NEŠTRUKTÚROVANÉ ROZPRAVY O ŠTRUKTÚRACH

Kapitoly z matematiky pre informatikov

2

Peter Kostolányi

13. apríla 2025

Obsah

Kapitola 1

Metrické priestory

Počiatky abstraktnej matematickej analýzy – oblasti, do ktorej možno zaradiť aj obsahovú náplň tejto kapitoly – siahajú do obdobia na prelome devätnásteho a dvadsiateho storočia. Klasické oblasti matematickej analýzy, ako napríklad diferenciálny a integrálny počet jednej či viacerých reálnych premenných alebo komplexná analýza, už v tej dobe tvorili dobre etablované, veľmi rozsiahle a – hoci v mnohom nápadne podobné – viac-menej nezávislé oblasti matematiky. Do popredia sa tak prirodzene dostávala snaha odhaľovať princípy a myšlienky týmto klasickým odvetviam spoločné.

Teóriu metrických priestorov, ktorej vznik možno datovať k Fréchetovmu článku z roku 1906 [8], možno považovať za azda najelementárnejší príklad takéhoto abstraktného pohľadu na matematickú analýzu. Táto teória vychádza z pozorovania, že dva kľúčové pojmy matematickej analýzy – pojmy limity a spojitosti funkcií – potrebujú na svoju definíciu iba jediné: vedieť „rozumným spôsobom“ určovať vzdialenosti medzi bodmi množín, ktoré tvoria obor a koobor danej funkcie.

Napríklad *limitu postupnosti* bodov $(x_n)_{n=0}^{\infty}$ množiny X definujeme – bez ohľadu na to, či je množina X daná ako $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^2$, $\mathbb{R}^3$, alebo podobne – vždy ako bod $x \in X$ taký, že pre všetky $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ také, že pre všetky prirodzené $n \geq n_0$ je

$$d(x_n, x) < \varepsilon,$$

kde $d(x_n, x)$ je vzdialenosť bodov x_n a x – pri $\mathbb{R}$ alebo $\mathbb{C}$ je touto vzdialenosťou absolútna hodnota rozdielu oboch bodov, pri $\mathbb{R}^2$ alebo $\mathbb{R}^3$ najčastejšie bežná euklidovská vzdialenosť. Podobne definícia *limity funkcie* $f\colon X' \to Y$ v bode $a \in X$, kde $X' \subseteq X$ a a je hromadným bodom X' v X, sa dá obvykle sformulovať takto: ide o bod $b \in Y$ taký, že pre všetky $\varepsilon > 0$ existuje $\delta > 0$ také, že pre všetky $x \in X' \setminus \{a\}$ je

$$d_Y(f(x), b) < \varepsilon \qquad \text{kedykoľvek} \qquad d_X(x, a) < \delta;$$

pod d_X tu rozumieme vzdialenosť prvkov X a pod d_Y vzdialenosť prvkov Y. Definíciu *hromadného bodu* množiny X' v X pritom tiež vieme vyjadriť iba s použitím pojmu vzdialenosti: ide o bod $x \in X$ taký, že pre všetky $\varepsilon > 0$ existuje bod $x' \in X' \setminus \{x\}$ spĺňajúci $d_X(x, x') \leq \varepsilon$. Funkciu $f\colon X' \to Y$ pre $X' \subseteq X$ napokon nazveme *spojitou* v bode $a \in X'$, ak pre všetky $\varepsilon > 0$ existuje $\delta > 0$ také, že pre všetky $x \in X'$ je

$$d_Y(f(x), f(a)) < \varepsilon \qquad \text{kedykoľvek} \qquad d_X(x, a) < \delta;$$

pod d_X opäť rozumieme vzdialenosť prvkov X a pod d_Y vzdialenosť prvkov Y.

Ukazuje sa, že veľká časť teórie limít a spojitosti funkcií na $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^n$ pre $n \in \mathbb{R} \setminus \{0\}$ a podobných „klasických“ oboroch funkcií skúmaných v matematickej analýze, je založená už na tých najelementárnejších vlastnostiach funkcií vzdialenosti na týchto oboroch. Abstrakciou týchto vlastností dôjdeme k pojmom *metriky* a *metrického priestoru*, umožňujúcim študovať pojmy ako limita alebo spojitosť funkcií v spoločnom rámci. Nielenže tak dospejeme k zjednoteniu teórie okolo limít a spojitosti funkcií v rôznych klasických oboroch – pojem metrického priestoru nám tieto pojmy umožní študovať aj v nových, na pohľad aj pomerne odlišných situáciách, často s relatívne prekvapivými aplikáciami. Odporúčaným čítaním k tejto kapitole sú predovšetkým knihy [15, 11, 12, 4].

1.1 Pojem metrického priestoru

Definícia 1.1.1. *Metrický priestor* je dvojica (X, d), kde X je množina a $d\colon X^2 \to \mathbb{R}_{\geq 0}$ je zobrazenie spĺňajúce pre všetky $x, y, z \in X$ nasledujúce podmienky:

(*i*) $d(x, y) = 0$ práve vtedy, keď $x = y$;

(*ii*) $d(x, y) = d(y, x)$;

(*iii*) $d(x, y) + d(y, z) \geq d(x, z)$.

Zobrazenie d v takom prípade nazývame *metrikou* na X.

Podmienka (*ii*) uvedenej definície hovorí o *symetrii* metriky a podmienka (*iii*) sa zvykne nazývať *trojuholníkovou nerovnosťou*. Občas môže byť užitočné uvažovať aj nekonečné vzdialenosti dvoch bodov a niektorí autori túto možnosť zahŕňajú do svojej definície metrického priestoru [12]; my však budeme pracovať s o niečo častejšou definíciou, pri ktorej je vzdialenosť dvoch bodov vždy konečná.

Môžeme rovno zaviesť aj niekoľko príbuzných pojmov, aj keď tieto nebudú pre naše neskoršie účely kľúčové. V prípade, že v podmienke (*i*) nahradíme ekvivalenciu implikáciou sprava doľava, získame pojem takzvaného *pseudometrického priestoru*; od metrických priestorov sa pseudometrické priestory líšia tým, že môžu obsahovať rôzne body s nulovou vzdialenosťou. Upustením od podmienky symetrickosti metriky (*ii*) v definícii 1.1.1 dostávame *kvázimetrické priestory* a vypustením trojuholníkovej nerovnosti (*iii*) zas takzvané *polometrické priestory*. Ak napokon trojuholníkovú nerovnosť (*iii*) zosilníme do podoby

$$\max\{d(x, y), d(y, z)\} \geq d(x, z),$$

dospejeme k definícii *ultrametrických priestorov*, ktoré sú metrickými priestormi so špeciálnymi vlastnosťami.

Príklad 1.1.2. Na $\mathbb{R}$ definujeme *obvyklú metriku* $d\colon \mathbb{R}^2 \to \mathbb{R}_{\geq 0}$ pre všetky $x, y \in \mathbb{R}$ ako $d(x, y) = |x-y|$. Ukážeme, že $(\mathbb{R}, d)$ je metrický priestor:

(*i*) Pre $x, y \in \mathbb{R}$ je $d(x, y) = |x - y| = 0$ práve vtedy, keď $x - y = 0$, čo nastane práve vtedy, keď $x = y$.

(*ii*) Pre všetky $x, y \in \mathbb{R}$ je $d(x, y) = |x - y| = |-(x - y)| = |y - x| = d(y, x)$.

(*iii*) Pre všetky $x, y, z \in \mathbb{R}$ je $d(x, z) = |x-z| = |(x-y)+(y-z)| \leq |x-y|+|y-z| = d(x, y)+d(x, z)$.

Príklad 1.1.3. Podobne aj na $\mathbb{C}$ môžeme definovať *obvyklú metriku* $d\colon \mathbb{C}^2 \to \mathbb{R}_{\geq 0}$ pre všetky $z, w \in \mathbb{C}$ predpisom $d(z, w) = |z - w|$. Dokážeme, že $(\mathbb{C}, d)$ je metrický priestor:

(*i*) Pre všetky $z = a + ib$ a $w = c + id$ je $|z - w| = \sqrt{(a - c)^2 + (b - d)^2}$. Keďže $(a - c)^2 \geq 0$ aj $(b - d)^2 \geq 0$, je $|z - w| = 0$ práve vtedy, keď $a - c = 0$ a zároveň $b - d = 0$, čiže práve vtedy, keď $a = c$ a $b = d$. To je ale ekvivalentné rovnosti $z = w$.

(*ii*) Pre $z = a + ib$ a $w = c + id$ je $|z - w| = \sqrt{(a - c)^2 + (b - d)^2} = \sqrt{(c - a)^2 + (d - b)^2} = |w - z|$.

(*iii*) Nech $z, w \in \mathbb{C}$. Čitateľ istotne zvládne overiť všetky kroky nasledujúcej úvahy:

$$\begin{aligned} |z + w|^2 &= (z + w)\overline{(z + w)} = (z + w)(\overline{z} + \overline{w}) = |z|^2 + |w|^2 + (z\overline{w} + w\overline{z}) = \\ &= |z|^2 + |w|^2 + \left(z\overline{w} + \overline{z\overline{w}}\right) = |z|^2 + |w|^2 + 2\operatorname{Re}(z\overline{w}) \leq |z|^2 + |w|^2 + 2\,|z\overline{w}| = \\ &= |z|^2 + |w|^2 + 2|z|\,|\overline{w}| = |z|^2 + |w|^2 + 2|z||w| = (|z| + |w|)^2. \end{aligned}$$

Z toho vďaka nezápornosti $|z + w|$ a $|z| + |w|$ vyplýva aj nerovnosť $|z| + |w| \geq |z + w|$.

V nasledujúcich príkladoch splnenie jednotlivých axióm metrického priestoru nebudeme overovať – namiesto toho túto úlohu prenecháme čitateľovi ako cvičenie.

Príklad 1.1.4. Nech $n \in \mathbb{N} \setminus \{0\}$. Na $\mathbb{R}^n$ môžeme definovať *euklidovskú metriku* $d\colon \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ pre všetky $\mathbf{x} = (x_1, \ldots, x_n)$ a $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{R}^n$ ako

$$d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_2 := \sqrt{\sum_{k=1}^{n} (x_k - y_k)^2}.$$

Ide teda o bežne definovanú vzdialenosť dvoch bodov v euklidovskom priestore.

Príklad 1.1.5. Na $\mathbb{R}^n$ pre $n \in \mathbb{N} \setminus \{0\}$ možno definovať aj viacero ďalších metrík. Jednou z nich je takzvaná *manhattanská* alebo *taxikárska* metrika daná pre všetky $\mathbf{x} = (x_1, \ldots, x_n)$ a $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{R}^n$ predpisom

$$d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_1 := \sum_{k=1}^{n} |x_k - y_k|.$$

Kým euklidovská metrika zodpovedá „vzdialenosti vzdušnou čiarou“, pri manhattanskej metrike sú „povolené iba vodorovné a zvislé pohyby“, čo pripomína pohyb po mriežkovitých uliciach *Manhattanu* (pri pomenovaní „taxikárska metrika“ ide taktiež o manhattanského taxikára).

Príklad 1.1.6. Ďalšou dôležitou metrikou na $\mathbb{R}^n$ pre $n \in \mathbb{N} \setminus \{0\}$ je takzvaná *Čebyševova metrika* daná pre všetky $\mathbf{x} = (x_1, \ldots, x_n)$ a $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{R}^n$ ako

$$d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_\infty := \max_{k=1,\ldots,n} |x_k - y_k|.$$

Uvedené príklady možno zjednotiť do spoločného rámca takzvaných *Minkowského metrík* na $\mathbb{R}^n$. Dôkaz trojuholníkovej nerovnosti si už ale pri takýchto metrikách vyžaduje aplikovať *Minkowského nerovnosť*, presnejšie jej variant pre vektory z $\mathbb{R}^n$. Pre všetky $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$ a všetky reálne čísla $p \geq 1$ tu kladieme

$$\|\mathbf{x}\|_p := \left(\sum_{k=1}^{n} |x_k|^p \right)^{1/p}.$$

Ľahko vidieť, že $\|\mathbf{x}\|_p = 0$ práve vtedy, keď $\mathbf{x} = \mathbf{0}$, pričom v opačnom prípade je norma $\|\mathbf{x}\|_p$ vektora $\mathbf{x}$ vždy kladná.

Veta 1.1.7 (Minkowského nerovnosť pre $\mathbb{R}^n$)**.** *Nech $n \in \mathbb{N} \setminus \{0\}$ a $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. Pre všetky reálne $p \geq 1$ potom*

$$\|\mathbf{x} + \mathbf{y}\|_p \leq \|\mathbf{x}\|_p + \|\mathbf{y}\|_p.$$

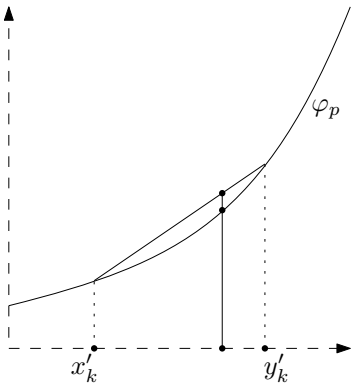
Dôkaz. Ak $\mathbf{x} = 0$ alebo $\mathbf{y} = 0$, je Minkowského nerovnosť triviálna. Predpokladajme teda, že sú oba vektory $\mathbf{x}$, $\mathbf{y}$ nenulové; normy $\|\mathbf{x}\|_p$ a $\|\mathbf{y}\|_p$ sú teda kladné. Nech $\mathbf{x}' := \mathbf{x}/\|\mathbf{x}\|_p$ a $\mathbf{y}' := \mathbf{y}/\|\mathbf{y}\|_p$. Ľahko potom vidieť, že $\|\mathbf{x}'\|_p = \|\mathbf{y}'\|_p = 1$. Položme $\mathbf{x}' =: (x'_1, \ldots, x'_n)$ a $\mathbf{y}' =: (y'_1, \ldots, y'_n)$. Z konvexnosti funkcie $\varphi_p\colon x \mapsto |x|^p$ potom pre $k = 1, \ldots, n$ a všetky $t \in [0, 1]$ dostávame

$$\left| t x'_k + (1-t) y'_k \right|^p \leq t |x'_k|^p + (1-t) |y'_k|^p. \tag{1.1}$$

Táto situácia je znázornená na obrázku 1.1.

Sčítaním obidvoch strán nerovnosti (1.1) cez $k = 1, \ldots, n$ dostávame nerovnosť

$$\|t\mathbf{x}' + (1-t)\mathbf{y}'\|_p^p \leq t\|\mathbf{x}'\|_p^p + (1-t)\|\mathbf{y}'\|_p^p = t + (1-t) = 1.$$



Obr. 1.1: Nerovnosť (1.1) z dôkazu Minkowského nerovnosti pre $\mathbb{R}^n$.

Pre $t = \|\mathbf{x}\|_p/(\|\mathbf{x}\|_p + \|\mathbf{y}\|_p)$ tak špeciálne dostávame

$$\left\| \frac{\|\mathbf{x}\|_p}{\|\mathbf{x}\|_p + \|\mathbf{y}\|_p}\mathbf{x}' + \frac{\|\mathbf{y}\|_p}{\|\mathbf{x}\|_p + \|\mathbf{y}\|_p}\mathbf{y}' \right\|_p^p = \frac{\|\mathbf{x}+\mathbf{y}\|_p^p}{(\|\mathbf{x}\|_p + \|\mathbf{y}\|_p)^p} \leq 1,$$

z čoho po prenásobení kladnou hodnotou $(\|\mathbf{x}\|_p + \|\mathbf{y}\|_p)^p$ prichádzame k nerovnosti

$$\|\mathbf{x}+\mathbf{y}\|_p^p \leq (\|\mathbf{x}\|_p + \|\mathbf{y}\|_p)^p$$

a vďaka nezápornosti hodnôt $\|\mathbf{x}+\mathbf{y}\|_p$ a $\|\mathbf{x}\|_p + \|\mathbf{y}\|_p$ tak aj ku kýženej nerovnosti

$$\|\mathbf{x}+\mathbf{y}\|_p \leq \|\mathbf{x}\|_p + \|\mathbf{y}\|_p,$$

čím je veta dokázaná. □

Príklad 1.1.8. Na $\mathbb{R}^n$ pre $n \in \mathbb{N}\setminus\{0\}$ môžeme pre každé reálne $p \geq 1$ definovať takzvanú *Minkowského p-metriku*. Tá je pre všetky $\mathbf{x} = (x_1, \ldots, x_n)$ a $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{R}^n$ daná ako

$$d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_p = \left(\sum_{k=1}^{n} |x_k - y_k|^p \right)^{1/p}.$$

Platnosť axióm (i) a (ii) definície metrického priestoru možno nahliadnuť okamžite. Trojuholníková nerovnosť je tu dôsledkom Minkowského nerovnosti: pre všetky $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^n$ je

$$d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) = \|\mathbf{x} - \mathbf{y}\|_p + \|\mathbf{y} - \mathbf{z}\|_p \geq \|(\mathbf{x} - \mathbf{y}) + (\mathbf{y} - \mathbf{z})\|_p = \|\mathbf{x} - \mathbf{z}\|_p = d(\mathbf{x}, \mathbf{z}).$$

Euklidovská aj manhattanská metrika sú evidentne špeciálnymi prípadmi p-metriky pre $p = 2$ resp. pre $p = 1$. Čebyševovu metriku môžeme z p-metrík získať limitným prechodom – nie je ťažké vidieť, že pre všetky $\mathbf{x} = (x_1, \ldots, x_n)$ a $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{R}^n$ je

$$\lim_{p\to\infty} \|\mathbf{x} - \mathbf{y}\|_p = \lim_{p\to\infty} \left(\sum_{k=1}^{n} |x_k - y_k|^p \right)^{1/p} = \max_{k=1,\ldots,n} |x_k - y_k| = \|\mathbf{x} - \mathbf{y}\|_\infty.$$

Pokračujme ďalšími príkladmi metrických priestorov, pri ktorých overenie axióm definície 1.1.1 prenechávame čitateľovi ako jednoduché cvičenie.

Príklad 1.1.9. Na ľubovoľnej množine X môžeme definovať takzvanú *diskrétnu metriku* $d\colon X^2 \to \mathbb{R}_{\geq 0}$ danú pre všetky $x, y \in X$ ako

$$d(x, y) = \begin{cases} 1 & \text{ak } x \neq y, \\ 0 & \text{ak } x = y. \end{cases}$$

Metrický – ba dokonca očividne aj ultrametrický – priestor (X, d) nazývame *diskrétnym metrickým priestorom* na X. Pomenovanie „diskrétny“ pri tomto priestore pochopíme onedlho.

Príklad 1.1.10. Vzdialenosť $\mathrm{dist}_{\mathcal{G}}(u, v)$ dvojice vrcholov u, v súvislého *neorientovaného grafu* $\mathcal{G}$, definovaná ako počet hrán na najkratšej ceste spájajúcej vrcholy u a v, je očividne metrikou na množine vrcholov grafu $\mathcal{G}$. Pri nesúvislých grafoch ide o metriku, ktorá môže nadobúdať aj hodnotu ∞ (vlastnosti takýchto metrík sú ale v mnohom podobné klasickým metrikám). Podobne pri súvislých ohodnotených neorientovaných grafoch, kde ohodnotenia hrán vyberáme z množiny $\mathbb{R}_{>0}$, možno uvažovať metriku na množine vrcholov, ktorá dvojici vrcholov u, v priradí cenu najlacnejšej cesty z u do v. V prípade ohodnotení z množiny $\mathbb{R}_{\geq 0}$ takto dostávame už len pseudometrický priestor.

Príklad 1.1.11. V *orientovaných grafoch* $\mathcal{G}$ zrejme nemožno očakávať prirodzený pojem vzdialenosti, ktorý by spĺňal axiómu symetrickosti. Ľahko ale vidieť, že množina vrcholov každého silne súvislého orientovaného grafu tvorí spolu s funkciou vzdialenosti z vrcholu u do vrcholu v, definovanou prostredníctvom počtu hrán na najkratšej orientovanej ceste z u do v, kvázimetrický priestor. Vo všeobecných orientovaných grafoch ide o kvázimetrický priestor, ktorého kvázimetrika môže nadobúdať aj hodnotu ∞. Podobne ako pri neorientovaných grafoch možno kvázimetriku definovať aj pomocou najlacnejších ciest v silne súvislých ohodnotených orientovaných grafoch nad $\mathbb{R}_{>0}$.

Nasledujúce dva príklady zohrávajú dôležitú úlohu predovšetkým v oblasti *funkcionálnej analýzy*.

Príklad 1.1.12. Uvažujme množinu $C([a, b])$ všetkých spojitých funkcií na uzavretom intervale $[a, b]$ pre nejaké $-\infty < a < b < \infty$. Všetky takéto funkcie sú ohraničené a riemannovsky integrovateľné. Navyše je zrejmé, že kladná reálna mocnina absolútnej hodnoty spojitej funkcie na $[a, b]$ je opäť spojitou funkciou na $[a, b]$. Pre všetky reálne $p \geq 1$ a všetky $f \in C([a, b])$ tak môžeme definovať *Minkowského p-normu* funkcie f predpisom

$$\|f\|_p := \left(\int_a^b |f(t)|^p \, \mathrm{d}t \right)^{1/p}.$$

Dôkaz Minkowského nerovnosti pre $\mathbb{R}^n$ ľahko upravíme na dôkaz Minkowského nerovnosti pre spojité funkcie: pre všetky $f, g \in C([a, b])$ a všetky $p \geq 1$ je

$$\|f + g\|_p \leq \|f\|_p + \|g\|_p.$$

Odtiaľ už rovnako ako v prípade Minkowského metrík na $\mathbb{R}^n$ vyplýva, že na množine $C([a, b])$ môžeme pre každé $p \geq 1$ a všetky $f, g \in C([a, b])$ definovať *Minkowského p-metriku* predpisom $d(f, g) = \|f - g\|_p$.

Ďalej môžeme pre všetky $f \in C([a, b])$ položiť

$$\|f\|_\infty := \max_{t \in [a,b]} |f(t)|$$

(existencia maxima tu vyplýva z uzavretosti a ohraničenosti obrazu funkcie f definovanej na ohraničenom intervale). Nie je potom ťažké overiť, že

$$\lim_{p \to \infty} \|f\|_p = \|f\|_\infty$$

a že funkcia d definovaná pre všetky $f, g \in C([a, b])$ ako $d(f, g) = \|f - g\|_\infty$ je metrikou na $C([a, b])$.

V skutočnosti možno podobné metriky definovať na omnoho väčších triedach funkcií – Minkowského p-normu môžeme definovať napríklad pre všetky lebesgueovsky integrovateľné funkcie (znalosť tohto pojmu tu nie je kľúčová) na podmnožine reálnej osi, pričom príslušnú p-metriku z nej získame rovnakým spôsobom. Takéto priestory sú v matematickej analýze známe ako L^p priestory. Charakterizácia metriky získaná v limite pre $p \to \infty$, prislúchajúca k tzv. L^∞ priestorom, je tu ale o niečo málo komplikovanejšia než pri priestoroch spojitých funkcií.

Príklad 1.1.13. Ďalším typom priestorov, na ktorom možno definovať obdobu Minkowského p-metrík, sú priestory vhodných nekonečných postupností (napríklad) reálnych čísel. Pre všetky $p \geq 1$ môžeme označiť ako ℓ^p priestor všetkých postupností $\mathbf{x} = (x_n)_{n=0}^{\infty}$ reálnych čísel takých, že rad

$$\sum_{n=0}^{\infty} |x_n|^p$$

konverguje. *Minkowského p-normu* postupnosti $\mathbf{x} = (x_n)_{n=0}^{\infty} \in \ell^p$ potom môžeme definovať ako

$$\|\mathbf{x}\|_p := \left(\sum_{n=0}^{\infty} |x_n|^p \right)^{1/p}$$

a príslušná *Minkowského p-metrika* je potom pre všetky $\mathbf{x}, \mathbf{y} \in \ell^p$ daná ako $d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_p$. Dôkaz, že skutočne ide o metriku, si opäť vyžaduje iba drobnú úpravu dôkazu Minkowského nerovnosti pre $\mathbb{R}^n$. Pre $p = \infty$ môžeme napokon vziať za ℓ^∞ priestor všetkých ohraničených reálnych postupností a pre každú takúto postupnosť $\mathbf{x} = (x_n)_{n=0}^{\infty}$ môžeme definovať

$$\|\mathbf{x}\|_\infty := \sup_{n=0,1,2,\ldots} |x_n|.$$

Príslušná metrika je opäť daná predpisom $d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_\infty$ pre všetky $\mathbf{x}, \mathbf{y} \in \ell^\infty$.

Zbierku príkladov metrických priestorov zavŕšme niekoľkými (z pohľadu matematickej analýzy) menej klasickými priestormi.

Príklad 1.1.14. Pre každú abecedu Σ a všetky $n \in \mathbb{N}$ môžeme na jazyku Σ^n všetkých slov dĺžky n nad abecedou Σ uvažovať *Hammingovu vzdialenosť* H definovanú pre každú dvojicu slov $u, v \in \Sigma^n$ ako počet pozícií, na ktorých tieto slová obsahujú rôzne písmená – čiže pre všetky $a_1, \ldots, a_n, b_1, \ldots, b_n \in \Sigma$ je

$$H(a_1 \ldots a_n, b_1 \ldots b_n) = |\{k \in [n] \mid a_k \neq b_k\}|.$$

Ľahko vidieť, že (Σ^n, H) je metrický priestor.

Príklad 1.1.15. Pomerne dôležitý príklad úplne odlišného druhu súvisí s formálnymi jazykmi: pre ľubovoľnú abecedu Σ a ľubovoľnú dvojicu jazykov $L, K \subseteq \Sigma^*$ môžeme definovať ich vzdialenosť nasledujúcim spôsobom:

$$d(L, K) = \begin{cases} 2^{-\min\{|w| \mid w \in \Sigma^*;\ w \in (L \setminus K) \cup (K \setminus L)\}} & \text{ak } L \neq K, \\ 0 & \text{ak } L = K. \end{cases}$$

Na výpočet vzdialenosti sa teda využíva dĺžka najkratšieho slova w, na ktorom sa jazyky L a K líšia – čiže jeden z jazykov slovo w obsahuje a druhý nie. Za vzdialenosť sa pritom pre takéto w berie hodnota $2^{-|w|}$; čím dlhšie je teda najkratšie slovo, na ktorom sa jazyky odlišujú, za tým bližšie sa tieto jazyky pokladajú. Nie je ťažké dokázať, že $(2^{\Sigma^*}, d)$ je metrický – dokonca ultrametrický – priestor.

Príklad 1.1.16. Techniku z predchádzajúceho príkladu možno ľahko rozšíriť aj na formálne mocninové rady o niekoľkých nekomutatívnych premenných s koeficientmi v polokruhu. Nech S je polokruh a Σ je abeceda. Pre ľubovoľnú dvojicu radov $r, s \in S\langle\langle \Sigma^* \rangle\rangle$ potom môžeme položiť

$$d(r, s) = \begin{cases} 2^{-\min\{|w| \mid w \in \Sigma^*;\ (r,w) \neq (s,w)\}} & \text{ak } r \neq s, \\ 0 & \text{ak } r = s. \end{cases}$$

Opäť možno ľahko dokázať, že $(S\langle\langle \Sigma^* \rangle\rangle, d)$ je metrickým a dokonca aj ultrametrickým priestorom. Podobne možno definovať metriku aj pre rady o niekoľkých komutatívnych premenných.

Príklad 1.1.17. Pomocou vzdialeností jazykov a formálnych mocninových radov z predchádzajúcich dvoch príkladov možno zaviesť metriky aj na množinách usporiadaných n-tíc jazykov alebo mocninových radov. Opíšeme všeobecnejšiu konštrukciu pre formálne mocninové rady s koeficientmi v polokruhu S (pre formálne jazyky stačí zvoliť $S = \mathbb{B}$). Pre každú abecedu Σ a každé $n \in \mathbb{N} \setminus \{0\}$ môžeme na $(S\langle\langle\Sigma^*\rangle\rangle)^n$ definovať vzdialenosť d' pre všetky $(r_1, \ldots, r_n), (s_1, \ldots, s_n) \in (S\langle\langle\Sigma^*\rangle\rangle)^n$ ako

$$d'((r_1, \ldots, r_n), (s_1, \ldots, s_n)) = \max_{k=1,\ldots,n} d(r_k, s_k),$$

kde d je vzdialenosť z príkladu 1.1.16. Opäť nie je ťažké dokázať, že $((S\langle\langle\Sigma^*\rangle\rangle)^n, d')$ je metrický priestor.

Je zrejmé, že pre ľubovoľný metrický priestor (X, d) a ľubovoľnú množinu $Y \subseteq X$ je $(Y, d|_{Y\times Y})$, kde $d|_{Y\times Y}$ označuje zúženie zobrazenia $d\colon X \times X \to \mathbb{R}_{\geq 0}$ na $Y \times Y$, opäť metrickým priestorom. Tým je zaručená korektnosť nasledujúcej definície.

Definícia 1.1.18. Nech (X, d) je metrický priestor. *Podpriestorom* priestoru (X, d) nazveme ľubovoľný metrický priestor (Y, d'), kde $Y \subseteq X$ a $d' = d|_{Y\times Y}$.

1.2 Základy topológie metrických priestorov

Definícia 1.2.1. Nech (X, d) je metrický priestor a $a \in X$ je jeho bod.

a) *Okolím* bodu a o polomere $r > 0$ nazveme množinu

$$D(a, r) := \{x \in X \mid d(a, x) < r\}.$$

b) *Uzavretým okolím* bodu a o polomere $r > 0$ nazveme množinu

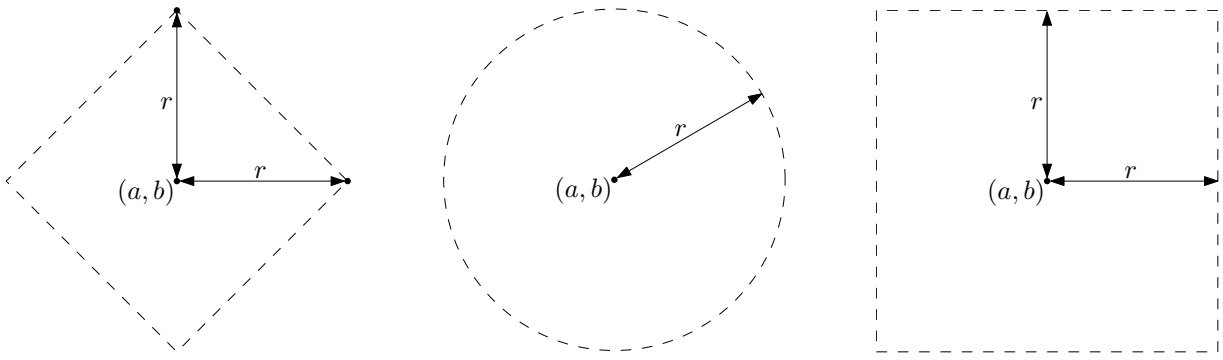
$$\overline{D}(a, r) := \{x \in X \mid d(a, x) \leq r\}.$$

c) *Prstencovým okolím* bodu a o polomere $r > 0$ nazveme množinu

$$D'(a, r) := D(a, r) \setminus \{a\}.$$

Príklad 1.2.2. V metrickom priestore $\mathbb{R}$ (s obvyklou metrikou) je okolím bodu $a \in \mathbb{R}$ o polomere r otvorený interval $(a - r, a + r)$.

Príklad 1.2.3. Okolia bodu (a, b) o polomere $r > 0$ v metrických priestoroch s nosnou množinou $\mathbb{R}^2$ a s manhattanskou, euklidovskou resp. Čebyševovou metrikou sú znázornené na obrázku 1.2.



(a) Pri manhattanskej metrike. **(b)** Pri euklidovskej metrike. **(c)** Pri Čebyševovej metrike.

Obr. 1.2: Okolia bodu $(a, b) \in \mathbb{R}^2$ o polomere $r > 0$ pri rôznych metrikách.

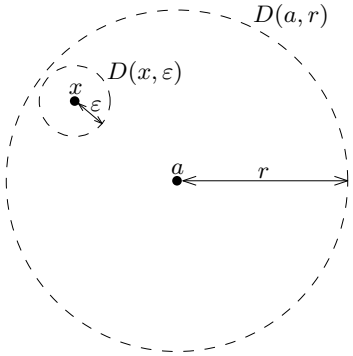
Príklad 1.2.4. V diskrétnom metrickom priestore (X, d) je pre ľubovoľný bod $a \in X$ okolie $D(a, r)$ rovné jednoprvkovej množine $\{a\}$ pre $0 < r \leq 1$ a celému metrickému priestoru X pre $r > 1$. Odtiaľ aj pomenovanie „diskrétny“ priestor – ku každému jeho bodu totiž možno nájsť okolie obsahujúce jedine tento bod sám.

Definícia 1.2.5. Nech (X, d) je metrický priestor a $S \subseteq X$ je množina. Hovoríme, že množina S je *otvorená* v X, ak pre všetky $x \in S$ existuje $\varepsilon > 0$ také, že $D(x, \varepsilon) \subseteq S$.

Príklad 1.2.6. V každom metrickom priestore (X, d) je každé okolie $D(a, r)$ pre $a \in X$ a $r > 0$ otvorenou množinou. Pre ľubovoľné $x \in D(a, r)$ totiž musí byť $d(a, x) < r$. Zvoľme $\varepsilon > 0$ tak, aby $\varepsilon \leq r - d(a, x)$. Potom $D(x, \varepsilon) \subseteq D(a, r)$, pretože pre všetky $y \in D(x, \varepsilon)$ z trojuholníkovej nerovnosti dostávame

$$d(a, y) \leq d(a, x) + d(x, y) < d(a, x) + \varepsilon \leq d(a, x) + (r - d(a, x)) = r.$$

Situácia je schematicky znázornená na obrázku 1.3.



Obr. 1.3: Každé okolie $D(a, r)$ bodu a je otvorenou množinou.

Príklad 1.2.7. Podobne možno ukázať, že v každom metrickom priestore (X, d) sú otvorené aj všetky množiny $\{x \in X \mid d(a, x) > r\}$ pre $a \in X$ a $r \geq 0$.

Príklad 1.2.8. Prázdna množina $\emptyset$ a celá nosná množina X sú triviálne otvorené v každom metrickom priestore (X, d).

Tvrdenie 1.2.9. *Nech (X, d) je metrický priestor. Množina $S \subseteq X$ je potom otvorená v X práve vtedy, keď je zjednotením nejakého systému okolí bodov priestoru X (ľubovoľnej kardinality).*

Dôkaz. Ak je S zjednotením systému okolí bodov X, pre všetky $x \in S$ musia existovať $a \in X$ a $r > 0$ také, že $x \in D(a, r) \subseteq S$. Okolie $D(a, r)$ je podľa príkladu 1.2.6 otvorenou množinou, a teda musí existovať $\varepsilon > 0$ také, že $D(x, \varepsilon) \subseteq D(a, r) \subseteq S$: množina S je otvorená.

Ak je naopak množina S otvorená, môžeme pre všetky $x \in S$ nájsť $\varepsilon_x > 0$ také, že $D(x, \varepsilon_x) \subseteq S$. Potom

$$S = \bigcup_{x \in S} D(x, \varepsilon_x),$$

pretože každé $x \in S$ je prvkom $D(x, \varepsilon_x)$. □

Veta 1.2.10. *Nech (X, d) je metrický priestor. Potom:*

(*i*) *Ľubovoľné zjednotenie otvorených množín v X je otvorená množina v X.*

(*ii*) *Ľubovoľný* konečný *prienik otvorených množín v X je otvorená množina v X.*

Dôkaz. Ľubovoľný bod x zjednotenia otvorených množín musí patriť do nejakej z týchto otvorených množín. Preto existuje $\varepsilon > 0$ také, že $D(x, \varepsilon)$ je podmnožinou tejto množiny a tým pádom aj pôvodne uvažovaného zjednotenia.

Ľubovoľný prvok x prieniku otvorených množín $S_1, \ldots, S_n$ musí patriť do každej z týchto množín, a teda pre $k = 1, \ldots, n$ existuje ε_k také, že $D(x, \varepsilon_k) \subseteq S_k$. Ak teda označíme ako ε najmenšiu spomedzi hodnôt $\varepsilon_1, \ldots, \varepsilon_n$, musí byť $D(x, \varepsilon) \subseteq S_1 \cap \ldots \cap S_n$. □

Definícia 1.2.11. Nech (X, d) je metrický priestor a $S \subseteq X$ je množina.

a) *Hromadným bodom* množiny S v X nazveme ľubovoľné $x \in X$ také, že pre všetky $\varepsilon > 0$ obsahuje prstencové okolie $D'(x, \varepsilon)$ aspoň jeden bod množiny S.

b) *Izolovaným bodom* množiny S nazveme bod $x \in S$, ktorý nie je hromadným bodom množiny S v X.

c) Množina S je *uzavretá* v X, ak je množina $X \setminus S$ otvorená v X.

d) *Uzáverom* množiny S v X nazveme množinu $\overline{S}$ danú zjednotením S s množinou všetkých jej hromadných bodov v X.

Príklad 1.2.12. Z príkladu 1.2.7 je zrejmé, že v každom metrickom priestore (X, d) je uzavreté okolie $\overline{D}(a, r)$ uzavretou množinou pre všetky $a \in X$ a $r > 0$.

Príklad 1.2.13. Z príkladu 1.2.8 vidieť, že množiny $\emptyset$ a X sú v každom metrickom priestore (X, d) súčasne otvorené aj uzavreté.

Príklad 1.2.14. Ľahko vidieť, že každá podmnožina diskrétneho metrického priestoru je súčasne otvorená aj uzavretá.

Tvrdenie 1.2.15. *Nech (X, d) je metrický priestor a $S \subseteq X$ je množina. Množina S je uzavretá v X práve vtedy, keď obsahuje všetky svoje hromadné body v X.*

Dôkaz. Množina S je uzavretá v X práve vtedy, keď je množina $X \setminus S$ otvorená. To je pravda práve vtedy, keď pre všetky $x \in X \setminus S$ existuje $\varepsilon > 0$ také, že $D(x, \varepsilon) \subseteq X \setminus S$, čiže $D'(x, \varepsilon)$ neobsahuje žiaden bod množiny S. To je práve vtedy, keď žiadne $x \in X \setminus S$ nie je hromadným bodom S, t.j. keď S obsahuje všetky svoje hromadné body. □

Tvrdenie 1.2.16. *Nech (X, d) je metrický priestor a $S \subseteq X$ je množina. Potom je množina $\overline{S}$ uzavretá.*

Dôkaz. Nech $x \in X$ je hromadný bod množiny $\overline{S}$. Pre všetky $\varepsilon > 0$ potom $D'(x, \varepsilon)$ obsahuje aspoň jeden bod $a \in \overline{S}$. Potom buď $a \in S$, alebo je bod a hromadným bodom množiny S, a teda pre všetky $\delta > 0$ obsahuje $D'(a, \delta)$ aspoň jeden bod množiny S; v druhom prípade zvoľme δ tak, aby bolo $\delta < \min\{d(a, x), \varepsilon - d(a, x)\}$. Zisťujeme potom, že $D'(x, \varepsilon)$ obsahuje aspoň jeden bod množiny S; keďže je $\varepsilon > 0$ ľubovoľné, je x hromadným bodom množiny S, a teda patrí do $\overline{S}$. Množina $\overline{S}$ teda obsahuje všetky svoje hromadné body a je uzavretá podľa tvrdenia 1.2.15. □

Tvrdenie 1.2.17. *Nech (X, d) je metrický priestor a $S \subseteq X$ je množina. Potom:*

(i) Množina S je uzavretá v X práve vtedy, keď $\overline{S} = S$.

(ii) Uzáver $\overline{S}$ množiny S je najmenšou uzavretou množinou T spĺňajúcou $S \subseteq T \subseteq X$.

Dôkaz. Tvrdenie (i) je bezprostredným dôsledkom tvrdenia 1.2.15 a definície uzáveru. Na dôkaz (ii) si stačí uvedomiť, že vďaka tvrdeniu 1.2.15 a definícii uzáveru musí každá uzavretá nadmnožina S obsahovať $\overline{S}$, z čoho $T \supseteq \overline{S}$; opačná inklúzia je dôsledkom tvrdenia 1.2.16. □

Veta 1.2.18. *Nech (X, d) je metrický priestor. Potom:*

(*i*) *Ľubovoľné* konečné *zjednotenie uzavretých množín v X je uzavretá množina v X.*

(*ii*) *Ľubovoľný prienik uzavretých množín v X je uzavretá množina v X.*

Dôkaz. Ide o bezprostredný dôsledok vety 1.2.10 a definície uzavretých množín. □

Definícia 1.2.19. Nech (X, d) je metrický priestor a $S \subseteq X$ je množina.

a) *Vnútorným bodom* množiny S v X nazveme ľubovoľný bod $x \in S$ taký, že pre nejaké $\varepsilon > 0$ je $D(x, \varepsilon) \subseteq S$.

b) *Vnútrom* množiny S v X nazveme množinu $\mathrm{Int}(S)$ všetkých jej vnútorných bodov.

c) *Hraničným bodom* množiny S v X nazveme ľubovoľný bod $x \in X$ taký, že pre všetky $\varepsilon > 0$ obsahuje $D(x, \varepsilon)$ aspoň jeden bod v S a aspoň jeden bod v $X \setminus S$.

d) *Hranicou* množiny S v X nazveme množinu ∂S všetkých jej hraničných bodov.

Tvrdenie 1.2.20. *Nech (X, d) je metrický priestor a $S \subseteq X$ je množina. Potom:*

a) Vnútro $\mathrm{Int}(S)$ *množiny S je otvorená množina v X.*

b) Vnútro $\mathrm{Int}(S)$ *množiny S je najväčšou podmnožinou S otvorenou v X.*

c) Množina S je otvorená v X práve vtedy, keď $S = \mathrm{Int}(S)$.

d) Množiny $\mathrm{Int}(S)$ *a ∂S sú disjunktné a $\overline{S} = \mathrm{Int}(S) \cup \partial S$.*

e) Hranica ∂S množiny S je uzavretá množina v X.

f) Platí $\partial S = \partial(X \setminus S)$.

g) Množina S je uzavretá v X práve vtedy, keď $\partial S \subseteq S$.

Dôkaz. Prenechávame čitateľovi ako cvičenie. □

1.3 Konvergencia v metrických priestoroch

S využitím aparátu okolí môžeme definíciu limity postupnosti v metrickom priestore (X, d) sformulovať napríklad nasledovne:

Definícia 1.3.1. Nech (X, d) je metrický priestor a $(x_n)_{n=0}^{\infty}$ je postupnosť bodov X. Hovoríme, že postupnosť $(x_n)_{n=0}^{\infty}$ *konverguje* k bodu $x \in X$, ak pre všetky $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ také, že pre všetky prirodzené $n \geq n_0$ je $x_n \in D(x, \varepsilon)$. V takom prípade tiež hovoríme, že x je *limitou* postupnosti $(x_n)_{n=0}^{\infty}$ v X a píšeme $x = \lim_{n\to\infty} x_n$ alebo $x_n \to x$ pre $n \to \infty$.

Uvedená podmienka na postupnosť $(x_n)_{n=0}^{\infty}$ je samozrejme ekvivalentná tomu, že pre všetky $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ také, že pre všetky $n \geq n_0$ je $d(x, x_n) < \varepsilon$.

Príklad 1.3.2. V metrických priestoroch $\mathbb{R}$ a $\mathbb{C}$ s obvyklou metrikou špecializáciou definície 1.3.1 evidentne získavame zvyčajnú definíciu limity postupnosti.

Príklad 1.3.3. Zvyčajný pojem limity tiež zrejme dostaneme v priestore $\mathbb{R}^m$ pre $m \in \mathbb{N}\setminus\{0\}$ s euklidovskou metrikou. Ukážeme teraz, že ten istý pojem limity dostaneme aj pri manhattanskej a Čebyševovej metrike: budú konvergovať rovnaké postupnosti, a to k rovnakým limitám. Skutočne: pre ľubovoľný vektor $\mathbf{x} = (x_1, \ldots, x_m)$ uvažujme jeho normy

$$\|\mathbf{x}\|_1 = \sum_{k=1}^{m} |x_k|, \qquad \|\mathbf{x}\|_2 = \sqrt{\sum_{k=1}^{m} x_k^2}, \qquad \|\mathbf{x}\|_\infty = \max_{k=1,\ldots,m} |x_k|.$$

Zrejme

$$m\|\mathbf{x}\|_\infty \geq \|\mathbf{x}\|_1 \geq \|\mathbf{x}\|_2 \geq \|\mathbf{x}\|_\infty. \tag{1.2}$$

Nech teraz $(\mathbf{x}_n)_{n=0}^\infty$ je ľubovoľná postupnosť vektorov z $\mathbb{R}^m$. Ak $\mathbf{x}_n \to \mathbf{x}$ pre $n \to \infty$ pri manhattanskej metrike, musí pre všetky $\varepsilon > 0$ existovať $n_0 \in \mathbb{N}$ také, že pre všetky prirodzené $n \geq n_0$ je

$$\|\mathbf{x}_n - \mathbf{x}\|_1 < \varepsilon.$$

Z (1.2) potom vyplýva, že aj

$$\|\mathbf{x}_n - \mathbf{x}\|_2 < \varepsilon$$

a $\mathbf{x}_n \to \mathbf{x}$ pre $n \to \infty$ pri euklidovskej metrike. Rovnako konvergencia k $\mathbf{x}$ pri euklidovskej metrike implikuje konvergenciu k $\mathbf{x}$ pri Čebyševovej metrike. Ak napokon $\mathbf{x}_n \to \mathbf{x}$ pre $n \to \infty$ pri Čebyševovej metrike, pre všetky $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ také, že pre všetky prirodzené $n \geq n_0$ je

$$\|\mathbf{x}_n - \mathbf{x}\|_\infty < \varepsilon/m,$$

z čoho podľa (1.2) dostávame

$$\|\mathbf{x}_n - \mathbf{x}\|_1 < \varepsilon.$$

Postupnosť $(\mathbf{x}_n)_{n=0}^\infty$ teda konverguje k $\mathbf{x}$ pri niektorej z uvažovaných metrík práve vtedy, keď konverguje k $\mathbf{x}$ pri ktorejkoľvek ďalšej z týchto metrík. V skutočnosti sme pri našej argumentácii využili *ekvivalenciu metrík*, čo je pojem, ktorým sa budeme zaoberať neskôr.

Príklad 1.3.4. Nech (X, d) je diskrétny metrický priestor. Ľahko potom vidieť, že postupnosť $(x_n)_{n=0}^\infty$ bodov priestoru X konverguje k bodu $x \in X$ práve vtedy, keď existuje $n_0 \in \mathbb{N}$ také, že pre všetky $n \geq n_0$ je $x_n = x$; postupnosť sa teda musí ustáliť na hodnote x.

Ako je dobre známe, konvergentnosť postupnosti *reálnych čísel* je ekvivalentná splneniu Cauchyho-Bolzanovho kritéria konvergencie. Ako uvidíme, v metrických priestoroch je splnenie tohto kritéria vo všeobecnosti iba nutnou podmienkou konvergencie postupnosti – postupnosti, ktoré ho spĺňajú nazveme *cauchyovskými*.

Definícia 1.3.5. Nech (X, d) je metrický priestor a $(x_n)_{n=0}^\infty$ je postupnosť bodov X. Hovoríme, že postupnosť $(x_n)_{n=0}^\infty$ je *cauchyovská*, ak pre všetky $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ také, že pre všetky prirodzené $n, m \geq n_0$ je $d(x_n, x_m) < \varepsilon$.

Tvrdenie 1.3.6. *Nech (X, d) je metrický priestor. Každá konvergentná postupnosť bodov X je potom cauchyovská.*

Dôkaz. Ak $x_n \to x$ pre $n \to \infty$, musí pre všetky $\varepsilon > 0$ existovať $n_0 \in \mathbb{N}$ také, že pre všetky prirodzené $n, m \geq n_0$ je $d(x, x_n) < \varepsilon/2$ a $d(x, x_m) < \varepsilon/2$. Z trojuholníkovej nerovnosti a symetrickosti metriky d potom $d(x_n, x_m) \leq d(x_n, x) + d(x, x_m) = d(x, x_n) + d(x, x_m) < \varepsilon$. □

Príklad 1.3.7. Uvažujme otvorený interval $(0, 1)$ ako podpriestor metrického priestoru $\mathbb{R}$ s obvyklou metrikou. Postupnosť $(1/n)_{n=1}^\infty$ je potom cauchyovská, ale nie je konvergentná v priestore $(0, 1)$. V priestoroch $[0, 1]$, $[0, 1)$, alebo $\mathbb{R}$ by už išlo o konvergentnú postupnosť.

Tvrdenie 1.3.8. *Nech (X,d) je metrický priestor a $(a_n)_{n=0}^{\infty}$ je konvergentná postupnosť bodov X taká, že množina $A=\{a_n \mid n\in\mathbb{N}\}$ je nekonečná. Potom je limita postupnosti $(a_n)_{n=0}^{\infty}$ hromadným bodom množiny A.*

Dôkaz. Nech $\lim_{n\to\infty} a_n = a$ a nech a nie je hromadný bod množiny A. V takom prípade existuje $\varepsilon>0$ také, že $D'(a,\varepsilon)\cap A=\emptyset$. Podľa definície limity postupnosti ale pre to isté $\varepsilon>0$ musí existovať $n_0\in\mathbb{N}$ také, že pre všetky prirodzené $n\geq n_0$ je $a_n\in D(a,\varepsilon)$. Všetky tieto hodnoty sú ale v A priamo z definície tejto množiny. Z toho vyplýva, že pre všetky $n\geq n_0$ musí byť $a_n=a$ a množina A je tým pádom konečná. □

Pojem limity zobrazenia medzi dvoma metrickými priestormi je oproti pojmu limity postupnosti bodov metrického priestoru o niečo menej dôležitý; pre úplnosť ho ale tiež aspoň v krátkosti preskúmajme.

Definícia 1.3.9. Nech (X,d) a (X',d') sú metrické priestory, $S\subseteq X$ je množina a $f\colon S\to X'$ je zobrazenie. Nech a je hromadný bod množiny S v metrickom priestore X. Hovoríme, že zobrazenie f nadobúda v bode a limitu $b\in X'$, ak pre všetky $\varepsilon>0$ existuje $\delta>0$ také, že pre všetky $x\in D'(a,\delta)\cap S$ je $f(x)\in D(b,\varepsilon)$. V takom prípade píšeme $b=\lim_{x\to a} f(x)$ alebo $f(x)\to b$ pre $x\to a$.

Veta 1.3.10 (Heineho definícia limity)**.** *Nech (X,d) a (X',d') sú metrické priestory, $S\subseteq X$ je množina a $f\colon S\to X'$ je zobrazenie. Nech a je hromadný bod množiny S v metrickom priestore X a $b\in X'$. Potom $\lim_{x\to a} f(x)=b$ práve vtedy, keď pre všetky postupnosti $(x_n)_{n=0}^{\infty}$ bodov $S\setminus\{a\}$ konvergujúce k bodu a je $\lim_{n\to\infty} f(x_n)=b$.*

Dôkaz. Predpokladajme najprv, že $\lim_{x\to a} f(x)=b$ a uvažujme ľubovoľnú postupnosť $(x_n)_{n=0}^{\infty}$ bodov $S\setminus\{a\}$ konvergujúcu k a. Pre všetky $\delta>0$ potom existuje $n_0\in\mathbb{N}$ také, že pre všetky prirodzené $n\geq n_0$ je $d(a,x_n)<\delta$. Z konvergencie funkcie f v bode a k b ďalej vyplýva, že pre všetky $\varepsilon>0$ existuje $\delta>0$ také, že pre všetky $x\in S\setminus\{a\}$ s $d(a,x)<\delta$ je $d(b,f(x))<\varepsilon$. Spojením týchto dvoch vlastností dohromady zisťujeme, že pre všetky $\varepsilon>0$ existuje $n_0\in\mathbb{N}$ také, že pre všetky prirodzené $n\geq n_0$ je $d(b,f(x_n))<\varepsilon$. Postupnosť $(f(x_n))_{n=0}^{\infty}$ teda konverguje k bodu b.

Naopak predpokladajme, že pre všetky postupnosti $(x_n)_{n=0}^{\infty}$ bodov $S\setminus\{a\}$ konvergujúce k a je $f(x_n)\to b$ pre $n\to\infty$. Za účelom sporu predpokladajme, že limita $\lim_{x\to a} f(x)$ neexistuje, alebo nie je rovná b. To znamená, že existuje $\varepsilon>0$ také, že pre všetky $\delta>0$ existuje bod $x\in D'(a,\delta)\cap S$ taký, že $f(x)\notin D(b,\varepsilon)$. Pre dané ε s touto vlastnosťou potom môžeme postupne voliť $\delta=1/n$ pre $n=1,2,3,\ldots$ a získať tak postupnosť $(x_n)_{n=0}^{\infty}$ bodov $S\setminus\{a\}$ takú, že pre všetky $n\in\mathbb{N}\setminus\{0\}$ je $d(a,x_n)<1/n$ a súčasne $d(b,f(x_n))\geq\varepsilon$. Táto postupnosť $(x_n)_{n=0}^{\infty}$ evidentne konverguje k a, avšak postupnosť $(f(x_n))_{n=0}^{\infty}$ zrejme nemôže konvergovať k b – spor s naším pôvodným predpokladom. □

1.4 Úplné metrické priestory

Vrátime sa teraz ku konvergencii postupností bodov metrického priestoru a preskúmame významnú triedu metrických priestorov, pre ktoré je konvergencia postupnosti ekvivalentná jej cauchyovskosti. Takéto metrické priestory nazveme *úplnými*.

Definícia 1.4.1. Metrický priestor (X,d) je *úplný*, ak je každá cauchyovská postupnosť $(x_n)_{n=0}^{\infty}$ bodov priestoru X konvergentná v X.

Príklad 1.4.2. Metrické priestory $\mathbb{R}$ a $\mathbb{C}$ s obvyklými metrikami sú úplné.

Príklad 1.4.3. Diskrétny metrický priestor (X,d) nad ľubovoľnou nosnou množinou X je úplný, pretože pre každú cauchyovskú postupnosť $(x_n)_{n=0}^{\infty}$ bodov X musí evidentne existovať $n_0\in\mathbb{N}$ také, že pre všetky prirodzené $n,m\geq n_0$ je $x_n=x_m=x$. Takáto postupnosť potom konverguje k bodu x.

Veta 1.4.4. *Nech (X,d) je úplný metrický priestor a $Y \subseteq X$. Podpriestor $(Y, d|_{Y\times Y})$ priestoru X je potom úplný práve vtedy, keď je množina Y uzavretá v X.*

Dôkaz. Predpokladajme najprv, že $Y \subseteq X$ je množina taká, že priestor $(Y, d|_{Y\times Y})$ je úplný. Aby sme dokázali, že je množina Y uzavretá v X, stačí podľa tvrdenia 1.2.15 dokázať, že Y obsahuje všetky svoje hromadné body v X. Nech je teda a hromadný bod množiny Y v X. Pre všetky $\varepsilon > 0$ potom $D'(a,\varepsilon) \cap Y \neq \emptyset$. Pre $n = 1, 2, 3, \ldots$ postupne zvoľme $a_n \in D'(a, 1/n) \cap Y$. Postupnosť bodov $(a_n)_{n=0}^{\infty}$ množiny Y potom v priestore X evidentne konverguje k bodu a. Podľa tvrdenia 1.3.6 tak musí byť cauchyovská. Z úplnosti podpriestoru Y teda vyplýva, že $(a_n)_{n=0}^{\infty}$ musí konvergovať aj v priestore Y. Je jasné, že jedinou možnou limitou postupnosti $(a_n)_{n=0}^{\infty}$ je a – preto $a \in Y$. Množina Y je teda skutočne uzavretá.

Nech je naopak množina Y uzavretá v X. Uvažujme ľubovoľnú cauchyovskú postupnosť $(a_n)_{n=0}^{\infty}$ bodov množiny Y. Ako postupnosť v úplnom metrickom priestore X musí $(a_n)_{n=0}^{\infty}$ konvergovať k nejakému bodu $a \in X$. Na dôkaz úplnosti podpriestoru Y potrebujeme ukázať, že $a \in Y$. Ak je množina $A = \{a_n \mid n \in \mathbb{N}\}$ konečná, evidentne $a \in A \subseteq Y$. Ak je táto množina nekonečná, musí byť a podľa tvrdenia 1.3.8 hromadným bodom množiny A, a teda aj množiny $Y \supseteq A$. Z uzavretosti množiny Y teda vyplýva, že skutočne $a \in Y$ a podpriestor Y je úplný. □

Definícia 1.4.5. Nech (X,d) je metrický priestor a $S \subseteq X$. *Priemer* množiny S je hodnota

$$d(S) = \sup\{d(x,y) \mid x, y \in S\} \in \mathbb{R}_{\geq 0} \cup \{\infty\}.$$

Veta 1.4.6. *Nech (X,d) je metrický priestor. Nasledujúce tvrdenia sú potom ekvivalentné:*

(i) Metrický priestor (X,d) je úplný.

(ii) Pre ľubovoľný nekonečný reťazec $A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots$ neprázdnych uzavretých množín v X spĺňajúci $d(A_n) \to 0$ pre $n \to \infty$ je prienik $\bigcap_{n=0}^{\infty} A_n$ neprázdny.

(iii) Pre ľubovoľný nekonečný reťazec $A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots$ neprázdnych uzavretých množín v X spĺňajúci $d(A_n) \to 0$ pre $n \to \infty$ obsahuje prienik $\bigcap_{n=0}^{\infty} A_n$ práve jeden prvok.

Dôkaz. Dokážme najprv, že z tvrdenia *(i)* vyplýva tvrdenie *(ii)*. Predpokladajme, že je priestor (X,d) úplný a uvažujme nekonečný reťazec $A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots$ uzavretých množín v X spĺňajúci $d(A_n) \to 0$ pre $n \to \infty$. Pre všetky $n \in \mathbb{N}$ zvoľme prvok $a_n \in A_n$. Postupnosť $(a_n)_{n=0}^{\infty}$ je potom cauchyovská, pretože z konvergencie priemerov množín A_n k nule vyplýva, že pre všetky $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ také, že pre všetky prirodzené $n \geq n_0$ je $d(A_n) < \varepsilon$; pre všetky $m \geq n \geq n_0$ teda tiež

$$d(a_n, a_m) \leq \sup\{d(x,y) \mid x, y \in A_n\} = d(A_n) < \varepsilon.$$

Z úplnosti priestoru X teda vyplýva, že postupnosť $(a_n)_{n=0}^{\infty}$ konverguje k limite $a \in X$. Ak je teraz množina $A = \{a_n \mid n \in \mathbb{N}\}$ konečná, musí existovať $n_0 \in \mathbb{N}$ také, že $a_n = a$ pre všetky $n \geq n_0$. Z toho vyplýva, že $a \in A_n$ pre všetky $n \in \mathbb{N}$, a teda aj $a \in \bigcap_{n=0}^{\infty} A_n$. Ak je naopak množina $A = \{a_n \mid n \in \mathbb{N}\}$ nekonečná, musí byť a podľa tvrdenia 1.3.8 jej hromadným bodom. Navyše musí byť pre všetky $m \in \mathbb{N}$ nekonečná aj množina $A(m) = \{a_n \mid n \geq m\}$ a bod a tak musí byť aj jej hromadným bodom. Keďže ale $A(m) \subseteq A_m$, je bod a hromadným bodom množiny A_m a z uzavretosti množiny A_m vyplýva $a \in A_m$. Keďže je $m \in \mathbb{N}$ ľubovoľné, opäť dostávame $a \in \bigcap_{n=0}^{\infty} A_n$.

Z tvrdenia *(ii)* evidentne vyplýva tvrdenie *(iii)*: keďže $d(A_n) \to 0$ pre $n \to \infty$, nemôže prienik $\bigcap_{n=0}^{\infty} A_n$ obsahovať dva rôzne prvky, ktoré by museli mať nenulovú vzdialenosť.

Dokážme napokon, že z tvrdenia *(iii)* vyplýva tvrdenie *(i)*. Predpokladajme platnosť tvrdenia *(iii)* a uvažujme ľubovoľnú cauchyovskú postupnosť $(x_n)_{n=0}^{\infty}$ bodov priestoru X. Pre všetky $n \in \mathbb{N}$ položme $X_n := \overline{\{x_m \mid m \geq n\}}$. Evidentne potom $X_0 \supseteq X_1 \supseteq X_2 \supseteq \ldots$ a z cauchyovskosti postupnosti $(x_n)_{n=0}^{\infty}$ ľahko vidieť, že $d(X_n) \to 0$ pre $n \to \infty$. Podľa tvrdenia *(iii)* tak existuje bod $x \in \bigcap_{n=0}^{\infty} X_n$. Dokážeme, že ide o limitu postupnosti $(x_n)_{n=0}^{\infty}$. Skutočne: pre všetky $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ také, že pre všetky $n \geq n_0$ je $d(X_n) < \varepsilon$. Špeciálne $d(X_{n_0}) < \varepsilon$, a teda aj $d(x, x_n) < \varepsilon$ pre všetky $n \geq n_0$. Naozaj teda $x_n \to x$ pre $n \to \infty$ a veta je dokázaná. □

Naším ďalším cieľom bude dokázať, že priestory ako napríklad $\mathbb{R}^n$ pre $n \in \mathbb{N} \setminus \{0\}$ a rozličné Minkowského metriky sú úplné. Tento fakt ale odvodíme z o niečo všeobecnejšieho pozorovania.

Nech $p \geq 1$ je reálne číslo. Pre ľubovoľné prirodzené $n \geq 1$ a ľubovoľných n metrických priestorov $(X_1, d_1), \ldots, (X_n, d_n)$ potom môžeme na nosnej množine

$$X_1 \times X_2 \times \ldots \times X_n$$

definovať tzv. *súčinovú p-metriku* d pre všetky $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in X_1 \times \ldots \times X_n$ predpisom

$$d((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \left(\sum_{k=1}^{n} (d_k(x_k, y_k))^p \right)^{1/p} = \|(d_1(x_1, y_1), \ldots, d_n(x_n, y_n))\|_p.$$

Overme, že skutočne ide o metriku. Keďže pre $k = 1, \ldots, n$ je $d_k(x_k, y_k) = 0$ práve vtedy, keď $x_k = y_k$, je jasné, že $d((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = 0$ práve vtedy, keď $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$. Podobne zo symetrickosti metrík $d_1, \ldots, d_n$ zrejme vyplýva symetrickosť metriky d. Z trojuholníkovej nerovnosti v jednotlivých metrických priestoroch $X_1, \ldots, X_n$ a z Minkowského nerovnosti pre $\mathbb{R}^n$ napokon pre všetky $(x_1, \ldots, x_n), (y_1, \ldots, y_n), (z_1, \ldots, z_n) \in X_1 \times \ldots \times X_n$ dostávame

$$\begin{aligned}
d((x_1, \ldots, x_n), (z_1, \ldots, z_n)) &= \|(d_1(x_1, z_1), \ldots, d_n(x_n, z_n))\|_p \leq \\
&\leq \|(d_1(x_1, y_1) + d_1(y_1, z_1), \ldots, d_n(x_n, y_n) + d_n(y_n, z_n))\|_p = \\
&= \|(d_1(x_1, y_1), \ldots, d_n(x_n, y_n)) + (d_1(y_1, z_1), \ldots, d_n(y_n, z_n))\|_p \leq \\
&\leq \|(d_1(x_1, y_1), \ldots, d_n(x_n, y_n))\|_p + \|(d_1(y_1, z_1), \ldots, d_n(y_n, z_n))\|_p = \\
&= d((x_1, \ldots, x_n), (y_1, \ldots, y_n)) + d((y_1, \ldots, y_n), (z_1, \ldots, z_n)).
\end{aligned}$$

Pre $p = \infty$ definujeme súčinovú Čebyševovu metriku pre $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in X_1 \times \ldots \times X_n$ predpisom

$$d((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \max_{k=1,\ldots,n} d_k(x_k, y_k) = \|(d_1(x_1, y_1), \ldots, d_n(x_n, y_n))\|_\infty.$$

Dôkaz, že skutočne ide o metriku, prenechávame čitateľovi.

Veta 1.4.7. *Nech $(X_1, d_1), \ldots, (X_k, d_k)$, kde $k \geq 1$, sú úplné metrické priestory a $p \in [1, \infty) \cup \{\infty\}$. Nech d je súčinová p-metrika na $X_1 \times \ldots \times X_k$. Potom je metrický priestor $(X_1 \times \ldots \times X_k, d)$ úplný.*

Dôkaz. Všimnime si najprv, že nech je p akékoľvek, pre všetky $(x_1, \ldots, x_k), (y_1, \ldots, y_k) \in X_1 \times \ldots \times X_k$ určite

$$\|(d_1(x_1, y_1), \ldots, d_k(x_k, y_k))\|_\infty \leq \|(d_1(x_1, y_1), \ldots, d_k(x_k, y_k))\|_p \leq k\|(d_1(x_1, y_1), \ldots, d_k(x_k, y_k))\|_\infty,$$

čiže

$$\max_{j=1,\ldots,k} d_j(x_j, y_j) \leq d((x_1, \ldots, x_k), (y_1, \ldots, y_k)) \leq k \cdot \max_{j=1,\ldots,k} d_j(x_j, y_j). \tag{1.3}$$

Nech $(\mathbf{x}_n)_{n=0}^\infty$ je cauchyovská postupnosť prvkov priestoru $X_1 \times \ldots \times X_k$. Pre všetky $n \in \mathbb{N}$ položme $\mathbf{x}_n =: (x_n[1], \ldots, x_n[k])$. Pre všetky $\varepsilon > 0$ potom existuje $n_0 \in \mathbb{N}$ také, že pre všetky $n, m \geq n_0$ je $d(\mathbf{x}_n, \mathbf{x}_m) < \varepsilon$. Podľa (1.3) potom pre všetky $n, m \geq n_0$ aj

$$\max_{j=1,\ldots,k} d_j(x_n[j], x_m[j]) < \varepsilon,$$

a teda

$$d_j(x_n[j], x_m[j]) < \varepsilon$$

pre $j = 1, \ldots, k$. Postupnosti $(x_n[j])_{n=0}^\infty$ sú teda cauchyovské pre $j = 1, \ldots, k$ a z úplnosti priestorov $X_1, \ldots, X_k$ vyplýva, že pre $j = 1, \ldots, k$ existuje $x[j] \in X$ také, že pre $n \to \infty$ je $x_n[j] \to x[j]$. To

znamená, že pre $j = 1, \ldots, k$ a všetky $\varepsilon > 0$ existuje $n_0[j] \in \mathbb{N}$ také, že pre všetky $n \geq n_0[j]$ je $d_j(x_n[j], x[j]) < \varepsilon/k$. Ak teraz za n_0 vezmeme najväčšie spomedzi čísel $n_0[1], \ldots, n_0[k]$, zistíme, že $d_j(x_n[j], x[j]) < \varepsilon/k$ pre všetky $n \geq n_0$ a $j = 1, \ldots, k$. Pre všetky $n \geq n_0$ preto aj

$$\max_{j=1,\ldots,k} d_j(x_n[j], x[j]) < \varepsilon/k$$

a podľa (1.3) teda pre $\mathbf{x} = (x[1], \ldots, x[k])$ dostávame

$$d(\mathbf{x}_n, \mathbf{x}) < \varepsilon.$$

Keďže je $\varepsilon > 0$ ľubovoľné, je postupnosť $(\mathbf{x}_n)_{n=0}^{\infty}$ konvergentná; a keďže je $(\mathbf{x}_n)_{n=0}^{\infty}$ ľubovoľná cauchyovská postupnosť v $X_1 \times \ldots \times X_k$, je tento metrický priestor úplný. □

Príklad 1.4.8. Nech $n \in \mathbb{N} \setminus \{0\}$, $p \in [1, \infty) \cup \{\infty\}$ a d je p-metrika na $\mathbb{R}^n$. Metrika d je potom evidentne súčinovou p-metrikou pre n kópií metrického priestoru $\mathbb{R}$ s obvyklou metrikou. Keďže je metrický priestor $\mathbb{R}$ úplný, musí byť podľa vety 1.4.7 úplný aj metrický priestor $(\mathbb{R}^n, d)$.

Naše prvotné skúmanie úplných metrických priestorov ukončíme pozorovaním zásadného významu: *ľubovoľný* metrický priestor možno zúplniť, t.j. rozšíriť na úplný metrický priestor. Ešte prv si však musíme vyjasniť, čo presne budeme mať pod týmto zúplnením resp. rozšírením na mysli. Neuspokojíme sa pritom s pozorovaním, že každý metrický priestor je podpriestorom *nejakého* úplného priestoru, ale budeme sa snažiť pridať čo možno najmenej nových bodov. To vyjadríme požiadavkou, aby bol pôvodne uvažovaný metrický priestor vo svojom zúplnení *hustý*. Naopak – v súlade s dobrými zvykmi pri skúmaní matematických štruktúr – umožníme za účelom sprehľadnenia celej konštrukcie „premenovanie bodov“ pôvodne uvažovaného priestoru; ten teda nemusí byť priamo podmnožinou svojho zúplnenia, ale musí byť nejakej podmnožine zúplnenia „izomorfný“, pričom pod „izomorfizmom“ budeme v tomto prípade chápať surjektívne *izometrie* definované nižšie.[1]

Definícia 1.4.9. Nech (X, d) je metrický priestor a $S \subseteq X$. Množina S je *hustá* v X, ak $\overline{S} = X$.

Definícia 1.4.10. Nech (X, d), (X', d') sú metrické priestory. *Izometriou* medzi priestormi X a X' nazveme ľubovoľné zobrazenie $\varphi\colon X \to X'$ také, že pre všetky $x, y \in X$ je $d'(\varphi(x), \varphi(y)) = d(x, y)$.

Ľahko vidieť, že každá izometria musí byť injektívna. Surjektívne izometrie sú teda nutne bijektívne a možno ich považovať za druh „izomorfizmu“ metrických priestorov (rozumných konceptov „izomorfizmu“ ale pri metrických priestoroch existuje viacero).

Definícia 1.4.11. Nech (X, d) je metrický priestor. *Zúplnením* priestoru (X, d) nazveme ľubovoľný úplný metrický priestor (X', d'), pre ktorý existuje izometria $\varphi\colon X \to X'$ taká, že množina $\varphi(X)$ je v priestore X' hustá.

Nižšie budeme dokazovať, že ku každému metrickému priestoru možno skonštruovať jeho zúplnenie. Konštrukciu pritom do veľkej miery založíme na nasledujúcej leme.

Lema 1.4.12. *Nech (X, d) je metrický priestor a $(x_n)_{n=0}^{\infty}$ a $(y_n)_{n=0}^{\infty}$ sú cauchyovské postupnosti v X. Potom existuje limita*

$$\lim_{n\to\infty} d(x_n, y_n).$$

Dôkaz. Keďže sú obidve uvažované postupnosti cauchyovské, pre všetky $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ také, že pre všetky $n, m \geq n_0$ je $d(x_n, x_m) < \varepsilon/2$, ako aj $n_1 \in \mathbb{N}$ také, že pre všetky $n, m \geq n_1$ je $d(y_n, y_m) < \varepsilon/2$.

[1] V prípade potreby by sme body obrazu pôvodného metrického priestoru v jeho zúplnení samozrejme mohli „premenovať nazad“ a získať tak úplný metrický priestor, ktorý je skutočným nadpriestorom pôvodne uvažovaného. Avšak jediné, čo by sme tým dosiahli, by bolo značné zneprehľadnenie konštrukcie.

Nech N je väčšie spomedzi čísel n_0, n_1. Pre všetky $n, m \geq N$ potom $d(x_n, x_m) < \varepsilon/2$ a $d(y_n, y_m) < \varepsilon/2$. V dôsledku toho s využitím trojuholníkovej nerovnosti pre všetky $n, m \geq N$ dostávame

$$d(x_n, y_n) \leq d(x_n, x_m) + d(x_m, y_m) + d(y_m, y_n) < d(x_m, y_m) + \varepsilon$$

a naopak

$$d(x_m, y_m) \leq d(x_m, x_n) + d(x_n, y_n) + d(y_n, y_m) < d(x_n, y_n) + \varepsilon.$$

Keďže je ε ľubovoľné, je postupnosť $(d(x_n, y_n))_{n=0}^{\infty}$ bodov úplného metrického priestoru $\mathbb{R}$ cauchyovská, a teda musí konvergovať k nejakej limite. □

Nech (X, d) je ľubovoľný metrický priestor. Uvažujme množinu $\mathrm{cau}(X)$ všetkých cauchyovských postupností bodov X. Definujme na nej reláciu $\sim$ nasledovne: pre dvojicu cauchyovských postupností $(x_n)_{n=0}^{\infty}$ a $(y_n)_{n=0}^{\infty}$ položíme $(x_n)_{n=0}^{\infty} \sim (y_n)_{n=0}^{\infty}$ práve vtedy, keď

$$\lim_{n\to\infty} d(x_n, y_n) = 0.$$

Ako triviálne cvičenie prenechávame čitateľovi dôkaz, že $\sim$ je relácia ekvivalencie na $\mathrm{cau}(X)$.

Označenie 1.4.13. Nech (X, d) je metrický priestor. Potom $U(X) := \mathrm{cau}(X)/\sim$.

Definujme teraz na $U(X)$ zobrazenie $d_{U(X)} \colon U(X)^2 \to \mathbb{R}_{\geq 0}$ pre všetky $(x_n)_{n=0}^{\infty}, (y_n)_{n=0}^{\infty} \in \mathrm{cau}(X)$ predpisom

$$d_{U(X)}\left([(x_n)_{n=0}^{\infty}]_{\sim}, [(y_n)_{n=0}^{\infty}]_{\sim}\right) = \lim_{n\to\infty} d(x_n, y_n).$$

Čitateľovi prenechávame ako cvičenie dôkaz, že zobrazenie $d_{U(X)}$ nezávisí od výberu reprezentantov a že ide o metriku na $U(X)$.

Veta 1.4.14. *Nech (X, d) je metrický priestor. Potom je metrický priestor $(U(X), d_{U(X)})$ zúplnením metrického priestoru (X, d).*

Dôkaz. Dokážme najprv, že je metrický priestor $(U(X), d_{U(X)})$ úplný. Uvažujme ľubovoľnú cauchyovskú postupnosť $([(x_{m,n})_{n=0}^{\infty}]_{\sim})_{m=0}^{\infty}$ bodov priestoru $U(X)$. Pre všetky $\varepsilon > 0$ potom existuje $m_0(\varepsilon) \in \mathbb{N}$ také, že pre všetky $m, m' \geq m_0(\varepsilon)$ je vzdialenosť $[(x_{m,n})_{n=0}^{\infty}]_{\sim}$ od $[(x_{m',n})_{n=0}^{\infty}]_{\sim}$ pri metrike $d_{U(X)}$ menšia ako ε. To znamená, že

$$\lim_{n\to\infty} d(x_{m,n}, x_{m',n}) < \varepsilon.$$

Pre všetky $m \in \mathbb{N}$ je navyše postupnosť $(x_{m,n})_{n=0}^{\infty}$ cauchyovská. Existuje teda $n_0(m) \in \mathbb{N}$ také, že pre všetky prirodzené $n, n' \geq n_0(m)$ je

$$d(x_{m,n}, x_{m,n'}) < 1/m.$$

Bez ujmy na všeobecnosti predpokladajme, že pre všetky prirodzené $m \leq m'$ je $n_0(m) \leq n_0(m')$.

Uvažujme teraz postupnosť $(x_{m,n_0(m)})_{m=0}^{\infty}$. Dokážme najprv, že táto postupnosť je cauchyovská. Nech $\varepsilon > 0$ je ľubovoľné a nech $M \in \mathbb{N}$ je také, že $1/M < \varepsilon/4$ a súčasne $M \geq m_0(\varepsilon/4)$. Vezmime ľubovoľné $m' \geq m \geq M$. Pre všetky $n \geq n_0(m')$ potom

$$\begin{aligned} d(x_{m,n_0(m')}, x_{m',n_0(m')}) &< d(x_{m,n_0(m')}, x_{m,n}) + d(x_{m,n}, x_{m',n}) + d(x_{m',n}, x_{m',n_0(m')}) < \\ &< 1/m + d(x_{m,n}, x_{m',n}) + 1/m' < 2/M + d(x_{m,n}, x_{m',n}) < \\ &< \varepsilon/2 + d(x_{m,n}, x_{m',n}). \end{aligned} \tag{1.4}$$

Pritom

$$\lim_{n\to\infty} d(x_{m,n}, x_{m',n}) < \varepsilon/4,$$

takže musí existovať $n \geq n_0(m')$ také, že $d(x_{m,n}, x_{m',n}) < \varepsilon/4$. Podľa (1.4) teda zisťujeme, že pre všetky $m' \geq m \geq M$ je

$$d(x_{m,n_0(m')}, x_{m',n_0(m')}) < 3\varepsilon/4.$$

S použitím trojuholníkovej nerovnosti potom

$$\begin{aligned} d(x_{m,n_0(m)}, x_{m',n_0(m')}) &\leq d(x_{m,n_0(m)}, x_{m,n_0(m')}) + d(x_{m,n_0(m')}, x_{m',n_0(m')}) < \\ &< 1/m + d(x_{m,n_0(m')}, x_{m',n_0(m')}) < \varepsilon/4 + 3\varepsilon/4 = \varepsilon \end{aligned}$$

a keďže je $\varepsilon > 0$ ľubovoľné, je postupnosť $(x_{m,n_0(m)})_{m=0}^{\infty}$ cauchyovská. V nasledujúcom budeme pri tejto postupnosti namiesto indexovej premennej m používať premennú n.

Dokážeme, že postupnosť $([(x_{m,n})_{n=0}^{\infty}]_{\sim})_{m=0}^{\infty}$ konverguje v priestore $U(X)$ k bodu $[(x_{n,n_0(n)})_{n=0}^{\infty}]_{\sim}$, z čoho bezprostredne vyplynie úplnosť priestoru $U(X)$. Za tým účelom je potrebné ukázať, že

$$\lim_{m\to\infty} \lim_{n\to\infty} d(x_{m,n}, x_{n,n_0(n)}) = 0. \tag{1.5}$$

Nech $\varepsilon > 0$ je ľubovoľné. Zvoľme $M \in \mathbb{N}$ tak, aby $1/M < \varepsilon/2$ a aby pre všetky $k, k' \geq M$ bolo $d(x_{k,n_0(k)}, x_{k',n_0(k')}) < \varepsilon/2$. Pre všetky $m \geq M$ zvoľme $N \in \mathbb{N}$ tak, aby $N \geq M$ a $N \geq n_0(m)$. Pre všetky $n \geq N$ potom z trojuholníkovej nerovnosti

$$d(x_{m,n}, x_{n,n_0(n)}) \leq d(x_{m,n}, x_{m,n_0(m)}) + d(x_{m,n_0(m)}, x_{n,n_0(n)}) < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

Pre všetky $m \geq M$ teda

$$\lim_{n\to\infty} d(x_{m,n}, x_{n,n_0(n)}) \leq \varepsilon$$

a keďže je ε ľubovoľné, je rovnosť (1.5), ako aj úplnosť priestoru $U(X)$, dokázaná.

Zostáva nájsť izometriu $\varphi\colon X \to U(X)$ takú, že množina $\varphi(X)$ je hustá v $U(X)$. Dokážeme, že hľadaná izometria je pre všetky $x \in X$ daná predpisom

$$\varphi(x) = [(x)_{n=0}^{\infty}]_{\sim}.$$

Je triviálnym cvičením dokázať, že skutočne ide o izometriu. Aby sme dokázali, že množina $\varphi(x)$ je v priestore $U(X)$ hustá, potrebujeme dokázať, že pre každú cauchyovskú postupnosť $(x_n)_{n=0}^{\infty}$ prvkov X je $[(x_n)_{n=0}^{\infty}]_{\sim}$ prvkom alebo hromadným bodom množiny $\varphi(X)$.

Dokážeme, že $[(x_n)_{n=0}^{\infty}]_{\sim}$ je prvkom alebo hromadným bodom množiny

$$E = \{[(x_k)_{n=0}^{\infty}]_{\sim} \mid k \in \mathbb{N}\}$$

a tým pádom aj množiny $\varphi(X)$. Skutočne: keďže je postupnosť $(x_n)_{n=0}^{\infty}$ cauchyovská, musí pre všetky $\varepsilon > 0$ existovať $n_0 \in \mathbb{N}$ také, že pre všetky $n \geq n_0$ je $d(x_{n_0}, x_n) < \varepsilon/2$. Potom

$$\lim_{n\to\infty} d(x_{n_0}, x_n) \leq \varepsilon/2,$$

kde existencia limity vyplýva z lemy 1.4.12. Vzdialenosť bodov $[(x_{n_0})_{n=0}^{\infty}]_{\sim} \in E$ a $[(x_n)_{n=0}^{\infty}]_{\sim}$ priestoru $U(X)$ je preto menšia ako ε. Pre všetky $\varepsilon > 0$ tak okolie $D([(x_n)_{n=0}^{\infty}]_{\sim}, \varepsilon)$ obsahuje aspoň jeden bod množiny E. Ak je niektorým z nich bod $[(x_n)_{n=0}^{\infty}]_{\sim}$ sám, je $[(x_n)_{n=0}^{\infty}]_{\sim} \in E$; v opačnom prípade je $[(x_n)_{n=0}^{\infty}]_{\sim}$ hromadným bodom množiny E v $U(X)$. □

Hoci sa práve opísaná konštrukcia môže zdať trochu umelá, jej výsledky sa vo väčšine prípadov zhodujú s tým, čo by sme od zúplnenia intuitívne očakávali. Tak napríklad pre ľubovoľný *úplný* metrický priestor X je $U(X)$ stále len metrickým priestorom X (resp. jeho obrazom pri vhodnej izometrii). Každá cauchyovská postupnosť $(x_n)_{n=0}^{\infty}$ bodov priestoru X totiž konverguje k nejakej limite L a ľahko vidieť, že v takom prípade musí byť $[(x_n)_{n=0}^{\infty}]_{\sim} = [(L)_{n=0}^{\infty}]_{\sim} \in \varphi(X)$. Čitateľ tiež pomocou analogickej argumentácie ľahko overí, že pre ľubovoľný podpriestor Y úplného metrického priestoru X možno priestor $U(Y)$ stotožniť s uzáverom priestoru Y v X, čiže s najmenším úplným podpriestorom X obsahujúcim Y.

1.5 Spojité zobrazenia na metrických priestoroch

Spojité zobrazenia medzi dvojicou metrických priestorov definujeme, podobne ako pri limitách, priamočiarym zovšeobecnením definície pre reálne funkcie reálnej premennej.

Definícia 1.5.1. Nech (X,d) a (X',d') sú metrické priestory, $S \subseteq X$ je množina a $f\colon S \to X'$ je zobrazenie. Hovoríme, že zobrazenie f je *spojité* v bode $a \in S$, ak pre všetky $\varepsilon > 0$ existuje $\delta > 0$ také, že pre všetky $x \in D(a,\delta) \cap S$ je $f(x) \in D(f(a),\varepsilon)$.

Zobrazenie f je teda spojité v bode $a \in S$ práve vtedy, keď pre všetky $\varepsilon > 0$ existuje $\delta > 0$ také, že pre všetky $x \in S$ je $d'(f(a),f(x)) < \varepsilon$ kedykoľvek $d(a,x) < \delta$. Všimnime si, že z uvedenej definície bezprostredne vyplýva, že každé zobrazenie je spojité v izolovaných bodoch svojho definičného oboru; hodnotu δ totiž v takom prípade možno zvoliť tak, aby bolo $D'(a,\delta) \cap S = \emptyset$.

Podobne ako pre reálne funkcie reálnej premennej platia nasledujúce jednoduché ekvivalentné charakterizácie spojitosti v bode.

Tvrdenie 1.5.2. *Nech (X,d) a (X',d') sú metrické priestory, $S \subseteq X$ je množina a $f\colon S \to X'$ je zobrazenie. Zobrazenie f je spojité v bode $a \in S$ práve vtedy, keď je a izolovaným bodom množiny S, alebo je a hromadným bodom množiny S a $\lim_{x\to a} f(x) = f(a)$.*

Dôkaz. Ako sme už pozorovali, zobrazenie f je nutne spojité vo všetkých izolovaných bodoch svojho oboru S. Stačí teda ukázať, že $f\colon S \to X'$ je spojité v hromadnom bode $a \in S$ množiny S práve vtedy, keď $\lim_{x\to a} f(x) = f(a)$. Avšak spojitosť zobrazenia f v bode a znamená, že pre všetky $\varepsilon > 0$ existuje $\delta > 0$ také, že pre všetky $x \in D(a,\delta) \cap S$ je $f(x) \in D(f(a),\varepsilon)$. Keďže triviálne $f(a) \in D(f(a),\varepsilon)$, možno túto vlastnosť ekvivalentne sformulovať s $x \in D'(a,\delta) \cap S$. To už však je priamo z definície limity zobrazenia ekvivalentné tomu, že $\lim_{x\to a} f(x) = f(a)$. □

Tvrdenie 1.5.3. *Nech (X,d) a (X',d') sú metrické priestory, $S \subseteq X$ je množina a $f\colon S \to X'$ je zobrazenie. Zobrazenie f je spojité v bode $a \in S$ práve vtedy, keď pre všetky postupnosti $(x_n)_{n=0}^{\infty}$ bodov množiny S spĺňajúce $\lim_{n\to\infty} x_n = a$ je $\lim_{n\to\infty} f(x_n) = f(a)$.*

Dôkaz. Ak je a izolovaným bodom množiny S, musí pre každú postupnosť $(x_n)_{n=0}^{\infty}$ bodov S spĺňajúcu $\lim_{n\to\infty} x_n = a$ existovať $n_0 \in \mathbb{N}$ také, že pre všetky $n \geq n_0$ je $x_n = a$. Evidentne teda $\lim_{n\to\infty} f(x_n) = f(a)$. Ak je naopak $a \in S$ hromadným bodom množiny S, je podľa tvrdenia 1.5.2 zobrazenie f spojité v bode a práve vtedy, keď $\lim_{x\to a} f(x) = f(a)$. To je podľa Heineho definície limity ekvivalentné tomu, že pre všetky postupnosti $(x_n)_{n=0}^{\infty}$ bodov $S \setminus \{a\}$ je $\lim_{n\to\infty} f(x_n) = f(a)$ kedykoľvek $\lim_{n\to\infty} x_n = a$. To je však ďalej ekvivalentné tomu, že táto vlastnosť platí pre všetky postupnosti $(x_n)_{n=0}^{\infty}$ bodov S: pre ľubovoľnú takúto postupnosť totiž buď $x_n = a$ pre všetky dostatočne veľké n, alebo podpostupnosť jej prvkov rôznych od a konverguje k a; v oboch prípadoch ľahko vidieť, že $\lim_{n\to\infty} f(x_n) = f(a)$. □

Definícia 1.5.4. Nech (X,d) a (X',d') sú metrické priestory, $S \subseteq X$ je množina a $f\colon S \to X'$ je zobrazenie. Hovoríme, že f je *spojité* na množine $T \subseteq S$, ak je spojité v každom bode $a \in T$. Hovoríme, že f je *spojité*, ak je spojité na S.

Príklad 1.5.5. Každé zobrazenie $f\colon X \to X'$ z diskrétneho metrického priestoru (X,d) do *ľubovoľného* metrického priestoru (X',d') je spojité, pretože každý bod priestoru X je izolovaný.

Príklad 1.5.6. Každá izometria $f\colon X \to X'$ medzi dvojicou metrických priestorov (X,d) a (X',d') je spojité zobrazenie. Nech totiž zvolíme $a \in X$ ľubovoľne, tak pre všetky $\varepsilon > 0$ a všetky $x \in X$ z nerovnosti $d(a,x) < \varepsilon$ vyplýva $d'(f(a),f(x)) = d(a,x) < \varepsilon$.

Nasledujúca veta síce ľahko vyplýva z tvrdenia 1.5.3, no napriek tomu ide o dôležitú charakterizáciu spojitých zobrazení: spojité zobrazenia sú zobrazenia zachovávajúce limity postupností.

Veta 1.5.7. *Nech (X,d) a (X',d') sú metrické priestory, $S \subseteq X$ je množina a $f\colon S \to X'$ je zobrazenie. Zobrazenie f je spojité práve vtedy, keď pre všetky postupnosti $(x_n)_{n=0}^{\infty}$ bodov množiny S spĺňajúce $\lim_{n\to\infty} x_n = x$ pre nejaké $x \in S$ je $\lim_{n\to\infty} f(x_n) = f(x)$. To znamená:*

$$\lim_{n\to\infty} f(x_n) = f\left(\lim_{n\to\infty} x_n\right)$$

kedykoľvek limita $\lim_{n\to\infty} x_n$ existuje a patrí do S.

Dôkaz. Bezprostredne z tvrdenia 1.5.3 a definície spojitého zobrazenia. □

Dokážme teraz ďalšiu dôležitú charakterizáciu spojitých zobrazení medzi metrickými priestormi, na ktorej je okrem iného založená definícia spojitých zobrazení medzi topologickými priestormi. Obmedzíme sa pritom na zobrazenia, ktorých oborom je celý metrický priestor. V prípade potreby uvažovať zobrazenia definované na podmnožine metrického priestoru je vždy možné interpretovať túto podmnožinu ako podpriestor pôvodne uvažovaného priestoru a aplikovať nasledujúcu vetu na tento podpriestor. Je však v takom prípade potrebné mať na pamäti, že systémy otvorených a uzavretých množín sa takýmto zúžením podpriestoru môžu podstatne zmeniť.

Veta 1.5.8. *Nech (X,d) a (X',d') sú metrické priestory a $f\colon X \to X'$ je zobrazenie. Potom sú nasledujúce tvrdenia ekvivalentné:*

(*i*) *Zobrazenie f je spojité.*

(*ii*) *Pre všetky otvorené množiny $T \subseteq X'$ v priestore X' je množina $f^{-1}(T)$ otvorená v X.*

(*iii*) *Pre všetky uzavreté množiny $T \subseteq X'$ v priestore X' je množina $f^{-1}(T)$ uzavretá v X.*

Dôkaz. Predpokladajme najprv, že je zobrazenie f spojité a uvažujme ľubovoľnú otvorenú množinu $T \subseteq X'$. Pre všetky $a \in f^{-1}(T)$ potom existuje $b \in T$ také, že $f(a) = b$. Keďže je množina T otvorená, musí existovať $\varepsilon > 0$ také, že $D(b,\varepsilon) \subseteq T$. Zo spojitosti zobrazenia f na druhej strane vyplýva existencia $\delta > 0$ takého, že pre všetky $x \in D(a,\delta)$ je $f(x) \in D(b,\varepsilon) \subseteq T$, a teda $D(a,\delta) \subseteq f^{-1}(T)$. Keďže je bod $a \in f^{-1}(T)$ ľubovoľný, je množina $f^{-1}(T)$ otvorená. Implikácia z (*i*) do (*ii*) je dokázaná.

Dokážeme teraz implikáciu z (*ii*) do (*iii*). Predpokladajme, že platí tvrdenie (*ii*) a uvažujme ľubovoľnú uzavretú množinu $T \subseteq X'$. Jej komplement $X' \setminus T$ je potom otvorená množina a podľa (*ii*) tak musí byť otvorená aj množina $f^{-1}(X' \setminus T)$. Množina $f^{-1}(T) = X \setminus f^{-1}(X' \setminus T)$ tak musí byť uzavretá.

Predpokladajme napokon, že platí tvrdenie (*iii*); množina $f^{-1}(T)$ je teda uzavretá v X pre všetky uzavreté $T \subseteq X'$. Zvoľme ľubovoľné $a \in X$ a $\varepsilon > 0$. Množina $X' \setminus D(f(a),\varepsilon)$ je potom uzavretá v X' a v X je tak uzavretá množina $f^{-1}(X' \setminus D(f(a),\varepsilon)) = X \setminus f^{-1}(D(f(a),\varepsilon))$. Množina $f^{-1}(D(f(a),\varepsilon))$ je preto otvorená, pričom evidentne musí byť $a \in f^{-1}(D(f(a),\varepsilon))$. Musí preto existovať $\delta > 0$ také, že $D(a,\delta) \subseteq f^{-1}(D(f(a),\varepsilon))$. To znamená: pre všetky $a \in X$ a všetky $\varepsilon > 0$ existuje $\delta > 0$ také, že pre všetky $x \in D(a,\delta)$ je $f(x) \in D(f(a),\varepsilon)$. Zobrazenie f je spojité. □

Príklad 1.5.9. Spojité zobrazenie $f\colon X \to X'$ medzi dvojicou metrických priestorov (X,d) a (X',d') *nemusí* zobrazovať otvorené množiny na otvorené množiny. Jednoduchým príkladom takéhoto zobrazenia môže byť napríklad ľubovoľná konštantná funkcia na $\mathbb{R}$. Zobrazenie f také, že $f(S)$ je otvorená množina pre všetky otvorené množiny S, sa nazýva *otvorené*. Spojité a súčasne otvorené bijekcie sú v literatúre známe ako *homeomorfizmy*.

V kontexte metrických priestorov teraz definujeme silnejší variant spojitosti – *rovnomernú spojitosť*. Definíciu (obyčajnej) spojitosti zobrazenia $f\colon X \to X'$ možno pre dvojicu metrických priestorov (X,d) a (X',d') sformulovať takto: pre všetky $a \in X$ a všetky $\varepsilon > 0$ existuje $\delta > 0$ také, že pre všetky $x \in D(a,\delta)$ je $f(x) \in D(f(a),\varepsilon)$. Pri rovnomernej spojitosti je kvantifikácia cez všetky $a \in X$ presunutá až za existenciu $\delta > 0$; požaduje sa teda, aby k danému $\varepsilon > 0$ bolo možné vybrať *spoločné* $\delta > 0$ *pre všetky* $a \in X$.

Definícia 1.5.10. Nech (X, d) a (X', d') sú metrické priestory a $f\colon X \to X'$ je zobrazenie. Hovoríme, že f je *rovnomerne spojité*, ak pre všetky $\varepsilon > 0$ existuje $\delta > 0$ také, že pre všetky $a \in X$ a všetky $x \in D(a, \delta)$ je $f(x) \in D(f(a), \varepsilon)$.

Príklad 1.5.11. Každá izometria je očividne rovnomerne spojitá.

Príklad 1.5.12. Funkcia $1/x$ je na intervale $(0, 1)$ spojitá, ale nie je rovnomerne spojitá.

1.6 Ekvivalencie metrík

V príklade 1.3.3 sme ukázali, že v $\mathbb{R}^n$ pre $n \in \mathbb{N} \setminus \{0\}$ dostaneme ten istý pojem limity bez ohľadu na to, či na tejto množine uvažujeme euklidovskú, manhattanskú, alebo Čebyševovu metriku; v skutočnosti by sme rovnako dobre mohli uvažovať aj ľubovoľnú Minkowského p-metriku. V tomto oddiele zavedieme dva pojmy ekvivalencie metrík, ktoré sú základom pre výsledky podobného typu. Najprv definujeme pojem *topologickej ekvivalencie*; limity pri topologicky ekvivalentných metrikách sú vždy rovnaké a nemení sa pri nich ani trieda spojitých funkcií. Následne definujeme o niečo silnejšiu *lipschitzovskú ekvivalenciu*, ktorá bude mať oproti topologickej ekvivalencii výhodu ľahšej overiteľnosti.

Definícia 1.6.1. Nech X je množina a $d_1, d_2\colon X^2 \to \mathbb{R}_{\geq 0}$ sú metriky na X. Metriky d_1 a d_2 sú *topologicky ekvivalentné*, ak pre všetky $S \subseteq X$ je množina S otvorená v (X, d_1) práve vtedy, keď je otvorená v (X, d_2).

Veta 1.6.2. *Nech X je množina a $d_1, d_2\colon X^2 \to \mathbb{R}_{\geq 0}$ sú topologicky ekvivalentné metriky na X. Nech $(x_n)_{n=0}^{\infty}$ je ľubovoľná postupnosť bodov množiny X a $x \in X$. Potom $x_n \to x$ pre $n \to \infty$ v metrickom priestore (X, d_1) práve vtedy, keď $x_n \to x$ pre $n \to \infty$ v metrickom priestore (X, d_2).*

Dôkaz. Pre všetky $a \in X$ a $r > 0$ označme ako $D_1(a, r)$ okolie bodu a o polomere r v priestore (X, d_1) a ako $D_2(a, r)$ označme také isté okolie v (X, d_2). Nech $x_n \to x$ pre $n \to \infty$ v (X, d_1). Nech $\varepsilon > 0$ je dané ľubovoľne. Vďaka topologickej ekvivalencii metrík d_1 a d_2 je množina $D_2(x, \varepsilon)$ otvorená aj v (X, d_1). Existuje preto $\delta > 0$ taká, že $D_1(x, \delta) \subseteq D_2(x, \varepsilon)$. Keďže postupnosť $(x_n)_{n=0}^{\infty}$ v (X, d_1) konverguje k x, musí pre dané δ existovať $n_0 \in \mathbb{N}$ také, že pre všetky prirodzené $n \geq n_0$ je $x_n \in D_1(x, \delta) \subseteq D_2(x, \varepsilon)$. Preto $x_n \to x$ pre $n \to \infty$ aj v priestore (X, d_2). Na dôkaz opačnej implikácie stačí vymeniť d_1 a d_2. □

Veta 1.6.3. *Nech X, X' sú množiny, $d_1, d_2\colon X^2 \to \mathbb{R}_{\geq 0}$ sú topologicky ekvivalentné metriky na X a $d_1', d_2'\colon (X')^2 \to \mathbb{R}_{\geq 0}$ sú topologicky ekvivalentné metriky na X'. Nech $f\colon X \to X'$ je zobrazenie. Potom je f spojité ako zobrazenie $f\colon (X, d_1) \to (X', d_1')$ práve vtedy, keď je spojité ako zobrazenie $f\colon (X, d_2) \to (X', d_2')$.*

Dôkaz. Ide o dôsledok viet 1.5.7 a 1.6.2. □

Definícia 1.6.4. Nech X je množina a $d_1, d_2\colon X^2 \to \mathbb{R}_{\geq 0}$ sú metriky na X. Metriky d_1 a d_2 sú *lipschitzovsky ekvivalentné*, ak existujú reálne čísla $s, t > 0$ také, že pre všetky $x, y \in X$ je

$$s d_2(x, y) \leq d_1(x, y) \leq t d_2(x, y).$$

Tvrdenie 1.6.5. *Nech X je množina a $d_1, d_2\colon X^2 \to \mathbb{R}_{\geq 0}$ sú metriky na X. Metriky d_1 a d_2 sú* lipschitzovsky ekvivalentné *práve vtedy, keď existujú reálne čísla $u, v > 0$ také, že pre všetky $x, y \in X$ je $d_1(x, y) \leq u d_2(x, y)$ a $d_2(x, y) \leq v d_1(x, y)$.*

Dôkaz. Ak sú metriky d_1 a d_2 lipschitzovsky ekvivalentné pre nejaké konštanty $s, t > 0$, stačí vziať $u = t$ a $v = 1/s$. Ak naopak existujú konštanty u, v zo znenia tvrdenia, stačí vziať $t = u$ a $s = 1/v$ a metriky sú lipschitzovsky ekvivalentné s konštantami s a t. □

Čitateľ ľahko dokáže, že lipschitzovská ekvivalencia je skutočne reláciou ekvivalencie na množine všetkých metrík na X.

Príklad 1.6.6. Všetky p-metriky pre $p \in [1, \infty) \cup \{\infty\}$ na $\mathbb{R}^n$ pre $n \in \mathbb{N} \setminus \{0\}$ sú vzájomne lipschitzovsky ekvivalentné, čo je napríklad dôsledkom nerovností (1.3) pozorovaných v dôkaze vety 1.4.7.

Príklad 1.6.7. Nech d je diskrétna metrika na množine X. Ľahko vidieť, že táto metrika je pre všetky $q > 0$ ekvivalentná metrike $d' \colon X^2 \to \mathbb{R}_{\geq 0}$ danej pre všetky $x, y \in X$ ako

$$d'(x, y) = \begin{cases} q & \text{ak } x \neq y, \\ 0 & \text{ak } x = y. \end{cases}$$

Z toho dôvodu sa aj takéto metriky d' obyčajne nazývajú diskrétnymi metrikami.

Veta 1.6.8. *Nech X je množina a $d_1, d_2 \colon X^2 \to \mathbb{R}_{\geq 0}$ sú lipschitzovsky ekvivalentné metriky na X. Potom sú metriky d_1 a d_2 topologicky ekvivalentné.*

Dôkaz. Pre všetky $a \in X$ a $r > 0$ označme ako $D_1(a, r)$ okolie bodu a o polomere r v priestore (X, d_1) a ako $D_2(a, r)$ označme také isté okolie v (X, d_2). Keďže sú metriky d_1 a d_2 lipschitzovsky ekvivalentné, existujú konštanty $s, t > 0$ také, že pre všetky $x, y \in X$ je

$$s d_2(x, y) \leq d_1(x, y) \leq t d_2(x, y).$$

Nech $S \subseteq X$ je otvorená množina v metrickom priestore (X, d_1). Pre všetky $a \in S$ potom existuje $\varepsilon > 0$ také, že $D_1(a, \varepsilon) \subseteq S$. Potom však aj $D_2(a, \varepsilon/t) \subseteq S$ a množina S je otvorená v metrickom priestore (X, d_2). Opačná implikácia sa dokáže symetricky. □

Príklad 1.6.9. Opačná implikácia k implikácii z predchádzajúcej vety nie je pravdivá. Uvažujme napríklad podpriestor $\mathbb{Z}$ metrického priestoru $\mathbb{R}$ s bežnou metrikou. Metrika d na $\mathbb{Z}$ je tu teda daná ako $d(p, q) = |p - q|$ pre všetky $p, q \in \mathbb{Z}$. Táto metrika je topologicky ekvivalentná diskrétnej metrike na $\mathbb{Z}$, keďže všetky podmnožiny $\mathbb{Z}$ sú v metrickom priestore $(\mathbb{Z}, d)$ zrejme otvorené. Metrika d však evidentne nie je lipschitzovsky ekvivalentná diskrétnej metrike na $\mathbb{Z}$.

1.7 Kompaktné metrické priestory

Podmnožiny $\mathbb{R}^n$ pre $n \in \mathbb{N} \setminus \{0\}$ alebo $\mathbb{C}$, ktoré sú uzavreté a súčasne ohraničené, sa nazývajú aj *kompaktnými*. Takéto množiny vykazujú množstvo dôležitých vlastností: z každej postupnosti prvkov kompaktnej podmnožiny $\mathbb{R}^n$ alebo $\mathbb{C}$ napríklad možno vybrať konvergentnú podpostupnosť; je tiež dobre známe, že funkcie spojité na kompakte sú v skutočnosti rovnomerne spojité.

V nasledujúcom budeme skúmať vhodné zovšeobecnenie tohto pojmu kompaktnosti v kontexte metrických priestorov. Kritériom vhodnosti takéhoto zovšeobecnenia pre nás pritom bude práve zachovanie uvedených vlastností kompaktných podmnožín $\mathbb{R}^n$ a $\mathbb{C}$.

Za našu definíciu kompaktného metrického priestoru zvolíme vlastnosť, ktorá je na prvý pohľad spomínaným vlastnostiam kompaktných podmnožín klasických analytických oborov trochu vzdialená. Pôjde ale o najobvyklejšiu definíciu v kontexte metrických priestorov, ktorá umožňuje priamočiare zovšeobecniť pojem kompaktnosti aj na priestory topologické. Následne si ukážeme niekoľko ekvivalentných charakterizácií kompaktných metrických priestorov, z ktorých každú by sme mohli zvoliť za definíciu kompaktnosti. Práve tieto charakterizácie nám pomôžu vidieť, že pojem kompaktných metrických priestorov je ozajstným zovšeobecnením kompaktnosti pod $\mathbb{R}^n$ a pod $\mathbb{C}$.

Definícia 1.7.1. Nech (X, d) je metrický priestor. *Otvoreným pokrytím* priestoru X nazveme ľubovoľný systém $(S_i \mid i \in I)$ otvorených podmnožín priestoru X taký, že

$$\bigcup_{i \in I} S_i = X.$$

Otvoreným podpokrytím pokrytia $(S_i \mid i \in I)$ nazveme ľubovoľné otvorené pokrytie $(S_i \mid i \in I')$ priestoru X také, že $I' \subseteq I$. Otvorené pokrytie $(S_i \mid i \in I)$ priestoru X nazveme *konečným*, ak je I konečná množina.

Definícia 1.7.2. Metrický priestor (X, d) je *kompaktný*, ak každé jeho otvorené pokrytie má aspoň jedno konečné podpokrytie.

Príklad 1.7.3. Každý konečný metrický priestor, čiže metrický priestor s konečnou nosnou množinou, je evidentne kompaktný.

Príklad 1.7.4. Ak X je množina a $d_1, d_2 \colon X^2 \to \mathbb{R}_{\geq 0}$ sú topologicky ekvivalentné metriky na X, je priestor (X, d_1) kompaktný práve vtedy, keď je kompaktný priestor (X, d_2).

Onedlho ukážeme, že sú kompaktnými aj všetky ohraničené a súčasne uzavreté podpriestory priestorov $\mathbb{R}^n$ pre $n \in \mathbb{N} \setminus \{0\}$ a $\mathbb{C}$ s bežnými metrikami. Najľahšie to ale vyplynie z ekvivalentných charakterizácií kompaktných metrických priestorov, ktoré dokážeme vo vete 1.7.11 nižšie. Najprv si ale dokážme dve o niečo jednoduchšie tvrdenia o kompaktných metrických priestoroch.

Tvrdenie 1.7.5. *Nech (X, d) je kompaktný metrický priestor a $Y \subseteq X$ je uzavretá množina v X. Potom je metrický priestor $(Y, d|_{Y\times Y})$ tiež kompaktný.*

Dôkaz. Nech $\mathscr{S} = (S_i \mid i \in I)$ je ľubovoľné otvorené pokrytie priestoru Y. To znamená, že pre všetky $i \in I$ je $S_i \subseteq Y$ množina otvorená v Y; ku každej takejto množine S_i evidentne existuje množina $T_i \subseteq X$ otvorená v X taká, že $T_i \cap Y = S_i$.[2] Tieto množiny T_i pre $i \in I$ tvoria spolu s množinou $X \setminus Y$ otvorené pokrytie priestoru X, z ktorého možno vybrať konečné otvorené podpokrytie $\mathscr{U} = (U_j \mid j \in J)$. Neprázdne spomedzi množín $U_j \cap Y$ pre $j \in J$ potom evidentne tvoria konečné podpokrytie pôvodného pokrytia $\mathscr{S}$ priestoru Y. □

Tvrdenie 1.7.6. *Nech (X_1, d_1) je kompaktný metrický priestor, (X_2, d_2) je ľubovoľný metrický priestor a $f \colon X_1 \to X_2$ je spojité zobrazenie. Potom je priestor $(f(X_1), d_2|_{f(X_1)\times f(X_1)})$ kompaktný.*

Dôkaz. Uvažujme ľubovoľné otvorené pokrytie $\mathscr{S} = (S_i \mid i \in I)$ priestoru $f(X_1)$. Rovnako ako v dôkaze predchádzajúceho tvrdenia musí pre každé $i \in I$ existovať množina $T_i \subseteq X_2$ otvorená v X_2 taká, že $T_i \cap f(X_1) = S_i$. Pre všetky $i \in I$ pritom $f^{-1}(T_i) = f^{-1}(S_i)$. Vďaka spojitosti zobrazenia f a vete 1.5.8 je teda $\mathscr{S}' = (f^{-1}(T_i) \mid i \in I) = (f^{-1}(S_i) \mid i \in I)$ otvoreným pokrytím priestoru X_1. Priestor X_1 je kompaktný, a teda musí existovať konečné podpokrytie $\mathscr{T}' = (f^{-1}(S_j) \mid j \in J)$ pokrytia $\mathscr{S}'$. Je potom zrejmé, že $\mathscr{T} = (S_j \mid j \in J)$ musí byť konečným podpokrytím pokrytia $\mathscr{S}$. □

Na sformulovanie ekvivalentných charakterizácií kompaktných metrických priestorov budeme potrebovať pojem *totálne ohraničeného metrického priestoru*.

Definícia 1.7.7. Nech (X, d) je metrický priestor a $S \subseteq X$. Množina S je:

a) *Ohraničená v X*, ak existuje reálne číslo $r \geq 0$ také, že pre všetky $x, y \in S$ je $d(x, y) \leq r$.

b) *Totálne ohraničená* v X, ak pre všetky $\varepsilon > 0$ existuje *konečná* podmnožina $S_\varepsilon \subseteq S$ taká, že

$$S \subseteq \bigcup_{a\in S_\varepsilon} D(a, \varepsilon).$$

Metrický priestor (X, d) je:

a) *Ohraničený*, ak je množina X ohraničená v X – čiže ak existuje reálne číslo $r \geq 0$ také, že pre všetky $x, y \in X$ je $d(x, y) \leq r$.

b) *Totálne ohraničený*, ak je množina X totálne ohraničená v X – čiže ak pre všetky $\varepsilon > 0$ existuje *konečná* podmnožina $X_\varepsilon \subseteq X$ taká, že

$$X = \bigcup_{a\in X_\varepsilon} D(a, \varepsilon).$$

[2] Pre všetky $x \in S_i$ môžeme napríklad vziať $\varepsilon_x > 0$ také, že pre okolie $D_Y(x, \varepsilon_x)$ bodu x o polomere ε_x v metrickom priestore Y je $D_Y(x, \varepsilon_x) \subseteq S_i$. Označme ako $D_X(x, \varepsilon_x)$ príslušné okolie v metrickom priestore X. Množinu T_i potom môžeme definovať ako $T_i = \bigcup_{x\in S_i} D_X(x, \varepsilon_x)$.

Tvrdenie 1.7.8. *Nech (X, d) je metrický priestor. Potom je každá jeho totálne ohraničená podmnožina $S \subseteq X$ ohraničená.*

Dôkaz. Nech $x, y \in S$. Z totálnej ohraničenosti množiny S potom napríklad vyplýva existencie konečnej podmnožiny $S_1 \subseteq S$ takej, že

$$S \subseteq \bigcup_{a \in S_1} D(a, 1).$$

Ľahko vidieť, že ak $|S_1| = n$, tak nutne $d(x, y) \leq 2n$. □

Príklad 1.7.9. Pojem totálne ohraničeného priestoru je silnejší, než pojem ohraničeného metrického priestoru: je napríklad zrejmé, že ľubovoľný diskrétny metrický priestor s nekonečnou nosnou množinou je ohraničený, avšak nemôže byť totálne ohraničený (pre $\varepsilon \leq 1$ môže každé z okolí obsahovať nanajvýš jeden bod).

Príklad 1.7.10. Podmnožina priestoru $\mathbb{R}^n$ pre $n \in \mathbb{N} \setminus \{0\}$ s euklidovskou metrikou, prípadne podmnožina priestoru $\mathbb{C}$ s bežnou metrikou, je totálne ohraničená práve vtedy keď je ohraničená. Dôkaz prenechávame čitateľovi ako jednoduché cvičenie.

Nasledujúca veta hovorí o troch ekvivalentných charakterizáciách kompaktnosti metrických priestorov. Z príkladu 1.7.10 a vety 1.4.4 vyplýva, že podpriestor priestoru $\mathbb{R}^n$ pre $n \in \mathbb{N}\setminus\{0\}$ s euklidovskou metrikou, prípadne priestoru $\mathbb{C}$ s bežnou metrikou, je totálne ohraničený a úplný práve vtedy, keď je nosná množina tohto podpriestoru ohraničená a uzavretá. Pre podpriestory $\mathbb{R}^n$ pre $n \in \mathbb{N} \setminus \{0\}$ a $\mathbb{C}$ teda možno ekvivalentnú podmienku (iv) nasledujúcej vety preformulovať ako ohraničenosť a uzavretosť nosnej množiny, čím sa dostávame k bežnej definícii kompaktných podmnožín $\mathbb{R}^n$ a $\mathbb{C}$. Implikáciu z (i) do (iii) navyše možno v nasledujúcej vete pre podpriestory týchto metrických priestorov interpretovať ako znenie Bolzanovej-Weierstrassovej vety.

Veta 1.7.11. *Nech (X, d) je metrický priestor. Potom sú nasledujúce tvrdenia ekvivalentné:*

(i) *Priestor X je kompaktný.*

(ii) *Každá nekonečná podmnožina X má hromadný bod v X.*

(iii) *Z každej postupnosti bodov X možno vybrať konvergentnú podpostupnosť.*[3]

(iv) *Priestor X je súčasne úplný a totálne ohraničený.*

Dôkaz. Dokážeme reťaz implikácií $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i)$.

Predpokladajme, že je priestor X kompaktný a uvažujme ľubovoľnú jeho nekonečnú podmnožinu $S \subseteq X$. Za účelom sporu predpokladajme, že S nemá hromadný bod v X. Potom je každý bod x množiny S izolovaný, a teda preň existuje $\varepsilon_x > 0$ také, že $D(x, \varepsilon_x) \cap S = \{x\}$. Pre každé $y \in X \setminus S$ tiež vieme zvoliť $\varepsilon_y > 0$ tak, aby $D(y, \varepsilon_y) \cap S = \emptyset$. Systém $\mathscr{S} = (D(x, \varepsilon_x) \mid x \in X)$ je potom evidentne otvoreným pokrytím množiny X – pre každé $x \in X$ totiž obsahuje kruhové okolie so stredom v x; nemožno však z neho vybrať konečné podpokrytie, pretože jedinou množinou pokrytia $\mathscr{S}$ obsahujúcou bod $x \in S$ je okolie $D(x, \varepsilon_x)$. To je spor s kompaktnosťou priestoru X. Implikácia z (i) do (ii) je dokázaná.

Na dôkaz implikácie z (ii) do (iii) predpokladajme, že má každá nekonečná podmnožina priestoru X aspoň jeden hromadný bod v X. Uvažujme ľubovoľnú postupnosť $(a_n)_{n=0}^{\infty}$ bodov priestoru X a položme $A := \{a_n \mid n \in \mathbb{N}\}$. Ak je množina A konečná, musí existovať $a \in X$ také, že pre nekonečne veľa rôznych $n \in \mathbb{N}$ je $a_n = a$. V takom prípade je teda $(a)_{n=0}^{\infty}$ konvergentnou podpostupnosťou postupnosti $(a_n)_{n=0}^{\infty}$. Ak je množina A nekonečná, musí mať podľa (ii) hromadný bod $a \in X$. Pre všetky prirodzené $k \geq 1$ potom môžeme zvoliť $n_k \in \mathbb{N}$ tak, aby $n_k > n_{k-1} > \ldots > n_1$ a súčasne $d(a_{n_k}, a) < 1/k$. Je potom zrejmé, že $a_{n_k} \to a$ pre $k \to \infty$ a postupnosť $(a_n)_{n=0}^{\infty}$ má konvergentnú podpostupnosť.

[3] Niekedy sa hovorí, že je priestor X *sekvenciálne kompaktný*; rozlišovanie medzi kompaktnosťou a sekvenciálnou kompaktnosťou má svoje korene v teórii topologických priestorov, kde tieto dva pojmy nie sú ekvivalentné.

Predpokladajme teraz platnosť tvrdenia (iii) a dokážme (iv). Aby sme dokázali, že priestor X musí byť úplný, uvažujme ľubovoľnú cauchyovskú postupnosť $(a_n)_{n=0}^{\infty}$ bodov priestoru X. Podľa (iii) z nej možno vybrať konvergentnú podpostupnosť konvergujúcu k nejakej limite a. Z toho vyplýva, že pre všetky $\varepsilon > 0$ existuje nekonečne veľa rôznych $n \in \mathbb{N}$ takých, že $d(a_n, a) < \varepsilon/2$. Súčasne však vďaka cauchyovskosti postupnosti $(a_n)_{n=0}^{\infty}$ pre to isté $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ také, že pre všetky $n, m \geq n_0$ je $d(a_n, a_m) < \varepsilon/2$. Z toho vyplýva, že pre všetky $n \geq n_0$ je $d(a_n, a) < \varepsilon$. Keďže je $\varepsilon > 0$ ľubovoľné, konverguje aj postupnosť $(a_n)_{n=0}^{\infty}$ k limite a. A keďže je ľubovoľná aj cauchyovská postupnosť $(a_n)_{n=0}^{\infty}$, je priestor X úplný.

Potrebujeme ešte dokázať, že v prípade platnosti (iii) musí byť priestor X totálne ohraničený. Predpokladajme, že to tak nie je. Nech $\varepsilon > 0$ je také, že X nemožno vyjadriť ako

$$X = \bigcup_{x \in X_\varepsilon} D(x, \varepsilon)$$

pre žiadnu konečnú množinu $X_\varepsilon \subseteq X$. Zvoľme bod $a_0 \in X$ ľubovoľne. Potom musí existovať bod $a_1 \in X$ taký, že $a_1 \notin D(a_0, \varepsilon)$, pretože inak by išlo o spor s voľbou $\varepsilon > 0$. Predpokladajme, že už máme dané body $a_0, \ldots, a_n \in X$ pre nejaké $n \in \mathbb{N}$. Potom môžeme vybrať $a_{n+1} \in X$ tak, aby

$$a_{n+1} \notin \bigcup_{k=0}^{n} D(a_k, \varepsilon),$$

pretože v opačnom prípade by opäť išlo o spor s voľbou $\varepsilon > 0$. Takto dostávame nekonečnú postupnosť $(a_n)_{n=0}^{\infty}$ bodov priestoru X takú, že pre všetky $n \in \mathbb{N}$ a všetky $m \in \{0, \ldots, n-1\}$ je $d(a_m, a_n) \geq \varepsilon$. Žiadna podpostupnosť postupnosti $(a_n)_{n=0}^{\infty}$ potom nemôže byť cauchyovská a podľa tvrdenia 1.3.6 teda ani konvergentná. To odporuje predpokladu platnosti tvrdenia (iii).

Zostáva dokázať implikáciu zo (iv) do (i). Predpokladajme, že je priestor X úplný a totálne ohraničený. Za účelom sporu predpokladajme, že priestor X nie je kompaktný – existuje teda jeho otvorené pokrytie $\mathscr{S} = (S_i \mid i \in I)$, z ktorého nemožno vybrať žiadne konečné otvorené podpokrytie. Z totálnej ohraničenosti priestoru X vyplýva existencia konečnej množiny $X_1 \subseteq X$ takej, že

$$X = \bigcup_{x \in X_1} D(x, 1).$$

Keby boli všetky z množín $D(x, 1)$ podmnožinou konečného zjednotenia množín S_i pre $i \in I' \subseteq I$, vedeli by sme takto skonštruovať konečné podpokrytie pokrytia $\mathscr{S}$. Existuje preto okolie $D_1 = D(x, 1)$ pre nejaké $x \in X_1$ také, že na jeho pokrytie je potrebných nekonečne veľa množín systému $\mathscr{S}$. Z totálnej ohraničenosti priestoru X potom opäť dostávame existenciu konečnej množiny $X_2 \subseteq X$ takej, že

$$X = \bigcup_{x \in X_2} D(x, 1/2),$$

z čoho

$$D_1 = \bigcup_{x \in X_2} (D(x, 1/2) \cap D_1).$$

Rovnaký argument ako vyššie ukazuje, že na pokrytie aspoň jednej z množín $D(x, 1/2) \cap D_1$ je potrebných nekonečne veľa množín systému $\mathscr{S}$. Pre príslušné x položme $D_2 = D(x, 1/2) \cap D_1$. Takto môžeme pokračovať a skonštruovať nekonečný reťazec neprázdnych množín $D_1 \supseteq D_2 \supseteq D_3 \supseteq \ldots$ taký, že pre všetky $n \in \mathbb{N} \setminus \{0\}$ je priemer množiny $\overline{D_n}$ najviac $2/n$ a súčasne je na pokrytie množiny D_n potrebných nekonečne veľa množín systému $\mathscr{S}$. Z úplnosti metrického priestoru X a vety 1.4.6 potom vyplýva existencia bodu

$$a \in \bigcap_{n=1}^{\infty} \overline{D_n}.$$

Bod a musí byť prvkom niektorej z množín S_i pre $i \in I$, keďže tie tvoria otvorené pokrytie priestoru X. Z otvorenosti množiny S_i potom vyplýva existencia $\varepsilon > 0$ takého, že $D(a, \varepsilon) \subseteq S_i$. Keďže sa však priemery množín D_n pre $n \to \infty$ limitne blížia k nule, musí existovať $n_0 \in \mathbb{N}$ také, že pre všetky $n \geq n_0$ je $D_n \subseteq D(a, \varepsilon) \subseteq S_i$. To je spor, pretože na pokrytie množiny D_n je potrebných nekonečne veľa množín systému $\mathscr{S}$. □

V nasledujúcom dokážeme ešte jednu dôležitú vlastnosť kompaktných metrických priestorov: každé spojité zobrazenie na kompaktnom metrickom priestore je rovnomerne spojité.

Veta 1.7.12. *Nech (X, d) je kompaktný metrický priestor, (X', d') je ľubovoľný metrický priestor a $f\colon X \to X'$ je spojité zobrazenie. Potom je zobrazenie f rovnomerne spojité.*

Dôkaz. Spojitosť zobrazenia $f\colon X \to X'$ znamená, že pre všetky $a \in X$ a všetky $\varepsilon > 0$ existuje $\delta_a > 0$ také, že pre všetky $x \in D(a, \delta_a)$ je $f(x) \in D(f(a), \varepsilon/2)$. Systém $(D(a, \delta_a/2) \mid a \in X)$ je teraz otvoreným pokrytím priestoru X a vďaka kompaktnosti tohto priestoru tak musí existovať jeho konečné otvorené podpokrytie $(D(a, \delta_a/2) \mid a \in X')$ pre nejakú konečnú množinu $X' \subseteq X$. Pre všetky $x \in X$ teda musí existovať $a \in X'$ také, že $x \in D(a, \delta_a/2)$. Ak položíme $\delta := \min\{\delta_a/2 \mid a \in X'\}$, tak pre všetky $y \in X$ také, že $d(x, y) < \delta$ navyše musí byť $y \in D(a, \delta_a)$. Pre všetky $x, y \in X$ s $d(x, y) < \delta$ teda existuje $a \in X'$ také, že $x, y \in D(a, \delta_a)$, a teda

$$d(f(x), f(y)) \leq d(f(x), f(a)) + d(f(a), f(y)) < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

Zobrazenie f je na X rovnomerne spojité. □

1.8 Banachova veta o pevnom bode

Dokážeme teraz jeden z kľúčových výsledkov teórie metrických priestorov – *Banachovu vetu o pevnom bode*, ktorá pre určité špeciálne spojité zobrazenia f na úplných metrických priestoroch garantuje existenciu *pevného bodu*, čiže bodu x takého, že $f(x) = x$.

Definícia 1.8.1. Nech (X, d) a (X', d') sú metrické priestory a $f\colon X \to X'$ je zobrazenie. Hovoríme, že zobrazenie f je:

a) *Lipschitzovsky spojité*, ak existuje reálna konštanta $L \geq 0$ taká, že pre všetky $x, y \in X$ je

$$d'(f(x), f(y)) \leq L d(x, y).$$

b) *Neexpanzívne*, ak je lipschitzovsky spojité pre $L = 1$, čiže ak pre všetky $x, y \in X$ je

$$d'(f(x), f(y)) \leq d(x, y).$$

V prípade $(X, d) = (X', d')$ navyše hovoríme, že zobrazenie $f\colon X \to X$ je:

c) *Kontraktívne* alebo *kontrakcia*, ak je lipschitzovsky spojité pre nejaké $0 \leq L < 1$, čiže ak existuje $L \in [0, 1)$ také, že pre všetky $x, y \in X$ je

$$d(f(x), f(y)) \leq L d(x, y).$$

Konštanta L z definície lipschitzovsky spojitých a kontraktívnych zobrazení sa nazýva aj *Lipschitzovou konštantou*.

Je zrejmé, že každá kontrakcia je neexpanzívna a každé neexpanzívne zobrazenie je lipschitzovsky spojité. Čitateľ naopak ľahko nájde príklad funkcie $f\colon \mathbb{R} \to \mathbb{R}$, ktorá je lipschitzovsky spojitá, ale nie je neexpanzívna, prípadne ktorá je neexpanzívna, ale nie je kontraktívna. Je tiež evidentné, že každá izometria na metrickom priestore obsahujúcom aspoň dva rôzne body je neexpanzívna, ale nie je kontraktívna.

V súvislosti s uvedenými definíciami si ešte potrebujeme ujasniť, prečo hovoríme o lipschitzovskej *spojitosti* – ako ukazuje nasledujúce tvrdenie, každé lipschitzovsky spojité zobrazenie je spojité.

Tvrdenie 1.8.2. *Nech (X, d) a (X', d') sú metrické priestory a $f\colon X \to X'$ je lipschitzovsky spojité zobrazenie. Potom je zobrazenie f spojité.*

Dôkaz. Nech $L \geq 0$ je Lipschitzova konštanta taká, že $d'(f(x), f(y)) \leq Ld(x, y)$ pre všetky $x, y \in X$. Nech $a \in X$ a $\varepsilon > 0$ sú ľubovoľné. Zvoľme $\delta := \varepsilon/L$. Pre všetky $x \in X$ také, že $d(a, x) < \delta$ je potom

$$d'(f(a), f(x)) \leq Ld(a, x) < L\delta = \varepsilon.$$

Zobrazenie f je teda spojité. □

Banachovu vetu o pevnom bode teraz sformulujeme ako tvrdenie hovoriace o špeciálnej vlastnosti *kontraktívnych* zobrazení na *úplných* metrických priestoroch.

Veta 1.8.3 (Banachova veta o pevnom bode)**.** *Nech (X, d) je úplný metrický priestor a $f\colon X \to X$ je kontrakcia. Potom existuje* práve jeden *pevný bod $x^* \in X$ zobrazenia f, čiže práve jeden bod $x^* \in X$ taký, že*

$$f(x^*) = x^*.$$

Ak navyše pre ľubovoľné $x_0 \in X$ definujeme postupnosť $(x_n)_{n=0}^{\infty}$ predpisom

$$x_{n+1} = f(x_n)$$

pre všetky $n \in \mathbb{N}$, je

$$\lim_{n\to\infty} x_n = x^*$$

a rýchlosť konvergencie možno odhadnúť pomocou nerovnosti

$$d(x_n, x^*) \leq \frac{L^n}{1 - L} d(x_0, x_1)$$

platnej pre všetky $n \in \mathbb{N}$, kde $L \in [0, 1)$ je Lipschitzova konštanta prislúchajúca ku kontrakcii f.

Dôkaz. Nech f je kontrakcia s Lipschitzovou konštantou L. Ukážeme najprv, že f nemôže mať dva rôzne pevné body. Sporom: nech $x_1^* \neq x_2^* \in X$ sú také, že $f(x_1^*) = x_1^*$ a $f(x_2^*) = x_2^*$. Potom

$$d(f(x_1^*), f(x_2^*)) = d(x_1^*, x_2^*) \not\leq Ld(x_1^*, x_2^*),$$

čo je spor s predpokladom, že f je kontrakcia s Lipschitzovou konštantou L.

Dokážme ďalej konvergenciu postupnosti $(x_n)_{n=0}^{\infty}$ pre ľubovoľne zvolené $x_0 \in X$. Keďže je metrický priestor X úplný, stačí ukázať, že je táto postupnosť cauchyovská. Pre všetky $n \in \mathbb{N}$ z kontraktívnosti zobrazenia f dostávame

$$d(x_{n+1}, x_{n+2}) = d(f(x_n), f(x_{n+1})) \leq Ld(x_n, x_{n+1}),$$

kde L je Lipschitzova konštanta prislúchajúca k zobrazeniu f. Indukciou teda ľahko dokážeme, že pre všetky $n \in \mathbb{N}$ je

$$d(x_n, x_{n+1}) \leq L^n d(x_0, x_1).$$

Pre všetky $n \leq m \in \mathbb{N}$ potom z trojuholníkovej nerovnosti dostávame

$$\begin{aligned} d(x_n, x_m) &\leq d(x_n, x_{n+1}) + d(x_{n+1}, x_{n+2}) + \ldots + d(x_{m-1}, x_m) \leq \\ &\leq L^n d(x_0, x_1) + L^{n+1} d(x_0, x_1) + \ldots + L^{m-1} d(x_0, x_1) = \\ &= L^n (1 + L + L^2 + \ldots + L^{m-n-1}) d(x_0, x_1) = \\ &= L^n \frac{1 - L^{m-n}}{1 - L} d(x_0, x_1) \leq \frac{L^n}{1 - L} d(x_0, x_1), \end{aligned} \tag{1.6}$$

pričom

$$\lim_{n \to \infty} \frac{L^n}{1 - L} d(x_0, x_1) = 0.$$

Pre všetky $\varepsilon > 0$, všetky dostatočne veľké n a všetky $m \geq n$ je teda $d(x_n, x_m) < \varepsilon$ a postupnosť je cauchyovská.

Vieme teda, že postupnosť $(x_n)_{n=0}^{\infty}$ konverguje k nejakému bodu $x^* \in X$. Aj bez toho, aby sme si boli istí, že je x^* pevným bodom zobrazenia f, môžeme odhadnúť rýchlosť konvergencie tejto postupnosti. Vďaka (1.6) totiž

$$d(x_n, x_m) \leq \frac{L^n}{1 - L} d(x_0, x_1)$$

pre všetky prirodzené $n \leq m$. Preto

$$d(x_n, x^*) = d\left(x_n, \lim_{m \to \infty} x_m\right) \leq \frac{L^n}{1 - L} d(x_0, x_1).$$

Na zavŕšenie dôkazu Banachovej vety už len teda stačí ukázať, že x^* musí byť pevným bodom zobrazenia f. Tu ale pre všetky $n \in \mathbb{N}$ s použitím trojuholníkovej nerovnosti dostávame

$$\begin{aligned} d(x^*, f(x^*)) &\leq d(x^*, x_{n+1}) + d(x_{n+1}, f(x^*)) \leq d(x^*, x_{n+1}) + d(f(x_n), f(x^*)) \leq \\ &\leq d(x^*, x_{n+1}) + L d(x_n, x^*) \to 0 \end{aligned}$$

pre $n \to \infty$. Preto $d(x^*, f(x^*)) = 0$ a v dôsledku toho $x^* = f(x^*)$: bod x^* je naozaj pevným bodom zobrazenia f. □

1.9 Vybrané aplikácie Banachovej vety

Banachova veta o pevnom bode má množstvo aplikácií v matematike aj mimo nej. K najznámejším patria jej aplikácie v samotnej matematickej analýze – vetu možno napríklad použiť na dôkaz *Picardovej vety* o existencii a jednoznačnosti riešení obyčajných diferenciálnych rovníc určitého typu a je základom aj pre súvisiacu *Picardovu metódu postupných aproximácií*. Dôležitou je tiež aplikácia Banachovej vety na dôkaz *vety o implicitnej funkcii*. My si teraz ukážeme niekoľko odlišných aplikácií Banachovej vety o pevnom bode. Začneme jednoduchou kuriozitou a postupne prejdeme k užitočnejším aplikáciám.

Príklad 1.9.1. Na stôl v Bratislave položíme mapu Bratislavy. Vďaka Banachovej vete o pevnom bode existuje práve jeden bod na tejto mape, ktorý zobrazuje miesto v rámci Bratislavy, na ktorom je reálne umiestnený. Mapu Bratislavy, pokiaľ sa nachádza vo vodorovnej polohe na území Bratislavy, totiž možno považovať za kontraktívne zobrazenie na metrickom priestore všetkých zemepisných súradníc v rámci Bratislavy (resp. v jej časti, ktorá je na mape zobrazená).

Príklad 1.9.2. Banachovu vetu o pevnom bode možno využiť na dôkaz konvergencie niektorých numerických metód riešenia rovníc. Uvažujme napríklad diferencovateľnú funkciu $f\colon [a, b] \to [a, b]$ na uzavretom intervale $[a, b]$ pre nejaké reálne čísla $a < b$. Predpokladajme navyše existenciu konštanty $L \in [0, 1)$ takej, že pre všetky $x \in [a, b]$ je $|f'(x)| \leq L$. Zobrazenie f je potom na $[a, b]$ určite

kontraktívne: pre všetky dvojice čísel $a' < b'$ z intervalu $[a, b]$ vyplýva z Lagrangeovej vety o strednej hodnote existencia $c \in (a', b')$ takého, že

$$f'(c) = \frac{f(b') - f(a')}{b' - a'},$$

z čoho pre všetky takéto $a' < b'$ pre nejaké $c \in (a', b')$ dostávame aj

$$|f(b') - f(a')| = |f'(c)||b' - a'| \leq L|b' - a'|;$$

podmienka $a' < b'$ je tu pritom evidentne nepodstatná.

Pre ľubovoľnú funkciu $f\colon [a, b] \to \mathbb{R}$ spĺňajúcu uvedené podmienky teda môžeme riešiť rovnicu

$$f(x) = x \tag{1.7}$$

tak, že zvolíme ľubovoľné $x_0 \in [a, b]$ a postupne iterujeme vzťah $x_{n+1} = f(x_n)$. Banachova veta o pevnom bode zaručuje, že hodnoty x_n budú pre $n \to \infty$ konvergovať k pevnému bodu funkcie f, čiže k jedinému riešeniu (1.7). Navyše nám aj poskytuje odhad rýchlosti tejto konvergencie, čo môže byť základom pre numerické riešenie uvedenej rovnice.

V praxi samozrejme častejšie nastáva potreba riešiť rovnice typu

$$f(x) = 0.$$

Aj takúto rovnicu ale často možno previesť na rovnicu typu (1.7), napríklad

$$f(x) + x = x.$$

Ak funkcia $f(x) + x$ spĺňa na nejakom intervale uvedenú podmienku na jej derivácie, možno na numerické riešenie tejto rovnice aplikovať postup opísaný vyššie.

V praxi sa obvykle používajú trochu rafinovanejšie iteratívne metódy numerického riešenia rovníc (najznámejšou a súčasne jednou z najjednoduchších je *Newtonova metóda*).

Príklad 1.9.3. Uvažujme pre $i = 1, \ldots, n$ bezkontextovú gramatiku $\mathcal{G}_i$ s množinou neterminálov $N = \{\alpha_1, \ldots, \alpha_n\}$, množinou terminálov T, počiatočným neterminálom α_i a prepisovacími pravidlami

$$\begin{aligned}
\alpha_1 &\to x_{1,1} \mid x_{1,2} \mid \ldots \mid x_{1,m_1} \\
\alpha_2 &\to x_{2,1} \mid x_{2,2} \mid \ldots \mid x_{2,m_2} \\
&\vdots \\
\alpha_n &\to x_{n,1} \mid x_{n,2} \mid \ldots \mid x_{n,m_n},
\end{aligned}$$

kde pre $i = 1, \ldots, n$ a $j = 1, \ldots, m_i$ je $x_{i,j} \in (N \cup T)^*$.

Ak teraz pre nejaké indexy i, j je $x_{i,j} = u_0\alpha_{k_1}u_1\alpha_{k_2}u_2 \ldots u_{s-1}\alpha_{k_s}u_s$ pre nejaké $u_0, \ldots, u_s \in T^*$ a $k_1, \ldots, k_s \in [n]$, položme

$$R_{i,j} := \{u_0\}Y_{k_1}\{u_1\}Y_{k_2}\{u_2\} \ldots \{u_{s-1}\}Y_{k_s}\{u_s\}.$$

Klasický výsledok teórie formálnych jazykov známy ako *Ginsburgova-Riceova veta* hovorí, že ak označíme pre $i = 1, \ldots, n$ ako $\|\mathcal{G}_i\|$ jazyk generovaný gramatikou $\mathcal{G}_i$, tak vektor

$$(\|\mathcal{G}_1\|, \ldots, \|\mathcal{G}_n\|)^T$$

je (vzhľadom na inklúziu) *najmenším* riešením systému rovníc

$$\begin{aligned}
Y_1 &= R_{1,1} \cup R_{1,2} \cup \ldots \cup R_{1,m_1} \\
Y_2 &= R_{2,1} \cup R_{2,2} \cup \ldots \cup R_{2,m_2} \\
&\vdots \\
Y_n &= R_{n,1} \cup R_{n,2} \cup \ldots \cup R_{n,m_n}
\end{aligned}$$

o neznámych $Y_1, \ldots, Y_n$ nad 2^{T^*}. Tento výsledok možno dokázať klasickými metódami teórie formálnych jazykov, prípadne s použitím viet o pevných bodoch v úplných čiastočne usporiadaných množinách (cpo). Keďže pre nás je Ginsburgova-Riceova veta dôležitá iba kvôli kontextu, obmedzíme sa iba na vysvetlenie toho, prečo je vektor $(\|\mathcal{G}_1\|, \ldots, \|\mathcal{G}_n\|)^T$ riešením uvedeného systému.

Jazyk $\|\mathcal{G}_i\|$ pre $i = 1, \ldots, n$ z definície pozostáva zo všetkých terminálnych slov odvoditeľných z neterminálu α_i. Ak teda dosadíme $\|\mathcal{G}_1\|, \ldots, \|\mathcal{G}_n\|$ za $Y_1, \ldots, Y_n$ do $R_{i,1} \cup \ldots \cup R_{i,m_i}$, dostaneme jazyk všetkých terminálnych slov odvoditeľných z niektorého zo slov $x_{i,1}, \ldots, x_{i,m_i}$. Ten je evidentne rovný jazyku všetkých terminálnych slov odvoditeľných z α_i, čiže $\|\mathcal{G}_i\|$. Z toho vyplýva, že vektor $(\|\mathcal{G}_1\|, \ldots, \|\mathcal{G}_n\|)^T$ je naozaj riešením.

Banachova veta o pevnom bode príde na rad pri dôkaze silnejšieho tvrdenia pre bezkontextové gramatiky *bez vymazávajúcich pravidiel* typu $\alpha_k \to \varepsilon$ a *bez reťazových pravidiel* typu $\alpha_k \to \alpha_\ell$ (evidentne ide o „skoro-normálny“ tvar bezkontextových gramatík). Tvrdíme, že pre bezkontextové gramatiky takéhoto typu je

$$(\|\mathcal{G}_1\|, \ldots, \|\mathcal{G}_n\|)^T$$

jediným „bezepsilonovým“ riešením príslušného systému rovníc, čiže jeho jediným riešením z $(2^{T^+})^n$. Na dôkaz využijeme metrický priestor na $(2^{T^*})^n$ z príkladu 1.1.17 (jazyky možno stotožniť s formálnymi mocninovými radmi nad $\mathbb{B}$). Čitateľovi prenechávame ako cvičenie dôkaz, že $(2^{T^+})^n$ tvorí úplný podpriestor priestoru $(2^{T^*})^n$.

Označme pre $i = 1, \ldots, n$ a $j = 1, \ldots, m_i$ ako $R_{i,j}(L_1, \ldots, L_n)$ jazyk, ktorý dostaneme dosadením jazykov $L_1, \ldots, L_n$ za premenné $Y_1, \ldots, Y_n$ do $R_{i,j}$. Zobrazenie $\varphi\colon (2^{T^+})^n \to (2^{T^+})^n$ dané ako

$$\begin{aligned}(L_1, \ldots, L_n)^T \mapsto (&R_{1,1}(L_1, \ldots, L_n) \cup \ldots \cup R_{1,m_1}(L_1, \ldots, L_n), \ldots, \\ &R_{n,1}(L_1, \ldots, L_n) \cup \ldots \cup R_{n,m_n}(L_1, \ldots, L_n))^T\end{aligned}$$

je potom kontraktívne. Ak sú totiž $(L_1, \ldots, L_n)^T$ a $(K_1, \ldots, K_n)^T$ dva vektory jazykov a najkratšie slovo, na ktorom sa „niektorý jazyk L_j líši od K_j“, má dĺžku $\ell \geq 1$, musí mať takéto najkratšie slovo pre dvojicu vektorov $\varphi((L_1, \ldots, L_n)^T)$ a $\varphi((K_1, \ldots, K_n)^T)$ dĺžku aspoň $\ell + 1$, práve kvôli neexistencii vymazávacích a reťazových pravidiel. To znamená, že vzdialenosť obrazov oboch vektorov pri zobrazení φ v uvažovanom metrickom priestore je nanajvýš polovičná oproti vzdialenosti pôvodných vektorov a zobrazenie φ je preto kontraktívne.

Vďaka Banachovej vete o pevnom bode potom existuje práve jedno riešenie uvažovaného systému rovníc, ktoré patrí do $(2^{T^+})^n$. Vzhľadom na to, že vektor $(\|\mathcal{G}_1\|, \ldots, \|\mathcal{G}_n\|)^T$ je vždy takýmto riešením, musí byť jediným „bezepsilonovým“ riešením daného systému práve tento vektor.

Príklad 1.9.4. Argumentáciu z predošlého príkladu možno rozšíriť aj na prípad bezkontextových gramatík s váhami, ktoré možno stotožniť so systémami rovníc nad $S\langle\!\langle \Sigma^* \rangle\!\rangle$ pre nejaký polokruh S a abecedu Σ. Rovnako ako v predchádzajúcom príklade zisťujeme, že pokiaľ daná gramatika neobsahuje vymazávajúce a reťazové pravidlá, musí mať príslušný systém práve jedno riešenie patriace do $(S\langle\!\langle \Sigma^+ \rangle\!\rangle)^n$, kde n je počet neterminálov gramatiky. Toto riešenie možno považovať za *definíciu* formálneho mocninového radu realizovaného danou bezkontextovou gramatikou s váhami. Keby sme naopak chceli uvažovať neobmedzené gramatiky s váhami, museli by sme podstatne obmedziť triedu uvažovaných polokruhov (napríklad na tzv. *spojité polokruhy*, ktoré súčasne tvoria cpo a dá sa v nich použiť argumentácia okolo Ginsburgovej-Riceovej vety, prípadne aspoň na *spočítateľne úplné polokruhy*).

Kapitola 2

Univerzálna algebra

Univerzálnu algebru možno definovať ako odvetvie abstraktnej algebry, ktoré sa namiesto vlastností algebier určitej triedy – napríklad grúp, pologrúp, okruhov, atď. – zaoberá spoločnými vlastnosťami rôznych tried algebier. Do popredia sa tak namiesto algebier samotných dostávajú ich triedy, predovšetkým tzv. *variety* algebier. Algebry sa tu pritom chápu v najvšeobecnejšom možnom slova zmysle – ako množiny vybavené nejakými systémami operácií na nich.

Z literatúry o univerzálnej algebre spomeňme predovšetkým učebnice [5, 9, 16, 2, 7] a skriptá [6]. Úvod do univerzálnej algebry prostredníctvom jazyka teórie kategórií možno nájsť v [3]. Základy univerzálnej algebry motivované použitím v teórii konečných pologrúp sú spracované aj v knihe [1].

2.1 Panoptikum algebraických štruktúr

Pripomeňme si niektoré už známe triedy algebier. Začnime algebrami, v ktorých je na nosnej množine daná jediná binárna operácia:

(*i*) *Grupoid*[1] (alebo *magma*) je množina X vybavená binárnou operáciou $\cdot\colon X^2 \to X$ – čiže usporiadaná dvojica $(X, \cdot)$.

(*ii*) *Pologrupa* je grupoid $(S, \cdot)$ taký, že binárna operácia $\cdot$ je asociatívna. Pre všetky $a, b, c \in S$ teda $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(*iii*) *Monoid* je pologrupa $(M, \cdot)$, v ktorej existuje neutrálny prvok 1_M vzhľadom na $\cdot$ – pre všetky $a \in M$ je teda $1_M \cdot a = a \cdot 1_M = a$.

(*iv*) *Grupa* je monoid $(G, \cdot)$, v ktorom pre každý prvok a existuje k nemu inverzný prvok a^{-1} taký, že $a^{-1} \cdot a = a \cdot a^{-1} = 1_G$

Z uvedených štyroch tried algebier možno pomerne rýchlo urobiť osem pridaním podmienky komutatívnosti binárnej operácie $\cdot$, t. j. vyžadovaním rovnosti $a \cdot b = b \cdot a$ pre všetky a, b z nosnej množiny.

K týmto pojmom ešte môžeme pridať pojem *polozväzu*. V reči teórie usporiadaní by sme mohli polozväz definovať ako čiastočne usporiadanú množinu $(S, \leq)$ takú, že pre ľubovoľnú dvojicu prvkov $a, b \in S$ existuje v $(S, \leq)$ ich *suprémum* $a \vee b$ – čiže najmenší prvok $s \in S$ taký, že súčasne $a \leq s$ aj $b \leq s$. Presnejšie v takom prípade ide o takzvaný *suprémový polozväz*; rovnako dobre by sme mohli uvažovať aj *infímový polozväz*, čo je čiastočne usporiadaná množina $(S, \leq)$ taká, že pre všetky $a, b \in S$ existuje ich *infímum* $a \wedge b$ – čiže najväčší prvok $i \in S$ taký, že súčasne $a \geq i$ a $b \geq i$. Nie je ťažké vidieť, že ak zabudneme na usporiadanie $\leq$ a sústredíme sa iba na operáciu $\vee$ resp. $\wedge$, dostaneme rovnakú triedu algebier; pre ľubovoľný suprémový polozväz $(S, \leq)$ je totiž $(S, \geq)$ infímový polozväz a naopak. Avšak hlavný dôvod, prečo pojem polozväzu na tomto mieste vôbec spomíname, je možnosť jeho alternatívnej algebraickej definície.

[1] Tento termín má ešte jeden nesúvisiaci a možno o trochu častejší význam v teórii kategórií.

(*v*) *Polozväz* je komutatívna a zároveň idempotentná pologrupa $(S, \cdot)$. Ide teda o grupoid $(S, \cdot)$ taký, že pre všetky $a, b, c \in S$ je $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $a \cdot b = b \cdot a$ a $a \cdot a = a$.

Čitateľ ľahko overí, že ak $(S, \leq)$ je suprémový polozväz, tak $(S, \vee)$ je polozväz a ak $(S, \leq)$ je infímový polozväz, tak $(S, \wedge)$ je polozväz. Ak je naopak $(S, \cdot)$ polozväz, môžeme skonštruovať suprémový polozväz $(S, \leq)$ taký, že pre všetky $a, b \in S$ je $a \vee b = a \cdot b$: pre všetky $a, b \in S$ stačí položiť $a \leq b$ práve vtedy, keď $a \cdot b = b$. Podobne môžeme ľubovoľný polozväz $(S, \cdot)$ chápať aj ako infímový polozväz $(S, \leq)$ taký, že pre všetky $a, b \in S$ je $a \wedge b = a \cdot b$: stačí položiť $a \leq b$ práve vtedy, keď $a \cdot b = a$.

V kontexte univerzálnej algebry je obvyklé považovať neutrálne prvky (a iné konštanty) za nulárne operácie a zobrazenie na inverzný prvok za unárnu operáciu. Monoid tak píšeme ako trojicu $(M, \cdot, 1)$ a grupu ako štvoricu $(G, \cdot, ^{-1}, 1)$. Zisťujeme potom, že všetky doposiaľ uvedené definície algebier možno vyjadriť *identitami*, ktoré musia platiť pre všetky k-tice prvkov nosnej množiny pre nejaké $k \in \mathbb{N}$ v prípade, že sú na ne aplikované niektoré z operácií. Takto chápané definície nami uvažovaných algebier sú zhrnuté v nasledujúcej tabuľke.

Grupoid	$(X, \cdot)$	$\cdot\colon X^2 \to X$	—
Pologrupa	$(S, \cdot)$	$\cdot\colon S^2 \to S$	$\forall a, b, c \in S : a \cdot (b \cdot c) = (a \cdot b) \cdot c$
Monoid	$(M, \cdot, 1)$	$\cdot\colon M^2 \to M$,	$\forall a, b, c \in M : a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
		$1\colon M^0 \to M$	$\forall a \in M : a \cdot 1 = a;\ 1 \cdot a = a$
Grupa	$(G, \cdot, ^{-1}, 1)$	$\cdot\colon G^2 \to G$,	$\forall a, b, c \in G : a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
		$^{-1}\colon G \to G$	$\forall a \in G : a \cdot 1 = a;\ 1 \cdot a = a$,
		$1\colon G^0 \to G$,	$\forall a \in G : a \cdot a^{-1} = 1;\ a^{-1} \cdot a = 1$
Polozväz	$(S, \cdot)$	$\cdot\colon S^2 \to S$	$\forall a, b, c \in S : a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
			$\forall a, b \in S : a \cdot b = b \cdot a$,
			$\forall a \in S : a \cdot a = a$

Tabuľka 2.1: Definície grupoidu, pologrupy, monoidu, grupy a polozväzu obvyklé v univerzálnej algebre.

V tomto duchu potom možno sformulovať aj definície niektorých tried algebier s viac než jednou binárnou operáciou:

(*vi*) *Polokruh* je pätica $(S, +, \cdot, 0, 1)$, kde S je množina a $+, \cdot\colon S^2 \to S$, $0, 1\colon S^0 \to S$ sú binárne resp. nulárne operácie na S také, že $(S, +, 0)$ je komutatívny monoid, $(S, \cdot, 1)$ je monoid a pre všetky $a, b, c \in S$ je $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$, $a \cdot 0 = 0$ a $0 \cdot a = 0$.

(*vii*) *Okruh* (s jednotkou) je šestica $(R, +, \cdot, -, 0, 1)$, kde R je množina a $+, \cdot\colon R^2 \to R$, $-\colon R \to R$, $0, 1\colon R^0 \to R$ sú binárne, unárne, resp. nulárne operácie na R také, že $(R, +, -, 0)$ je komutatívna grupa, $(R, \cdot, 1)$ je monoid a pre všetky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c$ a $(a + b) \cdot c = a \cdot c + b \cdot c$.

Hoci definícia poľa vyzerá na prvý pohľad podobne ako definícia okruhu, ukazuje sa, že čisto pomocou identít podobných ako vyššie ju sformulovať nemožno. Problémom je tu požiadavka, že multiplikatívna grupa má byť tvorená všetkými prvkami *rôznymi od nuly*. Momentálne nemáme ani len aparát na to, aby sme poriadne definovali, čo to identita vôbec je – a teda už tobôž nie na to, aby sme uvedené tvrdenie dokázali. Obidva tieto nedostatky ale napravíme v priebehu tejto kapitoly.

Ako posledný z príkladov algebier si tu ešte uveďme definíciu *zväzov*. Podobne ako pri polozväzoch ide o objekty opísateľné jazykom teórie usporiadaní: čiastočne usporiadaná množina $(L, \leq)$ je zväz, ak ide o suprémový a zároveň aj o infímový polozväz. Ukazuje sa, že táto požiadavka je – v rovnakom zmysle ako pri polozväzoch vyššie – ekvivalentná nasledujúcej algebraickej definícii.

(*viii*) *Zväz* je trojica $(L, \vee, \wedge)$ taká, že $(L, \vee)$ aj $(L, \wedge)$ sú komutatívne pologrupy a pre všetky $a, b \in L$ platia *absorpčné zákony* $a \vee (a \wedge b) = a$ a $a \wedge (a \vee b) = a$.

Skutočne: ľahko vidieť, že pre ľubovoľný zväz $(L, \leq)$ v zmysle definície prostredníctvom usporiadaní musí algebra $(L, \vee, \wedge)$ spĺňať uvedené podmienky. Ak je naopak $(L, \vee, \wedge)$ zväz v zmysle algebraickej definície, sú operácie $\vee$ a $\wedge$ nutne idempotentné – pre všetky $a \in L$ je $a \vee a = a \vee (a \wedge (a \vee a)) = a$, $a \wedge a = a \wedge (a \vee (a \wedge a)) = a$ – a algebry $(L, \vee)$, $(L, \wedge)$ sú teda polozväzy. Pre $a, b \in L$ je navyše $a \vee b = b$ práve vtedy, keď $a \wedge b = a$: z $a \vee b = b$ totiž dostávame $a \wedge b = a \wedge (a \vee b) = a$ a podobne pre obrátenú implikáciu. Usporiadaná množina $(L, \leq)$ taká, že pre všetky $a, b \in L$ je $a \leq b$ práve vtedy, keď $a \vee b = b$ resp. $a \wedge b = a$, je tak supremovým aj infímovým polozväzom, a teda aj zväzom.

2.2 Základné pojmy univerzálnej algebry

Budeme teraz študovať algebry v o niečo všeobecnejšom kontexte – iba ako nosné množiny spolu s nejakým systémom operácií na nej. *Typ algebry* pritom bude určený množinou symbolov pre uvažované operácie a aritou operácií, ktoré môžu tieto symboly realizovať.

Definícia 2.2.1. *Typ* – alebo *signatúra* – algebry je dvojica (τ, α), kde τ je množina *operačných symbolov* a $\alpha \colon \tau \to \mathbb{N}$ je zobrazenie priraďujúce každému operačnému symbolu $f \in \tau$ jeho *aritu* $\alpha(f)$. Ak $\alpha(f) = n$ pre nejaké $n \in \mathbb{N}$, hovoríme, že f je *n-árny operačný symbol* (prípadne nulárny[2], unárny, binárny, resp. ternárny pre $n = 0, 1, 2, 3$).

V prípade, že nebude hroziť nedorozumenie, budeme pre typ algebry namiesto (τ, α) písať iba τ. Aj v takom prípade budeme aritu jednotlivých operačných symbolov $f \in \tau$ označovať ako $\alpha(f)$. Zobrazenie α teda v takom prípade považujeme za dané. Je však podstatné mať aj pri tejto konvencii na pamäti, že to sú práve arity jednotlivých operácií, ktoré sú na určenie typu algebry podstatné.

Označenie 2.2.2. Systém prvkov $(a_i \mid i \in I)$ budeme v nasledujúcom zapisovať aj ako $(a_i)_{i \in I}$.

Definícia 2.2.3. *Algebrou* typu τ nazveme dvojicu $\mathscr{A} = (A, (f^{\mathscr{A}})_{f \in \tau})$, kde A je *nosná množina* (alebo *univerzum*) algebry $\mathscr{A}$ a pre všetky $f \in \tau$ je

$$f^{\mathscr{A}} \colon A^{\alpha(f)} \to A$$

$\alpha(f)$-árna operácia na nosnej množine A nazývaná *realizáciou* alebo *interpretáciou* operačného symbolu f v algebre $\mathscr{A}$.

Poznámka 2.2.4. Mnohí autori v definícii algebry predpokladajú neprázdnosť nosnej množiny. Upustenie od tejto požiadavky ale nevedie k žiadnym neprekonateľným problémom.

Občas budeme operačné symboly a ich realizácie v jednotlivých algebrách stotožňovať a namiesto $f^{\mathscr{A}}$ písať iba f. Často tiež budeme niektoré špeciálne operácie zapisovať v tvare, ktorý je pre ne obvyklejší, než $f(a_1, \ldots, a_n)$. Napríklad pre binárne operácie $\circ \colon A^2 \to A$ budeme väčšinou namiesto zápisu $\circ(a, b)$ používať infixový zápis $a \circ b$. Podobne napríklad pre unárnu operáciu $^{-1}$ v grupách budeme namiesto $^{-1}(a)$ písať a^{-1}, atď.

Hoci vo všeobecnosti pripúšťame aj algebry s nekonečne veľa operáciami, najdôležitejšie pre nás budú algebry, ktorých typom je konečná množina operačných symbolov. V takom prípade používame nasledujúcu, o čosi menej ťažkopádnu, notáciu.

Označenie 2.2.5. Nech τ je typ taký, že $\tau = \{f_1, \ldots, f_k\}$ pre nejaké $k \in \mathbb{N}$ a operačné symboly $f_1, \ldots, f_k$, pričom pre $i = 1, \ldots, k$ je $\alpha(f_i) = n_i$. Algebru $\mathscr{A}$ typu τ potom namiesto $\mathscr{A} = (A, (f)_{f \in \tau})$ zapisujeme ako $\mathscr{A} = (A, f_1, \ldots, f_k)$. Vzhľadom na to, že arita operácií je to jediné, čo z takéhoto zápisu algebry nemusí byť zrejmé, tiež v takom prípade hovoríme, že algebra $\mathscr{A}$ je typu $(n_1, \ldots, n_k)$.

[2] Niekedy tiež *konštantný*.

Príklad 2.2.6. Algebry prázdneho typu $\tau = \emptyset$ pozostávajú iba z nosnej množiny – ide teda o *množiny* samotné, ktoré budeme považovať za veľmi špeciálnu triedu algebier.

Príklad 2.2.7. *Grupoidy* sú práve algebry typu (2) – to jest typu $\tau = \{\cdot\}$, kde $\alpha(\cdot) = 2$. Ide totiž o práve všetky algebry $\mathscr{A} = (A, \cdot^{\mathscr{A}})$ také, že $\cdot^{\mathscr{A}} \colon A^2 \to A$ je binárna operácia na A.

Príklad 2.2.8. *Pologrupy* sú tiež algebrami typu (2), ale musia navyše spĺňať podmienku asociatívnosti príslušnej binárnej operácie. Takýmito triedami algebier, ktoré sú okrem typu dané aj nejakou množinou identít, sa budeme zaoberať neskôr.

Príklad 2.2.9. *Monoidy* tvoria podtriedu všetkých algebier typu $(2, 0)$, čiže typu $\tau = \{\cdot, 1\}$, kde $\alpha(\cdot) = 2$ a $\alpha(1) = 0$. Napríklad pre monoid $\mathscr{A} = (\mathbb{N}, +, 0)$ potom je $\cdot^{\mathscr{A}} = +$ a $1^{\mathscr{A}} = 0$.

Príklad 2.2.10. *Grupy* tvoria podtriedu algebier typu $(2, 1, 0)$, čiže typu $\tau = \{\cdot, {}^{-1}, 1\}$, kde $\alpha(\cdot) = 2$, $\alpha({}^{-1}) = 1$ a $\alpha(1) = 0$. Napríklad pre grupu $\mathscr{A} = (\mathbb{Z}, +, -, 0)$ potom je $\cdot^{\mathscr{A}} = +$, ${}^{-1^{\mathscr{A}}} = -$ a $1^{\mathscr{A}} = 0$.

Príklad 2.2.11. *Okruhy* (s jednotkou) tvoria podtriedu algebier typu $(2, 2, 1, 0, 0)$; to znamená typu $\tau = \{+, \cdot, -, 0, 1\}$, kde $\alpha(+) = \alpha(\cdot) = 2$, $\alpha(-) = 1$ a $\alpha(0) = \alpha(1) = 0$.

Príklad 2.2.12. *Vektorové priestory nad poľom* $\mathbb{F}$ možno považovať za algebry s nekonečným systémom operácií: ide o podtriedu algebier typu $\tau = \{+, \mathbf{0}, -\} \cup \{x\cdot \mid x \in \mathbb{F}\}$, kde $\alpha(+) = 2$, $\alpha(\mathbf{0}) = 0$, $\alpha(-) = 1$ a pre všetky $x \in \mathbb{F}$ je $\alpha(x\cdot) = 1$.

Pre každý typ τ existuje až na izomorfizmus[3] jediná jednoprvková algebra $\mathscr{A} = (\{\bullet\}, (f^{\mathscr{A}})_{f\in\tau})$, kde pre všetky $f \in \tau$ je $f^{\mathscr{A}}(\bullet, \dots, \bullet) = \bullet$. Takéto algebry nazývame *triviálnymi*. Algebru nazveme *prázdnou*, *konečnou*, resp. *nekonečnou* práve vtedy, keď má danú vlastnosť jej nosná množina.

Tvrdenie 2.2.13. *Nech τ je typ. Prázdna algebra typu τ potom existuje práve vtedy, keď τ neobsahuje nulárne operačné symboly.*

Dôkaz. Ak τ neobsahuje nulárne symboly, pre všetky $f \in \tau$ je $\emptyset^{\alpha(f)} = \emptyset$ a za $f^{\mathscr{A}} \colon \emptyset^{\alpha(f)} \to \emptyset$ môžeme vziať jediné zobrazenie z prázdnej množiny do prázdnej množiny. Dostávame tak dobre definovanú algebru $\mathscr{A} = (\emptyset, (f^{\mathscr{A}})_{f\in\tau})$. Ak naopak τ nulárne symboly obsahuje, pre každú algebru $\mathscr{A}$ s prázdnou nosnou množinou a pre každé nulárne $f \in \tau$ by muselo byť $f^{\mathscr{A}} \colon \emptyset^0 \to \emptyset$, pričom množina $\emptyset^0$ je jednoprvková; takéto zobrazenie teda neexistuje. □

Definícia 2.2.14. Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ je algebra typu τ. *Podalgebrou* algebry $\mathscr{A}$ nazveme algebru $\mathscr{B} = (B, (f^{\mathscr{B}})_{f\in\tau})$ typu τ, kde $B \subseteq A$ je množina taká, že pre všetky $f \in \tau$ a $a_1, \dots, a_{\alpha(f)} \in B$ je

$$f^{\mathscr{A}}(a_1, \dots, a_{\alpha(f)}) \in B$$

a pre všetky $f \in \tau$ je

$$f^{\mathscr{B}} = f^{\mathscr{A}}|_{B^{\alpha(f)}}.$$

Podalgebra algebry $\mathscr{A}$ je teda daná podmnožinou B jej nosnej množiny A uzavretou na všetky operácie, na ktorej sú uvažované zúženia všetkých pôvodných operácií. Uvedomme si tiež, že požiadavka uzavretosti B na nulárne operácie znamená príslušnosť týchto konštánt do B.

Príklad 2.2.15. Podalgebra typu $(2, 1, 0)$ grupy $\mathscr{G} = (G, \cdot, {}^{-1}, 1)$ je podľa uvedenej definície daná ako algebra $\mathscr{H} = (H, \cdot', {}^{-1'}, 1')$ typu $(2, 1, 0)$, kde $H \subseteq G$ je množina obsahujúca prvok 1 uzavretá na binárnu operáciu $\cdot$ a na unárnu operáciu ${}^{-1}$, kde $\cdot'$ je zúžením $\cdot$ na H^2, $h^{-1'} = h^{-1}$ pre všetky $h \in H$ a $1' = 1$. Je teda jasné, že musí ísť o podgrupu grupy $\mathscr{G}$.

[3] Presnú definíciu izomorfizmu ešte uvedieme nižšie. Čitateľ by ju ale s najväčšou pravdepodobnosťou uhádol aj sám; v prípade jednoprvkových algebier nepôjde o nič iné, než o premenovanie ich jediného prvku a operácií na ňom.

Príklad 2.2.16. Uvažujme monoid $\mathscr{M} = (M, \cdot, 1)$, ktorý je súčasne aj grupou. Podalgebra typu $(2,0)$ monoidu $\mathscr{M}$ je potom z podobných dôvodov ako vyššie podmonoidom monoidu $\mathscr{M}$. Nemusí ale ísť o grupu. Vezmime napríklad $\mathscr{M} = (\mathbb{Z}, +, 0)$. Potom $(\mathbb{N}, +, 0)$ je podalgebra typu $(2,0)$ a súčasne podmonoid monoidu $\mathscr{M}$, ktorý nie je grupou.

Definícia 2.2.17. Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ je algebra typu τ a $X \subseteq A$. *Podalgebrou algebry $\mathscr{A}$ generovanou množinou X* nazveme najmenšiu podalgebru $\langle X\rangle = (M, (f^{\langle X\rangle})_{f\in\tau})$ algebry $\mathscr{A}$ takú, že $X \subseteq M$.

Tvrdenie 2.2.18. *Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ je algebra typu τ a $X \subseteq A$. Podalgebra $\langle X\rangle$ algebry $\mathscr{A}$ generovaná množinou X vždy existuje a jej nosná množina je daná ako*

$$M = \bigcap_{\substack{(B,(f)_{f\in\tau}) \text{ je podalgebra } \mathscr{A} \\ X\subseteq B}} B.$$

Dôkaz. Množina M je uzavretá na všetky operácie $f^{\mathscr{A}}$ pre $f \in \tau$. Ak je totiž $f \in \tau$ nejaká n-árna operácia a $x_1, \ldots, x_n \in M$ sú ľubovoľné, nutne aj $x_1, \ldots, x_n \in B$ pre všetky $B \subseteq A$, ktoré obsahujú X a sú nosnou množinou nejakej podalgebry $\mathscr{A}$; preto aj $f^{\mathscr{A}}(x_1, \ldots, x_n) \in B$ pre všetky takéto množiny B. Keďže toto platí pre ľubovoľné B uvedeného typu, dostávame príslušnosť $f^{\mathscr{A}}(x_1, \ldots, x_n)$ do M. Na druhej strane je priamo z definície množiny M zrejmé, že pre ľubovoľnú podalgebru $(B, (f)_{f\in\tau})$ algebry $\mathscr{A}$ spĺňajúcu $X \subseteq B$ musí byť $M \subseteq B$. Preto M spolu s príslušnými zúženiami operácií $f^{\mathscr{A}}$ pre $f \in \tau$ naozaj tvorí najmenšiu podalgebru $\mathscr{A}$ obsahujúcu X, čiže algebru $\langle X\rangle$. □

Definícia 2.2.19. Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ a $\mathscr{B} = (B, (f^{\mathscr{B}})_{f\in\tau})$ sú nejaké dve algebry spoločného typu τ. Zobrazenie $\varphi\colon A \to B$ sa nazýva *homomorfizmom* algebry $\mathscr{A}$ do algebry $\mathscr{B}$, ak pre všetky $f \in \tau$ a všetky $a_1, \ldots, a_{\alpha(f)} \in A$ je

$$\varphi\left(f^{\mathscr{A}}\left(a_1, \ldots, a_{\alpha(f)}\right)\right) = f^{\mathscr{B}}\left(\varphi\left(a_1\right), \ldots, \varphi\left(a_{\alpha(f)}\right)\right).$$

V takom prípade tiež píšeme $\varphi\colon \mathscr{A} \to \mathscr{B}$.

Čitateľ isto ľahko samostatne overí, že pre ľubovoľnú dvojicu homomorfizmov algebier $\varphi\colon \mathscr{A} \to \mathscr{B}$ a $\psi\colon \mathscr{B} \to \mathscr{C}$ je ich zloženie $\psi \circ \varphi\colon \mathscr{A} \to \mathscr{C}$ opäť homomorfizmus.

Príklad 2.2.20. Pre algebry $\mathscr{A} = (A, \cdot, {}^{-1_A}, 1_A)$ a $\mathscr{B} = (B, \circ, {}^{-1_B}, 1_B)$ typu $(2,1,0)$ musí homomorfizmus $\varphi\colon \mathscr{A} \to \mathscr{B}$ pre všetky $a, b \in A$ spĺňať $\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$, $\varphi(a^{-1_A}) = \varphi(a)^{-1_B}$ a $\varphi(1_A) = 1_B$. Ak sú teda $\mathscr{A}$ a $\mathscr{B}$ grupy, ide vždy o homomorfizmus grúp. Je navyše známe, že hoci v definícii homomorfizmu grúp stačí podmienka $\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$, sú v takom prípade zvyšné dve podmienky $\varphi(a^{-1_A}) = \varphi(a)^{-1_B}$ a $\varphi(1_A) = 1_B$ automaticky splnené. Homomorfizmy algebier typu $(2,1,0)$ z grupy do grupy sú teda práve všetky grupové homomorfizmy medzi týmito dvoma grupami.

Príklad 2.2.21. Uvažujme dvojicu vektorových priestorov $\mathscr{U}$, $\mathscr{V}$ nad poľom $\mathbb{F}$ chápaných ako algebry $\mathscr{U} = (U, (f^{\mathscr{U}})_{f\in\tau})$ a $\mathscr{V} = (V, (f^{\mathscr{V}})_{f\in\tau})$ typu $\tau = \{+, \mathbf{0}, -\} \cup \{x\cdot \mid x \in \mathbb{F}\}$. Homomorfizmus $\varphi\colon \mathscr{U} \to \mathscr{V}$ algebier typu τ potom musí pre všetky $\mathbf{u}, \mathbf{v} \in U$ spĺňať $\varphi(\mathbf{u} +^{\mathscr{U}} \mathbf{v}) = \varphi(\mathbf{u}) +^{\mathscr{V}} \varphi(\mathbf{v})$, $\varphi(\mathbf{0}^{\mathscr{U}}) = \mathbf{0}^{\mathscr{V}}$, $\varphi(-^{\mathscr{U}}\mathbf{u}) = -^{\mathscr{V}}\varphi(\mathbf{u})$ a $\varphi(x \cdot^{\mathscr{U}} \mathbf{u}) = x \cdot^{\mathscr{V}} \varphi(\mathbf{u})$ pre všetky $x \in \mathbb{F}$. Je teda zrejmé, že homomorfizmami algebier typu τ z vektorového priestoru do vektorového priestoru sú práve všetky lineárne zobrazenia medzi nimi.

Príklad 2.2.22. Uvažujme ľubovoľnú algebru $\mathscr{A} = (A, (f)_{f\in\tau})$ ľubovoľného typu τ. Potom je identické zobrazenie $\mathrm{id}_A\colon A \to A$ homomorfizmom z algebry $\mathscr{A}$ do samej seba (ide teda o *endomorfizmus*). Skutočne: pre všetky $f \in \tau$ a všetky $a_1, \ldots, a_{\alpha(f)} \in A$ je

$$\mathrm{id}_A(f(a_1, \ldots, a_{\alpha(f)})) = f(a_1, \ldots, a_{\alpha(f)}) = f(\mathrm{id}_A(a_1), \ldots, \mathrm{id}_A(a_{\alpha(f)})).$$

Definícia 2.2.23. Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ a $\mathscr{B} = (B, (f^{\mathscr{B}})_{f\in\tau})$ sú nejaké dve algebry spoločného typu τ. Homomorfizmus $\varphi\colon \mathscr{A} \to \mathscr{B}$ nazveme *izomorfizmom*, ak je bijektívny. Algebry $\mathscr{A}, \mathscr{B}$ nazveme *izomorfnými*, ak existuje izomorfizmus $\varphi\colon \mathscr{A} \to \mathscr{B}$. V takom prípade píšeme $\mathscr{A} \cong \mathscr{B}$.

Je jednoduchým, ale vcelku užitočným cvičením dokázať, že zloženie izomorfizmov je izomorfizmus, že inverzné zobrazenie k izomorfizmu je takisto izomorfizmus a že $\cong$ je v dôsledku týchto vlastností reláciou ekvivalencie na triede všetkých algebier typu τ.

Príklad 2.2.24. Identické zobrazenie z príkladu 2.2.22 je evidentne bijektívne. Ide teda o izomorfizmus z $\mathscr{A}$ do $\mathscr{A}$ (to jest o *automorfizmus*).

Definícia 2.2.25. Nech $(\mathscr{A}_i)_{i\in I}$ je ľubovoľný systém algebier spoločného typu τ, kde pre všetky $i \in I$ je $\mathscr{A}_i = (A_i, (f^{\mathscr{A}_i})_{f\in\tau})$. *Priamym súčinom* systému $(\mathscr{A}_i)_{i\in I}$ nazveme algebru

$$\prod_{i\in I} \mathscr{A}_i = \left(\prod_{i\in I} A_i, \left(f^{\prod_{i\in I}\mathscr{A}_i} \right)_{f\in\tau} \right),$$

kde pre všetky $f \in \tau$ a všetky $a_{i,k} \in A_i$ pre $i \in I$ a $k = 1, \ldots, \alpha(f)$ je

$$f^{\prod_{i\in I}\mathscr{A}_i}\left((a_{i,1})_{i\in I}, \ldots, (a_{i,\alpha(f)})_{i\in I}\right) = \left(f^{\mathscr{A}_i}(a_{i,1}, \ldots, a_{i,\alpha(f)})\right)_{i\in I}.$$

Priamy súčin algebier teda pozostáva z karteziánskeho súčinu ich nosných množín spolu s operáciami po zložkách. Pokiaľ budeme hovoriť iba o *súčine*, budeme mať vždy na mysli priamy súčin. Existujú však aj iné typy súčinov. Priamy súčin nazveme *konečným* resp. *nekonečným*, ak má príslušnú vlastnosť indexová množina I. Prázdnym súčinom algebier ľubovoľného typu τ je vždy nejaká bližšie neurčená – avšak *pevne daná* – triviálna algebra typu τ; až na izomorfizmus je táto algebra určená jednoznačne.

Definícia 2.2.26. Nech $(\mathscr{A}_i)_{i\in I}$ je systém algebier spoločného typu τ, kde pre všetky $i \in I$ je $\mathscr{A}_i = (A_i, (f^{\mathscr{A}_i})_{f\in\tau})$; nech $j \in I$. Pod *j-tou projekciou* na $\prod_{i\in I}\mathscr{A}_i$ rozumieme zobrazenie

$$\pi_j\colon \prod_{i\in I} A_i \to A_j$$

dané pre všetky systémy prvkov $a_i \in A_i$ pre $i \in I$ ako

$$\pi_j\left((a_i)_{i\in I}\right) = a_j.$$

Tvrdenie 2.2.27. *Nech $(\mathscr{A}_i)_{i\in I}$ je systém algebier spoločného typu τ taký, že pre všetky $i \in I$ je $\mathscr{A}_i = (A_i, (f^{\mathscr{A}_i})_{f\in\tau})$; nech $j \in I$. Zobrazenie j-tej projekcie π_j na $\prod_{i\in I}\mathscr{A}_i$ je potom homomorfizmom*

$$\pi_j\colon \prod_{i\in I} \mathscr{A}_i \to \mathscr{A}_j$$

algebry $\prod_{i\in I}\mathscr{A}_i$ do $\mathscr{A}_j$. Ak navyše $A_i \neq \emptyset$ pre všetky $i \in I \setminus \{j\}$, je homomorfizmus π_j surjektívny.

Dôkaz. Uvažujme ľubovoľný operačný symbol $f \in \tau$ a ľubovoľný systém prvkov $a_{i,k} \in A_i$ pre $i \in I$ a $k = 1, \ldots, \alpha(f)$. Potom

$$\begin{aligned}\pi_j\left(f^{\prod_{i\in I}\mathscr{A}_i}\left((a_{i,1})_{i\in I}, \ldots, (a_{i,\alpha(f)})_{i\in I}\right)\right) &= \pi_j\left(\left(f^{\mathscr{A}_i}(a_{i,1}, \ldots, a_{i,\alpha(f)})\right)_{i\in I}\right) = \\ &= f^{\mathscr{A}_j}(a_{j,1}, \ldots, a_{j,\alpha(f)}) \\ &= f^{\mathscr{A}_j}\left(\pi_j\left((a_{i,1})_{i\in I}\right), \ldots, \pi_j\left((a_{i,\alpha(f)})_{i\in I}\right)\right),\end{aligned}$$

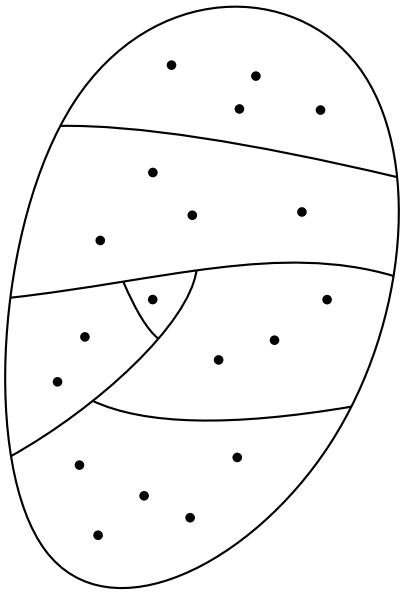
čo dokazuje, že π_j je skutočne homomorfizmus. Ak navyše $A_i \neq \emptyset$ pre všetky $i \in I \setminus \{j\}$, zvoľme pre všetky $i \in I \setminus \{j\}$ nejaký pevne daný prvok $a_i \in A_i$. Pre všetky $a_j \in A_j$ je potom

$$a_j = \pi_j\left((a_i)_{i\in I}\right),$$

čo dokazuje surjektívnosť homomorfizmu $\pi_j\colon \prod_{i\in I}\mathscr{A}_i \to \mathscr{A}_j$. □

2.3 Kongruencie, faktorové algebry a prvá veta o izomorfizme

Chceli by sme teraz definovať faktorové algebry podobným spôsobom ako boli definované faktorové grupy alebo faktorové okruhy. Klasické definície faktorovej grupy podľa normálnej podgrupy alebo faktorového okruhu podľa ideálu by však boli do kontextu univerzálnej algebry zovšeobecniteľné iba ťažko. Namiesto toho sa pozrime od základu na to, čo je samotnou ideou faktorizácie algebier: ide o *zovšeobecnenie rozkladu množiny na triedy ekvivalencie*. Množiny sú algebrami typu $\tau = \emptyset$, pričom za faktorovú množinu množiny S by sme chceli považovať ľubovoľný rozklad $S/\equiv$ množiny S na triedy ľubovoľnej relácie ekvivalencie $\equiv$ – napríklad taký, ako je znázornený na obrázku 2.1.



Obr. 2.1: Rozklad množiny S na triedy ekvivalencie $\equiv$. Prvky množiny S sú tu znázornené „kolečkami“, pričom $x \equiv y$ práve vtedy, keď sú tieto dva prvky súčasťou rovnakej „bunky“, t. j. triedy rozkladu S podľa $\equiv$. Faktorová množina $S/\equiv$ množiny S je množinou práve všetkých takýchto „buniek“.

Trieda ekvivalencie $\equiv$ obsahujúca prvok $a \in S$ je daná ako množina $[a]_\equiv = \{x \in S \mid x \equiv a\}$ a faktorová množina $S/\equiv$ je potom daná ako

$$S/\equiv = \{\, [a]_\equiv \mid a \in S\}.$$

Množina $S/\equiv$ je teda akýmsi „oddialeným pohľadom“ na množinu S, pri ktorom už nerozlišujeme medzi prvkami z rovnakej triedy ekvivalencie, ale stále rozlišujeme medzi prvkami z rôznych tried ekvivalencie.

Ak namiesto množiny S vezmeme algebru $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ – možno si tu predstaviť napríklad grupu alebo okruh – chceli by sme jej faktorové algebry definovať tak, aby predstavovali rovnaký „oddialený pohľad“ na algebru $\mathscr{A}$. Avšak pri jednej základnej podmienke: *výsledkom faktorizácie by opäť mala byť algebra rovnakého typu*. To znamená, že algebry už nebudeme môcť faktorizovať podľa ľubovoľnej relácie ekvivalencie $\equiv$, ale iba podľa takých relácií ekvivalencie, pri ktorých budeme vedieť s výslednými triedami $[a]_\equiv$ pre $a \in A$ počítať ako v algebre typu τ. Napríklad z grúp by sme faktorizáciou mali dostať opäť grupu – alebo aspoň algebru typu $(2, 0, 1)$.[4]

Výsledná algebra na množine tried by nemala byť úplne hocijaká, ale mala by rešpektovať ideu faktorovej algebry ako reprezentácie „oddialeného pohľadu“ na pôvodnú algebru. To znamená, že ak z niektorej triedy ekvivalencie „vidíme“ jeden prvok – nejakého *reprezentanta* a tejto triedy – a z inej triedy „vidíme“ iný prvok b, mali by sme aplikovaním binárnej operácie $\circ$ na dané dve triedy dostať triedu obsahujúcu $a \circ b$. Podobná vlastnosť by mala platiť aj pre operácie ľubovoľnej inej arity.

[4] Tieto podmienky sú v skutočnosti ekvivalentné, vyplynie to ale až z našich neskorších úvah.

Túto vlastnosť možno vyjadriť ako nezávislosť operácií $f^{\mathscr{A}}$ pre $f \in \tau$ od výberu reprezentantov tried ekvivalencie relácie $\equiv$: pre všetky $a_1, \ldots, a_{\alpha(f)}, b_1, \ldots, b_{\alpha(f)} \in A$ spĺňajúce $a_k \equiv b_k$ pre $k = 1, \ldots, \alpha(f)$ musí byť

$$f^{\mathscr{A}}(a_1, \ldots, a_{\alpha(f)}) \equiv f^{\mathscr{A}}(b_1, \ldots, b_{\alpha(f)}). \tag{2.1}$$

Potom totiž môžeme korektne – to jest nezávisle od výberu reprezentantov – definovať

$$f^{\mathscr{A}/\equiv}([a_1]_\equiv, \ldots, [a_{\alpha(f)}]_\equiv) = \left[f^{\mathscr{A}}(a_1, \ldots, a_{\alpha(f)})\right]_\equiv$$

Týmto sa dostávame k dôležitému pojmu *kongruencií* na algebre, čo budú práve relácie ekvivalencie na jej nosnej množine spĺňajúce pre všetky $f \in \tau$ vlastnosť (2.1).

Definícia 2.3.1. Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ je algebra typu τ. *Kongruenciou* na $\mathscr{A}$ nazveme reláciu ekvivalencie $\equiv$ na množine A takú, že pre všetky $f \in \tau$ a všetky $a_1, \ldots, a_{\alpha(f)}, b_1, \ldots, b_{\alpha(f)} \in A$ spĺňajúce $a_k \equiv b_k$ pre $k = 1, \ldots, \alpha(f)$ je $f^{\mathscr{A}}(a_1, \ldots, a_{\alpha(f)}) \equiv f^{\mathscr{A}}(b_1, \ldots, b_{\alpha(f)})$.

Kongruencie na algebre teda tvoria podtriedu relácií ekvivalencie na jej nosnej množine tvorenú tými reláciami, podľa ktorých bude možné danú algebru korektne faktorizovať. Než sa ale dostaneme k zavedeniu samotného pojmu faktorovej algebry, preskúmajme kongruencie o čosi detailnejšie. Začnime jednoduchou alternatívnou charakterizáciou kongruencií a niekoľkými príkladmi.

Tvrdenie 2.3.2. *Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ je algebra typu τ. Relácia ekvivalencie $\equiv$ na A je kongruencia práve vtedy, keď pre všetky $f \in \tau$, $k = 1, \ldots, \alpha(f)$, všetky $x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_{\alpha(f)} \in A$ a $a_k, b_k \in A$ spĺňajúce $a_k \equiv b_k$ je $f^{\mathscr{A}}(x_1, \ldots, x_{k-1}, a_k, x_{k+1}, \ldots, x_{\alpha(f)}) \equiv f^{\mathscr{A}}(x_1, \ldots, x_{k-1}, b_k, x_{k+1}, \ldots, x_{\alpha(f)})$.*

Dôkaz. Ak je $\equiv$ kongruencia, evidentne spĺňa aj podmienku zo znenia tohto tvrdenia. Zostáva dokázať opačnú implikáciu. Ak ale $\equiv$ spĺňa podmienku zo znenia tohto tvrdenia, tak pre všetky $f \in \tau$ a všetky $a_1, \ldots, a_{\alpha(f)}, b_1, \ldots, b_{\alpha(f)} \in A$ také, že pre $i = 1, \ldots, \alpha(f)$ je $a_i \equiv b_i$, dostávame

$$\begin{aligned} f^{\mathscr{A}}(a_1, a_2, a_3, \ldots, a_{\alpha(f)}) &\equiv f^{\mathscr{A}}(b_1, a_2, a_3, \ldots, a_{\alpha(f)}) \equiv \\ &\equiv f^{\mathscr{A}}(b_1, b_2, a_3, \ldots, a_{\alpha(f)}) \equiv \\ &\vdots \\ &\equiv f^{\mathscr{A}}(b_1, b_2, b_3, \ldots, b_{\alpha(f)}). \end{aligned}$$

Relácia $\equiv$ je teda kongruencia. □

Príklad 2.3.3. Kongruencia na *pologrupe* $(S, \cdot)$ je podľa definície 2.3.1 relácia ekvivalencie $\equiv$ na S taká, že pre všetky $a, b, a', b' \in S$ spĺňajúce $a \equiv a'$ a $b \equiv b'$ je aj $a \cdot b \equiv a' \cdot b'$. Podľa charakterizácie z tvrdenia 2.3.2 ide o práve všetky relácie ekvivalencie $\equiv$ na S také, že sú súčasne splnené nasledujúce dve podmienky:

(*i*) Pre všetky $a, a' \in S$ spĺňajúce $a \equiv a'$ a všetky $b \in S$ je $a \cdot b \equiv a' \cdot b$.

(*ii*) Pre všetky $b, b' \in S$ spĺňajúce $b \equiv b'$ a všetky $a \in S$ je $a \cdot b \equiv a \cdot b'$.

V kontexte pologrúp sa relácia ekvivalencie spĺňajúca prvú z týchto podmienok nazýva *pravou kongruenciou* a relácia ekvivalencie spĺňajúcu druhú z podmienok *ľavou kongruenciou*. Tvrdenie 2.3.2 teda hovorí, že relácia ekvivalencie na pologrupe je kongruencia práve vtedy, keď je to ľavá a súčasne pravá kongruencia.

Príklad 2.3.4. Na pologrupe $(\mathbb{N}, +)$ sú kongruenciami napríklad nasledujúce relácie ekvivalencie:

(*i*) Relácia $\equiv_1$ taká, že $a \equiv_1 b$ práve vtedy, keď $a = 0 = b$ alebo $a \neq 0 \neq b$.

(*ii*) Relácia $\equiv_2$ taká, že $a \equiv_2 b$ práve vtedy keď $a \equiv b \pmod 2$.

(*iii*) Relácia $\mathbb{N} \times \mathbb{N}$ ako najhrubšia – t. j. najväčšia – kongruencia na pologrupe $(\mathbb{N}, +)$.

(*iv*) Relácia rovnosti ako najjemnejšia – t. j. najmenšia – kongruencia na pologrupe $(\mathbb{N}, +)$.

Príklady (*iii*) a (*iv*) sú v podstate univerzálne a podobne definované relácie sú najhrubšou resp. najjemnejšou kongruenciou na ľubovoľnej algebre.

Príklad 2.3.5. Kongruencia na *monoide* $(M, \cdot, 1)$ je podľa definície 2.3.1 relácia ekvivalencie $\equiv$ na M taká, že $a \cdot b \equiv a' \cdot b'$ kedykoľvek $a \equiv a'$ a súčasne $b \equiv b'$ pre nejaké $a, b, a', b' \in M$ a zároveň taká, že $1 \equiv 1$. Podmienka $1 \equiv 1$ je ale splnená triviálne pre všetky relácie ekvivalencie: nulárne operácie sú z hľadiska kongruencií bezvýznamné. Relácia ekvivalencie $\equiv$ je teda kongruenciou na monoide $(M, \cdot, 1)$ práve vtedy, keď je kongruenciou na pologrupe $(M, \cdot)$.

Príklad 2.3.6. Ukážeme, že aj kongruenciami na *grupe* $(G, \cdot, ^{-1}, 1)$ sú práve všetky kongruencie na pologrupe $(G, \cdot)$. Podľa definície 2.3.1 a pozorovania z predchádzajúceho príkladu je kongruenciou na $(G, \cdot, ^{-1}, 1)$ relácia ekvivalencie $\equiv$ na G taká, že $a \cdot b \equiv a' \cdot b'$ kedykoľvek $a \equiv a'$ a súčasne $b \equiv b'$ pre nejaké $a, b, a', b' \in G$ a $a^{-1} \equiv b^{-1}$ kedykoľvek $a \equiv b$ pre nejaké $a, b \in G$. Aby sme dospeli ku kýženému záveru, potrebujeme ukázať, že druhá z uvedených vlastností je dôsledkom prvej. Ak má ale relácia ekvivalencie $\equiv$ prvú z týchto vlastností a $a \equiv b$, dostávame $1 = a \cdot a^{-1} \equiv b \cdot a^{-1}$. Teda $1 \equiv b \cdot a^{-1}$, z čoho $b^{-1} = b^{-1} \cdot 1 \equiv b^{-1} \cdot b \cdot a^{-1} = a^{-1}$, a teda naozaj $a^{-1} \equiv b^{-1}$.[5]

Príklad 2.3.7. Pozorovanie z predošlého príkladu rozhodne neplatí pre ľubovoľnú algebru $(A, \cdot, u, 1)$ typu $(2, 1, 0)$, a to hoci aj v prípade, že $(A, \cdot, 1)$ je monoid. Napríklad monoid $(\mathbb{N}, +, 0)$ môžeme rozšíriť o unárnu operáciu $u\colon \mathbb{N} \to \mathbb{N}$ takú, že

$$u(n) = \begin{cases} 1 & \text{ak } n = 0, \\ n & \text{inak.} \end{cases}$$

Je potom zrejmé, že kongruencia $\equiv_2$ na pologrupe $(\mathbb{N}, +)$ z príkladu 2.3.4(*ii*), ktorá je podľa pozorovania z príkladu 2.3.5 kongruenciou aj na monoide $(\mathbb{N}, +, 0)$, nie je kongruenciou na algebre $(\mathbb{N}, +, u, 0)$.

Príklad 2.3.8. Z pozorovaní učinených v príkladoch 2.3.5 a 2.3.6 vyplýva, že kongruenciami na okruhu $(R, +, \cdot, -, 0, 1)$ sú práve všetky relácie ekvivalencie $\equiv$ na R také, že pre všetky $a, b, a', b' \in R$ spĺňajúce $a \equiv a'$ a $b \equiv b'$ je $a + b \equiv a' + b'$ a $a \cdot b \equiv a' \cdot b'$.

Príklad 2.3.9. Pre všetky $n \in \mathbb{N} \setminus \{0\}$ je relácia ekvivalencie $\equiv$ na $\mathbb{Z}$ taká, že pre všetky $a, b \in \mathbb{Z}$ je $a \equiv b$ práve vtedy, keď $a \equiv b \pmod n$, evidentne kongruenciou na okruhu $(\mathbb{Z}, +, \cdot, -, 0, 1)$.

Definícia 2.3.10. Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f \in \tau})$ je algebra typu τ a $R \subseteq A \times A$ je binárna relácia na A. *Kongruenciou na $\mathscr{A}$ generovanou reláciou R* nazveme najmenšiu – čiže najjemnejšiu – kongruenciu $\langle R \rangle_{\mathscr{A}}$ na algebre $\mathscr{A}$ takú, že $R \subseteq \langle R \rangle_{\mathscr{A}}$.

Tvrdenie 2.3.11. *Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f \in \tau})$ je algebra typu τ a $R \subseteq A \times A$ je binárna relácia na A. Kongruencia $\langle R \rangle_{\mathscr{A}}$ na algebre $\mathscr{A}$ vždy existuje a*

$$\langle R \rangle_{\mathscr{A}} = \bigcap_{\substack{\varrho \text{ je kongruencia na } \mathscr{A} \\ R \subseteq \varrho}} \varrho.$$

[5] Priamočiarejšie toto pozorovanie vyplýva zo súvisu medzi kongruenciami a homomorfizmami, na ktorý poukážeme nižšie.

Dôkaz. Ľubovoľný prienik kongruencií je evidentne opäť kongruencia. Na druhej strane je zrejmé, že každá kongruencia obsahujúca R musí obsahovať kongruenciu

$$\bigcap_{\substack{\varrho \text{ je kongruencia na } \mathscr{A} \\ R \subseteq \varrho}} \varrho.$$

Preto je tento prienik najjemnejšou kongruenciou na $\mathscr{A}$ obsahujúcou R, čiže kongruenciou $\langle R \rangle_{\mathscr{A}}$. □

Môžeme teraz pristúpiť k definícii faktorizácie algebry $\mathscr{A}$ nejakého typu τ podľa kongruencie $\equiv$ na $\mathscr{A}$. Pre kongruencie pritom používame – rovnako ako pre všetky ostatné relácie ekvivalencie – bežnú notáciu $[x]_{\equiv}$ pre triedu ekvivalencie $\equiv$ obsahujúcu prvok x nosnej množiny algebry $\mathscr{A}$.

Definícia 2.3.12. Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f \in \tau})$ je algebra typu τ a $\equiv$ je kongruencia na $\mathscr{A}$. *Faktorovou algebrou* algebry $\mathscr{A}$ podľa kongruencie $\equiv$ nazveme algebru $\mathscr{A}/{\equiv} = (A/{\equiv}, (f^{\mathscr{A}/\equiv})_{f \in \tau})$, kde pre všetky $f \in \tau$ a všetky $a_1, \ldots, a_{\alpha(f)} \in A$ je

$$f^{\mathscr{A}/\equiv}\left([a_1]_{\equiv}, \ldots, [a_{\alpha(f)}]_{\equiv}\right) = \left[f^{\mathscr{A}}\left(a_1, \ldots, a_{\alpha(f)}\right)\right]_{\equiv}.$$

Tvrdenie 2.3.13. *Definícia 2.3.12 je korektná – definícia operácií $f^{\mathscr{A}/\equiv}$ nezávisí od výberu reprezentantov jednotlivých tried a $\mathscr{A}/{\equiv} = (A/{\equiv}, (f^{\mathscr{A}/\equiv})_{f \in \tau})$ je opäť algebrou typu τ.*

Dôkaz. V prípade, že dokážeme nezávislosť definície $f^{\mathscr{A}/\equiv}$ od výberu reprezentantov, bude druhá časť tvrdenia zrejmá. Avšak vzhľadom na to, že je $\equiv$ kongruencia, musí pre všetky $b_1 \equiv a_1, \ldots, b_{\alpha(f)} \equiv a_{\alpha(f)}$ byť

$$f^{\mathscr{A}}\left(a_1, \ldots, a_{\alpha(f)}\right) \equiv f^{\mathscr{A}}\left(b_1, \ldots, b_{\alpha(f)}\right),$$

z čoho

$$\begin{aligned} f^{\mathscr{A}/\equiv}\left([b_1]_{\equiv}, \ldots, [b_{\alpha(f)}]_{\equiv}\right) &= \left[f^{\mathscr{A}}\left(b_1, \ldots, b_{\alpha(f)}\right)\right]_{\equiv} = \left[f^{\mathscr{A}}\left(a_1, \ldots, a_{\alpha(f)}\right)\right]_{\equiv} = \\ &= f^{\mathscr{A}/\equiv}\left([a_1]_{\equiv}, \ldots, [a_{\alpha(f)}]_{\equiv}\right) \end{aligned}$$

a tvrdenie je dokázané. □

Zakončime tento oddiel dôkazom dôležitého pozorovania, ktoré možno na neformálnej úrovni zhrnúť takto: *kongruencie a surjektívne homomorfizmy sú rovnakými objektmi nazeranými z dvoch rôznych uhlov pohľadu.* Najprv si ukážme spôsob, ako z kongruencie získať surjektívny homomorfizmus.

Veta 2.3.14. *Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f \in \tau})$ je algebra typu τ a $\equiv$ je kongruencia na $\mathscr{A}$.* Prirodzená projekcia *$\nu \colon A \to A/{\equiv}$, definovaná pre všetky $a \in A$ predpisom*

$$\nu(a) = [a]_{\equiv},$$

je potom surjektívnym homomorfizmom $\nu \colon \mathscr{A} \to \mathscr{A}/{\equiv}$ algebier typu τ.

Dôkaz. Pre všetky $f \in \tau$ a všetky $a_1, \ldots, a_{\alpha(f)} \in A$ je

$$\begin{aligned} \nu\left(f^{\mathscr{A}}(a_1, \ldots, a_{\alpha(f)})\right) &= \left[f^{\mathscr{A}}(a_1, \ldots, a_{\alpha(f)})\right]_{\equiv} = f^{\mathscr{A}/\equiv}\left([a_1]_{\equiv}, \ldots, [a_{\alpha(f)}]_{\equiv}\right) = \\ &= f^{\mathscr{A}/\equiv}\left(\nu(a_1), \ldots, \nu(a_{\alpha(f)})\right) \end{aligned}$$

a ν je skutočne homomorfizmus algebry $\mathscr{A}$ do $\mathscr{A}/{\equiv}$. Jeho surjektívnosť je zrejmá, pretože pre všetky $a \in A$ je $a \in [a]_{\equiv}$, a teda $[a]_{\equiv} = \nu(a)$. □

Ku každému homomorfizmu algebier $\varphi\colon \mathscr{A} \to \mathscr{B}$ teraz definujeme jeho *jadro* $\ker\varphi$. Tým ale nebude ako pri klasicky definovaných jadrách homomorfizmov grúp alebo okruhov špeciálna podalgebra, ale bude ním určitá kongruencia na $\mathscr{A}$. Následne dokážeme *prvú vetu o izomorfizme* – univerzálny variant vety dobre známej pre grupy alebo okruhy – podľa ktorej bude algebra $\mathscr{A}/\ker\varphi$ vždy izomorfná obrazu homomorfizmu φ. Ak je teda homomorfizmus φ surjektívny, možno $\ker\varphi$ považovať za kongruenciu, ktorá v istom slova zmysle „opisuje ten istý objekt“ ako homomorfizmus φ.

Definícia 2.3.15. Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$, $\mathscr{B} = (B, (f^{\mathscr{B}})_{f\in\tau})$ sú algebry typu τ a $\varphi\colon \mathscr{A} \to \mathscr{B}$ je homomorfizmus. *Jadrom* homomorfizmu φ nazveme reláciu $\ker\varphi = \{(a,b) \in A^2 \mid \varphi(a) = \varphi(b)\}$.

Tvrdenie 2.3.16. *Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$, $\mathscr{B} = (B, (f^{\mathscr{B}})_{f\in\tau})$ sú algebry typu τ a $\varphi\colon \mathscr{A} \to \mathscr{B}$ je homomorfizmus. Potom je relácia $\ker\varphi$ kongruenciou na $\mathscr{A}$.*

Dôkaz. Nech $f \in \tau$ a $(a_1,b_1),\dots,(a_{\alpha(f)},b_{\alpha(f)}) \in \ker\varphi$. Potom $\varphi(a_1) = \varphi(b_1),\dots,\varphi(a_{\alpha(f)}) = \varphi(b_{\alpha(f)})$ a

$$\varphi(f^{\mathscr{A}}(a_1,\dots,a_{\alpha(f)})) = f^{\mathscr{B}}(\varphi(a_1),\dots,\varphi(a_{\alpha(f)})) = f^{\mathscr{B}}(\varphi(b_1),\dots,\varphi(b_{\alpha(f)})) = \varphi(f^{\mathscr{A}}(b_1,\dots,b_{\alpha(f)})),$$

z čoho

$$\left(f^{\mathscr{A}}(a_1,\dots,a_{\alpha(f)}), f^{\mathscr{A}}(b_1,\dots,b_{\alpha(f)})\right) \in \ker\varphi.$$

Relácia $\ker\varphi$ je teda skutočne kongruenciou na $\mathscr{A}$. □

Obrazom homomorfizmu $\varphi\colon \mathscr{A} \to \mathscr{B}$ nazveme podalgebru algebry $\mathscr{B}$ s nosnou množinou $\varphi(A)$, kde A je nosná množina algebry $\mathscr{A}$. Je jednoduché cvičenie dokázať, že v takom prípade ide naozaj o podalgebru. Obraz homomorfizmu $\varphi\colon \mathscr{A} \to \mathscr{B}$ označíme $\operatorname{im}\varphi$.

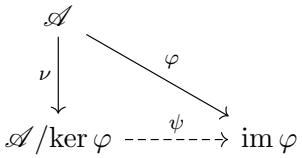
Veta 2.3.17 (Prvá veta o izomorfizme)**.** *Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$, $\mathscr{B} = (B, (f^{\mathscr{B}})_{f\in\tau})$ sú algebry typu τ a $\varphi\colon \mathscr{A} \to \mathscr{B}$ je homomorfizmus. Potom $\mathscr{A}/\ker\varphi \cong \operatorname{im}\varphi$.*

Dôkaz. Pre všetky $a \in A$ položme $\psi([a]_{\ker\varphi}) = \varphi(a)$. Je zrejmé, že táto definícia nezávisí od výberu reprezentanta triedy $[a]_{\ker\varphi}$ a že takto získané zobrazenie $\psi\colon A/\ker\varphi \to \varphi(A)$ je bijektívne. Ľahko napokon dokážeme, že ide o homomorfizmus $\psi\colon \mathscr{A}/\ker\varphi \to \operatorname{im}\varphi$: pre všetky $f \in \tau$ a $a_1,\dots,a_{\alpha(f)} \in A$ je

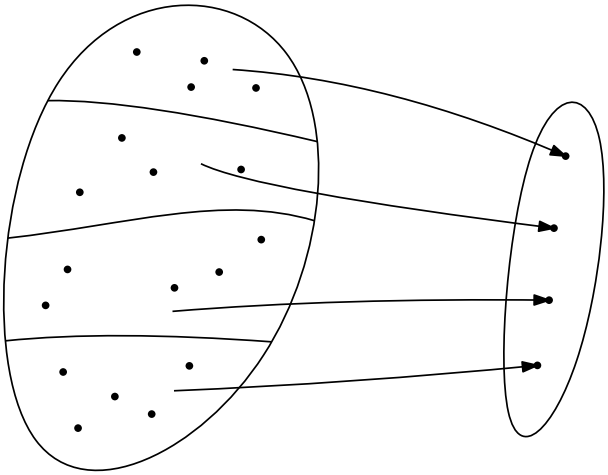
$$\begin{aligned}
\psi\left(f^{\mathscr{A}/\ker\varphi}\left([a_1]_{\ker\varphi},\dots,[a_{\alpha(f)}]_{\ker\varphi}\right)\right) &= \psi\left(\left[f^{\mathscr{A}}\left(a_1,\dots,a_{\alpha(f)}\right)\right]_{\ker\varphi}\right) = \\
&= \varphi\left(f^{\mathscr{A}}\left(a_1,\dots,a_{\alpha(f)}\right)\right) = \\
&= f^{\mathscr{B}}\left(\varphi\left(a_1\right),\dots,\varphi\left(a_{\alpha(f)}\right)\right) = \\
&= f^{\operatorname{im}\varphi}\left(\psi\left([a_1]_{\ker\varphi}\right),\dots,\psi\left([a_{\alpha(f)}]_{\ker\varphi}\right)\right).
\end{aligned}$$

Zobrazenie ψ je teda skutočne izomorfizmus. □

Poznámka 2.3.18. Dôkaz predchádzajúcej vety by sme mohli preformulovať aj tak, že by sme namiesto notácie pre triedy kongruencie $\ker\varphi$ používali prirodzenú projekciu $\nu\colon \mathscr{A} \to \mathscr{A}/\ker\varphi$. V takom prípade by sme zistili komutativitu nasledujúceho diagramu.



Kongruencie na algebre typu τ a surjektívne homomorfizmy medzi takýmito algebrami sú teda naozaj „odlišnými pohľadmi na ten istý objekt“. Kedykoľvek máme danú kongruenciu $\equiv$ na $\mathscr{A}$, je prirodzená projekcia $\nu\colon \mathscr{A} \to \mathscr{A}/{\equiv}$ surjektívnym homomorfizmom; kedykoľvek máme naopak daný surjektívny homomorfizmus $\varphi\colon \mathscr{A} \to \mathscr{B}$, je algebra $\mathscr{B} = \operatorname{im}\varphi$ izomorfná algebre $\mathscr{A}/\ker\varphi$. Súvis kongruencií so surjektívnymi homomorfizmami možno ilustrovať aj obrázkom 2.2.



Obr. 2.2: Na ilustráciu prvej vety o izomorfizme.

V klasickej algebre sa faktorové grupy a okruhy obyčajne nedefinujú s použitím kongruencií. Namiesto toho sa grupy faktorizujú podľa ich normálnych podgrúp a okruhy sa faktorizujú podľa ideálov. Ukážeme teraz, že tieto zvyčajné prístupy nie sú nijak náhodné, ale sú oba v skutočnosti ekvivalentné faktorizácii podľa kongruencií. Ukážeme, že kedykoľvek je $\equiv$ kongruencia na grupe resp. na okruhu, tak jej trieda obsahujúca prvok 1 resp. 0 nutne tvorí normálnu podgrupu resp. ideál. Naopak tiež ukážeme, že ľubovoľnú normálnu podgrupu grupy a ľubovoľný ideál okruhu možno využiť na definíciu kongruencie takej, že daná normálna podgrupa resp. ideál tvorí triedu obsahujúcu prvok 1 resp. 0.

Príklad 2.3.19. Uvažujme ľubovoľnú normálnu podgrupu H grupy $(G, \cdot, ^{-1}, 1)$.[6] Z klasickej algebry je známe, že binárna relácia $\equiv$ na G taká, že $a \equiv b$ práve vtedy, keď $aH = bH$, je reláciou ekvivalencie s triedami $[a]_{\equiv} = aH$ pre všetky $a \in G$. Ukážeme, že v skutočnosti ide o kongruenciu. Podľa pozorovania z príkladu 2.3.6 stačí ukázať, že ide o kongruenciu na pologrupe $(G, \cdot)$.

Nech $a, b, a', b' \in G$ sú také, že $a \equiv a'$ a $b \equiv b'$. Potom $aH = a'H$ a $bH = b'H$. Vďaka normálnosti podgrupy H teda dostávame

$$abH = aHb = a'Hb = a'bH = a'b'H,$$

a preto aj $ab \equiv a'b'$. Relácia $\equiv$ je teda naozaj kongruencia, pričom evidentne $H = [1]_{\equiv}$.

Uvažujme teraz naopak ľubovoľnú kongruenciu $\equiv$ na grupe $(G, \cdot, ^{-1}, 1)$ a dokážme, že $[1]_{\equiv}$ je nutne normálnou podgrupou grupy G. Ak $a, b \in [1]_{\equiv}$, tak $a \equiv 1$ a $b \equiv 1$, z čoho s využitím definície kongruencie dostávame $a^{-1} \equiv 1^{-1} = 1$ a následne aj $a^{-1}b \equiv 1$, čo znamená, že $a^{-1}b \in [1]_{\equiv}$. Trieda $[1]_{\equiv}$ je teda podgrupou grupy G.

Zostáva dokázať, že ide o normálnu podgrupu. To urobíme tak, že pre všetky $a \in G$ dokážeme rovnosti $a[1]_{\equiv} = [1]_{\equiv}a = [a]_{\equiv}$. Na jednej strane pre všetky $x \equiv 1$ máme $ax \equiv a$ a $xa \equiv a$, z čoho $a[1]_{\equiv} \subseteq [a]_{\equiv}$, ako aj $[1]_{\equiv}a \subseteq [a]_{\equiv}$. Ak naopak $y \in [a]_{\equiv}$, tak $y = aa^{-1}y \equiv a$ a $a^{-1}y \equiv 1$. Zisťujeme teda, že $y = aa^{-1}y \in a[1]_{\equiv}$ a symetricky dokážeme aj $y \in [1]_{\equiv}a$. Takto dostávame aj opačné inklúzie $a[1]_{\equiv} \supseteq [a]_{\equiv}$ a $[1]_{\equiv}a \supseteq [a]_{\equiv}$.

Príklad 2.3.20. Uvažujme teraz ľubovoľný ideál I v okruhu $(R, +, \cdot, -, 0, 1)$.[7] Z klasickej algebry je opäť známe, že binárna relácia $\equiv$ na R taká, že $a \equiv b$ práve vtedy, keď $a + I = b + I$, je reláciou ekvivalencie. Aby sme dokázali, že ide o kongruenciu na okruhu R, stačí podľa pozorovania z príkladu 2.3.8 dokázať, že ide o kongruenciu na pologrupách $(R, +)$ a $(R, \cdot)$.

Ak sú pritom $a, b, a', b' \in R$ prvky také, že $a \equiv a'$ a $b \equiv b'$, tak $a + b \equiv a' + b'$ vyplýva už z pozorovaní učinených v príklade 2.3.19, pretože $(R, +, -, 0)$ je komutatívna grupa a ideál I je jej podgrupa, ktorá

[6] Pripomeňme si, že podgrupa H grupy G je *normálna*, ak pre všetky $a \in G$ je $aH = Ha$.

[7] Množina $I \subseteq R$ tvorí *ideál* v okruhu R, ak pre všetky $a, b \in I$ a $x \in R$ je $a + b \in I$, $a \cdot x \in I$ a $x \cdot a \in I$.

musí byť vďaka komutatívnosti $(R, +, -, 0)$ nutne normálna. Z toho následne dostávame $a - a' \equiv 0$ a $b - b' \equiv 0$, čiže $a - a' \in I$ a $b - b' \in I$. Potom ale aj

$$ab - a'b' = a(b - b') + (a - a')b' \in I,$$

z čoho $ab - a'b' \equiv 0$ a v dôsledku toho $ab \equiv a'b'$. Relácia ekvivalencie $\equiv$ je teda naozaj kongruencia na okruhu R.

Naopak teraz predpokladajme, že je daná kongruencia $\equiv$ na okruhu R. Ukážeme, že $[0]_\equiv$ je ideál v R. Pre všetky $a, b \in [0]_\equiv$ ale musí platiť $a \equiv 0$ a zároveň $b \equiv 0$, z čoho už priamo dostávame $a+b \equiv 0$, a teda aj $a + b \in [0]_\equiv$. Ak ďalej $a \in [0]_\equiv$ a $x \in R$, tak $a \equiv 0$, z čoho $a \cdot x \equiv 0$, ako aj $x \cdot a \equiv 0$, čiže $a \cdot x \in [0]_\equiv$ a $x \cdot a \in [0]_\equiv$. Trieda $[0]_\equiv$ kongruencie $\equiv$ teda naozaj tvorí ideál v R.

Ukážme si ešte, že pri monoidoch vo všeobecnosti *nemožno* nahradiť kongruencie ich triedami obsahujúcimi neutrálny prvok.

Príklad 2.3.21. Uvažujme monoid $(\mathbb{N}, +, 0)$. Na ňom existuje nekonečne veľa rôznych kongruencií $\equiv$ takých, že $[0]_\equiv = \{0\}$. Napríklad môžeme pre všetky $n \in \mathbb{N}$ a všetky $a, b \in \mathbb{N}$ položiť $a \equiv_n b$ práve vtedy, keď $a = b$ alebo $a, b \in \mathbb{N} \setminus \{0, \ldots, n\}$.

2.4 Algebry termov

Pre každý typ τ teraz definujeme špeciálne algebry, ktoré sú svojím spôsobom predobrazom všetkých ostatných algebier typu τ – takzvané *algebry termov* typu τ.

Definícia 2.4.1. Nech τ je typ a X je množina taká, že $X \cap \tau = \emptyset$. Množina $T_\tau(X)$ všetkých *termov* typu τ nad množinou premenných X je jazyk nad (vo všeobecnosti nekonečnou) abecedou obsahujúcou všetky premenné z X, všetky operačné symboly z τ, symboly pre zátvorky a čiarku, definovaný nasledovne:

(*i*) Pre všetky $x \in X$ je $x \in T_\tau(X)$.

(*ii*) Pre všetky $f \in \tau$ a všetky $t_1, \ldots, t_{\alpha(f)} \in T_\tau(X)$ je slovo $f(t_1, \ldots, t_{\alpha(f)}) \in T_\tau(X)$.

(*iii*) Nič iné nie je v $T_\tau(X)$.

Naša dohoda, podľa ktorej budeme pre niektoré druhy operácií používať obvyklejšiu notáciu, sa premietne aj do nášho chápania termov. Napríklad pre typ $\tau = \{\cdot, ^{-1}, 1\}$ s aritami $\alpha(\cdot) = 2$, $\alpha(^{-1}) = 1$ a $\alpha(1) = 0$ budeme term $\cdot(x, y)$ písať aj ako $x \cdot y$ a term $^{-1}(x)$ aj ako x^{-1}.

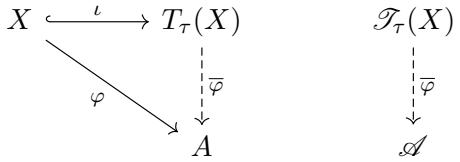
Príklad 2.4.2. Pre všetky typy τ zodpovedá $T_\tau(\emptyset)$ výrazom budovaných na konštantách, číže nulárnych operačných symboloch. Táto množina je teda neprázdna práve vtedy, keď v τ existuje aspoň jeden nulárny operačný symbol.

Na termoch typu τ nad X môžeme prirodzeným spôsobom definovať algebru typu τ – každý operačný symbol interpretujeme ako operáciu vytvorenia príslušného termu. Takúto algebru nazveme *algebrou termov* typu τ nad množinou premenných X a budeme ju označovať ako $\mathscr{T}_\tau(X)$.

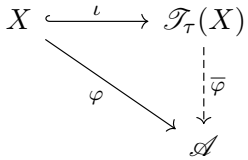
Definícia 2.4.3. Nech τ je typ a X je množina taká, že $X \cap \tau = \emptyset$. *Algebrou termov* typu τ nad množinou premenných X nazveme algebru $\mathscr{T}_\tau(X) = (T_\tau(X), (f^{\mathscr{T}_\tau(X)})_{f \in \tau})$ typu τ, kde pre všetky $f \in \tau$ a $t_1, \ldots, t_{\alpha(f)} \in T_\tau(X)$ je

$$f^{\mathscr{T}_\tau(X)}(t_1, \ldots, t_{\alpha(f)}) = f(t_1, \ldots, t_{\alpha(f)}).$$

Kľúčovou vlastnosťou algebier termov je *vlastnosť univerzálneho zobrazenia*, ktorá je sformulovaná v nasledujúcej vete. Ak označíme ako $\iota\colon X \hookrightarrow T_\tau(X)$ vloženie množiny X do množiny $T_\tau(X)$, hovorí táto veta nasledovné: pre všetky zobrazenia $\varphi\colon X \to A$, kde A je nosná množina algebry $\mathscr{A}$, existuje jediný homomorfizmus algebier $\overline{\varphi}\colon \mathscr{T}_\tau(X) \to \mathscr{A}$ taký, že trojuholník v nasledujúcom diagrame komutuje.



V prípade, že nebudeme striktne rozlišovať zobrazenia medzi množinami od homomorfizmov algebier, môžeme tento diagram nakresliť v nasledujúcej zjednodušenej – a v kontexte univerzálnej algebry obvyklejšej – podobe.



Veta 2.4.4. *Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ je algebra typu τ a X je množina taká, že $X \cap \tau = \emptyset$. Pre všetky zobrazenia $\varphi\colon X \to A$ potom existuje práve jeden homomorfizmus algebier $\overline{\varphi}\colon \mathscr{T}_\tau(X) \to \mathscr{A}$ taký, že pre všetky $x \in X$ je $\overline{\varphi}(x) = \varphi(x)$.*

Dôkaz. Definujme zobrazenie $\overline{\varphi}\colon T_\tau(X) \to A$ induktívne ako $\overline{\varphi}(x) = \varphi(x)$ pre všetky $x \in X$ a ako

$$\overline{\varphi}\left(f(t_1, \ldots, t_{\alpha(f)})\right) = f^{\mathscr{A}}\left(\overline{\varphi}(t_1), \ldots, \overline{\varphi}(t_{\alpha(f)})\right)$$

pre všetky $f \in \tau$ a $t_1, \ldots, t_{\alpha(f)} \in T_\tau(X)$. Zrejme potom ide o homomorfizmus algebier $\overline{\varphi}\colon \mathscr{T}_\tau(X) \to \mathscr{A}$, pretože pre všetky $f \in \tau$ a $t_1, \ldots, t_{\alpha(f)} \in T_\tau(X)$ je

$$\overline{\varphi}\left(f^{\mathscr{T}_\tau(X)}(t_1, \ldots, t_{\alpha(f)})\right) = \overline{\varphi}\left(f(t_1, \ldots, t_{\alpha(f)})\right) = f^{\mathscr{A}}\left(\overline{\varphi}(t_1), \ldots, \overline{\varphi}(t_{\alpha(f)})\right).$$

Zostáva dokázať jedinečnosť homomorfizmu $\overline{\varphi}$. Nech $\psi\colon \mathscr{T}_\tau(X) \to \mathscr{A}$ je ľubovoľný homomorfizmus taký, že pre všetky $x \in X$ je $\psi(x) = \varphi(x)$. Okamžite potom zisťujeme, že $\psi(x) = \overline{\varphi}(x)$ pre všetky $x \in X$; ak ďalej $f \in \tau$ a $t_1, \ldots, t_{\alpha(f)} \in T_\tau(X)$ sú termy také, že $\psi(t_1) = \overline{\varphi}(t_1), \ldots, \psi(t_{\alpha(f)}) = \overline{\varphi}(t_{\alpha(f)})$, z vlastnosti homomorfizmu dostávame

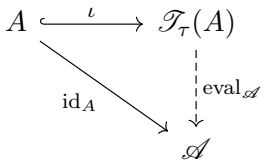
$$\begin{aligned}\psi\left(f(t_1, \ldots, t_{\alpha(f)})\right) &= \psi\left(f^{\mathscr{T}_\tau(X)}(t_1, \ldots, t_{\alpha(f)})\right) = f^{\mathscr{A}}\left(\psi(t_1), \ldots, \psi(t_{\alpha(f)})\right) = \\ &= f^{\mathscr{A}}\left(\overline{\varphi}(t_1), \ldots, \overline{\varphi}(t_{\alpha(f)})\right) = \overline{\varphi}\left(f(t_1, \ldots, t_{\alpha(f)})\right).\end{aligned}$$

Preto $\psi(t) = \overline{\varphi}(t)$ pre všetky $t \in \mathscr{T}_\tau(X)$, z čoho $\psi = \overline{\varphi}$. □

Vďaka práve dokázanej vlastnosti sa algebra termov $\mathscr{T}_\tau(X)$ nazýva aj (*absolútne*) *voľnou* algebrou typu τ nad množinou generátorov X. Voľnými algebrami sa ešte budeme podrobnejšie zaoberať neskôr.

Homomorfizmus $\overline{\varphi}\colon \mathscr{T}_\tau(X) \to \mathscr{A}$, o ktorého existencii hovorí predchádzajúca veta, možno chápať ako *vyhodnotenie termov* v algebre $\mathscr{A}$ v prípade, že sú za všetky premenné $x \in X$ dosadené hodnoty $\varphi(x)$. Pre všetky premenné $x \in X$ totiž tento homomorfizmus spĺňa $\overline{\varphi}(x) = \varphi(x)$ a pre všetky termy $t = f(t_1, \ldots, t_{\alpha(f)})$ je $\overline{\varphi}(t) = f^{\mathscr{A}}(\overline{\varphi}(t_1), \ldots, \overline{\varphi}(t_{\alpha(f)}))$; ak sú teda $\overline{\varphi}(t_1), \ldots, \overline{\varphi}(t_{\alpha(f)})$ vyhodnoteniami termov $t_1, \ldots, t_{\alpha(f)}$ v $\mathscr{A}$ vzhľadom na φ, je aj $\overline{\varphi}(t)$ vyhodnotením termu t v $\mathscr{A}$ vzhľadom na φ.

Veľmi špeciálny prípad homomorfizmu $\overline{\varphi}$ dostaneme vtedy, keď za množinu premenných X vezmeme nosnú množinu A algebry $\mathscr{A}$ a zobrazenie φ definujeme predpisom $\varphi(a) = a$ pre všetky $a \in A$. Namiesto premenných teda akoby vezmeme konštanty a termy budujeme na nich; homomorfizmus $\overline{\varphi}$ pritom takéto termy, ktoré možno považovať za reprezentácie *výrazov* v algebre $\mathscr{A}$, vyhodnocuje v algebre $\mathscr{A}$. Homomorfizmus $\overline{\varphi}$ preto nazveme *vyhodnocovacím homomorfizmom* pre algebru $\mathscr{A}$ a budeme ho označovať ako $\mathrm{eval}_{\mathscr{A}}$.



Definícia 2.4.5. Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ je algebra typu τ a $\mathrm{id}_A\colon A \to A$ je identické zobrazenie na A. *Vyhodnocovacím homomorfizmom* pre algebru $\mathscr{A}$ nazveme homomorfizmus $\mathrm{eval}_{\mathscr{A}} := \overline{\mathrm{id}_A}\colon \mathscr{T}_\tau(A) \to \mathscr{A}$.

2.5 Variety algebier

Posunieme sa teraz o úroveň abstrakcie vyššie a namiesto vlastností algebier z nejakej triedy sa začneme zaoberať spoločnými znakmi rôznych *tried algebier* s určitými vlastnosťami. Naším hlavným cieľom pritom bude charakterizovať a preskúmať tie triedy, ktoré sú okrem typu jednoznačne určené už len nejakou množinou *identít* platných pre všetky ich prvky: napríklad splnenie identity $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ – t. j. $\cdot(x, \cdot(y, z)) = \cdot(\cdot(x, y), z)$ – pre všetky prvky x, y, z nosnej množiny algebry typu $\tau = \{\cdot\}$ s $\alpha(\cdot) = 2$ jednoznačne opisuje triedu všetkých pologrúp. V oddiele 2.1 sme videli, že podobným spôsobom možno opísať aj triedy všetkých grupoidov – čo sú jednoducho všetky algebry typu (2) –, monoidov, grúp, polozväzov, polokruhov, okruhov, či zväzov. Podobne aj vektorové priestory nad poľom $\mathbb{F}$, chápané v zmysle príkladu 2.2.12, možno opísať pomocou nekonečnej množiny identít. Spomedzi známych tried algebier ale čisto pomocou identít nebude možné opísať polia alebo napríklad obory integrity.

Trieda algebier opísateľná pomocou identít sa nazýva *varietou*. Toto pomenovanie je sčasti inšpirované klasickou algebraickou geometriou, kde sa pod varietou rozumie množina riešení systému polynomických rovníc. Podobne aj varieta v našom ponímaní bude trieda určená množinou identít; hlbší súvis medzi oboma pojmami ale neexistuje.

Hoci za cieľ nasledujúcich úvah možno považovať charakterizáciu variet v tomto ponímaní, je v súčasnosti častejší opačný prístup, ktorého sa budeme držať aj my: varietu nedefinujeme ako triedu opísateľnú pomocou identít, ale prostredníctvom jej uzáverových vlastností. Až následne dokážeme, že triedy s uzáverovými vlastnosťami vyžadovanými definíciou variety sú aj opísateľné pomocou identít a naopak. Z charakterizácie variet sa teda stáva ich definícia a naopak.

Obraz $\mathrm{im}\,\varphi$ homomorfizmu algebier $\varphi\colon \mathscr{A} \to \mathscr{B}$ v nasledujúcom označujeme ako $\varphi(\mathscr{A})$.

Definícia 2.5.1. Nech $\mathcal{C}$ je trieda algebier typu τ. Potom:

a) Trieda $\mathbf{H}\mathcal{C}$ pozostáva z práve všetkých homomorfných obrazov $\varphi(\mathscr{A})$ pre $\mathscr{A} \in \mathcal{C}$ a ľubovoľný homomorfizmus $\varphi\colon \mathscr{A} \to \mathscr{B}$ algebier typu τ.

b) Trieda $\mathbf{S}\mathcal{C}$ pozostáva z práve všetkých podalgebier $\mathscr{B}$ algebier $\mathscr{A} \in \mathcal{C}$.

c) Trieda $\mathbf{P}\mathcal{C}$ pozostáva z práve všetkých súčinov $\prod_{i\in I} \mathscr{A}_i$, kde I je indexová množina a $\mathscr{A}_i \in \mathcal{C}$ pre všetky $i \in I$.

d) Trieda $\mathbf{P}_{\mathrm{fin}}\mathcal{C}$ pozostáva z práve všetkých konečných súčinov $\prod_{i\in I} \mathscr{A}_i$, kde I je konečná indexová množina a $\mathscr{A}_i \in \mathcal{C}$ pre všetky prvky $i \in I$.

e) Trieda $\mathbf{I}\mathcal{C}$ pozostáva z práve všetkých algebier typu τ izomorfných nejakej algebre $\mathscr{A} \in \mathcal{C}$.

Niektorí autori zahŕňajú operátor $\mathbf{I}$ už do definícií operátorov $\mathbf{S}$, $\mathbf{P}$ a $\mathbf{P}_{\mathrm{fin}}$, ktoré definujú ako naše $\mathbf{IS}$, $\mathbf{IP}$ resp. $\mathbf{IP}_{\mathrm{fin}}$.

Práve sme teda pre všetky typy τ zaviedli päť operátorov $\mathbf{H}, \mathbf{S}, \mathbf{P}, \mathbf{P}_{\text{fin}}, \mathbf{I}$ na univerze všetkých tried algebier typu τ. Ako prvé tvrdenie dokážeme, že pri $\mathbf{H}$, $\mathbf{S}$, $\mathbf{IP}$ a $\mathbf{IP}_{\text{fin}}$ ide o *uzáverové operátory*. Operátor $\mathbf{F}\colon 2^{\mathcal{U}} \to 2^{\mathcal{U}}$ pre nejakú triedu $\mathcal{U}$ je *uzáverový*, ak pre všetky $\mathcal{C} \subseteq \mathcal{U}$ je $\mathbf{F}\mathcal{C} \supseteq \mathcal{C}$ (extenzívnosť), pre všetky $\mathcal{C} \subseteq \mathcal{D} \subseteq \mathcal{U}$ je $\mathbf{F}\mathcal{C} \subseteq \mathbf{F}\mathcal{D}$ (izotónnosť) a pre všetky $\mathcal{C} \subseteq \mathcal{U}$ je $\mathbf{F}\mathbf{F}\mathcal{C} = \mathbf{F}\mathcal{C}$ (idempotentnosť). Podmienka extenzívnosti hovorí, že uzáverový operátor prvky do triedy iba pridáva; idempotentnosť hovorí, že po aplikovaní uzáveru je už trieda uzavretá a izotónnosť hovorí, že v takom prípade vždy pôjde o najmenšiu uzavretú nadtriedu pôvodnej triedy. Ľahko teda vidieť, že $\mathbf{F}$ je uzáverový operátor práve vtedy, keď pre všetky $\mathcal{C} \subseteq \mathcal{U}$ je $\mathbf{F}\mathcal{C}$ najmenšia trieda obsahujúca $\mathcal{C}$ a uzavretá na $\mathbf{F}$.

Tvrdenie 2.5.2. *Operátory* $\mathbf{H}$, $\mathbf{S}$, $\mathbf{IP}$ *a* $\mathbf{IP}_{\text{fin}}$ *na univerze všetkých tried algebier typu* τ *sú uzáverové.*

Dôkaz. Extenzívnosť vyplýva pri $\mathbf{H}$ zo skutočnosti, že pre všetky algebry $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ typu τ je $\mathrm{id}_A\colon \mathscr{A} \to \mathscr{A}$ homomorfizmus; pri $\mathbf{S}$ zo skutočnosti, že každá algebra je podalgebrou seba samej; pri $\mathbf{IP}$ a $\mathbf{IP}_{\text{fin}}$ zo skutočnosti, že každú algebru $\mathscr{A}$ možno vyjadriť ako

$$\mathscr{A} = \prod_{i\in\{\bullet\}} \mathscr{A}.$$

Izotónnosť všetkých štyroch operátorov je zrejmá. Rovnosť $\mathbf{HH} = \mathbf{H}$ vyplýva zo skutočnosti, že zloženie dvoch surjektívnych homomorfizmov je opäť surjektívny homomorfizmus.Rovnosť $\mathbf{SS} = \mathbf{S}$ vyplýva zo skutočnosti, že podalgebra podalgebry algebry $\mathscr{A}$ je evidentne vždy aj podalgebrou algebry $\mathscr{A}$. Napokon rovnosti $\mathbf{IPIP} = \mathbf{IP}$ a $\mathbf{IP}_{\text{fin}}\mathbf{IP}_{\text{fin}} = \mathbf{IP}_{\text{fin}}$ vyplývajú zo skutočnosti, že ak

$$\mathscr{B}_i \cong \prod_{j\in J_i} \mathscr{A}_{i,j}$$

pre všetky $i \in I$, tak

$$\prod_{i\in I} \mathscr{B}_i \cong \prod_{i\in I}\prod_{j\in J_i} \mathscr{A}_{i,j} \cong \prod_{(i,j)\in\bigcup_{i\in I}(\{i\}\times J_i)} \mathscr{A}_{i,j};$$

táto vlastnosť pritom evidentne platí bez ohľadu na to, či sú množiny I a J_i pre $i \in I$ ľubovoľné, alebo konečné. □

Definícia 2.5.3. Trieda $\mathcal{V}$ algebier typu τ je *varieta*, ak je uzavretá na operátory $\mathbf{H}$, $\mathbf{S}$ a $\mathbf{P}$, čiže ak $\mathbf{H}\mathcal{V} = \mathbf{S}\mathcal{V} = \mathbf{P}\mathcal{V} = \mathcal{V}$.

Ekvivalentne by sme definíciu variety mohli sformulovať aj prostredníctvom uzavretosti na operátory $\mathbf{H}$, $\mathbf{S}$ a $\mathbf{IP}$ – pre všetky triedy $\mathcal{C}$ algebier typu τ je totiž zrejme $\mathbf{P}\mathcal{C} \subseteq \mathbf{IP}\mathcal{C} \subseteq \mathbf{HP}\mathcal{C}$.

Pre ľubovoľnú triedu $\mathcal{C}$ algebier typu τ je *varieta generovaná triedou* $\mathcal{C}$ – čiže najmenšia varieta algebier typu τ obsahujúca triedu $\mathcal{C}$ – očividne daná zjednotením všetkých tried $\mathbf{F}_1\mathbf{F}_2\ldots\mathbf{F}_k\mathcal{C}$ cez všetky $k \in \mathbb{N}$ a $\mathbf{F}_1, \ldots, \mathbf{F}_k \in \{\mathbf{H}, \mathbf{S}, \mathbf{P}\}$. V nasledujúcom budeme dokazovať jednoduchšiu charakterizáciu tejto generovanej variety, podľa ktorej stačí na $\mathcal{C}$ postupne aplikovať operátory $\mathbf{P}$, $\mathbf{S}$ a $\mathbf{H}$, a to zakaždým iba raz. Prvým krokom pritom bude nasledujúce tvrdenie.

Tvrdenie 2.5.4. *Nech* $\mathcal{C}$ *je trieda algebier typu* τ. *Potom* $\mathbf{SHC} \subseteq \mathbf{HSC}$, $\mathbf{PSC} \subseteq \mathbf{SPC}$ *a* $\mathbf{PHC} \subseteq \mathbf{HPC}$.

Dôkaz. Ak $\mathscr{B} \in \mathbf{SHC}$, tak existuje algebra $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau}) \in \mathcal{C}$ a homomorfizmus $\varphi\colon \mathscr{A} \to \mathscr{X}$ taký, že $\mathscr{B} = (B, (f^{\mathscr{B}})_{f\in\tau})$ je podalgebrou $\varphi(\mathscr{A})$. Nech $A' = \varphi^{-1}(B)$. Pre všetky $f \in \tau$ a $a_1, \ldots, a_{\alpha(f)} \in A'$ potom

$$\varphi\left(f^{\mathscr{A}}\left(a_1, \ldots, a_{\alpha(f)}\right)\right) = f^{\varphi(\mathscr{A})}\left(\varphi(a_1), \ldots, \varphi(a_{\alpha(f)})\right) = f^{\mathscr{B}}\left(\varphi(a_1), \ldots, \varphi(a_{\alpha(f)})\right) \in B,$$

pretože $\varphi(a_1), \ldots, \varphi(a_{\alpha(f)}) \in B$ a $\mathscr{B}$ je podalgebrou $\varphi(\mathscr{A})$. Preto

$$f^{\mathscr{A}}\left(a_1, \ldots, a_{\alpha(f)}\right) \in \varphi^{-1}(B) = A',$$

z čoho vyplýva, že $\mathscr{A}' = (A', (f^{\mathscr{A}'})_{f\in\tau})$, kde pre všetky $f \in \tau$ je

$$f^{\mathscr{A}'} = f^{\mathscr{A}}|_{(A')^{\alpha(f)}},$$

je podalgebrou algebry $\mathscr{A}$. Keďže ale $B \subseteq \varphi(A)$ a $A' = \varphi^{-1}(B)$, nutne $\varphi(A') = B$ resp. $\varphi(\mathscr{A}') = \mathscr{B}$. Preto naozaj $\mathscr{B} \in \mathbf{HS}\mathcal{C}$.

Nech ďalej $\mathscr{A} \in \mathbf{PS}\mathcal{C}$. Potom existuje množina I taká, že pre všetky $i \in I$ existuje nejaká algebra $\mathscr{A}_i \in \mathcal{C}$ a jej podalgebra $\mathscr{B}_i$ tak, že

$$\mathscr{A} = \prod_{i\in I} \mathscr{B}_i.$$

Algebra $\mathscr{A}$ je potom ale evidentne podalgebrou súčinu

$$\prod_{i\in I} \mathscr{A}_i,$$

a teda $\mathscr{A} \in \mathbf{SP}\mathcal{C}$.

Nech napokon $\mathscr{B} \in \mathbf{PH}\mathcal{C}$. Potom existuje množina I a pre všetky $i \in I$ algebra $\mathscr{A}_i = (A_i, (f^{\mathscr{A}_i})_{f\in\tau})$ z triedy $\mathcal{C}$ spolu s homomorfizmom $\varphi_i \colon \mathscr{A}_i \to \mathscr{X}_i$ tak, že

$$\mathscr{B} = \prod_{i\in I} \varphi_i(\mathscr{A}_i).$$

Definujme homomorfizmus

$$\varphi \colon \prod_{i\in I} \mathscr{A}_i \to \prod_{i\in I} \mathscr{X}_i$$

pre všetky $(a_i \in A_i \mid i \in I)$ ako

$$\varphi(a_i \in A_i \mid i \in I) = (\varphi_i(a_i) \mid i \in I).$$

Evidentne potom

$$\mathscr{B} = \varphi\left(\prod_{i\in I} \mathscr{A}_i\right),$$

v dôsledku čoho $\mathscr{B} \in \mathbf{HP}\mathcal{C}$. □

Definícia 2.5.5. Nech $\mathcal{C}$ je trieda algebier typu τ. *Varietou generovanou triedou* $\mathcal{C}$ nazveme najmenšiu varietu $\mathcal{V}$ takú, že $\mathcal{C} \subseteq \mathcal{V}$. Varietu generovanú triedou $\mathcal{C}$ označíme $\mathbf{V}\mathcal{C}$.

Veta 2.5.6 (Tarski)**.** *Nech $\mathcal{C}$ je trieda algebier typu τ. Potom $\mathbf{V}\mathcal{C} = \mathbf{HSP}\mathcal{C}$.*

Dôkaz. Zrejme $\mathbf{HSP}\mathcal{C} \subseteq \mathbf{V}\mathcal{C}$. Aby sme dokázali rovnosť týchto dvoch tried, stačí ukázať, že je trieda $\mathbf{HSP}\mathcal{C}$ uzavretá na operátory $\mathbf{H}$, $\mathbf{S}$ a $\mathbf{P}$. Z tvrdení 2.5.2 a 2.5.4 ale dostávame $\mathbf{HHSP}\mathcal{C} = \mathbf{HSP}\mathcal{C}$, $\mathbf{SHSP}\mathcal{C} \subseteq \mathbf{HSSP}\mathcal{C} = \mathbf{HSP}\mathcal{C}$ a $\mathbf{PHSP}\mathcal{C} \subseteq \mathbf{HPSP}\mathcal{C} \subseteq \mathbf{HSPP}\mathcal{C} \subseteq \mathbf{HSIPIP}\mathcal{C} = \mathbf{HSIP}\mathcal{C} \subseteq \mathbf{HSHP}\mathcal{C} \subseteq \mathbf{HHSP}\mathcal{C} = \mathbf{HSP}\mathcal{C}$. □

2.6 Identity a Birkhoffova veta o varietach

Budeme teraz dokazovať *Birkhoffovu vetu o varietach*, podľa ktorej sú varietami práve tie triedy algebier, ktoré sú opísateľné pomocou identít. Avšak na to, aby sme túto vetu vedeli vôbec sformulovať, potrebujeme upresniť, čo budeme pod identitami rozumieť.

Definícia 2.6.1. Nech τ je typ algebier. *Identitou* typu τ potom nazveme ľubovoľnú dvojicu termov $(t_1, t_2) \in \mathscr{T}_\tau(X) \times \mathscr{T}_\tau(X)$ pre nejakú množinu premenných X takú, že $X \cap \tau = \emptyset$. Namiesto (t_1, t_2) píšeme aj $t_1 \approx t_2$.[8]

Definícia 2.6.2. Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ je algebra typu τ a $t_1 \approx t_2 \in \mathscr{T}_\tau(X) \times \mathscr{T}_\tau(X)$ je identita toho istého typu τ pre nejaké X také, že $X \cap \tau = \emptyset$. Hovoríme, že identita $t_1 \approx t_2$ je *splnená* v algebre $\mathscr{A}$, ak pre všetky zobrazenia $\varphi\colon X \to A$ je $\overline{\varphi}(t_1) = \overline{\varphi}(t_2)$. V takom prípade píšeme aj $\mathscr{A} \models t_1 \approx t_2$.

Vďaka vete 2.4.4 sú homomorfizmy $\psi\colon \mathscr{T}_\tau(X) \to \mathscr{A}$ jednoznačne určené obrazmi $\psi(x)$ pre $x \in X$. Každé zobrazenie $\varphi\colon X \to A$ naopak indukuje jediný homomorfizmus $\overline{\varphi}\colon \mathscr{T}_\tau(X) \to \mathscr{A}$. Z toho vyplýva, že $\mathscr{A} \models t_1 \approx t_2$ práve vtedy, keď $\psi(t_1) = \psi(t_2)$ pre všetky homomorfizmy $\psi\colon \mathscr{T}_\tau(X) \to \mathscr{A}$.

Poznámka 2.6.3. Ešte inak môžeme splnenie identity algebrou vyjadriť aj nasledujúcim spôsobom: k ľubovoľnému termu $t \in \mathscr{T}_\tau(X)$ môžeme na každej algebre $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ typu τ uvažovať ním určenú *termovú operáciu* $t^{\mathscr{A}}\colon A^X \to A$ danú pre všetky zobrazenia $\varphi\colon X \to A$ predpisom $t^{\mathscr{A}}(\varphi) = \overline{\varphi}(t)$. (Pre konečnú množinu premenných $X = \{x_1, \dots, x_n\}$ a zobrazenie $\varphi\colon x_k \mapsto a_k$ pre $k = 1, \dots, n$ pritom môžeme pre $t^{\mathscr{A}}(\varphi)$ písať aj $t^{\mathscr{A}}(a_1, \dots, a_n)$.) Takáto operácia teda zodpovedá vyhodnoteniu termu t v algebre $\mathscr{A}$ pri dosadení argumentov termovej operácie za jednotlivé premenné množiny X. Identita $t_1 \approx t_2$ je potom splnená v algebre $\mathscr{A}$ práve vtedy, keď $t_1^{\mathscr{A}} = t_2^{\mathscr{A}}$.

Definícia 2.6.4. Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ je algebra typu τ a $T \subseteq \mathscr{T}_\tau(X) \times \mathscr{T}_\tau(X)$ je množina identít. Potom $\mathscr{A} \models T$, ak $\mathscr{A} \models t_1 \approx t_2$ pre všetky $t_1 \approx t_2 \in T$.

Definícia 2.6.5. Nech τ je typ a $T \subseteq \mathscr{T}_\tau(X) \times \mathscr{T}_\tau(X)$ je množina identít. Pre triedu všetkých algebier typu τ spĺňajúcich identity z T budeme písať

$$[\![T]\!]_\tau := \{\mathscr{A} \text{ typu } \tau \mid \mathscr{A} \models T\}.$$

V prípade, že $T = \{s_1 \approx t_1, s_2 \approx t_2, \dots, s_n \approx t_n\}$ je konečná množina identít, píšeme aj

$$[\![T]\!]_\tau = [\![s_1 \approx t_1, s_2 \approx t_2, \dots, s_n \approx t_n]\!]_\tau.$$

Dolný index τ vynechávame v prípadoch, keď je typ algebry zrejmý z kontextu.

Príklad 2.6.6. Trieda všetkých pologrúp $(S, \cdot)$ je daná ako $[\![x \cdot (y \cdot z) \approx (x \cdot y) \cdot z]\!]_\tau$ pre $\tau = \{\cdot\}$ s $\alpha(\cdot) = 2$.

Príklad 2.6.7. Trieda všetkých monoidov $(M, \cdot, 1)$ je daná ako

$$[\![x \cdot (y \cdot z) \approx (x \cdot y) \cdot z,\ x \cdot 1 \approx x,\ 1 \cdot x \approx x]\!]_\tau$$

pre $\tau = \{\cdot, 1\}$ s $\alpha(\cdot) = 2$ a $\alpha(1) = 0$.

Príklad 2.6.8. Trieda všetkých grúp $(G, \cdot, {}^{-1}, 1)$ je daná ako

$$[\![x \cdot (y \cdot z) \approx (x \cdot y) \cdot z,\ x \cdot 1 \approx x,\ 1 \cdot x \approx x,\ x \cdot x^{-1} \approx 1,\ x^{-1} \cdot x \approx 1]\!]_\tau$$

pre $\tau = \{\cdot, {}^{-1}, 1\}$ s $\alpha(\cdot) = 2$, $\alpha({}^{-1}) = 1$ a $\alpha(1) = 0$.

Príklad 2.6.9. Trieda všetkých grupoidov $(X, \cdot)$ je daná ako $[\![\emptyset]\!]_\tau$ pre $\tau = \{\cdot\}$ s $\alpha(\cdot) = 2$.

Hovoríme, že identita $t_1 \approx t_2$ typu τ je *ekvivalentná* identite $t_1' \approx t_2'$, ak pre všetky algebry $\mathscr{A}$ typu τ je $\mathscr{A} \models t_1 \approx t_2$ práve vtedy, keď $\mathscr{A} \models t_1' \approx t_2'$. Špeciálnymi dvojicami ekvivalentných identít sú očividne tie, ktoré sa od seba líšia iba názvami jednotlivých premenných. Keďže navyše každý term – a tým pádom aj každá identita – obsahuje iba konečne veľa rôznych premenných, zisťujeme, že pre ľubovoľnú spočítateľne nekonečnú množinu premenných X spĺňajúcu $X \cap \tau = \emptyset$ existuje ku každej identite $t_1 \approx t_2$ typu τ s ňou ekvivalentná identita $t_1' \approx t_2' \in \mathscr{T}_\tau(X) \times \mathscr{T}_\tau(X)$.

[8] Častejšie sa identity zapisujú ako $t_1 = t_2$; v takom prípade ale treba pamätať na skutočnosť, že *nejde o rovnosť termov*, ale o rovnaké označenie inej relácie na termoch. Z tohto dôvodu budeme namiesto $=$ používať označenie $\approx$, pri ktorom nedorozumenia ohľadom významu hroziť nebudú.

Definícia 2.6.10. Nech $\mathcal{C}$ je trieda algebier typu τ a X je množina premenných taká, že $X \cap \tau = \emptyset$. Množinu všetkých identít nad X platných v $\mathcal{C}$ potom definujeme ako

$$\mathrm{Id}_X(\mathcal{C}) := \{t_1 \approx t_2 \in \mathscr{T}_\tau(X) \times \mathscr{T}_\tau(X) \mid \forall \mathscr{A} \in \mathcal{C} : \mathscr{A} \models t_1 \approx t_2\}.$$

Z vyššie uvedeného vyplýva, že množinu $\mathrm{Id}_X(\mathcal{C})$ budeme väčšinou uvažovať pre nejakú (hoci aj pevne danú) spočítateľne nekonečnú množinu X – v takom prípade totiž $\mathrm{Id}_X(\mathcal{C})$ obsahuje až na ekvivalenciu všetky identity splnené vo všetkých algebrách triedy $\mathcal{C}$.

Naším cieľom teraz bude postupne dospieť k Birkhoffovej vete, podľa ktorej sú varietami práve tie triedy algebier, ktoré sú opísateľné ako $[\![T]\!]$ pre nejakú množinu identít T nad nekonečnou množinou premenných X. Ako prvý krok smerom k tejto vete teraz dokážeme, že $[\![T]\!]$ je vždy varieta.

Lema 2.6.11. *Nech τ je typ, X je množina taká, že $X \cap \tau = \emptyset$ a $T \subseteq \mathscr{T}_\tau(X) \times \mathscr{T}_\tau(X)$ je množina identít typu τ nad množinou premenných X. Potom je trieda $[\![T]\!]$ varieta.*

Dôkaz. Potrebujeme dokázať uzavretosť triedy $[\![T]\!]$ na homomorfné obrazy, podalgebry a súčiny.

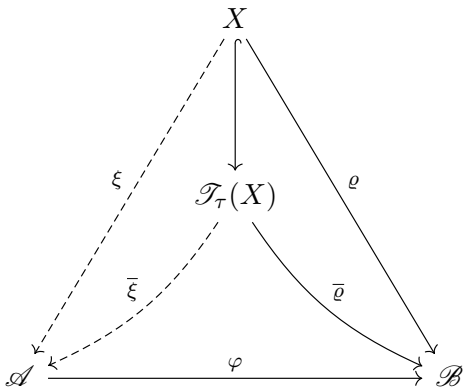
Uvažujme najprv ľubovoľnú algebru $\mathscr{A} \in [\![T]\!]$ – čiže algebru $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$ typu τ takú, že $\mathscr{A} \models T$ – a ľubovoľný surjektívny homomorfizmus $\varphi\colon \mathscr{A} \to \mathscr{B}$ algebier typu τ. Dokážeme, že v takom prípade musí byť aj algebra $\mathscr{B} = (B, (f^{\mathscr{B}})_{f\in\tau})$ v triede $[\![T]\!]$ – t. j. $\mathscr{B} \models T$. Na to stačí ukázať, že pre ľubovoľnú identitu $t_1 \approx t_2 \in \mathscr{T}_\tau(X) \times \mathscr{T}_\tau(X)$ je $\mathscr{B} \models t_1 \approx t_2$ kedykoľvek $\mathscr{A} \models t_1 \approx t_2$. Predpokladajme teda, že $\mathscr{A} \models t_1 \approx t_2$. Pre všetky zobrazenia $\psi\colon X \to A$ je potom $\overline{\psi}(t_1) = \overline{\psi}(t_2)$. Uvažujme ľubovoľné zobrazenie $\varrho\colon X \to B$; potrebujeme dokázať, že $\overline{\varrho}(t_1) = \overline{\varrho}(t_2)$. Zo surjektívnosti homomorfizmu φ ale vyplýva, že pre všetky $x \in X$ existuje $a \in A$ také, že $\varrho(x) = \varphi(a)$. Označme ľubovoľné takéto a ako $\xi(x)$, čím dostávame zobrazenie $\xi\colon X \to A$ také, že $\varrho = \varphi \circ \xi$. Teraz

$$\overline{\varrho} = \overline{\varphi \circ \xi} = \varphi \circ \overline{\xi},$$

pretože $\varphi\circ\overline{\xi}\colon \mathscr{T}_\tau(X) \to \mathscr{B}$ je homomorfizmus taký, že pre všetky $x \in X$ je $(\varphi\circ\overline{\xi})(x) = (\varphi\circ\xi)(x)$, avšak jediným takýmto homomorfizmom je podľa vety 2.4.4 homomorfizmus $\overline{\varphi \circ \xi}$. Keďže $\mathscr{A} \models t_1 \approx t_2$, je $\overline{\xi}(t_1) = \overline{\xi}(t_2)$. Zisťujeme teda, že

$$\overline{\varrho}(t_1) = \varphi(\overline{\xi}(t_1)) = \varphi(\overline{\xi}(t_2)) = \overline{\varrho}(t_2),$$

a to pre všetky zobrazenia $\varrho\colon X \to B$. Nutne teda $\mathscr{B} \models t_1 \approx t_2$ a uzavretosť triedy $[\![T]\!]$ na homomorfné obrazy je dokázaná.



Ak je $\mathscr{B} = (B, (f^{\mathscr{B}})_{f\in\tau})$ podalgebrou algebry $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$, v ktorej je splnená identita $t_1 \approx t_2$, musí byť táto identita splnená aj v $\mathscr{B}$: každé zobrazenie $\varrho\colon X \to B$ totiž jednoznačne určuje zobrazenie $\xi\colon X \to A$ také, že $\xi(x) = \varrho(x)$ pre všetky $x \in X$; pre všetky $t \in \mathscr{T}_\tau(X)$ potom evidentne aj $\overline{\xi}(t) = \overline{\varrho}(t)$. Ak teda $\mathscr{A} \models t_1 \approx t_2$, musí byť $\overline{\xi}(t_1) = \overline{\xi}(t_2)$, a teda aj

$$\overline{\varrho}(t_1) = \overline{\xi}(t_1) = \overline{\xi}(t_2) = \overline{\varrho}(t_2),$$

z čoho $\mathscr{B} \models t_1 \approx t_2$. Uzavretosť triedy $[\![T]\!]$ na podalgebry je dokázaná.

Zostáva dokázať uzavretosť triedy $[\![T]\!]$ na súčiny. Pre všetky i z nejakej množiny I vezmime algebru $\mathscr{A}_i = (A_i, (f^{\mathscr{A}_i})_{f\in\tau})$ typu τ takú, že $\mathscr{A}_i \models T$. Nech $\varrho\colon X \to \prod_{i\in I} A_i$ je dané ľubovoľne. Pre všetky $x \in X$ a $i \in I$ označme i-tu projekciu $\varrho(x)$ ako $\varrho_i(x)$. Pre všetky $t_1 \approx t_2 \in T$ potom

$$\overline{\varrho}(t_1) = (\overline{\varrho_i}(t_1) \mid i \in I) = (\overline{\varrho_i}(t_2) \mid i \in I) = \overline{\varrho}(t_2),$$

pretože $\mathscr{A}_i \models T$ pre všetky $i \in I$. To znamená, že

$$\prod_{i\in I} \mathscr{A}_i \models t_1 \approx t_2$$

a keďže je identita $t_1 \approx t_2 \in T$ ľubovoľná, je uzavretosť triedy $[\![T]\!]$ na súčiny dokázaná. □

Dokázali sme teda, že každá trieda algebier určená množinou identít je varieta. V nasledujúcom budeme dokazovať, že aj naopak každá varieta je určená nejakou množinou identít. Ako prvý krok k tomuto výsledku sa pozrieme na množinu všetkých identít $\mathrm{Id}_X(\mathcal{V})$ nad množinou premenných X, platných v nejakej variete algebier $\mathcal{V}$, ako na binárnu reláciu na $\mathscr{T}_\tau(X)$ – ňou totiž ako množina dvojíc termov z $\mathscr{T}_\tau(X)$ aj formálne je. Dokážeme teraz, že relácia $\mathrm{Id}_X(\mathcal{V})$ je kongruenciou na $\mathscr{T}_\tau(X)$.

Tvrdenie 2.6.12. *Nech $\mathcal{V}$ je ľubovoľná varieta algebier typu τ a X je množina premenných taká, že $X \cap \tau = \emptyset$. Potom je $\mathrm{Id}_X(\mathcal{V})$ kongruencia na algebre termov $\mathscr{T}_\tau(X)$. Navyše*

$$\mathrm{Id}_X(\mathcal{V}) = \bigcap_{\substack{\equiv \text{ je kongruencia na } \mathscr{T}_\tau(X).\\ \mathscr{T}_\tau(X)/\equiv \,\in \mathcal{V}}} \equiv.$$

Dôkaz. Keďže ľubovoľný prienik kongruencií je zrejme opäť kongruencia, stačí dokázať druhú časť tvrdenia. Uvažujme najprv ľubovoľnú identitu $t_1 \approx t_2 \in \mathrm{Id}_X(\mathcal{V})$. Pre ľubovoľnú kongruenciu $\equiv$ na $\mathscr{T}_\tau(X)$ spĺňajúcu $\mathscr{T}_\tau(X)/\equiv \in \mathcal{V}$ potom $t_1 \equiv t_2$, pretože prirodzená projekcia $\nu\colon \mathscr{T}_\tau(X) \to \mathscr{T}_\tau(X)/\equiv$ je homomorfizmus a $\mathscr{T}_\tau(X)/\equiv \models t_1 \approx t_2$ implikuje $\nu(t_1) = \nu(t_2)$, čo už je uvedenej skutočnosti ekvivalentné. Keďže je $\equiv$ ľubovoľná kongruencia taká, že $\mathscr{T}_\tau(X)/\equiv \in \mathcal{V}$, nutne aj

$$(t_1, t_2) \in \bigcap_{\substack{\equiv \text{ je kongruencia na } \mathscr{T}_\tau(X).\\ \mathscr{T}_\tau(X)/\equiv \,\in \mathcal{V}}} \equiv.$$

Predpokladajme naopak, že $t_1 \equiv t_2$ pre všetky kongruencie $\equiv$ na $\mathscr{T}_\tau(X)$ také, že $\mathscr{T}_\tau(X)/\equiv \in \mathcal{V}$. Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau}) \in \mathcal{V}$ je algebra $\varphi\colon X \to A$ je zobrazenie. Faktorová algebra $\mathscr{T}_\tau(X)/\ker\overline{\varphi}$ je potom podľa prvej vety o izomorfizme izomorfná podalgebre $\mathrm{im}\,\overline{\varphi}$ algebry $\mathscr{A}$. Keďže je teda $\mathcal{V}$ varieta a $\mathscr{A} \in \mathcal{V}$, musí byť aj $\mathscr{T}_\tau(X)/\ker\overline{\varphi} \in \mathcal{V}$, z čoho podľa nášho predpokladu vyplýva $(t_1, t_2) \in \ker\overline{\varphi}$, t. j. $\overline{\varphi}(t_1) = \overline{\varphi}(t_2)$. Keďže je zobrazenie $\varphi\colon X \to A$ ľubovoľné, zisťujeme, že $\mathscr{A} \models t_1 \approx t_2$; a keďže je ľubovoľná aj algebra $\mathscr{A} \in \mathcal{V}$, je $t_1 \approx t_2 \in \mathrm{Id}_X(\mathcal{V})$. □

Poznámka 2.6.13. V predchádzajúcom tvrdení je predpoklad, že $\mathcal{V}$ je varieta, zbytočne silný – využili sme totiž iba uzavretosť $\mathcal{V}$ na operátory **S** a **I**.

Faktorizácia algebry $\mathscr{T}_\tau(X)$ podľa kongruencie $\mathrm{Id}_X(\mathcal{V})$ intuitívne zodpovedá stotožneniu všetkých termov, ktoré možno jeden z druhého získať tak, že postupne nahradíme niekoľko ich podtermov „ekvivalentnými“ termami; „ekvivalencia“ termov t_1, t_2 tu pritom znamená, že pre nejaké zobrazenie $\varphi\colon X \to T_\tau(X)$ a identitu $t_1' \approx t_2' \in \mathrm{Id}_X(\mathcal{V})$ je $\overline{\varphi}(t_1') = t_1$ a $\overline{\varphi}(t_2') = t_2$, alebo naopak. Vzhľadom na to, že identita $t_1' \approx t_2'$ je splnená vo všetkých algebrách variety $\mathcal{V}$, nie je prekvapivé, že faktorová algebra $\mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{V})$ bude mať vlastnosť univerzálneho zobrazenia sformulovanú v nasledujúcom tvrdení.

Tvrdenie 2.6.14. *Nech $\mathcal{V}$ je ľubovoľná varieta algebier typu τ a X je množina premenných taká, že $X \cap \tau = \emptyset$. Pre ľubovoľnú algebru $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau}) \in \mathcal{V}$ a ľubovoľné zobrazenie $\varphi\colon X \to A$ potom existuje práve jeden homomorfizmus algebier $\hat{\varphi}\colon \mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{V}) \to \mathscr{A}$ taký, že pre všetky $x \in X$ je $\hat{\varphi}(\nu(x)) = \varphi(x)$, kde $\nu\colon \mathscr{T}_\tau(X) \to \mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{V})$ je prirodzená projekcia.*

Dôkaz. Podľa vety 2.4.4 možno zobrazenie $\varphi\colon X \to A$ rozšíriť na homomorfizmus $\overline{\varphi}\colon \mathscr{T}_\tau(X) \to \mathscr{A}$ taký, že pre všetky $x \in X$ je $\overline{\varphi}(x) = \varphi(x)$. Podľa prvej vety o izomorfizme je $\mathscr{T}_\tau(X)/\ker\overline{\varphi} \cong \operatorname{im}\overline{\varphi}$ a z uzavretosti variet na operátory $\mathbf{S}$ a $\mathbf{I}$ tak dostávame $\mathscr{T}_\tau(X)/\ker\overline{\varphi} \in \mathcal{V}$. Z tvrdenia 2.6.12 preto $\mathrm{Id}_X(\mathcal{V}) \subseteq \ker\overline{\varphi}$. Ak teda definujeme $\hat{\varphi}\colon T_\tau(X)/\mathrm{Id}_X(\mathcal{V}) \to A$ pre všetky $t \in T_\tau(X)$ ako

$$\hat{\varphi}\left([t]_{\mathrm{Id}_X(\mathcal{V})}\right) = \overline{\varphi}(t), \tag{2.2}$$

pôjde nielen o korektne definované zobrazenie, ale aj o homomorfizmus $\hat{\varphi}\colon \mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{V}) \to \mathscr{A}$, pretože pre všetky $f \in \tau$ a $t_1, \ldots, t_{\alpha(f)} \in \mathscr{T}_\tau(X)$ je

$$\begin{aligned}\hat{\varphi}\left(f^{\mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{V})}\left([t_1]_{\mathrm{Id}_X(\mathcal{V})}, \ldots, \left[t_{\alpha(f)}\right]_{\mathrm{Id}_X(\mathcal{V})}\right)\right) &= \hat{\varphi}\left(\left[f^{\mathscr{T}_\tau(X)}(t_1, \ldots, t_{\alpha(f)})\right]_{\mathrm{Id}_X(\mathcal{V})}\right) = \\ &= \overline{\varphi}\left(f^{\mathscr{T}_\tau(X)}(t_1, \ldots, t_{\alpha(f)})\right) = f^{\mathscr{A}}\left(\overline{\varphi}(t_1), \ldots, \overline{\varphi}(t_{\alpha(f)})\right) = \\ &= f^{\mathscr{A}}\left(\hat{\varphi}\left([t_1]_{\mathrm{Id}_X(\mathcal{V})}\right), \ldots, \hat{\varphi}\left(\left[t_{\alpha(f)}\right]_{\mathrm{Id}_X(\mathcal{V})}\right)\right).\end{aligned}$$

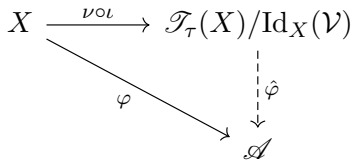
Platnosť rovnosti

$$\hat{\varphi}(\nu(x)) = \varphi(x)$$

pre všetky $x \in X$ je bezprostredným dôsledkom (2.2) a rovnosti $\overline{\varphi}(x) = \varphi(x)$ pre všetky $x \in X$.

Zostáva teda už len dokázať jedinečnosť homomorfizmu $\hat{\varphi}$. Štrukturálnou indukciou však ľahko dokážeme, že z požadovanej rovnosti $\hat{\varphi}(\nu(x)) = \varphi(x)$ pre všetky $x \in X$ vyplýva aj $\hat{\varphi}(\nu(t)) = \overline{\varphi}(t)$ pre všetky $t \in \mathscr{T}_\tau(X)$, čo už je len iným vyjadrením definície (2.2) homomorfizmu $\hat{\varphi}$. □

Práve dokázanú vlastnosť univerzálneho zobrazenia možno vyjadriť aj komutatívnosťou nasledujúceho diagramu, v ktorom $\iota\colon X \to \mathscr{T}_\tau(X)$ je vloženie X do $\mathscr{T}_\tau(X)$.



Algebra $\mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{V})$ sa pritom nazýva aj *(relatívne) voľnou $\mathcal{V}$-algebrou* alebo *algebrou voľnou vo $\mathcal{V}$*. Voľnými algebrami sa ešte budeme zaoberať podrobnejšie. Avšak uvedená terminológia už predpokladá platnosť nasledujúceho tvrdenia.

Tvrdenie 2.6.15. *Nech $\mathcal{V}$ je ľubovoľná varieta algebier typu τ a X je množina premenných taká, že $X \cap \tau = \emptyset$. Potom $\mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{V}) \in \mathcal{V}$.*

Dôkaz. Nech K je množina všetkých kongruencií $\equiv$ na $\mathscr{T}_\tau(X)$ takých, že $\mathscr{T}_\tau(X)/{\equiv} \in \mathcal{V}$. Vďaka tvrdeniu 2.6.12 potom pre všetky $(t_1, t_2) \in \mathrm{Id}_X(\mathcal{V})$ musí byť aj $t_1 \equiv t_2$ pre všetky $\equiv \in K$ a naopak ak $(t_1, t_2) \notin \mathrm{Id}_X(\mathcal{V})$, musí existovať kongruencia $\equiv \in K$ taká, že $t_1 \not\equiv t_2$. To znamená, že homomorfizmus

$$\psi\colon \mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{V}) \to \prod_{\equiv \in K} \mathscr{T}_\tau(X)/{\equiv},$$

daný pre všetky $t \in \mathscr{T}_\tau(X)$ ako

$$\psi\left([t]_{\mathrm{Id}_X(\mathcal{V})}\right) = \left([t]_\equiv \mid \equiv \in K\right),$$

je dobre definovaný a injektívny. Algebra $\mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{V})$ je teda izomorfná podalgebre súčinu algebier z $\mathcal{V}$, a teda musí aj sama patriť do $\mathcal{V}$. □

Lema 2.6.16. *Nech $\mathcal{V}$ je varieta algebier typu τ a X je nekonečná množina taká, že $X \cap \tau = \emptyset$. Potom $\mathcal{V} = [\![\mathrm{Id}_X(\mathcal{V})]\!]_\tau$.*

Dôkaz. Zrejme $\mathcal{V} \subseteq [\![\mathrm{Id}_X(\mathcal{V})]\!]$; zostáva teda už len dokázať opačnú inklúziu $\mathcal{V} \supseteq [\![\mathrm{Id}_X(\mathcal{V})]\!]$. Nech $\mathscr{A} \in [\![\mathrm{Id}_X(\mathcal{V})]\!]$. Vďaka nekonečnosti množiny X potom aj $\mathscr{A} \in [\![\mathrm{Id}_A(\mathcal{V})]\!]$, čiže $\mathscr{A} \models \mathrm{Id}_A(\mathcal{V})$. Špeciálne pre vyhodnocovací homomorfizmus $\mathrm{eval}_{\mathscr{A}} \colon \mathscr{T}_\tau(A) \to \mathscr{A}$ tak pre všetky $t_1 \approx t_2 \in \mathrm{Id}_A(\mathcal{V})$ dostávame $\mathrm{eval}_{\mathscr{A}}(t_1) = \mathrm{eval}_{\mathscr{A}}(t_2)$, z čoho $\mathrm{Id}_A(\mathcal{V}) \subseteq \ker \mathrm{eval}_{\mathscr{A}}$. Podobne ako v dôkaze tvrdenia 2.6.14 tak môžeme definovať homomorfizmus $\varphi \colon \mathscr{T}_\tau(A)/\mathrm{Id}_A(\mathcal{V}) \to \mathscr{A}$ predpisom $\varphi([t]_{\mathrm{Id}_A(\mathcal{V})}) = \mathrm{eval}_{\mathscr{A}}(t)$ pre všetky $t \in \mathscr{T}_\tau(A)$. Homomorfizmus φ je pritom surjektívny, pretože vyhodnocovací homomorfizmus $\mathrm{eval}_{\mathscr{A}}$ je surjektívny. To znamená, že $\mathscr{A}$ je homomorfným obrazom algebry $\mathscr{T}_\tau(A)/\mathrm{Id}_A(\mathcal{V})$. Avšak $\mathscr{T}_\tau(A)/\mathrm{Id}_A(\mathcal{V}) \in \mathcal{V}$ podľa tvrdenia 2.6.15 – preto $\mathscr{A} \in \mathcal{V}$ a lema je dokázaná. □

Môžeme pristúpiť k formulácii Birkhoffovej vety o varietach, vďaka vete 2.5.6 často nazývanej aj Birkhoffovou **HSP** vetou. Pôjde už pritom o bezprostredný dôsledok tvrdení dokázaných vyššie.

Veta 2.6.17 (Birkhoffova veta o varietach)**.** *Nech $\mathcal{C}$ je trieda algebier typu τ a X je nekonečná množina taká, že $X \cap \tau = \emptyset$. Potom je $\mathcal{C}$ varieta práve vtedy, keď existuje množina identít $T \subseteq \mathscr{T}_\tau(X) \times \mathscr{T}_\tau(X)$ taká, že $\mathcal{C} = [\![T]\!]_\tau$.*

Dôkaz. Ak je $\mathcal{C}$ varieta, podľa lemy 2.6.16 dostávame $\mathcal{C} = [\![\mathrm{Id}_X(\mathcal{C})]\!]_\tau$. Ak naopak $\mathcal{C} = [\![T]\!]$ pre nejakú množinu identít $T \subseteq \mathscr{T}_\tau(X) \times \mathscr{T}_\tau(X)$, musí byť $\mathcal{C}$ varieta podľa lemy 2.6.11. □

Príklad 2.6.18. Grupoidy, pologrupy, monoidy, grupy, polozväzy, polokruhy, okruhy, zväzy a vektorové priestory tvoria variety algebier svojho typu.

Príklad 2.6.19. Polia netvoria varietu algebier, pretože napríklad $\mathbb{R}$ je pole, ale $\mathbb{R} \times \mathbb{R}$ už pole nie je; trieda všetkých polí teda nie je uzavretá na súčiny.

Príklad 2.6.20. Pre ľubovoľný typ τ evidentne existuje práve jedna *triviálna varieta* $\mathcal{V} = [\![x \approx y]\!]$ pozostávajúca z práve všetkých triviálnych algebier typu τ a – v prípade, že typ τ neobsahuje žiaden nulárny operačný symbol – z prázdnej algebry typu τ. Zvyšné variety nazývame *netriviálnymi*.

2.7 Podvariety

Definícia 2.7.1. Nech $\mathcal{V}$ je varieta algebier typu τ. *Podvarietou* variety $\mathcal{V}$ nazveme ľubovoľnú varietu $\mathcal{W}$ algebier typu τ takú, že $\mathcal{W} \subseteq \mathcal{V}$.

Ak je $\mathcal{W}$ podvarieta variety $\mathcal{V}$, pre všetky množiny premenných X spĺňajúce $X \cap \tau = \emptyset$ je evidentne $\mathrm{Id}_X(\mathcal{V}) \subseteq \mathrm{Id}_X(\mathcal{W})$. Čitateľ pritom ľahko dokáže, že

$$\mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{W}) = \left(\mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{V})\right) / \left(\mathrm{Id}_X(\mathcal{W})/\mathrm{Id}_X(\mathcal{V})\right),$$

kde $\mathrm{Id}_X(\mathcal{W})/\mathrm{Id}_X(\mathcal{V}) = \{[t_1]_{\mathrm{Id}_X(\mathcal{V})} \approx [t_2]_{\mathrm{Id}_X(\mathcal{V})} \mid t_1 \approx t_2 \in \mathrm{Id}_X(\mathcal{W})\}$ – ide tu o špeciálny prípad tzv. *tretej vety o izomorfizme*. To znamená, že ak $\mathcal{V} = [\![T]\!]$ a $\mathcal{W} = [\![U]\!]$ pre nejaké množiny identít $U \supseteq T$, je varieta $\mathcal{W}$ ako podvarieta variety $\mathcal{V}$ jednoznačne určená obrazmi jednotlivých identít z U pri prirodzenej projekcii $\nu \colon \mathscr{T}_\tau(X) \to \mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{V})$. V mnohých prípadoch ako tento obraz dostaneme $[t]_{\mathrm{Id}_X(\mathcal{V})} \approx [t]_{\mathrm{Id}_X(\mathcal{V})}$ pre nejaký term $t \in \mathscr{T}_\tau(X)$. Takto sa teda dá – za predpokladu, že sa pohybujeme pod varietou $\mathcal{V}$ – množina identít potrebná na opis variety $\mathcal{W}$ podstatne zredukovať. Ak označíme výslednú množinu identít ako U', môžeme písať

$$\mathcal{W} = [\![U']\!]_{\mathcal{V}},$$

pričom v prípadoch, keď je z kontextu zrejmé, že sa pohybujeme pod varietou $\mathcal{V}$, budeme písať iba $\mathcal{W} = [\![U']\!]$. Namiesto o podvarietach variety $\mathcal{V}$ pritom často budeme hovoriť o *varietach $\mathcal{V}$-algebier*; ak špeciálne $\mathcal{V}$ pozostáva z algebier nejakého známeho typu, napr. zo všetkých pologrúp, monoidov, grúp, okruhov, atď., budeme hovoriť o podvarietach týchto variet ako o *varietach pologrúp, monoidov, grúp, okruhov, atď.*

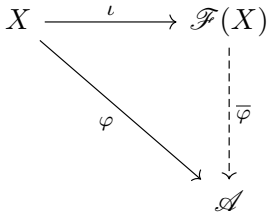
Príklad 2.7.2. Komutatívne pologrupy tvoria varietu pologrúp danú (vo variete všetkých pologrúp) ako $[\![xy \approx yx]\!]$. Ako varieta algebier typu (2) sú ale dané ako $[\![x(yz) \approx (xy)z, xy \approx yx]\!]$.

Príklad 2.7.3. Monoidy *netvoria* varietu pologrúp, pretože netvoria dokonca ani varietu typu (2). To je zrejmé napríklad z toho, že podpologrupa $(\mathbb{N} \setminus \{0\}, +)$ monoidu $(\mathbb{N}, +, 0)$ chápaného ako pologrupa $(\mathbb{N}, +)$, nie je monoid. Trieda všetkých monoidov chápaných ako pologrupy teda nie je uzavretá na podalgebry a tým pádom nemôže tvoriť varietu.

2.8 Voľné algebry

Bližšie sa teraz pozrime na pojem *voľnej algebry* v nejakej triede algebier $\mathcal{C}$. Pripomeňme si najprv jeho definíciu prostredníctvom vlastnosti univerzálneho zobrazenia.

Definícia 2.8.1. Nech $\mathcal{C}$ je trieda algebier typu τ a X je množina taká, že $X \cap \tau = \emptyset$. Hovoríme, že algebra $\mathscr{F}(X) \in \mathcal{C}$ je *voľná* v triede $\mathcal{C}$ nad množinou X vzhľadom na zobrazenie $\iota\colon X \to \mathscr{F}(X)$, ak pre ľubovoľnú algebru $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau}) \in \mathcal{C}$ a ľubovoľné zobrazenie $\varphi\colon X \to A$ existuje práve jeden homomorfizmus algebier $\overline{\varphi}\colon \mathscr{F}(X) \to \mathscr{A}$ taký, že pre všetky $x \in X$ je $\overline{\varphi}(\iota(x)) = \varphi(x)$.



Poznámka 2.8.2. V prípade, že trieda $\mathcal{C}$ obsahuje algebru s nosnou množinou kardinality aspoň $|X|$, musí byť pre každú algebru voľnú v $\mathcal{C}$ nad X príslušné zobrazenie $\iota\colon X \to \mathscr{F}(X)$ evidentne injektívne – t. j. musí ísť o *vloženie* X do $\mathscr{F}(X)$. To je okrem iného prípad algebier voľných v ľubovoľnej *netriviálnej* variete nad ľubovoľnou množinou X.

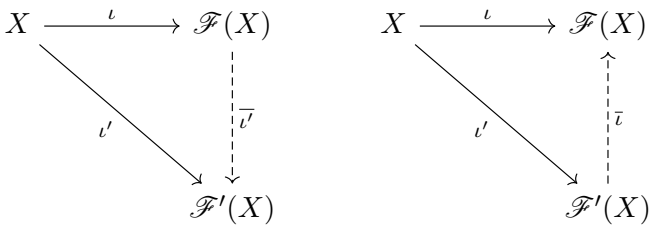
Z oddielu 2.6 vieme, že v každej *variete* algebier $\mathcal{V}$ existuje nad každou množinou X spĺňajúcou $X \cap \tau = \emptyset$ voľná algebra $\mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{V})$. To vysvetľuje pojem „voľná“ algebra: rovnosti medzi jej prvkami sú výhradne dôsledkami identít, ktoré musia platiť v ktorejkoľvek algebre z $\mathcal{V}$; prvky tak nie sú viazané žiadnymi ďalšími „zbytočnými“ rovnosťami.

Na rozdiel od variet nemusí každá *trieda* algebier obsahovať voľnú algebru. Dokážeme teraz, že kedykoľvek v nejakej triede voľná algebra nad X existuje, je táto daná jednoznačne až na izomorfizmus. Vďaka tomu nie je potrebné v súvislosti s voľnými algebrami explicitne uvádzať zobrazenie ι.

Tvrdenie 2.8.3. *Nech $\mathcal{C}$ je trieda algebier typu τ a X je ľubovoľná množina taká, že $X \cap \tau = \emptyset$. Až na izomorfizmus potom v $\mathcal{C}$ existuje najviac jedna voľná algebra $\mathscr{F}(X)$ nad množinou X.*

Dôkaz. Uvažujme ľubovoľnú dvojicu voľných algebier $\mathscr{F}(X), \mathscr{F}'(X)$ v triede $\mathcal{C}$ nad množinou X, kde $\mathscr{F}(X)$ je voľná vzhľadom na $\iota\colon X \to \mathscr{F}(X)$ a $\mathscr{F}'(X)$ je voľná vzhľadom na $\iota'\colon X \to \mathscr{F}'(X)$. Skonštruujeme izomorfizmus medzi $\mathscr{F}(X)$ a $\mathscr{F}'(X)$.

Z definície voľných algebier vyplýva, že k zobrazeniam ι a ι' možno uvažovať homomorfizmy $\overline{\iota'}\colon \mathscr{F}(X) \to \mathscr{F}'(X)$ a $\overline{\iota}\colon \mathscr{F}'(X) \to \mathscr{F}(X)$ také, že komutujú nasledujúce diagramy.

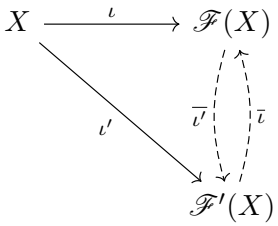


Teraz $\bar{\iota} \circ \overline{\iota'} \circ \iota = \bar{\iota} \circ \iota' = \iota$, z čoho vďaka jednoznačnosti homomorfizmu $\tilde{\iota}\colon \mathscr{F}(X) \to \mathscr{F}(X)$ spĺňajúceho $\tilde{\iota}(\iota(x)) = \iota(x)$ pre všetky $x \in X$ dostávame

$$\bar{\iota} \circ \overline{\iota'} = \mathrm{id}_{\mathscr{F}(X)} \tag{2.3}$$

a $\overline{\iota'} \circ \bar{\iota} \circ \iota' = \overline{\iota'} \circ \iota = \iota'$, z čoho vďaka jednoznačnosti homomorfizmu $\tilde{\iota'}\colon \mathscr{F}'(X) \to \mathscr{F}'(X)$ spĺňajúceho $\tilde{\iota'}(\iota'(x)) = \iota'(x)$ pre všetky $x \in X$ dostávame

$$\overline{\iota'} \circ \bar{\iota} = \mathrm{id}_{\mathscr{F}'(X)}. \tag{2.4}$$



Z rovností (2.3) a (2.4) bezprostredne vyplýva, že $\bar{\iota}$ a $\overline{\iota'}$ sú vzájomne inverzné bijekcie; keďže súčasne ide o homomorfizmy, je $\overline{\iota'}$ hľadaným izomorfizmom z $\mathscr{F}(X)$ do $\mathscr{F}'(X)$. □

Dokážeme teraz, že *vo variete* je voľná algebra $\mathscr{F}(X)$ nad množinou X vždy generovaná obrazmi prvkov X pri uvažovanom zobrazení z X do $\mathscr{F}(X)$, ktoré často stotožňujeme priamo s prvkami X.[9] To vysvetľuje, prečo sa často hovorí aj o *voľnej algebre nad množinou generátorov* X.

Tvrdenie 2.8.4. *Nech $\mathcal{V}$ je varieta algebier typu τ a X je množina taká, že $X \cap \tau = \emptyset$. Voľná algebra $\mathscr{F}(X)$ vo $\mathcal{V}$ vzhľadom na zobrazenie $\iota\colon X \to \mathscr{F}(X)$ je potom generovaná množinou $\iota(X)$.*

Dôkaz. Pre voľnú algebru vzhľadom na zobrazenie ι musí platiť $\mathscr{F}(X) \cong \mathscr{T}_\tau(\iota(X))/\mathrm{Id}_{\iota(X)}(\mathcal{V})$, pričom izomorfizmus zobrazuje $\iota(x)$ na $[\iota(x)]_{\mathrm{Id}_{\iota(X)}(\mathcal{V})}$. Keďže je množinou $\iota(X)$ generovaná algebra $\mathscr{T}_\tau(\iota(X))$, je zrejmé, že jej faktorová algebra $\mathscr{T}_\tau(\iota(X))/\mathrm{Id}_{\iota(X)}(\mathcal{V})$ musí byť generovaná množinou $\nu(\iota(X))$, kde $\nu\colon \mathscr{T}_\tau(\iota(X)) \to \mathscr{T}_\tau(\iota(X))/\mathrm{Id}_{\iota(X)}(\mathcal{V})$ je prirodzená projekcia. Tým pádom musí byť množinou $\iota(X)$ generovaná aj algebra $\mathscr{F}(X)$. □

2.9 Príklady voľných algebier

Uveďme si teraz niekoľko dôležitých príkladov voľných algebier vo varietach. Užitočným cvičením môže byť pre každú z nich dokázať, že skutočne má vlastnosť univerzálneho zobrazenia v príslušnej variete. V nasledujúcom už pre identity namiesto notácie $t_1 \approx t_2$ používame obvyklejšiu notáciu $t_1 = t_2$.

Príklad 2.9.1. Pre všetky prípustné množiny X je *voľným monoidom* nad X monoid $(X^*, \cdot, \varepsilon)$ všetkých slov nad abecedou X, ktorá však môže byť aj prázdna alebo nekonečná. Vieme už totiž, že pre $\tau = \{\cdot, 1\}$ s $\alpha(\cdot) = 2$ a $\alpha(1) = 0$ musí ísť o algebru $\mathscr{T}_\tau(X)/\mathrm{Id}_X([\![x(yz) = (xy)z, x1 = x, 1x = x]\!])$. To ale znamená, že v termoch typu τ nad X stotožníme všetky podtermy typu $t_1(t_2t_3)$ s $(t_1t_2)t_3$ a všetky podtermy typu $t1$ alebo $1t$ s t. Zostanú nám tak iba neprázdne slová zložené z premenných množiny X a neutrálny prvok 1, ktorý môžeme označiť aj ako ε. Pre $X = \emptyset$ obsahuje voľný monoid nad X iba prázdne slovo ε a pre jednoprvkovú množinu X je izomorfný s monoidom $(\mathbb{N}, +, 0)$.

Príklad 2.9.2. Pre všetky prípustné množiny X je *voľná pologrupa* nad X daná ako $(X^+, \cdot)$, teda ako pologrupa všetkých neprázdnych slov nad X. Musí totiž ísť o algebru $\mathscr{T}_\tau(X)/\mathrm{Id}_X([\![x(yz) = (xy)z]\!])$ pre $\tau = \{\cdot\}$ s $\alpha(\cdot) = 2$, pričom po stotožnení všetkých termov typu $t_1(t_2t_3)$ s $(t_1t_2)t_3$ nám zostanú iba neprázdne slová nad množinou X. Voľná pologrupa nad $\emptyset$ je prázdna a nad jednoprvkovým X je izomorfná s $(\mathbb{N} \setminus \{0\}, +)$.

[9] To znamená, že keď vezmeme podalgebru $\mathscr{F}(X)$ generovanú týmito prvkami, dostaneme kompletnú algebru $\mathscr{F}(X)$.

Príklad 2.9.3. *Voľný grupoid* nad X je jednoducho algebra termov $\mathscr{T}_\tau(X)$ pre $\tau = \{\cdot\}$ s $\alpha(\cdot) = 2$. Ide teda o grupoid všetkých „plne uzátvorkovaných“ neprázdnych slov nad abecedou X. Tie možno interpretovať aj ako binárne stromy, ktorých listy zodpovedajú premenným z X a ktorých vnútorné vrcholy zodpovedajú jednotlivým aplikáciám binárnej operácie $\cdot$. Voľný grupoid nad $\emptyset$ je prázdny a nad jednoprvkovou množinou ho možno chápať ako grupoid všetkých binárnych stromov s jediným druhom listov.

Príklad 2.9.4. *Voľný komutatívny monoid* dostaneme z voľného monoidu tak, že stotožníme všetky slová typu uv a vu. To znamená, že poradie jednotlivých písmen v slovách prestane byť dôležité a jedinou podstatnou vlastnosťou sa stane počet výskytov jednotlivých písmen v danom slove. Ako taký je voľný komutatívny monoid X izomorfný monoidu $(\mathbb{N}^X, +, \mathbf{0})$ a pre konečné množiny X s $|X| = k$ monoidu $(\mathbb{N}^k, +, \mathbf{0})$.

Príklad 2.9.5. Opis *voľnej grupy* je o niečo komplikovanejší, než tomu bolo v predchádzajúcich príkladoch. Grupy sú algebrami typu $(2, 1, 0)$ resp. $\tau = \{\cdot, {}^{-1}, 1\}$ s $\alpha(\cdot) = 2$, $\alpha({}^{-1}) = 1$ a $\alpha(1) = 0$. Uvažujme ľubovoľnú množinu X spĺňajúcu $X \cap \tau = \emptyset$, ktorú môžeme chápať ako (vo všeobecnosti aj prázdnu alebo nekonečnú) abecedu. Položme $X^{-1} := \{a^{-1} \mid a \in X\}$ a bez ujmy na všeobecnosti predpokladajme, že $X \cap X^{-1} = \emptyset$. Pre dvojicu slov $u, v \in (X \cup X^{-1})^*$ položíme $u \to v$, ak existujú slová $x, y \in (X \cup X^{-1})^*$ a $a \in X$ také, že $u = xaa^{-1}y$ a $v = xy$, alebo $u = xa^{-1}ay$ a $v = xy$. Slovo $x \in (X \cup X^{-1})^*$ nazveme *redukovaným*, ak neexistuje žiadne slovo x' také, že $x \to x'$.

Je teraz potrebné dokázať, že ak $u \to^* v_1$ a $u \to^* v_2$, kde v_1 a v_2 sú redukované slová, tak $v_1 = v_2$. To vyplýva z nasledujúcej vlastnosti konfluencie: ak $x \to y_1$ a $x \to y_2$, tak existuje z také, že $y_1 \to^* z$ a $y_2 \to^* z$ (kde hviezdičku by sme skutočnosti vždy mohli nahradiť jednotkou alebo nulou). Táto vlastnosť platí preto, lebo existujú iba dve možnosti, ako môžu elementárne redukcie $x \to y_1$ a $x \to y_2$ vyzerať: buď ide o redukcie „neprekrývajúcich sa dvojíc“ a v takom prípade možno po jednej vzápätí vykonať tú druhú, alebo sa redukované dvojice prekrývajú (či už na jednom alebo obidvoch písmenách) a v takom prípade $y_1 = y_2$. Tvrdenie o jednoznačnosti redukovaného slova potom možno dokázať indukciou vzhľadom na $|u|$. Pre $u = \varepsilon$ tvrdenie evidentne platí; ak je teraz slovo u neprázdne a $u \to u_1 \to^* v_1$, $u \to u_2 \to^* v_2$, sú slová u_1 a u_2 kratšie ako u a vzťahuje sa na ne indukčný predpoklad znamenajúci, že všetky redukované slová, ktoré možno získať z u_1, si sú navzájom rovné a podobne pre u_2. Vďaka vlastnosti konfluencie ale existuje z také, že $u_1 \to^* z$ a $u_2 \to^* z$ a všetky redukované slová, ktoré možno získať či už z u_1 alebo z u_2 tak musia byť rovné redukovanému slovu, ktoré možno získať zo z. Ak slová u_1, u_2 ako vyššie neexistujú, musí byť redukovaným samotné slovo u.

Označme pre všetky $x \in (X \cup X^{-1})^*$ ako $\varrho(x)$ redukované slovo také, že $x \to^* \varrho(x)$. Voľnú grupu F_X nad množinou X potom možno opísať ako množinu $\{\varrho(x) \mid x \in (X \cup X^{-1})^*\}$ s nasledujúcimi operáciami: $\varrho(x)\varrho(y) = \varrho(xy)$ pre všetky $x, y \in (X \cup X^{-1})^*$ a ak

$$\varrho(x) = a_1^{e_1} \dots a_n^{e_n}$$

pre $a_1, \dots, a_n \in X$ a $e_1, \dots, e_n \in \{1, -1\}$, tak

$$\varrho(x)^{-1} = a_n^{-e_n} \dots a_1^{-e_1}.$$

Binárna operácia je dobre definovaná – ak totiž $\varrho(x) = \varrho(x')$ a $\varrho(y) = \varrho(y')$, tak $\varrho(xy) = \varrho(x'y')$, lebo

$$xy \to^* \varrho(x)\varrho(y) = \varrho(x')\varrho(y') \leftarrow^* x'y'$$

a teda

$$\varrho(xy) = \varrho(\varrho(x)\varrho(y)) = \varrho(\varrho(x')\varrho(y')) = \varrho(x'y').$$

Z predpisu $\varrho(x)\varrho(y) = \varrho(xy)$ je potom evidentná asociatívnosť binárnej operácie. Neutrálnosť prázdneho slova je evidentná a rovnako evidentná je aj skutočnosť, že $\varrho(x)^{-1}$ je pre všetky $x \in (X \cup X^{-1})^*$ dobre definované, pričom $\varrho(x)\varrho(x)^{-1} = \varrho(x)^{-1}\varrho(x) = \varepsilon$.

Dôkaz vlastnosti univerzálneho zobrazenia voľnej grupy prenechávame čitateľovi ako cvičenie.

Príklad 2.9.6. *Voľnú komutatívnu grupu* nad X získame z voľnej grupy F_X stotožnením všetkých redukovaných slov $\varrho(x)$ a $\varrho(y)$ pre $x, y \in (X \cup X^{-1})^*$ líšiace sa iba v poradí písmen z $X \cup X^{-1}$. Z každého redukovaného slova z F_X pritom možno permutáciou jeho písmen získať slovo $a_1^{e_1} a_1^{-e'_1} a_2^{e_2} a_2^{-e'_2} \dots a_n^{e_n} a_n^{-e'_n}$ pre nejaké $a_1, \dots, a_n \in X$ a $e_1, \dots, e_n, e'_1, \dots, e'_n \in \mathbb{N}$; redukované slovo prislúchajúce k tomuto slovu je teda dané ako $a_1^{e_1 - e'_1} a_2^{e_2 - e'_2} \dots a_n^{e_n - e'_n}$. Jediné, na čom teda vo výsledku záleží, je pre každé $a \in X$ rozdiel počtu výskytov písmena a a počtu výskytu písmena a^{-1}. Skrz izomorfizmus teda zisťujeme, že voľnou komutatívnou grupou nad X je $(\mathbb{Z}^X, +, \mathbf{0})$, pričom pre konečné X s $|X| = k$ ide o grupu $(\mathbb{Z}^k, +, \mathbf{0})$.

Príklad 2.9.7. *Voľný polokruh* nad X z algebry termov $\mathscr{T}_{(2,2,0,0)}(X) = (T_{(2,2,0,0)}(X), +, \cdot, 0, 1)$ získame stotožnením všetkých dvojíc termov, ktoré po dosadení vhodných podtermov za premenné tvoria ľavú a pravú stranu niektorej polokruhovej identity. Vďaka distributívnosti môžeme uvažovať iba súčty súčinov prvkov $X \cup \{0, 1\}$ (každú zátvorku vieme roznásobiť). Vďaka multiplikatívnej štruktúre polokruhu možno chápať súčiny prvkov $X \cup \{0, 1\}$ ako prvky $X^* \cup \{0\}$ a vďaka jeho aditívnej štruktúre sú súčty súčinov prvkov $X \cup \{0, 1\}$ dané iba počtom výskytov každého zo slov v X^* ako členu v súčte. Zisťujeme teda, že voľným polokruhom nad X je polokruh nekomutatívnych polynómov $\mathbb{N}\langle X^* \rangle$.

Príklad 2.9.8. *Voľný okruh* nad X vznikne z voľného polokruhu pridaním aditívnych inverzných prvkov a stotožnením všetkých polynómov typu $w + (-w)$ a $(-w) + w$ pre nejaké $w \in X^*$ s 0. Voľným okruhom je teda okruh nekomutatívnych polynómov $\mathbb{Z}\langle X^* \rangle$.

Príklad 2.9.9. Vo *voľnom komutatívnom okruhu* navyše stotožníme tie slová $w \in X^*$, ktoré sa líšia iba v poradí jednotlivých písmen. Zisťujeme teda, že voľným komutatívnym okruhom je okruh všetkých komutatívnych polynómov o premenných z X a s koeficientmi v $\mathbb{Z}$. Pre konečnú množinu $X = \{x_1, \dots, x_k\}$ je teda voľným komutatívnym okruhom nad X bežný okruh polynómov $\mathbb{Z}[x_1, \dots, x_k]$.

Príklad 2.9.10. Zrejme existujú iba dve variety typu $\tau = \emptyset$ – varieta všetkých množín $[\![\emptyset]\!]$ a triviálna varieta najviac jednoprvkových množín $[\![x = y]\!]$. Ľahko pritom vidieť, že vo variete všetkých množín $[\![\emptyset]\!]$ sú nad ľubovoľnou množinou X voľné práve všetky množiny kardinality $|X|$.

Príklad 2.9.11. *Voľné pole* – čiže voľná algebra v triede všetkých polí – *neexistuje*. Keby totiž pre nejaké X takéto pole $\mathbb{F}(X) = (\mathbb{F}(X), +, \cdot, 0_{\mathbb{F}(X)}, 1_{\mathbb{F}(X)})$ existovalo, musel by pre každé iné pole $\mathbb{K} = (\mathbb{K}, +, \cdot, 0_{\mathbb{K}}, 1_{\mathbb{K}})$ existovať homomorfizmus $\varphi\colon \mathbb{F}(X) \to \mathbb{K}$. To ale nie je možné, pretože homomorfizmy polí zachovávajú charakteristiku poľa. Skutočne: keby bola charakteristika poľa $\mathbb{F}(X)$ rovná $p \in \mathbb{N} \setminus \{0\}$, bolo by $p \cdot 1_{\mathbb{F}(X)} = 0_{\mathbb{F}(X)}$, a teda aj $p \cdot 1_{\mathbb{K}} = p \cdot \varphi(1_{\mathbb{F}(X)}) = \varphi(p \cdot 1_{\mathbb{F}(X)}) = \varphi(0_{\mathbb{F}(X)}) = 0_{\mathbb{K}}$, takže charakteristika poľa $\mathbb{K}$ by určite delila p; keďže je charakteristika poľa navyše vždy prvočíselná, bola by nutne rovná p. Keby bola charakteristika poľa $\mathbb{F}(X)$ nulová, bolo by $s \cdot 1_{\mathbb{F}(X)} \neq 0_{\mathbb{F}(X)}$ pre všetky $s \in \mathbb{N} \setminus \{0\}$, a teda aj $s \cdot 1_{\mathbb{K}} = s \cdot \varphi(1_{\mathbb{F}(X)}) = \varphi(s \cdot 1_{\mathbb{F}(X)}) \neq 0_{\mathbb{K}}$, pretože homomorfizmy polí zobrazujú nenulové prvky na nenulové. Charakteristika poľa $\mathbb{K}$ by teda tiež bola nulová.

Voľné pole teda skutočne neexistuje, čo možno vďaka tvrdeniu 2.6.15 chápať aj ako alternatívny dôkaz skutočnosti, že trieda všetkých polí *netvorí* varietu algebier.

2.10 Prezentácie algebier

Nech $\mathcal{V}$ je varieta algebier typu τ. Pre všetky množiny X spĺňajúce $X \cap \tau = \emptyset$ potom $\mathcal{V}$ obsahuje voľnú algebru $\mathscr{F}(X) = \mathscr{T}_\tau(X)/\mathrm{Id}_X(\mathcal{V})$. Pod *prezentáciou* $\mathcal{V}$-algebry $\mathscr{A}$ budeme v princípe rozumieť jej zadanie v podobe faktorovej algebry voľnej algebry $\mathscr{F}(X)$ podľa nejakej kongruencie $\equiv$; avšak s tým, že stačí zadať množinu generátorov X a ľubovoľnú binárnu reláciu $R \subseteq \mathscr{F}(X) \times \mathscr{F}(X)$ generujúcu kongruenciu $\equiv$. *Prezentáciou* $\mathcal{V}$-algebry $\mathscr{A}$ teda rozumieme ľubovoľný zápis tvaru

$$\mathscr{A} = \langle X \mid R \rangle$$

vyjadrujúci, že

$$\mathscr{A} = \mathscr{F}(X)/\langle R\rangle_{\mathscr{F}(X)}.$$

Pri použití tejto notácie je potrebné, aby bolo z kontextu zrejmé, pod ktorou varietou $\mathcal{V}$ sa pohybujeme. Jedna prezentácia môže v rôznych varietach zjavne opisovať rôzne algebry. Prvky (x, y) relácie R budeme obyčajne zapisovať ako rovnosti $x = y$; podobne ako pri identitách ale treba mať na pamäti, že nejde o bežnú reláciu rovnosti na $\mathscr{F}(X)$.

Nasledujúce jednoduché tvrdenie hovorí, že každú algebru je v princípe možné zadať prezentáciou.

Tvrdenie 2.10.1. *Nech $\mathcal{V}$ je varieta algebier typu τ obsahujúca pre všetky množiny X spĺňajúce $X \cap \tau = \emptyset$ voľnú algebru $\mathscr{F}(X)$. Nech $\mathscr{A} \in \mathcal{V}$ je algebra. Potom existuje množina X spĺňajúca $X \cap \tau = \emptyset$ a binárna relácia $R \subseteq \mathscr{F}(X) \times \mathscr{F}(X)$ taká, že*

$$\mathscr{A} \cong \langle X \mid R\rangle.$$

Dôkaz. Nech $\mathscr{A} = (A, (f^{\mathscr{A}})_{f\in\tau})$. Zvoľme $X = A$ a

$$R = \left\{ f(a_1, \ldots, a_{\alpha(f)}) = a \;\middle|\; f \in \tau;\ a, a_1, \ldots, a_{\alpha(f)} \in A;\ f^{\mathscr{A}}(a_1, \ldots, a_{\alpha(f)}) = a \right\}.$$

Ľahko vidieť, že $\mathscr{F}(A)/\langle R\rangle_{\mathscr{F}(A)} \cong \mathscr{A}$. □

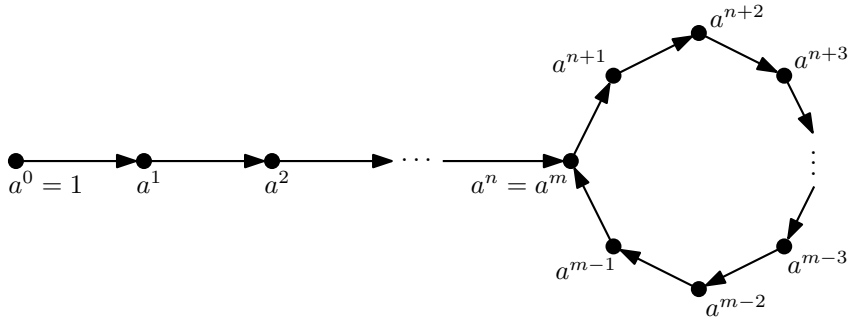
Prezentácia použitá v dôkaze uvedeného tvrdenia samozrejme nemá vôbec žiaden praktický význam, keďže algebru $\mathscr{A}$ opisujeme pomocou nej samotnej. Užitočné sú predovšetkým *konečné prezentácie* algebier – čiže prezentácie, v ktorých je konečná ako množina generátorov X, tak aj relácia R; algebry, ktoré možno zadať konečnou prezentáciou, nazývame aj *konečne prezentovateľnými*. Ak je v takom prípade $X = \{a_1, \ldots, a_n\}$ a $R = \{x_1 = y_1, \ldots, x_m = y_m\}$, píšeme prezentáciu väčšinou v podobe

$$\mathscr{A} = \langle a_1, \ldots, a_n \mid x_1 = y_1, \ldots, x_m = y_m\rangle.$$

Najčastejšie sa prezentáciami zadávajú grupy, monoidy a pologrupy. V nasledujúcom sa teda bližšie zameriame na prípad monoidov. Začnime niekoľkými jednoduchými príkladmi. Ak budeme hovoriť, že je nejaký monoid zadaný nejakou prezentáciou, budeme mať väčšinou na mysli „až na izomorfizmus“.

Príklad 2.10.2. Prezentácia $\langle a \mid a^n = 1\rangle$ zadáva monoid $\mathbb{Z}_n$, ktorý je súčasne aj cyklickou grupou.

Príklad 2.10.3. Prezentácia $\langle a \mid a^n = a^m\rangle$ pre $n < m$ zadáva monoid znázornený na obrázku 2.3.



Obr. 2.3: Monoid $\langle a \mid a^n = a^m\rangle$. Šípky znázorňujú násobenie prvkom a.

Príklad 2.10.4. Prezentácia $\langle a, b \mid ab = ba\rangle$ zadáva voľný komutatívny monoid $(\mathbb{N}^2, +, \mathbf{0})$.

Príklad 2.10.5. Prezentácia $\langle a, b, c \mid ab = ba\rangle$ zadáva monoid „slov“ nad abecedou $\{a, b, c\}$, v ktorých navzájom komutujú písmená a a b. Takéto „čiastočne komutatívne slová“ sa zvyknú nazývať aj *stopy*.

Ukážeme teraz, že prezentácie monoidov sú v princípe ekvivalentné prepisovacím systémom nazývaným aj *polothueovskými* (angl. *semi-Thue systems*). Ide o dvojice (X, R), kde X je ľubovoľná množina neobsahujúca $\cdot$ a 1 (chápaná ako abeceda, ktorá ale môže byť aj nekonečná alebo prázdna) a $R \subseteq X^* \times X^*$ je nejaká binárna relácia na slovách nad X. Pre $u, v \in X^*$ potom píšeme $u \to_R v$ – prípadne iba $u \to v$ – ak existuje $(x, y) \in R$ a slová $u_1, u_2 \in X^*$ také, že $u = u_1 x u_2$ a $v = u_1 y u_2$. Prvky R nazývame *prepisovacími pravidlami* a reláciu $\to$ reláciou *kroku odvodenia*.

Ak označíme $\overset{*}{\longleftrightarrow}$ reflexívno-tranzitívno-symetrický uzáver binárnej relácie $\to$ na X^*, evidentne dostávame kongruenciu generovanú reláciou R. Pri prezentácii $\langle X \mid R \rangle$ teda stotožňujeme práve všetky dvojice slov u, v také, že v polothueovskom prepisovacom systéme (X, R) je $u \overset{*}{\longleftrightarrow} v$.

Definícia 2.10.6. Polothueovský prepisovací systém (X, R) nazveme:

a) *Konfluentným*, ak pre všetky $x, u, v \in X^*$ spĺňajúce $x \to^* u$ a $x \to^* v$ existuje $z \in X^*$ také, že $u \to^* z$ a $v \to^* z$.

b) *Lokálne konfluentným*, ak pre všetky $x, u, v \in X^*$ spĺňajúce $x \to u$ a $x \to v$ existuje $z \in X^*$ také, že $u \to^* z$ a $v \to^* z$.

c) Majúcim *Churchovu-Rosserovu vlastnosť*, ak pre všetky $u, v \in X^*$ spĺňajúce $u \overset{*}{\longleftrightarrow} v$ existuje $x \in X^*$ také, že $u \to^* x$ a $v \to^* x$.

d) *Terminujúcim*, ak neexistuje žiadna nekonečná postupnosť slov $x_1, x_2, x_3, \ldots$ nad abecedou X takých, že $x_1 \to x_2 \to x_3 \to \ldots$

Tvrdenie 2.10.7. *Polothueovský prepisovací systém (X, R) je konfluentný práve vtedy, keď má tento systém Churchovu-Rosserovu vlastnosť.*

Dôkaz. Predpokladajme najprv, že je systém (X, R) konfluentný. Pre všetky $u, v \in X^*$ spĺňajúce $u \overset{*}{\longleftrightarrow} v$ existuje $n \in \mathbb{N}$ také, že $u \overset{n}{\longleftrightarrow} v$. Indukciou vzhľadom na n dokážeme existenciu $x \in X^*$ takého, že $u \to^* x$ a $v \to^* x$. Ak $n = 0$, nutne $u = v$ a možno vziať napríklad $x = u = v$. Predpokladajme teraz, že tvrdenie platí pre $n = k$ a uvažujme $n = k + 1$. Ak $u \overset{k+1}{\longleftrightarrow} v$, tak existuje $w \in X^*$ také, že buď $u \overset{k}{\longleftrightarrow} w \to v$, alebo $u \overset{k}{\longleftrightarrow} w \leftarrow v$. V oboch prípadoch existuje vďaka indukčnému predpokladu $y \in X^*$ také, že $u \to^* y$ a $w \to^* y$. Ak pritom $u \overset{k}{\longleftrightarrow} w \to v$, existuje vďaka konfluencii $x \in X^*$ také, že $u \to^* y \to^* x$ a $v \to^* x$. Ak $u \overset{k}{\longleftrightarrow} w \leftarrow v$, máme priamo $u \to^* y$ aj $v \to^* y$.

Ak má naopak prepisovací systém (X, R) Churchovu-Rosserovu vlastnosť, musí byť aj konfluentný, pretože zjavne $u \overset{*}{\longleftrightarrow} v$ kedykoľvek súčasne $x \to^* u$ a $x \to^* v$. □

Je teda zrejmé, že pokiaľ je polothueovský systém súčasne konfluentný – to jest má Churchovu-Rosserovu vlastnosť – a terminujúci,[10] existuje pre každú triedu $C \in X^*/\overset{*}{\longleftrightarrow}$ kongruencie $\overset{*}{\longleftrightarrow}$ práve jedna „normálna forma“, čiže práve jedno slovo $w \in X^*$ také, že $u \to^* w$ pre všetky $u \in C$. Prepisovací systém, ktorý sme použili pri konštrukcii voľnej grupy, mal evidentne tieto vlastnosti. Vyššie sme pritom dokázali, že kedykoľvek zodpovedá prezentácii monoidu konfluentný a súčasne terminujúci polothueovský systém, možno tento monoid ekvivalentne opísať aj ako monoid „normálnych foriem“ tried kongruencie $\overset{*}{\longleftrightarrow}$.

Vlastnosť konfluencie však vo všeobecnosti nepatrí k ľahko overiteľným. Zíde sa preto nasledujúca charakterizácia *terminujúcich* konfluentných systémov.

[10] Takéto prepisovacie systémy sa niekedy nazývajú aj *konvergentnými*.

Tvrdenie 2.10.8. *Nech (X, R) je terminujúci polothueovský systém. Potom je systém (X, R) konfluentný práve vtedy, keď je lokálne konfluentný.*

Dôkaz. Každý konfluentný systém je priamo z definície súčasne aj lokálne konfluentný. Zostáva teda dokázať, že terminujúci lokálne konfluentný polothueovský systém je konfluentný. Nech je teda systém terminujúci a lokálne konfluentný a za účelom sporu predpokladajme, že nie je konfluentný. Potom existujú $x, u, v \in X^*$ také, že $x \to^* u$, $x \to^* v$ a súčasne neexistuje žiadne $z \in X^*$ také, že zároveň $u \to^* z$ a $v \to^* z$. Keďže je systém terminujúci, môžeme navyše predpokladať, že pre všetky $w \in X^*$ také, že $x \to^+ w$, sú odvodenia z w konfluentné; to jest ak $w \to^* u'$ a $w \to^* v'$, existuje $z' \in X^*$ spĺňajúce $u' \to^* z'$ a $v' \to^* z'$.

Ak ale v takom prípade $x \to x_1 \to^* u$ a $x \to x_2 \to^* v$, z lokálnej konfluencie dostávame existenciu $y \in X^*$ takého, že $x_1 \to^* y$ a $x_2 \to^* y$. Súčasne ale vďaka konfluentnosti odvodení začínajúcich v x_1 a x_2 dostávame existenciu slov $y_1, y_2 \in X^*$ takých, že $u \to^* y_1$ a súčasne $y \to^* y_1$ a $v \to^* y_2$ a súčasne $y \to^* y_2$. Z konfluentnosti odvodení začínajúcich v y napokon dostávame existenciu $z \in X^*$ takého, že súčasne

$$x \to x_1 \to^* y \to^* y_1 \to^* z, \qquad \text{a teda aj} \qquad u \to^* y_1 \to^* z$$

a

$$x \to x_2 \to^* y \to^* y_2 \to^* z, \qquad \text{a teda aj} \qquad v \to^* y_2 \to^* z.$$

To odporuje nášmu predpokladu o neexistencii takéhoto z. □

Ako ďalší príklad konečne prezentovaného monoidu teda môžeme pridať – napriek tomu, že sa dá dokázať, že grupy netvoria varietu monoidov – voľnú grupu.

Príklad 2.10.9. Nech X je množina neobsahujúca $\cdot$, 1, nech $X^{-1} = \{a^{-1} \mid a \in X\}$ a bez ujmy na všeobecnosti predpokladajme, že $X \cap X^{-1} = \emptyset$. Voľnú grupu F_X nad X potom môžeme zadať ako konečne prezentovaný *monoid* $F_X = \langle X \cup X^{-1} \mid R\rangle$, kde $R = \{aa^{-1} = 1, a^{-1}a = 1 \mid a \in X\}$. Kongruencia generovaná reláciou R sa niekedy nazýva aj *Dyckovou kongruenciou.*

Príklad 2.10.10. Nech X je množina neobsahujúca $\cdot$, 1, nech $X^{-1} = \{a^{-1} \mid a \in X\}$ a $X \cap X^{-1} = \emptyset$. Monoidom z istého pohľadu podobným voľnej grupe je takzvaný *bicyklický* alebo *involutívny monoid* nad X daný prezentáciou $P_X = \langle X \cup X^{-1} \mid S\rangle$ pre $S = \{aa^{-1} = 1 \mid a \in X\}$; „normálnymi formami“ sú tu teda slová neobsahujúce žiadne „dobre uzátvorkované“ podslová, pretože tie môžeme stotožniť s prázdnym slovom. Kongruencia S sa nazýva aj *Šamirovou kongruenciou* a bicyklický monoid samotný možno použiť aj na opis zásobníkových automatov.

Kapitola 3

Algebraická teória jazykov I

V tejto kapitole sa zameriame na niektoré najelementárnejšie výsledky dávajúce do súvisu formálne jazyky s pologrupami a monoidmi; vybudujeme tak základy *algebraickej teórie jazykov*. K algebraickej teórii jazykov sa neskôr ešte vrátime v súvislosti so skúmaním variet jazykov. Odporúčaným čítaním k tejto kapitole je [10, 13, 14].

3.1 Rozoznávanie jazykov monoidmi

K viacerým už známym charakterizáciám racionálnych – alebo regulárnych – jazykov teraz pridáme ďalšiu: ukážeme, že ide práve o takzvané *rozoznateľné jazyky*, čiže jazyky rozoznávané homomorfizmami z voľných do konečných monoidov.

Definícia 3.1.1. Nech Σ je abeceda, $L \subseteq \Sigma^*$ je jazyk, M je monoid a $\varphi\colon \Sigma^* \to M$ je homomorfizmus monoidov. Hovoríme, že jazyk L je *rozoznávaný homomorfizmom* φ, ak existuje množina $F \subseteq M$ taká, že $L = \varphi^{-1}(F)$. V takom prípade tiež hovoríme, že L je *rozoznávaný monoidom* M.

Jazyk rozoznávaný homomorfizmom $\varphi\colon \Sigma^* \to M$ teda pre nejakú množinu $F \subseteq M$ pozostáva z práve všetkých slov $w \in \Sigma^*$ takých, že $\varphi(w) \in F$. Nasledujúce jednoduché tvrdenie ukazuje, že v skutočnosti stačí overiť jednu špeciálnu množinu F.

Tvrdenie 3.1.2. *Nech $L \subseteq \Sigma^*$ je jazyk a $\varphi\colon \Sigma^* \to M$ je homomorfizmus monoidov. Potom je jazyk L rozoznávaný homomorfizmom φ práve vtedy, keď $L = \varphi^{-1}(\varphi(L))$.*

Dôkaz. Ak $L = \varphi^{-1}(\varphi(L))$, stačí za F zvoliť množinu $\varphi(L)$. Ak naopak existuje množina $F \subseteq M$ taká, že $L = \varphi^{-1}(F)$, tak $\varphi(w) \in F$ pre všetky $w \in L$ a $\varphi(w) \notin F$ pre všetky $w \notin L$ – pre všetky $w \in \Sigma^*$ teda $\varphi(w) \in F$ práve vtedy, keď $\varphi(w) \in \varphi(L)$ a $L = \varphi^{-1}(F) = \varphi^{-1}(\varphi(L))$. □

Bez obmedzenia na monoid M nie je trieda jazykov rozoznávaných homomorfizmami $\varphi\colon \Sigma^* \to M$ nijak zaujímavá – *ľubovoľný* jazyk $L \subseteq \Sigma^*$ totiž možno vyjadriť ako $L = \mathrm{id}_{\Sigma^*}^{-1}(L)$, kde $\mathrm{id}_{\Sigma^*}\colon \Sigma^* \to \Sigma^*$ je identický homomorfizmus na voľnom monoide Σ^*. Zaujímavejšia začne byť situácia v momente, keď sa obmedzíme na homomorfizmy do *konečných* monoidov. Jazyky rozoznávané takýmito homomorfizmami nazveme *rozoznateľnými*.

Definícia 3.1.3. Nech Σ je abeceda. Jazyk $L \subseteq \Sigma^*$ nazveme *rozoznateľným*, ak existuje *konečný* monoid M a homomorfizmus monoidov $\varphi\colon \Sigma^* \to M$ rozoznávajúci jazyk L. Množinu všetkých rozoznateľných jazykov nad abecedou Σ označujeme $\mathrm{Rec}(\Sigma^*)$.

Jazyk $L \subseteq \Sigma^*$ je teda rozoznateľný v prípade, že existuje konečný monoid M a homomorfizmus $\varphi\colon \Sigma^* \to M$ tak, že $L = \varphi^{-1}(F)$ pre nejakú množinu $F \subseteq M$, čo podľa tvrdenia 3.1.2 nastane práve vtedy, keď $L = \varphi^{-1}(\varphi(L))$. Ak teda poznáme konečnú množinu $F = \varphi(L)$, možno príslušnosť slov do jazyka L kontrolovať tak, že dané slovo zobrazíme homomorfizmom φ a zistíme, či je jeho obraz prvkom F.

Príklad 3.1.4. Pre $\Sigma = \{a, b\}$ je jazyk $L = \{w \in \Sigma^* \mid |w|_a \equiv 0 \pmod 2\}$ rozoznateľný. Evidentne totiž $L = \varphi^{-1}(0)$ pre homomorfizmus $\varphi\colon \Sigma^* \to (\mathbb{Z}_2, +, 0)$ daný ako $\varphi(a) = 1$ a $\varphi(b) = 0$; tento predpis určuje jednoznačne daný homomorfizmus vďaka tomu, že Σ^* je voľný monoid nad Σ.

Príklad 3.1.5. Každý konečný jazyk $L \subseteq \Sigma^*$ je rozoznateľný. Nech $n \in \mathbb{N}$ je ľubovoľné prirodzené číslo také, že pre všetky $w \in L$ je $|w| \leq n$. Potom môžeme uvažovať monoid $(\Sigma^{\leq n} \cup \{0\}, \circ, \varepsilon)$, kde bez ujmy na všeobecnosti predpokladáme, že $0 \notin \Sigma^*$,

$$\Sigma^{\leq n} = \bigcup_{k=0}^{n} \Sigma^k,$$

a pre všetky $u, v \in \Sigma^{\leq n} \cup \{0\}$ je

$$u \circ v = \begin{cases} uv & \text{ak } u, v \in \Sigma^{\leq n} \text{ a } |u| + |v| \leq n, \\ 0 & \text{inak.} \end{cases}$$

Keďže je monoid Σ^* voľný nad Σ, existuje homomorfizmus $\varphi\colon \Sigma^* \to (\Sigma^{\leq n} \cup \{0\}, \circ, \varepsilon)$ taký, že pre všetky $c \in \Sigma$ je $\varphi(c) = c$, ak $n \geq 1$ a $\varphi(c) = 0$, ak $n = 0$. Ak potom L interpretujeme ako podmnožinu monoidu $(\Sigma^{\leq n} \cup \{0\}, \circ, \varepsilon)$, evidentne $L = \varphi^{-1}(L)$.

Uvažujme teraz bežným spôsobom definovaný *deterministický konečný automat* $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ nad abecedou Σ, kde Q je konečná množina stavov, $\delta\colon Q \times \Sigma \to Q$ je prechodová funkcia, $q_0 \in Q$ je počiatočný stav a $F \subseteq Q$ je množina koncových stavov. Prechodovú funkciu δ možno rozšíriť na zobrazenie $\hat{\delta}\colon Q \times \Sigma^* \to Q$ nasledujúcim spôsobom: pre všetky $q \in Q$ je $\hat{\delta}(q, \varepsilon) = q$ a pre všetky $q \in Q$, $x \in \Sigma^*$ a $c \in \Sigma$ je $\hat{\delta}(q, xc) = \delta(\hat{\delta}(q, x), c)$. *Jazyk rozoznávaný automatom* $\mathcal{A}$ potom môžeme definovať aj ako

$$\|\mathcal{A}\| := \{w \in \Sigma^* \mid \hat{\delta}(q_0, w) \in F\}.$$

Je pritom zrejmé, že takto definované zobrazenie $\hat{\delta}$ je *pravou akciou monoidu* Σ^* *na množine* Q: pre všetky $q \in Q$ je $\hat{\delta}(q, \varepsilon) = q$ a $\hat{\delta}(q, xy) = \hat{\delta}(\hat{\delta}(q, x), y)$ pre všetky $x, y \in \Sigma^*$. Môžeme teda namiesto $\hat{\delta}$ používať aj notáciu, ktorá je pre akcie monoidov na množinách bežná: namiesto $\hat{\delta}(q, x)$ pre $q \in Q$ a $x \in \Sigma^*$ budeme často písať aj $q{\cdot}x$, prípadne môžeme namiesto $\cdot$ používať nejaký variant tohto symbolu, napríklad $\circ, \bullet, \cdot$ s indexom a pod. Samotný automat potom píšeme aj ako päticu $\mathcal{A} = (Q, \Sigma, \cdot, q_0, F)$.

V tomto momente ale pre nás budú dôležitejšie zobrazenia, ktoré vzniknú zo zobrazenia $\hat{\delta}$ zafixovaním druhého argumentu. Pre všetky $x \in \Sigma^*$ tak budeme písať $\delta_x\colon Q \to Q$ pre zobrazenie dané pre všetky $q \in Q$ ako $\delta_x(q) = \hat{\delta}(q, x)$. Pre všetky $x, y \in \Sigma^*$ potom evidentne $\delta_{xy} = \delta_y \circ \delta_x$, kde $\circ$ označuje bežné skladanie zobrazení.

Definícia 3.1.6. Nech $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ je deterministický konečný automat. *Prechodovým monoidom* automatu $\mathcal{A}$ nazveme konečný monoid $(\mathcal{T}(\mathcal{A}), \cdot, \delta_\varepsilon)$, kde $\mathcal{T}(\mathcal{A}) = \{\delta_x \mid x \in \Sigma^*\}$ a pre všetky $x, y \in \Sigma^*$ je $\delta_x \cdot \delta_y := \delta_{xy} = \delta_y \circ \delta_x$.

Poznámka 3.1.7. Napriek tomu, že zápis $\mathcal{T}(\mathcal{A}) = \{\delta_x \mid x \in \Sigma^*\}$ pripomína definíciu nekonečnej množiny, je monoid $\mathcal{T}(\mathcal{A})$ skutočne vždy konečný: každé δ_x je totiž zobrazením z Q do Q a všetkých takýchto zobrazení je len konečne veľa.

Lema 3.1.8. *Nech $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ je deterministický konečný automat. Monoid $\mathcal{T}(\mathcal{A})$ potom rozoznáva jazyk $\|\mathcal{A}\|$.*

Dôkaz. Uvažujme homomorfizmus $\varphi\colon \Sigma^* \to \mathcal{T}(\mathcal{A})$ daný pre všetky $c \in \Sigma$ ako $\varphi(c) = \delta_c$. Indukciou potom ľahko dokážeme, že pre všetky $x \in \Sigma^*$ musí byť $\varphi(x) = \delta_x$. Potom

$$\|\mathcal{A}\| = \varphi^{-1}\left(\{\delta_w \mid w \in \Sigma^*;\ \delta_w(q_0) \in F\}\right),$$

pretože $x \in \|\mathcal{A}\|$ práve vtedy, keď $\hat{\delta}(q_0, x) \in F$, čiže keď $\delta_x(q_0) \in F$. To nastane práve vtedy, keď je $\varphi(x) = \delta_x$ zobrazením z množiny $\{\delta_w \mid w \in \Sigma^*;\ \delta_w(q_0) \in F\}$. □

Nech je teraz Σ abeceda, $(M, \cdot, 1)$ konečný monoid a $\varphi\colon \Sigma^* \to M$ homomorfizmus monoidov. Pre všetky $F \subseteq M$ potom môžeme uvažovať konečný automat $\mathcal{A}_{\varphi,F} = (M, \Sigma, \bullet, 1, F)$ taký, že pre všetky $s \in M$ a $c \in \Sigma$ je $s \bullet c = s \cdot \varphi(c)$.

Lema 3.1.9. *Nech Σ je abeceda, $(M, \cdot, 1)$ konečný monoid a $\varphi\colon \Sigma^* \to M$ homomorfizmus monoidov. Automat $\mathcal{A}_{\varphi,F}$ potom rozoznáva jazyk $\varphi^{-1}(F)$.*

Dôkaz. Nech $w \in \Sigma^*$. Indukciou možno ľahko dokázať, že $1 \bullet w = \varphi(w)$. Potom $w \in \|\mathcal{A}_{\varphi,F}\|$ práve vtedy, keď $1 \bullet w = \varphi(w) \in F$, čiže keď $w \in \varphi^{-1}(F)$. □

Veta 3.1.10. *Nech Σ je abeceda a $L \subseteq \Sigma^*$ je jazyk. Potom je jazyk L rozoznateľný práve vtedy, keď $L = \|\mathcal{A}\|$ pre nejaký deterministický konečný automat $\mathcal{A}$.*

Dôkaz. Ak je jazyk L rozoznateľný, existuje konečný monoid M, homomorfizmus $\varphi\colon \Sigma^* \to M$ a množina $F \subseteq M$ tak, že $L = \varphi^{-1}(F)$. Podľa lemy 3.1.9 potom $L = \|\mathcal{A}_{\varphi,F}\|$. Ak naopak $L = \|\mathcal{A}\|$ pre nejaký deterministický konečný automat $\mathcal{A}$, je podľa lemy 3.1.8 jazyk L rozoznávaný konečným prechodovým monoidom $\mathcal{T}(\mathcal{A})$. □

Dokázali sme teda *rovnosť tried rozoznateľných a racionálnych jazykov*: pre všetky abecedy Σ je $\mathrm{Rec}(\Sigma^*) = \mathrm{Rat}(\Sigma^*)$, kde ako $\mathrm{Rat}(\Sigma^*)$ môžeme označiť množinu všetkých racionálnych jazykov nad abecedou Σ – za definíciu racionálnosti jazyka tu môžeme vziať napríklad jeho opísateľnosť racionálnym výrazom, čo je samozrejme ekvivalentné rozoznateľnosti deterministickým konečným automatom.

Dôvod na rozlišovanie medzi pojmami „rozoznateľný“ a „racionálny“ – oboje možno v kontexte jazykov nahradiť aj zaužívaným termínom „regulárny“ – má korene v skutočnosti, že ekvivalencia rozoznateľnosti a racionálnosti prestane platiť v prípade, keď začneme namiesto jazykov – čiže podmnožín voľného monoidu – skúmať podmnožiny všeobecných monoidov. Takéto zovšeobecnenie môže byť motivované napríklad skúmaním prekladov, jazykov stôp, a pod. Ukazuje sa, že pre podmnožiny monoidov je prirodzeným spôsobom definovaná rozoznateľnosť pomocou homomorfizmov do konečných monoidov stále ekvivalentná rozoznateľnosti vhodnou obdobou deterministických konečných automatov, definovaných pomocou pojmu akcie monoidu na množine. Neplatí však ekvivalencia týchto dvoch druhov rozoznateľnosti s realizovateľnosťou nedeterministickými konečnými automatmi nad monoidmi – pre monoid $(M, \cdot, 1)$ ide o 2^M_{fin}-automaty[1] nad polokruhom $(2^M, \cup, \cdot, \emptyset, \{1\})$ – ktoré sú však stále ekvivalentné racionálnym výrazom, a teda realizujú práve racionálne podmnožiny monoidu M.

O rozoznateľných a racionálnych podmnožinách monoidov resp. pologrúp sa možno dočítať napríklad v [14, 13].

3.2 Rozoznávanie jazykov pologrupami

Podobne ako rozoznávanie ľubovoľných jazykov (konečnými) monoidmi možno definovať aj rozoznávanie jazykov neobsahujúcich prázdne slovo – čiže podmnožín voľnej pologrupy Σ^+ pre nejakú abecedu Σ – (konečnými) pologrupami. Jazyk $L \subseteq \Sigma^+$ tak nazveme *pologrupovo rozoznateľným*, ak existuje konečná pologrupa S a homomorfizmus pologrúp $\varphi\colon \Sigma^+ \to S$ taký, že $L = \varphi^{-1}(F)$ pre nejakú množinu $F \subseteq S$, alebo ekvivalentne $L = \varphi^{-1}(\varphi(L))$.

Analogicky k prechodovým monoidom môžeme definovať aj *prechodovú pologrupu* $\mathcal{T}^+(\mathcal{A})$ deterministického konečného automatu $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ – jej prvkami budú opäť zobrazenia δ_x s rovnakou operáciou ako pri $\mathcal{T}(\mathcal{A})$, avšak v tomto prípade pre všetky $x \in \Sigma^+$. Ak teda neexistuje žiadne $x \in \Sigma^+$ také, že $\delta_x = \delta_\varepsilon$, pôjde o podpologrupu monoidu $\mathcal{T}(\mathcal{A})$ na nosnej množine danej ako $\mathcal{T}(\mathcal{A}) \setminus \{\delta_\varepsilon\}$; v opačnom prípade pôjde o monoid $\mathcal{T}(\mathcal{A})$ samotný (chápaný ako pologrupa). Konštrukcia automatu $\mathcal{A}_{\varphi,F}$ sa dá evidentne upraviť aj pre pologrupy – jediným podstatným rozdielom je, že namiesto počiatočného stavu daného neutrálnym prvkom monoidu je potrebné pridať nový počiatočný stav, ktorý nikdy nemôže byť akceptačný. Z uvedených úvah vyplýva platnosť nasledujúcej vety.

[1] Pod 2^M_{fin} tu rozumieme množinu všetkých konečných podmnožín množiny M.

Veta 3.2.1. *Nech Σ je abeceda a $L \subseteq \Sigma^+$ je jazyk. Potom je jazyk L pologrupovo rozoznateľný práve vtedy, keď $L = \|\mathcal{A}\| \setminus \{\varepsilon\}$ pre nejaký deterministický konečný automat $\mathcal{A}$.*

Trieda všetkých pologrupovo rozoznateľných jazykov je v očakávanom vzťahu k triede všetkých rozoznateľných jazykov. Ak teda budeme pracovať modulo prázdne slovo, nemusíme rozoznateľnosť a pologrupovú rozoznateľnosť jazykov vôbec rozlišovať – zatiaľ.

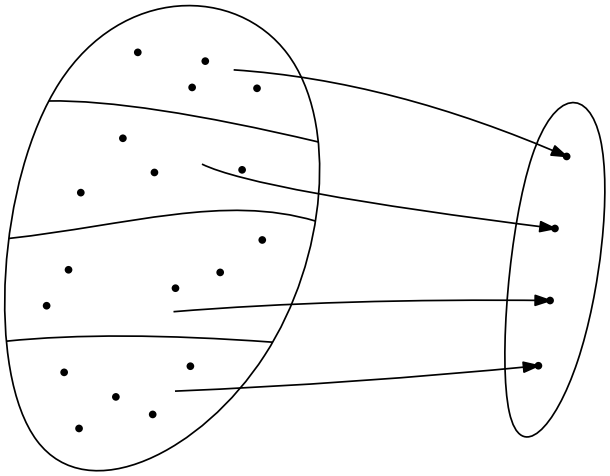
Tvrdenie 3.2.2. *Nech Σ je abeceda a $L \subseteq \Sigma^*$ je jazyk. Potom je jazyk L rozoznateľný práve vtedy, keď je jazyk $L \setminus \{\varepsilon\} \subseteq \Sigma^+$ pologrupovo rozoznateľný.*

Dôkaz. Vyplýva bezprostredne z charakterizácií pomocou konečných automatov. Uveďme ešte dôkaz čisto pomocou pologrúp a monoidov. Ak je jazyk L rozoznateľný, existuje konečný monoid M a monoidový homomorfizmus $\varphi\colon \Sigma^* \to M$ taký, že $L = \varphi^{-1}(F)$ pre nejaké $F \subseteq M$. Monoid M možno súčasne považovať aj za pologrupu, pričom homomorfizmus φ určuje pologrupový homomorfizmus $\varphi|_{\Sigma^+}\colon \Sigma^+ \to M$. Zrejme potom $L \setminus \{\varepsilon\} = \varphi|_{\Sigma^+}^{-1}(F)$. Ak je na druhej strane jazyk $L \setminus \{\varepsilon\}$ rozoznávaný homomorfizmom $\varphi\colon \Sigma^+ \to S$ pre nejakú konečnú pologrupu S, môžeme uvažovať monoid $S \cup \{1\}$, kde 1 je nový neutrálny prvok a definovať homomorfizmus $\varphi_1\colon \Sigma^* \to S \cup \{1\}$ predpismi $\varphi_1(\varepsilon) = 1$ a $\varphi_1(w) = \varphi(w)$ pre všetky $w \in \Sigma^+$. Ak $L \setminus \{\varepsilon\} = \varphi^{-1}(F)$ pre nejakú množinu $F \subseteq S$, evidentne $L = \varphi_1^{-1}(F \cup \{1\})$ alebo $L = \varphi_1^{-1}(F)$ podľa toho, či L obsahuje alebo neobsahuje prázdne slovo. □

Pozorovania učinené v tomto oddiele sa síce môžu oprávnene zdať triviálnymi, avšak rozdiel medzi rozoznávaním pologrupami a monoidmi zohráva v algebraickej teórii jazykov prekvapivo dôležitú úlohu pri klasifikácii podtried rozoznateľných jazykov. To je ale problematika, ktorou sa budeme zaoberať až v samom závere tohto semestra. V nasledujúcom budeme pracovať predovšetkým s monoidmi.

3.3 Rozoznateľné jazyky, kongruencie a pravé kongruencie

Ak je jazyk $L \subseteq \Sigma^*$ rozoznávaný homomorfizmom φ do konečného monoidu, musí byť rozoznávaný aj nejakým *surjektívnym homomorfizmom* do konečného monoidu – obraz $\operatorname{im}\varphi$ homomorfizmu φ je totiž monoid. V kapitole o univerzálnej algebre sme navyše argumentovali, že surjektívne homomorfizmy a kongruencie sú len dvoma odlišnými pohľadmi na ten istý objekt: pre surjektívny homomorfizmus $\varphi\colon \Sigma^* \to M$, kde M je monoid, je $\ker\varphi = \{(u,v) \in \Sigma^* \times \Sigma^* \mid \varphi(u) = \varphi(v)\}$ kongruencia na Σ^* a faktorový monoid $\Sigma^*/\ker\varphi$ je izomorfný monoidu M. Ak je naopak $\equiv$ kongruencia na Σ^*, je prirodzená projekcia $\nu\colon \Sigma^* \to \Sigma^*/\equiv$ surjektívnym homomorfizmom.



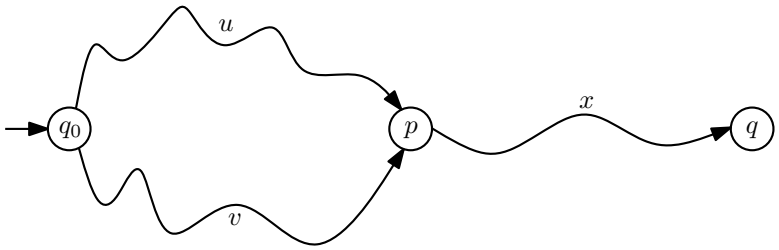
Obr. 3.1: Pripomenutie súvisu kongruencií a surjektívnych homomorfizmov.

Ak sú teda surjektívny homomorfizmus $\varphi\colon \Sigma^* \to M$ a kongruencia $\equiv$ na Σ^* v opísanej korešpondencii, sú triedy kongruencie $\equiv$ práve jazykmi typu $\varphi^{-1}(s)$ pre nejaké $s \in M$. To znamená, že $L = \varphi^{-1}(F)$ pre nejaké $F \subseteq M$ práve vtedy, keď je L zjednotením tried kongruencie $\equiv$ prislúchajúcich k $\varphi^{-1}(s)$ pre $s \in F$. *Jazyk $L \subseteq \Sigma^*$ je teda rozoznávaný homomorfizmom φ práve vtedy, keď kongruencia $\equiv$ nasycuje L*, t. j. práve vtedy, keď je L zjednotením niekoľkých tried kongruencie $\equiv$. Poznamenajme napokon, že konečnosť monoidu M sa na kongruencii $\equiv$ prejaví tým, že táto bude *konečného indexu* – čiže rozklad Σ^* podľa nej bude pozostávať iba z konečného počtu tried. *Surjektívne homomorfizmy voľného monoidu Σ^* do konečného monoidu teda zodpovedajú kongruenciám konečného indexu na Σ^*.*

Možno ešte o niečo povedomejším bude čitateľovi súvis medzi *deterministickými konečnými automatmi* bez nedosiahnuteľných stavov a *pravými kongruenciami*[2] konečného indexu na Σ^*. Pripomeňme si, že pravou kongruenciou na Σ^* rozumieme reláciu ekvivalencie $\equiv$ takú, že pre všetky $u, v, x \in \Sigma^*$ spĺňajúce $u \equiv v$ je aj $ux \equiv vx$. Pre každý deterministický konečný automat $\mathcal{A} = (Q, \Sigma, \cdot, q_0, F)$ môžeme na Σ^* definovať reláciu $\equiv_{\mathcal{A}}$ pre všetky $u, v \in \Sigma^*$ ako

$$u \equiv_{\mathcal{A}} v \qquad \text{práve vtedy, keď} \qquad q_0 \cdot u = q_0 \cdot v.$$

Očividne ide o pravú kongruenciu, pretože $q_0 \cdot u = q_0 \cdot v$ evidentne pre všetky $x \in \Sigma^*$ implikuje $q_0 \cdot ux = q_0 \cdot vx$. To je znázornené aj na obrázku 3.2. Navyše musí ísť o reláciu konečného indexu, pretože existuje bijekcia medzi jej triedami a dosiahnuteľnými stavmi automatu $\mathcal{A}$: každá trieda pravej kongruencie $\equiv_{\mathcal{A}}$ pozostáva, pre nejaký dosiahnuteľný stav $q \in Q$, z práve všetkých slov $w \in \Sigma^*$ takých, že $q_0 \cdot w = q$. Dôsledkom tiež je, že pravá kongruencia $\equiv_{\mathcal{A}}$ nasycuje jazyk $\|\mathcal{A}\|$ – tento jazyk tak musí byť daný zjednotením tried pravej kongruencie $\equiv_{\mathcal{A}}$.



Obr. 3.2: Relácia $\equiv_{\mathcal{A}}$ je pravá kongruencia.

K ľubovoľnej pravej kongruencii konečného indexu $\equiv$ na Σ^* naopak môžeme skonštruovať deterministický konečný automat $\mathcal{A}_{\equiv} = (\Sigma^*/{\equiv}, \Sigma, \cdot, [\varepsilon]_{\equiv}, F)$ tak, že pre všetky $x \in \Sigma^*$ a $c \in \Sigma$ položíme $[x]_{\equiv} \cdot c = [xc]_{\equiv}$. Vďaka vlastnosti pravej kongruencie je táto definícia skutočne nezávislá od výberu reprezentantov a vďaka konečnosti indexu pravej kongruencie $\equiv$ je automat $\mathcal{A}_{\equiv}$ konečný; každý stav automatu $\mathcal{A}_{\equiv}$ je ďalej evidentne dosiahnuteľný. Je teraz jasné, že ľubovoľný jazyk L nasýtený pravou kongruenciou $\equiv$,

$$L = \bigcup_{w \in L} [w]_{\equiv},$$

môžeme vyjadriť ako $L = \|\mathcal{A}\|$ v prípade, že vezmeme

$$F = \{[w]_{\equiv} \mid w \in L\}.$$

Podobne ako sú teda rovnakými objektmi nazeranými z rôznych uhlov pohľadu kongruencie konečného indexu na Σ^* a surjektívne homomorfizmy zo Σ^* do konečných monoidov, *sú odlišnými pohľadmi na ten istý objekt aj deterministické konečné automaty bez nedosiahnuteľných stavov a pravé kongruencie na Σ^* konečného indexu.* Dokázali sme tak ďalšie dve charakterizácie rozoznateľných – či racionálnych – jazykov.

[2] Niekedy nazývanými aj *sprava invariantnými reláciami ekvivalencie.*

Veta 3.3.1. *Nech Σ je abeceda a $L \subseteq \Sigma^*$ je jazyk. Potom sú nasledujúce tvrdenia ekvivalentné:*

(*i*) *Jazyk L je rozoznateľný.*

(*ii*) *Jazyk L je nasýtený kongruenciou konečného indexu na Σ^*.*

(*iii*) *Jazyk L je nasýtený pravou kongruenciou konečného indexu na Σ^*.*

Každá kongruencia je pritom evidentne aj pravou kongruenciou – ak pritom o kongruencii uvažujeme ako o pravej kongruencii, v princípe ide o rovnaký prechod ako v predchádzajúcom oddiele od konečného monoidu k deterministickému konečnému automatu.

Podobné charakterizácie ako vyššie by bolo možné odvodiť aj v kontexte pologrúp – akurát by bolo všade potrebné zameniť Σ^* za Σ^+.

3.4 Syntaktická kongruencia a pravá syntaktická kongruencia

Nech $L \subseteq \Sigma^*$ je jazyk a $x \in \Sigma^*$ je slovo. *Kontextom* slova x v jazyku L nazveme ľubovoľnú dvojicu $(u, v) \in \Sigma^* \times \Sigma^*$ takú, že $uxv \in L$. *Pravým kontextom* slova x v L nazveme slovo $v \in \Sigma^*$ také, že $xv \in L$. Pre množiny všetkých resp. všetkých pravých kontextov slova x v L budeme používať označenie $\mathbf{C}_L(x)$ resp. $\mathbf{C}_L^r(x)$ prevzaté z [13] – čiže

$$\mathbf{C}_L(x) = \{(u, v) \in \Sigma^* \times \Sigma^* \mid uxv \in L\},$$
$$\mathbf{C}_L^r(x) = \{v \in \Sigma^* \mid xv \in L\}.$$

Obdobne by sme mohli zaviesť aj pojem ľavého kontextu.

Definícia 3.4.1. Nech Σ je abeceda a $L \subseteq \Sigma^*$ je jazyk. *Syntaktickou kongruenciou* jazyka L nazveme binárnu reláciu $\sim_L \subseteq \Sigma^* \times \Sigma^*$ takú, že pre všetky $x, y \in \Sigma^*$ je $x \sim_L y$ práve vtedy, keď $\mathbf{C}_L(x) = \mathbf{C}_L(y)$. *Pravou syntaktickou kongruenciou* jazyka L nazveme binárnu reláciu $\sim_L^r \subseteq \Sigma^* \times \Sigma^*$ takú, že pre všetky $x, y \in \Sigma^*$ je $x \sim_L^r y$ práve vtedy, keď $\mathbf{C}_L^r(x) = \mathbf{C}_L^r(y)$.

Relácie $\sim_L$ a $\sim_L^r$ obidve očividne nasycujú jazyk L – stačí totiž vziať zjednotenie tried pozostávajúcich zo slov $x \in \Sigma^*$ takých, že $(\varepsilon, \varepsilon) \in \mathbf{C}_L(x)$ resp. $\varepsilon \in \mathbf{C}_L^r(x)$.

Tvrdenie 3.4.2. *Pre každý jazyk $L \subseteq \Sigma^*$ je $\sim_L$ kongruencia a $\sim_L^r$ pravá kongruencia.*

Dôkaz. Na dôkaz, že je $\sim_L$ kongruencia, stačí ukázať, že ide súčasne o ľavú a pravú kongruenciu. Uvažujme teda ľubovoľnú dvojicu slov $x, y \in \Sigma^*$ spĺňajúcich $x \sim_L y$ a ľubovoľné $z \in \Sigma^*$. Podmienka $x \sim_L y$ je ekvivalentná rovnosti $\mathbf{C}_L(x) = \mathbf{C}_L(y)$ a na dôkaz vzťahov $xz \sim_L yz$ a $zx \sim_L zy$ musíme ukázať, že $\mathbf{C}_L(xz) = \mathbf{C}_L(yz)$ a $\mathbf{C}_L(zx) = \mathbf{C}_L(zy)$. Uvažujme ale ľubovoľné $(u, v) \in \mathbf{C}_L(xz)$. Potom $(u, zv) \in \mathbf{C}_L(x) = \mathbf{C}_L(y)$, a teda $(u, v) \in \mathbf{C}_L(yz)$. Zvyšné tri inklúzie sa dokážu analogicky.

Podobne dokážeme, že $\sim_L^r$ je pravá kongruencia. Nech $x, y \in \Sigma^*$ sú také, že $x \sim_L^r y$ a $z \in \Sigma^*$ je ľubovoľné. Z $x \sim_L^r y$ máme $\mathbf{C}_L^r(x) = \mathbf{C}_L^r(y)$; potrebujeme dokázať rovnosť $\mathbf{C}_L^r(xz) = \mathbf{C}_L^r(yz)$. Uvažujme ale ľubovoľné $v \in \mathbf{C}_L^r(xz)$. Potom $zv \in \mathbf{C}_L^r(x) = \mathbf{C}_L^r(y)$, a teda $v \in \mathbf{C}_L^r(yz)$; opačná inklúzia sa dokáže symetricky. □

Je evidentné, že ak nejaká relácia ekvivalencie na Σ^* nasycuje jazyk $L \subseteq \Sigma^*$ – jazyk L sa dá vyjadriť ako zjednotenie časti jej tried ekvivalencie – tak je jazyk L nasýtený aj ľubovoľnou *jemnejšou*[3] reláciou ekvivalencie. Z nasledujúcej vety vyplynie, že $\sim_L$ je *najhrubšou kongruenciou* na Σ^* nasycujúcou L.

[3] To jest menšou v zmysle množinovej inklúzie.

Veta 3.4.3. *Nech Σ je abeceda, $L \subseteq \Sigma^*$ je jazyk a $\equiv$ je kongruencia na Σ^*. Kongruencia $\equiv$ potom nasycuje jazyk L práve vtedy, keď je $\equiv$ zjemnením kongruencie $\sim_L$ – čiže keď $\equiv \subseteq \sim_L$.*

Dôkaz. Nech $\equiv$ nasycuje L a $x, y \in \Sigma^*$ sú slová také, že $x \equiv y$. Keďže je relácia $\equiv$ kongruencia, musí aj pre všetky $u, v \in \Sigma^*$ byť $uxv \equiv uyv$. Kongruencia $\equiv$ ale nasycuje jazyk L, čo znamená, že $uxv \in L$ práve vtedy, keď $uyv \in L$. V dôsledku toho $(u, v) \in \mathbf{C}_L(x)$ práve vtedy, keď $(u, v) \in \mathbf{C}_L(y)$, z čoho $\mathbf{C}_L(x) = \mathbf{C}_L(y)$, a teda $x \sim_L y$.

Ak naopak $\equiv \subseteq \sim_L$, ide o zjemnenie relácie nasycujúcej L a z pozorovania učineného pred vyslovením dokazovanej vety vyplýva, že $\equiv$ musí tiež nasycovať L. □

Podobne môžeme dokázať, že pre všetky $L \subseteq \Sigma^*$ je $\sim_L^r$ *najhrubšou pravou kongruenciou* na Σ^* nasycujúcou jazyk L.

Veta 3.4.4. *Nech Σ je abeceda, $L \subseteq \Sigma^*$ je jazyk a $\equiv$ je pravá kongruencia na Σ^*. Pravá kongruencia $\equiv$ potom nasycuje jazyk L práve vtedy, keď je $\equiv$ zjemnením pravej kongruencie $\sim_L^r$ – čiže keď $\equiv \subseteq \sim_L^r$.*

Dôkaz. Ak $x \equiv y$, z vlastnosti pravej kongruencie dostávame aj $xv \equiv yv$ pre všetky $v \in \Sigma^*$. Keďže teraz $\equiv$ nasycuje jazyk L, je $xv \in L$ práve vtedy, keď $yv \in L$ – to jest $v \in \mathbf{C}_L^r(x)$ práve vtedy, keď $v \in \mathbf{C}_L^r(y)$. Preto $\mathbf{C}_L^r(x) = \mathbf{C}_L^r(y)$, a teda $x \sim_L^r y$. Ak naopak $\equiv \subseteq \sim_L^r$, musí pravá kongruencia $\equiv$ ako zjemnenie relácie ekvivalencie nasycujúcej L tiež nasycovať L. □

Bezprostredným dôsledkom našich predchádzajúcich úvah je *Myhillova-Nerodova veta*. Niekedy sa za súčasť tejto vety považujú aj zistenia nasledujúceho oddielu.

Veta 3.4.5 (Myhill, Nerode)**.** *Nech Σ je abeceda a $L \subseteq \Sigma^*$ je jazyk. Potom sú nasledujúce tvrdenia ekvivalentné:*

(*i*) *Jazyk L je rozoznateľný.*

(*ii*) *Jazyk L je nasýtený kongruenciou konečného indexu na Σ^*.*

(*iii*) *Kongruencia $\sim_L$ je konečného indexu.*

(*iv*) *Jazyk L je nasýtený pravou kongruenciou konečného indexu na Σ^*.*

(*v*) *Pravá kongruencia $\sim_L^r$ je konečného indexu.*

Dôkaz. Podľa vety 3.3.1 sú ekvivalentné tvrdenia (*i*), (*ii*) a (*iv*). Tvrdenie (*iii*) triviálne implikuje (*ii*). Ak naopak platí (*ii*) a L je nasýtený kongruenciou konečného indexu $\equiv$, musí byť podľa vety 3.4.3 relácia $\equiv$ zjemnením kongruencie $\sim_L$: ak je teda konečného indexu kongruencia $\equiv$, musí byť konečného indexu aj kongruencia $\sim_L$. Podobne tvrdenie (*v*) triviálne implikuje tvrdenie (*iv*), kým opačná implikácia vyplýva z vety 3.4.4. □

Poznamenajme ešte, že konečnosť indexu pravej kongruencie $\sim_L^r$ sa dá vyjadriť aj pomocou kvocientov: index relácie $\sim_L^r$ je konečný práve vtedy, keď je konečná množina pravých kontextov

$$\{\mathbf{C}_L^r(x) \mid x \in \Sigma^*\}.$$

Avšak evidentne $\mathbf{C}_L^r(x) = x^{-1}L$, kde $x^{-1}L$ označuje ľavý kvocient jazyka L podľa x. Triedy pravej kongruencie $\sim_L^r$ teda zodpovedajú ľavým kvocientom jazyka L podľa slov a index pravej kongruencie $\sim_L^r$ je konečný práve vtedy, keď je konečná množina kvocientov $\{x^{-1}L \mid x \in \Sigma^*\}$.

3.5 Syntaktický monoid a minimálny automat

Definícia 3.5.1. Nech Σ je abeceda a $L \subseteq \Sigma^*$ je jazyk. *Syntaktickým monoidom* jazyka L nazveme monoid $M_L = \Sigma^*/\sim_L$ a *syntaktickým homomorfizmom* jazyka L nazveme prirodzenú projekciu $\nu_L \colon \Sigma^* \to \Sigma^*/\sim_L$.

Keďže relácia $\sim_L$ nasycuje jazyk L, je zrejmé, že syntaktický homomorfizmus ν_L – a tým pádom aj syntaktický monoid M_L – rozoznáva jazyk L. Ľubovoľný monoid izomorfný syntaktickému monoidu M_L budeme tiež nazývať syntaktickým monoidom jazyka L.

Skutočnosť, že $\sim_L$ je najhrubšia kongruencia rozoznávajúca jazyk L, má svoje vyjadrenie aj v reči monoidov – hovorí o ňom nasledujúca veta. Hovoríme, že monoid M *delí* monoid N, ak je monoid M homomorfným obrazom podmonoidu monoidu N.

Veta 3.5.2. *Nech Σ je abeceda a $L \subseteq \Sigma^*$ je jazyk. Syntaktický monoid M_L potom delí všetky monoidy rozoznávajúce jazyk L. Jazyk L je teda rozoznateľný práve vtedy, keď je jeho syntaktický monoid M_L konečný.*

Dôkaz. Nech N je monoid rozoznávajúci jazyk L. Potom existuje homomorfizmus $\varphi \colon \Sigma^* \to N$ rozoznávajúci L. Uvažujme namiesto neho homomorfizmus $\varphi' \colon \Sigma^* \to \operatorname{im}\varphi$ taký, že pre všetky $w \in \Sigma^*$ je $\varphi'(w) = \varphi(w)$. Tento surjektívny homomorfizmus potom tiež rozoznáva L, z čoho $\ker\varphi' \subseteq \sim_L$. Podľa prvej vety o izomorfizme navyše $\operatorname{im}\varphi = \operatorname{im}\varphi' \cong \Sigma^*/\ker\varphi'$, pričom môžeme definovať projekciu $\psi \colon \Sigma^*/\ker\varphi' \to \Sigma^*/\sim_L$ pre všetky $w \in \Sigma^*$ predpisom

$$\psi\left([w]_{\ker\varphi'}\right) = [w]_{\sim_L}.$$

Syntaktický monoid $M_L = \Sigma^*/\sim_L$ je teda homomorfným obrazom podmonoidu $\operatorname{im}\varphi$ monoidu N, a teda monoid M_L delí monoid N. Druhá časť vety je zrejmá. □

Podobne ako syntaktickej kongruencii zodpovedá syntaktický homomorfizmus a predovšetkým syntaktický monoid, zodpovedá pravej syntaktickej kongruencii *minimálny automat* – v prípade rozoznateľnosti jazyka L stačí použiť korešpondenciu medzi pravými kongruenciami konečného indexu a deterministickými konečnými automatmi z oddielu 3.3 a pozrieť sa na pravú syntaktickú kongruenciu $\sim_L^r$ ako na automat.[4] Pre rozoznateľný jazyk L je tak jeho minimálny automat (až na izomorfizmus) jednoznačne daným automatom s najmenším počtom stavov rozoznávajúcim jazyk L. Avšak minimalita automatu tu znamená ešte o niečo viac: minimálny automat pre rozoznateľný jazyk L možno z *ľubovoľného* deterministického konečného automatu rozoznávajúceho L získať prípadným odstránením nedosiahnuteľných stavov a následným stotožnením niekoľkých dvojíc stavov. Takéto stotožnenie stavov možno aj sformalizovať a často sa nazýva *homomorfizmom* automatov.

Veta 3.5.3. *Nech Σ je abeceda, $L \subseteq \Sigma^*$ je rozoznateľný jazyk a $\mathcal{A}$ je minimálny automat rozoznávajúci jazyk L. Potom $\mathcal{T}(\mathcal{A}) \cong M_L$.*

Dôkaz. Uvažujme prechodový monoid $(\mathcal{T}(\mathcal{A}), \cdot, \delta_\varepsilon)$ minimálneho automatu $\mathcal{A} = (Q, \Sigma, \cdot, q_0, F)$ pre jazyk L, ktorý je daný takto:

$$\mathcal{T}(\mathcal{A}) = \{\delta_x \colon Q \to Q \mid x \in \Sigma^*\},$$

kde pre všetky $x \in \Sigma^*$ a $q \in Q$ je $\delta_x(q) = q \cdot x$; pre všetky $x, y \in \Sigma^*$ pritom $\delta_x \cdot \delta_y = \delta_{xy}$.

Dokážeme, že pre všetky $x, y \in \Sigma^*$ je $\delta_x = \delta_y$ práve vtedy, keď $x \sim_L y$. Predpokladajme totiž najprv $\delta_x = \delta_y$ a uvažujme ľubovoľné $(u, v) \in \mathbf{C}_L(x)$. Potom $uxv \in L$, čo znamená, že

$$q_0 \cdot uxv = ((q_0 \cdot u) \cdot x) \cdot v = ((q_0 \cdot u) \cdot y) \cdot v = q_0 \cdot uyv \in F.$$

[4] V skutočnosti možno minimálny automat definovať aj pre nerozoznateľné jazyky – v takom prípade ale tento automat bude mať nekonečne veľa stavov.

Preto aj $(u, v) \in \mathbf{C}_L(y)$ a keďže je $(u, v) \in \mathbf{C}_L(x)$ ľubovoľné, je $\mathbf{C}_L(x) \subseteq \mathbf{C}_L(y)$; opačnú inklúziu možno dokázať rovnakým spôsobom. Dostávame teda rovnosť $\mathbf{C}_L(x) = \mathbf{C}_L(y)$ a vďaka nej aj vzťah $x \sim_L y$.

Nech naopak $x \sim_L y$. Za účelom sporu predpokladajme, že $\delta_x \neq \delta_y$. Potom existuje $q \in Q$ také, že $q \cdot x \neq q \cdot y$. Z minimality automatu $\mathcal{A}$ evidentne vyplýva, že stav q musí byť dosiahnuteľný – existuje teda $w \in \Sigma^*$ také, že $q_0 \cdot w = q$. V dôsledku toho $q_0 \cdot wx \neq q_0 \cdot wy$, kým z vlastnosti kongruencie dostávame $wx \sim_L wy$. Avšak $wx \sim_L wy$ evidentne implikuje aj $wx \sim_L^r wy$. To znamená, že stavy automatu $\mathcal{A}$ nie sú v bijektívnej korešpondencii s triedami pravej kongruencie $\sim_L^r$: spor s minimalitou automatu $\mathcal{A}$.

Uvažujme teraz homomorfizmus $\psi\colon \mathcal{T}(\mathcal{A}) \to M_L$ daný ako

$$\psi\colon \delta_x \mapsto [x]_{\sim_L}$$

pre všetky $x \in \Sigma^*$. Z dokázaného vyplýva, že ide o dobre definovanú bijekciu – a teda aj o hľadaný izomorfizmus. □

Celú teóriu z tohto a predchádzajúceho oddielu by iba s drobnými rozdielmi bolo možné preniesť aj do kontextu pologrúp – možno teda hovoriť o syntaktickej kongruencii jazyka $L \subseteq \Sigma^+$ na voľnej pologrupe Σ^+, o syntaktickej pologrupe, a pod.

3.6 Rozoznávanie jazykov usporiadanými monoidmi

Definíciu jazykov rozoznávaných homomorfizmami do monoidov teraz rozšírime tak, že budeme jazyky rozoznávať homomorfizmami do *usporiadaných* monoidov. Rozoznávanie usporiadanými monoidmi nebude silnejšie, než rozoznávanie monoidmi bez usporiadania – pre konečné usporiadané monoidy pôjde o ďalšiu ekvivalentnú charakterizáciu rozoznateľných resp. racionálnych jazykov. Avšak jeden usporiadaný monoid bude vo všeobecnosti rozoznávať menej jazykov, než ten istý monoid bez usporiadania. Triedy konečných usporiadaných monoidov teda neskôr budeme môcť použiť na jemnejšiu klasifikáciu tried rozoznateľných jazykov, než je možné dosiahnuť skúmaním tried neusporiadaných monoidov.

Predusporiadaním alebo *kváziusporiadaním* na množine X rozumieme ľubovoľnú reflexívnu a súčasne tranzitívnu reláciu $\preceq \subseteq X^2$. Ide teda o zovšeobecnené čiastočné usporiadania, ktoré nemusia byť antisymetrické. Pre každé predusporiadanie $\preceq$ na X môžeme na X definovať reláciu ekvivalencie $\equiv$ takú, že pre $x, y \in X$ je $x \equiv y$ práve vtedy, keď $x \preceq y$ a súčasne $y \preceq x$. Na faktorovej množine $X/\equiv$ potom predusporiadanie $\preceq$ indukuje čiastočné usporiadanie $\leq$ také, že $[x]_\equiv \leq [y]_\equiv$ práve vtedy, keď $x \preceq y$.

Predusporiadania okrem čiastočných usporiadaní zovšeobecňujú aj relácie ekvivalencie – je totiž evidentné, že každá relácia ekvivalencie je predusporiadaním, pričom indukovaným čiastočným usporiadaním na triedach ekvivalencie je usporiadanie rovnosťou. Obdobou kongruencií pre predusporiadania sú takzvané *izotónne predusporiadania* (častejšie nazývané *monotónnymi*). Hoci by sme tento pojem mohli zaviesť aj na úrovni univerzálnej algebry, obmedzíme sa teraz na definíciu izotónneho predusporiadania na monoide, pričom rovnaká je aj definícia pre pologrupy. *Izotónne predusporiadanie* na monoide $(M, \cdot, 1)$ je predusporiadanie $\preceq \subseteq M^2$ také, že pre všetky $a, a', b, b' \in M$ spĺňajúce $a \preceq a'$ a $b \preceq b'$ je $a \cdot b \preceq a' \cdot b'$.

Definícia 3.6.1. *Usporiadaný monoid* je štvorica $(M, \cdot, 1, \leq)$, kde $(M, \cdot, 1)$ je monoid a $\leq$ je izotónne čiastočné usporiadanie na monoide $(M, \cdot, 1)$.

Každý monoid $(M, \cdot, 1)$ možno chápať aj ako usporiadaný monoid $(M, \cdot, 1, =)$. Definícia rozoznávania jazykov usporiadanými monoidmi je podobná definícii rozoznávania neusporiadanými monoidmi – od podmnožiny F usporiadaného monoidu ale navyše požadujeme, aby bola nahor uzavretá.

Definícia 3.6.2. Nech Σ je abeceda, $L \subseteq \Sigma^*$ je jazyk, $(M, \cdot, 1, \leq)$ je usporiadaný monoid a $\varphi\colon \Sigma^* \to M$ je homomorfizmus monoidov. Hovoríme, že homomorfizmus φ *rozoznáva* jazyk L, ak existuje nahor uzavretá množina $F \subseteq M$ taká, že $L = \varphi^{-1}(F)$. V takom prípade tiež hovoríme, že je jazyk L *rozoznávaný* usporiadaným monoidom $(M, \cdot, 1, \leq)$.

Je jasné, že jazyk $L \subseteq \Sigma^*$ je rozoznávaný monoidom $(M, \cdot, 1)$ práve vtedy, keď je rozoznávaný usporiadaným monoidom $(M, \cdot, 1, =)$ – každá podmnožina takéhoto usporiadaného monoidu je totiž nahor uzavretá. Ak je navyše jazyk L rozoznávaný ľubovoľným usporiadaným monoidom $(M, \cdot, 1, \leq)$, musí byť rozoznávaný aj monoidom $(M, \cdot, 1)$. Z týchto pozorovaní vyplýva, že jazyk L je rozoznávaný *konečným* usporiadaným monoidom práve vtedy, keď je rozoznateľný (to jest racionálny).

Podobne ako surjektívne homomorfizmy zo Σ^* do konečného monoidu zodpovedajú – vďaka konceptom jadra homomorfizmu a prirodzenej projekcie – kongruenciám konečného indexu na Σ^*, zodpovedajú surjektívne homomorfizmy zo Σ^* do konečného usporiadaného monoidu *izotónnym predusporiadaniam* konečného indexu na Σ^*; konečnosť indexu predusporiadania $\preceq$ pritom znamená konečnosť indexu ním určenej relácie ekvivalencie, v ktorej sú všetky dvojice x, y také, že $x \preceq y$ a $y \preceq x$. Je totiž zrejmé, že pre ľubovoľný homomorfizmus $\varphi\colon \Sigma^* \to (M, \cdot, 1, \leq)$ je relácia $\preceq\ \subseteq \Sigma^* \times \Sigma^*$, pre všetky $x, y \in \Sigma^*$ daná ako $x \preceq y$ práve vtedy keď $\varphi(x) \leq \varphi(y)$, izotónnym predusporiadaním konečného indexu: reflexívnosť a tranzitívnosť tejto relácie sú zrejmé a je izotónnosť vyplýva zo skutočnosti, že pre všetky $x, x', y, y' \in \Sigma^*$ spĺňajúce $x \preceq x'$ a $y \preceq y'$ je $\varphi(x) \leq \varphi(x')$ a $\varphi(y) \leq \varphi(y')$, z čoho vďaka izotónnosti usporiadania na M dostávame

$$\varphi(xy) = \varphi(x)\varphi(y) \leq \varphi(x')\varphi(y') = \varphi(x'y'),$$

čiže $xy \preceq x'y'$. Pre ľubovoľné izotónne predusporiadanie $\preceq$ konečného indexu na Σ^* naopak môžeme uvažovať ním určenú reláciu ekvivalencie $\equiv$ takú, že $x \equiv y$ práve vtedy, keď $x \preceq y$ a zároveň $y \preceq x$; evidentne ide o kongruenciu. Faktorový monoid $\Sigma^*/{\equiv}$ je potom konečný a možno na ňom uvažovať čiastočné usporiadanie $\leq$ dané ako $[x]_\equiv \leq [y]_\equiv$ práve vtedy, keď $x \preceq y$. Toto čiastočné usporiadanie je evidentne izotónne. Prirodzenú projekciu $\nu\colon \Sigma^* \to \Sigma^*/{\equiv}$ tak možno chápať aj ako homomorfizmus zo Σ^* do konečného usporiadaného monoidu $(\Sigma^*/{\equiv}, \cdot, [\varepsilon]_\equiv, \leq)$.

Ak je teraz $\varphi\colon \Sigma^* \to M$ homomorfizmus do usporiadaného monoidu a $\preceq$ je izotónne predusporiadanie na Σ^* zodpovedajúce homomorfizmu φ podľa vyššie opísanej korešpondencie, možno jazyk $L \subseteq \Sigma^*$ vyjadriť ako $L = \varphi^{-1}(F)$ pre nejakú nahor uzavretú množinu $F \subseteq M$ práve vtedy, keď je L nahor uzavretá vzhľadom na predusporiadanie $\preceq$. To znamená, že tak ako rozoznávanie jazykov homomorfizmami do neusporiadaných monoidov zodpovedá nasycovaniu jazykov kongruenciami, *zodpovedá rozoznávanie jazykov homomorfizmami do usporiadaných monoidov ich uzavretosti nahor vzhľadom na izotónne predusporiadania*. Pre konečné usporiadané monoidy pritom ide o izotónne predusporiadania konečného indexu.

Usporiadania možno v kontexte rozoznávania jazykov zaviesť nielen na monoidoch – alebo všeobecnejšie na pologrupách – ale aj na konečných automatoch.

Definícia 3.6.3. *Usporiadaný deterministický konečný automat* je šestica $\mathcal{A} = (Q, \Sigma, \cdot, q_0, F, \leq)$, kde $(Q, \Sigma, \cdot, q_0, F)$ je deterministický konečný automat a $\leq\ \subseteq Q^2$ je čiastočné usporiadanie na množine stavov Q také, že pre všetky $p, q \in Q$ a $c \in \Sigma$ je $p \cdot c \leq q \cdot c$ kedykoľvek $p \leq q$ a množina F je nahor uzavretá vzhľadom na $\leq$.

Je evidentné, že ľubovoľný neusporiadaný deterministický konečný automat $\mathcal{A} = (Q, \Sigma, \cdot, q_0, F)$ možno chápať aj ako usporiadaný automat $(Q, \Sigma, \cdot, q_0, F, =)$ a že tento automat rozoznáva všetky jazyky rozoznávané usporiadanými automatmi, ktoré sa s ním zhodujú na prvých piatich zložkách. Jazyk je teda rozoznávaný usporiadaným deterministickým konečným automatom práve vtedy, keď je rozoznateľný (resp. racionálny). Na *každom* deterministickom konečnom automate $\mathcal{A} = (Q, \Sigma, \cdot, q_0, F)$ navyše možno prirodzene definovať usporiadanie pomocou budúcností stavov – to znamená jazykov $\mathrm{fut}(q) = \{w \in \Sigma^* \mid q \cdot w \in F\}$ pre všetky $q \in Q$: môžeme položiť $p \leq q$ práve vtedy, keď $\mathrm{fut}(p) \subseteq \mathrm{fut}(q)$.

Nie je navyše ťažké vidieť, že podobne ako neusporiadané deterministické konečné automaty bez nedosiahnuteľných stavov možno chápať aj ako pravé kongruencie konečného indexu na Σ^*, možno usporiadané deterministické konečné automaty bez nedosiahnuteľných stavov chápať ako *sprava izotónne predusporiadania* na Σ^*, čiže predusporiadania $\preceq \subseteq \Sigma^* \times \Sigma^*$ také, že pre všetky $u, v, x \in \Sigma^*$ je $ux \preceq vx$ kedykoľvek $u \preceq v$: pre usporiadaný automat $\mathcal{A} = (Q, \Sigma, \cdot, q_0, F, \leq)$ môžeme položiť $u \preceq v$ práve vtedy, keď $q_0 \cdot u \leq q_0 \cdot v$. Relácia $\preceq$ je potom evidentne sprava izotónnym predusporiadaním na Σ^*. Skutočnosť, že je jazyk L rozoznávaný automatom $\mathcal{A}$ s nahor uzavretou množinou koncových stavov F sa pritom odzrkadlí v skutočnosti, že je množina L nahor uzavretá vzhľadom na $\preceq$. Ku každému sprava izotónnemu predusporiadaniu $\preceq$ takému, že je jazyk L nahor uzavretý vzhľadom na $\preceq$, môžeme naopak uvažovať automat $(\Sigma^*/\equiv, \Sigma, \cdot, [\varepsilon]_\equiv, F, \leq)$, kde $\equiv$ je relácia ekvivalencie určená predusporiadaním $\preceq$ – t. j. $u \equiv v$ práve vtedy, keď $u \preceq v$ a zároveň $v \preceq u$. Ľahko vidieť, že $\equiv$ je pravá kongruencia. Pre všetky $x \in \Sigma^*$ a $c \in \Sigma$ tak môžeme korektne definovať $[x]_\equiv \cdot c = [xc]_\equiv$. Za F môžeme vziať konečnú množinu $F = \{[x]_\equiv \mid x \in L\}$ a usporiadanie $\leq$ môžeme definovať ako $[x]_\equiv \leq [y]_\equiv$ práve vtedy, keď $x \preceq y$.

Pozorovania doposiaľ učinené v rámci tohto oddielu tak možno zhrnúť nasledujúcou vetou.

Veta 3.6.4. *Nech Σ je abeceda a $L \subseteq \Sigma^*$ je jazyk. Potom sú nasledujúce tvrdenia ekvivalentné:*

(*i*) *Jazyk L je rozoznateľný.*

(*ii*) *Jazyk L je rozoznávaný homomorfizmom zo Σ^* do konečného usporiadaného monoidu.*

(*iii*) *Jazyk L je nahor uzavretý vzhľadom na nejaké izotónne predusporiadanie konečného indexu na Σ^*.*

(*iv*) *Jazyk L je rozoznávaný usporiadaným deterministickým konečným automatom.*

(*v*) *Jazyk L je nahor uzavretý vzhľadom na sprava izotónne predusporiadanie konečného indexu na Σ^*.*

Definícia 3.6.5. Nech Σ je abeceda a $L \subseteq \Sigma^*$ je jazyk. *Syntaktickým predusporiadaním* daným jazykom L nazveme binárnu reláciu $\preceq_L \subseteq \Sigma^* \times \Sigma^*$ takú, že pre všetky $x, y \in \Sigma^*$ je $x \preceq_L y$ práve vtedy, keď $\mathbf{C}_L(x) \subseteq \mathbf{C}_L(y)$. *Pravým syntaktickým predusporiadaním* daným jazykom L nazveme binárnu reláciu $\preceq^r_L \subseteq \Sigma^* \times \Sigma^*$ takú, že pre všetky $x, y \in \Sigma^*$ je $x \preceq^r_L y$ práve vtedy, keď $\mathbf{C}^r_L(x) \subseteq \mathbf{C}^r_L(y)$.

Ľahko možno dokázať, že v prvom prípade ide o izotónne predusporiadanie a v druhom o sprava izotónne predusporiadanie, pričom relácia ekvivalencie určená syntaktickým predusporiadaním je syntaktická kongruencia jazyka L a relácia ekvivalencie určená pravým syntaktickým predusporiadaním je pravá syntaktická kongruencia jazyka L. Význam práve definovaných predusporiadaní však ide ďalej – medzi (sprava) izotónnymi predusporiadaniami, vzhľadom na ktoré je jazyk L nahor uzavretý, zohrávajú podobnú úlohu ako syntaktická kongruencia a pravá syntaktická kongruencia medzi (pravými) kongruenciami nasycujúcimi jazyk L.

Veta 3.6.6. *Nech Σ je abeceda, $L \subseteq \Sigma^*$ je jazyk a $\preceq$ je izotónne predusporiadanie na Σ^*. Jazyk L je potom nahor uzavretý vzhľadom na $\preceq$ práve vtedy, keď $\preceq \subseteq \preceq_L$.*

Dôkaz. Nech je L nahor uzavretý vzhľadom na $\preceq$ a $x, y \in \Sigma^*$ sú slová také, že $x \preceq y$. Z izotónnosti predusporiadania $\preceq$ potom aj pre všetky $u, v \in \Sigma^*$ dostávame $uxv \preceq uyv$. Keďže je L nahor uzavretý vzhľadom na $\preceq$, je $uyv \in L$ kedykoľvek $uxv \in L$, a teda $\mathbf{C}_L(y) \supseteq \mathbf{C}_L(x)$. Z toho vyplýva, že musí platiť aj $x \preceq_L y$.

Ak naopak $\preceq \subseteq \preceq_L$ je izotónne predusporiadanie, musí byť L určite nahor uzavretý vzhľadom na $\preceq$; ak totiž $x \in L$ a $x \preceq y$, tak $(\varepsilon, \varepsilon) \in \mathbf{C}_L(x)$ a $x \preceq_L y$, z čoho $(\varepsilon, \varepsilon) \in \mathbf{C}_L(y)$ a $y \in L$. □

Veta 3.6.7. *Nech Σ je abeceda, $L \subseteq \Sigma^*$ je jazyk a $\preceq$ je sprava izotónne predusporiadanie na Σ^*. Jazyk L je potom nahor uzavretý vzhľadom na $\preceq$ práve vtedy, keď $\preceq \subseteq \preceq^r_L$.*

Dôkaz. Podobne ako pri predchádzajúcej vete. □

Definícia 3.6.8. Nech Σ je abeceda a $L \subseteq \Sigma^*$ je jazyk. *Usporiadaným syntaktickým monoidom* jazyka L nazveme usporiadaný monoid $M_L^{\leq} = (\Sigma^*/{\sim_L}, \cdot, [\varepsilon]_{\sim_L}, \leq)$, kde $[x]_{\sim_L} \leq [y]_{\sim_L}$ práve vtedy, keď $x \preceq_L y$. Prirodzenú projekciu $\nu\colon \Sigma^* \to \Sigma^*/{\sim_L}$, chápanú ako homomorfizmus do usporiadaného monoidu $M_L^{\leq}$, nazveme *syntaktickým homomorfizmom do usporiadaného monoidu.*

Práve uvedená definícia teda zodpovedá pohľadu na syntaktické predusporiadanie ako na homomorfizmus do usporiadaného monoidu. Podobne sa môžeme pozrieť aj na pravé syntaktické predusporiadanie ako na usporiadaný automat a získame tak pojem *minimálneho usporiadaného automatu.* Keby sme navyše pre usporiadané automaty definovali ich usporiadané prechodové monoidy s usporiadaním po zložkách, bolo by možné dokázať, že usporiadaný prechodový monoid minimálneho usporiadaného automatu pre jazyk L je izomorfný usporiadanému syntaktickému monoidu jazyka L.

Literatúra

[1] Almeida, J.: *Finite Semigroups and Universal Algebra*. Singapur: World Scientific, 1994.

[2] Bergman, C.: *Universal Algebra*. Boca Raton: CRC Press, 2012.

[3] Bergman, C.: *An Invitation to General Algebra and Universal Constructions*. Cham: Springer, druhé vydanie, 2015.

[4] Brabec, J.; Hrůza, B.: *Matematická analýza II*. Praha: SNTL, 1986.

[5] Burris, S.; Sankappanavar, H. P.: *A Course in Universal Algebra*. New York: Springer, 1981.

[6] Chajda, I.: *Algebra III*. Olomouc: Univerzita Palackého v Olomouci, 1991.

[7] Cohn, P. M.: *Universal Algebra*. Dordrecht: D. Reidel Publishing Company, 1981.

[8] Fréchet, M.: Sur quelques points du calcul fonctionnel. *Rendiconti del Circolo Matematico di Palermo*, ročník 22, č. 1, 1906: s. 1–72.

[9] Grätzer, G.: *Universal Algebra*. New York: Springer, druhé vydanie, 2008.

[10] Howie, J. M.: *Automata and Languages*. Oxford: Clarendon Press, 1991.

[11] Kaplansky, I.: *Set Theory and Metric Spaces*. Boston: Allyn and Bacon, 1972.

[12] Kriz, I.; Pultr, A.: *Introduction to Mathematical Analysis*. Basel: Birkhäuser, 2013.

[13] Kunc, M.: Pologrupy a formální jazyky. 2024.
URL `https://www.math.muni.cz/~kunc/vyuka/pologrupy_text.pdf`

[14] Sakarovitch, J.: *Elements of Automata Theory*. Cambridge: Cambridge University Press, 2009.

[15] Simmons, G. F.: *Introduction to Topology and Modern Analysis*. New York: McGraw-Hill, 1963.

[16] Wechler, W.: *Universal Algebra for Computer Scientists*. Heidelberg: Springer, 1992.