0. ZÁKLADNÉ POJMY Z LOGIKY A TEÓRIE MNOŽÍN

V tejto kapitole zavedieme niektoré základné logické a množinové pojmy a dohodneme sa na štandardnej symbolike, ktorú budeme ďalej používať. Nebudeme však systematicky budovať axiomatickú *teóriu množín*, práve naopak, s množinami budeme narábať skôr intutívne. Čitateľ, ktorý základné množinové pojmy ovláda, môže túto kapitolu vynechať, prípadne ju len letmo prelistovať, aby sa oboznámil s našou terminológiou a symbolikou.

0.1. Logické spojky a kvantifikátory

Kvôli prehľadnosti budeme niektoré matematické tvrdenia zapisovať v symbolickej podobe ako *matematické formuly*. S príkladmi rôznych formúl sa ešte stretneme. V tejto chvíli sa zameriame len na spôsob, ako možno z daných tvrdení či formúl tvoriť nové pomocou *logických spojok* a *kvantifikátorov*.

Nech P, Q sú ľubovoľné tvrdenia.

(a) Tvrdenie, ktoré je pravdivé práve vtedy, keď tvrdenie P je nepravdivé, nazývame *negáciou* tvrdenia P, značíme ho $\neg P$ a čítame ho „nie P“, prípadne „non P“.
(b) Tvrdenie, ktoré je pravdivé práve vtedy, keď sú pravdivé obe tvrdenia P, Q, nazývame *konjunkciou* alebo *logickým súčinom* tvrdení P, Q, značíme ho $P \mathbin{\&} Q$ a čítame „P a zároveň Q“, krátko len „P a Q“, prípadne „P et Q“.
(c) Tvrdenie, ktoré je pravdivé práve vtedy, keď je pravdivé aspoň jedno z tvrdení P, Q, nazývame *alternatívou* alebo *disjunkciou* či *logickým súčtom* tvrdení P, Q, značíme ho $P \vee Q$, a čítame „P alebo Q“, prípadne „P vel Q“.
(d) Tvrdenie $\neg P \vee Q$ skrátene označujeme $P \Rightarrow Q$ a nazývame ho *implikáciou* tvrdení P, Q. Výraz $P \Rightarrow Q$ čítame „ak P, tak Q“ alebo „z P vyplýva Q“, prípadne „P implikuje Q“. Tvrdenie P nazývame *predpokladom* a tvrdenie Q *záverom* implikácie $P \Rightarrow Q$. Uvedomte si, že implikácia $P \Rightarrow Q$ je nepravdivá jedine v tom prípade, ak predpoklad P je pravdivý a záver Q je nepravdivý.
(e) Tvrdenie $(P \Rightarrow Q) \mathbin{\&} (Q \Rightarrow P)$ skrátene označujeme $P \Leftrightarrow Q$ a nazývame ho *ekvivalenciou* tvrdení P, Q. Výraz $P \Leftrightarrow Q$ čítame „P práve vtedy, keď Q“, prípadne „P je ekvivalentné s Q“. Zrejme ekvivalencia $P \Leftrightarrow Q$ je pravdivá vtedy a len vtedy, keď tvrdenia P, Q sú zároveň obe pravdivé alebo zároveň obe nepravdivé.

Znaky $\neg$, $\&$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ nazývame *logickými spojkami.* V literatúre sa možno tiež stretnúť s označením P', $-P$ alebo $\sim P$ pre negáciu, $P \wedge Q$ pre konjunciu, $P \to Q$ alebo $P \supset Q$ pre implikáciu a $P \leftrightarrow Q$ alebo $P \equiv Q$ pre ekvivalenciu.

Okrem tvrdení zapisujeme formulami aj vlastnosti objektov a vzťahy medzi nimi. Na tento účel používame formuly s *voľnými premennými.* Označujeme ich $P(x)$, $Q(x,y)$, $R(x_1,\dots,x_n)$ a pod. Dosadením konkrétnych objektov do formúl namiesto voľných premenných dostávame tvrdenia. Napríklad, ak $Q(x,y)$ je formula s voľnými premennými x, y a a, b sú nejaké objekty, tak $Q(a,b)$ je tvrdenie, ktoré je pravdivé práve vtedy, keď sa objekty a, b nachádzajú vo vzťahu označenom formulou Q.

Zrejme aj na formuly s voľnými premennými možno aplikovať logické spojky, ktoré si pritom zachovajú svoj doterajší význam. Popri logických spojkách možno z formúl tvoriť nové formuly či tvrdenia aj pomocou *kvantifikátorov.*

Nech $P(x)$ je ľubovoľná formula.

(a) Tvrdenie „existuje x také, že $P(x)$“ skrátene zapisujeme $(\exists\, x)P(x)$.
(b) Tvrdenie „pre každé (pre všetky) x platí $P(x)$“ skrátene zapisujeme $(\forall\, x)P(x)$.

Znaky $\exists$ resp. $\forall$ sú *kvantifikátory*; $\exists$ nazývame *existenčný* a $\forall$ *univerzálny* alebo tiež *všeobecný kvantifikátor.* Zrejme premenná x už nie je vo formulách $(\forall\, x)P(x)$ a $(\exists\, x)P(x)$ voľná ale *viazaná*; ak x je jediná voľná premenná vo formule $P(x)$, tak $(\forall\, x)P(x)$ a $(\exists\, x)P(x)$ sú tvrdenia. Oba uvedené kvantifikátory sú zviazané pravidlami negácie kvantifikovaných formúl:

$$\neg(\exists\, x)P(x) \;\Leftrightarrow\; (\forall\, x)\neg P(x),$$
$$\neg(\forall\, x)P(x) \;\Leftrightarrow\; (\exists\, x)\neg P(x).$$

Pomocou existenčného a univerzálneho kvantifikátora už vieme vyjadriť i *kvantifikátor jednoznačnej existencie.* Ak $P(x)$ je nejaká vlastnosť, tak tvrdenie „existuje práve jedno x také, že $P(x)$“, t. j. tvrdenie

$$(\exists\, x)(P(x) \mathbin{\&} (\forall\, y)(P(y) \Rightarrow y = x)),$$

skrátene zapisujeme v tvare $(\exists! x)P(x)$. Toto tvrdenie je zrejme ekvivalentné s tvrdením

$$(\exists\, x)(\forall\, y)(P(y) \Leftrightarrow y = x).$$

0.2. Množiny

Pod *množinou* rozumieme ľubovoľné jednoznačne vymedzené zoskupenie nejakých (často i značne rôznorodých) objektov – *prvkov množiny* – chápané ako jediný objekt. Množiny budeme väčšinou značiť veľkými latinskými písmenami, ich prvky malými písmenami.

Tvrdenie „objekt x je prvkom množiny X“, zapisujeme $x \in X$; hovoríme tiež, že *x patrí* do množiny X. Tvrdenie „objekt x nie je prvkom množiny X“, t. j. x nepatrí do množiny X, zapisujeme $x \notin X$.

Množina je jednoznačne zadaná zoskupením svojich prvkov. Preto dve množiny, nezávisle od spôsobu ich zadania, považujeme za totožné, ak majú tie isté prvky. Pre ľubovoľné množiny X, Y teda platí

$$X = Y \;\Leftrightarrow\; (\forall\, x)(x \in X \Leftrightarrow x \in Y).$$

Túto vlastnosť množín nazývame *extenzionalitou.*

Hovoríme, že množina X je *podmnožinou* množiny Y, označenie $X \subseteq Y$, ak každý prvok množiny X patrí aj do množiny Y, t. j.

$$X \subseteq Y \;\Leftrightarrow\; (\forall\, x)(x \in X \Rightarrow x \in Y).$$

Vzťah $\subseteq$ nazývame *vzťahom inklúzie* Extenzionalitu množín teraz možno skrátene vyjadriť v tvare konjunkcie dvoch inklúzií

$$X = Y \;\Leftrightarrow\; X \subseteq Y \mathbin{\&} Y \subseteq X.$$

Kvantifikácie uvedené v predchádzajúcom paragrafe sa nazývajú *neohraničené*, lebo oblasť pôsobnosti kvantifikátorov v nich nebola nijako ohraničená. V matematike (i v bežnom živote) sa však častejšie vyskytujú *ohraničené kvantifikácie*, v ktorých je oblasť pôsobnosti príslušného kvantifikátora ohraničená nejakou množinou X. Ide o kvantifikácie tvaru $(\exists\, x \in X)$, $(\forall\, x \in X)$ a $(\exists !x \in X)$, ktoré čítame postupne „existuje x z množiny X“, „pre každé (pre všetky) x z množiny X“, resp. „existuje práve jedno (jediné) x z množiny X“. Tieto kvantifikácie možno vyjadriť pomocou neohraničených kvantifikácii nasledujúcim spôsobom: Ak $P(x)$ je ľubovoľná vlastnosť a X je množina, kladieme

$$\begin{aligned}
(\exists\, x \in X)P(x) \;&\Leftrightarrow\; (\exists\, x)(x \in X \;\&\; P(x)),\\
(\forall\, x \in X)P(x) \;&\Leftrightarrow\; (\forall\, x)(x \in X \;\Rightarrow\; P(x)),\\
(\exists !x \in X)P(x) \;&\Leftrightarrow\; \big(\exists\, x \in X\big)\big(P(x) \;\&\; (\forall\, y \in X)(P(y) \;\Rightarrow\; y = x)\big).
\end{aligned}$$

V poslednom prípade môžeme tiež použiť vyjadrenie

$$(\exists !x \in X)P(x) \;\Leftrightarrow\; (\exists\, x \in X)(\forall\, y \in X)(P(y) \;\Leftrightarrow\; y = x).$$

Množinu nazývame *konečnou*, ak ju možno zadať vymenovaním všetkých jej prvkov. Ak X je konečná množina a $x_1, x_2, \dots, x_n$ sú všetky jej prvky, píšeme

$$X = \{x_1, x_2, \dots, x_n\}.$$

Z extenzionality potom vyplýva, že nezáleží na poradí vymenovania prvkov množiny X. Taktiež sa môže stať, že X má menej než n prvkov – v takom prípade sa niektoré z prvkov $x_1, \dots, x_n$ opakujú a v zápise množiny X môžeme (no nemusíme) opakujúce sa prvky až na jeden z nich vynechať. Napríklad $\{x, y\} = \{y, x\}$, a ak $x = y$, tak $\{x, y\} = \{x\} = \{y\}$. Okrem množín, ktoré majú nejaké prvky, zavádzame aj tzv. *prázdnu množinu* $\emptyset$, ktorá neobsahuje nijaký prvok. Z extenzionality vyplýva, že prázdna množina je touto podmienkou jednoznačne určená.

Popri konečných množinách však v matematike často pracujeme i s *nekonečnými* množinami, t. j. takými, ktoré nemožno zadať vymenovaním všetkých ich jednotlivých prvkov. Takéto množiny zvykneme zadávať nejakou *charakteristickou vlastnosťou.* Ak $P(x)$ je nejaká vlastnosť, píšeme

$$X = \{x;\, P(x)\},$$

čím myslíme, že pre ľubovoľné x platí $x \in X$ práve vtedy, keď x spĺňa $P(x)$. Z extenzionality vyplýva, že takto definovaná množina X je určená jednoznačne. Napríklad vlastnosťou „x je párne celé číslo“ je určená množina všetkých párnych celých čísel.

Poznamenajme, že z rovnosti $X = \{x;\, P(x)\}$ ešte nijako nevyplýva, že množina X je nekonečná – rovnako dobre môže byť aj konečná, dokonca prázdna.

Na tomto mieste je potrebné poznamenať, že uvedený princíp, ktorý nám umožňuje zadávať množiny akýmikoľvek vlastnosťami ich prvkov, vedie k logickým sporom, a je preto v uvedenej intuitívnej a neobmedzenej podobe nepoužiteľný. Keďže sa však nehodláme púšťať do jeho upresňovania, čo by si vyžiadalo vybudovať základy axiomatickej teórie množín, nezostáva nám než čitateľovi vopred zaručiť, že všetky prípady

použitia tohto princípu, ktoré sa v tomto texte vyskytnú, budú plne legálne z hľadiska teórie množín, a požiadať ho o dôveru. Zatiaľ stačí, ak prezradíme, že všetky množiny netvoria množinu, t. j. neexistuje množina všetkých množín. To znamená, že vlastnosťou „x je množina“ nie je vymedzená nijaká množina.

Najčastejšie budeme spomínaný princíp používať na vymedzovanie podmnožín nejakej vopred danej *množiny* pomocou vlastností popísaných *matematickými formulami.* Ak M je množina a $P(x)$ je nejaká (matematická) vlastnosť, tak existuje množina X všetkých tých prvkov x množiny M, ktoré majú vlastnosť $P(x)$, t. j. množina

$$X = \{x \in M;\, P(x)\} = \{x;\, x \in M \;\&\; P(x)\}.$$

Nech X, Y sú ľubovoľné množiny. *Prienikom*, *zjednotením*, a *rozdielom* množín X, Y nazývame porade nasledujúce množiny:

$$\begin{aligned}
X \cap Y &= \{x;\, x \in X \;\&\; x \in Y\},\\
X \cup Y &= \{x;\, x \in X \;\vee\; x \in Y\},\\
X \smallsetminus Y &= \{x;\, x \in X \;\&\; x \notin Y\}.
\end{aligned}$$

Množiny X, Y nazývame *disjunktné*, ak $X \cap Y = \emptyset$. Čitateľovi prenechávame, aby si sám premyslel základné vlastnosti uvedených množinových operácií.

Pod usporiadanou dvojicou objektov x, y rozumieme objekt označovaný (x, y), taký, že pre všetky x, y, u, v platí:

$$(x, y) = (u, v) \;\Leftrightarrow\; (x = u \;\&\; y = v).$$

Uvedomme si, že nepotrebujeme vedieť, čo je „naozaj“ usporiadaná dvojica (x, y), dôležitá je len uvedená vlastnosť. Analogicky zavádzame pre ľubovoľné celé číslo $n \geq 2$ usporiadanú n-ticu $(x_1, \dots, x_n)$ tak, že pre všetky $x_1, \dots, x_n$, $y_1, \dots, y_n$ platí

$$(x_1, \dots, x_n) = (y_1, \dots, y_n) \;\Leftrightarrow\; (x_1 = y_1 \;\&\; \dots \;\&\; x_n = y_n).$$

Množiny

$$\begin{aligned}
X \times Y &= \{(x, y);\, x \in X \;\&\; y \in Y\},\\
X_1 \times \dots \times X_n &= \{(x_1, \dots, x_n);\, x_1 \in X_1 \;\&\; \dots \;\&\; x_n \in X_n\}
\end{aligned}$$

nazývame *karteziánskym súčinom* množín X, Y, resp. množín $X_1, \dots, X_n$. V prípade, že $X_1 = \dots = X_n = X$, píšeme

$$X_1 \times \dots X_n = X^n.$$

Pre úplnosť ešte kladieme

$$X^1 = X, \qquad X^0 = \{\emptyset\}.$$

X^n nazývame *n-tou karteziánskou mocninou* množiny X.

Počet prvkov konečnej množiny X budeme značiť $\#\, X$. Taktiež prázdna množina je konečná a platí $\#\,\emptyset = 0$. Pre nekonečnú množinu X píšeme $\#\, X = \infty$. Zrejme pre ľubovoľné konečné množiny X, Y platí

$$\#(X \cup Y) = \#X + \#Y - \#(X \cap Y),$$
$$\#(X \times Y) = \#X \cdot \#Y.$$

Z poslednej rovnosti vyplýva, že

$$\#X^n = (\#X)^n$$

pre každé celé číslo $n \geq 0$ a konečnú množinu X.

0.3. Zobrazenia

Zobrazením alebo tiež *funkciou* z množiny X do množiny Y rozumieme ľubovoľný predpis, ktorý každému prvku x množiny X priradí jednoznačne určený prvok y množiny Y. Zápis $f\colon X \to Y$ označuje, že f je zobrazenie (funkcia) z X do Y. Ten jednoznačne určený prvok $y \in Y$, ktorý zobrazenie f priradí prvku $x \in X$, budeme značiť $f(x)$, prípadne len fx alebo f_x. Vo vzťahu $y = f(x)$ nazývame x *nezávisle premennou* alebo *argumentom* a y *závisle premennou* alebo *funkčnou hodnotou* funkcie f. Píšeme tiež $f\colon x \mapsto y$.

Dve zobrazenia $f, g\colon X \to Y$ *sa rovnajú*, ak pre každé $x \in X$ platí $f(x) = g(x)$.

Množinu všetkých zobrazení z množiny X do množiny Y budeme označovať Y^X; teda

$$Y^X = \{f;\, f\colon X \to Y\}.$$

Toto označenie je motivované vzorcom pre počet prvkov množiny Y^X. Pre konečné množiny X, Y totiž platí

$$\#\left(Y^X\right) = (\#Y)^{(\#X)}.$$

(Samostatne si rozmyslite prečo!)

Zobrazenie $f\colon X \to X$ sa nazýva *transformáciou* množiny X alebo tiež *unárnou* (t. j. jednomiestnou) *operáciou* na množine X.

Zobrazenie $f\colon X \to Y$ sa nazýva *prosté* alebo tiež *injektívne* či *injekcia*, ak rôznym prvkom $x_1, x_2 \in X$ priraďuje rôzne prvky $f(x_1), f(x_2) \in Y$, t. j. ak platí

$$(\forall x_1, x_2 \in X)(x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)).$$

Uvedenú podmienku možno ekvivalentne vyjadriť v tvare

$$(\forall x_1, x_2 \in X)(f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$$

Zobrazenie $f\colon X \to Y$ sa nazýva zobrazenie *na množinu* Y alebo tiež *surjektívne* či *surjekcia*, ak na každý prvok množiny Y sa zobrazí nejaký prvok množiny X, t. j. ak platí

$$(\forall y \in Y)(\exists x \in X)(y = f(x)).$$

Hovoríme, že $f\colon X \to Y$ je *prosté zobrazenie* X *na* Y alebo tiež *bijektívne zobrazenie* či *bijekcia*, ak f je zároveň prosté a na, t. j. injektívne i surjektívne. Ešte inak to môžeme vyjadriť podmienkou

$$(\forall y \in Y)(\exists! x \in X)(y = f(x)).$$

Namiesto uvedených pojmov niekedy tiež hovoríme, že f je *vzájomne jednoznačné zobrazenie množiny* X *na množinu* Y.

Ak $f\colon X \to Y$ je bijekcia, tak existuje jednoznačne určené zobrazenie $g\colon Y \to X$, ktoré každému $y \in Y$ priradí ten jediný prvok $x \in X$, pre ktorý platí $y = f(x)$. Toto zobrazenie nazývame *inverzným zobrazením* k zobrazeniu f a označujeme ho f^{-1}. Zrejme $f^{-1}\colon Y \to X$ je tiež bijekcia a pre všetky $x \in X$, $y \in Y$ platí

$$f^{-1}\bigl(f(x)\bigr) = x, \qquad f\bigl(f^{-1}(y)\bigr) = y.$$

Nech $f\colon X \to Y$, $g\colon Y \to Z$ sú zobrazenia. *Kompozíciou* zobrazení f, g alebo aj *zloženým zobrazením* z f a g rozumieme zobrazenie označené ako $g \circ f\colon X \to Z$, dané pre každé $x \in X$ predpisom

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

Zložené zobrazenie možno znázorniť pomocou tzv. *komutatívneho diagramu*

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "g \circ f"'] & Y \arrow[d, "g"] \\ & Z \end{tikzcd}$$

(Všimnite si, že zobrazenie $g \circ f$ zapisujeme „v obrátenom poradí“ – najprv totiž na prvok x aplikujeme f a až potom g. Núti nás k tomu zaužívaná konvencia, podľa ktorej argument x píšeme napravo od funkcie f. Poznamenajme, že niektorí autori dávajú prednosť „prirodzenému poradiu“ a kompozíciu zobrazení $f\colon X \to Y$, $g\colon Y \to Z$, zapisujú ako $f \circ g$. Kvôli tomu však opúšťajú spomínanú konvenciu a namiesto $f(x)$ píšu xf. V tomto duchu fungujú napr. niektoré kalkulačky.)

Skladanie zobrazení je *asociatívne* v nasledujúcom zmysle: ak $f\colon X \to Y$, $g\colon Y \to Z$ a $h\colon Z \to W$ sú zobrazenia, tak

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

Ľahko totiž nahliadneme, že jedno i druhé zobrazenie priradí prvku $x \in X$ prvok $h(g(f(x))) \in W$.

Na každej množine X máme definované *identické zobrazenie* $\mathrm{id}_X\colon X \to X$, nazývané tiež *identita na* X, také, že

$$\mathrm{id}_X(x) = x$$

pre každé $x \in X$. Zrejme id_X je bijekcia pre každé X, a pre ľubovoľné zobrazenie $f\colon X \to Y$ platí

$$f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f.$$

Ak $f\colon X \to Y$ je bijekcia, tak k nej inverzné zobrazenie $f^{-1}\colon Y \to X$ teraz môžeme charakterizovať rovnosťami

$$f^{-1} \circ f = \mathrm{id}_X, \qquad f \circ f^{-1} = \mathrm{id}_Y .$$

Čitateľ sám ľahko nahliadne, že pre ľubovoľné zobrazenia $f\colon X \to Y$, $g\colon Y \to Z$ platí:

(a) Ak f, g sú injektívne, tak aj $g \circ f$ je injektívne.
(b) Ak f, g sú surjektívne, tak aj $g \circ f$ je surjektívne.
(c) Ak f, g sú bijektívne, tak aj $g \circ f$ je bijektívne.
(d) Ak $g \circ f$ je injektívne, tak aj f je injektívne.
(e) Ak $g \circ f$ je surjektívne, tak aj g je surjektívne.
(f) Ak $g \circ f$ je bijektívne, tak f je injektívne a g je surjektívne.

Nech $f\colon X \to Y$ je nejaké zobrazenie a $A \subseteq X$. *Zúžením zobrazenia* f na množinu A nazývame zobrazenie $f \restriction A\colon A \to Y$ také, že

$$(f \restriction A)(x) = f(x)$$

pre každé $x \in A$. *Obrazom množiny* A v zobrazení f nazývame množinu

$$f(A) = \{f(x);\, x \in A\} \subseteq Y.$$

Špeciálne, množinu $f(X)$ nazývame *obrazom zobrazenia* f a značíme ju

$$\operatorname{Im} f = f(X) = \{f(x);\, x \in X\}.$$

Pre $f\colon X \to Y$ a $A \subseteq X$ platí $\operatorname{Im}(f \restriction A) = f(A)$; zrejme f je surjekcia práve vtedy, keď $\operatorname{Im} f = Y$,

Podobne, *vzorom množiny* $B \subseteq Y$ v zobrazení $f\colon X \to Y$ nazývame množinu

$$f^{-1}(B) = \{x \in X;\, f(x) \in B\} \subseteq X.$$

Pre ľubovoľné $A \subseteq X$, $B \subseteq Y$ možno jednoducho overiť inklúzie

$$A \subseteq f^{-1}\bigl(f(A)\bigr), \qquad f\bigl(f^{-1}(B)\bigr) \subseteq B.$$

0.4. Binárne operácie

Ak X, Y, Z sú množiny, tak zobrazenie $f\colon X \times Y \to Z$ nazývame *binárnou* (t. j. dvojmiestnou) *operáciou na množinách X, Y s hodnotami v množine Z*. Binárne operácie väčšinou označujeme znakmi umiestňovanými medzi hodnoty argumentov, ako napr $+$, $\cdot$, $\circ$, $*$ a pod. Hodnotu takej operácie na dvojici prvkov $x \in X$, $y \in Y$ potom označujeme $x + y$, $x \cdot y$ (prípadne len xy), $x \circ y$, $x * y$ a pod.

Najčastejšie budeme pracovať s binárnymi operáciami tvaru $f\colon X \times X \to X$, ktoré nazývame jednoducho *binárnymi operáciami na množine X*.

Binárna operácia $*$ na množine X sa nazýva *asociatívna*, ak pre všetky $x, y, z \in X$ platí

$$x * (y * z) = (x * y) * z.$$

Asociativita operácie nám dovoľuje vynechávať zátvorky a písať len $x * y * z$. Podobne si možno počínať i v prípade viacerých argumentov.

Binárna operácia $*$ na množine X sa nazýva *komutatívna*, ak pre všetky $x, y \in X$ platí

$$x * y = y * x.$$

Prvok $e \in X$ sa nazýva *neutrálny prvok* binárnej operácie $*$ na množine X, ak pre všetky $x \in X$ platí

$$e * x = x * e = x.$$

Napríklad pre ľubovoľnú množinu X kompozícia $\circ$ je asociatívna binárna operácia na množine X^X všetkých transformácií množiny X s neutrálnym prvkom id_X. Zrejme ak $\# X \geq 2$, tak táto operácia nie je komutatívna.

Binárnu operáciu $*$ na konečnej množine X možno zadať pomocou tzv. *multiplikatívnej tabuľky*, ktorej stĺpce i riadky sú označené prvkami množiny X. Do poľa tabuľky ležiaceho v priesečníku x-tého riadku a y-tého stĺpca vpíšeme hodnotu $x * y$.

Napr. tabuľkami

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

sú zadané dve asociatívne a komutatívne operácie $+$ a $\cdot$ na množine $\{0, 1, 2, 3, 4\}$. Navyše 0 je neutrálny prvok operácie $+$ a 1 je neutrálny prvok operácie $\cdot$.

Komutativitu binárnej operácie možno ľahko nahliadnuť z jej multiplikatívnej tabuľky – prejaví sa symetriou tabuľky podľa hlavnej diagonály spájajúcej ľavý horný a pravý dolný roh. Taktiež neutrálny prvok možno odhaliť na prvý pohľad, lebo v jeho riadku i stĺpci sa zreprodukuje riadok resp. stĺpec zo záhlavia tabuľky. Asociatívnosť, žiaľ, tak jednoducho nahliadnuť nemožno.

Podobným spôsobom možno zaviesť aj n-miestne operácie $X_1 \times \ldots \times X_n \to Y$, prípadne $X^n \to Y$, či $X^n \to X$ pre ľubovoľné celé číslo $n \geq 0$.

0.5. Permutácie

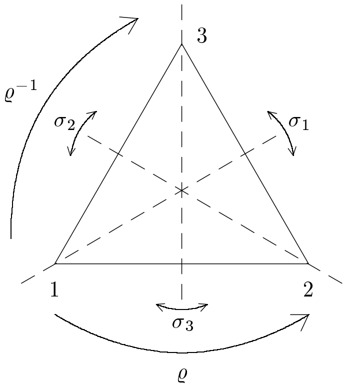
Kým znalosť predchádzajúcich paragrafov je nevyhnutným predpokladom, aby čitateľ mohol začať so štúdiom kapitoly 1, tento paragraf budeme potrebovať až neskôr, keď začneme preberať determinanty.

Nech X je ľubovoľná množina. *Permutáciou* množiny X rozumieme ľubovoľné bijektívne zobrazenie $\sigma\colon X \to X$. Množinu všetkých permutácií množiny X značíme $\mathcal{S}(X)$. Ak X je konečná množina, tak počet prvkov množiny $\mathcal{S}(X)$ je daný známym vzťahom

$$\# \mathcal{S}(X) = (\# X)!\,,$$

kde $n! = 1 \cdot 2 \cdot \ldots \cdot n$ je *faktoriál* prirodzeného čísla n (pritom $0! = 1! = 1$).

Uvedomme si, že transformácia $f\colon X \to X$ *konečnej* množiny X je injektívna práve vtedy, keď je surjektívna. Jedna i druhá podmienka totiž hovorí, že množina $f(X) \subseteq X$ má rovnaký počet prvkov ako X. Teda už jedna z uvedených podmienok je postačujúca na to, aby f bola permutáciou konečnej množiny X.



Keďže zloženie $\sigma \circ \tau$ dvoch permutácií $\sigma, \tau \in \mathcal{S}(X)$ dáva opäť permutáciu množiny X, kompozícia $\circ$ je asociatívna binárna operácia na množine $\mathcal{S}(X)$ a id_X je jej neutrálny prvok. Ľahko sa možno presvedčiť, že – okrem prípadu, keď $\# X \le 2$, – táto operácia nie je komutatívna.

Pre $X = \{1, 2, \dots, n\}$ namiesto $\mathcal{S}(X)$ píšeme $\mathcal{S}_n$. Permutáciu $\sigma \in \mathcal{S}_n$ zvyčajne zapisujeme v tvare

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

Prvky množiny $\mathcal{S}_3$, t. j. permutácie množiny $\{1, 2, 3\}$, si môžeme predstaviť ako symetrie rovnostranného trojuholníka s vrcholmi označenými číslami 1, 2, 3. Ak si identickú permutáciu tejto množiny označíme ako ι, otočenia okolo ťažiska trojuholníka proti smeru resp. v smere hodinových ručičiek o uhol $\pi/3$ ako ϱ resp. ϱ^{-1}, a osovú súmernosť podľa osi prechádzajúcej i-tým vrcholom a stredom protiľahlej strany ako σ_i, pre $i = 1, 2, 3$, tak množina permutácií $\mathcal{S}_3$ bude pozostávať z permutácií

$$\iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \varrho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \varrho^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Multiplikatívna tabuľka binárnej operácie $\circ$ na množine $\mathcal{S}_3$ vyzerá takto:

$\circ$	ι	ϱ	ϱ^{-1}	σ_1	σ_2	σ_3
ι	ι	ϱ	ϱ^{-1}	σ_1	σ_2	σ_3
ϱ	ϱ	ϱ^{-1}	ι	σ_3	σ_1	σ_2
ϱ^{-1}	ϱ^{-1}	ι	ϱ	σ_2	σ_3	σ_1
σ_1	σ_1	σ_2	σ_3	ι	ϱ	ϱ^{-1}
σ_2	σ_2	σ_3	σ_1	ϱ^{-1}	ι	ϱ
σ_3	σ_3	σ_1	σ_2	ϱ	ϱ^{-1}	ι

Permutáciu $\sigma \in \mathcal{S}(X)$ nazývame *transpozíciou*, ak existujú $x, y \in X$ také, že $x \ne y$, $\sigma(x) = y$, $\sigma(y) = x$ a $\sigma(z) = z$ pre každé $z \in X \setminus \{x, y\}$. Inak povedané, transpozícia je výmena dvoch prvkov množiny X.

Zrejme $\sigma_1, \sigma_2, \sigma_3 \in \mathcal{S}_3$ sú transpozície.

Z názoru je zrejmé (a nebudeme to dokazovať), že každú permutáciu σ konečnej množiny X možno získať postupnými výmenami dvojíc prvkov, teda každá taká permutácia je kompozíciou transpozícií. Tento rozklad na transpozície nie je jednoznačný: napr. $\iota \in \mathcal{S}_3$ možno zapísať ako ι, t. j. kompozíciu 0 transpozícií, a taktiež ako $\iota = \sigma_1 \circ \sigma_1 = \sigma_2 \circ \sigma_2 = \sigma_3 \circ \sigma_3$, t. j. aspoň troma ďalšími spôsobmi ako kompozíciu dvoch transpozícií.

Dĺžkou permutácie σ konečnej množiny X nazveme najmenší počet transpozícií, na kompozíciu ktorých možno σ rozložiť, a označíme ju $|\sigma|$. Samotná dĺžka $|\sigma|$ nie je dôležitá, význam má len parita tohto čísla, t. j. vlastne výraz $\operatorname{sgn} \sigma = (-1)^{|\sigma|}$, ktorý nazývame *znakom*, prípadne *znamienkom permutácie* σ.

Permutácia σ konečnej množiny X sa nazýva *párna* resp. *nepárna*, ak číslo $|\sigma|$ je párne resp. nepárne, t. j. ak jej znak je 1 resp. -1.

Z nasledujúcej vety vyplýva, že pri určovaní znamienka permutácie σ môžeme použiť jej *ľubovoľný* rozklad na transpozície $\sigma = \tau_1 \circ \ldots \circ \tau_k$ a nemusíme sa starať o to, či tento rozklad je naozaj najkratší – pre ľubovoľný taký rozklad totiž platí

$$(-1)^{|\sigma|} = (-1)^k.$$

0.5.1. Veta. *Nech X je konečná množina. Potom pre ľubovoľné $\sigma, \tau \in \mathcal{S}(X)$ platí*

$$(-1)^{|\sigma \circ \tau|} = (-1)^{|\sigma|} \cdot (-1)^{|\tau|}.$$

Dôkaz. Zrejme stačí dokázať uvedenú rovnosť pre prípad, keď τ je transpozícia a $X = \{1, 2, \dots, n\}$.

Pre každé $\sigma \in \mathcal{S}_n$ označme $p(\sigma)$ súčin všetkých rozdielov tvaru $\sigma(j) - \sigma(i)$, kde $1 \le i < j \le n$. Zrejme pre všetky $\sigma \in \mathcal{S}_n$ majú výrazy $p(\sigma)$ rovnakú absolútnu hodnotu a líšia sa nanajvýš znamienkom. Toto znamienko závisí od parity počtu záporných členov v súčine $p(\sigma)$. Člen $\sigma(j) - \sigma(i)$ je záporný práve vtedy, keď $i < j$ a $\sigma(i) > \sigma(j)$, – každú takú dvojicu (i, j) nazývame *inverziou* permutácie σ. Identita id_X má 0 inverzií a $p(\mathrm{id}_X) = 1^{n-1} \cdot 2^{n-2} \cdot \ldots \cdot (n-1)^1 = 1! \cdot 2! \cdot \ldots \cdot (n-1)! > 0$.

Stačí teda dokázať, že počet inverzií permutácií σ a $\sigma \circ \tau$ sa líši o nepárnu hodnotu. Nech $1 \le k < l \le n$ sú tie dva prvky, ktoré vymieňa transpozícia τ. Potom

$$\sigma = \begin{pmatrix} 1 & \dots & k & \dots & l & \dots & n \\ \sigma(1) & \dots & \sigma(k) & \dots & \sigma(l) & \dots & \sigma(n) \end{pmatrix},$$

$$\sigma \circ \tau = \begin{pmatrix} 1 & \dots & k & \dots & l & \dots & n \\ \sigma(1) & \dots & \sigma(l) & \dots & \sigma(k) & \dots & \sigma(n) \end{pmatrix}.$$

Inverzie (i, j) permutácie σ, v ktorých nevystupuje k ani l, sú tiež inverziami permutácie $\sigma \circ \tau$. Inverzie, v ktorých vystupujú prvky i, k, a i, l, kde $i \ne k, l$, alebo obe súčasne vzniknú alebo súčasne zaniknú v $\sigma \circ \tau$ oproti σ. Konečne, pokiaľ (k, l) nebola inverziou v σ, stane sa ňou v $\sigma \circ \tau$; pokiaľ ňou bola, táto inverzia v $\sigma \circ \tau$ zanikne. Teda celkový rozdiel počtu inverzií permutácií σ a $\sigma \circ \tau$ je nepárny.

0.6. Ekvivalencie a rozklady

Podobne ako predošlý, i tento paragraf môže čitateľ zatiaľ preskočiť. Jeho znalosť bude potrebná až neskôr, v súvislosti s niektorými otázkami teórie grúp. S pojmom ekvivalencie sa síce stretneme už predtým, dovtedy ho však nebudeme systematicky využívať.

Nech $\sim$ je nejaký dvojmiestny vzťah, do ktorého vstupujú prvky nejakého oboru objektov $\mathcal{M}$ (tento obor môže, ale nemusí byť množinou). Zápisom $x \sim y$ značíme, že prvky $x, y \in \mathcal{M}$ sa nachádzajú vo vzťahu $\sim$; ak sa $x, y \in \mathcal{M}$ nenachádzajú v tomto vzťahu, píšeme $x \not\sim y$.

Hovoríme, že vzťah $\sim$ je na obore $\mathcal{M}$

(a) *reflexívny*, ak pre všetky $x \in \mathcal{M}$ platí $x \sim x$;
(b) *symetrický*, ak pre všetky $x, y \in \mathcal{M}$ platí $x \sim y \;\Rightarrow\; y \sim x$;
(c) *tranzitívny*, ak pre všetky $x, y, z \in \mathcal{M}$ platí $x \sim y \;\&\; y \sim z \;\Rightarrow\; x \sim y$.

Vzťah $\sim$, ktorý je reflexívny, symetrický a tranzitívny na obore $\mathcal{M}$, nazývame *vzťahom ekvivalencie* alebo len krátko *ekvivalenciou* na obore $\mathcal{M}$. Ekvivalencie budeme väčšinou značiť znakmi $\sim$, $\approx$, $\equiv$ a pod.

Každý vzťah ekvivalencie na nejakej množine či obore objektov $\mathcal{M}$ predstavuje isté hľadisko, z ktorého považujeme niektoré prvky z $\mathcal{M}$ za rovnocenné, t. j. ekvivalentné, a iné nie. Napr. na množine všetkých hracích guličiek v danej jamke možno zaviesť vzťah ekvivalencie, v ktorom sa nachádzajú ľubovoľné dve guličky práve vtedy, keď majú rovnakú farbu. Vzťah, v ktorom sa nachádzajú dve takéto guličky práve vtedy, keď majú rovnakú hmotnosť, je iným príkladom ekvivalencie na tejto množine.

Jedným dychom však poznamenajme, že uvedené príklady neslobodno brať príliš vážne, lebo rovnocennosť sa v nich mieša s podobnosťou, – „naozajstné“ ekvivalencie predstavujú len v značne idealizovanom prípade. S reflexívnosťou a symetriou nie je problém, v reálnom živote však zvykne zlyhať tranzitívnosť. Môžeme sa napríklad zhodnúť, že guličky a, b majú rovnakú farbu, a takisto majú rovnakú farbu guličky b, c. No farba guličiek a, c sa nám už rovnakou zdať nemusí. Podobne môžeme v rámci presnosti našich váh dospieť k záveru, že guličky p, q ako aj guličky q, r majú rovnakú hmotnosť. Avšak hmotnosť guličiek p, r sa nám už vážením môže podariť rozlíšiť. Lepším príkladom ekvivalencie je tak vzťah na množine všetkých bankoviek danej meny, v ktorom sa nachádzajú dve bankovky práve vtedy, keď majú rovnakú nominálnu hodnotu.

Na rozdiel od reálneho života sa v matematike nemusíme trápiť podobnými ťažkosťami. Všetky ekvivalencie, s ktorými sa tu stretneme, budú mať v plnej miere všetky tri uvedené vlastnosti. Ešte jeden príklad za všetky: vzťahom

$$x \sim y \;\Leftrightarrow\; |x| = |y|$$

je definovaná ekvivalencia „mať rovnakú absolútnu hodnotu“ na množine $\mathbb{C}$ všetkých komplexných čísel.

Nech $\sim$ je ekvivalencia na množine X. Pre $x \in X$ označme

$$\tilde{x} = \{u \in X;\, u \sim x\}$$

množinu všetkých prvkov $u \in X$ ekvivalentných s x, ktorú nazývame *triedou* alebo *blokom ekvivalencie* prvku x. Zrejme pre ľubovoľné $x \in X$ platí $x \in \tilde{x}$. Ľahko tiež

možno dokázať (skúste sami), že

$$\tilde{x} = \tilde{y} \;\Leftrightarrow\; x \sim y \;\Leftrightarrow\; \tilde{x} \cap \tilde{y} \neq \emptyset$$

pre všetky $x, y \in X$. Množinu

$$X/{\sim} = \{\tilde{x};\, x \in X\}$$

všetkých tried ekvivalencie prvkov množiny X nazývame *faktorovou množinou* množiny X podľa ekvivalencie $\sim$. (Podotýkame, že v zhode s paragrafom 0.2 sa každá trieda $\tilde{x}$ nachádza v množine $X/{\sim}$ iba raz, i keď prvkov $y \in X$, pre ktoré platí $\tilde{x} = \tilde{y}$, môže byť mnoho.)

Priradením $x \mapsto \tilde{x}$ je definované surjektívne zobrazenie $X \to X/{\sim}$, ktoré nazývame *prirodzenou* alebo tiež *kanonickou projekciou* množiny X na faktorovú množinu $X/{\sim}$.

Na faktorovú množinu $X/{\sim}$ sa možno dívať dvojakým spôsobom. Jednak ako na výsledok stotožnenia či zlepenia navzájom ekvivalentných prvkov množiny X; v takom prípade sa na bloky $\tilde{x}$ dívame predovšetkým ako na *prvky*, ktoré vznikli „stiahnutím“ celej triedy $\tilde{x}$ do jediného bodu, a vedome zanedbávame fakt, že sú to zároveň množiny. Použitím názvu „faktorová množina“ naznačujeme, že v danej chvíli dávame tomuto pohľadu prednosť. Na druhej strane sa na množinu $X/{\sim}$ možno dívať ako na *rozklad* množiny X na navzájom disjunktné neprázdne množiny $\tilde{x}$.

Rozkladom množiny X nazývame ľubovoľný systém (t. j. množinu) jej neprázdnych podmnožín $\mathcal{R}$ taký, že každý prvok množiny X padne do práve jednej množiny zo systému $\mathcal{R}$. Inými slovami, systém $\mathcal{R}$ neprázdnych podmnožín množiny X je jej rozkladom práve vtedy, keď spĺňa nasledujúce dve podmienky:

(1) zjednotením všetkých množín $A \in \mathcal{R}$ je celá množina X, t. j. $(\forall\, x \in X)(\exists\, A \in \mathcal{R})(x \in A)$;
(2) množiny z $\mathcal{R}$ sú navzájom disjunktné, t. j. $(\forall\, A, B \in \mathcal{R})(A \neq B \;\Rightarrow\; A \cap B = \emptyset)$.

Ľahko možno nahliadnuť, že faktorová množina $X/{\sim}$ množiny X podľa ekvivalencie $\sim$ je zároveň rozkladom množiny X, ktorý je tvorený triedami navzájom ekvivalentných prvkov. Taktiež naopak, každý rozklad $\mathcal{R}$ množiny X určuje predpisom

$$x \sim_{\mathcal{R}} y \;\Leftrightarrow\; (\exists\, A \in \mathcal{R})(x, y \in A)$$

ekvivalenciu na množine X. Inak povedané, prvky $x, y \in X$ sú vo vzťahu ekvivalencie určenej rozkladom $\mathcal{R}$ práve vtedy, keď sa nachádzajú v tej istej (jednoznačne určenej) množine z tohto rozkladu. Čitateľovi prenechávame, aby si samostane overil, že takto definovaný vzťah $\sim_{\mathcal{R}}$ je reflexívny, symetrický a tranzitívny, t. j. má všetky tri požadované vlastnosti ekvivalencie, ako aj rovnosť $X/{\sim_{\mathcal{R}}} = \mathcal{R}$, t. j. že rozklad (faktorová množina) určený ekvivalenciou $\sim_{\mathcal{R}}$ splýva s pôvodným rozkladom $\mathcal{R}$.

0.6.1. Príklad. Rozklad prislúchajúci k spomínanej ekvivalencii $x \sim y \Leftrightarrow |x| = |y|$ na množine $\mathbb{C}$ je vlastne rozkladom komplexnej roviny na navzájom sústredné kružnice so stredom v počiatku 0 a ľubovoľným polomerom $r \geq 0$ (kružnicu s nulovým polomerom prirodzene stotožňujeme s jej stredom).

0.7. O matematických dôkazoch

Matematika je veda vybudovaná prevažne (hoci nie výlučne) *deduktívne.* To znamená, že v tej-ktorej matematickej teórii vychádzame z určitých základných pojmov, ktoré považujeme za intuitívne jasné vďaka istým s nimi spojeným názorným predstavám. Ďalšie pojmy potom definujeme pomocou pojmov základných alebo skôr definovaných. Základné pojmy označujú základné objekty, ktoré tvoria predmet nášho štúdia, alebo určité základné vzťahy medzi nimi. Tieto objekty a vzťahy sú charakterizované istými východzími tvrdeniami, ktorým hovoríme *axiómy.* V najjednoduchších prípadoch je platnosť axióm jasná z názoru, ktorý stojí v pozadí príslušnej teórie. V zložitejších prípadoch však môžu názorné predstavy zlyhať – vtedy sa na axiómy dívame ako na *implicitné definície* základných pojmov. To znamená, že rezignujeme na otázku, čo „naozaj“ označujú základné pojmy. Môžu označovať čokoľvek, čo spĺňa dané axiómy – to je všetko, čo o nich predpokladáme. Zisk z takéhoto prístupu spočíva v *univerzálnosti matematiky* – aj výsledky matematických teórií sa potom vzťahujú na veľmi rôznorodé oblasti reality. Totiž na tie, v ktorých možno interpretovať základné pojmy danej teórie tak, že sú pritom splnené jej axiómy.

Pri deduktívnej výstavbe nejakej teórie vyvodzujeme ďalšie poznatky z jej axióm logickými prostriedkami, t. j. dokazujeme ich. Týmto dokázaným poznatkom hovoríme *vety*, *tvrdenia*, *lemy* a *dôsledky*, čím naznačujeme rôzny stupeň dôležitosti, ktorý im pripisujeme. Názvom *veta* označujeme tie najdôležitejšie z nich, menej dôležité nazývame *tvrdeniami* a tvrdenia pomocného charakteru označujeme ako *lemy*. *Dôsledky*, ako už samotný názov napovedá, pripájame ako bezprostredné dôsledky niektorých viet, tvrdení či liem, pokiaľ ich význam nedosahuje úroveň viet. Poznamenajme, že toto rozdelenie má značne subjektívny charakter a vývoj ho často zvykne prekonať. Mnohé vety časom upadajú do zabudnutia, kým naopak mnohé lemy postupne nadobúdajú na význame.

Základným prostriedkom odvodzovania nových poznatkov v deduktívnej teórii je *dôkaz.* V tomto paragrafe sa veľmi stručne zoznámime s hlavnými typmi matematických dôkazov: s *priamym dôkazom*, s *nepriamym dôkazom* a s *dôkazom sporom.* Uvidíme, že toto rozdelenie tak trochu súvisí so stratégiou vedenia príslušného dôkazu. V nasledujúcom paragrafe sa ešte zoznámime s *dôkazom matematickou indukciou.*

Väčšina matematických tvrdení má tvar implikácie $P \Rightarrow Q$, t. j. tvrdí sa v nich, že z predpokladu P vyplýva záver Q. Pritom predpoklad P je často konjunkciou nejakých dielčích predpokladov, čiže má tvar $P_1 \,\&\, \dots \,\&\, P_n$. Na tomto mieste sa obmedzíme na niekoľko poznámok o dôkazoch tvrdení takéhoto tvaru.

0.7.1. Priamy dôkaz. Pri *priamom dôkaze* implikácie $P \Rightarrow Q$ dokazujeme (či sa aspoň pokúšame dokázať) záver Q z predpokladu P. Spočiatku sa snažíme dokázať priamo záver Q z daných axióm a už skôr dokázaných tvrdení. Postupujeme pri tom tak ďaleko, ako sa len dá, pričom jedným očkom stále poškuľujeme po predpoklade P, či dielčích predpokladoch $P_1, \dots, P_n$. Vo chvíli, keď už nevieme, ako ďalej, siahneme po tom z dielčích predpokladov P_i, ktorý nám umožní pohnúť sa dopredu. Opäť postupujeme ďalej a vo vhodnej chvíli zasa použijeme niektorý dielčí predpoklad P_j (nie nevyhnutne rôzny od P_i). Ak sme úspešní, nakoniec sa nám podarí dospieť k záveru Q, čím dôkaz končí. Ak sme neúspešní, musíme to skúsiť inak, prípadne sa zamyslieť nad otázkou, či spomínaná implikácia vôbec platí.

Môže sa stať, že pri našom úspešnom dôkaze sme nepoužili všetky dielčie predpoklady $P_1, \dots, P_n$, ale povedzme prvý a posledný z nich sme nepotrebovali. To znamená, že miesto pôvodného tvrdenia $(P_1 \,\&\, P_2 \,\&\, \dots \,\&\, P_{n-1} \,\&\, P_n) \Rightarrow Q$ sme dokázali *silnejšie* tvrdenie $(P_2 \,\&\, \dots \,\&\, P_{n-1}) \Rightarrow Q$.

0.7.2. Nepriamy dôkaz. Pri *nepriamom dôkaze* implikácie $P \Rightarrow Q$ dokazujeme miesto nej logicky ekvivalentnú tzv. *transponovanú implikáciu* $\neg Q \Rightarrow \neg P$ práve opísanou metódou priameho dôkazu. Za tým účelom býva často užitočné (pokiaľ to ide) rozčleniť predpoklad $\neg Q$ na konjunkciu dielčích predpokladov $R_1 \,\&\, \dots \,\&\, R_m$. Ak pôvodný predpoklad P bol konjunkciou dielčích predpokladov $P_1 \,\&\, \dots \,\&\, P_n$, tak jeho negácia $\neg P$ je ekvivalentná s alternatívou $\neg P_1 \vee \dots \vee \neg P_n$. Potom transponovaná implikácia $\neg Q \Rightarrow \neg P$ je logicky ekvivalentná s ľubovoľnou z implikácií

$$(\neg Q \,\&\, P_1 \,\&\, \dots \,\&\, P_{i-1} \,\&\, P_{i+1} \,\&\, \dots \,\&\, P_n) \Rightarrow \neg P_i,$$

kde $1 \le i \le n$. Nový záver $\neg P_i$ sa, samozrejme, usilujeme vybrať čo najvýhodnejšie, na čo neexistuje jednoznačný recept, no časom sa nám azda podarí nadobudnúť cit, ktorým sa budeme môcť riadiť.

0.7.3. Dôkaz sporom. *Dôkaz sporom* do istej miery pripomína nepriamy dôkaz a často sa s ním zvykne zamieňať. Najmä začiatočník by mal k nemu siahnuť až vtedy, keď sa mu priamy ani nepriamy dôkaz nedarí, prípadne keď v ňom skrsne podozrenie, že dokazované tvrdenie neplatí. Namiesto dokazovanej implikácie $P \Rightarrow Q$ prijmeme predpoklad $P \,\&\, \neg Q$, ktorý je logicky ekvivalentný s jej negáciou $\neg(P \Rightarrow Q)$. Tento predpoklad sa usilujeme *doviesť k sporu*, čím sa myslí nejaký logicky absurdný záver, ako napr. $x \ne x$, alebo spor s niektorým z pôvodných predpokladov P, $\neg Q$, prípadne spor s niektorou z axióm alebo s niektorým zo skôr dokázaných tvrdení.

Na rozdiel od priameho alebo nepriameho dôkazu, dôkaz sporom nemá vopred stanovený smer určený nejakým známym záverom – ten by sa mal objaviť až v jeho priebehu. Ak sa ani pokus doviesť k sporu predpoklad $P \,\&\, \neg Q$ neskončí úspešne, je namieste pokúsiť sa ho dokázať, to znamená vyvrátiť pôvodnú hypotézu $P \Rightarrow Q$.

0.7.4. Dôkaz ekvivalencie. Niekedy sa nám môže podariť dokázať ekvivalenciu $P \Leftrightarrow Q$ postupnosťou logicky ekvivalentných krokov, no to je skôr výnimka než pravidlo. Vo všeobecnosti si jej dôkaz vyžaduje dokázať zvlášť každú z implikácií $P \Rightarrow Q$, $Q \Rightarrow P$. Pritom na každú z nich možno použiť ľubovoľnú z troch skôr spomínaných metód. Často sa jedna z uvedených implikácií dokazuje priamo a druhá nepriamo, teda dôkaz uvedenej ekvivalencie pozostáva napr. z priamych dôkazov implikácií $P \Rightarrow Q$ a $\neg P \Rightarrow \neg Q$.

V našom kurze sa neraz stretneme s vetami, v ktorých sa tvrdí ekvivalencia viacerých podmienok $P_1, \dots, P_n$. V tom je zahrnutých $n(n-1)$ jednotlivých implikácií $P_i \Rightarrow P_j$ pre rôzne $i, j \le n$. Dokazovať ich všetky by pre $n \ge 3$ bolo značne neefektívne a taktiež zbytočné. Stačí totiž dokázať n implikácií tvoriacich cyklus

$$P_{\sigma(1)} \Rightarrow P_{\sigma(2)} \Rightarrow \dots \Rightarrow P_{\sigma(n-1)} \Rightarrow P_{\sigma(n)} \Rightarrow P_{\sigma(1)},$$

kde σ je ľubovoľná permutácia množiny indexov $\{1, \dots, n\}$, ktorú si volíme tak, aby to bolo čo najvýhodnejšie.

S príkladmi všetkých uvedených typov dôkazov sa budeme v našom kurze neustále stretávať.

0.8. Matematická indukcia a rekurzia

Množinu všetkých nezáporných celých čísel značíme $\mathbb{N} = \{0, 1, 2, \dots, \}$ a nazývame ju tiež množinou všetkých *prirodzených čísel*.

0.8.1. Dôkaz matematickou indukciou. Platnosť nejakého tvrdenia $P(n)$ pre všetky prirodzené čísla, t. j. tvrdenie $(\forall n \in \mathbb{N})P(n)$ sa obvykle dokazuje *matematickou indukciou*. Dôkaz indukciou spočíva v dôkaze dvoch tvrdení: nato, aby sme dokázali, že každé prirodzené číslo n má vlastnosť P, stačí dokázať, že platí

1° $P(0)$, t. j. 0 má vlastnosť P;

2° $(\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))$,
t. j. ak n je ľubovoľné prirodzené číslo, ktoré má vlastnosť P, tak aj číslo $n+1$ má vlastnosť P.

Štruktúru *dôkazu matematickou indukciou* tak možno zhrnúť do schémy

$$\big(P(0) \ \& \ (\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))\big) \Rightarrow (\forall n \in \mathbb{N})P(n).$$

Bod 2° vlastne tvrdí platnosť všetkých implikácií $P(0) \Rightarrow P(1)$, $P(1) \Rightarrow P(2)$, $P(2) \Rightarrow P(3)$, ... Z bodu 1° a prvej z nich vyplýva $P(1)$, z toho spolu s druhou implikáciou dostávame $P(2)$, z čoho pomocou tretej implikácie plynie $P(3)$, atď.

Princíp matematickej indukcie je logicky ekvivalentný so zdanlivo očividným *princípom dobrého usporiadania*, ktorý tvrdí, že každá neprázdna množina $A \subseteq \mathbb{N}$ má najmenší prvok. Keďže pre väčšinu študentov býva tento princíp ľahšie prijateľný než princíp indukcie, predvedieme ako možno princíp indukcie z neho dokázať. Dôkaz princípu dobrého usporiadania z princípu indukcie prenechávame na rozmyslenie čitateľovi.

Predpokladajme teda platnosť princípu dobrého usporiadania. Nech P je vlastnosť taká, že platí $P(0)$ a $(\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))$. Označme $A = \{n \in \mathbb{N};\ \neg P(n)\}$. Ak neplatí $(\forall n \in \mathbb{N})P(n)$, tak $A \neq \emptyset$. Nech m je najmenší prvok množiny A. Potom zrejme $m \neq 0$ a $m - 1 \notin A$, teda platí $P(m-1)$. No keďže $P(m-1) \Rightarrow P(m)$, platí $P(m)$, čiže $m \notin A$, čo je spor.

Z pedagogických dôvodov sa budeme (najmä spočiatku) pri dôkazoch indukciou odvolávať radšej na princíp dobrého usporiadania než na princíp indukcie, a tomu tiež podriadime redakciu dôkazu.

Poznámka. (a) Niekedy je potrebné miesto počiatočného tvrdenia 1° osobitne dokázať niekoľko prvých tvrdení $P(0), P(1), \dots, P(k)$ a potom prejsť k dôkazu modifikovaného tvrdenia 2°, totiž $(\forall n \geq k)(P(n) \Rightarrow P(n+1))$.

(b) Indukciou možno dokazovať aj tvrdenia tvaru $(\forall n \geq m)P(n)$, kde m je nejaké pevné prirodzené číslo. Stačí dokázať mierne upravené verzie tvrdení 1° a 2°: $P(m)$ a $(\forall n \geq m)(P(n) \Rightarrow P(n+1))$.

(c) Pri dôkaze indukciou možno bod 2° nahradiť tvrdením

$$(\forall n \in \mathbb{N})\big((P(0) \ \& \ \dots \ \& \ P(n)) \Rightarrow P(n+1)\big).$$

Inak povedané, pri dôkaze záveru $P(n+1)$ v bode 2° sa nemusíme opierať len o predpoklad $P(n)$, ale v prípade potreby môžeme ako predpoklady použiť všetky predchádzajúce tvrdenia $P(0), \dots, P(n)$. Takýto dôkaz indukciou sa vlastne riadi schémou

$$(\forall n \in \mathbb{N})\big((\forall k < n)P(k) \Rightarrow P(n)\big) \Rightarrow (\forall n \in \mathbb{N})P(n).$$

Rozmyslite si, jednak ako je predpoklad 1°, t. j. tvrdenie $P(0)$, už zahrnutý v predpoklade novej schémy pre $n = 0$, t. j. v tvrdení $(\forall k < 0)(P(k) \Rightarrow P(0))$, jednak ako možno transpozíciou uvedenej implikácie priamo dostať matematickú formuláciu princípu dobrého usporiadania.

0.8.2. Rekurzia. Princíp matematickej indukcie sa používa nielen na dôkazy tvrdení o prirodzených číslach. Možno ho použiť aj na konštrukciu rôznych, či už konečných alebo nekonečných postupností. V takom prípade miesto indukcie budeme radšej hovoriť o postupnosti definovanej či zostrojenej *rekurziou*.

Nech X je množina a F je zobrazenie, ktoré každej konečnej postupnosti, (usporiadanej n-tici) $(x_1, \dots, x_n)$ prvkov z X (akejkoľvek dĺžky $n \in \mathbb{N}$) priradí nejaký prvok $F(x_1, \dots, x_n) \in X$. Pomocou zobrazenia F možno zostrojiť nekonečnú postupnosť $(a_n)_{n=0}^{\infty}$ prvkov z X tak, že položíme

$$a_0 = F(\emptyset), \qquad a_{n+1} = F(a_0, a_1, \dots, a_n)$$

pre každé $n \in \mathbb{N}$. V takom prípade, hovoríme, že postupnosť (a_n) je definovaná *rekurziou* pomocou zobrazenia F.

Druhú rovnosť možno samozrejme zapísať v tvare $a_n = F(a_0, a_1, \dots, a_{n-1})$ pre $n > 0$. Taktiež možno definíciu rekurziou obmedziť len na nejaký počiatočný úsek $0, 1, \dots, n$ množiny prirodzených čísel a dostať tak rekurziou konečnú postupnosť $(a_0, a_1, \dots, a_n)$. Niekedy rekurziu začíname nie od nuly ale od jednotky, prípadne od ľubovoľného prirodzeného čísla k.

Prvým členom postupnosti (a_n) zostrojenej rekurziou pomocou zobrazenia F je prvok $a_0 = F(\emptyset) \in X$. Ďalšie členy potom vyzerajú takto: $a_1 = F(a_0)$, $a_2 = F(a_0, a_1)$, $a_3 = F(a_0, a_1, a_2)$, ..., $a_n = F(a_0, \dots, a_{n-1})$, $F(n+1) = F(a_0, \dots, a_n)$, atď.

Najčastejšie sa stretáme s prípadom, keď sa pri rekurzívnej konštrukcii člena a_{n+1} nepoužíva celá predchádzajúca časť postupnosti $(a_0, \dots, a_n)$ ale len jej posledný člen a_n. Napríklad v aritmetickej postupnosti reálnych čísel s počiatočným členom a_0 a diferenciou d platí $a_{n+1} = a_n + d$; podobne rekurentný vzťah pre geometrickú postupnosť reálnych čísel s počiatočným členom a_0 a kvocientom q má tvar $a_{n+1} = qa_n$.

Iným známym číselným príkladom je tzv. *Fibonacciho postupnosť* $(\phi_n)_{n=0}^{\infty}$, ktorej rekurzívna definícia

$$\phi_0 = \phi_1 = 1, \qquad \phi_{n+2} = \phi_n + \phi_{n+1}$$

používa dva predchádzajúce členy. Rozmyslite si, ako táto definícia zapadá do našej všeobecnej schémy.

0.8.3. Príklad. *Bellove čísla* sú definované rekurziou

$$B_0 = 1, \qquad B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k,$$

pri ktorej sa využívajú všetky predchádzajúce členy. (Pre istotu pripomíname, že $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ označuje binomický koeficient udávajúci počet k-prvkových podmnožín

n-prvkovej množiny.) Vypočítame niekoľko počiatočných hodnôt Bellových čísel:

$$B_0 = 1, \qquad B_1 = \binom{0}{0} B_0 = 1, \qquad B_2 = \binom{1}{0} B_0 + \binom{1}{1} B_1 = 2,$$

$$B_3 = \binom{2}{0} B_0 + \binom{2}{1} B_1 + \binom{2}{2} B_2 = 5,$$

$$B_4 = \binom{3}{0} B_0 + \binom{3}{1} B_1 + \binom{3}{2} B_2 + \binom{3}{3} B_3 = 15,$$

$$B_5 = \binom{4}{0} B_0 + \binom{4}{1} B_1 + \binom{4}{2} B_2 + \binom{4}{3} B_3 + \binom{4}{4} B_4 = 52, \ \dots$$

Matematickou indukciou teraz dokážeme, že počet všetkých rozkladov n-prvkovej množiny (teda aj ekvivalencií na n-prvkovej množine) je rovný číslu B_n. Zrejme na prázdnej možine existuje jediný rozklad $\mathcal{R} = \emptyset$. Predpokladajme teraz, že pre každé $k \leq n$ existuje práve B_k rozkladov k-prvkovej množiny. Všetky rozklady $(n+1)$-prvkovej množiny $\{0, 1, \dots, n\}$ možno získať nasledujúcim spôsobom:

(1) zvolíme si ľubovoľné $k \leq n$ a ľubovoľnú k-prvkovú podmnožinu A množiny $\{1, \dots, n\}$ – to pre dané k možno urobiť práve $\binom{n}{k}$ spôsobmi;

(2) vezmeme ľubovoľný rozklad $\mathcal{R}$ množiny A – ten podľa indukčného predpokladu možno vybrať práve B_k spôsobmi – a množinu $A' = \{0, 1, \dots, n\} \smallsetminus A$ pridáme k pôvodnému rozkladu $\mathcal{R}$.

Zrejme sme takto získali nejaký rozklad $\mathcal{R}_A = \mathcal{R} \cup \{A'\}$ $(n+1)$-prvkovej množiny $\{0, 1, \dots, n\}$, pričom každý rozklad $\mathcal{S}$ množiny $\{0, 1, \dots, n\}$ má tvar $\mathcal{S} = \mathcal{R}_A$ pre jednoznačne určenú dvojicu $(\mathcal{R}, A)$. Všetkých rozkladov $(n+1)$-prvkovej množiny teda je $\sum_{k=0}^{n} \binom{n}{k} B_k = B_{n+1}$.