočteme pro $u = x_1u_1 + \dots + x_nu_n$, $v = y_1u_1 + \dots + y_nu_n$

$$u \cdot v = (x_1u_1 + \dots + x_nu_n) \cdot (y_1u_1 + \dots + y_nu_n) = x_1\bar{y}_1 + \dots + x_n\bar{y}_n.$$

(6): Potřebujeme ukázat, že pro libovolnou dvojici V_i, V_j ze zadaných podprostorů je jejich průnik triviální. Je-li však

$u \in V_i$ a zároveň $u \in V_j$, pak je $u \perp u$, tj. $u \cdot u = 0$. To je ale možné pouze pro nulový vektor $u \in V$.
(7): Nechť $u, v \in A^\perp$. Pak $(au + bv) \cdot w = 0$ pro všechny $w \in A$, $a, b \in \mathbb{K}$ (z distributivity skalárního součinu). Tím jsme ověřili, že $A^\perp$ je unitární podprostor ve V. Nechť $(v_1, \dots, v_k)$ je nějaká báze $\langle A \rangle$, vybraná z prvků A, $(u_1, \dots, u_k)$ ortonormální báze vzniklá z Grammovy–Schmidtovy ortogonalizace vektorů $(v_1, \dots, v_k)$. Doplňme ji na ortonormální bázi celého V (obojí existuje podle již dokázaných částí věty). Protože se jedná o ortogonální bázi, je nutně $\langle u_{k+1}, \dots, u_n \rangle = \langle u_1, \dots, u_k \rangle^\perp = A^\perp$ a $A \subset \langle u_{k+1}, \dots, u_n \rangle^\perp$ (jak plyne z vyjádření souřadnic v ortonormální bázi). Je-li $u \perp \langle u_{k+1}, \dots, u_n \rangle$, pak u je nutně lineární kombinací vektorů $u_1, \dots, u_k$, to je ale právě tehdy, když je lineární kombinací vektorů $v_1, \dots, v_k$, což je ekvivalentní příslušnosti u do $\langle A \rangle$.
(8): Je pouze ekvivalentní formulací existence ortonormální báze. □

3.32

3.22. Důležité vlastnosti velikosti. Nyní máme vše připraveno pro základní vlastnosti spojené s naší definicí velikostí vektorů. Hovoříme také o *normě* definované skalárním součinem. Všimněme si také, že všechna tvrzení se týkají vždy konečných množin vektorů a jejich platnost proto nezávisí na dimenzi prostoru V, ve kterém se vše odehrává.

Věta. *Pro libovolné vektory u, v v prostoru V se skalárním součinem platí*

(1) $\|u+v\| \le \|u\| + \|v\|$ *Přitom rovnost nastane právě, když jsou u a v lineárně závislé.*
(trojúhelníková nerovnost)
(2) $|u \cdot v| \le \|u\| \, \|v\|$ *Přitom rovnost nastane právě, když jsou u a v lineárně závislé.*
(Cauchyova nerovnost)
(3) pro každý ortonormální systém vektorů $(e_1, \dots, e_k)$ platí $\|u\|^2 \ge |u \cdot e_1|^2 + \dots + |u \cdot e_k|^2$
(Besselova nerovnost).
(4) Pro ortonormální systém vektorů $(e_1, \dots, e_k)$ je vektor u v podprostoru $\in \langle e_1, \dots, e_k \rangle$ právě když

$$\|u\|^2 = |u \cdot e_1|^2 + \dots + |u \cdot e_k|^2.$$

(Parsevalova rovnost)
(5) Pro ortonormální systém vektorů $(e_1, \dots, e_k)$ a $u \in V$ je vektor

$$w = (u \cdot e_1)e_1 + \dots + (u \cdot e_k)e_k$$

jediným vektorem, který minimalizuje velikost $\|u - v\|$ pro všechny $v \in \langle e_1, \dots, e_k \rangle$.

Důkaz. Všechny důkazy spočívají v podstatě v přímých výpočtech:
(2): Definujme vektor $w := u - \frac{u \cdot v}{v \cdot v} v$, tzn. $w \perp v$ a počítejme

$$0 \le \|w\|^2 = \|u\|^2 - \frac{(\overline{u \cdot v})}{\|v\|^2}(u \cdot v) - \frac{u \cdot v}{\|v\|^2}(v \cdot u) + \frac{(u \cdot v)(\overline{u \cdot v})}{\|v\|^4}\|v\|^2$$

$$0 \le \|w\|^2 \|v\|^2 = \|u\|^2 \|v\|^2 - 2(u \cdot v)(\overline{u \cdot v}) + (u \cdot v)(\overline{u \cdot v})$$

Odtud již přímo plyne, že $\|u\|^2\|v\|^2 \geq |u \cdot v|^2$ a rovnost nastane právě tehdy, když $w = 0$, tj. když jsou u a v lineárně závislé.
(1): Opět stačí počítat

$$\begin{aligned}\|u + v\|^2 &= \|u\|^2 + \|v\|^2 + u \cdot v + v \cdot u \\ &= \|u\|^2 + \|v\|^2 + 2\,\mathrm{Re}(u \cdot v) \\ &\leq \|u\|^2 + \|v\|^2 + 2|u \cdot v| \leq \|u\|^2 + \|v\|^2 + 2\|u\|\|v\| \\ &= (\|u\| + \|v\|)^2\end{aligned}$$

Protože se přitom jedná o kladná reálná čísla, je opravdu $\|u+v\| \leq \|u\| + \|v\|$. Navíc, při rovnosti musí nastat rovnost ve všech předchozích nerovnostech, to však je ekvivalentní podmínce, že u a v jsou lineárně závislé (podle předchozí části důkazu).
(3), (4): Nechť $(e_1, \dots, e_k)$ je ortonormální systém vektorů. Doplníme jej do ortonormální báze $(e_1, \dots, e_n)$ (to vždy jde podle předchozí věty). Pak, opět podle předchozí věty, je pro každý vektor $u \in V$

$$\|u\|^2 = \sum_{i=1}^{n}(u \cdot e_i)(\overline{u \cdot e_i}) = \sum_{i=1}^{n} |u \cdot e_i|^2 \geq \sum_{i=1}^{k} |u \cdot e_i|^2$$

To je ale právě dokazovaná Besselova nerovnost. Přitom rovnost může nastat právě tehdy, když $u \cdot e_i = 0$ pro všechny $i > k$, a to dokazuje Parsevalovu rovnost.
(5): Zvolme libovolný $v \in \langle e_1, \dots, e_k\rangle$ a doplňme daný ortonormální systém na ortonormální bázi $(e_1, \dots, e_n)$. Nechť $(u_1, \dots, u_n)$ a $(x_1, \dots, x_k, 0, \dots, 0)$ jsou souřadnice u a v v této bázi. Pak

$$\|u-v\|^2 = |u_1-x_1|^2+\dots+|u_k-x_k|^2+|u_{k+1}|^2+\dots+|u_n|^2$$

a tento výraz je zjevně minimalizován při volbě jednotlivých vektorů $x_1 = u_1, \dots, x_k = u_k$. □

3.33 **3.23. Vlastnosti unitárních zobrazení.** Vlastnosti ortogonálních zobrazení mají přímočarou obdobu v komplexním oboru. Můžeme je snadno zformulovat a dokázat společně:

Tvrzení. *Uvažme lineární zobrazení (endomorfismus) $\varphi : V \to V$ na prostoru se skalárním součinem. Pak jsou následující podmínky ekvivalentní:*

(1) φ je unitární nebo ortogonální transformace
(2) φ je lineární isomorfismus a pro každé $u, v \in V$ platí $\varphi(u) \cdot v = u \cdot \varphi^{-1}(v)$
(3) matice A zobrazení φ v libovolné ortonormální bázi splňuje $A^{-1} = \bar{A}^T$ (pro euklidovské prostory to znamená $A^{-1} = A^T$)
(4) matice A zobrazení φ v některé ortonormální bázi splňuje $A^{-1} = \bar{A}^T$
(5) řádky matice A zobrazení φ v ortonormální bázi tvoří ortonormální bázi prostoru $\mathbb{K}^n$ se standardním skalárním součinem
(6) sloupce matice A zobrazení φ v ortonormální bázi tvoří ortonormální bázi prostoru $\mathbb{K}^n$ se standardním skalárním součinem

Důkaz. (1) $\Rightarrow$ (2): Zobrazení φ je prosté, proto musí být i na. Platí přitom $\varphi(u)\cdot v = \varphi(u)\cdot\varphi(\varphi^{-1}(v)) = u\cdot\varphi^{-1}(v)$.
(2) $\Rightarrow$ (3): Standardní skalární součin je v $\mathbb{K}^n$ vždy dán pro sloupce x, y skalárů výrazem $x \cdot y = x^T E \bar{y}$, kde E je jednotková matice. Vlastnost (2) tedy znamená, že matice A zobrazení φ je invertibilní a platí $(Ax)^T \bar{y} = x^T \overline{A^{-1} y}$. To znamená $\bar{x}^T(\bar{A}^T y - A^{-1} y) = 0$ pro všechny $x \in \mathbb{K}^n$. Zejména dosazením výrazu v závorce za x zjistíme, že to je možné pouze při $\bar{A}^T = A^{-1}$.
(3) $\Leftrightarrow$ (4): Je-li $\bar{A}^T = A^{-1}$ v některé ortonormální bázi, pak to zaručuje platnost podmínky (2) ($\varphi(u) \cdot v = (Ax)^T E \bar{y} = x^T E \overline{A^{-1} y} = u \cdot \varphi^{-1}(v)$) a tedy i (3).
(4) $\Rightarrow$ (5) Dokazované tvrzení je vyjádřeno prostřednictvím matice A zobrazení φ vztahem $A\bar{A}^T = E$, to je ale zaručeno podmínkou (4).
(5) $\Rightarrow$ (6): Protože pro determinant platí $|\bar{A}^T A| = |E| = |A\bar{A}^T| = |A||\overline{A}| = 1$, existuje inverzní matice A^{-1}. Přitom je $A\bar{A}^T A = A$, proto i $\bar{A}^T A = E$ což vyjadřuje právě (6).
(6) $\Rightarrow$ (1): Ve vybrané ortonormální bázi je

$$\varphi(u) \cdot \varphi(v) = (Ax)^T \overline{(Ay)} = x A^T \bar{A} \bar{y} = x^T \bar{E} \bar{y} = x^T \bar{y}$$

kde x a y jsou sloupce souřadnic vektorů u a v. Tím je zaručeno zachovávání skalárního součinu. $\square$

Charakterizace z předchozí věty si zaslouží několik poznámek. Matice $A \in \mathrm{Mat}_n(\mathbb{K})$ s vlastností $A^{-1} = \bar{A}^T$ se nazývají *unitární matice* pro komplexní skaláry (a v případě $\mathbb{R}$ jsme jim již říkali *ortogonální matice*). Z definiční vlastnosti plyne, že součin unitárních (resp. ortogonálních) matic je unitární (resp. ortogonální), stejně pro inverze. Unitární matice tedy tvoří podgrupu $U(n) \subset \mathrm{Mat}_n(\mathbb{C})$, ortogonální matice tvoří podgrupu $O(n) \subset \mathrm{Mat}_n(\mathbb{R})$. Hovoříme o *unitární grupě* a o *ortogonální grupě*.

Jednoduchý výpočet

$$1 = \det E = \det(A\bar{A}^T) = \det A\, \overline{\det A} = |\det A|^2$$

ukazuje, že determinant unitární matice má vždy velikost rovnu jedné, v případě reálných skalárů pak determinant musí být ± 1. Dále, je-li $Ax = \lambda x$ pro unitární či ortogonální matici, pak $(Ax) \cdot (Ax) = x \cdot x = |\lambda|^2 (x \cdot x)$. Proto jsou vlastní hodnoty ortogonálních matic v reálném oboru rovny ± 1, vlastní hodnoty unitárních matic jsou vždy komplexní jednotky v komplexní rovině.

Stejně jako u ortogonálních zobrazení také docela snadno ověříme, že ortogonální doplňky k invariantním podprostorům vzhledem k unitárnímu $\varphi : V \to V$ jsou vždy také invariatní. Skutečně, je-li $\varphi(U) \subset U$, $u \in U$ a $v \in U^\perp$ libovolné, pak

$$\varphi(v) \cdot \varphi(\varphi^{-1}(u)) = v \cdot \varphi^{-1}(u).$$

Protože je zúžení $\varphi_{|U}$ také unitární, musí to tedy být bijekce, zejména je $\varphi^{-1}(u) \in U$. Pak ovšem $\varphi(v) \cdot u = 0$, protože $v \in U^\perp$. To znamená, že i $\varphi(v) \in U^\perp$.

Odtud ovšem v komplexním oboru okamžitě dotáváme užitečný

Důsledek. *Nechť $\varphi : V \to V$ je unitární zobrazení komplexních vektorových prostorů. Pak je V ortogonálním součtem jednorozměrných vlastních podprostorů.*

Důkaz. Jistě existuje alespoň jeden vlastní vektor $v \in V$. Pak je zúžení φ na invariantní podprostor $\langle v\rangle^{\perp}$ opět unitární a jistě má opět nějaký vlastní vektor. Po n takovýchto krocích obdržíme hledanou ortogonální bázi z vlastních vektorů. Po vynormování vektorů získáme ortonormální bázi. □

Nyní už je možné snadno pochopit detaily důkazu spektrálního rozkladu ortogonálního zobrazení z 2.48 na konci druhé kapitoly — reálnou matici ortogonálního zobrazení interpretujeme jako matici unitárního zobrazení na komplexním rozšíření euklidovského prostoru a pečlivě sledujeme důsledky struktury kořenů reálného charakteristického polynomu nad komplexním oborem. Automaticky přitom dostáváme invariantní dvourozměrné podprostory zadané dvojicemi komplexně sdružených vlastních čísel a tedy příslušné rotace pro zúžené původní reálné zobrazení.

3.34

3.24. Duální a adjungovaná zobrazení. Při diskusi vektorových prostorů a lineárních zobrazení jsme již ve druhé kapitole letmo zmínili duální vektorový prostor V^* všech lineárních forem na vektorovém prosotru V, viz 2.37.

Pro každé lineární zobrazení mezi vektorovými prostory $\psi : V \to W$ můžeme přirozeně definovat zobrazení $\psi^* : W^* \to V^*$ vztahem

$$\langle v, \psi^*(\alpha)\rangle = \langle \psi(v), \alpha\rangle,$$

kde $\langle\ ,\ \rangle$ značí vyčíslení formy (druhý argument) na vektoru (první argument), $v \in V$ a $\alpha \in W^*$ jsou libovolné. Zvolme si báze $\underline{v}$ na V, $\underline{w}$ na W a matici A pro zobrazení ψ v těchto bazích. Pak snadno spočteme v duálních bazích matici zobrazení ψ^* v příslušných duálních bazí na duálních prostorech. Skutečně, definiční vztah říká, že pokud bychom reprezentovali vektory z W^* v souřadnicích jako řádky skalárů, pak je zobrazení ψ^* je dáno toutéž maticí jako ψ, pokud jí násobíme řádkové vektory zprava:

$$\langle \psi(v), \alpha\rangle = (\alpha_1, \dots, \alpha_n)\cdot A \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \langle v, \psi^*(\alpha)\rangle.$$

To znamená, že maticí duálního zobrazení ψ^* je transponovaná matice A^T, protože $\alpha \cdot A = (A^T \cdot \alpha^T)^T$.

Předpokládejme nadále, že se pohybujeme ve vektorovém prostoru se skalárním součinem. Jestliže tedy zvolíme pevně jeden vektor $v \in V$, dosazování vektorů za druhý argument ve skalárním součinu nám dává zobrazení $V \to V^* = \mathrm{Hom}(V, \mathbb{K})$

$$V \ni v \mapsto (w \mapsto \langle v, w\rangle \in \mathbb{K}).$$

Podmínka nedegenerovanosti skalárního součinu nám zaručuje, že toto zobrazení je bijekcí. Zároveň víme, že jde skutečně o lineární zobrazení nad komplexními nebo reálnými skaláry, protože jsme pevně zvolili druhý argument.

Na první pohled je vidět, že vektory ortonormální báze jsou takto zobrazeny na formy tvořící bázi duální, a každý vektor můžeme prostřednictvím skalárního součinu chápat také jako lineární formu.

V případě vektorových prostorů se skalárním součinem proto převádí naše ztotožnění vektorového prostoru se svým duálem také duální zobrazení ψ^* na zobrazení $\psi^* : W \to V$ zadané formulí

$$\langle \psi(u), v \rangle = \langle u, \psi^*(v) \rangle,$$

kde stejným značením závorek nyní myslíme skalární součin. Tomuto zobrazení se říká *adjungované zobrazení* k ψ. Ekvivalentně lze brát poslední vztah za definici zobrazení ψ^*, např. dosazením všech dvojic vektorů ortonormální báze za vektory u a v dostáváme přímo všechny hodnoty matice zobrazení ψ^*.

Předchozí výpočet pro duální zobrazení v souřadnicích nyní můžeme zopakovat, pouze musíme mít na paměti, že v ortonormálních bazích na unitárních prostorech vystupují souřadnice druhého argumentu konjugované:

$$\begin{aligned}
\langle \psi(v), w \rangle &= \overline{(w_1, \dots, w_n)} \cdot A \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \\
&= \overline{\left(\bar{A}^T \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \right)}^T \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \langle v, \psi^*(w) \rangle
\end{aligned}$$

Vidíme proto, že je-li A matice zobrazení ψ v ortonormální bázi, pak matice adjungovaného zobrazení ψ^* je matice transponovaná a konjugovaná, kterou značíme $A^* = \bar{A}^T$.

Zvláštním případem lineárních zobrazení jsou tedy ty, které jsou rovny svému adjungovanému zobrazení: $\psi^* = \psi$. Takovým zobrazením říkáme *samoadjungovaná*. Ekvivalentně můžeme říci, že jsou to ta zobrazení, jejichž matice A v jedné a tedy ve všech ortonormálních bazích splňují $A = A^*$.

V případě euklidovských prostorů jsou samoadjungovaná zobrazení tedy ta, která mají v některé ortonormální bázi (a pak už všech) symetrickou matici. Často se jim proto říká symetrické matice a symetrická zobrazení. V komplexním oboru se maticím splňujícím $A = A^*$ říká *hermiteovské matice*. Všimněme si, že hermiteovské matice tvoří reálný vektorový podprostor v prostoru všech komplexních matic, není však podprostorem v komplexním oboru.

Poznámka. Obzvlášť zajímavý je v této souvislosti následující postřeh. Jestliže hermiteovskou matici A vynásobíme imaginární jednotkou, dostáváme matici $B = i\,A$, která má vlastnost $B^* = \bar{i}\,\bar{A}^T = -B$. Takovým maticím říkáme anti–hermiteovské. Tak jako je tedy každá reálná matice součtem své symetrické a antisymetrické části

$$A = \frac{1}{2}(A + A^T) + \frac{1}{2}(A - A^T),$$

je v koplexním oboru obdobně

$$A = \frac{1}{2}(A + A^*) + \frac{1}{2}(A - A^*),$$

tj. můžeme vyjadřit každou komplexní matici právě jedním způsobem jako součet

$$A = B + i\,C$$

s hermiteovskými maticemi B a C. Jde o obdobu rozkladu komplexního čísla na reálnou a ryze imaginární komponentu.

V řeši lineárních zobrazení to tedy znamená, že každý komplexní lineární automorfismus můžeme takto jednoznačně vyjádřit pomocí dvou samoadjungovaných zobrazení.

3.35

3.25. Spektrální rozklad samoadjungovaných zobrazení. Uvažujme samoadjungované zobrazení $\psi : V \to V$ s maticí A v nějaké ortonormální bázi a zkusme postupovat obdobně jako v 2.48. Opět se nejprve obecně podíváme na invariantní podprostory samoadjungovaných zobrazení a jejich ortogonální doplňky. Jestliže pro libovolný podprostor $W \subset V$ a samoadjungované zobrazení $\psi : V \to V$ platí $\psi(W) \subset W$, pak také platí pro všechny $v \in W^{\perp}$, $w \in W$

$$\langle \psi(v), w \rangle = \langle v, \psi(w) \rangle = 0.$$

To ale znamená, že také $\psi(W^{\perp}) \subset W^{\perp}$.

Uvažme nyní matici A samoadjungovaného zobrazení v nějaké ortonormální bázi a $A \cdot x = \lambda x$ pro nějaký vlastní vektor $x \in \mathbb{C}^n$. Dostáváme

$$\lambda \langle x, x \rangle = \langle Ax, x \rangle = \langle x, Ax \rangle = \bar{\lambda} \langle x, x \rangle.$$

Kladným reálným číslem $\langle x, x \rangle$ můžeme krátit a proto musí být $\bar{\lambda} = \lambda$, tj. vlastní čísla jsou vždy reálná.

Komplexních kořenů má charakteristický polynom $\det(A - \lambda E)$ tolik, kolik je dimenze čtvercové matice A, a všechny jsou ve skutečnosti reálné. Dokázali jsme tak důležitý obecný výsledek:

Tvrzení. *Ortogonální doplněk k invariantnímu podprostoru pro samoadjungované zobrazení je také invariantní. Navíc jsou všechna vlastní čísla samoadjungované matice A vždy reálná.*

Ze samotné definice je zřejmé, že zúžení samoadjungovaného zobrazení na invariantní podprostor je opět samoadjungované. Předchozí tvrzení nám tedy zaručuje, že bude vždy existovat báze V z vlastních vektorů. Skutečně, zúžení ψ na ortogonální doplněk invariantního podprostoru je opět ortogonální zobrazení, takže můžeme do báze přibírat jeden vlastní vektor za druhým, až dostaneme celý rozklad V. Vlastní vektory příslušející různým vlastním číslům jsou navíc kolmé, protože z rovností $\psi(u) = \lambda u$, $\psi(v) = \mu v$ vyplývá

$$\lambda \langle u, v \rangle = \langle \psi(u), v \rangle = \langle u, \psi(v) \rangle = \mu \langle u, v \rangle.$$

Obvykle bývá náš výsledek formulován pomocí projekcí na vlastní podprostory. O projektoru $P : V \to V$ říkáme, že je *kolmý*, je-li $\operatorname{Im} P \perp \operatorname{Ker} P$. Dva kolmé projektory P, Q jsou *vzájemně kolmé*, je-li $\operatorname{Im} P \perp \operatorname{Im} Q$.

Věta (O spektrálním rozkladu). *Pro každé samoadjungované zobrazení $\psi : V \to V$ na vektorovém prostoru se skalárním součinem existuje ortonormální báze z vlastních vektorů. Jsou-li $\lambda_1, \dots, \lambda_k$ všechna různá vlastní čísla f a $P_1, \dots, P_k$ příslušné kolmé a navzájem kolmé projektory na vlastní podprostory, pak*

$$f = \lambda_1 P_1 + \dots + \lambda_k P_k.$$

Dimenze obrazů těchto projektorů je přitom vždy rovna algebraické násobnosti vlastních čísel λ_i.

3.36

3.26. Ortogonální diagonalizace. Zamysleme se, jak vypadají zobrazení, pro která lze najít ortonormální bázi jako v předchozí větě o spektrálním rozkladu se nazývají *normální*. Pro euklidovský případ je to snadné: diagonální matice jsou zejména symetrické, jedná se tedy právě o samoadjungovaná zobrazení. Jako důsledek získáváme tvrzení, že ortogonální zobrazení euklidovského prostoru do sebe je ortogonálně diagonalizovatelné právě, když je zároveň samoadjungované (jsou to právě ta samoadjungovaná zobrazení s vlastními hodnotami ± 1).

U komplexních unitárních prostorů je situace složitější. Uvažme libovolné lineární zobrazení $\varphi : V \to V$ unitárního prostoru a nechť $\varphi = \psi + i\eta$ je (jednoznačně daný) rozklad φ na hermiteovskou a antihermiteovskou část. Má-li φ ve vhodné ortonormální bázi diagonální matici D, pak $D = \mathrm{re} D + i \mathrm{im} D$, kde reálná a imaginární část jsou právě matice ψ a η (plyne z jednoznačnosti rozkladu). Zejména tedy platí $\psi \circ \eta = \eta \circ \psi$ a $\varphi \circ \varphi^* = \varphi^* \circ \varphi$. Zobrazení $\varphi : V \to V$ s poslední uvedenou vlastností se nazývají *normální*.

Vzájemné souvislosti ukazuje následující věta (pokračujeme ve značení tohoto odstavce):

Tvrzení. *Následující podmínky jsou ekvivalentní:*

(1) φ *je ortogonálně diagonalizovatelné*
(2) $\varphi^* \circ \varphi = \varphi \circ \varphi^*$ *(tj. φ je normální zobrazení)*
(3) $\psi \circ \eta = \eta \circ \psi$
(4) Pro matici $A = (a_{ij})$ zobrazení φ v nějaké ortonormální bázi a jejích $m = \dim V$ vlastních čísel λ_i platí $\sum_{i,j} |a_{ij}|^2 = \sum_{i=1}^m |\lambda_i|^2$.

Stručný důkaz. Implikaci (1) $\Rightarrow$ (2) jsme již diskutovali.

(2) $\Leftrightarrow$ (3): Stačí provést přímý výpočet

$$\varphi\varphi^* = (\psi + i\eta)(\psi - i\eta) = \psi^2 + \eta^2 + i(\eta\psi - \psi\eta)$$
$$\varphi^*\varphi = (\psi - i\eta)(\psi + i\eta) = \psi^2 + \eta^2 + i(\psi\eta - \eta\psi)$$

Odečtením dostaneme $2i(\eta\psi - \psi\eta)$.

(2) $\Rightarrow$ (1): Nechť $u \in V$ je vlastní vektor normálního zobrazení φ. Pak

$$\varphi(u) \cdot \varphi(u) = \langle \varphi^*\varphi(u), u \rangle = \langle \varphi\varphi^*(u), u \rangle = \varphi^*(u) \cdot \varphi^*(u)$$

zejména tedy $|\varphi(u)| = |\varphi^*(u)|$. Je-li φ normální, je $(\varphi - \lambda \,\mathrm{id}\, V)^* = (\varphi^* - \bar{\lambda}\,\mathrm{id}\, V)$ a je proto i $(\varphi - \lambda\,\mathrm{id}\, V)$ normální zobrazení. Z předešlé rovnosti tedy plyne, že je-li $\varphi(u) = \lambda u$, pak $\varphi^*(u) = \bar{\lambda}u$. Tzn., že φ a φ^* mají stejné vlastní vektory a konjugované vlastní hodnoty.

Stejně jako u samoadjungovaných teď snadno dokážeme ortogonální diagonalizovatelnost. K tomu je nutné a stačí, aby ortogonální doplněk každého vlastního podprostoru pro normální φ byl invariantní (je totiž zúžení normálního zobrazení na invariantní podprostor opět normální). Uvažme vlastní vektor $u \in V$ s vlastní hodnotou λ, $v \in \langle u \rangle^{\perp}$. Platí

$$\varphi(v) \cdot u = v \cdot \varphi^*(u) = \langle v, \bar{\lambda}u \rangle = \lambda u \cdot v = 0$$

a tedy opět $\varphi(v) \in \langle u \rangle^{\perp}$.

(1) $\Leftrightarrow$ (4): Výraz $\sum_{i,j} |a_{ij}|^2$ je právě stopa matice AA^*, to je matice zobrazení $\varphi \circ \varphi^*$. Proto nezávisí na volbě ortonormální báze. Je-li tedy φ diagonalizovatelné, je tento výraz roven právě $\sum_i |\lambda_i|^2$.

Opačná implikace je přímým důsledkem Schurovy věty o unitární triangulovatelnosti libovolného lineárního zobrazení $V \to V$, kterou dokážeme později v 3.32. Podle ní totiž existuje pro každé lineární zobrazení $\varphi : V \to V$ ortonormální báze, ve které má φ horní trojúhelníkovou matici. Na její diagonále pak musí být právě všechny vlastní hodnoty φ. Jak jsme již ukázali, výraz $\sum_{i,j} |a_{ij}|^2$ nezávisí na volbě ortonormální báze, proto z předpokládané rovnosti vyplývá, že všechny prvky mimo diagonálu musí být v této matici nulové. □

V termínech matic zobrazení dostáváme: zobrazení je normální právě, když jeho matice v některé ortonormální bázi (a ekvivalentně v každé) splňuje $AA^* = A^*A$. Takové matice nazýváme *normální matice*.

Poznámka. Všimněme si, že pro počet s lineárními zobrazeními na komplexním unitárním prostoru lze poslední větu chápat také jako zobecnění běžných počtů s komplexními čísly v goniometrickém tvaru (roli reálných čísel zde hrají samoadjungovaná zobrazení). Roli komplexních jednotek pak hrají unitární zobrazení. Zejména si všimněme analogie k jejich tvaru $\cos t + i \sin t$ s vlastností $\cos^2 t + \sin^2 t = 1$:

Důsledek. *Unitární zobrazení na unitárním prostoru V jsou právě ta normální zobrazení, pro která výše užívaný jednoznačný rozklad $\varphi = \psi + i\eta$ splňuje $\psi^2 + \eta^2 = \mathrm{id}\, V$*

Důkaz. Pro unitární je $\varphi\varphi^* = \mathrm{id}\, V = \varphi^*\varphi$ a tedy $\varphi\varphi^* = (\psi + i\eta)(\psi - i\eta) = \psi^2 + 0 + \eta^2 = \mathrm{id}\, V$. Naopak, pro normální poslední výpočet ukazuje, že opačná implikace platí také. □

2.48

3.27. Nezáporná zobrazení a odmocniny. Nezáporná reálná čísla jsou právě ta, která umíme psát jako druhé mocniny. Zobecnění takového chování pro matice a zobrazení lze vidět u součinů $B = A^* \cdot A$ (tj. složení zobrazení $\psi^* \circ \psi$):

$$\langle B \cdot x, x \rangle = \langle A^* \cdot A \cdot x, x \rangle = \langle A \cdot x, A \cdot x \rangle \geq 0$$

pro všechny vektory x. Navíc zjevně

$$B^* = (A^* \cdot A)^* = A^* \cdot A = B.$$

Hermiteovských maticím B s takovou vlastností říkáme *pozitivně semidefinitní* a pokud nastane nulová hodnota pouze pro $x = 0$, pak jim říkáme *pozitivně definitní*. Obdobně hovoříme o *pozitivě definitních* a *a positivně semidefinitních* zobrazeních $\psi : V \to V$.

Pro každé pozitivně semidefinitní zobrazení $\psi : V \to V$ umíme najít jeho odmocninu, tj. zobrazení η takové, že $\eta \circ \eta = \psi$. Nejjednodušeji to uvidíme v ortonormální bázi, ve které bude mít ψ diagonální matici. Taková podle našich předchozích úvah vždy existuje a matice A zobrazení ψ v ní bude mít na diagonále nezáporná reálná vlastní čísla zobrazení ψ. Kdyby totiž bylo některé z nich záporné, nebyla by splněna podmínka nezápornosti již pro některý z bázových vektorů. Pak ovšem stačí definovat zobrazení η pomocí matice B s odmocninami příslušných vlastních čísel na diagonále.

2.32

3.28. Spektra a nilpotentní zobrazení. Na závěr této části se vrátíme k otázce, jak se mohou chovat lineární zobrazení v úplné obecnosti. Budeme i nadále pracovat s reálnými nebo komplexními vektorovými prostory.

Připomeňme, že *spektrum lineárního zobrazení* $f : V \to V$ je posloupnost kořenů charakteristického polynomu zobrazení f, včetně násobností. *Algebraickou násobností* vlastní hodnoty rozumíme její násobnost jako kořenu charakteristického polynomu, *geometrická násobnost* vlastní hodnoty je dimenze příslušného podprostoru vlastních vektorů.

Lineární zobrazení $f : V \to V$ se nazývá *nilpotentní*, jestliže existuje celé číslo $k \geq 1$ takové, že iterované zobrazení f^k je identicky nulové. Nejmenší číslo k s touto vlastností se nazývá *stupněm nilpotentnosti* zobrazení f. Zobrazení $f : V \to V$ se nazývá *cyklické*, jestliže existuje báze $(u_1, \dots, u_n)$ prostoru V taková, že $f(u_1) = 0$ a $f(u_i) = u_{i-1}$ pro všechna $i = 2, \dots, n$. Jinými slovy, matice f v této bázi je tvaru

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & & \ddots \end{pmatrix}.$$

Je-li $f(v) = a \cdot v$, pak pro každé přirozené k je $f^k(v) = a^k \cdot v$. Zejména tedy může spektrum nilpotentního zobrazení obsahovat pouze nulový skalár (a ten tam vždy je).

Přímo z definice plyne, že každé cyklické zobrazení je nilpotentní, navíc je jeho stupeň nilpotentnosti roven dimenzi prostoru V. Operátor derivování na polynomech, $D(x^k) = kx^{k-1}$, je příkladem cyklického zobrazení na $\mathbb{K}_n[x]$ pro libovolné n.

Kupodivu to platí i naopak a každé nilpotentní zobrazení je přímým součtem cyklických. Důkaz tohoto tvrzení nám dá hodně práce, proto napřed zformulujeme další výsledky a pak se teprve dáme do technické práce. Ve výsledné větě o *Jordanově rozkladu* vvystupují vektorové (pod)prostory a lineární zobrazení na nich s jediným vlastním číslem λ a maticí

$$J = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & \dots & \lambda \end{pmatrix}.$$

Takovýmto maticím (a odpovídajícím invariantním podprostorům) se říká *Jordanův blok*.

Věta (Jordanova věta o kanonickém tvaru)**.** *Nechť V je vektorový prostor dimenze n a $f : V \to V$ je lineární zobrazení s n vlastními čísly včetně algebraických násobností. Pak existuje jednoznačný rozklad prostoru V na přímý součet podprostorů*

$$V = V_1 \oplus \dots \oplus V_k$$

takových, že $f(V_i) \subset V_i$, zúžení f na každé V_i má jediné vlastní číslo λ_i a zúžení $f - \lambda_i \cdot \mathrm{id}$ na V_i je buď cyklické nebo nulové zobrazení.

Věta tedy říká, že ve vhodné bázi má každé lineární zobrazení blokově diagonální tvar s Jordanovými bloky podél diagonály. Celkový počet jedniček nad diagonálou v takovém tvaru je roven rozdílu mezi celkovou algebraickou a geometrickou násobností vlastních čísel.

Všimněme si, že jsme tuto větu plně dokázali v případech, kdy jsou všechna vlastní čísla různá nebo když jsou geometrické a algebraické násobnosti vlastních čísel stejné. Také jsme ji plně dokázali pro unitární a samoadjungovaná zobrazení.

Také si všimněme, že v situaci, kdy jsou vlastní hodnoty v absolutní hodnotě menší než jedna, opakované působení lineárního zobrazení na jakémkoliv vektoru v z jednoho z podprostorů V_i ve větě vede k rychlému zmenšování všech jeho souřadnic nad všechny meze. Skutečně, předpokládejme pro jednoduchost, že na celém V_i je naše zobrazení cyklické, příslušná vlastní hodnota je λ a $v_1, \dots, v_\ell$ nechť je příslušná báze. Pak podmínka z věty říká, že $f(v_2) = \lambda v_2 + v_1$, $f^2(v_j) = \lambda^2 v_2 + \lambda v_1 + \lambda v_1$, a podobně pro ostatní v_i a vyšší mocniny. V každém případě při iterování dostáváme stále vyšší a vyšší mocniny λ u všech nenulových komponent.

Zbytek této části je věnován důkazu Jordanovy věty a několika k tomu potřebným pojmům. Je výrazně obtížnější než dosavadní text a čtenář jej může případně přeskočit až do začátku 5. části této kapitoly.

3.37

3.29. Kořenové prostory. Na příkladech jsme viděli, že vlastní podprostory popisují dostatečně geometrické vlastnosti jen některých lineárních zobrazení. Zavedeme nyní jemnější nástroj, tzv. kořenové podprostory.

Definice. Nenulový vektor $u \in V$ se nazývá *kořenovým vektorem* lineárního zobrazení $\varphi : V \to V$, jestliže existuje $a \in \mathbb{K}$ a celé číslo $k > 0$ takové, že $(\varphi - a \cdot \mathrm{id}_V)^k(u) = 0$, tj. k-tá iterace uvedeného zobrazení zobrazuje u na nulu. Množinu všech kořenových vektorů příslušných k pevnému skaláru λ doplněnou o nulový vektor nazýváme *kořenovým prostorem* příslušným ke skaláru $\lambda \in \mathbb{K}$, značíme $\mathcal{R}_\lambda$.

Je-li u kořenový vektor a k z definice je vybráno nejmenší možné, pak $(\varphi - a \cdot \mathrm{id}_V)^{k-1}(u)$ je vlastní vektor s vlastní hodnotou a. Je tedy $\mathcal{R}_\lambda = \{0\}$ pro všechny skaláry λ, které neleží ve spektru zobrazení φ.

Tvrzení. *Pro lineární zobrazení φ $V \to V$ platí*

(1) Pro každé $\lambda \in \mathbb{K}$ je $\mathcal{R}_\lambda \subset V$ vektorový podprostor.

(2) Pro každé $\lambda, \mu \in \mathbb{K}$ je $\mathcal{R}_\lambda$ invariantní vzhledem k lineárnímu zobrazení $(\varphi - \mu \cdot \mathrm{id}_V)$, zejména tedy je $\mathcal{R}_\lambda$ invariantní vzhledem k φ.

(3) Je-li $\mu \neq \lambda$, pak $(\varphi - \mu \cdot \mathrm{id}_V)|_{\mathcal{R}_\lambda}$ je invertibilní.

(4) Zobrazení $(\varphi - \lambda \cdot \mathrm{id}_V)|_{\mathcal{R}_\lambda}$ je nilpotentní.

Důkaz. (1) Ověření vlastností vektorového podprostoru je jednoduché a ponecháváme jej čtenáři.

(2) Předpokládejme, že $(\varphi - \lambda \cdot \mathrm{id}_V)^k(u) = 0$ a uvažme $v = (\varphi - \mu \cdot \mathrm{id}_V)(u)$. Pak

$$\begin{aligned}(\varphi - \lambda \cdot \mathrm{id}_V)^k(v) &= \\ &= (\varphi - \lambda \cdot \mathrm{id}_V)^k((\varphi - \lambda \cdot \mathrm{id}_V) + (\lambda - \mu) \cdot \mathrm{id}_V)(u) \\ &= (\varphi - \lambda \cdot \mathrm{id}_V)^{k+1}(u) + (\lambda - \mu) \cdot (\varphi - \lambda \cdot \mathrm{id}_V)^k(u) \\ &= 0\end{aligned}$$

(3) Je-li $u \in \mathrm{Ker}(\varphi - \mu \cdot \mathrm{id}_V)|_{\mathcal{R}_\lambda}$, pak

$$(\varphi - \lambda \cdot \mathrm{id}_V)(u) = (\varphi - \mu \cdot \mathrm{id}_V)(u) + (\mu - \lambda) \cdot u = (\mu - \lambda) \cdot u$$

Odtud $0 = (\varphi - \lambda \cdot \mathrm{id}_V)^k(u) = (\mu - \lambda)^k \cdot u$ a je tedy nutně $u = 0$ pro $\lambda \neq \mu$.

(4) Zvolme bázi $e_1, \dots, e_p$ podprostoru $\mathcal{R}_\lambda$. Protože podle definice existují čísla k_i taková, že $(\varphi - \lambda \cdot \mathrm{id}_V)^{k_i}(e_i) = 0$, je nutně celé zobrazení $(\varphi - \lambda \cdot \mathrm{id}_V)|_{\mathcal{R}_\lambda}$ nilpotentní. □

3.37a **3.30. Faktorové prostory.** Našim dalším cílem je ukázat, že dimenze kořenových prostorů je vždy rovna algebraické násobnosti příslušných vlastních čísel. Nejprve však zavedeme šikovné technické nástroje.

Definice. Nechť $U \subset V$ je vektorový podprostor. Na množině všech vektorů ve V definujeme ekvivalenci takto: $v_1 \sim v_2$ právě tehdy, když $v_1 - v_2 \in U$. Axiomy ekvivalence jdou ověřit snadno. Množina V/U tříd této ekvivalence, spolu s operacemi definovanými pomocí reprezentantů, tj. $[v] + [w] = [v + w]$, $a \cdot [u] = [a \cdot u]$, tvoří vektorový prostor, který nazýváme *faktorový vektorový prostor* prostoru V podle podprostoru U. Ověřte si korektnost definice operací a platnost všech axiomů vektorového prostoru!

Třídy (vektory) ve faktorovém prostoru V/U budeme často označovat jako formální součet jednoho reprezentanta se všemi vektory podprostoru U, např. $u + U \in V/U$, $u \in V$. Nulový vektor ve V/U je právě třída $0 + U$, tj. vektor $u \in V$ reprezentuje nulový vektor ve V/U právě, když je $u \in U$.

Jako jednoduché příklady si rozmyslete $V/\{0\} \cong V$, $V/V \cong \{0\}$ a faktorový prostor roviny $\mathbb{R}^2$ podle libovolného jednorozměrného podprostoru, kde každý jednorozměrný podprostor $U \subset \mathbb{R}^2$ je přímka procházející počátkem, třídy ekvivalence jsou rovnoběžky s touto přímkou.

Tvrzení. *Nechť $U \subset V$ je vektorový podprostor a $u_1, \dots, u_n$ je taková báze V, že $u_1, \dots, u_k$ je báze U. Pak* $\dim V/U = n - k$ *a* $u_{k+1} + U, \dots, u_n + U$ *je báze* V/U.

DŮKAZ. Protože $V = \langle u_1, \dots, dotsun\rangle$, je i $V/U = \langle u_1 + U, \dots, u_n + U\rangle$. Přitom ale je prvních k generátorů nulových, takže je $V/U = \langle u_{k+1} + U, \dots, u_n + U\rangle$. Předpokládejme, že $a_{k+1} \cdot (u_{k+1} + U) + \dots + a_n \cdot (u_n + U) = (a_{k+1} \cdot u_{k+1} + \dots + a_n \cdot u_n) + U = 0 \in V/U$. To je ale ekvivalentní příslušnosti lineární kombinace vektorů $u_{k+1}, \dots, u_n$ do podprostoru U. Protože U je generováno zbylými vektory, je nutně tato kombinace nulová, tj. všechny koeficienty a_i jsou nulové. □

3.37b

3.31. Indukovaná zobrazení na faktorových prostorech. Předpokládejme, že $U \subset V$ je invariantní podprostor vzhledem k lineárnímu zobrazení $\varphi : V \to V$ a zvolme bázi $u_1, \dots, u_n$ prostoru V, že prvních k vektorů této báze je bazí U. V této bázi má φ polorozpadlou matici $A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$. Pak budeme umět dokázat následující tvrzení:

Lemma. *(1) Zobrazení φ indukuje lineární zobrazení $\varphi_{V/U} : V/U \to V/U$, $\varphi_{V/U}(v + U) = \varphi(v) + U$ s maticí D v indukované bázi $u_{k+1} + U, \dots, u_n + U$ na V/U.*
(2) Charakteristický polynom $\varphi_{V/U}$ dělí charakteristický polynom φ.

DŮKAZ. Pro $v, w \in V$, $u \in U$, $a \in \mathbb{K}$ máme $\varphi(v + u) \in \varphi(v) + U$ (protože U je invariantní), $(\varphi(v) + U) + (\varphi(w) + U) = \varphi(v + w) + U$ a $a \cdot (\varphi(v) + U) = a \cdot \varphi(v) + U = \varphi(a \cdot v) + U$ (protože φ je lineární), je tedy zobrazení $\varphi_{V/U}$ dobře definované a lineární. Navíc je přímo z definice matice zobrazení patrné, že matice $\varphi_{V/U}$ v indukované bázi na V/U je právě matice D (při počítání obrazů bázových prvků nám koeficienty z matice C přispívají pouze do třídy U). Charakteristický polynom indukovaného zobrazení $\varphi_{V/U}$ je tedy $|D - \lambda \cdot E|$, zatímco charakteristický polynom původního zobrazení φ je $|A - \lambda \cdot E| = |B - \lambda \cdot E||D - \lambda \cdot E|$. □

Důsledek. *Nechť V je vektorový prostor nad $\mathbb{K}$ dimenze n a nechť $\varphi : V \to V$ je lineární zobrazení, jehož spektrum obsahuje n prvků (tj. všechny kořeny charakteristického polynomu leží v $\mathbb{K}$ a počítáme je včetně násobnosti). Pak existuje posloupnost invariantních podprostorů $\{0\} = V_0 \subset V_1 \subset \dots \subset V_n = V$ s dimenzemi* $\dim V_i = i$. *V bázi $u_1, \dots, u_n$ prostoru V takové, že $V_i = \langle u_1, \dots, u_i\rangle$, má φ horní trojúhelníkovou matici:*

$$\begin{pmatrix} \lambda_1 & \dots & * \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{pmatrix},$$

kde $\lambda_1, \dots, \lambda_n$ je posloupnost prvků spektra.

DŮKAZ. Konstrukci podprostorů V_i provedeme induktivně. Nechť $\lambda_1, \dots, \lambda_n$ jsou prvky ve spektru zobrazení φ, tzn. charakteristický polynom zobrazení φ je tvaru $(\lambda -$

$\lambda_1) \cdot \dots \cdot (\lambda - \lambda_n)$. Zvolme $V_0 = \{0\}$, $V_1 = \langle u_1 \rangle$, kde u_1 je libovolný vlastní vektor s vlastní hodnotou λ_1. Podle předešlé věty je charakteristický polynom zobrazení φ_{V/V_1} tvaru $(\lambda - \lambda_2) \cdot \dots \cdot (\lambda - \lambda_n)$. Předpokládejme, že jsme již sestrojili lineárně nezávislé vektory $u_1, \dots, u_k$ a invariantní podprostory $V_i = \langle u_1 \dots, u_i \rangle$, $i = 1, \dots, k < n$, takové, že charakteristický polynom φ_{V/V_k} je tvaru $(\lambda - \lambda_{k+1}) \cdot \dots \cdot (\lambda - \lambda_n)$ a $\varphi(u_i) \in (\lambda_i \cdot u_i + V_{i-1})$ pro všechna $i = 1, \dots, k$.

Zejména tedy existuje vlastní vektor $u_{k+1} + V_k \in V/V_k$ zobrazení φ_{V/V_k} s vlastní hodnotou λ_{k+1}. Uvažme nyní prostor $V_{k+1} = \langle u_1, \dots, u_{k+1} \rangle$. Kdyby byl vektor u_{k+1} lineární kombinací vektorů $u_1, \dots, u_k$, znamenalo by to, že $u_{k+1} + V_k$ je nulová třída v V/V_k, to ale není možné. Je proto $\dim V_{k+1} = k + 1$. Zbývá studovat indukované zobrazení $\varphi_{V/V_{k+1}}$. Charakteristický polynom tohoto zobrazení je stupně $n - k - 1$ a dělí charakteristický polynom zobrazení φ. Přitom doplněním vektorů $u_1, \dots, u_{k+1}$ do báze V dostaneme polorozpadlou matici zobrazení φ s horní trojúhelníkovou submaticí B v horním levém rohu, jejíž diagonální prvky jsou právě skaláry $\lambda_1, \dots, u_{k+1}$. Proto mají kořeny charakteristického polynomu indukovaného zobrazení požadované vlastnosti. $\square$

3.37c

3.32. Poznámky. Pokud existuje rozklad celého prostoru V na přímý součet vlastních podprostorů, existuje báze z vlastních podprostorů a předchozí věta vlastně neříká vůbec nic zajímavého. Její síla ovšem spočívá v tom, že jediným jejím předpokladem je existence $\dim V$ kořenů charakteristického polynomu (včetně násobností). To je ovšem zaručeno, je-li pole $\mathbb{K}$ algebraicky uzavřené, např. pro komplexní čísla $\mathbb{C}$. Přímým důsledkem pak jsou zajímavá tvrzení o determinantu a stopě zobrazení: jsou vždy součinem, resp. součtem prvků ve spektru. Tuto skutečnost můžeme použít i pro všechny reálné matice. Můžeme je totiž vždy považovat za komplexní, spočítat potřebné, a protože determinant i stopa jsou algebraické výrazy v prvcích matice, výsledkem budou právě hledané reálné hodnoty.

Když je na vektorovém prostoru V zadán skalární součin, můžeme v každém induktivním kroku důkazu předchozího tvrzení využít skutečnosti, že vždy $V/V_k \simeq V_k^\perp$ a $V_k^\perp \ni u \mapsto (u + V_k) \in V/V_k$. To znamená, že v každé třídě rozkladu V/V_k existuje právě jeden vektor z $V_k^\perp$. Skutečně, tuto vlastnost má faktorový prostor podle libovolného podprostoru v unitárním prostoru – pokud $u, v \in V_k^\perp$ jsou v jedné třídě, pak jejich rozdíl patří do $V_k \cap V_k^\perp$, tedy jsou stejné. Můžeme tedy jako reprezentanta u_{k+1} nalezené třídy, tedy vlastního vektoru φ_{V/V_k}, zvolit právě vektor z $V_k^\perp$. Touto modifikací dojdeme k ortogonální bázi s vlastnostmi požadovanými v tvrzení o triangulovatelnosti. Proto existuje i taková ortonormální báze:

Důsledek (Schurova věta o ortogonální triangulovatelnosti)**.** *Nechť $\varphi : V \to V$ je libovolné lineární zobrazení (reálného nebo komplexního) unitárního prostoru s $m = \dim V$ vlastními hodnotami (včetně násobonosti). Pak existuje ortonormální báze prostoru V taková, že φ v ní má horní trojúhelníkovou matici s vlastními čísly $\lambda_1, \dots, \lambda_m$ na diagonále.*

3.37d **3.33. Věta.** *Nechť φ $V \to V$ je lineární zobrazení. Součet kořenových prostorů*

$$\mathcal{R}_{\lambda_1}, \dots, \mathcal{R}_{\lambda_k}$$

příslušných různým vlastním hodnotám $\lambda 1' \dots, \lambda_k$ je přímý. Navíc je pro každou vlastní hodnotu λ dimenze podprostoru $\mathcal{R}_\lambda$ rovna její algebraické násobnosti.

Důkaz. Důkaz provedeme indukcí přes počet k kořenových prostorů. Předpokládejme, že tvrzení vždy platí pro méně než k prostorů a že pro vektory $u_1 \in \mathcal{R}_{\lambda_1}, \dots, u_k \in \mathcal{R}_{\lambda_k}$ platí $u_1 + \dots + u_k = 0$. Pro vhodné j pak $(\varphi - \lambda_k \cdot \mathrm{id}_V)^j(u_k) = 0$ a zároveň jsou $y_i = (\varphi - \lambda_k \cdot \mathrm{id}_V)^j(u_i)$ nenulové vektory v $\mathcal{R}_{\lambda_i}$, $i = 1, \dots, k-1$, pokud u_i jsou nenulové, viz. předchozí věta. Přitom ale

$$y_1 + \dots + y_{k-1} = \sum_{i=1}^{k} (\varphi - \lambda_k \cdot \mathrm{id}_V)^j(u_i) = 0$$

a tedy podle indukčního předpokladu jsou všechny y_i nulové. Pak ovšem i $u_k = 0$ a lineární nezávislost je dokázána.

Zbývá ukázat, že dimenze každého kořenového prostoru $\mathcal{R}_\lambda$ je rovna algebraické násobnosti kořenu λ charakteristického polynomu. Nechť tedy je λ vlastní hodnota φ, označme $\bar{\varphi}$ zúžení $\varphi|_{\mathcal{R}_\lambda}$ a ψ $V/\mathcal{R}_\lambda \to V/\mathcal{R}_\lambda$ nechť je zobrazení indukované φ na faktorovém prostoru. Předpokládejme, že dimenze $\mathcal{R}_\lambda$ je menší než násobnost kořenu λ charakteristického polynomu. Podle věty **??** to znamená, že λ je i vlastní hodnotou zobrazení ψ. Nechť $(v + \mathcal{R}_\lambda) \in V/\mathcal{R}_\lambda$ je příslušný vlastní vektor, tj. $\psi(v + \mathcal{R}_\lambda) = \lambda \cdot (v + \mathcal{R}_\lambda)$ což podle definice značí $v \notin \mathcal{R}_\lambda$ a $\varphi(v) = \lambda \cdot v + w$ pro vhodné $w \in \mathcal{R}_\lambda$. Máme tedy $w = (\varphi - \lambda \cdot \mathrm{id}_V)(v)$ a $(\varphi - \lambda \cdot \mathrm{id}_V)^j(w) = 0$ pro vhodné j. Celkem tedy $(\varphi - \lambda \cdot \mathrm{id}_V)^{j+1}(v) = 0$ což je ve sporu s volbou $v \notin \mathcal{R}_\lambda$. Tím jsme dokázali, že dimenze $\mathcal{R}_\lambda$ je rovna násobnosti kořene λ charakteristického polynomu φ. □

Důsledek. *Pro každé lineární zobrazení $\varphi : V \to V$, jehož celé spektrum je v $\mathbb{K}$, je $V = \mathcal{R}_{\lambda_1} \oplus \dots \oplus \mathcal{R}_{\lambda_n}$ přímým součtem kořenových podprostorů. Zvolíme-li vhodně báze těchto podprostorů, pak φ má v této bázi blokově diagonální tvar s horními trojúhelníkovými maticemi v blocích a vlastními hodnotami λ_i na diagonále.*

3.38 **3.34. Nilpotentní a cyklická zobrazení.** Nyní již máme skoro vše připraveno pro diskusi kanonických tvarů matic. Zbývá jen vyjasnit vztah mezi cyklickými a nilpotentními zobrazeními a poskládat dohromady již připravené výsledky.

Věta. *Nechť φ $V \to V$ je nilpotentní lineární zobrazení. Pak existuje rozklad V na přímý součet podprostorů $V = V_1 \oplus \dots \oplus V_k$ takových, že zúžení φ na kterýkoliv z nich je cyklické.*

Důkaz. Ověření je docela jednoduché a spočívá v konstrukci takové báze prostoru V, že akce zobrazení φ na bázových vektorech přímo ukazuje rozklad na cyklická zobrazení. Postup bude ale poněkud zdlouhavý.

Nechť k je stupeň nilpotentnosti zobrazení φ a označme $P_i = \operatorname{im}(\varphi^i)$, $i = 0, \dots, k$, tzn.

$$\{0\} = P_k \subset P_{k-1} \subset \cdots \subset P_1 \subset P_0 = V.$$

Vyberme libovolnou bázi $e_1^{k-1}, \dots, e_{p_{k-1}}^{k-1}$ prostoru P_{k-1}, kde $p_{k-1} > 0$ je dimenze P_{k-1}. Z definice plyne, že $P_{k-1} \subset \operatorname{Ker}\varphi$, tj. vždy $\varphi(e_j^{k-1}) = 0$.

Předpokládejme, že $P_{k-1} \neq V$. Protože $P_{k-1} = \varphi(P_{k-2})$, nutně existují v P_{k-2} vektory e_j^{k-2}, $j = 1, \dots, p_{k-1}$, takové, že $\varphi(e_j^{k-2}) = e_j^{k-1}$. Předpokládejme

$$a_1 e_1^{k-1} + \cdots + a_{p_{k-1}} e_{p_{k-1}}^{k-1} + b_1 e_1^{k-2} + \cdots + b_{p_{k-1}} e_{p_{k-1}}^{k-2} = 0.$$

Aplikací zobrazení φ na tuto lineární kombinaci získáme $b_1 e_1^{k-1} + \cdots + b_{p_{k-1}} e_{p_{k-1}}^{k-1} = 0$, proto jsou všechny $b_j = 0$. Pak ale i $a_j = 0$, protože se jedná o kombinaci bázových vektorů. Celkem jsme tedy ověřili lineární nezávislost všech $2p_{k-1}$ zvolených vektorů. Doplňme je do báze

$$\begin{array}{l} e_1^{k-1}, \dots, e_{p_{k-1}}^{k-1} \\ e_1^{k-2}, \dots, e_{p_{k-1}}^{k-2}, e_{p_{k-1}+1}^{k-2}, \dots, e_{p_{k-2}}^{k-2} \end{array}$$

prostoru P_{k-2}. Navíc jsou obrazy přidaných bázových prvků v P_{k-1}, nutně tedy musejí být lineárními kombinacemi bázových prvků $e_1^{k-1}, \dots, e_{p_{k-1}}^{k-1}$. Můžeme proto zaměnit zvolené vektory $e_{p_{k-1}+1}^{k-2}, \dots, e_{p_{k-2}}^{k-2}$ vektory $e_j^{k-2} - \varphi(e_j^{k-2})$. Tím docílíme, že doplněné vektory do báze P_{k-2} patří do jádra zobrazení φ. Předpokládejme to přímo o zvolené bázi (1).

Předpokládejme dále, že již máme sestrojenu bázi podprostoru $P_{k-\ell}$ takovou, že ji můžeme poskládat do schématu

$$\begin{array}{l} e_1^{k-1}, \dots, e_{p_{k-1}}^{k-1} \\ e_1^{k-2}, \dots, e_{p_{k-1}}^{k-2}, e_{p_{k-1}+1}^{k-2}, \dots, e_{p_{k-2}}^{k-2} \\ e_1^{k-3}, \dots, e_{p_{k-1}}^{k-3}, e_{p_{k-1}+1}^{k-3}, \dots, e_{p_{k-2}}^{k-3}, e_{p_{k-2}+1}^{k-3}, \dots, e_{p_{k-3}}^{k-3} \\ \vdots \\ e_1^{k-\ell}, \dots, e_{p_{k-1}}^{k-\ell}, e_{p_{k-1}+1}^{k-\ell}, \dots, e_{p_{k-2}}^{k-\ell}, e_{p_{k-2}+1}^{k-\ell}, \dots, e_{p_{k-3}}^{k-\ell}, \dots e_{p_{k-\ell}}^{k-\ell} \end{array}$$

kde hodnota zobrazení φ na libovolném bázovém vektoru se nachází nad ním, nebo je nulová, pokud nad zvoleným vektorem báze již nic není. Pokud je $P_{k-\ell} \neq V$, opět musí existovat vektory $e_1^{k-\ell-1}, \dots, e_{p_{k-\ell}}^{k-\ell-1}$, které se zobrazují na $e_1^{k-\ell}, \dots, e_{p_{k-\ell}}^{k-\ell}$ a můžeme je doplnit do báze P_{k-l-1}, řekněme vektory

$$e_{p_{k-\ell}+1}^{k-\ell-1}, \dots, e_{p_{k-\ell-1}}^{k-\ell-1}.$$

Přitom postupným odečítáním hodnot iterací zobrazení φ na těchto vektorech dosáhneme opět toho, že doplněné vektory do báze $P_{k-\ell-1}$ budou ležet v jádru φ a analogicky jako výše ověříme, že skutečně dostaneme bázi $P_{k-\ell-1}$.

Po k krocích získáme bázi celého V, která má vlastnosti uvedené pro bázi (2) prostoru $P_{k-\ell}$. Jednotlivé sloupce výsledného schématu pak generují hledané podprostory V_i a navíc jsme přímo našli báze těchto podprostorů ukazující, že příslušná zúžení φ jsou cyklická zobrazení. □

3.35. Důkaz Jordanovy věty. Nechť $\lambda_1, \dots, \lambda_k$ jsou všechny různé vlastní hodnoty zobrazení φ. Z předpokladů Jordanovy věty plyne, že $V = \mathcal{R}_{\lambda_1} \oplus \cdots \oplus \mathcal{R}_{\lambda_k}$. Zobrazení $\varphi_i = (\varphi|_{\mathcal{R}_{\lambda_i}} - \lambda_i \cdot \mathrm{id}_{\mathcal{R}_{\lambda_i}})$ jsou nilpotentní a proto je každý z kořenových prostorů přímým součtem

$$\mathcal{R}_{\lambda_i} = P_{1,\lambda_i} \oplus \cdots \oplus P_{j_i,\lambda_i}$$

prostorů na nichž je zúžení zobrazení $\varphi - \lambda_i \cdot \mathrm{id}_V$ cyklické. Matice těchto zúžených zobrazení na $P_{r,s}$ jsou Jordanovy bloky příslušné k nulové vlastní hodnotě, zúžené zobrazení $\varphi|_{P_{r,s}}$ má proto za matici Jordanův blok s vlastní hodnotou λ_i.

Pro důkaz Jordanovy věty zbývá dokázat tvrzení o jednoznačnosti. Protože diagonální hodnoty λ_i jsou dány jako kořeny charakteristického polynomu, je jejich jednoznačnost zřejmá. Vyjádříme rozměry jednotlivých Jordanových bloků prostřednictvím hodností $r_k(\lambda_i)$ zobrazení $(\varphi - \lambda_i \cdot \mathrm{id}_V)^k$. Tím bude jasné, že až na pořadí jsou bloky jednoznačně určeny. Naopak, přehození bloků odpovídá přečíslování vektorů báze, lze je tedy získat v libovolném pořadí.

Je-li ψ cyklický operátor na n-rozměrném prostoru, pak defekt iterovaného zobrazení ψ^k je k pro $0 \le k \le n$ a je n pro všechna $k \ge n$. Odtud plyne, že pokud matice J zobrazení φ obsahuje $d_k(\lambda)$ Jordanových bloků řádu k s vlastní hodnotou λ, pak defekt matice $(J - \lambda \cdot E)^\ell$ je

$$d_1(\lambda) + 2d_2(\lambda) + \dots \ell d_\ell(\lambda) + \ell d_{\ell+1}(\lambda) + \dots$$

Odtud spočítáme

$$n - r_\ell(\lambda) = d_1(\lambda) + 2d_2(\lambda) + \cdots + \ell d_\ell(\lambda) + \ell d_{\ell+1}(\lambda) + \dots$$
$$d_k(\lambda) = r_{k-1}(\lambda) - 2r_k(\lambda) + r_{k+1}(\lambda)$$

(kde poslední řádek vznikne kombinací předchozího pro hodnoty $\ell = k-1, k, k+1$).

3.36. Poznámka. Důkaz věty o existenci Jordanova kanonického tvaru byl sice konstruktivní, nedává nám ale dokonale efektivní algoritmický postup pro jejich hledání. Nyní shrneme již odvozený postup explicitního výpočtu báze, v níž má dané zobrazení $\varphi\ V \to V$ matici v kanonickém Jordanově tvaru.

(1) Najdeme kořeny charakteristického polynomu.
(2) Jestliže jich je méně než $n = \dim V$, včetně násobností, kanonický tvar neexistuje.
(3) Je-li n lineárně nezávislých vlastních vektorů, získáme bázi V z vlastních vektorů a v ní má φ diagonální matici.
(4) Nechť λ je vlastní hodnota s geometrickou násobností menší než algebraickou a $v_1, \dots, v_k$ nechť jsou příslušné vlastní vektory. To by měly být vektory na horním okraji schématu z důkazu věty 3.34, je ovšem nutné najít vhodnou bázi aplikacemi iterací $\varphi - \lambda \cdot \mathrm{id}_V$. Zároveň přitom zjistíme ve kterém řádku se vektory nacházejí a najdeme lineárně nezávislá řešení w_i rovnic $(\varphi - \lambda\,\mathrm{id})(x) = v_i$ z řádků pod nimi. Postup opakujeme iterativně (tj. pro w_i atd.). Najdeme tak „řetízky" bázových vektorů zadávajících podprostory, kde $\varphi - \lambda\,\mathrm{id}$ je cyklické.

Postup je praktický pro matice, kde násobnosti vlastních hodnot jsou malé, nebo aspoň diskutované stupně nilpotentnosti jsou malé. Např. pro matici

$$A = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

dostaneme dvourozměrný podprostor vlastních vektorů

$$\langle (1,0,0), (0,1,0) \rangle.$$

Potřebujeme proto najít řešení rovnic $(A-2E)x = (a,b,0)^T$ pro vhodné konstanty a, b. Tento systém je ovšem řešitelný pouze pro $a = b$ a jedno z možných řešení je $v = (0,0,1)$, $a = b = 1$. Celá hledaná báze pak je $(1,1,0)$, $(0,0,1)$, $(1,0,0)$. Všimněme si, že jsme měli spoustu voleb a bazí s požadovanými vlastnostmi je tedy mnoho.

5. Rozklady matic a pseudoinverze

V minulé části jsme s soustředili na geometrický popis struktury zobrazení. Teď naše výsledky přeložíme do jazyku tzv. rozkladů matic, což je obzvlášť důležité téma pro numerické postupy a maticový počet obecně.

I při počítání s reálnými čísly užíváme pro zjednodušení rozklady na součiny. Nejjednodušším je vyjádření každého reálného čísla jednoznačně ve tvaru

$$a = \operatorname{sgn}(a) \cdot |a|,$$

tj. jako součin znaménka a abolutní hodnoty. V dalším textu si uvedeme stručně přehled několika takových rozkladů pro různé typy matic, které bývají nesmírně užitečné při numerických výpočtech s maticemi. Například jsme vhodný rozklad pro pozitivně semidefinitní symetrické matice využili v odstavci 3.27 pro konstrukci odmocniny z matice.

3.40 **3.37. LU–rozklad.** Začneme přeformulováním několika výsledků, které jsme už dávno odvodili. V odstavcích 2.7 a 2.8 jsme upravovali matice nad skaláry z libovolného pole na řádkový schodovitý tvar. K tomu jsme používali elementární úpravy, které spočívaly v postupném násobení naší matice invertibilními dolními trojúhelníkovými maticemi P_i, které postihovaly přičítání násobků řádků pod právě zpravovávaným. Předpokládejme pro jednoduchost, že naše matice A je čtvercová a že při Gausově eliminaci nejsme nuceni přehazovat řádky a proto všechny naše matice P_i mohou být dolní trojúhelníkové s jedničkami na diagonálách. Konečně, stačí si povšimnout, že inverzní matice k takovýmto P_i jsou opět dolní trojúhelníkové s jedničkami na diagonálách a dostáváme

$$U = P \cdot A = P_k \cdots P_1 \cdot A$$

kde U je horní trojúhelníková matice a tedy

$$A = L \cdot U$$

kde L je dolní trojúhelníková matice s jedničkami na diagonále a U je horní trojúhelníková. Tomuto rozkladu se říká *LU–rozklad* matice A.

V případě obecné matice můžeme při Gausově eliminaci na řádkově schodovitý tvar potřebovat navíc permutace řádků, někdy i sloupců matice. Pak dostáváme obecněji $A = P \cdot L \cdot U \cdot Q$, kde P a Q jsou nějaké permutační matice.

3.41

3.38. Poznámky. Přímým důsledkem Gausovy eliminace bylo také zjištění, že až na volbu vhodných bází na definičním oboru a oboru hodnot je každé zobrazení $f : V \to W$ zadáno maticí v blokově diagonálním tvaru s jednotkovou maticí, s rozměrem daným dimenzí obrazu f, a s nulovými bloky všude kolem. To lze přeformulovat takto: Každou matici A typu m/n nad polem skalárů $\mathbb{K}$ lze rozložit na součin

$$A = P \cdot \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix} \cdot Q,$$

kde P a Q jsou vhodné invertibilní matice.

Pro čtvercové matice jsme v 3.28 ukázali při diskusi vlastností lineárních zobrazení $f : V \to V$ na komplexních vektorových prostorech, že každou čtvercovou matici A dimenze m umíme rozložit na součin

$$A = P \cdot B \cdot P^{-1}$$

kde B je blokově diagonální s Jordanovými bloky příslušnými k vlastním číslům na diagonále. Skutečně jde o pouhé přepsání Jordanovy věty, protože násobení maticí P a její inverzí z opačných stran odpovídá v tomto případě právě změně báze na vektorovém prostoru V a citovaná věta říká, že ve vhodné bázi má každé zobrazení Jordanův kanonický tvar.

Obdodně jsme tedy při diskusi samoadjungovaných zobrazení dokázali, že pro reálné symetrické nebo komplexní Hermiteovské matice existuje vždy rozklad na součin

$$A = P \cdot B \cdot P^*,$$

kde B je diagonální matice se všemi (vždy reálnými) vlastními čísly na diagonále, včetně násobností. Skutečně, jde opět o součin s maticemi vystihující změnu báze, nicméně připouštíme nyní pouze změny mezi mezi ortonormálními bazemi a proto i matice přechodu P musí být ortogonální. Odtud $P^{-1} = P^*$.

Pro reálná ortogonální zobrazení jsme odvodili obdobné vyjádření jako u symetrických, pouze naše B bude blokově diagonální s bloky rozměru dva nebo jedna vyjadřujícími buď rotaci nebo zrcadlení nebo identitu vzhledem k příslušným podprostorům.

3.42

3.39. Věta o singulárním rozkladu. Nyní se vrátíme k obecným lineárním zobrazením mezi (obecně různými) vektorovými prostory. Jestliže na nich je definován skalární součin a omezíme se přitom na ortonormální báze, musíme postupovat o hodně rafinovaněji, než v případě bazí libovolných :

Věta. *Nechť A je libovolná matice typu m/n nad reálnými nebo komplexními skaláry. Pak existují čtvercové unitární* *matice U a V dimenzí m a n, a reálná diagonální matice s nezápornými prvky D dimenze r, $r \leq \min\{m,n\}$, takové, že*

$$A = USV^*, \quad S = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

a r je hodnost matice AA^*. Přitom je S určena jednoznačně až na pořadí prvků a prvky diagonální matice D jsou druhé odmocniny vlastních čísel d_i matice AA^*. Pokud je A reálná matice, pak i matice U a V jsou ortogonální.

Důkaz. Předpokládejme nejprve $m \leq n$ a označme $\varphi : \mathbb{K}^n \to \mathbb{K}^m$ zobrazení mezi reálnými nebo komplexními prostory se standardními skalárními součiny, zadané maticí A ve standardních bazích.

Tvrzení věty můžeme přeformulovat tak, že existují ortonormální báze na $\mathbb{K}^n$ a $\mathbb{K}^m$ ve kterých bude mít φ matici S z tvrzení věty.

Jak jsme viděli dříve, matice A^*A je pozitivně semidefinitní. Proto má samá reálná nezáporná vlastní čísla a existuje ortonormální báze $\underline{w}$ v $\mathbb{K}^n$, ve které má příslušné zobrazení $\varphi^* \circ \varphi$ diagonální matici s vlastními čísly na diagonále. Jinými slovy, existuje unitární matice V taková, že $A^*A = VBV^*$ pro reálnou diagonální matici s nezápornými vlastními čísly $(d_1, d_2, \dots, d_r, 0, \dots, 0)$ na diagonále, $d_i \neq 0$ pro vąechny $i = 1, \dots, r$. Odtud

$$B = V^*A^*AV = (AV)^*(AV).$$

To je ale je ekvivalentní tvrzení, že prvních r sloupců matice AV je ortogonálních a zbývající jsou nulové, protože mají nulovou velikost.

Označme nyní prvních r sloupců $v_1, \dots, v_r \in \mathbb{R}^m$. Platí tedy $\langle v_i, v_i \rangle = d_i$, $i = 1, \dots, r$ a normované vektory $u_i = \frac{1}{\sqrt{d_i}} v_i$ tvoří ortonormální systém nenulových vektorů. Doplňme je na ortonormální bázi $\underline{u} = u_1, \dots, u_n$ celého $\mathbb{K}^m$. Vyjádříme-li naše původní zobrazení zobrazení φ v bazích $\underline{w}$ na $\mathbb{K}^n$ a $\underline{u}$ na $\mathbb{K}^m$, dostáváme matici $\sqrt{B}$. Přechody od standardních bází k nově vybraným odpovídají násobení zleva ortogonálními maticemi U a zprava $V^{-1} = V^*$.

Pokud je $m > n$, můžeme aplikovat předchozí část důkazu na matici A^*. Odtud pak přímo plyne požadované tvrzení.

Pokud pracujeme nad reálnými skaláry, jsou všechny naše kroky v důkazu výše také realizovány v reálném oboru. □

Tento důkaz věty o singulárním rozkladu je konstruktivní a můžeme jej opravdu použít pro výpočet unitárních, resp. ortogonálních, matic U, V a diagonálních nenulových prvků
3.43 matice S.

3.40. Geometrická interpretace singulárního rozkladu. Diagonálním hodnotám matice D z předchozí věty se říká *singulární hodnoty matice A*. Přeformulujme si tuto větu v reálném případě geometričtěji.

Pro příslušné lineární zobrazení $\varphi : \mathbb{R}^n \to \mathbb{R}^m$ mají singulární hodnoty skutečně jednoduchý geometrický význam: Nechť $K \subset \mathbb{R}^n$ je jednotková sféra pro standardní skalární součin. Obrazem $\varphi(K)$ pak vždy bude (případně degenerovaný) m-rozměrný elipsoid. Singulární čísla matice A jsou přitom velikosti hlavních poloos a věta navíc říká, že původní sféra vždy připouští ortogonální sdružené průměry, jejichž obrazem budou právě všechny poloosy tohoto elipsoidu.

Pro čtvercové matice je vidět, že A je invertibilní právě, když všechna singulární čísla jsou nenulová. Poměr největšího a nejmenšího singulárního čísla je důležitým parametrem pro robustnost řady numerických výpočtů s maticemi, např. pro výpočet inverzní matice. Poznamejme také, že existují rychlé metody výpočtů, resp. odhadů, vlastních čísel, proto je se singulárním rozkladem velmi efektivně pracovat.

3.44

3.41. Věta o polárním rozkladu. Věta o singulárním rozkladu je východiskem pro mnoho mimořádně užitečných nástrojů. Uvažujme nyní nad několika přímými důsledky (které samy o sobě jsou dosti netriviální). Tvrzení věty říká pro libovolnou matici A, ať už reálnou nebo komplexní, $A = USW^*$ s diagonální S s nezápornými reálnými čísly na diagonále a unitárními U, W. Pak ovšem také $A = USU^*UW^*$ a pojmenujme si matice $P = USU^*$, $V = UW^*$. První z nich, P je hermiteovská (v reálném případě symetrická) a pozitivně semidefinitní, protože jde jen o zápis zobrazení s reálnou diagonální maticí S v jiné ortonormální bázi, zatímco V je coby součin dvou unitárních opět unitární (v reálném případě ortogonální). Navíc $A^* = WSU^*$ a tedy $AA^* = USSU^* = P^2$ a naše matice P je vlastně odmocninou ze snadno spočítatelné hermiteovské matice AA^*.

Předpokládejme, že $A = PV = QU$ jsou dva takové rozklady matice A na součin positivně semidefinitní hermiteovské a unitární matice a předpokládejme, že A je invertibilní. Pak ovšem je $AA^* = PVV^*P = P^2 = QUU^*Q = Q^2$ pozitivně definitní a proto jsou matice $Q = P = \sqrt{AA^*}$ jednoznačně určené a invertibilní. Pak ovšem také $U = V = P^{-1}A$.

Beze zbytku jsme tedy odvodili velice užitečnou analogii rozkladu reálného čísla na znaménko (ortogonální matice v případě dimenze jedna jsou právě ± 1) a absolutní hodnotu (matice P, ke které umíme odmocninu).

Věta (Věta o polárním rozkladu)**.** *Každou čtvercovou komplexní matici A dimenze n lze vždy vyjádřit ve tvaru $A = P \cdot V$, kde P je hermiteovská a positivně definitní čtvercová matice téže dimenze a V je unitární. Přitom $P = \sqrt{AA^*}$. Je-li A invertibilní, je rozklad jednoznačný a $V = (\sqrt{AA^*})^{-1}A$.*

Pokud pracujeme nad reálnými skaláry, je P symetrická a V ortogonální.

Když budeme tutéž větu aplikovat na A^* místo A, dostaneme tentýž výsledek, ovšem s obráceným pořadím hermiteovských a unitárních matic. Matice v příslušných pravých a levých rozkladech budou samozřejmě obecně různé.

V komplexním případě je analogie s rozkladem čísel ještě zábavnější — pozitivně semidefinitní P hraje opět roli absolutní hodnoty komplexního čísla, unitární matice V pak má jednoznačné vyjádření jako součet $V = V_r + i\,V_i$ s hermiteovkými V_r a V_i s vlastností $V_r^2 + V_i^2 = E$, tj. dostáváme plnou analogii goniometrického tvaru komplexních čísel (viz závěrečná poznámka v 3.26). Všimněme si ale, že ve vícerozměrném případě je podstané, v jakém pořadí tento „goniometrický tvar" matice píšeme. Jde to oběma způsoby, vysledky jsou ale obecně různé.

Pro řadu praktických aplikací bývá rychlejší použití tzv. *QR rozkladu* matic, který je obdobou Schurovy věty o ortogonální triangulaci:

3.45 **3.42. Věta.** *Pro každou komplexní matici A typu m/n existuje unitární matice Q a horní trojúhelníková matice R takové, že $A = Q^T R$.*

Pokud pracujeme nad reálnými skaláry, jsou Q i R reálné.

Důkaz. V geometrické formulaci potřebujeme dokázat, že pro každé zobrazení $\varphi : \mathbb{K}^n \to \mathbb{K}^m$ s maticí A ve standardních bazích můžeme zvolit novou ortonormální bázi na $\mathbb{K}^m$ tak, aby potom φ mělo horní trojúhelníkovou matici.

Uvažme obrazy $\varphi(e_1), \dots, \varphi(e_n) \in \mathbb{K}^m$ vektorů standardní ortonormální báze, vyberme z nich maximální lineárně nezávislý systém $v_1, \dots, v_k$ takovým způsobem, že vypouštěné závislé vektory jsou vždy lineární kombinací předchozích vektorů, a doplňme jej do báze $v_1, \dots, v_m$. Nechť $u_1, \dots, u_m$ je ortonormální báze $\mathbb{K}^m$ vzniklá Gramm-Schmidtovou ortogonalizací tohoto systému vektorů.

Nyní pro každé e_i je $\varphi(e_i)$ buď jedno z v_j, $j \le i$, nebo je lineární kombinací $v_1, \dots, v_{i-1}$, proto ve vyjádření $\varphi(e_i)$ v bázi $\underline{u}$ vystupují pouze vektory $u_1, \dots, u_i$. Zobrazení φ má proto ve standardní bázi na $\mathbb{K}^n$ a ortonormální bázi $\underline{u}$ na $\mathbb{K}^m$ horní trojúhelníkovou matici R. Přechod k bázi $\underline{u}$ na $\mathbb{R}^m$ odpovídá násobení ortogonální maticí Q zleva, tj. $R = QA$, ekvivalentně $A = Q^* R$. □

Závěrem této části textu si všimněme mimořádně užitečné a důležité aplikace našich výsledků pro přibližné numerické výpočty.

3.46 **3.43. Definice.** Nechť A je reálná matice typu m/n a nechť

$$A = USV^*, \quad S = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

je její singulární rozklad (zejména D je invertibilní). Matici

$$A^{(-1)} := VS'U^*, \quad S' = \begin{pmatrix} D^{-1} & 0 \\ 0 & 0 \end{pmatrix}$$

nazýváme *pseudoinverzní matice* k matici A.

Jak ukazuje následující věta, je pseudoinverze důležité zobecnění pojmu inverzní matice.

3.47 **3.44. Věta.** *Nechť A je reálná nebo komplexní matice typu m/n. Pak pro její pseudoinverzní matici platí:*

(1) Je-li A invertibilní (zejména tedy čtvercová), pak

$$A^{(-1)} = A^{-1}.$$

(2) *pro pseudoinverzi $A^{(-1)}$ platí, že $A^{(-1)}A$ i $AA^{(-1)}$ jsou hermiteovské (v reálném případě) symetrické a*

$$AA^{(-1)}A = A, \quad A^{(-1)}AA^{(-1)} = A^{(-1)}.$$

(3) *Je-li A matice systému lineárních rovnic $Ax = b$, s pravou stranou $b \in \mathbb{K}^m$, pak vektor $y = A^{(-1)}b \in \mathbb{K}^n$ minimalizuje velikost $\|Ax - b\|$ pro všechny vektory $x \in \mathbb{K}^n$.*

Důkaz. (1): Je-li A invertibilní, pak je matice $S = U^*AV$ také invertibilní a přímo z definice je $S' = S^{-1}$. Odtud vyplývá $A^{(-1)}A = AA^{(-1)} = E$.

(2): Přímým výpočtem dostáváme $SS'S = S$ a $S'SS' = S'$, proto

$$AA^{(-1)}A = USV^*VS'U^*USV^* = USS'SV^* = USV^* = A$$

a analogicky pro druhou rovnost. Dále

$$\begin{aligned}(AA^{(-1)})^* &= (USS'U^*)^* = U(S')^*S^*U^* \\ &= U(SS')^*U^* = USS'U^* = AA^{(-1)}\end{aligned}$$

a podobně se ukáže $(A^{(-1)}A)^* = A^{(-1)}A$.

(3): Uvažme zobrazení $\varphi : \mathbb{K}^n \to \mathbb{K}^m$, $x \mapsto Ax$, a přímé součty $\mathbb{K}^n = (\operatorname{Ker}\varphi)^\perp \oplus \operatorname{Ker}\varphi$, $\mathbb{K}^m = \operatorname{Im}\varphi \oplus (\operatorname{Im}\varphi)^\perp$. Zúžené zobrazení $\tilde{\varphi} := \varphi_{|(\operatorname{Ker}\varphi)^\perp} : (\operatorname{Ker}\varphi)^\perp \to \operatorname{Im}\varphi$ je lineární isomorfismus. Zvolíme-li vhodně ortonormální báze na $(\operatorname{Ker}\varphi)^\perp$ a $\operatorname{Im}\varphi$ a doplníme je na ortonormální báze na celých prostorech, bude mít φ matici S a $\tilde{\varphi}$ matici D z věty o singulárním rozkladu. Pro dané $b \in \mathbb{K}^m$ je bod $z \in \operatorname{Im}\varphi$ minimalizující vzdálenost $\|b - z\|$ (tj. realizující vzdálenost od podprostoru $\rho(b, \operatorname{Im}\varphi)$) právě komponenta $z = b_1$ rozkladu $b = b_1 + b_2$, $b_1 \in \operatorname{Im}\varphi$, $b_2 \in (\operatorname{Im}\varphi)^\perp$. Přitom ale ve zvolené bázi je zobrazení $\varphi^{(-1)}$, původně zadané ve standardních bazích pseudoinverzí $A^{(-1)}$, dáno maticí S' z věty o singulárním rozkladu, zejména je $\varphi^{(-1)}(\operatorname{Im}\varphi) = (\operatorname{Ker}\varphi)^\perp$ a D^{-1} maticí zúžení $\varphi^{(-1)}_{|\operatorname{Im}\varphi}$ a $\varphi^{(-1)}_{|(\operatorname{Im}\varphi)^\perp}$ je nulové. Je tedy skutečně

$$\varphi \circ \varphi^{(-1)}(b) = \varphi(\varphi^{(-1)}(z)) = z$$

a důkaz je ukončen. □

Lze také ukázat, že matice $A^{(-1)}$ minimalizuje výraz

$$\|AA^{(-1)} - E\|^2$$

tj. součet kvadrátů všech prvků uvedené matice.

3.48

3.45. Lineární regrese. Aproximační vlastnost (3) předchozí věty je velice užitečná v případech, kdy máme najít co nejlepší přiblížení (neexistujícího) řešení přeurčeného systému $Ax = b$, kde A je reálná matice typu m/n a m je větší než n.

Např. máme experimentem dáno mnoho naměřených reálných hodnot b_j a chceme najít lineární kombinaci několika funkcí f_i, která bude co nejlépe aproximovat hodnoty b_j. Skutečné hodnoty zvolených funkcí v bodech $y_j \in \mathbb{R}$ zadají matici $a_{ij} = f_j(y_i)$, jejíž sloupce jsou dány hodnotami jednotlivých funkcí f_j v uvažovaných bodech, a naším úkolem je tedy určit koeficienty $x_j \in \mathbb{R}$ tak, aby součet kvadrátů odchylek od skutečných hodnot

$$\sum_{i=1}^{m}(b_i - (\sum_{j=1}^{n} x_j f_j(y_i)))^2 = \sum_{i=1}^{m}(b_i - (\sum_{j=1}^{n} a_{ij}x_j))^2$$

byla minimální. Jinými slovy, hledáme lineární kombinaci funkcí f_i takovou, abychom „dobře" proložili zadané hodnoty b_i. Díky předchozí větě jsou hledané optimální koeficienty $A^{(-1)}b$.

Abychom měli konkrétnější představu, uvažujme pouze dvě funkce $f_1(x) = x$, $f_2(x) = x^2$ a předpokládejme, že „naměřené hodnoty" jejich neznámé kombinace $g(x) = y_1x + y_2x^2$ v celočíselných hodnotách pro x mezi 1 a 10 jsou

$$b^T = (1.44\ 10.64\ 4.48\ 14.56\ 31.12\ 39.20\ 54.88\ 71.28\ 85.92\ 104.16).$$

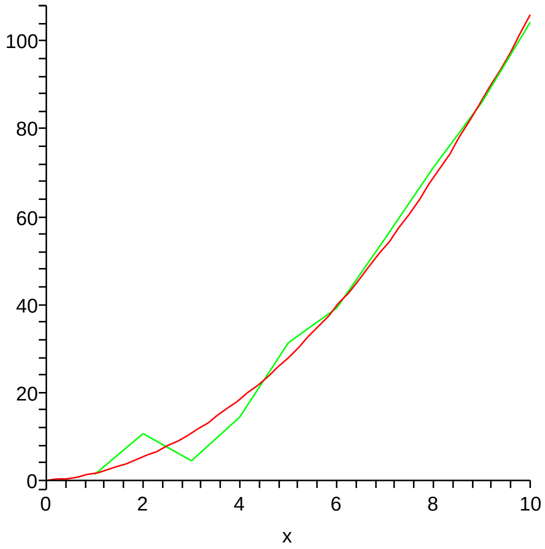
Tento vektor vzniknul výpočtem hodnot $x + x^2$ v daných bodech posunutých o náhodné hodnoty v rozmezí ± 8. Matice $A = (b_{ij})$ je tedy v našem případě rovna

$$A^T = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 4 & 9 & 16 & 25 & 36 & 49 & 64 & 81 & 100 \end{pmatrix}$$

a hledané koeficienty v kombinaci jsou

$$y = A^{(-1)} \cdot b = \begin{pmatrix} 0.61 \\ 0.99 \end{pmatrix}.$$

Výsledné proložení je možné dobře vidět na obrázku, kde zeleně jsou proloženy zadané hodnoty b lomenou čarou, zatímco červený je graf příslušné kombinace g. Výpočty byly provedeny v systému Maple pomocí příkazu *leastsqrs(B,b)*. Pokud jste s Maplem (nebo jiným podobným softwarem) spřáteleni, zkuste si zaexperimentovat s podobnými úlohami.



KAPITOLA 4

Analytická geometrie

poloha, incidence, projekce?
– a zase skončíme u matic...

Vrátíme se teď k úlohám elementární geometrie z podobného pohledu, jako když jsme zkoumali polohy bodů v rovině v 5. části první kapitoly, viz 1.23. Budeme se nejprve zajímat o vlastnosti objektů vymezených pomocí bodů, přímek, rovin apod. Podstatné přitom bude vyjasnění, které vlastnosti závisí či nezávisí na pojmu velikosti vektorů.

V další části pak použijeme lineární algebru pro studium objektů, které už lineárně definované nejsou. Opět přitom budeme potřebovat trochu více maticového počtu. Výsledky budou naprosto zásadní později při diskusi technik pro optimalizace, tj. hledání extrémů funčkních hodnot.

Projektivní rozšíření afinních prostorů nám v závěru kapitoly ukáže, jak lze překvapivě dosáhnout zjednodušení i stability algoritmických postupů typických pro práci s počítačovou grafikou.

1. Afinní a euklideovská geometrie

Když jsme si ujasňovali dopady obecné teorie na systémy rovnic v první části předchozí kapitoly, zjistili jsme v ostavci 3.1, že všechna řešení nehomogenních systémů rovnic sice netvoří vektorové podprostory, vždy ale vznikají tak, že k jednomu jedinému řešení přičteme celý vektorový prostor řešení příslušné homogenní soustavy. Naopak, rozdíl dvou řešení nehomogenní soustavy je vždy řešením homogenní. Obdobně se chovají lineární difereční rovnice, jak jsme viděli již v odstavci 3.11.

Návod na teoretické uchopení takové situace dává již diskuse geometrie roviny, viz odstavec 1.25 a dále. Tam jsme totiž popisovali přímky a body jako množiny řešení systémů lineárních rovnic. Přímka pro nás pak byla „jednorozměrným“ prostorem, přestože její body byly popisovány dvěmi souřadnicemi. Parametricky jsme ji zadávali tak, že k jednomu bodu (tj. dvojici souřadnic) jsme přičítali násobky pevně zvoleného směrového vektoru. Stejně budeme postupovat i teď v libovolné dimenzi.

4.1

4.1. Afinní prostory. *Standarní afinní prostor* $\mathcal{A}_n$ je množina všech bodů v $\mathbb{R}^n = \mathcal{A}_n$ spolu s operací, kterou k bodu $A = (a_1, \dots, a_n) \in \mathcal{A}_n$ a vektoru $v = (v_1, \dots, v_n) \in \mathbb{R}^n = V$ přiřadíme bod

$$A + v = (a_1 + v_1, \dots, a_n + v_n) \in \mathbb{R}^n = \mathcal{A}_n.$$

Tyto operace splňují následující tři vlastnosti:

(1) $A + 0 = A$ pro všechny body $A \in \mathcal{A}_n$ a nulový vektor $0 \in V$
(2) $A+(v+w) = (A+v)+w$ pro všechny vektory $v, w \in V$, $A \in \mathcal{A}_n$
(3) pro každé dva body $A, B \in \mathcal{A}_n$ existuje právě jeden vektor $v \in V$ takový, že $A + v = B$. Značíme jej $B - A$, někdy také $\vec{AB}$.

Vektorový prostor $\mathbb{R}^n$ nazýváme *zaměření afinního prostoru* $\mathcal{A}_n$.

Standardní afinní prostor

Všimněme si několika formálních nebezpečí. Používáme stejný symbol „+“ pro dvě různé operace: přičtení vektoru ze zaměření k bodu v afinním prostoru, ale také sčítání vektorů v zaměření $V = \mathbb{R}^n$. Také nezavádíme zvláštní písmena pro samotnou množinu bodů afinního prostoru, tj. $\mathcal{A}_n$ pro nás představuje jak samotnou množinu bodů, tak i celou strukturu definující afinní prostor.

Proč vlastně chceme rozlišovat množinu bodů prostoru $\mathcal{A}_n$ od jeho zaměření V, když se jedná jakoby o stejné $\mathbb{R}^n$? Jde o velice podstatný formální krok k pochopení geometrie v $\mathbb{R}^n$:

Geometrické objekty jako přímky, body, roviny apod. nejsou totiž přímo závislé na vektorové struktuře na množině $\mathbb{R}^n$ a už vůbec ne na tom, že pracujeme s n–ticemi skalárů. Potřebujeme jen umět říci, co to znamená pohybovat se „rovně v daném směru“. K tomu právě potřebujeme na jedné straně vnímat třeba rovinu jako neohraničenou desku bez zvolených souřadnic, ale s možností posunout se o zadaný vektor. Když přejdeme navíc k takovému abstraktnímu pohledu, budeme umět diskutovat „rovinnou geometrii“ pro dvourozměrné podprostory, tj. roviny ve vícerozměrných prostorech, „prostorovou“ pro třírozměrné atd., aniž bychom museli přímo manipulovat k–ticemi souřadnic.

Tento pohled je zachycen v následující definici:

4.1a **4.2. Definice.** Afinním prostorem $\mathcal{A}$ se zaměřením V rozumíme množinu *bodů* $\mathcal{P}$, spolu se zobrazením

$$\mathcal{P} \times V \to \mathcal{P}, \quad (A, v) \mapsto A + v,$$

splňujícím vlastnosti (1)–(3) výše.

Pro libovolný pevně zvolený vektor $v \in V$ je tak definováno *posunutí* $\tau_v : \mathcal{A} \to \mathcal{A}$ jako zúžené zobrazení

$$\tau_v : \mathcal{P} \simeq \mathcal{P} \times \{v\} \to \mathcal{P}, \quad A \mapsto A + v.$$

Dimenzí afinního prostoru $\mathcal{A}$ rozumíme dimenzi jeho zaměření.

Nadále nebudeme rozlišovat $\mathcal{A}$ a $\mathcal{P}$ v označení.

Z axiomů okamžitě plyne pro libovolné body A, B, C v afinním prostoru $\mathcal{A}$

$$A - A = 0 \in V \tag{4}$$

$$B - A = -(A - B) \tag{5}$$

$$(C - B) + (B - A) = (C - A). \tag{6}$$

Skutečně, (4) vyplývá z toho, že $A + 0 = 0$ a takový vektor musí být jednoznačný (první a třetí definiční vlastnost). Postupným přičtením $B - A$ a $A - B$ k A (v uvedeném pořadí), zjevně dostaneme podle druhé definiční vlastnosti opět A, tedy jsme přičetli nulový vektor a to dokazuje (5). Obdobně z platnosti (2) a jednoznačnosti vyplývá (6).

Všimněme si, že volba jednoho pevného bodu $A_0 \in \mathcal{A}$ nám určuje bijekci mezi V a $\mathcal{A}$. Při volbě pevné báze $\underline{u}$ ve V tak dostáváme pro každý bod $A \in \mathcal{A}$ jednoznačné vyjádření

$$A = A_0 + x_1 u_1 + \cdots + x_n u_n.$$

Hovoříme o *afinní soustavě souřadnic* $(A_0; u_1, \dots, u_n)$ zadané *počátkem afinní souřadné soustavy* A_0 a bazí zaměření $\underline{u}$. Hovoříme také o *afinním repéru* $(A_0, \underline{u})$.

Slovy můžeme shrnout situaci takto: Afinní souřadnice bodu A v soustavě $(A_0, \underline{u})$ jsou souřadnicemi vektoru $A - A_0$ v bázi $\underline{u}$ zaměření V.

Volba afinního souřadného systému ztotožňuje n-rozměrný afinní prostor $\mathcal{A}$ se standardním afinním prostorem
2.59 $\mathcal{A}_n$.

4.3. Afinní podprostory. Jestliže si vybereme v $\mathcal{A}$ jen body, které budou mít některé předem vybrané souřadnice nulové (třeba poslední jednu). Dostaneme opět množinu, která se bude chovat jako afinní prostor. Takto budeme skutečně parametricky popisovat tzv. afinní podprostory ve smyslu následující definice.

Definice. Neprázdná podmnožina $\mathcal{Q} \subset \mathcal{A}$ afinního prostoru $\mathcal{A}$ se zaměřením V se nazývá *afinní podprostor* v $\mathcal{A}$, je-li podmnožina $W = \{B - A; A, B \in \mathcal{Q}\} \subset V$ vektorovým podprostorem a pro libovolné $A \in \mathcal{Q}$, $v \in W$ je $A + v \in \mathcal{Q}$.

Je podstatné mít obě podmínky zahrnuty v definici, protože je snadné najít příklady podmnožin, které budou splňovat první, ale nikoliv druhou. Přemýšlejte např. o přímce v rovině s vyjmutým jedním bodem.

Pro libovolnou množinu bodů $M \subset \mathcal{A}$ v afinním prostoru se zaměřením V definujeme vektorový podprostor

$$Z(M) = \langle\{B - A; B, A \in M\}\rangle \subset V$$

všech vektorů generovaných rozdíly bodů z M.

Zejména je $V = Z(\mathcal{A})$ a každý afinní podprostor $\mathcal{Q} \subset \mathcal{A}$ splňuje sám axiomy afinního prostoru se zaměřením $Z(\mathcal{Q})$.

Přímo z definic je také zřejmé, že průnik libovolné množiny afinních podprostorů je buď opět afinní podprostor nebo prázdná množina.

Afinní podprostor $\langle M\rangle$ v $\mathcal{A}$ *generovaný* neprázdnou podmnožinou $M \subset \mathcal{A}$ je průnikem všech afinních podprostorů, které obsahují všechny body podmnožiny M.

Afinní podprostory si můžeme pěkně popsat pomocí jejich zaměření, jakmile si zvolíme jeden jejich bod $A_0 \in M$ v generující množině bodů M. Skutečně, dostáváme $\langle M \rangle = \{A_0 + v;\ v \in Z(M) \subset Z(\mathcal{A})\}$, tj. pro generování afinního podprostoru vezmeme vektorový podprostor $Z(M)$ v zaměření generovaný všemi rozdíly bodů z M a ten pak přičteme k libovolnému z nich. Hovoříme také o *afinním obalu* množiny bodů M v $\mathcal{A}$.

Naopak, kdykoliv zvolíme podprostor U v zaměření $Z(\mathcal{A})$ a jeden pevný bod $A \in \mathcal{A}$, pak podmnožina $A + U$ vzniklá všemi možnými součty jediného bodu A se všemi vektory v U je afinní podprostor. Takový postup vede k pojmu parametrizace podprostorů:

Nechť $\mathcal{Q} = A + Z(\mathcal{Q})$ je afinní podprostor v $\mathcal{A}_n$ a $(u_1, \dots, u_k)$ je báze $Z(\mathcal{Q}) \subset \mathbb{R}^n$. Pak vyjádření podprostoru

$$\mathcal{Q} = \{A + t_1 u_1 + \dots + t_k u_k;\ t_1, \dots, t_k \in \mathbb{R}\}$$

nazýváme *parametrický popis* podprostoru $\mathcal{Q}$.

Již jsme viděli jinou možnost zadávání afinních podprostorů: Jestliže máme zvoleny afinní souřadnice, pak lze zaměření podprostoru popsat pomocí homogenního systému lineárních rovnic v těchto souřadnicích. Dosazením souřadnic jednoho bodu našeho podprostoru $\mathcal{Q}$ do získaného systému rovnic dostaneme pravou stranu nehomogenního systému se stejnou maticí a celý podprostor $\mathcal{Q}$ je pak právě množinou řešení tohoto systému. Zadání podprostoru $\mathcal{Q}$ systémem rovnic v daných souřadnicích nazýváme *implicitní popis* podprostoru $\mathcal{Q}$.

Následující obecná věta říká, že takto umíme ve skutečnosti zadat všechny afinní podprostory a tím také ukazuje geometrickou podstatu vlastností množiny všech řešení systémů lineárních rovnic.

2.61 **4.4. Věta.** *Nechť $(A_0; \underline{u})$ je afinní souřadný systém v n-rozměrném afinním prostoru $\mathcal{A}$. Afinní podprostory dimenze k v $\mathcal{A}$, vyjádřené v daných souřadnicích, jsou právě množiny řešení řešitelných systémů $n - k$ lineárně nezávislých lineárních rovnic v n proměnných.*

Důkaz. Uvažujme libovolný řešitelný systém $n - k$ lineárně nezávislých rovnic $\alpha_i(x) = b_i$, $b_i \in \mathbb{R}$, $i = 1, \dots, n - k$. Je-li $A = (a_1, \dots, a_n)^T \in \mathbb{R}^n$ libovolné pevně zvolené řešení tohoto (nehomogenního) systému rovnic a je-li $U \subset \mathbb{R}^n$ vektorový podprostor všech řešení zhomogenizovaného systému $\alpha_i(x) = 0$, pak dimenze U je k a podmnožina všech řešení daného systému je tvaru $\{B;\ B = A + (y_1, \dots, y_n)^T,\ y = (y_1 \dots, y_n)^T \in U\} \subset \mathbb{R}^n$, viz. 3.1. Příslušný afinní podprostor je tím popsán parametricky ve výchozích souřadnicích $(A_0; \underline{u})$.

Naopak, uvažme libovolný afinní podprostor $\mathcal{Q} \subset \mathcal{A}_n$ a zvolme nějaký jeho bod B za počátek afinního souřadného systému $(B, \underline{v})$ pro afinní prostor $\mathcal{A}$. Protože $\mathcal{Q} = B + Z(\mathcal{Q})$, potřebujeme popsat zaměření podprostoru $\mathcal{Q}$ jako podprostor řešení homogenního systému rovnic. Zvolme tedy bázi $\underline{v}$ na $Z(\mathcal{A})$ tak, aby prvních k vektorů tvořilo bázi $Z(\mathcal{Q})$. Pak v těchto souřadnicích jsou vektory $v \in Z(\mathcal{Q})$ dány rovnostmi

$$\alpha_j(v) = 0, \quad j = k+1, \dots, n,$$

kde α_i jsou lineární formy z tzv. duální báze k $\underline{v}$, tj. funkce přiřazení jednotlivých souřadnic v naší bázi $\underline{v}$.

Náš vektorový podprostor $Z(\mathcal{Q})$ dimenze k v n-rozměrném $\mathbb{R}^n$ je tedy skutečně dán jako řešení homogenního systému $n-k$ nezávislých rovnic. Popis zvoleného afinního podprostoru ve vybraném souřadném systému $(A_0; \underline{u})$ je proto dán systémem homogenních lineárních rovnic.

Zbývá nám se vypořádat důsledky přechodu z původního zadaného souřadného systému $(A; \underline{u})$ do našeho přizpůsobeného $(B; \underline{v})$. Z obecné úvahy o transformacích souřadnic v následujícím odstavci vyplyne, že výsledný popis podprostoru bude opět pomocí systému rovnic, tentokrát ale už obecně nehomogenních. □

4.5

4.5. Transformace souřadnic. Dvě libovolně zvolené afinní soustavy souřadnic $(A_0, \underline{u})$, $(B_0, \underline{v})$ se obecně liší posunutím počátku o vektor $(B_0 - A_0)$ a jinou bazí zaměření. Transformační rovnice tedy vyčteme ze vztahu pro obecný bod $X \in \mathcal{A}$

$$X = B_0 + x_1' v_1 + \dots + x_n' v_n = B_0 + (A_0 - B_0) + x_1 u_1 + \dots + x_n u_n.$$

Označme $y = (y_1, \dots, y_n)^T$ sloupec souřadnic vektoru $(A_0 - B_0)$ v bázi $\underline{v}$ a $M = (a_{ij})$ buď matice vyjadřující bázi $\underline{u}$ prostřednictvím báze $\underline{v}$. Potom

$$\begin{aligned} x_1' &= y_1 + a_{11}x_1 + \dots + a_{1n}x_n \\ &\vdots \\ x_n' &= y_n + a_{n1}x_1 + \dots + a_{nn}x_n \end{aligned}$$

tj. maticově

$$x' = y + M \cdot x.$$

Jako příklad si můžeme spočítat dopad takové změny báze na vyjádření řešení systémů rovnic. Nechť v souřadnicích $(A_0; \underline{u})$ má systém rovnic tvar

$$S \cdot x = b$$

s maticí systému S. Pak $S \cdot x = S \cdot M^{-1} \cdot (y + M \cdot x) - S \cdot M^{-1} \cdot y = b$. Proto v nových výše uvažovaných souřadnicích $(B_0; \underline{v})$ bude mít náš systém rovnic tvar

$$(S \cdot M^{-1}) \cdot x' = b' = b + (S \cdot M^{-1}) \cdot y.$$

To plně dokončuje důkaz předchozí věty.

4.3

4.6. Příklady afinních podprostorů. (1) Jednorozměrný (standardní) afinní prostor je množina všech bodů reálné přímky $\mathcal{A}_1$. Její zaměření je jednorozměrný vektorový prostor $\mathbb{R}$ (a nosná množina také $\mathbb{R}$). Afinní souřadnice dostaneme volbou počátku a měřítka (tj. báze ve vektorovém prostoru $\mathbb{R}$). Všechny vlastní afinní podprostory jsou 0-rozměrné, jsou to právě všechny body reálné přímky $\mathbb{R}$.
(2) Dvourozměrný (standardní) afinní prostor je množina všech bodů prostoru $\mathcal{A}_2$ se zaměřením $\mathbb{R}^2$. (Nosnou množinou je $\mathbb{R}^2$.) Afinní souřadnice dostaneme volbou počátku a dvou

nezávislých vektorů (směrů a měřítek). Vlastní afinní podprostory jsou pak všechny body a přímky v rovině (0-rozměrné a 1-rozměrné). Přímky přitom jednoznačně zadáme jejich jedním bodem a jedním generátorem zaměření (tzv. parametrický popis přímky).
(3) Trojrozměrný (standardní) afinní prostor je množina všech bodů prostoru $\mathcal{A}_3$ se zaměřením $\mathbb{R}^3$. Afinní souřadnice dostaneme volbou počátku a tří nezávislých vektorů (směrů a měřítek). Vlastní afinní podprostory jsou pak všechny body, přímky a roviny (0-rozměrné, 1-rozměrné a 2-rozměrné).
(4) Podprostor všech řešení jedné lineární rovnice $a \cdot x = b$ pro neznámý bod $[x_1, \dots, x_n] \in \mathcal{A}_n$, známý nenulový vektor koeficientů $(a_1, \dots, a_n)$ a skalár $b \in \mathbb{R}$ je afinní podprostor dimenze $n - 1$ (říkáme také, že je kodimenze 1), tj. tzv. *nadrovina v A_n.*

4.6

4.7. Afinní kombinace bodů. Nechť $A_0, \dots, A_k$ jsou body v afinním prostoru $\mathcal{A}$. Jejich afinní obal $\langle\{A_0 \dots, A_k\}\rangle$ můžeme zapsat jako

$$\{A_0 + t_1(A_1 - A_0) + \dots + t_k(A_k - A_0);\, t_1, \dots, t_k \in \mathbb{R}\}$$

a v libovolných afinních souřadnicích (tj. A_i je vyjádřen sloupcem skalárů) můžeme tutéž množinu zapsat jako

$$\langle A_0, \dots, A_k\rangle = \{t_0A_0 + t_1A_1 + \dots + t_kA_k;\, t_i \in \mathbb{R}, \sum_{i=0}^{k} t_i = 1\}.$$

Obecně výrazy $t_0A_0 + t_1A_1 + \dots + t_kA_k$ s koeficienty splňujícími $\sum_{i=0}^{k} t_i = 1$ rozumíme body $A_0 + \sum_{i=1}^{k} t_i(A_i - A_0)$ a nazýváme je *afinní kombinace bodů.*

Body $A_0 \dots, A_k$ jsou v *obecné poloze*, jestliže generují k-rozměný podprostor. Z našich definic je vidět, že to nastane právě, když pro kterýkoliv z nich platí, že vektory vzniklé pomocí rozdílů tohoto pevného s ostatními jsou lineárně nezávislé. Všimněme si také, že zadání posloupnosti $\dim \mathcal{A}$ bodů v obecné poloze je ekvivalentní zadání afinního repéru se středem v prvním z nich.

Afinní kombinace je obdobná konstrukce pro body afinního prostoru jako byla lineární kombinace pro vektorové prostory. Skutečně, afinní podprostor generovaný body $A_0 \dots, A_k$ je roven množině všech afinních kombinací svých generátorů. Můžeme však nyní dobře zobecnit i pojem „mezi dvěma body na přímce“. V dvojrozměrném případě tomu odopovídá vnitřek trojúhelníku. Obecně budeme postupovat takto:

4.6a

4.8. Simplexy. Nechť $A_0, \dots, A_k$ je $k + 1$ bodů afinního prostoru $\mathcal{A}$ v obecné poloze. k–rozměrný *simplex* $\Delta = \Delta(A_0, \dots, A_k)$ generovaný těmito body je definován jako množina všech afinních kombinací bodů A_i s pouze nezápornými koeficienty, tzn.

$$\Delta = \{t_0A_0 + t_1A_1 + \dots + t_kA_k;\, t_i \in [0, 1] \subset \mathbb{R}, \sum_{i=0}^{k} t_i = 1\}.$$

Jednorozměrný simplex je *úsečka*, dvourozměrný *trojúhelník*, nula–rozměrný bod.

Všimněme si, že každý k–rozměrný simplex má právě $k+1$ *stěn*, které jsou postupně zadány rovnicemi $t_i = 0$, $i = 0, \dots, k$. Přímo z definice je vidět, že jde opět o $(k-1)$–rozměrné simplexy. Hovoříme o *hranici simplexu*. Např. trojúhelník má za svou hranici tři hrany, každá z nich pak dva body.

Zadání podprostoru jako množiny afinních kombinací bodů v obecné poloze je ekvivalentní parametrickému popisu. Obdobně pracujeme s parametrickými popisy simplexů.

4.7

4.9. Konvexní množiny. Podmnožina M afinního prostoru se nazývá *konvexní*, jestliže s každými svými dvěma body A, B obsahuje i celou úsečku $\Delta(A, B)$. Přímo z definice je vidět, že každá konvexní množina obsahuje s každými $k+1$ body v obecné poloze i celý jimi definovaný simplex (dokažte si formálně podrobně!). Konvexními množinami jsou např.
(1) prázdná podmnožina
(2) afinní podprostory
(3) úsečky, polopřímky $p = \{P + t \cdot v;\ t \geq 0\}$,
(4) obecněji k– rozměrné *poloprostory* $\alpha = \{P + t_1 \cdot v_1 + \dots + t_k \cdot v_k;\ t_1, \dots, t_k \in \mathbb{R}, t_k \geq 0\}$,
(5)) *úhly* v dvojrozměrných podprostorech $\beta = \{P + t_1 \cdot v_1 + t_2 \cdot v_2;\ t_1 \geq 0, t_2 \geq 0\}$, atd.

Přímo z definice také plyne, že průnik libovolného systému konvexních množin je opět konvexní. Průnik všech konvexních množin obsahujících danou množinu M nazýváme *konvexní obal* $\mathcal{K}(M)$ množiny M.

Věta. *Konvexní obal libovolné podmnožiny $M \subset \mathcal{A}$ je*

$$\mathcal{K}(M) = \{t_1 A_1 + \dots + t_s A_s;\ \sum_{i=1}^{s} t_i = 1,\ t_i \geq 0, A_i \in M\}$$

Důkaz. Označme S množinu všech afinních kombinací na pravé straně dokazované rovnosti. Nejprve ověříme, že je S konvexní. Zvolme tedy dvě sady parametrů t_i, $i = 1, .., s_1$, t'_j, $j = 1, \dots, s_2$ s požadovanými vlastnosti. Bez újmy na obecnosti můžeme předpokládat, že $s_1 = s_2$ a že v obou kombinacích vystupují stejné body z M (jinak prostě přidáme sčítance s nulovými koeficienty). Uvažme libovolný bod úsečky zadané takto získanými body:

$$\epsilon(t_1 A_1 + \dots + t_s A_s) + (1-\epsilon)(t'_1 A_1 + \dots + t'_s A_s),\ 0 \leq \epsilon \leq 1.$$

Zřejmě jsou opět všechny v S.

Zbývá ukázat, že konvexní obal bodů $A_1, \dots, A_s$ nemůže být menší než S. Samotné body A_i odpovídají volbě parametrů $t_j = 0$ pro všechny $j \neq i$ a $t_i = 1$. Předpokládejme, že tvrzení platí pro všechny množiny s nejvýše $s-1$ body. To znamená, že konvexní obal bodů $A_1, \dots, A_{s-1}$ je (podle předpokladu) tvořen právě těmi kombinacemi z pravé strany dokazované rovnosti, kde $t_s = 0$. Uvažme nyní libovolný bod $A = t_1 A_1 + \dots + t_s A_s \in S$, $t_s \neq 1$, a afinní kombinace

$$\epsilon(t_1 A_1 + \dots + t_{s-1} A_{s-1}) + (1 - \epsilon(1-t_s)) A_s,\ 0 \leq \epsilon \leq \tfrac{1}{1-t_s}.$$

Jde o úsečku s krajními body určenými parametry $\epsilon = 0$ (bod A_s) a $\epsilon = 1/(1-t_s)$ (bod v konvexním obalu bodů $A_1, \dots, A_{s-1}$). Bod A je vnitřním bodem této úsečky s parametrem $\epsilon = 1$. □

Konvexní obaly konečných množin bodů se nazývají *konvexní mnohostěny*. Jsou-li definující body $A_0, \dots, A_k$ konvexního mnohostěnu v obecné poloze, dostáváme právě k-rozměrný *simplex*. V případě simplexu je vyjádření jeho bodů ve tvaru afinní kombinace definujících vrcholů jednoznačné.

Zvláštním příkladem jsou konvexní mnohostěny generované jedním bodem a konečně mnoha vektory: Nechť $u_1, \dots, u_k$, jsou libovolné vektory v zaměření $\mathbb{R}^n$, $A \in \mathcal{A}_n$ je libovolný bod. *Rovnoběžnostěn* $\mathcal{P}_k(A; u_1, \dots, u_k) \subset \mathcal{A}_n$ je množina

$$\mathcal{P}_k(A; u_1, \dots, u_k) = \{A + c_1 u_1 + \dots + c_k u_k;\ 0 \le c_i \le 1\}.$$

Jsou-li vektory $u_1, \dots, u_k$ nezávislé, hovoříme o k-rozměrném rovnoběžnostěnu $\mathcal{P}_k(A; u_1, \dots, u_k) \subset \mathcal{A}_n$. Z definice je zřejmé, že rovnoběžnostěny jsou konvexní. Ve skutečnosti jde o konvexní obaly jejich vrcholů.

4.8

4.10. Příklady standardních afinních úloh. (1) *K podprostoru zadanému implicitně nalézt parametrický popis a naopak:*

Nalezením partikulárního řešení nehomogenního systému a fundamentálního řešení zhomogenizovaného systému rovnic získáme (v souřadnicích, ve kterých byly rovnice zadány) právě hledaný parametrický popis. Naopak, zapíšeme-li parametrický popis v souřadnicích, můžeme volné parametry $t_1, \dots, t_k$ vyeliminovat a získáme právě rovnice zadávající daný podprostor implicitně.

(2) *Nalézt podprostor generovaný několika podprostory $\mathcal{Q}_1, \dots, \mathcal{Q}_s$ (obecně různých dimenzí, např. v R_3 nalézt rovinu danou bodem a přímkou, třemi body apod.) a zadat jej implicitně či parametricky:*

Výsledný podprostor $\mathcal{Q}$ je vždy určen jedním pevně zvoleným bodem A_i v každém z nich a součtem všech zaměření. Např.

$$\mathcal{Q} = A_1 + (Z(\{A_1, \dots, A_k\}) + Z(\mathcal{Q}_1) + \dots + Z(\mathcal{Q}_s)).$$

Pokud jsou podprostory zadány implicitně, je možné je nejdříve převést na parametrický tvar. V konkrétních situacích bývají funkční i jiné postupy. Všimněme si, že obecně je skutečně nutné využít jednoho bodu z každého podprostoru. Např. dvě paralelní přímky v rovině vygenerují celou rovinu, ale sdílí totéž jednorozměrné zaměření.

(3) *Nalézt průnik podprostorů $\mathcal{Q}_1, \dots, \mathcal{Q}_s$:*

Pokud jsou zadány v implicitním tvaru, stačí sjednotit všechny rovnice do jednoho systému (a případně vynechat lineárně závislé). Pokud je vzniklý systém neřešitelný, je průnik prázdný. V opačném případě získáme implicitní popis afinního podprostoru, který je hledaným průnikem.

Pokud máme dány parametrické tvary, můžeme také hledat přímo společné body jako řešení vhodných rovnic, podobně jako při hledání průniků vektorových podprostorů. Získáme tak přímo opět parametrický popis. Pokud je podprostorů více než dva, musíme průnik hledat postupně.

Máme-li jeden prostor zadaný parametricky a ostatní implicitně, stačí dosadit parametrizované souřadnice a řešit výsledný systém rovnic.

(4) *Nalezení příčky mimoběžek p, q v $\mathcal{A}_3$ procházející daným bodem nebo mající předem daný směr (tj. zaměření):*
Příčkou rozumíme přímku, která má neprázdný průnik s oběmi mimoběžkami. Výsledná příčka r tedy bude jednorozměrným afinním podprostorem. Pokud máme zadán jeho bod $A \in r$, pak afinní podprostor generovaný p a A je buď přímka ($A \in p$) nebo rovina ($A \notin p$). V prvém případě máme nekonečně mnoho řešení, jedno pro každý bod z q, v druhém stačí najít průnik B roviny $\langle p \cup A\rangle$ s q a $r = \langle\{A, B\}\rangle$. Pokud je průnik prázdný, úloha nemá řešení, v případě že $q \subset \langle p \cup A\rangle$, máme opět nekonečně mnoho řešení, a pokud je průnik jednoprvkový, dostáváme právě jedno řešení.

Máme-li místo bodu dán směr $u \in \mathbb{R}^n$, tj. zaměření r, pak uvažujeme opět podprostor $\mathcal{Q}$ generovaný p a zaměřením $Z(p) + \langle u\rangle \subset \mathbb{R}^n$. Opět, pokud $q \subset \mathcal{Q}$, máme nekonečně mnoho řešení, jinak uvážíme průnik $\mathcal{Q}$ s q a úlohu dokončíme stejně jako v předchozím případě.

Řešení mnoha dalších standardních geometrických úloh spočívá v používání výše uvedených kroků.

4.9

4.11. Afinní zobrazení. Zobrazení $f : \mathcal{A} \to \mathcal{B}$ mezi afinními prostory nazýváme *afinní zobrazení*, jestliže mezi jejich zaměřeními existuje lineání zobrazení $\varphi : Z(\mathcal{A}) \to Z(\mathcal{B})$ takové, že pro všechny $A \in \mathcal{A}$, $v \in Z(\mathcal{A})$ platí

$$f(A + v) = f(A) + \varphi(v).$$

Zobrazení f a φ jsou jednoznačně zadána touto vlastností a libovolně zvolenými obrazy $(\dim \mathcal{A} + 1)$ bodů v obecné poloze.

Pro libovolnou afinní kombinaci bodů $t_0A_0 + \dots + t_sA_s \in \mathcal{A}$ pak dostaneme

$$\begin{aligned} f(t_0A_0 + \dots + t_sA_s) &= \\ &= f(A_0 + t_1(A_1 - A_0) + \dots + t_s(A_s - A_0)) \\ &= f(A_0) + t_1\varphi(A_1 - A_0) + \dots + t_s\varphi(A_s - A_0) \\ &= t_0 f(A_0) + t_1 f(A_1) + \dots + t_s f(A_s). \end{aligned}$$

Naopak, pokud pro nějaké zobrazení platí, že zachovává afinní kombinace, můžeme použít speciální případ kombinace dvou vektorů s koeficienty $t_0 = 0$ a $t_1 = 1$ pro definici zobrazení φ mezi zaměřeními. Pak lze číst předchozí výpočet v opačném pořadí a ověřit korektnost i linearitu φ a zjistíme, že se jedná o afinní zobrazení. Platí proto:

Věta. *Afinní zobrazení jsou právě ta zobrazení, která zachovávají afinní kombinace bodů.*

Volbou afinních souřadnic $(A_0, \underline{u})$ na $\mathcal{A}$ a $(B_0, \underline{v})$ na $\mathcal{B}$ dostáváme souřadné vyjádření afinního zobrazení $f : \mathcal{A} \to \mathcal{B}$. Přímo z definice je zřejmé, že stačí vyjádřit obraz $f(A_0)$ počátku souřadnic v $\mathcal{A}$ v souřadnicích na $\mathcal{B}$, tj. vyjádřit vektor $f(A_0) - B_0$ v bázi $\underline{v}$ jako sloupec souřadnic y_0 a vše ostatní je pak určeno násobením maticí zobrazení φ ve zvolených bazích a přičtením výsledku. Každé afinní zobrazení tedy v souřadnicích vypadá takto:

$$x \mapsto y_0 + Y \cdot x,$$

kde y_0 je jako výše a Y je matice zobrazení φ.

Transformace afinních souřadnic odpovídá, obdobně jako u lineárních zobrazení, vyjádření identického zobrazení v zvolených afinních repérech. Změna souřadného vyjádření afinního zobrazení v důsledku změny bazí se snadno spočte pomocí násobení a sčítání. Skutečně, při změně báze na definičním oboru daném posunutím w a maticí M (od staré k nové), a na oboru hodnot posunutím w a maticí N (od nové ke staré) dostáváme

$$\begin{aligned} y' &= z + N \cdot y = z + N \cdot (y_0 + Y \cdot x) \\ &= (z + N \cdot y_0 + N \cdot Y \cdot w) + (N \cdot Y \cdot M) \cdot x'. \end{aligned}$$

4.10 **4.12. Euklidovské bodové prostory.** Zatím jsme pro naše elementární geometrické úvahy nepotřebovali pojem vzdálenosti nebo velikosti. V mnoha praktických úlohách ale velikost vektorů a odchylka vektorů, tak jak jsme je zavedli na samém konci třetí části druhé kapitoly (viz 2.39 a dále), hrají podstatnou roli. Ve skutečnosti se ale dodatečné informace týkají opravdu jen vektorů v zaměření, takže nám nezbývá mnoho práce:

Definice. Standardní *bodový euklidovský prostor* $\mathcal{E}_n$ je afinní prostor $\mathcal{A}_n$, jehož zaměřením je standardní euklidovský prostor $\mathbb{R}^n$ se skalárním součinem

$$\langle x, y \rangle = y^T \cdot x.$$

Kartézská souřadná soustava je afinní souřadná soustava $(A_0; \underline{u})$ s ortonormální bazí $\underline{u}$.

Vzdálenost bodů $A, B \in \mathcal{E}_n$ definujeme jako velikost vektoru $\|B - A\|$, budeme ji značit $\rho(A, B)$.

Euklidovské podprostory v $\mathcal{E}_n$ jsou afinní podprostory jejichž zaměření uvažujeme spolu se zúženými skalárními součiny.

Bodovým euklidovským prostorem $\mathcal{E}$ dimenze n pak obecně rozumíme afinní prostor, jehož zaměření je reálný n–rozměrný euklidovský vektorový prostor. Pojem kartézské souřadné soustavy má opět jasný smysl. Každá volba takové souřadné soustavy ovšem zadává ztotožnění $\mathcal{E}$ se standardním prostorem $\mathcal{E}_n$. Proto se budeme v dalším, bez újmy na obecnosti, zabývat hlavně standardními euklidovskými prostory a jejich podprostory.

Z geometrického pohledu mají jednoduché vlastnosti skalárního součinu, jako jsou trojúhelníková nerovnost, Cauchyova nerovnost, Besselova nerovnost apod., odvozené ve čtvrté části předchozí kapitoly, viz 3.22, velmi užitečné přímé důsledky:

4.13 **4.13. Věta.** *Pro body $A, B, C \in \mathcal{E}_n$ platí*

(1) $\rho(A, B) = \rho(B, A)$
(2) $\rho(A, B) = 0$ *právě, když* $A = B$
(3) $\rho(A, B) + \rho(B, C) \geq \rho(A, C)$
(4) V každé kartézké souřadné soustavě $(A_0; \underline{e})$ *mají body*

$$A = A_0 + a_1e_1 + \cdots + a_ne_n, \quad B = A_0 + b_1e_1 + \cdots + b_ne_n$$

vzdálenost $\sqrt{\sum_{i=1}^{n}(a_i - b_i)^2}$.

(5) Je–li dán bod A a podprostor $\mathcal{Q}$ v $\mathcal{E}_n$, pak existuje bod $P \in \mathcal{Q}$ minimalizující vzdálenosti bodů $\mathcal{Q}$ od A. Vzdálenost bodů A a P je rovna velikosti kolmého průmětu vektoru $A - B$ do $Z(\mathcal{Q})^{\perp}$ pro libovolný $B \in \mathcal{Q}$.

(6) Obecněji, pro podprostory $\mathcal{R}$ a $\mathcal{Q}$ v $\mathcal{E}_n$ existují bod $P \in \mathcal{Q}$ a $Q \in \mathcal{R}$ minimalizující vzdálenosti bodů $B \in \mathcal{Q}$ a $A \in \mathcal{R}$. Vzdálenost bodů Q a P je rovna velikosti kolmého průmětu vektoru $A - B$ do $Z(\mathcal{Q})^{\perp}$ pro libovolné body $B \in \mathcal{Q}$ a $A \in \mathcal{R}$.

Důkaz. První tři vlastnosti vyplývají přímo z vlastností velikosti vektorů v prostorech se skalárním součinem, čtvrtá plyne přímo z vyjádření skalárního součinu v libovolné ortonormální bázi.

Podívejme se na vztah pro minimalizaci vzdleností $\rho(A, B)$ pro $B \in \mathcal{Q}$. Vektor $A - B$ se jednoznačně rozkládá na $A - B = u_1 + u_2$, $u_1 \in Z(\mathcal{Q})$, $u_2 \in Z(\mathcal{Q})^{\perp}$. Přitom u_2 nezávisí na volbě $B \in \mathcal{Q}$, protože případná změna bodu B se projeví přičtením vektoru ze $Z(\mathcal{Q})$.

Nyní zvolme $P = A + (-u_2) = B + u_1 \in \mathcal{Q}$. Dostáváme

$$\|A - B\|^2 = \|u_1\|^2 + \|u_2\|^2 \geq \|u_2\|^2 = \|A - P\|.$$

Odtud již vyplývá, že nejmenší možné vzdálenosti je skutečně dosaženo, a to právě pro náš bod P. Vypočtená vzdálenost je skutečně $\|u_2\|$.

Obdobně ukážeme obecný výsledek. Pro volbu libovolných bodů $A \in \mathcal{R}$ a $B \in \mathcal{Q}$ je jejich rozdíl dán jako součet vektorů $u_1 \in Z(\mathcal{R}) + Z(\mathcal{Q})$ a $u_2 \in (Z(\mathcal{R}) + Z(\mathcal{Q}))^{\perp}$, přičemž komponenta u_2 nezávisí na volbě bodů. Přičtením vhodných vektorů ze zaměření $\mathcal{R}$ a $\mathcal{Q}$ zjevně obdržíme body A' a B', jejichž vzdálenost je právě $\|u_2\|$. □

Rozšíříme nyní náš stručný přehled elementárních úloh v analytické geometrii.

4.14. Příklady standardních úloh. (1) *Najděte vzdálenost bodu $A \in \mathcal{E}_n$ od podprostoru $\mathcal{Q} \subset \mathcal{E}_n$:*

Postup při řešení je dán ve větě 4.13.

(2) *V $\mathcal{E}_2$ veďte bodem A přímku q svírající s danou přímkou p daný úhel:*

Připoměňme, že na úrovni rovinné geometrie jsme s odchylkami vektorů již pracovali (viz např. 2.42). Najdeme vektor $u \in \mathbb{R}^2$ ležící v zaměření přímky q a zvolíme vektor v

mající od u zadanou odchylku. Hledaná přímka je dána bodem A a zaměřením $\langle v\rangle$. Úloha má dvě nebo jedno řešení.
(3) *Spočtěte patu kolmice vedené bodem na danou přímku:*

Postup je uveden v důkazu předposledního bodu věty 4.13.
(4) *V $\mathcal{E}_3$ určete vzdálenost dvou přímek p, q:*

Zvolíme libovolně jeden bod z každé přímky, $A \in p$, $B \in q$. Komponenta vektoru $A - B$ v ortogonálním doplňku $(Z(p) + Z(q))^\perp$ má velikost rovnu vzdálenosti p a q.
(5) *V $\mathcal{E}_3$ najděte osu dvou mimoběžek p a q:*

Osou zde rozumíme příčku, která realizuje nejmenší možnou vzdálenost daných mimoběžek pomocí bodů průniku. Opět lze postup dovodit z důkazu věty 4.13 (poslední bod). Nechť η je podprostor generovaný jedním bodem $A \in p$ a součtem $Z(p) + (Z(p) + Z(q))^\perp$. Pokud nejsou přímky p a q rovnoběžné, půjde o rovinu. Pak průnik $\eta \cap q$ spolu se zaměřením $(Z(p) + Z(q))^\perp$ dávají parametrický popis hledané osy. Pokud jsou přímky rovnoběžné, bude mít úloha nekonečně mnoho řešení.

4.15

4.15. Odchylky. Stejně jako vzdálenost, i řada dalších geometrických pojmů jako odchylky, orientace, objem apod. je v bodových prostorech $\mathcal{E}_n$ zaváděna prostřednictvím vhodných pojmů ve vektorových euklidovských prostorech. Připomeňme, že odchylku dvou vektorů jsme definovali na konci třetí části druhé kapitoly, viz 2.42.

Skutečně, z Cauchyovy nerovnosti plyne $0 \le \frac{|u\cdot v|}{\|u\|\|v\|} \le 1$, měla tedy smysl definice *odchylky* $\varphi(u, v)$ *vektorů* $u, v \in V$ v reálném vektorovém prostoru se skalárním součinem vztahem

$$\cos\varphi(u, v) = \frac{u \cdot v}{\|u\|\,\|v\|}, \quad 0 \le \varphi(u, v) \le 2\pi.$$

To je zcela v souladu s praxí v dvourozměrném euklidovském prostoru $\mathbb{R}^2$ a naší filozofií, že pojem týkající se dvou věktorů je ve své podstatě záležitostí dvourozměrné geometrie. Ve vícerozměrných prostorech je proto odchylka dvou vektorů vždy měřena v rovině, kterou tyto vektory generují (nebo je nula) a náš definiční vztah odpovídá zvyklostem ve všech dimenzích.

V libovolném reálném vektorovém prostoru se skalárním součinem přímo z definic plyne

$$\begin{aligned}\|u - v\|^2 &= \|u\|^2 + \|v\|^2 - 2(u \cdot v)\\ &= \|u\|^2 + \|v\|^2 - 2\|u\|\,\|v\|\cos\varphi(u, v).\end{aligned}$$

To je patrně dobře známá *kosinová věta* z rovinné geometrie.

Dále platí pro každou ortonormální bázi $\underline{e}$ zaměření V a nenulový vektor $u \in V$ vztah $\|u\|^2 = \sum_i |u \cdot e_i|^2$. Podělením této rovnice číslem $\|u\|^2$ dostáváme

$$1 = \sum_i (\cos\varphi(u, e_i))^2,$$

což je obvyklé tvrzení o směrových kosinech $\varphi(u, e_i)$ vektoru u.

Z definice odchylek vektorů nyní můžeme dovodit rozumné definice pro odchylky obecných podprostorů v libovolném euklidovském vektorovém prostoru. Je přitom třeba rozhodnutí, jak se stavět k případům, kdy podprostory mají netriviální průnik. Např. za odchylku dvou přímek budeme chtít patrně brát menší ze dvou možných úhlů, u dvou nerovnoběžných rovin v $\mathbb{R}^3$ nebudeme chtít slyšet, že mají odchylku nula, protože mají společný alespoň jeden směr:

4.16 **4.16. Definice.** Nechť U_1, U_2 jsou konečněrozměrné podprostory v euklidovském vektorovém prostoru V libovolné dimenze. *Odchylka podprostorů* U_1, U_2 je reálné číslo $\alpha = \varphi(U_1, U_2) \in [0, \frac{\pi}{2}]$ splňující:

(1) Je-li $\dim U_1 = \dim U_2 = 1$, $U_1 = \langle u \rangle$, $U_2 = \langle v \rangle$, pak

$$\cos \alpha = \frac{|u.v|}{\|u\| \|v\|}.$$

(2) Jsou-li dimenze U_1, U_2 kladné a $U_1 \cap U_2 = \{0\}$, pak je odchylka minimem všech odchylek jednorozměrných podprostorů

$$\alpha = \min\{\varphi(\langle u \rangle, \langle v \rangle); 0 \neq u \in U_1, 0 \neq v \in U_2\}.$$

Ukážeme v zápětí, že takové minimum skutečně vždy existuje.

(3) Je-li $U_1 \subset U_2$ nebo $U_2 \subset U_1$ (zejména je-li jeden z nich nulový), je $\alpha = 0$.

(4) Je-li $U_1 \cap U_2 \neq \{0\}$ a $U_1 \neq U_1 \cap U_2 \neq U_2$, pak

$$\alpha = \varphi(U_1 \cap (U_1 \cap U_2)^{\perp}, U_2 \cap (U_1 \cap U_2)^{\perp}).$$

Odchylka podprostorů $\mathcal{Q}_1$, $\mathcal{Q}_2$ v bodovém euklidovském prostoru $\mathcal{E}_n$ se definuje jako odchylka jejich zaměření $Z(\mathcal{Q}_1)$, $Z(\mathcal{Q}_2)$.

Všimněme si, že odchylka je vždy dobře definována, zejména v posledním případě je

$$(U_1 \cap (U_1 \cap U_2)^{\perp}) \cap (U_2 \cap (U_1 \cap U_2)^{\perp}) = \{0\}$$

můžeme tedy opravdu odchylku určit podle bodu (2). Všimněme si také, že v případě $U_1 \cap U_2 = \{0\}$, jsou U_1 a U_2 kolmé podle našich dřívějších definic právě, když jejich odchylka je $\pi/2$. Pokud však mají netriviální průnik, nemohou být kolmé v dřívějším smyslu.

Ke korektosti definice zbývá ukázat, že ve skutečnosti vždy existují vektory $u \in U_1$, $v \in U_2$, pro které nabývá výraz pro odchylku požadovaného minima. Nejdříve speciální případ:

4.14 **4.17. Lemma.** *Nechť v je vektor v euklidovském prostoru V a $U \subset V$ libovolný podprostor. Označme $v_1 \in U$, $v_2 \in U^{\perp}$ (jednoznačně určené) komponenty vektoru v, tj. $v = v_1 + v_2$. Pak pro odchylku φ podprostoru generovaného v od U platí*

$$\cos \varphi(\langle v \rangle, U) = \cos \varphi(\langle v \rangle, \langle v_1 \rangle) = \frac{\|v_1\|}{\|v\|}.$$

DŮKAZ. Pro všechny vektory $u \in U$ platí díky Cauchyově nerovnosti

$$\frac{|u \cdot v|}{\|u\|\|v\|} = \frac{|u \cdot (v_1 + v_2)|}{\|u\|\|v\|} = \frac{|u \cdot v_1|}{\|u\|\|v\|}$$
$$\leq \frac{\|u\|\|v_1\|}{\|u\|\|v\|} = \frac{\|v_1\|}{\|v\|} = \frac{\|v_1\|^2}{\|v\|\|v_1\|} = \frac{|v_1 \cdot v|}{\|v\|\|v_1\|}.$$

Odtud plyne

$$\cos\varphi(\langle v\rangle, \langle u\rangle) \leq \cos\varphi(\langle v\rangle, \langle v_1\rangle) = \frac{\|v_1\|}{\|v\|}$$

a námi nalezený vektor v_1 tedy představuje největší možnou hodnotu pro kosinus úhlu mezi všemi volbami vektorů z U. Protože je funkce cos na intervalu $[0, \frac{\pi}{2}]$ klesající, dostáváme tak nejmenší možný úhel a tvrzení je dokázané. □

4.14a

4.18. Výpočet odchylek. Postupu v předchozím lemmatu můžeme rozumět tak, že jednorozměrný podprostor generovaný vektorem v kolmo promítneme do podprostoru U a podíváme se, jak moc se obrazy zmenšují. Podle toho pak poznáme odchylku. Podobný postup použijeme ve vyšších dimenzích také. Potíž je přitom ale s rozpoznáním, které směry nám svými průměty odchylku skutečně prozradí. V našem předchozím případě to můžeme dobře vidět, pokud nešikovně budeme promítat větší prostor U do jednorozměrného $\langle v\rangle$ a pak kolmo zpět do U. Zjistíme, že odchylku poznáme podle směru vlastního vektoru takového zobrazení, jeho vlastní číslo bude kvadrátem příslušného kosinu úhlu.

Uvažujme tedy dva obecné podprostory U_1, U_2 v euklidovském vektorovém prostoru V, předpokládejme $U_1 \cap U_2 = \{0\}$, a zvolme pevně ortonormální báze $\underline{e}$, a $\underline{e}'$ celého prostoru V tak, aby $U_1 = \langle e_1, \dots, e_k\rangle$, $U_2 = \langle e'_1, \dots, e'_l\rangle$.

Uvažujme kolmý průmět φ prostoru V na U_2, jeho zúžení na U_1 budeme opět značit $\varphi : U_1 \to U_2$. Zobrazení $\psi : U_2 \to U_1$ nechť vznikne podobně z kolmého průmětu na U_1. Tato zobrazení mají v bazích $(e_1, \dots, e_k)$ a $(e'_1, \dots, e'_l)$ matice

$$A = \begin{pmatrix} e_1 \cdot e'_1 & \dots & e_k \cdot e'_1 \\ \vdots & & \vdots \\ e_1 \cdot e'_l & \dots & e_k \cdot e'_l \end{pmatrix}, \quad B = \begin{pmatrix} e'_1 \cdot e_1 & \dots & e'_l \cdot e_1 \\ \vdots & & \vdots \\ e'_1 \cdot e_k & \dots & e'_l \cdot e_k \end{pmatrix}$$

Protože jde o skalární součiny na reálném vektorovém prostoru, platí $e_i \cdot e'_j = e'_j \cdot e_i$ pro všechny indexy i, j a proto zejména platí $B = A^T$.

Složené zobrazení $\psi \circ \varphi : U_1 \to U_1$ má tedy symetrickou pozitivně semidefinitní matici $A^T A$ a ψ je zobrazení adjungované k φ. Viděli jsme, že každé takové zobrazení má pouze nezáporná reálná vlastní čísla a že má ve vhodné ortonormální bázi diagonální matici s těmito vlastními čísly na diagonále, viz 3.25 a 3.27.

Nyní můžeme odvodit obecný postup pro výpočet odchylky $\alpha = \varphi(U_1, U_2)$.

Věta. *V předchozím označení nechť λ je největší vlastní hodnota matice $A^T A$. Pak* $\cos^2\alpha = \lambda$

Důkaz. Nechť $u \in U_1$ je vlastní vektor zobrazení $\psi \circ \varphi$ příslušný největší vlastní hodnotě λ. Uvažme všechna vlastní čísla $\lambda_1, \dots, \lambda_k$ (včetně násobnosti) a nechť $\underline{u} = (u_1, \dots, u_n)$ je příslušná ortonormální báze U_1 z vlastních vektorů. Můžeme přímo předpokládat, že $\lambda = \lambda_1$, $u = u_1$. Potřebujeme ukázat, že odchylka libovolného $v \in U_1$ od U_2 je nejméně tak velká jako odchylka u od U_2. Tzn. že kosinus příslušného úhlu nesmí být větší. Podle předchozího lemmatu stačí diskutovat odchylku u a $\varphi(u) \in U_2$ a přitom víme, že $\|u\| = 1$. Zvolme tedy $v \in U_1$, $v = a_1u_1 + \dots + a_ku_k$, $\sum_{i=1}^k a_i^2 = \|v\|^2 = 1$. Pak

$$\begin{aligned}\|\varphi(v)\|^2 &= \varphi(v) \cdot \varphi(v) = (\psi \circ \varphi(v)) \cdot v \\ &\le \|\psi \circ \varphi(v)\| \|v\| = \|\psi \circ \varphi(v)\|.\end{aligned}$$

Předchozí lemma navíc dává i vzorec pro odchylku α vektoru v od podprostoru U_2

$$\cos\alpha = \frac{\|\varphi(v)\|}{\|v\|} = \|\varphi(v)\|.$$

Protože jsme zvolili za λ_1 největší z vlastních hodnot a součet kvadrátů souřadnic a_i^2 je jedna, dostáváme

$$\begin{aligned}(\cos\alpha)^2 = \|\varphi(v)\|^2 \le \|\psi \circ \varphi(v)\| = \sqrt{\sum_{i=1}^k (\lambda_i a_i)^2} = \\ = \sqrt{\lambda_1^2 + \sum_{i=1}^k a_i^2(\lambda_i^2 - \lambda_1^2)} \le \sqrt{\lambda_1^2}.\end{aligned}$$

Při $v = u$ dostáváme ovšem přesně $\|\varphi(v)\|^2 = \lambda_1^2\|v\|^2 = \lambda^2$ a tedy odchylka dosahuje pro tento vektor minimální možné hodnoty. Tím je věta dokázána. □

4.21

4.19. Počítání objemu. S náznakem počítání objemu jsme se již setkali v rovinné geometrii v konci páté části první kapitoly (viz 1.34). Zjistili jsme přitom, že že podstatným pojmem je přitom tzv. orientace, kterou jsme si mohli představit jako rozhodnutí, zda se na naši rovinu $\mathbb{R}^2$ díváme zhora či zezdola. Rozdíl je přitom v pořadí standardních bázových vektorů e_1 a e_2 na jednotkové kružnici.

Stejně postupujeme obecně. Říkáme, že dvě báze $\underline{u}$ a $\underline{v}$ reálného vektorového prostoru V určují stejnou *orientaci*, jestliže má matice přechodu mezi nimi kladný determinant. Formálněji vzato, orientací reálného vektorového prostoru V tedy rozumíme třídu ekvivalence bazí $\underline{u}$ vzhledem k ekvivalenci, kterou jsme pomocí znaménka determinantu právě zavedli. Ekvivalentním bazím v tomto smyslu také říkáme souhlasné se zvolenou orientací.

Přímo z definice pak vyplývá, že na každém vektorovém prostoru jsou právě dvě orientace. Z každé souhlasné báze získáme snadno nesouhlasnou pomocí libovolné matice přechodu se záporným determinantem.

Vektorový prostor se zvolenou orientací nazýváme *orientovaný vektorový prostor*.

Orientovaný (bodový) euklidovský prostor je euklidovský bodový prostor, jehož zaměření je orientované. V dalším budeme uvažovat standardní $\mathcal{E}_n$ spolu s orientací zadanou standardní bazí $\mathcal{R}^n$.

Nechť $u_1, \dots, u_k$, jsou libovolné vektory v zaměření $\mathbb{R}^n$, $A \in \mathcal{E}_n$ je libovolný bod. Rovnoběžnostěn $\mathcal{P}_k(A; u_1, \dots, u_k) \subset \mathcal{E}_n$ jsme definovali jako příklad konvexní množiny

$$\mathcal{P}_k(A; u_1, \dots, u_k) = \{A + c_1u_1 + \dots + c_ku_k; 0 \le c_i \le 1\}.$$

Jsou-li vektory $u_1, \dots, u_k$ nezávislé, hovoříme o k–rozměrném rovnoběžnostěnu $\mathcal{P}_k(A; u_1 \dots, u_k) \subset \mathcal{E}_n$. Pro dané vektory $u_1, \dots, u_k$ máme k dispozici také rovnoběžnostěny menších dimenzí

$$\mathcal{P}_1(A; u_1), \dots, \mathcal{P}_k(A; u_1, \dots, u_k)$$

v euklidovských podprostorech $A + \langle u_1 \rangle, \dots, A + \langle u_1, \dots, u_k \rangle$.

Jsou-li $u_1, \dots, u_k$ lineárně závislé definujeme objem

$$\mathrm{Vol}\, P_k = 0.$$

Jinak uvažujeme jako při Grammově–Schmidtově ortogonalizaci

$$\langle u_1, \dots, u_k \rangle = \langle u_1, \dots, u_{k-1} \rangle \oplus \langle u_1, \dots, u_{k-1} \rangle^{\perp} \cap \langle u_1, \dots, u_k \rangle.$$

V tomto rozkladu se u_k jednoznačně vyjádří jako

$$u_k = u_k' + e_k$$

kde $e_k \perp \langle u_1, \dots, u_{k-1} \rangle$. Absolutní hodnotu objemu rovnoběžnostěnu definujeme induktivně tak, abychom naplnili představu, že jde o součin objemu „základny“ a „výšky“:

$$|\mathrm{Vol}|\mathcal{P}_1(A; u_1) = \|u_1\|$$
$$|\mathrm{Vol}|\mathcal{P}_k(A; u_1, \dots, u_k) = \|e_k\| |\mathrm{Vol}|\mathcal{P}_{k-1}(A; u_1, \dots, u_{k-1}).$$

Je-li $u_1, \dots, u_n$ báze souhlasná s orientací V, definujeme (orientovaný) objem rovnoběžnostěnu

$$\mathrm{Vol}\,\mathcal{P}_k(A; u_1, \dots, u_n) = |\mathrm{Vol}|\mathcal{P}_k(A; u_1, \dots, u_n),$$

v případě neosuhlasné báze klademe

$$\mathrm{Vol}\,\mathcal{P}_k(A; u_1, \dots, u_n) = -|\mathrm{Vol}|\mathcal{P}_k(A; u_1, \dots, u_n).$$

Následující tvrzení objasňuje naše dřívější poznámky, že determinant je v jistém smyslu nástroj vyjadřující objem. První tvrzení totiž říká právě, že na k–rozměrném prostoru dostaneme objem rovnoběžnostěnu nataženého na k vektorů tak, že jejich souřadnice (v ortonormální bázi) napíšeme do sloupců matice a spočteme determinant.

Výrazu ve druhém tvrzení se říká *Grammův determinant*. Jeho výhoda je, že je zcela nezávislý na volbě báze a zejména se s ním proto lépe pracuje v případě k menšího než je dimenze celého prostoru.

Věta. *Nechť $\mathcal{Q} \subset \mathcal{E}_n$ je euklidovský podprostor a nechť $(e_1, \dots, e_k)$ je jeho ortonormální báze. Pak pro libovolné vektory $u_1, \dots, u_k \in Z(\mathcal{Q})$ a $A \in \mathcal{Q}$ platí*

$$\textit{(1)}\quad \operatorname{Vol}\mathcal{P}_k(A; u_1, \dots, u_k) = \det \begin{pmatrix} u_1 \cdot e_1 & \dots & u_k \cdot e_1 \\ \vdots & & \vdots \\ u_1 \cdot e_k & \dots & u_k \cdot e_k \end{pmatrix}$$

$$\textit{(2)}\quad (\operatorname{Vol}\mathcal{P}_k(A; u_1, \dots, u_k))^2 = \det \begin{pmatrix} u_1 \cdot u_1 & \dots & u_k \cdot u_1 \\ \vdots & & \vdots \\ u_1 \cdot u_k & \dots & u_k \cdot u_k \end{pmatrix}$$

Důkaz. Matice

$$A = \begin{pmatrix} u_1 \cdot e_1 & \dots & u_k \cdot e_1 \\ \vdots & & \vdots \\ u_1 \cdot e_k & \dots & u_k \cdot e_k \end{pmatrix}$$

má ve sloupcích souřadnice vektorů $u_1, \dots, u_k$ ve zvolené ortonormální bázi. Platí

$$\begin{aligned} |A|^2 = |A||A| = |A^T||A| = |A^T A| \\ = \det \begin{pmatrix} u_1 \cdot u_1 & \dots & u_k \cdot u_1 \\ \vdots & & \vdots \\ u_1 \cdot u_k & \dots & u_k \cdot u_k \end{pmatrix}. \end{aligned}$$

Vidíme tedy, že pokud platí (1), platí i (2).

Přímo z definice je neorientovaný objem roven součinu

$$|\operatorname{Vol}|\mathcal{P}_k(A; u_1, \dots, u_k) = \|v_1\|\|v_2\| \dots \|v_k\|,$$

kde $v_1 = u_1$, $v_2 = u_2 + a_1^2 v_1, \dots, v_k = u_k + a_1^k v_1 + \dots + a_{k-1}^k v_{k-1}$ je výsledek Grammova-Schmidtova ortogonalizačního procesu. Je tedy

$$\begin{aligned} (\operatorname{Vol}\mathcal{P}_k(A; u_1, \dots, u_k))^2 &= \det \begin{pmatrix} v_1 \cdot v_1 & 0 & \dots & 0 \\ \vdots & \ddots & & \\ 0 & 0 & \dots & v_k \cdot v_k \end{pmatrix} \\ &= \det \begin{pmatrix} v_1 \cdot v_1 & \dots & v_k \cdot v_1 \\ \vdots & & \vdots \\ v_1 \cdot v_k & \dots & v_k \cdot v_k \end{pmatrix}. \end{aligned}$$

Označme B matici jejíž sloupce jsou souřadnice vektorů $v_1, \dots, v_k$ v ortonormální bázi $\underline{e}$. Protože $v_1, \dots, v_k$ vznikly z $u_1, \dots, u_k$ jako obrazy v lineární transformaci s horní trojúhelníkovou maticí C s jedničkami na diagonále, je $B = CA$ a $|B| = |C||A| = |A|$. Pak ovšem $|A|^2 = |B|^2 = |A||A|$, proto $\operatorname{Vol}\mathcal{P}_k(A; u_1, \dots, u_k) = \pm|A|$. Přitom pokud jsou vektory $u_1, \dots, u_k$ závislé vyjde objem nulový, pokud jsou nezávislé, pak znaménko determinantu je kladné právě když je báze $u_1, \dots, u_k$ kompatibilní s orientací danou bazí $\underline{e}$. □

V geometrické formulaci dostáváme jako velice důžitý důsledek následující tvrzení:

4.20. Důsledek. *Pro každé lineární zobrazení $\varphi : V \to V$ euklidovského vektorového prostoru V je* $\det\varphi$ *roven (orientovanému) objemu obrazu rovnoběžnostěnu určeného vektory ortonormální báze. Obecněji, obraz rovnoběžnostěnu $\mathcal{P}$ určeného libovolnými* $\dim V$ *vektory má objem roven* $\det\varphi$*–násobku původního objemu.*

4.21a

4.21. Vnější a vektorový součin vektorů. Předchozí úvahy úzce souvisí s tzv. vnějším tensorovým součinem vektorů. Nebudeme zacházet podrobně do této technicky poněkud nepřehledné oblasti, ale zmíníme alespoň případ vnějšího součinu $n = \dim V$ vektorů $u_1, \dots, u_n \in V$.

Nechť $(u_{1j}, \dots, u_{nj})^T$ jsou souřadná vyjádření vektorů u_j v nějaké pevně zvolené ortonormální bázi V a M nechť je matice s prvky (u_{ij}). Pak determinant $|M|$ nezávisí na volbě báze a jeho hodnotu nazýváme *vnějším součinem vektorů* $u_1, \dots, u_n$ a značíme $[u_1, \dots, u_n]$. Vnější součin je tedy právě orientovaný objem příslušného rovnoběžnostěnu, viz 4.19.

Přímo z definice nyní vyplývají užitečné vlastnosti vnějšího součinu

(1) Zobrazení $(u_1, \dots, u_n) \mapsto [u_1, \dots, u_n]$ je antisymetrické n–lineární zobrazení. Tzn., že je lineární ve všech argumentech a výměna dvou argumentů se vždy projeví změnou znaménka výsledku.
(2) Vnější součin je nulový právě, když jsou vektory $u_1, \dots, u_n$ lineárně závislé
(3) Vektory $u_1, \dots, u_n$ tvoří kladnou bázi právě, když je jejich vnější součin kladný.

V technických aplikacích ve $\mathbb{R}_3$ se často používá velmi úzce související operace, tzv. vektorový součin, který dvojici vektorů přiřazuje vektor třetí.

Uvažme obecný euklidovský vektorový prostor V dimenze $n \geq 2$ a vektory $u_1, \dots, u_{n-1} \in V$. Dosadíme-li těchto $n-1$ vektorů jako prvních $n-1$ argumentů n–lineárníhho zobrazení definovaného pomocí determinantu při výpočtu objemu výše, pak nám zbude jeden volný argument, tj. lineární forma na V. Protože však máme k dispozici skalární součin, odpovídá každá lineární forma právě jednomu vektoru. Tento vektor $v \in V$ nazveme *vektorový součin* vektorů $u_1, \dots, u_{n-1}$, tj. pro každý vektor $w \in V$ platí

$$\langle v, w \rangle = [u_1, \dots, u_{n-1}, w].$$

Značíme $v = u_1 \times \dots \times u_{n-1}$.

Jsou-li v nějaké ortonormální bázi souřadnice našich vektorů $v = (y_1, \dots, y_n)^T$, $w = (x_1, \dots, x_n)^T$ a $u_j = (u_{1j}, \dots u_{nj})^T$, naše definice má vyjádření

$$y_1x_1 + \cdots + y_nx_n = \begin{vmatrix} u_{11} & \dots & u_{1(n-1)} & x_1 \\ \vdots & & \vdots & \vdots \\ u_{n1} & \dots & u_{n(n-1)} & x_n \end{vmatrix}.$$

Odtud je přímo vidět, že vektor v je zadán jednoznačně a jeho souřadnice spočteme formálním rozvojem tohoto determinantu podle posledního sloupce. Zároveň jsou přímo z definice očekávatelné následující vlastnosti vektorového součinu:

Věta. *Pro vektorový součin* $v = u_1 \times \dots \times u_{n-1}$ *platí*

(1) $v \in \langle u_1, \dots, u_{n-1} \rangle^{\perp}$

(2) *v je nenulový vektor právě, když jsou vektory $u_1, \dots, u_{n-1}$ lineárně nezávislé*
(3) *velikost $\|v\|$ vektorového součinu je rovna absolutní hodnotě objemu rovnoběžníku $\mathcal{P}(0; u_1, \dots, u_{n-1})$*
(4) *$(u_1, \dots, u_{n-1}, v)$ je souhlasná báze orientovaného euklidovského prostoru V.*

Důkaz. První tvrzení plyne přímo z definičního vztahu pro v, protože dosazením libovolného vektoru u_j za w máme nalevo skalární součin $v \cdot u_j$ a napravo determinant s dvěma shodnými sloupci.

Hodnost matice s $n-1$ sloupci u_j je dána maximální velikostí nenulového minoru. Minory, které zadávají souřadnice vektorového součinu jsou stupně $n-1$ a tím je dokázáno tvrzení (2).

Jsou-li vektory $u_1, \dots, u_{n-1}$ závislé, pak platí i (3). Nechť jsou tedy nezávislé, v je jejich vektorový součin a zvolme libovolnou ortonormální bázi $(e_1, \dots, e_{n-1})$ prostoru $\langle u_1, \dots, u_{n-1} \rangle$. Z již dokázáného vyplývá, že existuje nějaký násobek $(1/\alpha)v$, $0 \neq \alpha \in \mathbb{R}$, takový, že $(e_1, \dots, e_k, (1/\alpha)v)$ je ortonormální báze celého V. Souřadnice našich vektorů v této bázi jsou

$$u_j = (u_{1j}, \dots, u_{(n-1)j}, 0)^T, \quad v = (0, \dots, 0, \alpha)^T.$$

Proto je vnější součin $[u_1, \dots, u_{n-1}, v]$ roven (viz. definice vektorového součinu)

$$\begin{aligned}[u_1, \dots, u_{n-1}, v] &= \begin{vmatrix} u_{11} & \dots & u_{1(n-1)} & 0 \\ \vdots & & \vdots & \vdots \\ u_{(n-1)1} & \dots & u_{(n-1)(n-1)} & 0 \\ 0 & \dots & 0 & \alpha \end{vmatrix} \\ &= \langle v, v \rangle = \alpha^2.\end{aligned}$$

Rozvojem determinantu podle posledního sloupce zároveň obdržíme

$$\alpha^2 = \alpha \operatorname{Vol} \mathcal{P}(0; u_1, \dots, i_{n-1}).$$

Odtud už vyplývají obě zbylá tvrzení věty. □

2. Geometrie kvadratických forem

V analytické geometrii roviny jsou po přímkách jako další nejjednodušší křivky na řadě tzv. kuželosečky. Jsou v kartézkých souřadnicích zadány kvadratickými rovnicemi a podle koeficientů poznáme, zda jde o kružnici, elipsu, parabolu nebo hyperbolu, případně ještě může jít o dvě přímky nebo bod (degenerované případy).

Uvidíme, že naše nástroje umožní vcelku účinnou klasifikaci takovýchto objektů v libovolných konečných dimenzích i práci s nimi.

4.22. Kvadriky v $\mathcal{E}_n$. V analogii k rovnicím kuželoseček v rovině začneme poznámkami o objektech v euklidovských bodových prostorech, které jsou v dané ortnonormální bázi zadány kvadratickými rovnicemi, hovoříme o *kvadrikách*.

Zvolme v $\mathcal{E}_n$ pevně kartézskou souřadnou soustavu (tj. bod a ortonormální bázi zaměření) a uvažme obecnou kvadratickou rovnici pro souřadnice $(x_1, \dots, x_n)^T$ bodů $A \in \mathcal{E}_n$

$$\sum_{i,j=1}^{n} a_{ij} x_i x_j + \sum_{i=1}^{n} 2 a_i x_i + a = 0,$$

kde bez újmy na obecnosti můžeme rovnou předpokládat symetrii $a_{ij} = a_{ji}$. Tuto rovnici můžeme zapsat jako $f(u) + g(u) + a = 0$ pro kvadratickou formu f (tj. zúžení symetrické bilineární formy F na dvojice stejných argumentů), lineární formu g a skalár $a \in \mathbb{R}$ a předpokládáme že alespoň jeden z koeficientů a_{ij} je nenulový (jinak by se jednalo o lineární rovnici popisující euklidovský podprostor).

Začněme s kvadratickou částí, tj. bilineární symetrickou formou $f : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$. Stejně dobře můžeme přemýšlet o obecné symetrické bilineární formě na libovolném vektorovém prostoru.

Pro libovolnou bázi na tomto vektorovém prostoru bude hodnota $f(x)$ na vektoru $x = x_1 e_1 + \dots + x_n e_n$ dána vztahem

$$f(x) = F(x, x) = \sum_{i,j} x_i x_j F(e_i, e_j) = x^T \cdot A \cdot x$$

kde $A = (a_{ij})$ je symetrická matice s prvky $a_{ij} = F(e_i, e_j)$. Takovýmto zobrazením f říkáme *kvadratické formy* a výše uvedený vzorec pro hodnotu formy s použitím zvolených souřadnic se nazývá *analytický tvar* formy. Jestliže změníme bázi e_i na jinou bázi $e'_1, \dots, e'_n$, dostaneme pro stejný vektor jiné souřadnice $x = S \cdot x'$ (zde S je příslušná matice přechodu) a tedy

$$f(x) = (S \cdot x')^T \cdot A \cdot (S \cdot x') = (x')^T \cdot (S^T \cdot A \cdot S) \cdot x'.$$

Předpokládejme opět, že je na našem vektorovém prostoru zadán skalární součin. Předchozí výpočet pak můžeme shrnout slovy, že matice bilineární formy F a tedy i kvadratické formy f se transformuje při změně souřadnic způsobem, který pro ortogonální změny souřadnic splývá s transformací matic zobrazení (skutečně, pak je $S^{-1} = S^T$). Tento výsledek můžeme intepretovat také jako následující pozorování:

Tvrzení. *Nechť V je reálný vektorový prostor se skalárním součinem. Pak vztah*

$$\varphi \mapsto F, \quad F(u, u) = \langle \varphi(u), u \rangle$$

zadává bijekci mezi symetrickými lineárními zobrazeními a kvadratickými formami na V.

Důkaz. Skutečně, bilineární forma s pevně zadaným druhým argumentem je lineární formou $\alpha_u = F(\ , u)$ a v přítomnosti skalárního součinu je nutně dána vztahem $\alpha(u)(v) = v \cdot w$ pro vhodný vektor w. Klademe $\varphi(u) = w$. Přímo ze vztahu v souřadnicích výše pak vyplývá, že φ je lineární zobrazení s maticí A. Je tedy samoadjungované. □

Z tohoto tvrzení vyplývá okamžitý důsledek, že pro každou kvadratickou formu f existuje ortonormální báze zaměření, ve které má f diagonální matici (a diagonální hodnoty jsou jednoznačně určeny až na pořadí). Předpokládejme tedy přímo rovnici ve tvaru

$$\sum_{i=1}^{n} \lambda_i x_i^2 + \sum_{i=1}^{n} b_i x_i + b = 0.$$

V dalším kroku pro souřadnice x_i s $\lambda_i \neq 0$ provedeme doplnění do čtverců, které „pohltí" kvadráty i lineární členy týchž neznámých (tzv. Lagrangeův algoritmus, kterému se budeme obecněji věnovat níže) . Tak nám zůstanou nejvýše ty neznámé, pro které byl jejich koeficient u kvadrátu nulový, a získáme tvar

$$\sum_{i=1}^{n} \lambda_i (x_i - p_i)^2 + \sum_{j \text{ splňující } \lambda_j = 0}^{n} b_j x_j + c = 0.$$

To odpovídá posunutí počátku souřadnic o vektor se souřadnicemi p_i a zároveň volbě báze zaměření tak, abychom dostali požadovaný diagonální tvar v kvadratické části. Ve výše odvozeném ztotožnění forem s symetrickými zobrazeními to znamená, že φ je diagonální na ortogonálním doplňku svého jádra. Pokud nám opravdu zůstaly nějaké lineární členy, můžeme upravit ortonormální bázi zaměření na jádru zobrazení φ tak, aby odpovídající lineární forma byla násobkem prvního prvku duální báze. Umíme tedy již dosáhnout výsledného tvaru

$$\sum_{i=1}^{k} \lambda_i y_i^2 + b y_{k+1} + c = 0,$$

kde k je hodnost matice kvadratické formy f. Pokud je $b \neq 0$, můžeme ještě další změnou počátku dosáhnout vynulování konstanty c v rovnici.

Celkem si tedy shrňme, že lineární člen se může (ale nemusí) objevit jen pokud je hodnost f menší než n, $c \in \mathbb{R}$ může být nenulové pouze když je $b = 0$. Výsledné rovnice nazýváme *kanonickými analytickými tvary* kvadrik.

4.23. Případ $\mathcal{E}_2$. Pro ilustraci předchozího postupu projděme celou diskusi ještě jednou pro nejjednodušší případ netriviální dimenze. Původní rovnice má tvar

$$a_{11}x^2 + a_{22}y^2 + 2a_{12}xy + a_1 x + a_2 y + a = 0.$$

Volbou vhodné báze zaměření a následným doplněním čtverců dosáhneme tvaru (opět používáme stejného značení x, y pro nové souřadnice):

$$a_{11}x^2 + a_{22}y^2 + a_1 x + a_2 y + a = 0$$

kde a_i může být nenulové pouze v případě, že a_{ii} je nulové. Posledním krokem obecného postupu, tj. v dimenzi $n = 2$ jen případnou volbou posunutí, dosáhneme právě jedné z rovnic:

$0 = x^2/a^2 + y^2/b^2 + 1$	prázdná množina
$0 = x^2/a^2 + y^2/b^2 - 1$	elipsa
$0 = x^2/a^2 - y^2/b^2 - 1$	hyperbola
$0 = x^2/a^2 - 2py$	parabola
$0 = x^2/a^2 + y^2/b^2$	bod
$0 = x^2/a^2 - y^2/b^2$	2 různoběžné přímky
$0 = x^2 - a^2$	2 rovnoběžné přímky
$0 = x^2$	2 splývající přímky
$0 = x^2 + a^2$	prázdná množina

Počátek kartézkých souřadnic je *středem* zkoumané kuželosečky, nalezená ortonormální báze zaměření zadává směr *poloos*, výsledné koeficienty a, b pak dávají velikosti poloos v nedegenerovaných směrech.

4.24. Afinní pohled. V předchozích dvou odstavcích jsme hledali podstatné vlastnosti a standardizované analytické popisy objektů zadávaných v euklidovských prostorech kvadratickými rovnicemi. Hledali jsme přitom co nejjednodušší rovnice v mezích daných volností výběru kartézských souřadnic. Geometrická formulace našeho výsledku pak může být taková, že pro dva různé objekty – kvadriky, zadané v obecně různých kartézských souřadnicích, existuje *euklidovská transformace* na $\mathcal{E}_n$ (tj. afinní bijektivní zobrazení zachovávající velikosti) tehdy a jen tehdy, pokud výše uvedený algoritmus vede na stejný analytický tvar, až na pořadí souřadnic. Navíc můžeme při našem postupu přímo získat kartézské souřadnice, kterých jsou naše objekty dány výslednými kanonickými tvary, a tím i explicitní vyjádření euklidovské transformace, která naše objekty na sebe převádí (jak víme bude vždy složena z operací posunutí, otočení a zrcadlení vůči nadrovině).

Pochopitelně se můžeme ptát, do jaké míry umíme podobnou věc v afinních prostorech s volností výběru jakékoliv afinní souřadné soustavy. Např. v rovině to bude znamenat, že neumíme rozlišit kružnici od elipsy, samozřejmě bychom ale měli odlišit hyperbolu a všechny ostatní typy kuželoseček. Hlavně ale splynou mezi sebou všechny hyperboly atd.

Ukážeme si hlavní rozdíl postupu na kvadratických formách a k záležitosti se pak ještě vrátíme ve třetí části této kapitoly.

Uvažme nějakou kvadratickou formu f na vektorovém prostoru V a její analytické vyjádření $f(u) = x^T Ax$ vzhledem ke zvolené bázi na V. Pro vektor $u = x_1 u_1 + \dots + x_n u_n$ pak také zapisujeme formu f ve tvaru

$$f(x_1, n) = \sum_{ij} a_{ij} x_i x_j,$$

V předchozích odstavcích jsme již s využitím skalárního součinu ukázali, že pro vhodnou bázi bude matice A diagonální, tj. že pro příslušnou symetrickou formu F bude platit $F(u_i, u_j) = 0$ při $i \neq j$. Každou takovou bázi nazýváme *polární báze* kvadratické formy f. Samozřejmě si pro takový účel můžeme vždy skalární součin vybrat. Dokážeme si ale toto tvrzení znovu bez využití skalárních součinů tak, že získáme daleko jednodušší algoritmus na to, jak takovou polární bázi najít mezi všemi bazemi. Tím se zároveň dovíme podstatné informace o afinních vlastnostech kvadratických forem. Nasledující věta bývá v literatuře uváděna pod názvem *Lagrangeův algoritmus*.

Věta. *Nechť V je reálný vektorový prostor dimenze n, $f : V \to \mathbb{R}$ kvadratická forma. Pak na V existuje polární báze pro f.*

Důkaz. (1) Nechť A je matice f v bázi $\underline{u} = (u_1, \dots, u_n)$ na V a předpokládejme $a_{11} \neq 0$. Pak můžeme psát

$$\begin{aligned} f(x_1, \dots, x_n) &= a_{11}x_1^2 + 2a_{12}x_1x_2 + \dots + a_{22}x_2^2 + \dots \\ &= a_{11}^{-1}(a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n)^2 + \text{členy neobsahující } x_1 \end{aligned}$$

Provedeme tedy transformaci souřadnic (tj. změnu báze) tak, aby v nových souřadnicích bylo

$$x_1' = a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n,\ x_2' = x_2, \dots, x_n' = x_n.$$

To odpovídá nové bázi (spočtěte si jako cvičení příslušnou matici přechodu!)

$$v_1 = a_{11}^{-1}u_1,\ v_2 = u_2 - a_{11}^{-1}a_{12}u_1, \dots, v_n = u_n - a_{11}^{-1}a_{1n}u_1$$

a tak jak lze očekávat, v nové bázi bude příslušná symetrická bilinerání forma splňovat $g(v_1, v_i) = 0$ pro všechny $i > 0$ (přepočtěte!). Má tedy f v nových souřadnicích analytický tvar $a_{11}^{-1}x_1'^2 + h$, kde h je kvadratická forma nezávislá na proměnné x_1.

Z technických důvodů bývá lepší zvolit v nové bázi $v_1 = u_1$, opět dostaneme výraz $f = f_1 + h$, kde f_1 závisí pouze na x_1', zatímco v h se x_1' nevyskytuje. Přitom pak $g(v_1, v_1) = a_{11}$.

(2) Předpokládejme, že po provedení kroku (1) dostaneme pro h matici (řádu o jedničku menšího) s koeficientem u $x_2'^2$ různým od nuly. Pak můžeme zopakovat přesně stejný postup a získáme vyjádření $f = f_1 + f_2 + h$, kde v h vystupují pouze proměnné s indexem větším než dvě. Tak můžeme postupovat tak dlouho, až buď provedeme $n - 1$ kroků a získáme diagonální tvar, nebo v řekněme i-tém kroku bude prvek a_{ii} dosud získané matice nulový.

(3) Nastane-li poslední možnost, ale přitom existuje jiný prvek $a_{jj} \neq 0$ s $j > i$, pak stačí přehodit i-tý prvek báze s j-tým a pokračovat podle předešlého postupu.

(4) Předpokládejme, že jsme narazili na situaci $a_{jj} = 0$ pro všechny $j \geq i$. Pokud přitom neexistuje ani žádný jiný prvek $a_{jk} \neq 0$ s $j \geq i, k \geq i$, pak jsme již úplně hotovi neboť jsme již dosáhli diagonální matici. Předpokládejme, že $a_{jk} \neq 0$. Použijeme pak transformaci $v_j = u_j + u_k$, ostatní vektory báze ponecháme (tj. $x_k' = x_k - x_j$, ostatní zůstávají). Pak $h(v_j, v_j) = h(u_j, u_j) + h(u_k, u_k) + 2h(u_k, u_j) = 2a_{jk} \neq 0$ a můžeme pokračovat podle postupu v (1). □

4.25. Afinní klasifikace kvadratických forem. Po výpočtu polární báze Lagrangeovým algoritmem můžeme ještě vylepšit bázové vektory pomocí násobení skalárem tak, aby v příslušném analytickém vyjádření naší formy vystupovaly v roli koeficientů u kvadrátů jednotlivých souřadnic pouze skaláry 1, -1 a 0. Následující *věta o setrvačnosti* říká navíc, že počet jedniček a mínus jedniček nezávisí na našich volbách v průběhu algoritmu. Tyto počty nyzýváme *signaturou kvadratické formy*. Opět tedy dostáváme úplný popis kvadratických forem ve smyslu, že dvě takové formy jsou převoditelná jedna na druhou pomocí afinní transformace tehdy a jen tehdy, když mají stejnou signaturu.

Věta. *Pro každou nenulovou kvadratickou formu hodnosti r na reálném vektorovém prostoru V existuje celé číslo $0 \le p \le r$ a r nezávislých lineárních forem $\varphi_1, \dots, \varphi_r \in V^*$ takových, že*

$$f(u) = (\varphi_1(u))^2 + \dots + (\varphi_p(u))^2 - (\varphi_{p+1}(u))^2 - \dots - (\varphi_r(u))^2.$$

Jinak řečeno, existuje polární báze, ve které má f analytické vyjádření

$$f(x_1, \dots, x_n) = x_1^2 + \dots + x_p^2 - x_{p+1}^2 - \dots - x_r^2.$$

Počet p kladných diagonálních koeficientů v matici dané kvadratické formy nezávisí na volbě polární báze.

Dvě symetrické matice A, B dimenze n jsou maticemi téže kvadratické formy v různých bazích právě, když mají stejnou hodnost a když matice příslušných forem v polární bázi mají stejný počet kladných koeficientů.

Důkaz. Lagrangeovým algoritmem obdržíme $f(x_1, \dots, x_n) = \lambda_1 x_1^2 + \dots + \lambda_r x_r^2$, $\lambda_i \neq 0$, v jisté bázi na V. Předpokládejme navíc, že právě prvních p koeficientů λ_i je kladných. Pak transformace $y_1 = \sqrt{\lambda_1} x_1, \dots, y_p = \sqrt{\lambda_p} x_p$, $y_{p+1} = \sqrt{-\lambda_{p+1}} x_{p+1}, \dots, y_r = \sqrt{-\lambda_r} x_r$, $y_{r+1} = x_{r+1}, \dots, y_n = x_n$ již vede na požadovaný tvar. Formy φ_i pak jsou právě formy z duální báze ve V^* k získané polární bázi. Musíme ale ještě ukázat, že p nezávisí na našem postupu. Přepokládejme, že se nám podařilo najít vyjádření téže formy f v polárních bazích $\underline{u}$, $\underline{v}$, tj.

$$f(x_1, \dots, x_n) = x_1^2 + \dots + x_p^2 - x_{p+1}^2 - \dots - x_r^2$$
$$f(y_1, \dots, y_n) = y_1^2 + \dots + y_q^2 - y_{q+1}^2 - \dots - y_r^2$$

a označme podprostor generovaný prvními p vektory prvé báze $P = \langle u_1, \dots, u_p \rangle$, a obdobně $Q = \langle v_{q+1}, \dots, v_n \rangle$. Pak pro každý $u \in P$ je $f(u) > 0$ zatímco pro $v \in Q$ je $f(v) \le 0$. Nutně tedy platí $P \cap Q = \{0\}$ a proto $\dim P + \dim Q \le n$. Odtud plyne $p + (n - q) \le n$, tj. $p \le q$. Opačnou volbou podprostorů však získáme i $q \le p$.

Je tedy p nezávislé na volbě polární báze. Pak ovšem pro dvě matice se stejnou hodností a stejným počtem kladných koeficientů v diagonálním tvaru příslušné kvadratické formy získáme stejný analytický tvar. □

Při diskusi symetrických zobrazení jsme hovořili o definitních a semidefitních zobrazeních. Tatáž diskuse má jasný smysl i pro symetrické bilineární formy a kvadratické formy. Kvadratickou formu f forma na reálném vektorovém prostoru V nazýváme

(1) *positivně definitní*, je-li $f(u) > 0$ pro všechny $u \neq 0$
(2) *positivně semidefinitní*, je-li $f(u) \geq 0$ pro všechny $u \in V$
(3) *negativně definitní*, je-li $f(u) < 0$ pro všechny $u \neq 0$
(4) *negativně semidefinitní*, je-li $f(u) \leq 0$ pro všechny $u \in V$
(5) *indefinitní*, je-li $f(u) > 0$ a $f(v) < 0$ pro vhodné $u, v \in V$.

Stejné názvy používáme i pro symetrické reálné matice, jsou-li maticemi patřičných kvadratických forem. Signaturou symetrické matice pak rozumíme signaturu přísluąné kvadratické formy.

3. Projektivní geometrie

V mnoha elementárních textech o analytické geometrii autoři končí afinními a euklidovskými objekty popsanými výše. Na mnoho praktických úloh euklidovská nebo afinní geometrie stačí, na jiné bohužel ale nikoliv.

Tak třeba při zpracovávání obrazu z kamery nejsou zachovávány úhly a rovnoběžné přímky se mohou (ale nemusí) protínat. Dalším dobrým důvodem pro hledání širšího rámce geometrických úloh a úvah je požadovaná robustnost a jednoduchost numerických operací. Daleko jednodušší jsou totiž operace prováděné prostým násobením matic a velice těžko se totiž od sebe odlišují malinké úhly od nulových, proto je lepší mít nástroje, které takové odlišení nevyžadují.

Základní ideou projektivní geometrie je rozšíření afinních prostorů o body v nekonečnu způsobem, který bude dobře umožňovat manipulace s lineárními objekty typu bodů, přímek, rovin, projekcí, apod.

4.26. Projektivní rozšíření afinní roviny. Začneme tím nejjednodušším zajímavým případem, geometrií v rovině. Jestliže si body roviny $\mathcal{A}_2$ představíme jako rovinu $z = 1$ v $\mathcal{R}^3$, pak každý bod P naší afinní roviny představuje vektor $u = (x, y, 1) \in \mathbb{R}^3$ a tím i jednorozměrný podprostor $\langle u \rangle \subset \mathbb{R}^3$. Naopak, skoro každý podprostor v $\mathbb{R}^3$ protíná naši rovinu v právě jednom bodě P a jednotlivé vektory takového podprostoru jsou dány souřadnicemi (x, y, z) jednoznačně, až na společný skalární násobek. Žádný průnik s naší rovinou nebudou mít pouze podprostory s body o souřadnicích $(x, y, 0)$.

Projektivní rovina $\mathcal{P}_2$ je množina všech jednorozměrných podprostorů v $\mathbb{R}^3$. *Homogenní souřadnice* bodu $P = (x : y : z)$ v projektivní rovině jsou trojice reálných čísel určené až na společný skalární násobek a alespoň jedno z nich musí být nenulové. Přímka v projektivní rovině je definována jako množina jednorozměrných podprostorů (tj. bodů v $\mathcal{P}_2$)

Příklad. V afinním prostoru $\mathbb{R}^2$ uvažujme dvě přímky $L_1 : y - x - 1 = 0$ a $L_2 : y - x + 1 = 0$.
Jestliže budeme body přímek L_1 a L_2 chápat jako konečné body v projektivním prostoru $\mathcal{P}_2$, budou zjevně jejich homogenní souřadnice $(x : y : z)$ splňovat rovnice

$$L_1 : y - x - z = 0, \quad L_2 : y - x + z = 0.$$

Podívejme se, jak budou rovnice těchto přímek vypadat v souřadnicích v afinní rovině, která bude dána jako $y = 1$. Za tím účelem stačí dosadit $y = 1$ do předchozích rovnic:

$$L_1' : 1 - x - z = 0, \quad L_2' : 1 - x + z = 0$$

Nyní jsou „nekonečné“ body naší původní afinní roviny dány vztahem $z = 0$ a vidíme, že naše přímky L_1' a L_2' se protínají v bodě $(1, 1, 0)$. To odpovídá geometrické představě, že rovnoběžné přímky L_1, L_2 v afinní rovině se protínají v nekonečnu (a to v bodě $(1 : 1 : 0)$).

4.27. Projektivní prostory a transformace. Postup z roviny se přirozeným způsobem zobecňuje na každou konečnou dimenzi. Volbou libovolné afinní nadroviny $\mathcal{A}_n$ ve vektorovém prostoru $\mathbb{R}^{n+1}$, která neprochází počátkem, můžeme ztotožnit body $P \in \mathcal{A}_n$ s jednorozměrnými podprostory, které tyto generují. Zbylé jednorozměrné podprostory vyplní rovinu rovnoběžnou s $\mathcal{A}_n$ a říkáme jim „nekonečné body“ v projektivním rozšíření $\mathcal{P}_n$ afinní roviny $\mathcal{A}_n$. Zjevně je vždy množina nekonečných bodů v $\mathcal{P}_n$ projektivním prostorem dimenze o jedničku nižším. Abstraktněji hovoříme o *projektivizaci vektorového prostoru*: pro libovolný vektorový prostor V dimenze $n + 1$ definujeme

$$\mathcal{P}(V) = \{P \subset V;\ P \text{ je jednorozměrný vektorový podprostor}\}.$$

Volbou libovolné báze $\underline{u}$ ve V dostáváme tzv. *homogenní souřadnice* na $\mathcal{P}(V)$ tak, že pro $P \in \mathcal{P}(V)$ použijeme jeho libovolný nenulový vektor $u \in V$ a souřadnice tohoto vektoru v bázi $\underline{u}$. Afinní přímka má tedy ve svém projektivním rozšíření pouze jediný bod (oba konce se „potkají“ v nekonečnu a projektivní přímka vypadá jako kružnice), projektivní rovina má projektivní přímku nekonečných bodů atd.

Při zvolených homogenních souřadnicích je možné jednu z jejich hodnot zafixovat na jedničku (tj. vyloučíme všechny body projektivního prostoru s touto souřadnicí nulovou) a získáme tak vložení n–rozměrného afinního prostoru $\mathcal{A}_n \subset \mathcal{P}(V)$. To je přesně konstrukce, kterou jsme použili v opačném směru v příkladu projektivní roviny.

Každé prosté lineární zobrazení $\tau : V_1 \to V_2$ mezi vektorovými prostory samozřejmě zobrazuje jednorozměrné podprostory na jednorozměrné podprostory. Tím vzniká zobrazení na projektivizacích $T : \mathcal{P}(V_1) \to \mathcal{P}(V_2)$. Takovým zobrazením říkáme *projektivní zobrazení*. Jinak řečeno, projektivní zobrazení je takové zobrazení mezi projektivními prostory, že v každé soustavě homogenních souřadnic na definičním oboru i obrazu je toto zobrazení zadáno násobením vhodnou maticí. Obecněji, pokud naše pomocné lineární zobrazení není prosté, definuje projektivní zobrazení pouze mimo svoje jádro, tj. na bodech, jejichž homogenní souřadnice se nezobrazují na nulu.

4.28. Perspektivní projekce. Velmi dobře jsou výhody projektivní geometrie vidět na perspektivní projekci $\mathbb{R}^3 \to \mathbb{R}^2$. Bod (X, Y, Z) „reálného světa“ se promítá na bod (x, y) na průmětně takto:

$$x = -f\frac{X}{Z}, \quad y = -f\frac{Y}{Z}.$$

To je nejen nelineární formule, ale navíc při Z malém bude velice problematická přesnost výpočtů.

Při rozšíření této transformace na zobrazení $\mathcal{P}_3 \to \mathcal{P}_2$ dostáváme zobrazení $(X : Y : Z : W) \mapsto (x : y : z) = (-fX : -fY : Z)$, tj. popsané prostou lineární formulí

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -f & 0 & 0 & 0 \\ 0 & -f & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} X \\ Y \\ Z \\ W \end{pmatrix}$$

Tento jednoduchý výraz zadává perspektivní projekci pro všechny konečné body v $\mathbb{R}^3 \subset \mathcal{P}_3$, které dosazujeme jako výrazy s $W = 1$. Navíc jsme odstranili problémy s body, jejichž obraz leží v nekonečnu. Skutečně, je–li Z-ová souřadnice skutečného bodu scény blízká nule, bude hodnota třetí homogenní souřadnice obrazu mít souřadnici blízkou nule, tj. bude představovat bod blízký nekonečnu.

4.29. Afinní a projektivní transformace. Invertibilní projektivní zobrazení projektivního prostoru $\mathcal{P}_n$ na sebe odpovídají v homogenních souřadnicích invertibilním maticím dimenze $n + 1$. Dvě takové matice zadávají stejnou projektivní transformaci právě, když se liší o konstantní násobek.

Jestliže si zvolíme první souřadnici jako tu, jejíž nulovost určuje nekonečné body, budou transformace, které zachovávají konečné body, dány maticemi, jejichž první řádek musí být až na první člen nulový. Jestliže budeme chtít přejít do afinních souřadnic konečných bodů, tj. zafixujeme si hodnotu první souřadnice na jedničku, musí být první prvek na prvním řádku být také rovný jedné. Matice projektivních transformací zachovávajících konečné body tedy mají tvar:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ b_1 & a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots & \\ b_n & a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

kde $b = (b_1, \dots, b_n)^T \in \mathbb{R}^n$ a $A = (a_{ij})$ je invertibilní matice dimenze n. Působení takové matice na vektoru $(1, x_1, \dots, x_n)$ je právě obecná afinní transformace.

4.30. Projektivní klasifikace kvadrik. Závěrem ještě poznámka o složitějších objektech studovaných v afinní geometrii nejlépe prostřednictvím projektivních rozšíření. Jestliže popíšeme kvadriku v afinních souřadnicích pomocí obecné kvadratické rovnice, viz výše, jejím přepsáním v homogenních souřadnicích dostaneme vždy výlučně homogenní výraz, jehož všechny členy jsou druhého řádu. Důvod je ten, že pouze takové homogenní výrazy budou mít pro homogenní souřadnice smysl nezávisle na zvoleném konstantním násobku souřadnic $(x_0, x_1, \dots, x_n)$. Hledáme tedy takový, jehož zúžením na afinní souřadnice, tj. dosazením $x_0 = 1$, získáme původní výraz. To je ale mimořádně jednoduché, prostě dopíšeme dostatek x_0 ke všem výrazům – žádny ke kvadratickým členům, jedno k lineárním a x_0^2 ke konstantnímu členu.

Získáme tak dobře definovanou kvadratickou formu na našem pomocném vektorovém prostoru $\mathbb{R}^{n+1}$, ale jsme už vůči libovolné volbě báze klasifikovali. Zkuste si samostatně převést tuto klasifikaci do projektivní i afinní podoby. (Hezké a náročné cvičení na závěr semestru!)