Drsná matematika

Martin Panák, Jan Slovák, ...

Pokus o učebnici pro začínající studenty přírodních věd, informatiky apod. přibližující podstatnou část matematiky v rozsahu čtyř semestrálních přednášek. Text by měl být dokončen a vydán v roce 2013.

KAPITOLA 1

První krůčky k řešení matematických problémů

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

Smyslem první kapitoly této učebnice je uvést čtenáře do fascinujícího světa matematického myšlení, a to na co nejkonkrétnějších příkladech 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. I to je důvod, proč se budeme k tématům postupně vracet.

Pokud se tedy přecházení od tématu k tématu bude jevit z počátku jako chaotické, snad se to postupně spraví při návratech v pozdějších kapitolách. Název kapitoly lze chápat i jako nabádání k trpělivosti. I nejjednodušší úlohy a úvahy budou snadné jen pro ty, co už podobné řešili (a půjde pro ně jen o opakování znalosti ze střední školy). Cesta k postupnému poznání a ovládnutí matematického myšlení je možná jen pozvolna.

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 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 1.2–násobek ceny díky 20% daně z přidané hodnoty.

1.1

1.1. Vlastnosti čísel. Abychom mohli s čísly pracovat doopravdy, musíme se jejich definici a vlastnostem věnovat pořádněji. V matematice se těm nejzákladnějším vlastnostem objektů, které předpokládáme aniž bychom se zabývali jejich dokazováním, říká *axiomy*.

Uvedeme si tedy základní vlastnosti operací sčítání a násobení pro naše počty s čísly, která budeme psát jako písmena $a, b, c, \dots$. 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 dvou operací jsou uvedeny v rámečku.

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

Když komutativní okruh navíc splňuje i (P), hovoříme o *poli* (často také o *komutativním tělese*). Poslední uvedená vlastnost je slabší. Např. okruh celých čísel $\mathbb{Z}$ nesplňuje (P), ale splňuje (OI). Hovoříme o *oboru integrity*.

Všimněme si, že množina všech nenulových prvků s operací násobení splňující (O1), (O2), (03), (P) je také komutativní grupa. Jen se místo sčítání mluví o násobení. Jako přílad můžeme vzít všechna nenulová reálná čísla.

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

Všechny vlastnosti KG1–KG4, O1–O4, P, OI z rámečku 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 proto i naše výsledky budou platné pro všechny objekty s těmito vlastnostmi. V tomto je pravá síla matematických

Vlastnosti sčítání:

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

(KG2) $a+b = b+a$, pro všechny a, b

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

(KG4) pro všechny a existuje $(-a)$ takový, že $a+(-a) = 0$.

Vlastnostem (KG1) – (KG4) říkáme vlastnosti *komutativní grupy*. Jsou to po řadě *asociativita*, *komutativita*, *existence neutrálního prvku*, *existence inverzního prvku*.

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.

Poslední vlastnosti O4 se říká *distributivita* sčítání vůči násobení. Množiny s operacemi $+, \cdot$ a vlastnostmi (KG1)–(KG4), (O1)–(O4) se nazývají *komutativní okruhy*.

Další vlastnosti násobení:

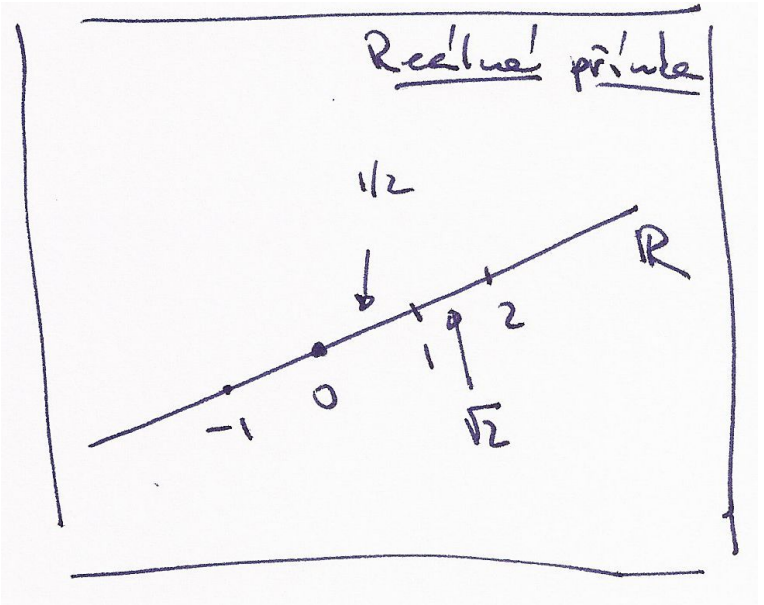
(P) pro každý $a \neq 0$ existuje a^{-1} takový, že $a \cdot a^{-1} = 1$.

(OI) $a \cdot b = 0 \quad \Rightarrow \quad$ buď $a = 0$ nebo $b = 0$.

1: *Vlastnosti skalárů*

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

K tomu aby ale skutečně bylo možné budovat matematickou teorii je třeba ověřit, že takové objekty mohou existovat.



Pro konstrukci přirozených čísel začneme s předpokladem, že víme, co jsou to množiny. Prázdnou množinu si označíme $\emptyset$ a definujeme

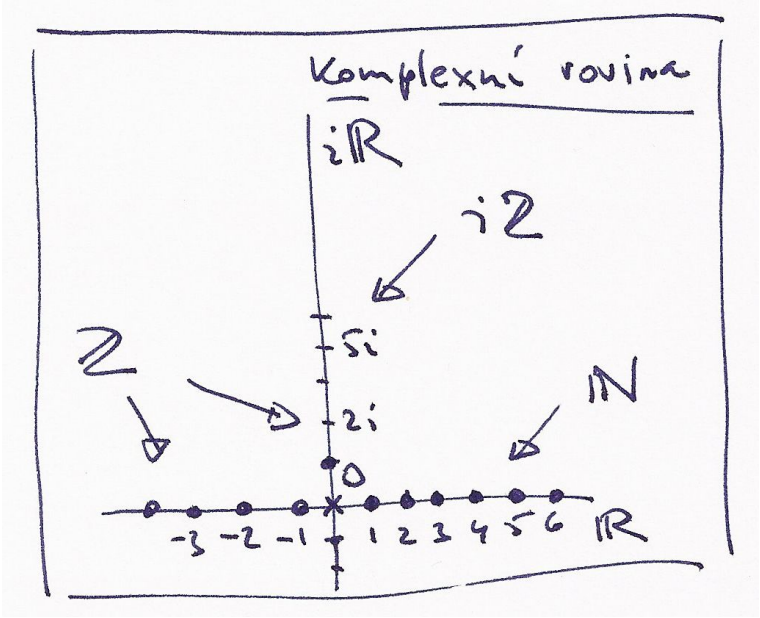
e1.1 (1.1) $\quad 0 := \emptyset,\ 1 := \{\emptyset\},\ 2 := \{\emptyset, 1\}, \ldots, n+1 := \{0, 1, \ldots, n\}.$

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

Přirozená čísla takto ztotožňujeme s mohutnostmi konkrétních konečných množin (dvě přirozená čísla a, b jsou stejná právě když příslušné množiny mají stejně prvků). 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 vlastnostní 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 podrobně zabývat a předpokládáme, že čtenář čísla racionální ($\mathbb{Q}$), reálná ($\mathbb{R}$) a komplexní ($\mathbb{C}$) důvěrně zná.

Budeme jen občas připomínat teoretické i praktické souvislosti při dalším výkladu. Podrobně bude konstrukce racionálních čísel z přirozených diskutována v 1.37. 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

1.2. 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 hodnoty 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

1.3. 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 mesíčními platy. Častěji ale máme místo hodnot pravidla, jak k hodnotám dojít.

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

$$f(0) = 1,\ \ f(n+1) = (n+1) \cdot f(n).$$

Píšeme $f(n) = n!$ a definice zjevně znamená $n! = n \cdot (n-1) \cdots 1$. Původní definice 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) a s většími 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 kartních a jiných her.

1.4

1.4. Permutace, kombinace a variace. 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. Hovoříme o *permutacích* prvků množiny S. Jestliže si předem prvky v S očíslujeme, tj. ztotožníme si S s množinou $S = \{1, \ldots, n\}$ 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 různých pořadí na konečné množině s n prvky je dán známou funkcí faktoriál:*

e1.1a

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

Dalším jednoduchým příkladem hodnoty určené formulí jsou tzv. *binomická 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 ale záleží i na pořadí vybrané k-tice prvků, hovoříme o *variaci k-tého stupně*. Jak jsme si již ověřili, počet kombinace a variace udávají následující vzorce, které také nejsou pro výpočet moc efektivní při velikých k a n, protože obsahují výrazy pro faktoriály.

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

e1.2

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

Pro variace platí

e1.2a

$$v(n,k) = n(n-1)\cdots(n-k+1) \tag{1.4}$$

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

2: *Kombinace a variace*

Binomická čísla dostala svůj název 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

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

a všimněme si, že pro odvození jsme potřebovali pouze distributivitu, komutativnost 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 **1.5. 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) 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

$$\sum_{k=0}^{n+1} \binom{n+1}{k} = \sum_{k=-1}^{n} \binom{n}{k} + \sum_{k=0}^{n+1} \binom{n}{k} = 2^n + 2^n = 2^{n+1}.$$

Prakticky stejně dokážeme i (4). Zjevně platí pro $n = 0$, předpokládejme, že platí pro nějaké n, a spočtěme příslušnou sumu pro $n + 1$ s využitím tvrzení (2). Dostaneme

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

□

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:

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

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

1.6. Permutace, kombinace a variace 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 $P(p_1, \ldots, p_k)$. 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

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

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

$$\boxed{V(n,k) = n^k.}$$

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 $0 \leq k$ a $0 < n$*

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

3: *Kombinace s opakováním*

Důkaz. Důkaz je opřen o trik (jednoduchý, když ho někdo už zná). Nechť $x_1, \ldots, x_k$ je kombinace libovolných prvků z dané množiny

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

na které si zafixujeme uvedené pořadí prvků. Jednotlivé volby x_i přidáme do pořadí $a_1, \ldots$ tam, kde je shodný prvek. Např. pro $S = \{a, b, c, d\}$ a volbu $x_1 = b$, $x_2 = c$, $x_3 = b$ dostaneme $S' = [a, b, b, b, c, c, d]$. Nyní si uvědomme, že pro rozpoznání původní kombinace nám stačí vědět, kolik je prvků v jednotlivých skupinách (je tam vždy právě o jeden prvek více než kolik patří do kombinace). Můžeme si to znázornit

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

protože příslušnost jednotlivých přihrádek k prvkům S je námi pevně zvolena.

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 $\mid$ mezi jednotlivé znaky. To odpovídá výběru $n - 1$ pozic z $n + k - 1$ možných. Protože je $c(k, n+k-1) = c(n+k-1-k, n+k-1)$, je věta dokázána. □

3. Diferenční rovnice

V předchozích odstavcích jsme viděli formule, které zadávaly hodnotu skalární funkce definované na přirozených číslech (faktoriál) nebo dvojicích čísel (binomická čísla) pomocí předcházejících hodnot. Tomu lze rozumět také tak, že místo hodnoty naší funkce zadáváme její změnu při odpovídající změně nezávislé proměnné. Porovnejte si formule v 1.4 a v 1.6. 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

1.7. Lineární 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. Je zřejmé, že takový vztah, spolu s volbou pro $f(0)$, zadává jednoznačně celou nekonečnou posloupnost hodnot

$$f(0), f(1), \ldots, f(n), \ldots.$$

Jako příklad může sloužit definiční formule pro faktoriál, tj.

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

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

Po konstantní závislosti je nejjednodušší tzv. *lineární diferenční rovnice*

e1.4

$$f(n+1) = a \cdot f(n) + b, \tag{1.6}$$

kde $a, b \in \mathbb{N}$. Takovou rovnici umíme snadno řešit, je-li $b = 0$. Pak totiž zjevně

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

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, tj.

e1.5

$$f(n+1) = a_n \cdot f(n) + b_n. \tag{1.7}$$

Pokud si budeme interpretovat lineární rovnici 1.6 jako matematický model pro spoření nebo splácení úvěru s pevnou úrokovou mírou a pevnou splátkou (tyto dva případy se liší pouze znaménkem u parametru b, tj. splátky), pak proměnné parametry povedou na 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 1.9 níže.

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

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

Důkaz. Tvrzení dokážeme matematickou indukcí. Pro zjednodušení zápisu užíváme konvenci, že konečný součin s prázdnou množinou součinitelů je roven jedné (podobně jako součet s prázdnou množinou sčítanců je roven nule). To je zapotřebí v samotné formuli v pravém sčítanci pro hodnotu $r = n - 1$, kde není žádné vyhovující i.

Zjevně pak 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 libovolné pevně zvolené n, můžeme snadno spočíst:

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

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 **1.9. 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 obecné formule dostáváme zjevně první sčítanec okamžitě. Pro vyčíslení součtu součinů v druhém 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 součet geometrické řady jsme využili existence inverze pro nenulové skaláry. To bychom nad celými čísly neuměli. Poslední výsledek tedy platí pro pole skalárů.

1.11

1.10. Rovnice druhého řádu. Uzavřeme tuto kapitolku několika poznámkami o obecnějších diferenčních rovnicích. Obecně nazýváme *diferenční rovnicí řádu k* vztah

$$f(n+k) = F(n, f(n), \dots, f(n+k-1)) = 0,$$

kde F je známá skalární funkce v $k+1$ proměnných skalárních veličinách. Stejně jako v případu rovnice prvního řádu výše je celá poslounost hodnot $f(n)$ jednoznačně určena volbou k-tice čísel $f(0), \dots, f(k-1)$.

V praktických problémech se často vyskytují vztahy závisející na dvou předchozích hodnotách. Lineární diferenční rovnicí druhého řádu rozumíme

e1.8

$$f(n+2) = a \cdot f(n+1) + b \cdot f(n) + c, \tag{1.10}$$

kde a, b, c jsou známé skalární koeficienty.

Např. v populačních modelech můžeme zohlednit, že jedinci v populaci dospívají a pořádně se rozmnožují se 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 je možná někdo pěstuje a průběžně ujídá si konstantní počet $c < 0$.

Speciálním takovým příkladem s $c = 0$ je např. Fibonacciho posloupnost čísel $y_0, y_1, \dots$, viz příklad **??**, 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 řešení podobných úloh. Zkusme proto dosadit do rovnice (1.10) s koeficientem $c = 0$ podobné řešení jako u 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 jsem 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 $\lambda_2 = \lambda_1$). A ještě k tomu potřebujeme obecně počítat nad komplexními čísly, abychom mohli spočítat všechny odmocniny. Co s tím?

Dostáváme se k velice podstatné úvaze. Dvě posloupnosti skalárů $f_1(n)$ a $f_2(n)$ můžeme sčítat po jednotlivých hodnotách a také násobit libovolnými pevně zvolenými skaláry a, b po jednotlivých hodnotách. Dostaneme pak posloupnost

$$g(n) = af_1(n) + bf_2(n).$$

Protože součet dvou řešení 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 vlastně 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). Ukažme si, že to může fungovat alespoň na jednom příkladě.

e1.9 (1.11)
$$\begin{aligned} y_{n+2} &= y_{n+1} + \frac{1}{2}y_n \\ y_0 &= 2, y_1 = 0. \end{aligned}$$

V našem případě je tedy $\lambda_{1,2} = \frac{1}{2}(1 \pm \sqrt{3})$ a zjevně $y_0 = C_1 + C_2 = 2$ a $y_1 = \frac{1}{2}C_1(1+\sqrt{3}) + \frac{1}{2}C_2(1-\sqrt{3})$ je splněno pro právě jednu volbu těchto konstant. Přímým výpočtem $C_1 = 1 - \frac{1}{3}\sqrt{3}$, $C_2 = 1 + \frac{1}{3}\sqrt{3}$.

Tento postup je velice poučný z mnoha důvodů. Na první pohled je vidět, že použitá metoda může fungovat i pro obecné lineární diferenční rovnice vyšších řádů. Vrátíme se k této problematice později.

Dále si všimněme, 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 utečou do neomezených kladných nebo záporných hodnot.

1.11

1.11. Nelineární příklad. Vraťme se na chvíli k rovnici prvního řádu, 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.

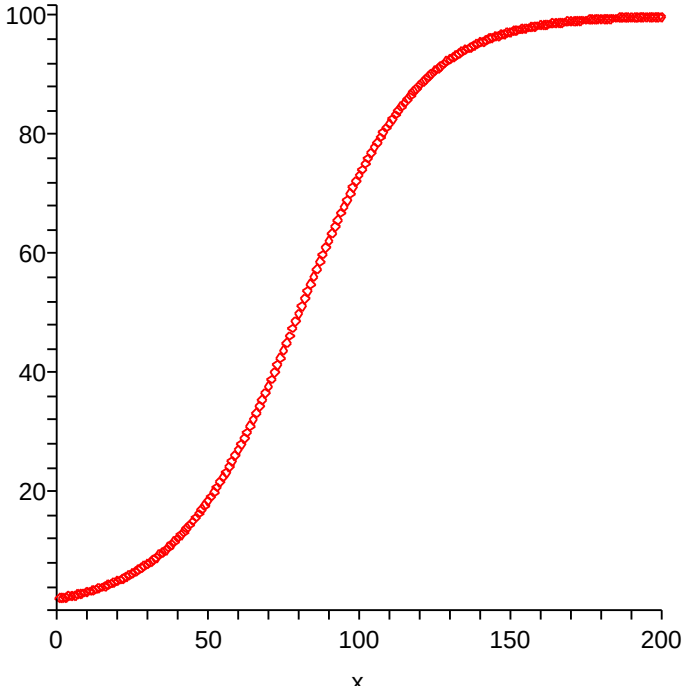
Realističtější model bude mít takto úměrnou změnu populace $\Delta p(n) = p(n+1) - p(n)$ jen při malých hodnotách p, tj. $\Delta p/p \sim r > 0$. Při určité limitní hodnotě $p = K > 0$ ale naopak už populace neroste a při ještě větších už klesá (třeba protože zdroje pro její obživu jsou omezené, jedinci ve veliké populaci si navzájem překáží apod.). Předpokládejme, že právě hodnoty $y_n = \Delta p(n)/p(n)$ závisí na $p(n)$ lineárně. Chceme tedy popsat přímku v rovině proměnných p a y, která prochází body $[0, r]$ a $[K, 0]$. Položíme proto

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

Dosazením y_n za y a $p(n)$ za p dostáváme $p(n+1) - p(n) = p(n)(-\frac{r}{K}p(n) + r)$, tj. diferenční rovnici prvního řádu

$$p(n+1) = p(n)(1 - \frac{r}{K}p(n) + r). \tag{1.12}$$

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 počáteční stav jsou právě dva jedinci.



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

1.12. Co je pravděpodobnost? Jako jednoduchý příklad může sloužit obvyklé házení kostkou s šesti stranami 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 strana 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 vybrali nedobře.

V dalším budeme pracovat s abstraktním matematickým popisem pravděpodobnosti v nejjednoduším 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 také (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 bude teorií umožňující posoudit, do jaké míry lze očekávat, že vybraný model je ve shodě s realitou, resp. umožňující určit parametry modelu tak, aby docházelo k co nejlepší shodě s pozorováním a odhadnout míru spolehlivosti. K tomu ovšem bude již potřebný 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 $p_1+p_2+p_3+p_4+p_5+p_6 = 1$. 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 abstraktně zachytit pravděpodobnostní úvahy ve formalizovaných matematických objektech. Následující odstavce tak budou ve své podstatě pouhými cvičeními v jednoduchých operacích nad množinami a kombinatorice.

1.13

1.13. 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

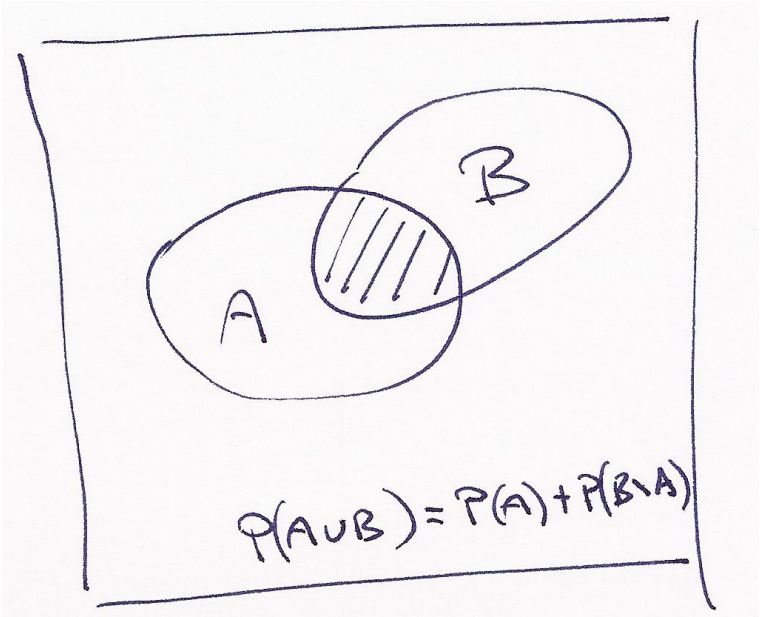
- $\Omega \in \mathcal{A}$, tj. základní prostor, je jevem,

- 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.

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 $\mathcal{A}$).

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

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



Pro naše házení kostkou je $\Omega = \{1, 2, 3, 4, 5, 6\}$ a jevové pole je tvořeno všemi podmnožinami. 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 $\{\omega\} \in \Omega$ 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 $A \subset B$,
- je-li $A \in \mathcal{A}$, pak se jev $B = \Omega \setminus A$ nazývá *opačný jev k jevu* A, píšeme $B = A^c$.

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

1.14. Definice. *Pravděpodobnostní prostor* je jevové pole $\mathcal{A}$ podmnožin (konečného) základního prostoru Ω, na kterém je definována skalární funkce $P : \mathcal{A} \to \mathbb{R}$ s následujícími vlastnosti:

- je nezáporná, tj. $P(A) \geq 0$ pro všechny jevy A,
- je aditivní, tj. $P(A \cup B) = P(A) + P(B)$, kdykoliv je $A \cap B = \emptyset$ a $A, B \in \mathcal{A}$,
- pravděpodobnost jistého jevu je 1.

Funkci P nazýváme *pravděpodobností* na jevovém poli $(\Omega, \mathcal{A})$.

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

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

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

$$P(\cup_{i\in I} A_i) = \sum_{i\in I} P(A_i), \text{ kdykoliv je } A_i \cap A_j = \emptyset,\ i \neq j,\ i, j \in I.$$

1.15. 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

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

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

1.16. Sčítání pravděpodobností. U neslučitelných jevů je sčítání pravděpodobností pro výskyt alespoň jednoho z nich přímo požadováno v základní definici pravděpodobnostního prostoru. 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.

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

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*

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

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

Skutečně, díky aditivní vlastnosti pravděpodobnosti si můžeme představit, že každý jev rozložíme na elementární (tj. jednobodové), jakkoliv ve skutečnosti nemusí jednoprvkové podmnožiny do jevového pole obecně patřit. Pak je pravděpodobnost každého jevu dána součtem pravděpodobností jednotlivých elementárních jevů do něj patřících a tvrzení věty můžeme číst následovně: sečteme všechny pravděpodobnosti výsledků ze všech 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.

Aby se takový postup stal důkazem, je zapotřebí si ujasnit, že skutečně všechny korekce, tak jak jsou napsány, 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“.

Důkaz. Pro $k = 1$ tvrzení zjevně platí a předpokládejme, že platí pro všechny počty množin menší než pevně zvolené $k > 1$. Nyní si uvědomme, že pro libovolné dva jevy platí

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

Odtud můžeme dosazením spočíst

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

a to je ale tvrzení naší věty pro $k = 2$. Nyní můžeme pracovat v indukčním kroku se vztahem pro $k + 1$ jevů, když sjednocení prvních k jevů bereme jako A ve formuli výše, zatímco zbývající jev hraje roli B:

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

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

1.17. Kombinatorický princip inkluze a exkluze. Speciálním případem předchozí věty je případ klasické pravděpodobnosti, tj. situace, kdy všechny konečné podmnožiny 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. Pak můžeme věty 1.16 vyčíst následující tvrzení pro mohutnosti obecné konečné

množiny M a jejích podmnožin $A_1, \dots, A_k$. Jako obvykla píšeme $|M|$ pro počet prvků množiny M.

e1.13a (1.13) $|M \setminus (\cup_{i=1}^k A_i)| =$

$$= |M| + \sum_{j=1}^{k} \left((-1)^i \sum_{1 \le i_1 < \dots < i_j \le k} |A_{i_1} \cap \dots \cap A_{i_j}| \right).$$

Skutečně, $|\cup_{i=1}^k A_i| + |M \setminus (\cup_{i=1}^k A_i)| = |M|$, tzn.

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

a dosazením z naší věty dostáváme právě požadované tvrzení. Říká se mu *princip inkluze a exkluze*.

1.18. Nezávislé jevy. Uvažme libovolný pravděpodobnostní prostor $(\Omega, \mathcal{A}, P)$ a v něm nějaké jevy $A_1, \dots, A_k$. 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

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

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

$$A_1 \cup \dots \cup A_k = (A_1^c \cap \dots \cap A_k^c)^c$$

a dostáváme:

e1.14a (1.14) $P(A_1 \cup \dots \cup A_k) = 1 - P(A_1^c \cap \dots \cap A_k^c) =$

$$= 1 - (1 - P(A_1)) \dots (1 - P(A_k)).$$

1.19. Podmíněná pravděpodobnost. Obvyklé je také klást dotazy s dodatečnou podmínkou. Např. „jaká je pravděpodobnost, že při hodu dvěmi kostkami padly dvě pětky, je-li součet hodnot deset?“. Formalizovat takové potřeby umíme následovně.

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

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

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

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

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.

1.20. 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 $\operatorname{vol}\Omega$ (symbol „vol“ 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.

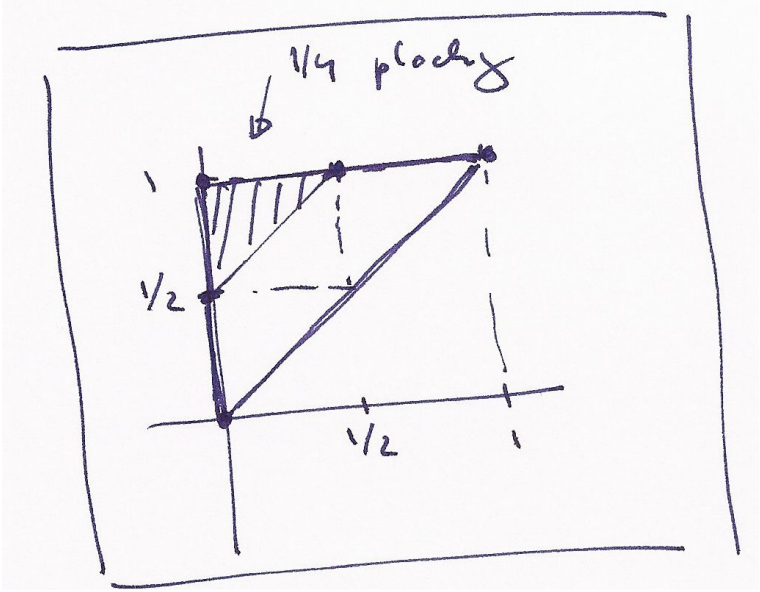
Podobně jako u klasické pravděpodobnosti pak definujeme pravděpodobnostní funkci $P : \mathcal{A} \to \mathbb{R}$ vztahem

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

Uvažme jako příklad problém, kdy náhodně vyberem 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?“.

Odpověď je docela jednoduchá: 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). Potřebujeme znát plochu podmnožiny, která odpovídá bodům s $b > a + \frac{1}{2}$, 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?“.



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 čtverce poloměru obecně. (Tady si také povšimněme východiska, které jsme nedokázali – proč by měl být obsah kruhu roven konstantnímu násobku čtverce poloměru? Matematicky to budeme umět ukázat, až zvládneme tzv. integraci. 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 $\operatorname{vol} A = \frac{1}{4}\pi$. Máme-li tedy spolehlivý generátor náhodných čísel mezi nulou a jedničkou a počítáme relativní četnosti, jak často bude vzdálenost vygenerované dvojice (a, b) menší než jedna, tj. $\sqrt{a^2 + b^2} < 1$, 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

Na konci minulé kapitoly jsme intuitivně používali elementární pojmy z geometrie reálné roviny. Budeme teď 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 $(w, z) = F(x, y)$.

1.23

1.21. 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 platit i pro naše nové sčítání vektorů. Zejména tedy máme tzv. *nulový vektor* $0 = (0, 0)$, jehož přičtením k jakémukoliv v dostaneme opět vektor v. Záměrně teď používáme tentýž symbol 0 pro vektor i jeho skalární složky – z kontextu musí být 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 zřetezení znaků $a\,v$ bude označovat skalární násobek vektoru. Přímo se ověří další vlastnosti pro násobení skaláry a, b a sčítání vektorů u, v, např.

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

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

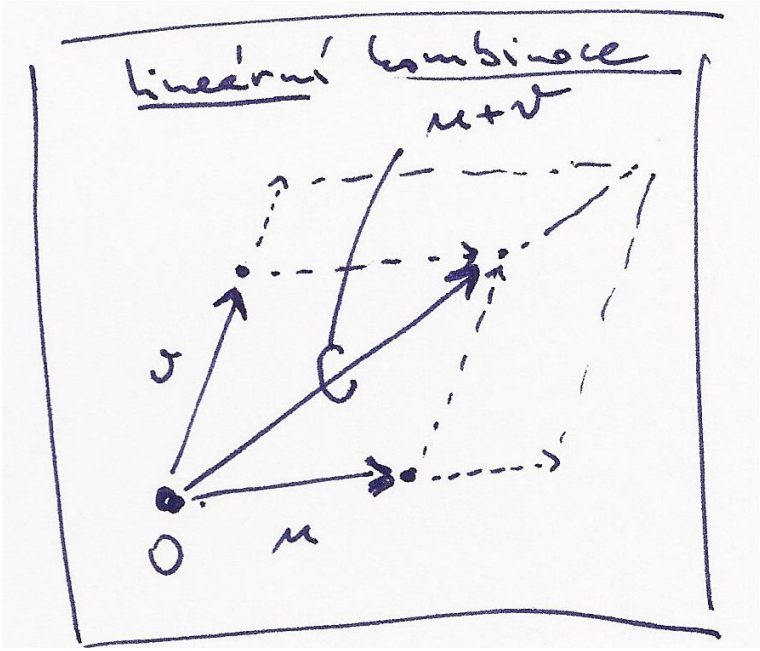
Tyto operace si můžeme dobře představit, jestliže uvažujeme vektory v jako šipky začínající v počátku $0 = (0, 0)$ a končící v bodě (x, y) v rovině. Takové šipky pak můžeme přikládat jednu za druhou a to přesně odpovídá sčítání vektorů. Násobení skalárem a pak odpovídá natažení dané šipky na a–násobek.

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

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

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

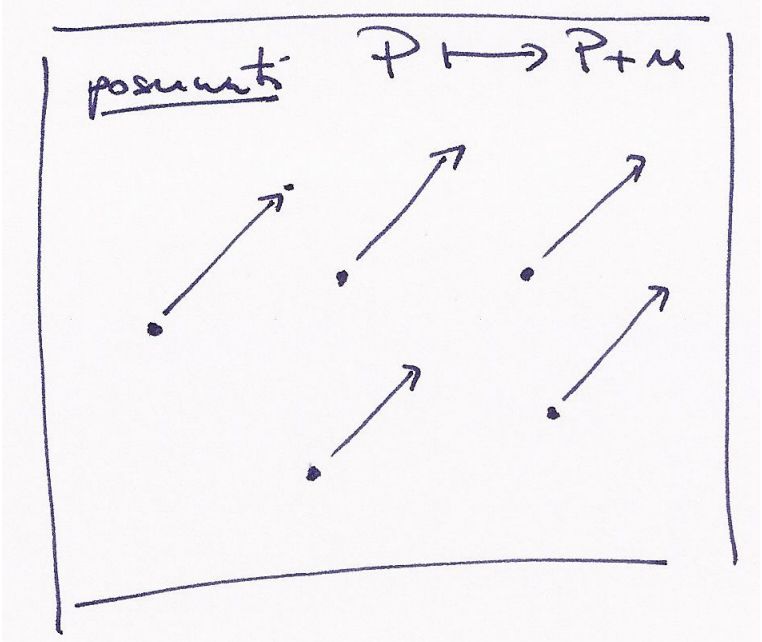
Jestliže si ale vybereme jiné dva vektory u, v, které nejsou jeden násobek druhého, tj. jinou bázi, budeme moci udělat totéž. Lineární kombinace $w = x\, u + y\, v$ nám pro všechny různé dvojice (x, y) dá právě všechny vektory w v rovině.



Nakonec můžeme nahlížet vektory jako naše šipky v abstraktní poloze, tj. zapomeneme na ztotožnění bodů v rovině s dvojicemi čísel. Zůstanou nám operace sčítání a násobení skaláry a teprve volbou báze e_1, e_2 ztotožníme naši rovinu šipek s $\mathbb{R}^2$.

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

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 v tom druhém.

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 $[a, b]$, které 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 závokami místo hranatých u souřadnic bodů v afinní rovině.

1.24

1.23. 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 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 $v = (\alpha, \beta)$:

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

Jednoduchým výpočtem dostaneme (vyloučíme t z parametrického vyjádření pro x a y, když pro určitost předpokládáme, že třeba $\alpha \neq 0$)

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

To je obecná rovnice přímky

e1.12 (1.15) $$ax + by = c,$$

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

e1.13 (1.16) $$a\alpha + b\beta = 0.$$

Výraz nalevo v rovnici přímky (1.15) 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, pro které body bude tato konstanta nula.

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 naráz. Pišme je takto

e1.14

$$\begin{aligned} ax + by &= r \\ cx + dy &= s. \end{aligned} \tag{1.17}$$

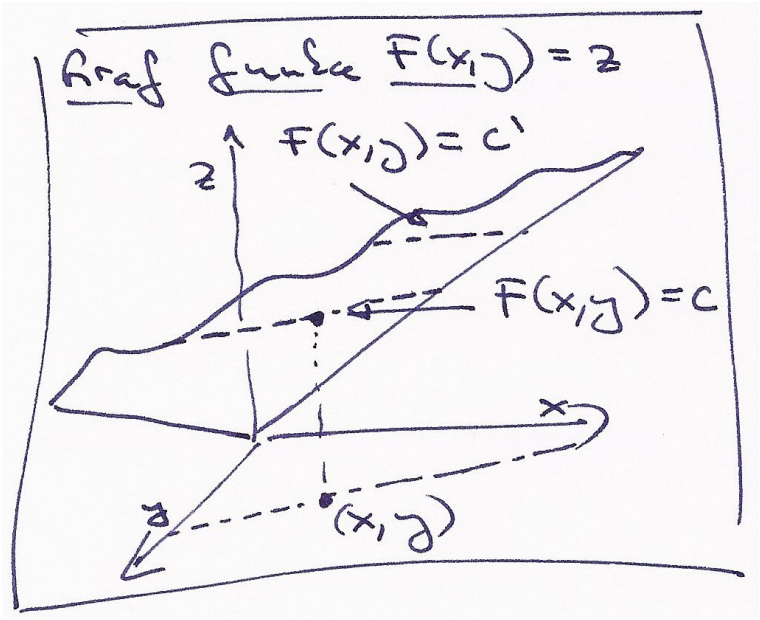
Opět můžeme levou stranu vnímat jako přiřazení, které každé dvojici souřadnic $[x, y]$ bodů P v rovině přiřadí vektor hodnot dvou skalárních funkcí F_1 a F_2 daných levými stranami jednotlivých rovnic (1.17). Můžeme tedy naše rovnice napsat jako jediný vztah $F(v) = w$, kde F je přiřazení, které vektor 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

1.24. 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:

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

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 $F : \mathbb{R}^2 \to \mathbb{R}^2$. Obdobně, v rovnici 1.15 pro přímku 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 vektoru B. 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 ale 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 $w^T = (a\ b)$ 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):

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

Stejně snadno je vidět i distributivita $A \cdot (B + C) = A \cdot B + A \cdot C$, neplatí však komutativita a existují „dělitelé nuly“. Např.

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

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

$$w^T \cdot v = \begin{pmatrix} a & b \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = c, \quad A \cdot v = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} r \\ s \end{pmatrix} = u$$

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 pomocí vztahu

e1.15

$$ad - bc = 0 \tag{1.18}$$

tj. vyjádření, kdy jsou nalevo v rovnicích (1.17) stejné výrazy až na skalární násobek (nebo jinak řečeno, sloupce matice A jsou stejné až na skalární násobek). V takovém případě bud nebude v průniku žádný bod (rovnoběžné různé přímky) nebo tam budou všechny body přímky (stejné přímky). Ověřte!

1.25a

1.25. Determinant matice. Výrazu nalevo v (1.18) říkáme *determinant* matice A a píšeme pro něj $\det A = ad - bc$, případně

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

Naši úvahu 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. Nad celými čísly obecně neplatí – když prostě spočteme pro rovnice s celočíselnými koeficienty výsledek, tak celočíselný být nemusí.

1.25b

1.26. Afinní zobrazení. Posunutí v afinní rovině $\mathbb{R}^2$ o pevný vektor $t = (r, s) \in \mathbb{R}^2$ umíme v maticové formě snadno zapsat takto:

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

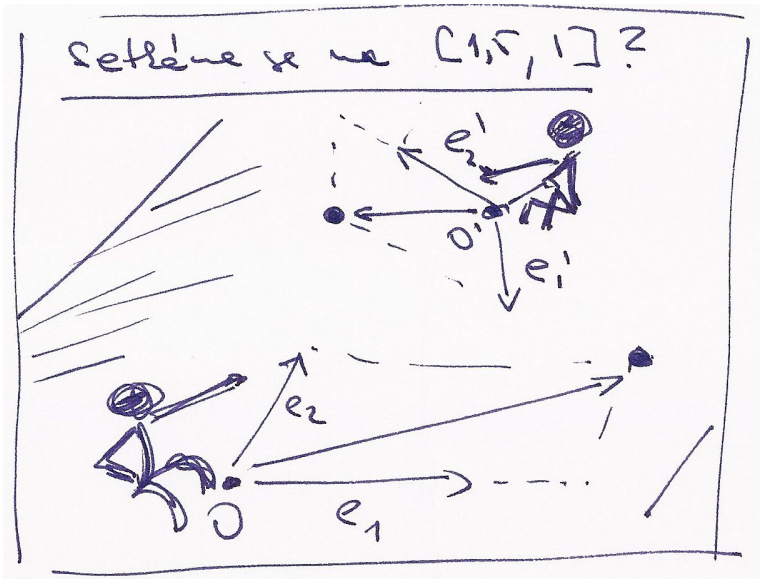
Jestliže k výsledku lineárního zobrazení ještě dovolíme přičíst pevný vektor $t = (r, s)$, pak naše zobrazení bude mít tvar

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

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

Známými příklady jsou všechny afinní podobnosti. Lineární zobrazení samozřejmě odpovídají právě těm afinním zobrazením, které zachovávají pevný počátek O, tj. nezahrnují žádné posunutí.

Jsou to právě ta zobrazení, která potřebujeme k přepočítávání souřadnic vzniklých různými volbami počátků a bází směrů pro posunutí. Co se stane, když náš pozorovatel z odstavce 1.21 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

1.27. 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 větu. Odtud vyjde právě výše uvedený vzorec.

Náš pozorovatel roviny 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 trojůhelníku o stranách s velikostmi 3, 4 a 5 zkonstruuje kolmý vektor o velikosti jedna a dále pokračuje jako výše.

Euklidovská rovina je afinní rovina se zavedeným pojmem vzdálenosti.

1.26a

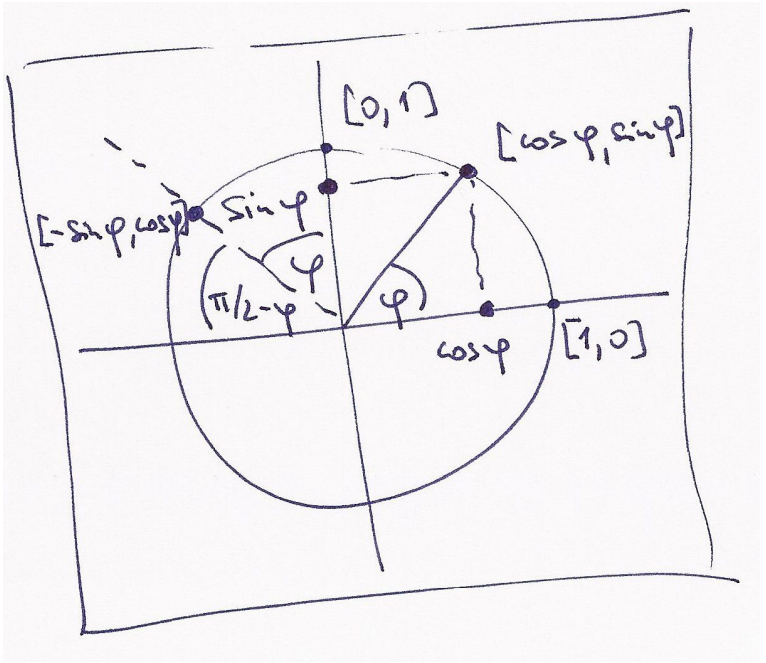
1.28. Úhel vektorů. Úhel φ dvou vektorů v, w v rovině zpravidla popisujeme s využitím tzv. goniometrické funkce $\cos\varphi$. Jak jsem již využívali při diskusi komplexních čísel coby bodů v rovině, vzorec pro funkci cos je dán hodnotou reálné první souřadnice jednotkového vektoru, jehož úhel s vektorem $(1, 0)$ je φ. Zjevně je pak druhá souřadnice takového vektoru dána reálnou hodnotou $0 \leq \sin\varphi \leq 1$ 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 $(1, 0)$ a náš vzorec uř je pouze opakováním definice funkce cosinus.

Zmíněné otočení je pak samozřejmě příkladem lineárního zobrazení, které zachovává velikosti, tj. zobrazení $F : \mathbb{R}^2 \to \mathbb{R}^2$, pro které platí, že $\|F(u)\| = \|u\|$.



1.26b

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

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

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

4: *Matice rotace*

Pokud bychom chtěli zapsat rotaci kolem jiného bodu $P = O + w$, $P = [w_x, w_y]$, snadno opět napíšeme potřebný vzorec pro matici pomocí translací. Stačí si ktomu 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. Počítejme:

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

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 translací, 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

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

a obecně můžeme psát (otočíme do „nulové“ polohy, odzrcadlíme a vrátíme zpět)

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

Můžeme proto (díky asociativitě násobení matic) spočíst:

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

Použili jsme přitom obvyklé součtové vzorce pro goniometrické funkce. Povšimněme si také, že

$$Z_\psi \cdot Z_0 = \begin{pmatrix} \cos 2\psi & \sin 2\psi \\ \sin 2\psi & -\cos 2\psi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos 2\psi & -\sin 2\psi \\ \sin 2\psi & \cos 2\psi \end{pmatrix}.$$

Toto pozorování lze zformulovat jako

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 zhrát 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

1.30. Věta. *Lineární zobrazení euklidovské roviny je složeno ze 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 přitom právě tehdy, když je determinant matice R roven jedné, což odpovídá sudému počtu zrcadlení. Při lichém počtu zdrcadlení je determinant roven -1.

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 první tvrzení dokazované věty.

Díky vztahu $a^2 + c^2 = 1$ můžeme předpokládat, že $a = \cos\varphi$ pro vhodný úhel a $c = \sin\varphi$. Jakmile takto zvolíme první sloupec matice A, 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 A:

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

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 1.29, každá rotace odpovídá dvěma zrcadlením

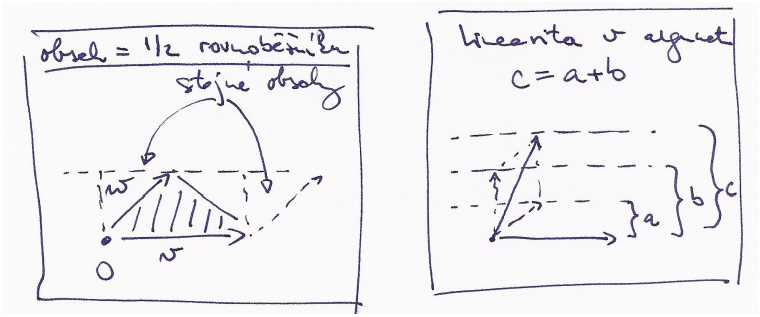
a determinant je v těchto dvou případech skutečně jedna nebo minus jedna a rozlišuje je. □

1.28

1.31. Obsah trojúhelníka. Závěrem našeho malého výletu do geometrie se zaměřme na pojem 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 $\operatorname{vol}\Delta(v,w)$ 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 (nebo prostě vidí z obrázku), že nutně platí

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



Přidejme ještě 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 $v = (1,0)$ a $w = (0,1)$ a evidentně tedy každá možnost pro $\operatorname{vol}\Delta$ je jednoznačně určena už vyčíslením na těchto vektorech. Protože ale pro obsah, stejně jako pro determinant, je zjevně

$\operatorname{vol}\Delta(v,v) = \operatorname{vol}\Delta(w,w) = 0$ (kvůli požadované antisymetrii), je nutně každá taková skalární funkce jednoznačně zadána hodnotou na jediné dvojici argumentů (v,w). Jsou si tedy všechny možnosti rovny až na skalární násobek. Ten umíme určit požadavkem

$$\operatorname{vol}\Delta(v,w) = \frac{1}{2},$$

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

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

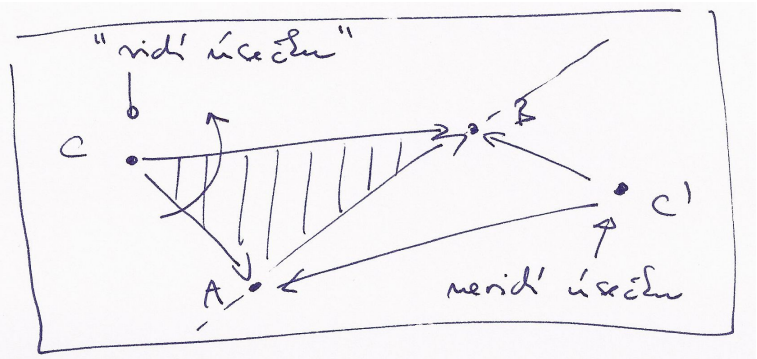
1.29

1.32. Viditelnost v rovině. Předchozí popis hodnot pro orientovaný objem nám dává do rukou elegantní nástroj pro určování viditelnosti orientovaných úseček. Orientovanou úsečkou rozumíme dva body v rovině $\mathbb{R}^2$ s určením pořadím. Můžeme si ji představovat jako šipku od prvého k druhému bodu. Taková orientovaná úsečka nám rozděluje rovinu na dvě poloroviny, říkejme jim „levou“ a „pravou“.

Jestliže uvažujeme obvyklou orientaci „proti směru hodinových ručiček“ pro hranici mnohoúhelníku, pak pozorovatel nalevo od orientované úsečky (tj. uvnitř takového mnohoúhelníka) tuto vidí a naopak pozorovatel napravo ji nevidí. Má tedy smysl ptát se, jestli je orientovaná úsečka $[A,B]$ v rovině viditelná z bodu C.

Spočtěme orientovanou plochu příslušného trojúhelníku zadaného vektory $A-C$ a $B-C$. Pokud jsme s bodem C nalevo od úsečky, pak při naší orientaci bude vektor $A-C$ dříve než ten druhý a proto výsledná plocha (tj. hodnota determinantu) bude kladná. To odpovídá situaci, kdy úsečku vidíme. Naopak, při opačné poloze bude výsledkem záporná hodnota determinantu a podle záporné hodnoty determinantu zjistíme, že úsečku nevidíme.

Uvedený jednoduchý postup je 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

1.33. Relace mezi množinami. *Binární relací* mezi množinami A a B rozumíme 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

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

Podobně *oborem hodnot relace* je podmnožina

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

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

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

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*
- *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

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

známe také pod názvem *graf zobrazení* f.

1.31

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

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

Ve značení používaném pro relace totéž můžeme zapsat jako

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

Zcela obdobně definujeme *skládání relací*, v předchozích vztazích jen doplníme existenční kvantifikátory, tj. musíme uvažovat všechny „vzory“ a všechny „obrazy“.Uvažme relace $R \subset A \times B$, $S \subset B \times C$. Potom

$$S \circ R \subset A \times C, \quad S \circ R = \{(a, c); \exists b \in B, (a, b) \in R, (b, c) \in S\}.$$

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 $R \subset A \times B$ 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 inverzní 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

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

- *reflexivní*, pokud $\mathrm{id}_A \subset R$ (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 $R^{-1} \cap R \subset \mathrm{id}_A$ (tj. pokud $(a,b) \in R$ a zároveň $(b,a) \in R$, pak $a = b$),
- *tranzitivní*, pokud $R \circ R \subset R$, 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.

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 $A \to B$) a na ní relací $X \subset Z$ danou vlastností „být podmnožinou“. Evidentně jsou splněny všechny tři vlastnosti pro uspořádání: skutečně, je–li $X \subset Y$ a zároveň $Y \subset X$ musí být nutně množiny X a Y stejné. Je–li $X \subset Y \subset Z$ je také $X \subset Z$ a také reflexivita je zřejmá.

Říkáme, že uspořádání je *úplné*, když pro každé dva prvky 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 $X \subset Y$ ani $Y \subset X$.

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

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

Definujeme relaci $m < n$ právě, když $m \in n$. 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

1.36. Rozklad podle ekvivalence. Každá ekvivalence R na množině A zadává zároveň *rozklad* množiny A na podmnožiny vzájemně ekvivalentních prvků, tzv. *třídy ekvivalance*. Klademe pro libovolné $a \in A$

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

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 podmnožina 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 suktečně rozloží na jednotlivé třídy.

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

1.34

1.37. Příklad – konstrukce celých a racionálních čísel. Na přirozených číslech umíme sice sčítat a víme, že přičtením nuly se číslo nezmění. Umíme i definovat odečítání, při něm ale jen někdy existuje výsledek.

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 v pravo 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 přklad 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 1.1 a 1.2. 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. Zároveň si povšimněte, že platí vlastnost oboru integrity (OI), viz 1.2, 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 $\mathbb{N}$. 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.

1.38. Příklad – zbytkové třídy. Jiným dobrým a jednoduchým příkladem jsou tzv. zbytkové třídy celých čísel. Pro pevně zvolené přirozené číslo k definujeme equivalenci $\sim_k$ 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 definovat násobení a sčítání. Zkuste si ověřit, že výsledná množina „skalárů“ je komutativním tělesem (tj. splňuje i vlastnost (P) z 1.2) právě když je k prvočíslo.

Literatura

[1] Marie Budíková, Štěpán Mikoláš, Pavel Osecký, Teorie pravděpodobnosti a matematická statistika (sbírka příkladů), Masarykova univerzita, 3. vydání, 2004, 117 stran, ISBN 80-210-3313-4.

[2] Marie Budíková, Štěpán Mikoláš, Pavel Osecký, Popisná statistika, Masarykova univerzita, 3. vydání, 2002, 48 stran, ISBN 80-210-1831-3.

[3] Marie Budíková, Tomáš Lerch, Štěpán Mikoláš, Základní statistické metody, Masarykova univerzita, 2005, 170 stran, ISBN 80-210-3886-1.

[4] Zuzana Došlá, Jaromír Kuben, Diferenciální počet funkcí jedné proměnné, MU Brno, 2003, 215 s., ISBN 80-210-3121-2.

[5] Zuzana Došlá, Roman Plch, Petr Sojka, Diferenciální počet funkcí více proměnných s programem Maple, MU Brno, 1999, 273 s.

[6] William J. Gilbert, W. Keith Nicholson, Modern algebra with applications, 2nd ed. John Wiley and Sons (Pure and applied mathematics) ISBN 0-471-41451-4

[7] Pavel Horák, Úvod do lineární algebry, MU Brno, skripta.

[8] Ivana Horová, Jiří Zelinka, Numerické metody, MU Brno, 2. rozšířené vydání, 2004, 294 s., ISBN 80-210-3317-7.

[9] Jiří Matoušek, Jaroslav Nešetřil, Kapitoly z diskrétní matematiky, Univerzita Karlova v Praze, Karolinum, Praha, 2000, 377 s.

[10] Luboš Motl, Miloš Zahradník, Pěstujeme lineární algebru, 3. vydání, Univerzita Karlova v Praze, Karolinum, 348 stran (elektronické vydání také na http://www.kolej.mff.cuni.cz/~lmotm275/skripta/).

[11] Riley, K.F., Hobson, M.P., Bence, S.J. Mathematical Methods for Physics and Engineering, second edition, Cambridge University Press, Cambridge 2004, ISBN 0 521 89067 5, xxiii + 1232 pp.

[12] František Šik, Lineární algebra zaměřená na numerickou analýzu, MU, 1998, 176 s. ISBN 80-210-1996-2.

[13] Jan Slovák, Lineární algebra. učební texty, Masarykova univerzita, elektronicky dostupné na www.math.muni.cz/~slovak

[14] Pavol Zlatoš, Lineárna algebra a geometria, skripta MFF Univerzity komenského v Bratislavě.

[15] Karel Zvára, Josef Štěpán, Pravděpodobnost a matematická statistika, Matfyzpress, Universita Karlova, 2006, 230 s.