verze 29/9/09

Toto je ‘prozatím definitivní’ verze provizorního textu o logice, aritmetice a množinách.

věnováno

Laskavým čtenářům a čtenářkám, kteří navštěvovali tyto přednášky.

poděkování

Za upozornění na řadu chyb děkuji M. Bizzarrimu.

Část I

Matematická logika

Kapitola 1

Úvod

Co je to logika? Třebaže je obtížné najít univerzálně přijatelnou definici (různých definic tohoto pojmu je prý asi 200), můžeme zjednodušeně říci, že logika je nauka o správném uvažování, o korektním vyvozování důsledků z daných předpokladů.

Základy logiky jako systematické disciplíny položil *Aristotelés* (384–322 př. n. l.) v pětisvazkovém díle *Organon* (Nástroj).

• • •

Kapitola 2

Výroková logika

2.1 Jazyk

Než se pustíme do výkladu výrokové logiky, musíme specifikovat její jazyk. Pro naše potřeby postačí definice jazyka, podle které ***jazyk*** tvoří následující součásti:

(1) ***abeceda*** (množina ***symbolů***),

(2) množina ***formulí*** (konečných posloupností symbolů abecedy).

U ***jazyka výrokové logiky***, $\mathcal{L}_V$, sestává abeceda ze symbolů

$$\neg \qquad \rightarrow \qquad (\qquad) \qquad A_0 \qquad A_1 \qquad A_2 \ldots$$

Symboly $\neg$ (***negace***) a $\rightarrow$ (***implikace***) jsou tzv. logické spojky. Symbol A_1 je *jediný* symbol, nikoli posloupnost symbolů 'A' a '1'. Všimněme si, že naše abeceda je nekonečná.

Formule jazyka $\mathcal{L}_V$ (nebo krátce formule) jsou konečné posloupnosti symbolů, vytvořené podle následujících pravidel:

(1) posloupnost o jediném symbolu A_i, kde i je přirozené číslo, je formule (tzv. ***atomická formule***),

(2) jsou-li φ a ψ formule, pak

$$(\neg\varphi) \qquad \text{a} \qquad (\varphi \rightarrow \psi)$$

jsou rovněž formule.

Délka formule je počet symbolů, z nichž se skládá. Mezi formule patří například posloupnosti

$$A_{10}, \quad (\neg(\neg A_1)) \quad \text{nebo} \quad (A_3 \rightarrow (\neg((\neg A_0) \rightarrow A_4))).$$

Formulí oproti tomu není například posloupnost

$$\neg A_1,$$

neboť v ní chybí předepsané vnější závorky. Pro lepší čitelnost formulí ovšem budeme v případech, kdy nevznikne žádná dvojznačnost, závorky obvykle vynechávat. Na výše uvedené definici formule se tím však nic nemění.

Formule φ je ***podformulí*** formule ψ, pokud platí některá z následujících možností:

(a) φ a ψ jsou shodné,

(b) ψ je negace $(\neg\alpha)$ a φ je podformulí formule α,

(c) ψ je implikace $(\alpha \to \beta)$ a φ je podformulí formule α nebo formule β.

Všimněme si, že v případech (b) a (c) je otázka, zda formule φ je podformulí formule ψ, převedena na otázku, zda je podformulí některé kratší formule. Po konečném počtu kroků je tedy možné ji zodpovědět.

Cvičení

► **2.1.1.** Kolik formulí jazyka $\mathcal{L}_V$ má délku 2?

► **2.1.2.** Rozhodněte, zda následující posloupnosti symbolů jsou formule jazyka $\mathcal{L}_V$:

(a) $((A_1A_2)A_3)$

(b) $(A_1 \to (\neg A_1))$

(c) $A_1 \to A_2$

(d) $(A_1 \leftarrow A_2)$

► **2.1.3.** Určete všechny podformule formule $((A_0 \to (\neg A_2)) \to (A_2 \to A_3))$.

2.2 Pravdivost formulí

Nesou formule nějaký *význam*? Podle definice je formule posloupností symbolů, pouhým formálním objektem. Pokud však zvolíme určitou interpretaci jednotlivých symbolů, mohou tím dostat "význam" i samotné formule.

Atomické formule můžeme nahlížet jako elementární výroky, které mohou nezávisle na sobě být pravdivé nebo nepravdivé. Dejme tomu, že pro každou atomickou formuli je určeno, která možnost nastává. Dokážeme pak posoudit pravdivost i u složitějších formulí? Bez dalšího upřesnění ne — nevíme

totiž, jak pravdivost ovlivňují logické spojky. Na jednu stranu tyto spojky samozřejmě sugerují jistý tradiční význam: je-li například formule A_0 označena za nepravdivou, budeme asi v pokušení vyhodnotit formuli $(\neg A_0)$ jako pravdivou. Na druhou stranu je užitečné si představit, že místo symbolů $\neg$ a $\rightarrow$ budeme psát například $\clubsuit$ a $\lhd$. Pro tyto symboly se již žádná interpretace nejeví jako samozřejmá.

Přesto budeme pravdivost formulí definovat právě v souladu s tradičním významem logických spojek, který je následující: negace formule φ je nepravdivá, právě když φ je pravdivá, a implikace $\varphi \rightarrow \psi$ je nepravdivá, právě když její předpoklad φ je pravdivý, ale její závěr ψ nikoli.

Definujme proto ***ohodnocení*** ν jako libovolné zobrazení, které každé formuli φ jazyka $\mathcal{L}_V$ přiřadí hodnotu $\nu(\varphi) \in \{0, 1\}$, a splňuje pro každou formuli φ, ψ rekurentní předpis

$$\nu\big((\neg\varphi)\big) = \begin{cases} 0 & \text{pokud } \nu(\varphi) = 1, \\ 1 & \text{jinak.} \end{cases} \tag{2.1}$$

$$\nu\big((\varphi \rightarrow \psi)\big) = \begin{cases} 0 & \text{pokud } \nu(\varphi) = 1 \text{ a } \nu(\psi) = 0, \\ 1 & \text{jinak.} \end{cases} \tag{2.2}$$

Hodnotu $\nu(\varphi)$ označujeme jako ***(pravdivostní) hodnotu*** formule φ při ohodnocení ν. Je-li $\nu(\varphi) = 1$, řekneme, že formule φ je ***pravdivá*** při ohodnocení ν.

K určení pravdivostních hodnot formule φ při různých ohodnoceních lze použít ***pravdivostní tabulku***. Řádky této tabulky odpovídají (obvykle všem) různým kombinacím hodnot atomických formulí obsažených ve formuli φ. Sloupce tabulky odpovídají podformulím formule φ. Položky v tabulce určují pravdivostní hodnoty příslušných podformulí při daném ohodnocení. Při jejich určování využíváme pravidla (2.1) a (2.2) a postupujeme od jednodušších podformulí ke složitějším. Konečným výsledkem je obsah sloupce odpovídajícího formuli φ.

Příklad 2.1. Určeme pravdivostní tabulku formule $\alpha \equiv (A_0 \rightarrow (\neg A_1))$. Hodnoty formule α jsou uvedeny v posledním sloupci.

A_1	A_2	$(\neg A_1)$	$((\neg A_1) \rightarrow A_2)$
0	0	1	0
0	1	1	1
1	0	0	1
1	1	0	1

Definujme ***booleovskou funkci*** n proměnných jako libovolné zobrazení $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Je-li φ formule s k různými atomickými podformulemi

a přiřadíme-li těmto atomickým podformulím proměnné $x_1, \ldots, x_k$, pak pravdivostní hodnoty formule φ při různých ohodnoceních vlastně určují booleovskou funkci f_φ k proměnných (řekneme, že f_φ je funkce ***realizovaná*** formulí φ). Pravdivostní tabulka představuje způsob, jak funkci f_φ spočítat.

Pro formuli α v příkladu 2.1 (a pro přiřazení proměnné x_i atomické formuli A_i, kde $i = 1, 2$) je funkce f_α dána předpisem

$$f_\alpha(x_1, x_2) = \begin{cases} 0 & \text{pokud } x_1 = x_2 = 0, \\ 1 & \text{jinak.} \end{cases}$$

Tato booleovská funkce se označuje jako ***disjunkce*** nebo ***logický součet***. Příbuzná funkce ***konjunkce*** (***logický součin***) má hodnotu 1, právě když oba její argumenty jsou rovny 1. Také konjunkci lze realizovat jako booleovskou funkci f_β nějaké formule β, například formule

$$\beta \;\equiv\; (\neg(A_1 \to (\neg A_2))). \tag{2.3}$$

(Viz cvičení 2.2.2.)

Vedeni tímto pozorováním můžeme pro lepší srozumitelnost formulí, se kterými budeme pracovat, zavést dodatečné logické spojky $\wedge$ pro konjunkci a $\vee$ pro disjunkci. Tyto spojky *nepřidáváme* do jazyka $\mathcal{L}_V$, ale definujeme je jako neformální zkratky. Jsou-li φ, ψ libovolné formule, položíme

$$\begin{aligned} (\varphi \vee \psi) &\;\equiv\; ((\neg\varphi) \to \psi), \\ (\varphi \wedge \psi) &\;\equiv\; (\neg(\varphi \to (\neg\psi))). \end{aligned}$$

Ekvivalence je booleovská funkce dvou proměnných

$$e(x_1, x_2) = 1, \quad \text{právě když } x_1 = x_2.$$

Pro tuto funkci zavedeme logickou spojku $\leftrightarrow$, a to předpisem

$$\varphi \leftrightarrow \psi \;\equiv\; ((\varphi \to \psi) \wedge (\psi \to \varphi)).$$

Význačné místo ve výrokové logice zaujímají ***tautologie***: formule, které jsou pravdivé při každém ohodnocení. Příkladem tautologie je formule

$$(A_0 \to A_0).$$

Protipólem tautologií jsou ***kontradikce***, formule nepravdivé při každém ohodnocení.

Definujme ***teorii*** jako libovolnou množinu formulí. Pojem pravdivosti lze rozšířit i na teorie: řekneme, že teorie T je ***pravdivá*** (***splněna***) při ohodnocení v, je-li při tomto ohodnocení pravdivá každá formule $\tau \in T$. Formule φ ***vyplývá*** z teorie T, psáno

$$T \vDash \varphi,$$

pokud φ je pravdivá pří každém ohodnocení ν, při němž je pravdivá teorie T. Všimněme si (cvičení 2.2.5), že φ je tautologií, právě když vyplývá z prázdné teorie $\emptyset$. Místo $\emptyset \vDash \varphi$ píšeme také $\vDash \varphi$.

Splnitelná je teorie, která je pravdivá při alespoň jednom ohodnocení.

Cvičení

► **2.2.1.** Určete booleovskou funkci realizovanou formulemi:

(a) $(A_1 \to ((\neg A_2) \to (\neg A_1))$,

(b) $(A_1 \to (A_2 \to A_1))$.

► **2.2.2.** Ověřte, že booleovská funkce realizovaná formulí (2.3) je logický součin.

► **2.2.3.** Ukažte, že každá booleovská funkce je realizována nějakou formulí.

► **2.2.4.** Najděte tautologii obsahující tři různé atomické podformule.

► **2.2.5.** Dokažte, že tautologie jsou právě formule, které vyplývají z prázdné teorie.

2.3 Odvozování

Jazyk $\mathcal{L}_V$ obsahuje následující tři ***schémata axiomů***:

(Ax1)

$$\varphi \to (\psi \to \varphi)$$

(Ax2)

$$(\varphi \to (\psi \to \sigma)) \to ((\varphi \to \psi) \to (\varphi \to \sigma))$$

(Ax3)

$$(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$$

Dosazením libovolných formulí za symboly φ, ψ, σ do některého schématu vznikne ***axiom*** jazyka $\mathcal{L}_V$.

Pozorování 2.2. *Každý axiom jazyka $\mathcal{L}_V$ je tautologie.*

Důkaz. K důkazu stačí pro každé schéma axiomů sestavit tabulku pravdivostních hodnot v závislosti na hodnotách dosazovaných formulí φ, ψ resp. σ. Pro schéma (Ax1) například dostáváme tabulku

φ	ψ	$\psi \to \varphi$	$\varphi \to (\psi \to \varphi)$
0	0	1	1
0	1	0	1
1	0	1	1
1	1	1	1

Ověření pro zbylá schémata ponecháváme na cvičení 2.3.1. □

V jazyce $\mathcal{L}_V$ je k dispozici jediné ***odvozovací pravidlo***, tzv. *modus ponens* (MP):

z formulí φ a $(\varphi \to \psi)$ lze odvodit formuli ψ.

Odvození formule φ v teorii T je konečná posloupnost formulí $\varphi_1, \varphi_2, \ldots, \varphi_n$ taková, že $\varphi_n = \varphi$ a pro každé $k \leq n$ platí:

(1) $\varphi_k \in T$ (takovým prvkům odvození se říká ***premisy***),

(2) φ_k je axiom, nebo

(3) φ_k lze odvodit z nějakých formulí φ_i a φ_j, kde $i, j < k$, pomocí pravidla *modus ponens*.

Místo 'odvození v teorii T' také budeme říkat krátce T-***odvození***. Formule φ je ***odvoditelná*** v teorii T (psáno $T \vdash \psi$), pokud existuje nějaké její T-odvození. Platí-li $\emptyset \vdash \varphi$ (tj. má-li formule φ odvození, ve kterém se nevyskytují žádné premisy), píšeme $\vdash \varphi$.

Věta 2.3 (Věta o korektnosti)**.** *Nechť T je teorie a φ formule taková, že $T \vdash \varphi$. Potom $T \vDash \varphi$.*

Důkaz. Indukcí podle délky nejkratšího T-odvození $\sigma_1, \ldots, \sigma_n$ formule φ. Pokud $n = 1$, pak φ je axiom nebo premisa (prvek teorie T). Je-li φ axiom, je to podle pozorování 2.2 tautologie, a tedy platí $T \vDash \varphi$. Pokud $\varphi \in T$, pak triviálně z definice plyne $T \vDash \varphi$.

Můžeme tedy předpokládat, že $n \geq 2$. Protože uvažované odvození je nejkratší možné, formule φ vznikla aplikací pravidla MP na nějaké formule σ_k, σ_ℓ, kde $k, \ell < n$. Bez újmy na obecnosti je tedy formule σ_ℓ tvaru $\sigma_k \to \varphi$. Formule σ_k a σ_ℓ mají kratší T-odvození než φ, takže platí

$$T \vDash \sigma_k,$$
$$T \vDash \sigma_k \to \varphi.$$

Z definice pravdivosti plyne $T \vDash \varphi$. Tím je důkaz proveden. □

Lemma 2.4. *Pro libovolné formule* φ, χ *platí*

$$\{\chi, \neg\chi\} \vdash \varphi.$$

Důkaz. Následující posloupnost je odvozením formule φ v teorii $\{\chi, \neg\chi\}$. U každého řádku je vpravo uvedeno, proč jeho zařazení odpovídá definici odvození: údaj jako (Ax1) nebo (Ax3) označuje axiom vzniklý podle příslušného schématu, údaj typu (MP $i + j$) pak formuli získanou pomocí pravidla *modus ponens* z formulí s čísly (i) a (j). Premisy jsou označeny symbolem (Prem).

(1) $\neg\chi \to (\neg\varphi \to \neg\chi)$ (Ax1)

(2) $\neg\chi$ (Prem)

(3) $\neg\varphi \to \neg\chi$ (MP 1+2)

(4) $(\neg\varphi \to \neg\chi) \to (\chi \to \varphi)$ (Ax3)

(5) $\chi \to \varphi$ (MP 3+4)

(6) χ (Prem)

(7) φ (MP 5+6)

□

Lemma 2.5. *Pro každou formuli* φ *platí*

$$\vdash \varphi \to \varphi.$$

Důkaz. Následující posloupnost formulí je odvozením formule $\varphi \to \varphi$:

(1) $(\varphi \to ((\varphi \to \varphi) \to \varphi)) \to ((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi))$ (Ax2)

(2) $\varphi \to ((\varphi \to \varphi) \to \varphi)$ (Ax1)

(3) $(\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)$ (MP 1+2)

(4) $\varphi \to (\varphi \to \varphi)$ (Ax1)

(5) $\varphi \to \varphi$ (MP 3+4)

□

Věta 2.6 (Věta o dedukci)**.** *Nechť* T *je teorie a* φ, ψ *jsou formule. Pak platí*

$$T \vdash \varphi \to \psi \quad \textit{právě když} \quad T + \varphi \vdash \psi.$$

Důkaz. '$\Rightarrow$': Libovolné odvození formule $\varphi \to \psi$ v teorii T je i odvozením v teorii $T+\varphi$. Přidáme-li k němu premisu φ a použijeme-li pravidlo MP na formule $\varphi \to \psi$ a φ, dostaneme odvození formule ψ v teorii $T+\varphi$.

'$\Leftarrow$': Implikaci zprava doleva dokážeme indukcí přes délku nejkratšího odvození formule ψ v teorii $T+\varphi$. Má-li ψ odvození délky 1, pak je to premisa z teorie $T+\varphi$ nebo axiom. Předpokládejme nejprve, že $\psi \in T$ nebo ψ je axiom. Pak následující odvození je odvozením formule $\varphi \to \psi$ v teorii T.

(1) $\psi \to (\varphi \to \psi)$ (Ax1)

(2) ψ (Prem)

(3) $\varphi \to \psi$ (MP 1+2)

Zbývá možnost, že $\varphi \equiv \psi$. V tomto případě podle lemmatu 2.5 platí dokonce $\vdash \varphi \to \varphi$, a tedy také $T \vdash \varphi \to \psi$.

Pro důkaz indukčního kroku předpokládejme, že nejkratší odvození formule ψ v teorii $T+\varphi$ je $\sigma_1, \ldots, \sigma_n$ (kde $n \geq 2$ a $\sigma_n \equiv \psi$), a že pro každou formuli ψ', která má v teorii $T+\varphi$ odvození délky menší než n, platí $T \vdash \varphi \to \psi'$.

Z minimality odvození $\sigma_1, \ldots, \sigma_n$ plyne, že formule $\sigma_n \equiv \psi$ vznikla aplikací pravidla MP na nějaké formule σ_k a σ_ℓ, kde $k, \ell < n$. Můžeme tedy předpokládat, že formule σ_ℓ je tvaru

$$\sigma_\ell \equiv \sigma_k \to \psi.$$

Protože σ_k a σ_ℓ mají v teorii $T+\varphi$ kratší odvození než formule ψ, lze pro ně použít indukční předpoklad, ze kterého plyne

$$T \vdash \varphi \to \sigma_k,$$
$$T \vdash \varphi \to (\sigma_k \to \psi).$$

Hledané odvození formule ψ v teorii T získáme následovně: vezmeme odvození formule $\varphi \to \sigma_k$, připojíme odvození formule $\varphi \to (\sigma_k \to \psi)$ a nakonec následující odvození:

(1) $(\varphi \to (\sigma_k \to \psi)) \to ((\varphi \to \sigma_k) \to (\varphi \to \psi))$ (Ax2)

(2) $(\varphi \to \sigma_k) \to (\varphi \to \psi)$ (MP)

(3) $\varphi \to \psi$ (MP)

Našli jsme odvození formule $\varphi \to \psi$ v teorii T. □

Lemma 2.7 (Tranzitivita implikace)**.** *Pro všechny formule* φ, ψ, σ *platí*

$$\{\varphi \to \psi, \psi \to \sigma\} \vdash \varphi \to \sigma.$$

Důkaz. Podle věty 2.6 stačí ukázat, že v teorii $\{\varphi \to \psi, \psi \to \sigma, \varphi\}$ je odvoditelná formule σ. To je snadné:

(1) $\varphi \to \psi$ (Prem)

(2) φ (Prem)

(3) ψ (MP 1+2)

(4) $\psi \to \sigma$ (Prem)

(5) σ (MP 3+4)

□

Tvrzení 2.8. *Pro každou formuli φ platí*

$$\vdash \neg\neg\varphi \to \varphi.$$

Důkaz. Podle lemmatu 2.4 platí

$$\{\neg\neg\varphi, \neg\varphi\} \vdash \neg\neg\neg\varphi.$$

Z věty 2.6 dostáváme první člen následujícího $\emptyset$-odvození:

(1) $\neg\neg\varphi \to (\neg\varphi \to \neg\neg\neg\varphi)$ (věta 2.6)

(2) $(\neg\varphi \to \neg\neg\neg\varphi) \to (\neg\neg\varphi \to \varphi)$ (Ax3)

(3) $\neg\neg\varphi \to \varphi$ (lemma 2.7)

□

Cvičení

► **2.3.1.** Dokažte pozorování 2.2.

► **2.3.2.** Dokažte, že pro každou formuli φ

$$\vdash \varphi \to \neg\neg\varphi.$$

► **2.3.3.** Dokažte, že pro všechny formule φ, ψ platí

$$\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi),$$
$$\vdash (\neg\varphi \to \psi) \to (\neg\psi \to \varphi),$$
$$\vdash (\varphi \to \neg\psi) \to (\psi \to \neg\varphi).$$

2.4 Úplnost

Množina formulí (teorie) T je ***nekonzistentní***, pokud pro nějakou formuli χ platí

$$T \vdash \chi \quad \text{a zároveň} \quad T \vdash \neg\chi.$$

V opačném případě je T ***konzistentní***.

V nekonzistentní teorii je možné odvodit libovolnou formuli:

Pozorování 2.9. *Nechť T je nekonzistentní teorie a ψ libovolná formule. Potom*

$$T \vdash \psi.$$

Důkaz. Podle lemmatu 2.4 platí $\{\chi, \neg\chi\} \vdash \psi$. □

Lemma 2.10. *Pokud $T \nvdash \neg\varphi$, pak teorie $T+\varphi$ je konzistentní.*

Důkaz. Dejme tomu, že teorie $T+\varphi$ je nekonzistentní. Uvažme libovolnou formuli ψ, pro kterou platí $\vdash \psi$. Podle pozorování 2.9 je $T+\varphi \vdash \neg\psi$, takže z věty 2.6 plyne $T \vdash \varphi \to \neg\psi$ a tedy $T \vdash \psi \to \neg\varphi$. Použitím pravidla MP dostáváme

$$T \vdash \neg\varphi,$$

což je spor s předpokladem. □

Lemma 2.11. *Všechny formule jazyka výrokové logiky je možné seřadit do posloupnosti $\sigma_1, \sigma_2, \ldots$.*

Důkaz. Přiřadíme každému symbolu abecedy jeho kód podle následujícího předpisu:

$\neg$	$\to$	$($	$)$	A_0	A_1	A_2	$\ldots$
1	2	3	4	5	6	7	$\ldots$

Výška $\ell(\varphi)$ formule φ je součet kódů všech symbolů ve formuli φ (násobné výskyty počítáme vícekrát). Při řazení formulí do posloupnosti $\sigma_1, \sigma_2, \ldots$ nejprve probíráme formule s výškou 1, poté s výškou 2, atd. Formule se stejnou výškou řadíme lexikograficky. Vzhledem k tomu, že formulí s omezenou výškou je konečně mnoho, objeví se ve výsledné posloupnosti každá formule. □

Konzistentní teorie T je ***maximálně konzistentní***, pokud pro každou formuli φ je buďto $\varphi \in T$ nebo $\neg\varphi \in T$.

Tvrzení 2.12. *Každou konzistentní teorii T je možné rozšířit na maximálně konzistentní teorii $S \supseteq T$.*

Důkaz. Uvažme všechny formule v pořadí $\sigma_1, \sigma_2, \ldots$ daném lemmatem 2.11. Budeme definovat posloupnost teorií $T = S_0 \subseteq S_1 \subseteq S_2 \subseteq \ldots$, a to následovně:

$$S_{i+1} = \begin{cases} S_i + \sigma_i & \text{pokud } S_i \nvdash \neg\sigma_i, \\ S_i & \text{jinak.} \end{cases} \tag{2.4}$$

Konečně položíme

$$S = \bigcup_{i \geq 0} S_i.$$

Tvrdíme především, že S je konzistentní teorie. Kdyby nebyla, bylo by možné v S odvodit spornou formuli. Odvození je ale konečné, a tak všechny jeho premisy musí být obsaženy již v některé teorii S_i. Ta je však konzistentní, což plyne z opakovaného použití lemmatu 2.10.

Dále musíme dokázat, že S je maximálně konzistentní. Dejme tomu, že pro nějakou formuli $\sigma_i \notin S$ je $S + \sigma_i$ konzistentní. Pak jistě $\neg\sigma_i \notin S$. Formule $\neg\sigma_i$ se rovněž vyskytuje v naší posloupnosti, dejme tomu jako formule σ_j. Jediným důvodem pro $\sigma_j \notin S_{j+1}$ je, že $S_j \vdash \neg\sigma_j$. Pak ale $S \vdash \neg\neg\sigma_i$ a tím pádem $S \vdash \sigma_i$. Na druhou stranu z $\sigma_i \notin S_{i+1}$ plyne $S_i \vdash \neg\sigma_i$, a tedy $S \vdash \neg\sigma_i$. Teorie S by tedy musela být nekonzistentní, což jsme vyloučili. Tím je důkaz proveden. □

Tvrzení 2.13. *Nechť S je maximálně konzistentní teorie. Pak funkce ν_S, která každé formuli přiřazuje hodnotu 0 nebo 1 podle předpisu*

$$\nu_S(\varphi) = 1 \quad \textit{právě když} \quad \varphi \in S,$$

je ohodnocení.

Důkaz. Musíme ověřit, že $\neg\varphi \in S$ právě když $\varphi \notin S$, a obdobné tvrzení pro implikaci $\varphi \to \psi$. Snadný důkaz ponecháváme na cvičení 2.4.2. □

Nyní již můžeme přikročit k důkazu věty o úplnosti.

Věta 2.14 (Věta o úplnosti)**.** *Pokud pro teorii T a formuli φ platí $T \models \varphi$, pak*

$$T \vdash \varphi.$$

Důkaz. Můžeme předpokládat, že T je konzistentní teorie, jinak není co dokazovat. Nechť $T \nvdash \varphi$. Podle lemmatu 2.10 je teorie $T + \neg\varphi$ konzistentní, takže tvrzení 2.12 umožňuje ji rozšířit na maximálně konzistentní teorii S. Ta určuje ohodnocení ν_S, při němž je splněna teorie $T + \neg\varphi$. Jinými slovy, ν_S splňuje teorii T, ale nesplňuje formuli φ. Je tedy 'svědkem', že platí $T \nvDash \varphi$, což jsme právě chtěli dokázat. □

Důležitým důsledkem věty o úplnosti je věta o kompaktnosti. O kompaktnosti obecně hovoříme v situacích, kdy lze na určitou vlastnost nekonečného objektu usoudit z toho, zda ji mají jeho konečné podobjekty.

Věta 2.15 (Věta o kompaktnosti)**.** *Teorie je splnitelná, právě když je každá její konečná podmnožina splnitelná.*

Důkaz. Netriviální implikace směřuje zprava doleva a dá se přeformulovat takto: Každá nesplnitelná teorie T obsahuje nějakou konečnou nesplnitelnou podteorii T′.

Je-li T nesplnitelná, pak $T \models \chi$, kde χ je negace libovolné tautologie. Podle věty o úplnosti je také $T \vdash \chi$. Odvození formule χ obsahuje konečný počet premis; nechť teorie T′ je právě množina těchto premis. Potom $T' \vdash \chi$ a podle věty o korektnosti $T' \models \chi$, takže i konečná teorie T′ je nesplnitelná. □

Cvičení

► **2.4.1.** Ukažte, že pro maximálně konzistentní teorii S je

$$S \vdash \varphi \quad \text{právě když} \quad \varphi \in S.$$

► **2.4.2.** Ukažte, že pro maximálně konzistentní teorii S platí

$$\begin{aligned} \neg\varphi \in S \quad &\text{právě když} \quad \varphi \notin S, \\ \varphi \to \psi \in S \quad &\text{právě když} \quad \varphi \notin S \text{ nebo } \psi \in S. \end{aligned}$$

Kapitola 3

Predikátová logika

3.1 Jazyk

Pro jazyk vymezíme především následující pojmy: symboly, termy a formule.

Symboly jazyka $\mathcal{L}$ predikátové logiky prvního řádu jsou:

(i) proměnné pro objekty: $x, y, z, x_0, x_1, \ldots,$

(ii) logické spojky: $\neg$ a $\rightarrow$,

(iii) obecný kvantifikátor: $\forall$,

(iv) pomocné symboly: $($, $)$,

(v) symbol pro rovnost: $=$,

(vi) konstanty,

(vii) funkční symboly,

(viii) predikátové symboly.

Poslední tři množiny symbolů (***mimologické symboly***) mohou být i prázdné. Pro každý funkční a predikátový symbol je dáno přirozené číslo $n \geq 1$, jeho ***četnost***. Říkáme, že jde o n-ární symbol.

Termy jazyka $\mathcal{L}$ jsou definovány následovně:

(1) každá proměnná x_i je term,

(2) každá konstanta c je term,

(3) pokud f je n-ární funkční symbol a $t_1, \ldots, t_n$ jsou termy, pak $f(t_1, \ldots, t_n)$ je term.

Formule jazyka $\mathcal{L}$ jsou definovány takto:

(1) Pokud P je n-ární predikátový symbol a $t_1, \ldots, t_n$ jsou termy, pak $P(t_1, \ldots, t_n)$ je (***atomická***) formule.

(2) Jsou-li t_1, t_2 termy, pak $t_1 = t_2$ je (***atomická***) formule.

(3) Jsou-li φ, ψ formule, pak $\neg\varphi$ a $\varphi \to \psi$ jsou formule.

(4) Je-li φ formule a x proměnná, pak $(\forall x)\ \varphi$ je formule.

Teorie T v jazyce $\mathcal{L}$ je libovolná množina formulí jazyka $\mathcal{L}$. O tomto jazyku budeme hovořit jako o ***jazyku teorie*** $\mathcal{L}$ a budeme jej označovat symbolem $\mathcal{L}(T)$. (Považujeme tedy jazyk za součást teorie a formálně bychom teorii definovali jako uspořádanou dvojici složenou z jazyka a množiny jejích formulí.)

Také v predikátové logice zavedeme logické spojky $\wedge$, $\vee$ a $\leftrightarrow$, a to stejně jako v odstavci 2.1. Kromě toho zavedeme ještě ***existenční kvantifikátor*** $\exists$ předpisem

$$(\exists x)\ \varphi \quad \equiv \quad \neg(\forall x)\ (\neg\varphi).$$

Výskyt proměnné x ve formuli φ je ***vázaný***, je-li součástí nějaké podformule tvaru $(\forall x)\ \psi$. V opačném případě je tento výskyt ***volný***. Proměnná x je ***volná*** ve formuli φ, má-li v ní volný výskyt. Formule je ***uzavřená***, není-li v ní žádná proměnná volná.

3.2 Pravdivost formulí

Ve výrokové logice nebylo obtížné definovat například pojem 'splnitelné' formule — je to taková formule, která je splněna při nějakém ohodnocení výrokových proměnných hodnotami 0 a 1. Interpretace formulí v predikátové logice ale přináší jednu potíž. Abychom mohli vyhodnotit atomické formule (nebot'o to hlavně jde), je třeba vědět, jaké *možné hodnoty* můžeme přisoudit jednotlivým proměnným.

Definice 3.1. ***Struktura*** $\mathcal{M}$ pro jazyk $\mathcal{L}$ má následující součásti:

(1) neprázdnou množinu M, označovanou jako ***nosič*** $|\mathcal{M}|$ realizace $\mathcal{M}$,

(2) pro každou konstantu c jazyka $\mathcal{L}$ obsahuje prvek

$$c_{\mathcal{M}} \in M,$$

(3) pro každý n-ární funkční symbol f jazyka $\mathcal{L}$ obsahuje funkci

$$f_{\mathcal{M}} : M^n \to M,$$

(4) pro každý n-ární predikátový symbol P jazyka $\mathcal{L}$ obsahuje relaci

$$P_{\mathcal{M}} \subseteq M^n.$$

Říkáme také, že $\mathcal{M}$ je ***struktura*** pro jazyk $\mathcal{L}$. ***Ohodnocení*** ve struktuře $\mathcal{M}$ je zobrazení e, které každé proměnné x_i jazyka $\mathcal{L}$ přiřadí prvek $e(x_i) \in |\mathcal{M}|$. Je-li t libovolný term, pak jeho ***hodnota*** $t[e]$ při ohodnocení e je definována následovně:

$$t[e] = \begin{cases} c_{\mathcal{M}} & \text{pokud } t \text{ je konstanta } c, \\ e(x_i) & \text{pokud } t \text{ je proměnná } x_i, \\ f_{\mathcal{M}}(t_1[e], \ldots, t_n[e]) & \text{pokud } t \text{ je tvaru } f(t_1, \ldots, t_n), \text{ kde } f \text{ je } n\text{-ární funkční symbol a } t_1, \ldots, t_n \text{ jsou termy.} \end{cases}$$

Je-li e ohodnocení, x proměnná a $m \in |\mathcal{M}|$, pak symbol $e_{x \mapsto m}$ označuje ohodnocení, které proměnné x přiřazuje hodnotu m a každé z ostatních proměnných y hodnotu $e(y)$.

Budeme nyní definovat, kdy je formule φ ***pravdivá v*** $\mathcal{M}$ ***při ohodnocení*** e. Tento vztah symbolicky označujeme zápisem $\mathcal{M} \models \varphi[e]$. Definice v závislosti na tvaru formule φ určuje následující tabulka.

φ je tvaru…	kde…	$\mathcal{M} \models \varphi[e]$, právě když…
$s = t$	s, t jsou termy	$s[e] = t[e]$
$P(t_1, \ldots, t_n)$	P je n-ární predikátový symbol a $t_1, \ldots, t_n$ jsou termy	n-tice $(t_1[e], \ldots, t_n[e])$ je prvkem relace $P_{\mathcal{M}}$
$\neg\psi$	ψ je formule	$\mathcal{M} \not\models \psi[e]$
$\psi \to \sigma$	ψ, σ jsou formule	$\mathcal{M} \not\models \psi[e]$ nebo $\mathcal{M} \models \sigma[e]$
$(\forall x)\, \psi$	x je proměnná a ψ je formule	pro každé $m \in \|\mathcal{M}\|$ je $\mathcal{M} \models \psi[e_{x \mapsto m}]$

Formule φ je ***pravdivá ve struktuře*** $\mathcal{M}$, je-li pravdivá v $\mathcal{M}$ při každém ohodnocení e.

Model teorie T je struktura pro jazyk $\mathcal{L}(T)$, v níž je pravdivá každá formule teorie T. V takovém případě píšeme $\mathcal{M} \models T$. Formule φ ***vyplývá*** z teorie T, psáno $T \models \varphi$, je-li φ pravdivá v každém modelu teorie T. Zápis $\models \varphi$ opět znamená $\emptyset \models \varphi$. Formule φ, pro něž je $\models \varphi$, jsou ***tautologie***.

Cvičení

► **3.2.1.** Nechť φ je formule, x proměnná a e ohodnocení ve struktuře $\mathcal{M}$. Odvoďte z definice, kdy platí

$$\mathcal{M} \models ((\exists x)\, \varphi)[e].$$

► **3.2.2.** Nechť $\mathcal{M}$ je struktura pro jazyk $\mathcal{L}$ a e je ohodnocení v $\mathcal{M}$. Dokažte, že pokud term t neobsahuje proměnnou x, pak pro libovolné $c \in |\mathcal{M}|$ platí

$$t[e] = t[e_{x \mapsto c}].$$

► **3.2.3.** Ukažte, že pro danou strukturu $\mathcal{M}$, formuli φ a proměnnou x platí

$$\mathcal{M} \vDash \varphi, \quad \text{právě když} \quad \mathcal{M} \vDash (\forall x)\, \varphi$$

► **3.2.4.** Nechť e je ohodnocení ve struktuře $\mathcal{M}$ pro jazyk $\mathcal{L}$ a nechť formule φ je uzavřená. Dokažte, že pro uzavřenou formuli φ platí

$$\mathcal{M} \vDash \varphi \quad \text{právě když} \quad \mathcal{M} \vDash \varphi[e].$$

► **3.2.5.** Nechť e je ohodnocení ve struktuře $\mathcal{M}$ pro jazyk $\mathcal{L}$ a nechť proměnná x není volná ve formuli φ.

(a) Dokažte indukcí podle složitosti formule φ, že pro každé $c \in |\mathcal{M}|$ platí

$$\mathcal{M} \vDash \varphi[e] \quad \text{právě když} \quad \mathcal{M} \vDash \varphi[e_{x \mapsto c}].$$

(b) Odvoďte, že

$$\mathcal{M} \vDash \varphi[e] \quad \text{právě když} \quad \mathcal{M} \vDash ((\forall x)\, \varphi)[e].$$

3.3 Substituce

V predikátové logice se můžeme setkat s několika druhy substituce:

- substituce formulí jazyka $\mathcal{L}$ za atomické formule výrokové logiky,
- substituce termu za proměnnou v jiném termu,
- substituce termu za proměnnou ve formuli.

V tomto odstavci postupně probereme základní vlastnosti těchto operací.

Začněme substitucí za atomické formule jazyka výrokové logiky $\mathcal{L}_V$. Nechť τ je formule v jazyce $\mathcal{L}_V$, která obsahuje atomické formule $A_{i_1}, \ldots, A_{i_\ell}$ (a žádné jiné). Nechť dále $\alpha_{i_1}, \ldots, \alpha_{i_\ell}$ jsou libovolné formule v jazyce predikátové logiky $\mathcal{L}$. Symbolem

$$\tau(A_{i_1}/\alpha_{i_1}, \ldots, A_{i_\ell}/\alpha_{i_\ell})$$

označíme formuli jazyka $\mathcal{L}$ vzniklou záměnou všech výskytů každé formule A_{i_k} ve formuli τ za formuli α_{i_k}.

Je-li například

$$\begin{aligned} \tau &\equiv (A_2 \to A_3), \\ \alpha_2 &\equiv (y < 0), \\ \alpha_3 &\equiv ((\forall x)\, x \neq x), \end{aligned}$$

pak $\tau(A_2/\alpha_2, A_3/\alpha_3)$ je formule

$$((y < 0) \to ((\forall x)\, x \neq x)).$$

Následující lemma ukazuje, že poznatky o tautologiích, získané v kapitole 2, se nám budou hodit i nadále.

Lemma 3.2. *Nechť τ je tautologie výrokové logiky $\mathcal{L}_V$ obsahující právě atomické formule $A_{i_1}, \ldots, A_{i_\ell}$, a nechť $\alpha_{i_1}, \ldots, \alpha_{i_\ell}$ jsou libovolné formule v jazyce predikátové logiky $\mathcal{L}$. Potom formule $\tau(A_{i_1}/\alpha_{i_1}, \ldots, A_{i_\ell}/\alpha_{i_\ell})$ je tautologie.*

Důkaz. Cvičení 3.3.1. □

Jestliže s, t jsou termy a x je proměnná, pak $s(x/t)$ je term, vzniklý nahrazením každého výskytu proměnné x v termu s termem t. Například pro

$$\begin{aligned} s &\equiv (x \cdot x), \\ t &\equiv (1 + 1) \end{aligned}$$

je term $s(x/t)$ roven termu $((1 + 1) \cdot (1 + 1))$. Pro hodnoty termu vzniklého substitucí platí následující jednoduché pozorování.

Lemma 3.3. *Nechť $\mathcal{M}$ je struktura pro jazyk $\mathcal{L}$ a e je ohodnocení v $\mathcal{M}$. Pro libovolnou proměnnou x a termy s, t platí*

$$s(x/t)[e] = s[e_{x \mapsto t[e]}].$$

Důkaz. Cvičení 3.3.2. □

Zbývá nám nejdůležitější typ substituce, kterým je substituce termu do formule. Je-li φ formule jazyka $\mathcal{L}$, x proměnná a t term, potom $\varphi(x/t)$ je formule vzniklá nahrazením každého *volného* výskytu proměnné x ve formuli φ termem t.

Například pro volbu

$$\begin{aligned} \varphi &\equiv ((\forall y)\, y = x) \wedge ((\forall x)\, x = x), \\ t &\equiv (1 + 1), \end{aligned}$$

je formule $\varphi(x/t)$ rovna formuli

$$((\forall y)\, y = (1 + 1)) \wedge ((\forall x)\, x = x).$$

Zde je ovšem třeba dát pozor na jedno nebezpečí. Od substituce přirozeně očekáváme, že je-li formule φ pravdivá v nějaké struktuře $\mathcal{M}$, pak zde bude pravdivá i formule $\varphi(x/t)$, a to pro libovolné x a t. To ale nemusí být vždy pravda: pokud do formule

$$((\exists y)\, \neg(y = x))$$

substituujeme za proměnnou x term y, výsledkem je formule

$$((\exists y)\, \neg(y = y)).$$

První formule je pravdivá v libovolné struktuře $\mathcal{M}$ s alespoň dvouprvkovou nosnou množinou, ale druhá formule je v každé struktuře nepravdivá. Problém spočívá v tom, že proměnná y, kterou jsme do formule φ dosadili, se substitucí ocitla v podformuli tvaru $((\forall y)\ldots)$. Původní volný výskyt proměnné x se tedy změnil ve vázaný výskyt proměnné y.

Abychom se podobným potížím vyhnuli, definujeme pojem substituovatelný term. Term t je ***substituovatelný*** za proměnnou x do formule φ, pokud žádný volný výskyt proměnné x není součástí podformule tvaru $(\forall y)\, \sigma$, kde y je libovolná proměnná s výskytem v termu t. S tímto omezením má substituce požadované vlastnosti:

Tvrzení 3.4. *Nechť $\mathcal{M}$ je struktura pro jazyk $\mathcal{L}$, φ formule, e ohodnocení v $\mathcal{M}$ a t term substituovatelný do φ za proměnnou x. Platí následující:*

$$\textit{pokud } \mathcal{M} \vDash \varphi, \quad \textit{pak} \quad \mathcal{M} \vDash \varphi(x/t).$$

Toto tvrzení je přímým důsledkem následujícího obecnějšího lemmatu:

Lemma 3.5. *Nechť $\mathcal{M}$ je struktura pro jazyk $\mathcal{L}$, φ formule, e ohodnocení v $\mathcal{M}$ a t term substituovatelný do φ za proměnnou x. Pak*

$$\mathcal{M} \vDash \varphi(x/t)[e], \quad \textit{právě když} \quad \mathcal{M} \vDash \varphi[e_{x\mapsto t[e]}]. \tag{3.1}$$

Důkaz. Důkaz provedeme indukcí podle složitosti formule φ. Je-li φ tvaru $s = t$ nebo $P(t_1, \ldots, t_n)$, pak tvrzení jednoduše plyne z lemmatu 3.3. Případ, že φ je tvaru $\neg\psi$ nebo $\psi \to \sigma$, je rovněž jednoduchý, vztah (3.1) plyne z indukčního předpokladu.

Zbývá probrat případ, že φ je tvaru $(\forall z)\, \psi$, kde z je nějaká proměnná. Je-li z totožná s x, pak φ neobsahuje žádný volný výskyt proměnné x, takže $\varphi(x/t) \equiv \varphi$. Na levé straně vztahu (3.1) tak dostáváme $\mathcal{M} \vDash \varphi[e]$, což je podle cvičení 3.2.5(a) ekvivalentní s pravou stranou.

Nechť tedy z a x jsou různé proměnné. Podle definice pravdivosti je levá strana vztahu (3.1) ekvivalentní tvrzení, že pro každé $c \in |\mathcal{M}|$ platí

$$\mathcal{M} \vDash \psi(x/t)[e_{z\mapsto c}],$$

což je podle indukčního předpokladu totéž co

$$\mathcal{M} \vDash \psi[(e_{z\mapsto c})_{x\mapsto t[e_{z\mapsto c}]}]. \tag{3.2}$$

Podívejme se na pravou stranu vztahu (3.1). Ta je (rovněž podle definice pravdivosti) ekvivalentní s tvrzením, že pro každé $c \in |\mathcal{M}|$ je

$$\mathcal{M} \vDash \psi[(e_{x\mapsto t[e]})_{z\mapsto c}]. \tag{3.3}$$

Tvrdíme, že ohodnocení ve vztazích (3.2) a (3.3) jsou pro každou volbu $c \in |\mathcal{M}|$ totožná. Pokud ne, liší se pouze v hodnotě proměnné x, která činí pro první ohodnocení $t[e_{z\mapsto c}]$ a pro druhé ohodnocení $t[e]$. Protože však term t je substituovatelný za x, neobsahuje žádný výskyt proměnné z a podle cvičení 3.2.2 platí $t[e_{z\mapsto c}] = t[e]$. Obě ohodnocení jsou tedy opravdu shodná. Z toho plyne ekvivalence vztahů (3.2) a (3.3), čímž je důkaz proveden. □

Cvičení

► **3.3.1.** Dokažte lemma 3.2.

► **3.3.2.** Dokažte lemma 3.3.

3.4 Odvozování

Predikátová logika má následující ***schémata axiomů***. Axiomy (pro daný jazyk predikátové logiky $\mathcal{L}$) z nich vzniknou nahrazením symbolů φ, ψ, σ libovolnými formulemi jazyka $\mathcal{L}$.

(Ax1)

$$\varphi \to (\psi \to \varphi)$$

(Ax2)

$$(\varphi \to (\psi \to \sigma)) \to ((\varphi \to \psi) \to (\varphi \to \sigma))$$

(Ax3)

$$(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$$

(Ax4) Axiom substituce:

$$((\forall x)\ \varphi) \to \varphi(x/t)$$

za předpokladu, že t je term *substituovatelný* za proměnnou x do formule φ.

(Ax5) Axiom distribuce:

$$((\forall x)\,(\varphi \to \psi)) \to (\varphi \to (\forall x)\,\psi)$$

za předpokladu, že proměnná x *není* ve formuli φ volná.

(Ax6)

$$t = t$$

(Ax7)

$$(t_1 = s_1 \wedge \ldots \wedge t_n = s_n) \to (P(t_1, \ldots, t_n) \to P(s_1, \ldots, s_n))$$

(Ax8)

$$(t_1 = s_1 \wedge \ldots \wedge t_n = s_n) \to (f(t_1, \ldots, t_n) = f(s_1, \ldots, s_n))$$

V posledních třech schématech je P libovolný n-ární predikátový symbol (včetně symbolu $=$), f je libovolný n-ární funkční symbol a t, t_i, s_i jsou termy.

Dedukční pravidla predikátové logiky jsou dvě:

(MP) *Modus ponens.*

Z formulí $\varphi \to \psi$ a φ je odvoditelná formule ψ.

(GEN) *Generalizace.*

Z formule φ je odvoditelná formule $(\forall x)\,\varphi$, kde x je libovolná proměnná.

Nechť φ je formule jazyka $\mathcal{L}$ a T je teorie, pro kterou platí $\mathcal{L}(T) \subseteq \mathcal{L}$. ***Odvození formule*** φ ***v teorii*** T ***a jazyce*** $\mathcal{L}$ je konečná posloupnost formulí jazyka $\mathcal{L}$ s vlastností, že

(1) poslední člen posloupnosti je φ,

(2) každý člen posloupnosti je axiom pro jazyk $\mathcal{L}$, formule z teorie T, nebo jej lze odvodit z předchozích členů posloupnosti použitím některého odvozovacího pravidla.

Ve speciálním případě $\mathcal{L} = \mathcal{L}(\mathsf{T})$ hovoříme pouze o ***odvození v teorii*** T.

Má-li formule φ odvození v T, je v T ***odvoditelná*** a píšeme pak $\mathsf{T} \vdash \varphi$. Ve vzácných případech, kdy je třeba specifikovat i jazyk odvození, používáme notaci $\mathsf{T} \vdash_{\mathcal{L}} \varphi$.

Je-li v T odvoditelná nějaká formule χ i její negace $\neg\chi$, je T ***nekonzistentní*** (***sporná***). V opačném případě je ***konzistentní***. Zápis $\vdash \varphi$ znamená, že φ má odvození v teorii $\emptyset$ a v minimálním jazyce, který zahrnuje všechny symboly obsažené ve formuli φ.

Lemma 3.6. *Nechť τ je tautologie výrokové logiky obsahující atomické formule $A_{i_1}, \ldots, A_{i_\ell}$ (a žádné jiné), a nechť $\alpha_{i_1}, \ldots, \alpha_{i_\ell}$ jsou libovolné formule v jazyce predikátové logiky $\mathcal{L}$. Potom formule $\tau(A_{i_1}/\alpha_{i_1}, \ldots, A_{i_\ell}/\alpha_{i_\ell})$ je odvoditelná v jazyce $\mathcal{L}$.*

Důkaz. Z věty o úplnosti výrokové logiky existuje odvození $\sigma_1, \ldots, \sigma_n$ formule τ v jazyce $\mathcal{L}_V$. Nechť množina atomických formulí, které se objevují v některé formuli σ_j, ale nikoli v τ, je $\{A_{i_{\ell+1}}, \ldots, A_{i_k}\}$. Zvolme libovolnou formuli β jazyka $\mathcal{L}$, třeba $\beta \equiv (x = x)$. Nahradíme-li každou formuli σ_k formulí

$$\sigma_k(A_{i_1}/\alpha_{i_1}, \ldots, A_{i_\ell}/\alpha_{i_\ell}, A_{i_{\ell+1}}/\beta, \ldots, A_{i_k}/\beta),$$

získáme odvození formule $\tau(A_{i_1}/\alpha_{i_1}, \ldots, A_{i_\ell}/\alpha_{i_\ell})$ v jazyce $\mathcal{L}$. □

Věta 3.7 (Věta o korektnosti)**.** *Nechť T je teorie v jazyce predikátové logiky $\mathcal{L}$ a σ je formule. Platí, že*

$$\textit{pokud} \quad \mathsf{T} \vdash \sigma, \quad \textit{pak} \quad \mathsf{T} \models \sigma.$$

Důkaz. Nechť $\mathcal{M}$ je model teorie T. Předpokládáme, že $\mathsf{T} \vdash \sigma$ a chceme ukázat, že $\mathcal{M} \models \sigma$. Postupujeme indukcí podle délky nejkratšího odvození formule σ v teorii T (označme ji k).

Pokud $k = 1$, σ je buďto premisa nebo axiom predikátové logiky. Pro premisu tvrzení platí z triviálních důvodů, nechť tedy σ je axiom. Axiomy (Ax1)–(Ax3) jsou v $\mathcal{M}$ pravdivé díky lemmatu 3.2.

Nechť σ je axiom (Ax4), tedy formule tvaru

$$((\forall x)\ \varphi) \to \varphi(x/t),$$

kde term t je substituovatelný do φ za x. Dejme tomu, že pro dané ohodnocení e je

$$\mathcal{M} \models (\forall x)\ \varphi[e]. \tag{3.4}$$

Chceme ukázat, že platí $\mathcal{M} \models \varphi(x/t)[e]$. Kdyby ne, pak podle lemmatu 3.5 platí $\mathcal{M} \not\models \varphi[e_{x \mapsto t[e]}]$. To je ale ve sporu s předpokladem (3.4), ze kterého plyne, že pro každé $c \in |\mathcal{M}|$ je $\mathcal{M} \models \varphi[e_{x \mapsto c}]$. Tím je případ axiomu (Ax4) uzavřen.

Uvažme nyní případ, že σ je axiom (Ax5), neboli formule tvaru

$$((\forall x)\ (\varphi \to \psi)) \to (\varphi \to ((\forall x)\ \psi)).$$

Pro spor předpokládejme, že pro nějaké ohodnocení e platí

$$\begin{aligned} &\mathcal{M} \models ((\forall x)\,(\varphi \to \psi))[e], \quad \text{ale} \\ &\mathcal{M} \not\models (\varphi \to ((\forall x)\,\psi))[e]. \end{aligned} \tag{3.5}$$

Podle druhého z těchto předpokladů platí $\mathcal{M} \models \varphi[e]$, ale existuje prvek $c \in |\mathcal{M}|$, pro který je

$$\mathcal{M} \not\models \psi[e_{x\mapsto c}].$$

Z předpokladu (3.5) dostaneme

$$\mathcal{M} \models (\varphi \to \psi)[e_{x\mapsto c}],$$

což spolu s předcházejícím vztahem implikuje

$$\mathcal{M} \not\models \varphi[e_{x\mapsto c}].$$

To je však podle cvičení 3.2.5(a) spor s výše zjištěným faktem, že $\mathcal{M} \models \varphi[e]$, neboť proměnná x není ve formuli φ volná. Důkaz pro axiom (Ax5) je tak proveden.

U axiomů rovnosti — (Ax6) až (Ax8) — je situace opět jednodušší. Například axiom $t = t$ je ve struktuře $\mathcal{M}$ pravdivý prostě proto, že vyhodnocením termu t na levé a na pravé straně rovnosti dostaneme totožný prvek $t[e]$ množiny $|\mathcal{M}|$. U zbylých dvou axiomů je argument podobný.

Uvažme nyní indukční krok. Není-li formule σ axiom ani premisa, lze ji získat pomocí odvozovacího pravidla z formulí, které se vyskytují v nejkratším odvození formule σ. U pravidla (MP) argumentujeme stejně jako v důkazu věty 2.3. Zbývá tedy pravidlo (GEN). Nechť σ je tvaru $(\forall x)\,\psi$, kde ψ je formule s kratším odvozením v T, a tedy lze použít indukční předpoklad, ze kterého plyne $\mathcal{M} \models \psi$. Podle cvičení 3.2.3 je rovněž $\mathcal{M} \models (\forall x)\,\psi$, tj. formule σ je pravdivá v $\mathcal{M}$. □

Uzávěr formule φ je uzavřená formule $\tilde{\varphi}$ tvaru

$$(\forall x_{i_1}) \ldots (\forall x_{i_n})\,\varphi,$$

kde $i_1 < \cdots < i_n$ a $x_{i_1}, \ldots, x_{i_n}$ jsou všechny volné proměnné ve formuli φ. Následující snadná věta ukazuje, že formule φ a $\tilde{\varphi}$ mají z hlediska odvoditelnosti podobné vlastnosti.

Věta 3.8 (Věta o uzávěru)**.** *Nechť T je teorie a φ formule. Pak*

$$T \vdash \varphi \quad \textit{právě když} \quad T \vdash \tilde{\varphi}.$$

Důkaz. Cvičení 3.4.1. □

I v predikátové logice platí věta o dedukci, ale s dodatečným předpokladem uzavřenosti formule. Následující příklad ukazuje, proč je tento předpoklad nutný.

Nechť $\mathcal{L}$ je jazyk s jediným mimologickým symbolem, kterým je konstanta 0, a nechť $\mathcal{M}$ je nějaká struktura pro jazyk $\mathcal{L}$ s dvouprvkovým nosičem. Pak platí

$$\mathcal{M} \not\models (x = 0 \to (\forall x)\,(x = 0)).$$

Podle věty 3.7 je tedy

$$\not\vdash (x = 0 \to (\forall x)\,(x = 0)).$$

Na druhou stranu jedním použitím pravidla generalizace dostáváme

$$\{x = 0\} \vdash (\forall x)\,(x = 0).$$

Věta 3.9 (Věta o dedukci)**.** *Pro* uzavřenou *formuli* φ *platí*

$$T \vdash (\varphi \to \psi) \quad \textit{právě když} \quad T + \varphi \vdash \psi.$$

Důkaz. Důkaz je z podstatné části shodný s důkazem věty 2.6. Hlavní rozdíl spočívá v tom, že u důkazu implikace '$\Leftarrow$' je nutno uvážit kromě odvozovacího pravidla (MP) také pravidlo (GEN). Tento argument probereme podrobněji, ostatní detaily důkazu ponecháváme jako cvičení 3.4.2.

Implikaci '$\Leftarrow$' dokazujeme indukcí podle délky nejkratšího odvození $\sigma_1, \ldots, \sigma_n$ formule ψ v teorii $T + \varphi$. Případ $n = 1$ a případ, že ψ vznikla použitím pravidla (MP), se dokazují stejně jako u věty 2.6. Předpokládejme proto, že formule ψ vznikla použitím pravidla (GEN) na nějakou formuli σ_k ($k < n$) a je tedy tvaru $(\forall x)\,\sigma_k$, kde x je nějaká proměnná.

Protože σ_k má kratší odvození v teorii $T + \varphi$ než formule ψ, podle indukčního předpokladu má formule $\varphi \to \sigma_k$ odvození v teorii T. Připojme k němu odvození

(1) $(\forall x)\,(\varphi \to \sigma_k)$ (GEN)

(2) $((\forall x)\,(\varphi \to \sigma_k)) \to (\varphi \to (\forall x)\,\sigma_k))$ (Ax5)

(3) $\varphi \to (\forall x)\,\sigma_k$ (MP)

a získáme odvození formule $\varphi \to \psi$ v teorii T. Všimněme si, že axiom (Ax5) lze použít jen díky tomu, že proměnná x není volná v uzavřené formuli φ. □

Cvičení

► **3.4.1.** Nechť T je teorie, φ formule a x proměnná. Ukažte, že

$$T \vdash \varphi \quad \text{právě když} \quad T \vdash (\forall x)\,\varphi.$$

Odvoďte větu 3.8.

► **3.4.2.** Dokažte podrobně větu 3.9.

3.5 Věta o konstantách

Pro důkaz věty o úplnosti predikátové logiky budeme potřebovat technické tvrzení, které nám umožní obohatit jazyk $\mathcal{L}$ o novou konstantu c a zaručí, že konzistentnost teorie v jazyce $\mathcal{L}$ se neporuší přidáním formule nového jazyka.

Označme symbolem $\mathcal{L} + c$ jazyk, vzniklý přidáním konstanty c k jazyku $\mathcal{L}$ (který ji neobsahuje). Je-li φ formule jazyka $\mathcal{L} + c$ a z je proměnná, pak formuli $\varphi(c/z)$ (jazyka $\mathcal{L}$) definujeme jako výsledek nahrazení každého výskytu konstanty c proměnnou z. Podobně pro term t jazyka $\mathcal{L} + c$ je $t(c/z)$ term jazyka $\mathcal{L}$ získaný záměnou každého výskytu konstanty c za proměnnou z.

Lemma 3.10. *Nechť φ je formule, ve které se nevyskytuje proměnná x. Má-li formule φ odvození v teorii T a jazyce $\mathcal{L}$, pak má i takové odvození (v T a $\mathcal{L}$), ve kterém se nevyskytuje proměnná x.*

Důkaz. Cvičení 3.5.1. □

Věta 3.11 (Věta o konstantách)**.** *Nechť T je teorie v jazyce $\mathcal{L}$, který neobsahuje konstantu c, a nechť φ je formule jazyka $\mathcal{L} + c$, v níž se nevyskytuje proměnná z. Má-li formule φ odvození v teorii T a v jazyce $\mathcal{L} + c$, pak formule $\varphi(c/z)$ má odvození v teorii T a v jazyce $\mathcal{L}$.*

Důkaz. Důkaz je jednoduchý, ale vzhledem k důležitosti věty jej probereme podrobně. Podle lemmatu 3.10 existuje odvození $\sigma_1, \ldots, \sigma_n$ formule φ v jazyce $\mathcal{L}+c$ a teorii T, které neobsahuje proměnnou z. Ukážeme, že nahrazením každé formule σ_i formulí $\sigma_i(c/z)$ získáme odvození formule $\varphi(c/z)$ v jazyce $\mathcal{L}$ a v teorii T. K tomu podle definice odvození stačí ověřit, že každá formule $\sigma_k(c/z)$ je axiom pro jazyk $\mathcal{L}$, prvek teorie T, nebo ji lze odvodit pomocí pravidla (MP) nebo (GEN) z formulí tvaru $\sigma_i(c/z)$, kde $i < k$. Rozlišíme tři případy podle typu formule σ_k a ukážeme, že $\sigma_k(c/z)$ je stejného typu.

(a) Formule σ_k je axiom pro jazyk $\mathcal{L} + c$, tj. vznikla dosazením formulí resp. termů jazyka $\mathcal{L} + c$ do schémat (Ax1)–(Ax8). Formule $\sigma_i(c/z)$, kterou získáme, pokud místo každé formule ψ dosadíme formuli $\psi(c/z)$ a místo každého termu t dosadíme term $t(c/z)$, je tedy axiomem pro jazyk $\mathcal{L}$. (Všimněme si, že nahrazením konstanty c proměnnou z se neporuší podmínky u axiomů (Ax4) a (Ax5), protože proměnná z se nevyskytuje v žádné z formulí σ_i.)

(b) Formule σ_k patří do teorie T. Taková formule ovšem neobsahuje konstantu c a je totožná s formulí $\sigma_k(c/z)$, která tak rovněž patří do teorie T.

(c) Formuli σ_k lze získat z formulí tvaru σ_i ($i < k$) pomocí některého odvozovacího pravidla. Zde stačí nahlédnout, že provedené nahrazení zachovává aplikovatelnost odvozovacích pravidel. Jinými slovy, z formulí $\psi(c/z)$ a $(\psi \to \tau)(c/z)$ lze pomocí pravidla (MP) odvodit formuli $\tau(c/z)$ a podobné tvrzení platí i pro pravidlo (GEN). □

Cvičení

► **3.5.1.** Dokažte lemma 3.10.

3.6 Úplnost predikátové logiky

V tomto odstavci dokážeme větu o úplnosti predikátové logiky:

Věta 3.12 (Věta o úplnosti)**.** *Nechť* T *je teorie v jazyce* $\mathcal{L}$ *a* φ *je formule tohoto jazyka. Je-li* $T \models \varphi$*, potom* $T \vdash \varphi$*.*

Větu 3.12 dokážeme v jiné podobě. Budeme k tomu potřebovat analogii lemmatu 2.10 pro predikátovou logiku:

Lemma 3.13. *Nechť* T *je teorie a* φ *je formule jazyka* $\mathcal{L} \supset \mathcal{L}(T)$*. Pokud* $\neg\varphi$ *nemá odvození v teorii* T *a jazyce* $\mathcal{L}$*, pak teorie* $T+\varphi$ *je konzistentní.*

Důkaz. Nejprve ukážeme, že stačí uvažovat uzavřené formule φ. Podle věty 3.8 platí $T \nvdash \neg\varphi$, právě když $T \nvdash \neg\tilde{\varphi}$. Na druhé straně (rovněž podle věty 3.8) je teorie $T+\varphi$ konzistentní, právě když je konzistentní teorie $T+\tilde{\varphi}$. Opravdu tedy stačí dokázat lemma pro uzavřené formule.

V tomto případě projde v podstatě beze změny důkaz lemmatu 2.10. Uzavřenost formule φ je potřeba k tomu, aby bylo možné použít větu o dedukci. □

Pro důkaz věty o úplnosti je klíčový následující fakt:

Tvrzení 3.14. *Nechť* T *je konzistentní teorie v jazyce* $\mathcal{L}$*, který neobsahuje konstantu* c*, a nechť* φ *je formule jazyka* $\mathcal{L}+c$*. Potom teorie* $T+\sigma$ *v jazyce* $\mathcal{L}+c$ *je konzistentní, kde* σ *je formule*

$$((\exists x)\ \varphi) \to \varphi(x/c). \tag{3.6}$$

Důkaz. Dejme tomu, že teorie $T+\sigma$ je nekonzistentní. Podle lemmatu 3.13 je v teorii T a jazyce $\mathcal{L}+c$ odvoditelná formule $\neg\sigma$. Jinak řečeno, platí

$$T \vdash_{\mathcal{L}+c} ((\exists x)\ \varphi) \wedge \neg\varphi(x/c).$$

Tím pádem je v T a $\mathcal{L}+c$ odvoditelná formule $\neg\varphi(x/c)$. Podle věty 3.11 je v T a $\mathcal{L}$ odvoditelná formule $\neg\varphi(x/z)$, kde z je proměnná, která ve φ nemá výskyt. Snadným použitím axiomu substituce (pro dosazení x za z) dostaneme $T \vdash \neg\varphi$ a tedy rovněž

$$T \vdash (\forall x)\ \neg\varphi.$$

Přitom je však v T odvoditelná i formule $(\exists x)\ \varphi$, což je jiný zápis pro formuli $\neg(\forall x)\ \neg\varphi$. Vidíme, že T je v rozporu s předpokladem nekonzistentní. □

Místo věty 3.12 dokážeme následující větu:

Věta 3.15. *Každá konzistentní teorie má model.*

Jak z věty 3.15 plyne věta o úplnosti? Je-li $T \nvdash \varphi$, pak lze k teorii T konzistentně přidat formuli $\neg\varphi$ (viz lemma 3.13) a model konzistentní teorie $T \cup \{\neg\varphi\}$ dosvědčuje, že $T \nvdash \varphi$.

Stačí tedy dokázat větu 3.15. Jak najít model konzistentní teorie T? Pro přesnost řekněme, že v průběhu důkazu se ukáže potřeba předem rozšířit jazyk $\mathcal{L}$ o některé nové konstanty a teorii T o jisté nové formule. Zatím se však touto technickou záležitostí nebudeme zabývat.

Přesto začneme rozšířením teorie T, a to (podobně jako v důkazu věty o úplnosti výrokové logiky) na maximální konzistentní teorii S. (Připomeňme, že teorie je ***maximální konzistentní***, pokud pro každou formuli ψ obsahuje buď formuli ψ nebo $\neg\psi$.) Postup konstrukce teorie S je stejný jako u výrokové logiky: probíráme formule v pevném očíslování $\varphi_1, \varphi_2, \ldots$ a lze-li uvažovanou formuli φ_i přidat bez porušení konzistence, pak ji přidáme.

Důležitou vlastností teorie S je její uzavřenost na odvozování:

$$S \vdash \psi, \quad \text{právě když} \quad \psi \in S,$$

kde ψ je libovolná formule. Klíčovou myšlenkou důkazu je vytvořit hledaný model na základě syntaktických prvků samotného jazyka $\mathcal{L}$. Nosnou množinou modelu $\mathcal{M}$ bude množina všech ***uzavřených termů*** jazyka $\mathcal{L}$, tj. termů neobsahujících proměnné. Předpis pro interpretaci konstant a funkčních symbolů v modelu $\mathcal{M}$ je nejpřirozenější možný. Pro konstantní symbol c položíme

$$c_{\mathcal{M}} = c.$$

Pro n-ární funkční symbol f a prvky $t_1, \ldots, t_n \in |\mathcal{M}|$ (což jsou uzavřené termy) bude

$$f_{\mathcal{M}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n).$$

(další uzavřený term).

Pozorování 3.16. *Hodnota* $t[e]$ *uzavřeného termu* t *při libovolném ohodnocení* e *je* t.

K interpretaci predikátových symbolů se dostaneme za chvíli.

Má-li $\mathcal{M}$ být model teorie S, musí pro každou formuli $\varphi \in S$ a libovolné ohodnocení e platit $\mathcal{M} \vDash \varphi[e]$. Z maximality teorie S ale plyne i opačný směr. Pokud totiž $\varphi \notin S$, pak $\neg\varphi \in S$, takže potřebujeme, aby pro každé e platilo $\mathcal{M} \vDash \neg\varphi[e]$, tj. ekvivalentně $\mathcal{M} \nvDash \varphi[e]$. V souhrnu tedy musíme zajistit, aby platil následující základní vztah:

$$\mathcal{M} \vDash \varphi, \quad \text{právě když} \quad \varphi \in S. \tag{3.7}$$

Pokud se nám to podaří, struktura $\mathcal{M}$ bude hledaným modelem teorie S. Jak interpretovat predikátové symboly? Nemáme na výběr. Je-li ψ uzavřená

atomická formule tvaru $P(t_1, \ldots, t_n)$, kde P je predikátový symbol a $t_1, \ldots, t_n$ jsou uzavřené termy, pak podle (3.7) a pozorování 3.16 potřebujeme, aby platilo

$$(t_1, \ldots, t_n) \in P_{\mathcal{M}}, \quad \text{právě když} \quad \psi \in S. \tag{3.8}$$

Tím je relace $P_{\mathcal{M}}$, která interpretuje predikátový symbol P, jednoznačně určena. (Symbol $=$ zatím uvažujme prostě jako jeden z predikátových symbolů; později se k němu vrátíme.) Co ale s atomickou formulí, která není uzavřená? Poněkud překvapivě se neuzavřenými formulemi vůbec nemusíme zabývat:

Lemma 3.17. *Nechť φ je libovolná formule a $\tilde{\varphi}$ její uzávěr. Potom*

$$\varphi \in S, \quad \textit{právě když} \quad \tilde{\varphi} \in S$$

a

$$\mathcal{M} \vDash \varphi \quad \textit{právě když} \quad \mathcal{M} \vDash \tilde{\varphi}.$$

Důkaz. Cvičení 3.6.1. □

Stačí nám tedy zajistit platnost vztahu (3.7) pro uzavřené formule. Zatím se nám to podařilo pro formule atomické. Dokazujme tedy vztah (3.7) indukcí přes složitost formule φ. Není-li atomická, musí být tvaru $\neg\psi$, $\psi \to \tau$ nebo $(\forall x)\,\tau$, kde ψ a τ jsou jednodušší formule a x je proměnná. Případ, kdy φ je $\neg\psi$, je zdárně ošetřen, protože klíčový vztah (3.7) jsme odvodili právě se zřetelem na negaci. Pokud φ je implikace $\psi \to \tau$, je situace přehledná. Platí totiž

$$\varphi \in S, \quad \text{právě když} \quad \psi \notin S \quad \text{nebo} \quad \tau \in S$$

(ze stejného důvodu jako u cvičení 2.4.2). Podobně pro ohodnocení e máme

$$\mathcal{M} \vDash \varphi[e], \quad \text{právě když} \quad \mathcal{M} \nvDash \psi[e] \quad \text{nebo} \quad \mathcal{M} \vDash \tau[e].$$

Z indukčního předpokladu a z faktu, že splněnost uzavřené formule ve struktuře nezávisí na ohodnocení (cvičení 3.2.4), plyne, že vztah (3.7) v tomto případě platí.

Poslední a nejtěžší případ je ten, ve kterém je formule φ tvaru $(\forall x)\,\psi$, přičemž ψ má nejvýše jednu volnou proměnnou (a to x). Předpokládejme nejprve, že platí $\varphi \in S$. Chceme ukázat, že pro libovolné ohodnocení e platí $\mathcal{M} \vDash \varphi[e]$, tj. $\mathcal{M} \vDash \psi[e_{x \mapsto t}]$, kde t je libovolný prvek množiny $|\mathcal{M}|$ (uzavřený term). S použitím axiomu substituce a pravidla MP odvodíme

$$S \vdash \psi(x/t),$$

z maximality pak $\psi(x/t) \in S$. Formule $\psi(x/t)$ je uzavřená, lze tedy použít indukční předpoklad, podle kterého je $\mathcal{M} \vDash \psi(x/t)[e]$ pro libovolné ohodnocení e. To podle lemmatu 3.5 znamená, že $\mathcal{M} \vDash \psi[e_{x \mapsto t}]$, čímž jsme dokázali jednu implikaci vztahu (3.7).

Nechť tedy naopak $\varphi \notin S$, tedy $\neg(\forall x)\ \psi \in S$. Potřebujeme dokázat, že $\mathcal{M} \not\models (\forall x)\,\psi$. K tomu je nutné najít uzavřený term t a ohodnocení e, pro které je $\mathcal{M} \not\models \psi[e_{x\mapsto t}]$, čili (podle lemmatu 3.5 a definice pravdivosti) $\mathcal{M} \models (\neg\psi(x/t))[e]$. Problém je v tom, že teorie S může obsahovat formuli tvaru $\neg(\forall x)\ \psi$, aniž by obsahovala jakoukoli formuli tvaru $\neg\psi(x/t)$.

Tato potíž se však dá obejít. Jak jsme naznačili na začátku důkazu, řešení vyžaduje předběžné rozšíření jazyka $\mathcal{L}$ a teorie (ještě před přechodem k teorii S). Konkrétně do jazyka $\mathcal{L}$ přidáme pro každou jeho uzavřenou formuli τ a pro každou proměnnou y speciální novou konstantu c (kterou v případě potřeby můžeme označit $c_{\tau,y}$) a novou formuli

$$((\exists y)\ \tau) \to \tau(y/c). \tag{3.9}$$

Konstanta c v této formuli 'dosvědčuje'[1] případnou pravdivost formule $(\exists x)\ \tau$. Podle tvrzení 3.14 každé takové rozšíření zachovává konzistentnost teorie. Tím pádem také výsledná teorie T', vzniklá přidáním všech formulí tvaru (3.9), je konzistentní (cvičení 3.6.2).

Nyní se přesvědčme, že nám uvedené rozšíření pomůže. Nechť $\neg(\forall x)\ \psi$ je ona problematická formule maximálně konzistentní teorie $S \supset T'$. Je snadné ukázat, že z formule $\neg(\forall x)\ \psi$ lze odvodit formuli $(\exists x)\ \neg\psi$ (cvičení 3.6.3). Platí tedy $(\exists x)\ \neg\psi \in S$. Zároveň teorie S obsahuje také formuli

$$((\exists x)\ \neg\psi) \to \neg\psi(x/c)$$

a tím pádem i formuli $\neg\psi(x/c)$. Ta je uzavřená a podle indukčního předpokladu platí $\mathcal{M} \models \neg\psi(x/c)[e]$. Podle lemmatu 3.5 pro libovolné ohodnocení e platí $\mathcal{M} \not\models \psi[e_{x\mapsto c}]$ a tedy $\mathcal{M} \not\models (\forall x)\,\psi$. K tomuto závěru jsme došli z předpokladu, že $(\forall x)\,\psi \notin S$. To znamená, že se nám podařilo dokázat vztah (3.7) i v posledním zbylém případě, kdy formule φ je tvaru $(\forall x)\ \psi$.

Našli jsme tedy model teorie T? Zatím ne tak docela. Poslední potíž představuje symbol $=$. Podle definice splňování totiž musí platit, že relace $=_{\mathcal{M}}$, která jej realizuje, obsahuje pouze dvojice (x, x), kde $x \in |\mathcal{M}|$. Teorie S, podle které jsme relace $P_{\mathcal{M}}$ vyráběli, ale může obsahovat i formule tvaru $s = t$, kde s a t jsou dva různé uzavřené termy. (V jazyce aritmetiky může jít třeba o formuli $0 + 0 = 0$.) Řešením je *ztotožnit* příslušné prvky struktury $\mathcal{M}$. Definujme na množině $|\mathcal{M}|$ relaci $\sim$ předpisem

$$s \sim t, \quad \text{právě když} \quad (s = t) \in S. \tag{3.10}$$

Není těžké ověřit, že $\sim$ je ekvivalence (viz cvičení 3.6.4). Hledaný model $\mathcal{M}'$ má nosnou množinu $|\mathcal{M}|/\sim$, jejíž prvky jsou třídy ekvivalence $\sim$. Stačí jen všude, kde jsme doposud uvažovali nějaký term t, místo toho hovořit o příslušné třídě ekvivalence $\sim$.

Shrňme tedy na závěr jednotlivé kroky důkazu věty 3.15:

[1] Teorie obohacená o formule tvaru (3.9) se v angličtině někdy označuje termínem *scapegoat theory*. Výraz *scapegoat* (obětní beránek) odkazuje na konstanty jako je c.

(1) Jazyk $\mathcal{L}$ obohatíme o nové konstanty $c_{\psi,y}$, kde ψ probíhá formule jazyka $\mathcal{L}$ a y probíhá proměnné. Do teorie přidáme formule tvaru (3.9). Výsledkem je jazyk $\mathcal{L}'$ a konzistentní teorie T'.

(2) Teorii T' rozšíříme na maximální konzistentní teorii S.

(3) Definujeme strukturu $\mathcal{M}'$ pro jazyk $\mathcal{L}'$, jejíž nosnou množinou je množina všech tříd ekvivalence $\sim$, definované vztahem (3.10) na množině všech uzavřených termů jazyka $\mathcal{L}'$. Realizace konstant a funkčních symbolů jazyka $\mathcal{L}'$ je definována přirozeným způsobem. Realizace predikátových symbolů je dána vztahem (3.8).

(4) Induktivně ověříme platnost vztahu (3.7), ze kterého vyplývá, že $\mathcal{M}'$ je modelem teorie S (a tedy i T). To je jednoduché pro atomické formule, negace a implikace. Pro kvantifikované formule je klíčovým bodem přítomnost formulí (3.9).

(5) Díky tomu, že uvažujeme třídy ekvivalence $\sim$, je správně realizován i predikát $=$.

Důkaz věty 3.15, a tedy i věty 3.12, je proveden. □

Cvičení

▶ **3.6.1.** Dokažte lemma 3.17.

▶ **3.6.2.** Dokažte, že teorie T' v důkazu věty o úplnosti (vzniklá přidáním všech formulí tvaru (3.9)) je konzistentní. (Postupujte jako u analogického důkazu pro maximálně konzistentní rozšíření S.)

▶ **3.6.3.** Ukažte, že

$$\{\neg(\forall x)\ \psi\} \vdash\ (\exists x)\ \neg\psi$$

▶ **3.6.4.** Dokažte, že relace $\sim$, definovaná vztahem (3.10), je ekvivalence.

Část II

Aritmetika

Kapitola 4

Přirozená čísla

4.1 Historie aritmetiky

...

4.2 Peanova aritmetika

Základní vlastnosti "přirozených čísel" zachycují *Peanovy postuláty*, poprvé formulované v roce 1879 R. Dedekindem:

(1) 0 je přirozené číslo,

(2) každé přirozené číslo x má následníka Sx,

(3) 0 není následníkem žádného přirozeného čísla,

(4) pokud $Sx = Sy$, pak $x = y$,

(5) je-li P nějaká vlastnost a platí-li

$$P(0) \wedge ((\forall n)\, P(n) \to P(Sn)),$$

potom platí $(\forall n)\, P(n)$.

Na těchto postulátech je založena tzv. *Peanova aritmetika* (PA), která je formalizací aritmetiky přirozených čísel. Vyjádříme ji jako teorii v rámci predikátové logiky 1. řádu v jazyce $\mathcal{L}_{\mathrm{PA}}$ se symboly 0 (konstanta), S (unární funkční symbol), $+$ a $\cdot$ (binární funkční symboly):

(P1) $Sx \neq 0$,

(P2) $Sx = Sy \to x = y$,

(P3) $x + 0 = x$,

(P4) $x + Sy = S(x + y)$,

(P5) $x \cdot 0 = 0$,

(P6) $x \cdot Sy = x \cdot y + x$,

(P7) je-li $\varphi(x)$ formule jazyka $\mathcal{L}_{\mathrm{PA}}$, pak formule

$$(\varphi(0) \wedge ((\forall x)\ \varphi(x) \to \varphi(Sx)) \to (\forall x)\ \varphi(x))$$

je axiomem PA.

Peanovy postuláty (1) a (2) jsou v Peanově aritmetice zahrnuty implicitně, postuláty (3) a (4) jako axiomy (P1) a (P2), a konečně postulát (5) jako schéma axiomů (P7).

Kapitola 5

Vyčíslitelnost

. . .

Kapitola 6

Gödelovy věty o neúplnosti

. . .

Část III

Teorie množin

Kapitola 7

Úvod

7.1 Začátky teorie množin

Teorii množin vytvořil v době po roce 1870 Georg Cantor. Představa množiny jako souboru objektů byla sice v historii matematiky běžná, Cantor byl však (s výjimkou českého matematika Bernarda Bolzana) prvním, kdo nahlížel soubor nekonečného množství objektů jako samostatně existující objekt.

Nová teorie množin brzy získala značnou popularitu, mimo jiné proto, že umožňovala převést nejrůznější odvětví matematiky na společný, jasně vymezený základ. Na počátku 20. století se ovšem ve slibné teorii objevily povážlivé trhliny v podobě řady ***paradoxů***, tedy tvrzení, která nejsou ani pravdivá, ani nepravdivá, a poukazují tak na to, že celá teorie je nekonzistentní.

Nejznámějším z množinových paradoxů je ***Russellův paradox***: Nechť $\mathfrak{m}$ je množina všech množin x s vlastností $x \notin x$. Platí $\mathfrak{m} \in \mathfrak{m}$? Pokud ano, mělo by podle definice být $\mathfrak{m} \notin \mathfrak{m}$, a ke stejnému sporu vede i druhá možnost.

Podobné problémy ukázaly nutnost precizovat a zpřísnit pravidla pro práci s množinami. Mezi různými pokusy o postavení teorie množin a celé matematiky na pevnější základ stojí na předním místě *Zermelo–Fraenkelova teorie množin* (1908–20), kterou se budeme zabývat v následujících kapitolách.

7.2 Axiomy teorie množin

V tomto odstavci začneme definovat ***množinové universum***, tedy svět, ve kterém množiny existují. Množiny jsou jediné objekty tohoto světa, neexistuje v něm nic kromě množin. Základní vztah, který mezi dvěma množinami může platit, je vztah ***náležení***: množina s může být ***prvkem*** množiny t. V takovém případě také říkáme, že množina t obsahuje množinu s. Každý prvek každé množiny je opět množina.

Vlastnosti množinového universa vymezují axiomy Zermelo–Fraenkelovy teorie množin, formulované v rámci predikátové logiky 1. řádu, v jazyce $\mathcal{L}_{\mathrm{ZF}}$

s jediným mimologickým symbolem $\in$. Jde o binární predikátový symbol pro vztah náležení (zápis $s \in t$ znamená, že množina s je prvkem množiny t).

V souladu s tím, že v množinovém universu existují jen množiny, může každá proměnná nabývat svou hodnotu jen mezi množinami. Zápis $(\exists x) \ldots$ tedy automaticky znamená "existuje *množina* x s vlastností $\ldots$". Někdy je ale vhodné uvažovat i o souboru množin s určitou vlastností, který sám množinou není. Příslušná vlastnost je vyjádřena formulí $\varphi(x)$ jazyka $\mathcal{L}_{\mathrm{ZF}}$. Soubor množin x, pro které je pravdivá formule $\varphi(x)$, označujeme zápisem

$$\{x : \varphi(x)\}.$$

Takový soubor označujeme jako ***třídu*** určenou formulí φ. Obecně nemusí být množinou, například pro formuli $x \notin x$ bychom v takovém případě narazili na Russellův paradox. Třídu, která není množinou, nazýváme ***vlastní třída***. Taková třída v množinovém universu *neexistuje*, jde jen o myšlenkový konstrukt. Nemůže být prvkem žádné množiny ani hodnotou žádné proměnné. Jde vlastně o alternativní pohled na formuli φ jazyka $\mathcal{L}_{\mathrm{ZF}}$.

Některé z dále uvedených axiomů (například axiom vydělení) tvrdí, že určité třídy *jsou* množinami. Pro takové případy se hodí následující zkratka. Zápis $\mathrm{Mn}\big(\{x : \varphi\}\big)$ znamená, že třída určená formulí φ je množinou. Definujeme jej vztahem

$$\mathrm{Mn}\big(\{x : \varphi\}\big) \;\equiv\; (\exists s)\,((\forall x)\,(x \in s \leftrightarrow \varphi(x)))$$

(kde s je proměnná neobsažená ve formuli φ). Je důležité, že tento zápis je jen zkratkou za formuli jazyka $\mathcal{L}_{\mathrm{ZF}}$.

První axiom Zermelo–Fraenkelovy teorie množin tvrdí, že existuje alespoň jedna množina:

Axiom 7.1 (Existence množin)**.**

$$(\exists x)\; x = x$$

Všimněme si, že rovnost $x = x$ platí pro každou množinu x díky jednomu z axiomů rovnosti, které jsou součástí predikátové logiky. Další z těchto axiomů implikuje, že jsou-li si množiny a a b rovny, pak mají tytéž prvky, tedy pro každou množinu x platí $x \in a$ právě když $x \in b$. Tzv. axiom extenzionality říká, že tato implikace platí i opačně:

Axiom 7.2 (Extenzionalita)**.**

$$s = t \quad \leftrightarrow \quad (\forall x)\,(x \in s \leftrightarrow x \in t)$$

Každá množina je tedy jednoznačně určena svými prvky.

Víme, že třída určená nějakou formulí φ nemusí být množinou. Následující schéma axiomů nicméně zaručuje, že pokud prvky, splňující vlastnost φ, vybíráme z určité množiny, pak výsledná třída je rovněž množinou.

Axiom 7.3 (Schéma vydělení)**.** *Nechť* φ *je formule jazyka* $\mathcal{L}_{\mathrm{ZF}}$*, neobsahující proměnnou* x*. Potom formule*

$$\mathrm{Mn}\big(\{x : x \in s \wedge \varphi(x)\}\big)$$

je axiom.

S použitím schématu vydělení můžeme definovat ***prázdnou množinu*** $\emptyset$, která nemá žádný prvek:

$$\emptyset := \{x : x \neq x\}.$$

Podle axiomu extenzionality je množina $\emptyset$ určena jednoznačně.

Dalším konstruktem, který lze díky schématu vydělení definovat, je ***průnik*** dvou množin s a t, který sestává ze všech jejich společných prvků:

$$s \cap t := \{x : x \in s \wedge x \in t\}.$$

Dvě množiny, jejichž průnik je prázdný, označujeme jako ***disjunktní*** množiny.

Následující axiom zaručuje, že pro libovolné množiny s a t existuje množina obsahující prvky s a t a žádné jiné. Jsou-li s a t různé, označujeme tuto množinu symbolem $\{s, t\}$, pro $s = t$ ji značíme $\{s\}$:

Axiom 7.4 (Axiom dvojice)**.**

$$\mathrm{Mn}\big(\{x : x = s \vee x = t\}\big)$$

.

Také zde (a u obou zbývajících axiomů v tomto oddílu) je jednoznačnost definované množiny zaručena axiomem extenzionality.

Oproti operaci průniku, kterou se nám podařilo definovat pomocí schématu vydělení, budeme pro sjednocení potřebovat speciální axiom. Místo sjednocení dvou množin $s \cup t$ zavedeme obecnější operaci ***sjednocení množiny***. Je-li m množina, pak její sjednocení $\bigcup m$ je třída všech množin x, které náleží do některého prvku množiny m. Axiom sjednocení říká, že $\bigcup m$ je množina:

Axiom 7.5 (Axiom sjednocení)**.**

$$\mathrm{Mn}\big(\{x : (\exists y)\, x \in y \wedge y \in m\}\big)$$

.

Sjednocení množin s a t můžeme s využitím axiomu dvojice definovat předpisem

$$s \cup t := \bigcup \{s, t\}.$$

Poslední z axiomů, které zavedeme v tomto odstavci, se týká podmnožin. Řekneme, že množina s je ***podmnožinou*** množiny t (psáno $s \subseteq t$), pokud každý prvek množiny s je prvkem množiny t. (Všimněme si, že tento vztah lze vyjádřit formulí jazyka $\mathcal{L}_{\mathrm{ZF}}$ — viz cvičení 7.2.2.) Třída všech podmnožin libovolné množiny s, kterou označujeme $\mathcal{P}(s)$, je podle axiomu potence množinou:

Axiom 7.6 (Axiom potence)**.**

$$\mathrm{Mn}\big(\{x : x \subseteq s\}\big)$$

.

V dalších kapitolách zavedeme postupně ještě zbylé čtyři axiomy Zermelo–Fraenkelovy teorie množin:

- axiom nekonečna,
- schéma nahrazení,
- axiom výběru,
- axiom regularity.

Cvičení

▶ **7.2.1.** Dokažte, že ***třída všech množin***,

$$V := \{x : x = x\},$$

není množinou.

▶ **7.2.2.** Vyjádřete výrok "množina s je podmnožinou množiny t" v jazyce $\mathcal{L}_{\mathrm{ZF}}$ (samozřejmě bez použití symbolu $\subseteq$).

▶ **7.2.3.** Jaké prvky má množina $\{\emptyset\}$? Jaké má podmnožiny?

7.3 Relace

V minulém oddílu jsme pro libovolné množiny x, y definovali dvojici $\{x, y\}$. ***Uspořádaná dvojice*** $\langle x, y\rangle$ je množina

$$\langle x, y\rangle = \{\{x\}, \{x, y\}\}.$$

Pozorování 7.7. *Pokud* $\langle x, y\rangle = \langle x', y'\rangle$*, pak* $x = x'$ *a* $y = y'$*.*

Kartézský součin $s \times t$ množin s a t je množina všech uspořádaných dvojic $\langle x, y\rangle$, kde $x \in s$ a $y \in t$. Jak plyne z následujícího tvrzení, taková množina skutečně existuje:

Tvrzení 7.8. *Třída*

$$s \times t = \{z : (\exists x)\,(\exists y)\, z = \langle x, y\rangle \wedge x \in s \wedge y \in t\}$$

je množinou.

Důkaz. Je-li $x \in s$ a $y \in t$, pak $\{x\}$ a $\{x, y\}$ jsou podmnožiny množiny $s \cup t$, a tedy prvky množiny $\mathcal{P}(s \cup t)$. Uspořádaná dvojice $\langle x, y\rangle$ je pak prvkem množiny $\mathcal{P}(\mathcal{P}(s \cup t))$. Dokázali jsme, že každý prvek z třídy $s \times t$ je prvkem množiny $\mathcal{P}(\mathcal{P}(s \cup t))$. Podle schématu vydělení je $s \times t$ množina. □

Relace z množiny s do množiny t je libovolná podmnožina kartézského součinu $s \times t$. ***Definiční obor*** relace $r \subseteq s \times t$ je množina

$$\mathrm{dom}(r) = \{x : (\exists y)\ \langle x, y\rangle \in r\}.$$

Obor hodnot relace r je množina

$$\mathrm{rng}(r) = \{y : (\exists x)\ \langle x, y\rangle \in r\}.$$

(Je opět třeba dokázat, že $\mathrm{dom}(r)$ a $\mathrm{rng}(r)$ jsou množiny — viz cvičení 7.3.1.)

Zúžení relace r na množinu s je relace

$$r \mid s = r \cap (s \times \mathrm{rng}(r)).$$

Obraz množiny s při relaci r je množina

$$r[x] = \mathrm{rng}(r \mid s).$$

Pomocí pojmu relace lze zavést další hojně používané pojmy, jako jsou zobrazení, uspořádání a ekvivalence. Připomeňme si příslušné definice.

Zobrazení je relace f, pro kterou platí, že pro každý prvek $x \in \mathrm{dom}(f)$ existuje ***právě jeden*** prvek $y \in \mathrm{rng}(f)$ s vlastností $\langle x, y\rangle \in f$. Tento prvek označujeme jako ***obraz*** prvku x a píšeme $y = f(x)$. Je-li $\mathrm{dom}(f) = r$ a $\mathrm{rng}(f) \subseteq s$, říkáme, že f je zobrazení množiny r do množiny s (psáno $f : r \to s$). Takové zobrazení je ***prosté***, pokud obrazy každých dvou různých prvků jsou různé, a je ***na***, pokud $\mathrm{rng}(f) = s$. Zobrazení $f : r \to s$, které je prosté a na, nazýváme ***bijekce*** mezi množinou r a s.

Pojem uspořádání budeme v tomto textu používat pouze v následující, méně obvyklé variantě. ***Ostré uspořádání*** na množině s je relace $r \subseteq s \times s$, která má následující vlastnosti:

(1) pro každé $x \in s$ je $\langle x, x\rangle \notin r$,

(2) pro každé $x, y, z \in s$ platí

$$\langle x, y\rangle \in r \wedge \langle y, z\rangle \in r \to \langle x, z\rangle \in r.$$

Obecně každou relaci s vlastností (1) označujeme jako ***antireflexívní*** a relaci s vlastností (2) jako ***tranzitivní***.

Ekvivalence na množině s je relace $r \subseteq s \times s$ s vlastnostmi:

(1) pro každé $x \in s$ je $\langle x, x\rangle \in r$ (***reflexivita***),

(2) pro každé $x, y \in s$ je $\langle x, y\rangle \in r \to \langle y, x\rangle \in r$ (***symetrie***),

(3) r je tranzitivní.

Cvičení

► **7.3.1.** Dokažte, že definiční obor a obor hodnot relace r jsou množiny. (Použijte množinu $\bigcup r$ a schéma vydělení.)

► **7.3.2.** Dokažte, že každé ostré uspořádání r je ***antisymetrické***, tj. platí

$$\langle x, y\rangle \in r \to \langle y, x\rangle \notin r.$$

► **7.3.3.** Nechť r je ekvivalence na množině s. Definujme ***třídu prvku*** $x \in s$ jako množinu

$$[x] = \{y : \langle x, y\rangle \in r\}.$$

Dokažte, že třídy $[x]$, kde $x \in s$, tvoří ***rozklad*** množiny s, tedy že každé dvě z nich jsou buďto shodné nebo disjunktní, a že sjednocením všech tříd $[x]$ je celá množina s.

Kapitola 8

Přirozená čísla v teorii množin

Naším záměrem v této kapitole je definovat přirozená čísla v teorii množin: zkonstruovat množiny, které je budou zastupovat, a zavést pro ně obvyklé početní operace sčítání a násobení.

8.1 Konstrukce přirozených čísel

Idea naší definice přirozených čísel je založena na von Neumannově reprezentaci přirozených čísel pomocí množin:

$$\begin{aligned}
&0 = \emptyset,\\
&1 = 0 \cup \{0\} = \{\emptyset\},\\
&2 = 1 \cup \{1\} = \{\emptyset, \{\emptyset\}\},\\
&3 = 2 \cup \{2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},\\
&\quad\vdots\\
&n = n \cup \{n\},\\
&\quad\vdots
\end{aligned}$$

Pomocí tohoto předpisu lze libovolnému přirozenému číslu n přiřadit množinu, která jej reprezentuje. Neumožňuje však například definovat množinu *všech* přirozených čísel. Proto přistoupíme k definici přirozených čísel trochu jinak.

Pro libovolnou množinu a definujme jejího ***následníka*** předpisem

$$a^+ = a \cup \{a\}.$$

Množina m je ***induktivní***, pokud

(1) $\emptyset \in m$,

(2) pro každé $a \in m$ platí $a^+ \in m$.

Axiom 8.1 (Axiom nekonečna)**.**

$$(\exists m)\,(\forall a)\,(\emptyset \in m \wedge a \in m \to a^+ \in m)$$

Protože průnik induktivních množin je induktivní, můžeme definovat nejmenší induktivní množinu:

$$\omega = \bigcap \{m : m \text{ je induktivní}\}.$$

(Třída $\{m : m \text{ je induktivní}\}$ nemusí být množinou, ale schéma vydělení umožňuje pracovat i s průnikem vlastní třídy.)

Prvky množiny ω označujeme jako ***přirozená čísla*** a místo $\emptyset$ píšeme 0.

8.2 Vlastnosti přirozených čísel

Věta 8.2 (Princip indukce)**.** *Pokud pro formuli* $\varphi(x)$ *platí*

(1) $\varphi(\emptyset)$,

(2) $(\forall n \in \omega)\,(\varphi(n) \to \varphi(n^+))$,

pak platí také $(\forall n \in \omega)\ \varphi(n)$.

Důkaz. Definujme množinu

$$b = \{n \in \omega : \text{platí } \varphi(n)\}.$$

Podle předpokladů je b induktivní. Protože ω je *nejmenší* induktivní množina, platí $\omega \subseteq b$. Formule $\varphi(n)$ tedy platí pro všechna přirozená čísla. □

Věta 8.3. *Nechť* $n \in \omega$.

(a) pokud $m \in n$, *pak* $m \in \omega$ *(prvky každého přirozeného čísla jsou přirozená čísla),*

(b) pokud $k \in m \in n$, *pak* $k \in n$.

Důkaz. (a) Definujme formuli

$$\varphi(n) \;\equiv\; (\forall m \in n)\ m \in \omega.$$

Ukážeme, že $\varphi(n)$ splňuje podmínky věty 8.2. Formule $\varphi(0)$ platí triviálně. Nechť $\varphi(n)$ a $m \in n^+$. Mohou nastat dva případy. Pokud $m \in n$, pak díky $\varphi(n)$ platí $m \in \omega$. Pokud $m = n$, je rovněž $m \in \omega$. Část (b) se dokazuje podobnou indukcí přes n (cvičení 8.2.1). □

Lemma 8.4. *Pro* $n \in \omega$ *platí*

$$n \notin n.$$

Důkaz. Indukcí podle n. Položme

$$\varphi(n) \;\equiv\; n \notin n.$$

Zřejmě platí $\varphi(0)$. Nechť platí $\varphi(n)$ a neplatí $\varphi(n^+)$. Nutně $n^+ \in n^+$. Rozlišíme dva případy. Buďto $n^+ \in n$, a pak podle věty 8.3(b) $n \in n$ ve sporu s předpokladem $\varphi(n)$. V opačném případě je $n \cup \{n\} = n^+ = n$, takže rovněž $n \in n$. Tím je důkaz proveden. □

Cvičení

▶ **8.2.1.** Dokažte větu 8.3(b).

▶ **8.2.2.** Dokažte, že větu 8.3 lze stručně vyjádřit takto: pokud $n \in \omega$, pak

$$\bigcup n \subseteq n \subseteq \omega.$$

8.3 Uspořádání

Na množině ω definujeme ostré uspořádání $<$ předpisem

$$m < n \iff m \subsetneq n.$$

S využitím věty 8.3(a) toto uspořádání definujeme i na každém přirozeném čísle $n \in \omega$ jako restrikci uspořádání $<$ na podmnožinu $n \subseteq \omega$.

Tvrzení 8.5. *Pro* $m, n \in \omega$ *platí*

$$m < n \quad \textit{právě když} \quad m \in n.$$

Důkaz. Směr "$\Leftarrow$" je v podstatě dokázán: pokud $m \in n$, pak z věty 8.3(b) plyne $m \subseteq n$ a z lemmatu 8.4 pak $m < n$.

Zbývá dokázat směr "$\Rightarrow$". Nechť $\varphi(n)$ je formule

$$\varphi(n) \;\equiv\; (\forall m \in \omega)\,(m \subsetneq n \to m \in n).$$

Dokážeme pomocí věty 8.2, že platí $(\forall n)\,\varphi(n)$. Množina 0 nemá žádnou vlastní podmnožinu, proto $\varphi(0)$ platí triviálně. Dejme tomu, že platí $\varphi(n)$ a $m \subsetneq n^+$. Chceme dokázat $m \notin n^+$.

Je-li $m \subsetneq n$, pak z indukčního předpokladu $m \in n$, a tedy $m \in n^+$. Podobně pro $m = n$ je $m \in n^+$. Všechny ostatní množiny $m \subsetneq n^+$ obsahují prvek n. Ovšem $n \in m$ podle věty 8.3(b) znamená $n \subsetneq m$, a tedy $n^+ \subseteq m$. To je spor s předpokladem $m \subsetneq n^+$. □

Věta 8.6. *Uspořádání $<$ na množině ω je* **lineární**, *tj. pro $m, n \in \omega$ platí právě jedna z možností*

$$m < n, \qquad m = n, \qquad m > n.$$

Důkaz. Více než jedna z těchto možností nemůže platit z triviálních důvodů. To, že platí *alespoň* jedna z nich, dokážeme indukcí přes n. Nechť $\varphi(n)$ je formule

$$\varphi(n) \;\equiv\; (\forall m \in \omega)\,(m \subseteq n \vee n \subseteq m).$$

Stačí dokázat, že pro všechna $n \in \omega$ platí $\varphi(n)$. Použijeme větu 8.2.

Formule $\varphi(0)$ platí triviálně. Předpokládejme tedy, že platí $\varphi(n)$, ale neplatí $\varphi(n^+)$. Uvažme $m \in \omega$ s vlastností

$$(m \not\subseteq n^+) \wedge (n^+ \not\subseteq m). \tag{8.1}$$

Z $m \not\subseteq n^+$ dostáváme $m \not\subseteq n$, takže platnost formule $\varphi(n)$ implikuje $n \subsetneq m$. Odtud $n < m$ a tedy (podle tvrzení 8.5) $n \in m$. Proto $n^+ = n \cup \{n\} \subseteq m$, spor s (8.1). □

Uspořádání $<$ na množině ω má ještě silnější vlastnost než je linearita. Řekneme, že uspořádání na množině X je ***dobré***, má-li každá neprázdná podmnožina Y množiny X nejmenší prvek. Množinu X s daným uspořádáním označujeme jako ***dobře uspořádanou***.

Věta 8.7. *Uspořádání $<$ na libovolném $n \in \omega$ je dobré.*

Důkaz. Nechť $\varphi(x)$ je formule

$$\varphi(x) \;\equiv\; (\forall z \subseteq x)\,(z \neq \emptyset \to (\exists m \in z)\,(\forall w \in z)\; m \subseteq w),$$

tedy "každá neprázdná podmnožina množiny x má nejmenší prvek". Ověříme podmínky věty 8.2. Podmínka (1) je splněna triviálně, protože pro $x = \emptyset$ přichází v úvahu jen podmnožina $z = \emptyset$. Nechť pro $n \in \omega$ platí $\varphi(n)$. Uvažme neprázdnou podmnožinu $z \subseteq n^+$ a definujme

$$z' = z \setminus \{n\}.$$

Mohou nastat dvě možnosti. Pokud $z' = \emptyset$, pak $z = \{n\}$ a množina z má nejmenší prvek n. Jinak je z' neprázdnou podmnožinou množiny n a protože platí $\varphi(n)$, má nejmenší prvek m. Všimněme si, že $m < n$ (neboť $m \in n$) a prvek m je tedy nejmenší i v množině z. V obou případech jsme ověřili, že platí $\varphi(n^+)$. Tvrzení tak plyne z věty 8.2. □

Věta 8.8. *Uspořádání $<$ na ω je dobré.*

Důkaz. Dokážeme nejprve, že libovolná neprázdná množina $z \subseteq \omega$ má *minimální* prvek. Zvolme $n \in z$ a uvažme množinu $n \cap z$. Je-li $n \cap z = \emptyset$, znamená to, že žádné $m \in n$ není prvkem množiny z, a tedy že n je minimální v z.

Můžeme proto předpokládat, že $n \cap z \neq \emptyset$. Protože $n \cap z \subseteq n$, podle věty 8.7 má množina $n \cap z$ nejmenší prvek m. Není-li m minimální v z, existuje nějaký prvek $y \in z$, pro který je $y \in m$. Protože $m \in n$, dostáváme

$$y < m < n$$

a z tranzitivity je $y < n$, tedy $y \in n$. To je spor s tím, že m je nejmenší v $n \cap z$.

Zbývá nahlédnout, že minimální prvek dobře (nebo i jen lineárně) uspořádané množiny z je nutně nejmenší. Tento snadný fakt ponecháváme na cvičení 8.3.2. □

Cvičení

► **8.3.1.** Dokažte, že každé dobré uspořádání je lineární.

► **8.3.2.** Dokažte, že v lineárně uspořádané množině je minimální prvek nutně nejmenší.

► **8.3.3.** Nechť s je množina s ostrým uspořádáním $\prec$. Zobrazení $f : \omega \to s$ je ***klesající***, pokud pro $m, n \in \omega$ platí

$$\text{pokud} \quad m < n, \quad \text{pak} \quad f(n) \prec f(m).$$

Dokažte, že je-li $\prec$ dobré uspořádání, pak žádné klesající zobrazení $f : \omega \to s$ neexistuje.

8.4 Rekurze na množině přirozených čísel

Věta 8.9 (Rekurze na ω). *Nechť $G : a \to a$ je zobrazení a $m_0 \in a$. Potom existuje právě jedno zobrazení $f : \omega \to a$ s vlastnostmi*

(1) $f(0) = m_0$,

(2) $f(n^+) = G(f(n))$ *pro každé přirozené* n.

Důkaz. Definujme ***úsekové zobrazení*** jako zobrazení h s vlastnostmi:

(i) $dom(h) \subseteq \omega$ a $rng(h) \subseteq a$,

(ii) je-li $0 \in dom(h)$, pak $h(0) = m_0$,

(iii) je-li $n^+ \in dom(h)$, pak $n \in dom(h)$ a $h(n^+) = G(h(n))$.

Nechť M je množina všech úsekových zobrazení. (Proč je to množina? viz cvičení 8.4.1). Definujme

$$f = \bigcup M.$$

Tvrdíme, že f je zobrazení s vlastnostmi (1) a (2) z tvrzení věty. K tomu stačí dokázat následující:

(a) f je zobrazení,

(b) f je úsekové zobrazení,

(c) $\mathrm{dom}(f) = \omega$,

(d) f je jediné zobrazení s vlastnostmi (1) a (2), definované na celém ω.

(a) f **je zobrazení.** Dokážeme, že

$$\begin{aligned}&\text{pro každé } n \in \omega \text{ existuje nejvýše jedno } y \in a \text{ s vlastností,} \\ &\text{že dvojice } \langle n, y\rangle \text{ patří do nějakého úsekového zobrazení.}\end{aligned} \tag{*}$$

Z tohoto tvrzení již plyne, že f je zobrazení.

Nechť $\varphi(x)$ je formule vyjadřující tvrzení "existuje nejvýše jedno $y \in a$ s vlastností, že $\langle x, y\rangle$ je prvkem nějakého úsekového zobrazení". (Formální zápis viz cvičení 8.4.2.) S ohledem na vlastnost (ii) z definice úsekového zobrazení platí $\varphi(0)$.

Dokážeme, že $\varphi(n) \to \varphi(n^+)$. Dejme tomu, že existují $y_1, y_2 \in a$ tak, že $\langle n^+, y_1\rangle, \langle n^+, y_2\rangle \in f$. Pak tedy existují úseková zobrazení h_1, h_2 s vlastností $h_i(n^+) = y_i$. Víme, že $h_1(n) = h_2(n)$, takže podle definice úsekového zobrazení je

$$y_1 = h_1(n^+) = G(h_1(n)) = G(h_2(n)) = h_2(n^+) = y_2$$

čili $y_1 = y_2$. Z předpokladu $\varphi(n)$ jsme tedy odvodili $\varphi(n^+)$. Z věty o indukci (věta 8.2) plyne tvrzení (*).

(b) f **je úsekové zobrazení.** Tato vlastnost plyne přímo z definice množiny f jako sjednocení úsekových zobrazení.

(c) $\mathrm{dom}(f) = \omega$**.** Zavedeme formuli $\psi(x)$:

$$\psi(x) \equiv \text{"}(\exists g)\ g \text{ je úsekové zobrazení a } x \in \mathrm{dom}(g)\text{"}.$$

Formule $\psi(0)$ platí například kvůli úsekovému zobrazení $\{\langle 0, m_0\rangle\}$. Platí-li $\psi(n)$, pak existuje úsekové zobrazení h definované v n. Snadno se ověří (cvičení 8.4.3), že zobrazení

$$h \cup \{\langle n^+, G(h(n))\rangle\} \tag{8.2}$$

je úsekové zobrazení definované v n^+. Platí tedy $\psi(n) \to \psi(n^+)$ a podle věty 8.2 je $(\forall n \in \omega)\ \psi(n)$. Odtud plyne, že f je definováno na celé množině ω.

(d) jednoznačnost. Nechť f' je zobrazení splňující podmínky (1) a (2) z tvrzení věty. Takové zobrazení je úsekové a definované na celé množině ω. Podle (*) ale pro každé $n \in \omega$ musí být

$$f(n) = f'(n).$$

□

Cvičení

► **8.4.1.** Proč je v důkazu věty 8.9 třída M množinou?

► **8.4.2.** Zapište přesně formuli φ z důkazu věty 8.9.

► **8.4.3.** Dokažte, že zobrazení (8.2) je úsekové.

8.5 Aritmetika

Abychom dokončili konstrukci přirozených čísel v teorii množin, je třeba na množině ω ještě definovat operace sčítání a násobení, vyhovující axiomům Peanovy aritmetiky. Začněme sčítáním.

Operaci $+$ lze jednoduše popsat rekurentním vzorcem, nabízí se proto možnost použít větu o rekurzi na množině ω. Ta však umožňuje definovat pouze funkce jedné proměnné, zatímco operace $+$ je binární. Zkonstruujeme proto nejprve pro každé pevné $m \in \omega$ funkci $A_m : \omega \to \omega$, jejíž hodnota $A_m(n)$ má vlastnosti očekávané od součtu $m + n$:

$$A_m(0) = m,$$
$$A_m(n^+) = (A_m(n))^+.$$

Ukážeme, že existence takové funkce a její jednoznačnost plyne z věty 8.9 při vhodné volbě hodnot a, m_0 a G. Dosaďme $a = \omega$, $m_0 = m$ a definujme zobrazení $G : \omega \to \omega$ předpisem

$$G(n) = n^+.$$

Zobrazení f ve větě 8.9 je pak právě funkce A_m.

Nyní již pro $m, n \in \omega$ stačí položit

$$m + n = A_m(n).$$

Operaci násobení definujeme analogicky, předpisem

$$m \cdot n = M_m(n),$$

kde $M_m : \omega \to \omega$ je (jednoznačně určená) funkce s vlastnostmi

$$M_m(0) = 0,$$
$$M_m(n^+) = M_m(n) + m.$$

Věta 8.10. *Množina ω spolu s operacemi $+$ a $\cdot$ (a operací $S(n) = n^+$) splňuje Peanovy axiomy (P1)–(P7).*

Důkaz. Ověříme pouze axiom (P2) a ostatní axiomy ponecháváme na cvičení 8.5.2. Dejme tomu, že pro $m, n \in \omega$ platí

$$m^+ = n^+ \tag{8.3}$$

a přitom $m \neq n$. Množina na levé straně rovnosti (8.3) zjevně obsahuje prvek n, takže buďto $n \in m$, nebo $n = m$. Druhou možnost náš předpoklad vylučuje, platí tedy $n \in m$. Symetrickým způsobem odvodíme $m \in n$. To je spor s faktem, že $\in$ je ostré uspořádání. □

Věta 8.11. *Pro přirozená čísla m, n, k platí*

(a) $m = n$ *právě když* $m + k = n + k$,

(b) $m < n$ *právě když* $m + k < n + k$.

Cvičení

► **8.5.1.** Vysvětlete podrobně způsob použití věty 8.9 při konstrukci operace násobení na ω.

► **8.5.2.** Dokažte větu 8.10.

Kapitola 9

Konstrukce reálných čísel

9.1 Celá čísla

Definujeme relaci $\sim$ na kartézském součinu $\omega \times \omega$:

$$(m, n) \sim (m', n') \text{ právě když } m + n' = m' + n.$$

Pozorování 9.1. *Relace $\sim$ je ekvivalence.*

Důkaz. Cvičení 9.1.1. □

Celé číslo definujeme jako libovolnou třídu $[(m, n)]$ ekvivalence $\sim$. ***Množina celých čísel*** $\mathbb{Z}$ je množina všech těchto tříd:

$$\mathbb{Z} = (\omega \times \omega)/\sim .$$

Pro přehlednost budeme třídu $[(m, n)]$ značit symbolem $[m, n]$. Zvláštní význam má třída $[0, 0]$, kterou budeme značit symbolem $0_{\mathbb{Z}}$ nebo prostě 0.

Chceme-li na množině $\mathbb{Z}$ zavést aritmetické operace, musíme definovat pravidla počítání s třídami. ***Sčítání*** definujeme předpisem

$$[m, n] + [m', n'] = [m + m', n + n'] .$$

Věta 9.2. *Sčítání na $\mathbb{Z}$ je dobře definováno a $(\mathbb{Z}, +)$ je abelovská grupa.*

Důkaz. Abychom ukázali, že součet $[m, n] + [m', n']$ je dobře definován, musíme ukázat, že výsledek operace nezávisí na volbě reprezentantů (m, n) a (m', n'). Jinými slovy je třeba ukázat, že pokud $(m, n) \sim (r, s)$ a $(m', n') \sim (r', s')$, pak platí

$$(m + m', n + n') \sim (r + r', s + s'). \tag{9.1}$$

Nechť je $(m, n) \sim (r, s)$ a $(m', n') \sim (r', s')$. Podle definice

$$m + s = n + r \quad \text{a} \quad m' + s' = n' + r',$$

takže (podle axiomů rovnosti)

$$(m + s) + (m' + s') = (n + r) + (n' + r').$$

Protože sčítání na množině ω je asociativní a komutativní, máme

$$(m + m') + (s + s') = (n + n') + (r + r'),$$

tj. $(m + m', n + n') \sim (r + r', s + s')$. Tím jsme ověřili platnost vztahu (9.1) a korektnost definice sčítání na $\mathbb{Z}$.

Zbývá ukázat, že $(\mathbb{Z}, +)$ je abelovská grupa. Prvek $0_{\mathbb{Z}} = [0, 0]$ je zjevně neutrálním prvkem, tj.

$$[m, n] + [0, 0] = [m, n] = [0, 0] + [m, n]\,.$$

Sčítání na $\mathbb{Z}$ je asociativní:

$$\begin{aligned}([m, n] + [r, s]) + [u, v] &= [m + r, n + s] + [u, v] \\ &= [(m + r) + u, (n + s) + v] \\ &= [m + (r + u), n + (s + v))] \\ &= [m, n] + [r + u, s + v] \\ &= [m, n] + ([r, s] + [u, v])\end{aligned}$$

(na třetím řádku jsme použili asociativitu sčítání na množině ω).

Sčítání na $\mathbb{Z}$ je rovněž komutativní (zde používáme komutativitu sčítání na ω):

$$\begin{aligned}[m, n] + [r, s] &= [m + r, n + s] \\ &= [r + m, s + n] \\ &= [r, s] + [m, n]\,.\end{aligned}$$

Konečně pro každý prvek $[m, n] \in \mathbb{Z}$ existuje inverzní prvek, totiž $[n, m]$:

$$[m, n] + [n, m] = [m + n, n + m] = [m + n, m + n] = 0_{\mathbb{Z}}.$$

Tím je důkaz proveden. □

Násobení celých čísel je definováno následovně:

$$[(a, b)] \cdot [(a', b')] = [(aa' + bb', ab' + a'b)].$$

Věta 9.3. *Rovněž násobení na $\mathbb{Z}$ je dobře definováno a je komutativní a asociativní. Pro $m, n, r \in \mathbb{Z}$ platí* **distributivní zákon***:*

$$m \cdot (n + r) = (m \cdot n) + (m \cdot r).$$

Uspořádání na $\mathbb{Z}$ je dáno vztahem

$$[(a, b)] < [(a', b')] \text{ pokud } a + b' \in a' + b.$$

Pozorování 9.4. *Relace $<$ je dobře definována a je to lineární uspořádání.*

Cvičení

► **9.1.1.** Dokažte pozorování 9.1.

9.2 Racionální čísla

Racionální čísla jsou zlomky s celočíselným čitatelem a jmenovatelem. Budeme je reprezentovat jako dvojice celých čísel, přitom však ztotožníme dvojice, které určují tentýž zlomek. Je zajímavé, že z formálního hlediska je definice racionálních čísel do značné míry obdobná definici čísel celých, s tím rozdílem, že sčítání je v jistém smyslu nahrazeno násobením. Definujeme relaci $\approx$ na kartézském součinu $\mathbb{Z} \times \mathbb{Z}^*$, kde $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$:

$$(a, b) \approx (a', b') \quad \text{právě když} \quad ab' = a'b.$$

Pozorování 9.5. *Relace $\approx$ je ekvivalence.*

Důkaz. Cvičení 9.2.1. □

Množina racionálních čísel $\mathbb{Q}$ je tvořena třídami ekvivalence $\approx$:

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\approx .$$

Racionální číslo je libovolný prvek $[(p, q)]_{\approx}$ množiny $\mathbb{Q}$. Pro jednoduchost takový prvek označujeme symbolem $[p, q]$.

Aritmetické operace a uspořádání na $\mathbb{Q}$ jsou definovány předpisy

$$\begin{aligned} [p, q] + [p', q'] &= [pq' + p'q, qq'], \\ [p, q] \cdot [p', q'] &= [pp', qq'], \\ [p, q] < [p', q'] &\quad \text{pokud} \quad q, q' > 0 \text{ a } pq' < p'q. \end{aligned}$$

Pozorování 9.6. *Operace $+, \cdot$ jsou dobře definovány. Relace $<$ rovněž a je to lineární uspořádání.*

Důkaz. Cvičení 9.2.2. □

Množina $\mathbb{Q}$ spolu s právě definovanými aritmetickými operacemi se vyznačuje vlastností, uvedenou v následující větě. Připomeňme, že ***těleso*** je trojice $(F, +, \cdot)$, kde F je množina a $+$, $\cdot$ jsou operace na množině F s následujícími vlastnostmi:

(i) $(F, +)$ je abelovská grupa,

(ii) $(F \setminus \{0\}, \cdot)$ je rovněž abelovská grupa, kde 0 je neutrální prvek v grupě $(F, +)$,

(iii) pro $x, y, z \in F$ platí ***distributivní zákon***:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z).$$

Věta 9.7. *Struktura* $(\mathbb{Q}, +, \cdot)$ *je těleso.*

Důkaz. Dokážeme pouze vlastnost (i) z definice tělesa, zbylé dvě části ponecháváme čtenáři jako cvičení 9.2.3. S využitím vět 9.2 a 9.3 dokážeme, že operace $+$ na $\mathbb{Q}$ je asociativní:

$$\begin{aligned}([p,q]+[r,s])+[u,v] &= [ps+qr,qs]+[u,v]\\ &= [(ps+qr)\cdot v + u\cdot(qs),(qs)\cdot v]\\ &= [(ps)v+(qr)v+u(qs),(qs)v]\\ &= [p(sv)+q(rv+us),q(sv)]\\ &= [p,q]+[rv+us,sv]\\ &= [p,q]+([r,s]+[u,v]).\end{aligned}$$

Operace $+$ je rovněž komutativní:

$$\begin{aligned}[p,q]+[r,s] &= [ps+rq,qs] = [rq+ps,sq]\\ &= [r,s]+[p,q]\,.\end{aligned}$$

Prvek $0_{\mathbb{Q}} = [0,1]$ je neutrálním prvkem operace $+$:

$$[p,q]+[0,1] = [p\cdot 1 + 0\cdot q, q\cdot 1] = [p,q]\,.$$

Konečně pro každý prvek $[p,q] \in \mathbb{Q}$ existuje inverzní prvek vzhledem k operaci $+$, totiž prvek $[-p,q]$, kde $-p$ je inverzní prvek k prvku $p \in \mathbb{Z}$ vzhledem ke sčítání celých čísel:

$$\begin{aligned}[p,q]+[-p,q] &= [pq+(-p)q,qq] = [q(p-p),qq]\\ &= [0,qq] = [0,1] = 0_{\mathbb{Q}}.\end{aligned}$$

□

Těleso F spolu s lineárním uspořádáním $<$ je ***uspořádané těleso***, pokud pro každé $x, x', y, y' \in F$ platí:

(1) pokud $x < x'$ a $y < y'$, pak $x + y < x' + y'$,

(2) pokud $x < x'$ a $y > 0$, pak $x \cdot y < x' \cdot y$.

Věta 9.8. *Dvojice* $(\mathbb{Q}, <)$ *je uspořádané těleso.*

Cvičení

► **9.2.1.** Dokažte pozorování 9.5.

► **9.2.2.** Dokažte pozorování 9.6.

► **9.2.3.** Dokažte větu 9.7.

9.3 Reálná čísla

K zavedení reálných čísel použijeme pojem řez, definovaný R. Dedekindem. ***Řez*** na množině $\mathbb{Q}$ je neprázdná vlastní podmnožina $r \subsetneq \mathbb{Q}$ s těmito vlastnostmi:

(1) r je ***dolní množina***, tj. pro $x, y \in \mathbb{Q}$ platí:

$$\text{pokud} \quad x < y \quad \text{a} \quad y \in r, \quad \text{pak} \quad x \in r,$$

(2) r nemá největší prvek.

Množinu reálných čísel $\mathbb{R}$ definujeme jako množinu všech řezů na množině $\mathbb{Q}$. Uspořádání je na $\mathbb{R}$ definováno velmi jednoduše, totiž inkluzí: pro $r, s \in \mathbb{R}$ je

$$r < s, \quad \text{pokud} \quad r \subsetneq s.$$

Sčítání na $\mathbb{R}$ je rovněž definováno přirozeně:

$$r + s = \{x + y : x \in r \quad \text{a} \quad y \in s\}.$$

Ukážeme, že $(\mathbb{R}, +)$ je abelovská grupa. Neutrální prvek vzhledem k operaci sčítání bude řez

$$0_{\mathbb{R}} = \{x \in \mathbb{Q} : x < 0\}.$$

U definice inverzního prvku $-r$ řezu r vzhledem ke sčítání je nutná opatrnost. Na první pohled je přirozeným kandidátem dolní množina

$$r' = \{x \in \mathbb{Q} : -x \notin r\}.$$

Uvažme ale například řez $r = 0_{\mathbb{R}}$: protože $0 \notin r$, platí $0 \in r'$. Množinu r' tedy tvoří všechna záporná čísla a 0. Pak ale r' není řez, neboť 0 je jejím největší prvkem.

Abychom získali řez, musíme definici trochu upravit:

$$-r = \{x \in \mathbb{Q} : (\exists y \in \mathbb{Q})\ y < -x \wedge (\forall z \in r)\ z < y\}. \tag{9.2}$$

Věta 9.9. *Množina $\mathbb{R}$ spolu s operací sčítání tvoří abelovskou grupu.*

Důkaz. Asociativitu a komutativitu ponecháváme na cvičení 9.3.1. Dokážeme, že $0_{\mathbb{R}}$ je neutrální prvek, tedy že pro každé $r \in \mathbb{R}$ je

$$r + 0_{\mathbb{R}} = r. \tag{9.3}$$

Dokážeme každou inkluzi zvlášť. Nechť $x \in r$ a $y \in 0_{\mathbb{R}}$, tedy $y < 0$. Pak $x + y < x + 0 = x \in r$, takže $x + y \in r$. Odtud $r + 0_{\mathbb{R}} \subseteq r$.

Opačně dokážeme, že každé $x \in r$ lze psát jako součet $w + s$, kde $w \in r$ a $s \in 0_{\mathbb{R}}$. Protože množina r je řez, x není její největší prvek, a v r tedy existuje $w > x$. Nyní stačí položit $s = x - w$. Tím je důkaz rovnosti (9.3) proveden.

Zbývá dokázat existenci inverzního prvku ke každému řezu r — přesněji ověřit, že takový prvek dostaneme z definice (9.2). □

Při vhodné definici násobení reálná čísla tvoří uspořádané těleso. Oproti racionálním číslům mají ještě jednu význačnou vlastnost. Nechť $m \subseteq \mathbb{R}$. Připomeňme, že ***horní mez*** množiny m je prvek $x \in \mathbb{R}$, který je větší nebo roven všem prvkům množiny m. Množina m je ***omezená***, pokud má nějakou horní mez. ***Supremum*** množiny m je její nejmenší horní mez (pokud existuje). Uspořádané těleso je ***úplné***, pokud každá jeho omezená podmnožina má supremum.

Věta 9.10. *Množina $\mathbb{R}$ spolu s operacemi $+$ a $\cdot$ a uspořádáním $<$ tvoří úplné uspořádané těleso. Je to navíc (až na isomorfismus) jediné těleso s těmito vlastnostmi.*

Cvičení

► **9.3.1.** Dokažte, že operace sčítání na reálných číslech je asociativní a komutativní.

Kapitola 10

Mohutnost

10.1 Stejně velké množiny

Množina x má ***mohutnost stejnou jako množina*** y, pokud existuje bijekce x na y. Říkáme také, že množiny x a y jsou ***ekvivalentní*** nebo ***ekvipotentní***, psáno $x \approx y$.

Množina x má ***mohutnost menší nebo rovnou mohutnosti množiny*** y ('x je subvalentní s y', $x \preceq y$), pokud existuje prosté zobrazení množiny x do množiny y.

Je-li $x \preceq y$ a $x \not\approx y$, píšeme $x \prec y$.

Tvrzení 10.1. *(i) Relace $\approx$ je ekvivalence.*

(ii) Relace $\preceq$ je neostré uspořádání.

10.2 Konečné a spočetné množiny

Množina je ***konečná***, je-li subvalentní nějakému přirozenému číslu.

Pozorování 10.2. *Je-li $s \subseteq t$ a t je konečná množina, pak s je rovněž konečná množina.*

Věta 10.3. *Jsou-li s, t konečné množiny, pak množina $s \cup t$ je rovněž konečná.*

Důkaz. Nechť pro nějaké $m, n \in \omega$ platí $s \preceq m$ a $t \preceq n$. Existují tedy prostá zobrazení

$$f : s \to m,$$
$$g : t \to n.$$

Definujme zobrazení $h : s \cup t \to \omega$ předpisem

$$h(x) = \begin{cases} f(x) & \text{pokud } x \in s, \\ m + g(x) & \text{jinak.} \end{cases}$$

Ukážeme, že h je prosté zobrazení do množiny $m + n$. Pro $x \in s \cup t$ nejprve dokažme, že $h(x) \in m + n$. Pro $x \in s$ to plyne ze vztahu

$$h(x) \in m \in m + n$$

(viz věta 8.11b) a tranzitivity relace $\in$ na ω. Pro $x \notin s$ je $g(x) \in n$, a tedy

$$h(x) = m + g(x) \in m + n,$$

opět podle věty 8.11b.

Předpokládejme nyní, že pro nějaké různé prvky $x, y \in s \cup t$ je $h(x) = h(y)$. Kdyby jak x, tak y byly prvky s, dostáváme spor, neboť zobrazení f je prosté. Podobně kdyby x, y byly prvky množiny $t \setminus s$, pak platí

$$m + g(x) = m + g(y),$$

což podle věty 8.11a znamená $g(x) = g(y)$, a tedy $x = y$, protože g je prosté. Můžeme tedy předpokládat, že $x \in s$ a $y \in t \setminus s$ a platí

$$f(x) = m + g(y).$$

Protože $f(x) \in m$, dostáváme

$$m + g(y) \in m$$

a věta 8.11b implikuje, že $g(y) \in 0$, což je spor. Důkaz je proveden. □

Důsledek 10.4. *Sjednocení konečně mnoha konečných množin je konečná množina. Přesněji: je-li m konečná množina a každý její prvek také, potom $\bigcup m$ je konečná množina.*

Důkaz. Indukcí s využitím formule

$$\varphi(n) \;\equiv\; (\forall s)\; s \preceq n \wedge ((\forall r)\; r \in s \to \text{“}r \text{ je konečná”}) \to \text{“}\textstyle\bigcup s \text{ je konečná”}.$$

Podrobnosti v cvičení 10.2.3. □

Tvrzení 10.5. *Konečná množina není ekvivalentní s žádnou svojí vlastní podmnožinou.*

Důkaz. Ukážeme indukcí, že pro každé $n \in \omega$ platí následující tvrzení: pokud $s \preceq n$ a $s \approx r \subseteq s$, pak $r = s$. Pro $n = \emptyset$ je tvrzení triviálně pravdivé.

Dokážeme indukční krok. Je-li $s \preceq n^+$ a $s \approx r \subseteq s$, pak nechť $f : s \to n^+$ je prosté zobrazení a $g : s \to r$ je bijekce. Zvolme prvek $x \in s \setminus r$ a položme

$$s' = s \setminus \{x\},$$
$$r' = r \setminus \{g(x)\}.$$

Potom $r' \approx s'$ (příslušnou bijekci získáme zúžením g na s') a $r' \subsetneq s'$. Definujme dále zobrazení $f' : s' \to n$ předpisem

$$f'(y) = \begin{cases} f(y) & \text{pokud } f(y) \in n, \\ f(x) & \text{jinak.} \end{cases}$$

Zobrazení f' je prosté a tedy $s' \preceq n$. Množina s' je ovšem ekvivalentní své vlastní podmnožině r', což je spor s indukčním předpokladem. □

Tvrzení 10.6. *Nechť* s, t *jsou konečné množiny. Potom*

(a) $s \times t$ *je konečná množina,*

(b) $\mathcal{P}(s)$ *je konečná množina.*

Důkaz. (a) Pro $x \in s$ definujme množinu t_x předpisem

$$t_x = \{\langle x, y\rangle : y \in t\}.$$

Zobrazení $f : t \to t_x$, které zobrazuje $y \in t$ na dvojici $\langle x, y\rangle$, je zjevně bijekce. Množina t_x je tedy konečná. Přitom platí

$$s \times t = \bigcup \{t_x : x \in s\},$$

což je jako sjednocení konečného počtu konečných množin podle důsledku 10.4 konečná množina.

(b) Dokážeme indukcí, že pro $n \in \omega$ platí:

$$\text{pokud } s \preceq n, \text{ pak } \mathcal{P}(s) \text{ je konečná množina.} \tag{10.1}$$

Je-li $n = 0$ a $s \preceq n$, pak $s = \emptyset$ a (10.1) zjevně platí.

Předpokládejme tedy platnost tvrzení (10.1) pro n a dejme tomu, že $s \preceq n^+$. Zvolme nějaké $x \in s$. Položme

$$p_0 = \{m \subseteq s : x \notin m\},$$
$$p_1 = \{m \subseteq s : x \in m\}.$$

Protože $\mathcal{P}(s) = p_0 \cup p_1$, stačí podle věty 10.3 ukázat, že obě tyto množiny jsou konečné. Ovšem $p_0 = \mathcal{P}(s \setminus \{x\})$, přičemž $s \setminus \{x\} \preceq n$ (příslušné prosté zobrazení je snadné najít). Podle indukčního předpokladu je tedy p_0 konečná množina. Zbývá si všimnout, že zobrazení $f : p_0 \to p_1$, definované předpisem

$$f(m) = m \cup \{x\},$$

je bijekce. I množina p_1 je tedy konečná, čímž je důkaz proveden. □

Množina je ***spočetná***, pokud je subvalentní množině ω. Každá konečná množina je tedy také spočetná.

Tvrzení 10.7. *Jsou-li* s, t *spočetné množiny, pak součin* $s \times t$ *je spočetný.*

Důkaz. Protože $s \times t \preceq \omega \times \omega$, stačí najít prosté zobrazení

$$f : \omega \times \omega \to \omega.$$

Vhodným zobrazením je například zobrazení

$$f(m, n) = (m + n)^2 + m.$$

Snadný důkaz, že f je prosté, přenecháváme na cvičení 10.2.4. □

Ke spočetným množinám se vrátíme v odstavci 12.2, kde dokážeme analogii důsledku 10.4.

Cvičení

▶ **10.2.1.** Dokažte, že každá konečná množina je ekvivalentní nějakému přirozenému číslu.

▶ **10.2.2.** Dokažte, že množina s je konečná, právě když každá neprázdná podmnožina množiny $\mathcal{P}(s)$, uspořádané inkluzí, má minimální prvek. (Tuto alternativní definici konečných množin zavedl A. Tarski.)

▶ **10.2.3.** Proveďte podrobně důkaz důsledku 10.4.

▶ **10.2.4.** Dokažte, že zobrazení f v důkazu tvrzení 10.7 je prosté.

10.3 Cantorova a Cantor–Bernsteinova věta

Věta 10.8 (Cantor)**.** *Pro každou množinu* m *platí:*

$$m \prec \mathcal{P}(m).$$

Důkaz. Abychom dokázali, že $m \preceq \mathcal{P}(m)$: stačí uvážit zobrazení $f : m \to \mathcal{P}(m)$ definované předpisem

$$f(x) = \{x\}.$$

Zbývá dokázat, že neplatí $m \approx \mathcal{P}(m)$. Budeme předpokládat, že existuje bijekce $g : m \to \mathcal{P}(m)$. Metoda, kterou dojdeme ke sporu, se nazývá Cantorova diagonální metoda.

Definujme množinu $s \subseteq m$ předpisem

$$s = \{x \in m : x \notin g(x)\}.$$

Neexistuje žádné $x \in m$, pro které by platilo $g(x) = s$, neboť $x \in s$ právě když $x \notin g(x)$. Přitom ale $s \in \mathcal{P}(m)$, takže g není zobrazení na množinu $\mathcal{P}(m)$. To je spor s předpokladem, že g je bijekce mezi m a $\mathcal{P}(m)$. □

Věta 10.9 (Cantor–Bernsteinova věta)**.** *Nechť* x, y *jsou množiny, pro něž platí*

$$x \preceq y \quad a \quad y \preceq x.$$

Pak $x \approx y$.

Důkaz. Můžeme předpokládat, že x a y jsou disjunktní množiny. (Pokud nejsou, vezmeme místo nich disjunktní kopie, třeba $x \times \{\emptyset\}$ a $y \times \{\{\emptyset\}\}$.)

Uvažme orientovaný graf G na vrcholech $V = x \cup y$, jehož hrany jsou (1) všechny uspořádané dvojice $(u, f(u))$ pro $u \in x$, a (2) všechny uspořádané dvojice $(v, g(v))$ pro $v \in y$. Všechny hrany tedy vedou mezi množinami x a y.

Do každého vrcholu grafu G vchází nejvýše jedna hrana a vychází z něj právě jedna. Není těžké nahlédnout, že každá komponenta takového grafu patří k některému z následujících typů:

- oboustranně nekonečná orientovaná cesta,
- jednostranně nekonečná orientovaná cesta,
- konečný cyklus sudé délky.

V každé komponentě tedy existuje perfektní párování. Z tohoto párování snadno získáme hledanou bijekci $h : x \to y$. □

Cvičení

► **10.3.1.** Ukažte, že

$$\mathcal{P}(\omega) \approx \mathbb{R},$$

a tedy $\omega \prec \mathbb{R}$.

► **10.3.2.** Dokažte následující tvrzení:

(a) $\omega \approx \omega \times \omega$,

(b) $x \times y \approx y \times x$,

(c) pokud $x \approx y$, pak $\mathcal{P}(x) \approx \mathcal{P}(y)$.

Kapitola 11

Ordinály

11.1 Dobrá uspořádání

Ostré částečné uspořádání $<$ na množině x je ***dobré***, pokud každá neprázdná množina $y \subseteq x$ má nejmenší prvek.

Pozorování 11.1. *Každé dobré uspořádání je lineární.*

Tvrzení 11.2. *Lineární uspořádání $<$ na X je dobré, právě když X neobsahuje žádnou nekonečnou klesající posloupnost $x_0 > x_1 > x_2 > \dots$.*

Důkaz. Nechť množina X obsahuje nekonečnou klesající posloupnost $(x_0, x_1, \dots)$. Je-li uspořádání $<$ dobré, pak množina všech prvků této posloupnosti má nejmenší prvek x_i. Přitom však $x_{i+1} < x_i$, což je spor. □

11.2 Ordinály

Množina m je ***tranzitivní***, pokud pro $x \in m$ je $x \subseteq m$. (Ekvivalentně: $y \in x \in m \to y \in m$.) ***Ordinál*** je tranzitivní množina, která je dobře uspořádána relací $\in$.

[interpretace dobrého uspořádání $\in$: (1) orientovaný graf, (2) minimální prvek množiny $y \subseteq \alpha$ je $x \in y$, který je s ní disjunktní]

Pozorování 11.3. *Množina ω i všechna přirozená čísla jsou ordinály.*

Důkaz. Tranzitivita množin ω i $n \in \omega$ plyne z věty 8.3. To, že uspořádání $\in$ je na nich dobré, plyne z vět 8.7 a 8.8. □

Třídu všech ordinálů značíme symbolem On.

Tvrzení 11.4. *Každý prvek ordinálu je ordinálem.*

Důkaz. Je-li α ordinál a $x \in \alpha$, pak z definice $x \subseteq \alpha$, takže $\in$ je dobré uspořádání na x. Zbývá ukázat, že x je tranzitivní množina. Nechť $u \in v \in x$. Protože α je tranzitivní, z $v \in x \in \alpha$ plyne $v \in \alpha$ a podobně dostáváme $u \in \alpha$. Relace $\in$ je na množině α tranzitivní, takže $u \in v \in x$ implikuje $u \in x$. Proto i množina x je tranzitivní. □

Tvrzení 11.5. *Pro ordinály α, β platí*

$$\alpha \in \beta \quad \textit{právě když} \quad \alpha \subsetneq \beta.$$

Důkaz. Nechť $\alpha \in \beta$. Pak (z tranzitivity β) $\alpha \subseteq \beta$. Určitě ale $\alpha \neq \beta$, jinak by bylo $\alpha \in \alpha$, což je ve sporu s antireflexivitou $\in$.

Opačný směr je těžší. Nechť $\alpha \subsetneq \beta$. Buď m nejmenší prvek množiny $\beta \setminus \alpha$. Tvrdíme, že $m = \alpha$. Důkaz rozdělíme na dvě inkluze.

Je-li u takové, že $u \in m$, pak $u \in \beta$, protože β je tranzitivní. Kdyby neplatilo $u \in \alpha$, bylo by $u \in \beta \setminus \alpha$ a tedy $m \in u$ — spor s předpokladem $u \in m$. Tedy $u \in \alpha$. Dokázali jsme inkluzi $m \subseteq \alpha$.

Nechť naopak $u \in \alpha$. u je jistě porovnatelné s m (neboť $\in$ je lineární na β). Která ze tří možností nastává? Možnosti $m \in u$ a $m = u$ implikují $m \in \alpha$ (první z nich s použitím tranzitivity), což je spor s $m \in \beta \setminus \alpha$. Zbývá pouze možnost $u \in m$. Celkem vzato je $\alpha \subseteq m$.

Platí tedy rovnost $m = \alpha$. Odtud plyne $\alpha \in \beta$ a lemma je dokázáno. □

V následující větě se zabýváme vlastnostmi 'relace' $\in$ na třídě On. Uvozovky jsou na místě, neboť se nejedná o množinu (definiční obor této 'relace' je celé množinové universum). Zavedeme proto třídovou variantu tohoto pojmu. ***Třídová relace*** je libovolná třída, každý jejíž prvek je uspořádaná dvojice. Obvyklé pojmy se vztahem k relacím (např. uspořádání) jsou pro třídové relace definovány analogicky.

Věta 11.6. *Třídová relace $\in$ je dobré uspořádání na třídě* On.

Důkaz. (i) $\in$ je antireflexivní na On. Kdyby pro $\alpha \in \mathrm{On}$ platilo $\alpha \in \alpha$, pak α jakožto prvek množiny α dosvědčuje, že $\in$ není antireflexivní na α. To nejde, protože α je ordinál.

(ii) $\in$ je tranzitivní na On. Nechť pro ordinály α, β, γ platí $\alpha \in \beta \in \gamma$. Z tranzitivity množiny γ plyne, že $\beta \subseteq \gamma$ a tedy $\alpha \in \gamma$.

(iii) Ostré uspořádání $\in$ na On je lineární. Mějme ordinály α, β. Z definice snadno plyne, že $\alpha \cap \beta$ je rovněž ordinál. Přitom máme

$$\alpha \cap \beta \subseteq \alpha \quad \text{a} \quad \alpha \cap \beta \subseteq \beta.$$

Kdyby obě inkluze platily jako ostré, pak podle tvrzení 11.5 by $\alpha \cap \beta$ bylo prvkem množiny α i β, tedy $\alpha \cap \beta \in \alpha \cap \beta$, což nejde.

Platí-li místo obou inkluzí rovnosti, dostáváme $\alpha = \beta$. Pokud je $\alpha = \alpha \cap \beta \subsetneq \beta$, je podle tvrzení 11.5 $\alpha \in \beta$. V jediném zbylém případě symetricky platí $\beta \in \alpha$. Linearita je tedy dokázána.

(iv) Lineární uspořádání $\in$ na On je dobré. Stačí ukázat, že každá neprádná množina $\mathfrak{a}$ ordinálních čísel má *minimální* prvek (podle (iii) je totiž nejmenší). Zvolme $\alpha \in \mathfrak{a}$. Nechť $b = \alpha \cap \mathfrak{a}$. Je-li $b = \emptyset$, pak α je minimální v $\mathfrak{a}$. V opačném případě nechť μ je *nejmenší* prvek množiny b (který existuje, protože α je ordinál). Tvrdíme, že μ je minimální v $\mathfrak{a}$. Pokud totiž pro $x \in \mathfrak{a}$ je $x \in \mu$, pak také $x \in \alpha$ (protože $\mu \in \alpha$) a tedy $x \in b = \mathfrak{a} \cap \alpha$. Ovšem μ je nejmenší v b, takže $\mu \in x$, což je spor. □

Důsledek 11.7. *Každá tranzitivní množina ordinálů je ordinál.*

Důsledek 11.8 (Burali–Forti)**.** On *není množina.*

Tvrzení 11.9. *Je-li α ordinál, pak α^+ je rovněž ordinál a je to nejmenší ordinál větší než α.*

Důkaz. Cvičení 11.2.1. □

Tvrzení 11.10. *Je-li $s \subseteq \mathrm{On}$, pak $\bigcup s$ je ordinál. Platí, že $\bigcup s$ je nejmenší ordinál β s vlastností $s \subseteq \beta$.*

Důkaz. Cvičení 11.2.2. □

Ordinál $\bigcup s$ označujeme jako ***supremum*** množiny s.

Cvičení

▶ **11.2.1.** Dokažte tvrzení 11.9.

▶ **11.2.2.** Dokažte tvrzení 11.10.

11.3 Ordinály jako typy dobrých uspořádání

V celém tomto odstavci nechť $(r, <)$ a $(s, \lhd)$ jsou dobře uspořádané množiny. Zápisem

$$f : r \rightsquigarrow s$$

označujeme fakt, že f je isomorfismus množiny $(r, <)$ s nějakou dolní podmnožinou množiny $(s, \lhd)$.

Tvrzení 11.11. *Pro dobrá uspořádání $(r, <)$ a $(s, \lhd)$ existuje nejvýše jedno zobrazení*

$$f : r \rightsquigarrow s.$$

Důkaz. Nechť f, g jsou dva různé isomorfismy množiny r s dolní podmnožinou množiny s. Definujme

$$m = \{x \in r : f(x) \neq g(x)\}.$$

Protože $f \neq g$, množina m je neprázdná a má tedy nejmenší prvek y. Prvky $f(y)$ a $g(y)$ jsou porovnatelné; bez újmy na obecnosti předpokládejme, že platí

$$f(y) \lhd g(y). \tag{11.1}$$

Protože $\operatorname{im} g$ je dolní podmnožina množiny s, musí platit $f(y) \in \operatorname{im} g$. Nechť $z \in r$ je prvek s vlastností $g(z) = f(y)$. Protože zobrazení f je prosté, platí $f(z) \neq g(z)$, a tedy $z \in m$. Na druhou stranu z nerovnosti (11.1) plyne, že $z < y$. To je spor s předpokladem, že y je nejmenší prvek množiny m. □

Důsledek 11.12. *Žádné dva různé ordinály nejsou isomorfní.*

Důkaz. Předpokládejme, že $f : \alpha \to \beta$ je isomorfismus, kde α, β jsou ordinály a (bez újmy na obecnosti) $\alpha \subsetneq \beta$. Nechť $i : \alpha \to \beta$ je identické zobrazení na ordinálu α, tj. $i(x) = x$ pro každé $x \in \alpha$. Protože α i β jsou dolní podmnožiny ordinálu β, platí

$$f : \alpha \rightsquigarrow \beta \quad \text{a} \quad i : \alpha \rightsquigarrow \beta,$$

což podle tvrzení 11.11 znamená $f = i$. Protože zobrazení f je na, také i je na a platí $\alpha = \beta$. To je spor. □

Tvrzení 11.13. *Pro dobrá uspořádání $(r, <)$ a $(s, \lhd)$ existuje zobrazení*

$$f : r \rightsquigarrow s$$

nebo zobrazení

$$g : s \rightsquigarrow r.$$

Obě zobrazení zároveň existují pouze v případě, že r a s jsou isomorfní.

Důkaz. Dejme tomu, že neexistuje ani jedno ze zobrazení f, g s uvedenou vlastností. Pro prvek $x \in r$ označme symbolem r_x množinu $\{y : y \leq x\}$ s dobrým uspořádáním $<$. Nechť m je množina všech prvků $x \in r$ s vlastností, že existuje zobrazení $f_x : r_x \rightsquigarrow s$. Pokud pro dané x takové zobrazení f_x existuje, je podle tvrzení 11.11 jednoznačně určeno. Definujeme-li tedy

$$h = \bigcup_{x \in m} f_x,$$

je h zobrazení a dokonce $h : m \rightsquigarrow s$. Podle předpokladu neexistuje zobrazení $f : r \rightsquigarrow s$ a je tedy $m \subsetneq r$. Kromě toho je také $\operatorname{im} h \subsetneq s$, neboť h^{-1} je isomorfismus množiny $\operatorname{im} h$ a dolní podmnožiny m množiny r, takže pro $\operatorname{im} h = s$ bychom dostali spor s předpokladem.

Nechť w je nejmenší prvek množiny $r \setminus m$ a z je nejmenší prvek množiny $s \setminus \operatorname{im} h$. Zobrazení $h' : r_w \to s$, definované předpisem

$$h'(x) = \begin{cases} z & \text{pro } x = w, \\ h(x) & \text{jinak,} \end{cases}$$

je zjevně isomorfismem množiny r_w a dolní podmnožiny množiny s. Dostáváme spor s předpokladem, že $w \notin m$.

Zbývá dokázat druhou část tvrzení. Nechť existují zobrazení $f : r \rightsquigarrow s$ a $g : s \rightsquigarrow r$. Podle tvrzení 11.11 je $f \restriction \operatorname{im} g = g^{-1}$, neboť obě zobrazení jsou isomorfismy množiny $\operatorname{im} g$ s dolní podmnožinou množiny s. Zobrazení $f \restriction \operatorname{im} g$ je tedy zobrazení *na* množinu s, takže

$$f^{-1} : s \rightsquigarrow r$$

a proto (opět podle tvrzení 11.11) $f^{-1} = g$, takže $\operatorname{im} g = r$ a g je isomorfismus mezi s a r. □

Třída F je ***třídové zobrazení***, pokud každý její prvek je uspořádaná dvojice a pro každé x, y, y' platí

$$\text{pokud} \quad \langle x, y\rangle \in F \quad \text{a} \quad \langle x, y'\rangle \in F, \quad \text{pak} \quad y = y'.$$

Je-li $\langle x, y\rangle \in F$, pak stejně jako u obvyklých zobrazení píšeme $F(x) = y$. ***Obraz*** $F[m]$ množiny m je třída definovaná předpisem

$$F[m] = \{y : (\exists x \in m)\ F(x) = y\}.$$

Axiom 11.14 (Schéma nahrazení)**.** *Nechť F je třídové zobrazení. Následující formule je axiom:*

$$(\forall m)\ \mathrm{Mn}\big(\, F[m] \,\big).$$

Věta 11.15 (Hartogs)**.** *Pro každou množinu s existuje ordinál α s vlastností, že*

$$\alpha \not\preceq s.$$

Důkaz. Nechť α je libovolný ordinál. Pokud dokazovaná věta neplatí, je $\alpha \preceq s$ a existuje tedy prosté zobrazení $h : \alpha \to s$. Na obrazu $h[\alpha]$ lze (právě jedním způsobem) definovat dobré uspořádání $<$ tak, že h je isomorfismus mezi výslednou uspořádanou množinou a ordinálem α:

$$h(x) < h(y), \quad \text{právě když} \quad x \in y.$$

Obecněji označme pojmem ***odraz*** libovolnou dvojici $(r, \lhd)$, kde $r \subseteq s$ a $\lhd$ je dobré uspořádání na množině r. Třídu všech odrazů označme symbolem

R. Ukážeme, že třída R je dokonce množina. Je-li $(r, \lhd)$ odraz, pak $r \in \mathcal{P}(s)$ a $\lhd \in \mathcal{P}(\mathcal{P}(\mathcal{P}(s)))$. Platí tedy

$$R \subseteq \mathcal{P}(\mathcal{P}(s) \times \mathcal{P}(\mathcal{P}(\mathcal{P}(s)))),$$

přičemž třída na pravé straně inkluze je množina. Díky schématu vydělení je tedy také třída R množinou.

Podle důsledku 11.12 je každý odraz isomorfní s nejvýše jedním ordinálem. Můžeme proto definovat třídové zobrazení F předpisem

$$F(x) = \begin{cases} \alpha & \text{pokud } x \text{ je odraz a existuje ordinál } \alpha \cong x, \\ \emptyset & \text{jinak.} \end{cases}$$

Protože každému ordinálu odpovídá alespoň jeden isomorfní odraz, platí $F[R] = \mathrm{On}$. Podle schématu nahrazení je tedy třída On množinou. To je spor s důsledkem 11.8. □

Důsledek 11.16. *Pro každou dobře uspořádanou množinu $(s, \lhd)$ existuje právě jeden ordinál τ s vlastností*

$$(s, \lhd) \cong (\tau, \in).$$

Důkaz. Z věty 11.15 plyne, že existuje ordinál α s vlastností $\alpha \not\preceq s$. Podle tvrzení 11.13 existuje zobrazení $f : s \rightsquigarrow \alpha$ nebo zobrazení $g : \alpha \rightsquigarrow s$. Druhá možnost je díky volbě ordinálu α vyloučena, proto uvažme zobrazení f. Jeho obor hodnot $\mathrm{rng}(f)$ je dolní podmnožina ordinálu α, tedy nějaký ordinál τ. Zobrazení f je isomorfismem uspořádaných množin $(s, \lhd)$ a $(\tau, \in)$.

Jednoznačnost plyne z důsledku 11.12. □

Ordinál τ z důsledku 11.16 označujeme jako ***typ*** dobře uspořádané množiny $(s, \lhd)$ a píšeme

$$\mathrm{typ}(s, \lhd) = \tau.$$

11.4 Ordinální aritmetika

Na ordinálních číslech můžeme definovat aritmetické operace, které zobecňují obvyklé sčítání a násobení přirozených čísel.

Nechť $(r, <)$ a $(s, \lhd)$ jsou lineárně uspořádané množiny. ***Lexikografické uspořádání*** součinu $r \times s$ je uspořádání $<_L$, definované předpisem

$$(x, y) <_L (x', y') \quad \text{pokud} \quad x < x' \text{ nebo } (x = x' \text{ a } y \lhd y').$$

Podobně je definováno tzv. ***hebrejské lexikografické uspořádání***[1] $<_H$:

$$(x, y) <_H (x', y') \quad \text{pokud} \quad y \lhd y' \text{ nebo } (y = y' \text{ a } x < x').$$

[1] Název odkazuje na skutečnost, že hebrejské písmo se píše zprava doleva.

Tvrzení 11.17. *Jsou-li* $(r, <)$ *a* $(s, \lhd)$ *dobře uspořádané množiny, pak uspořádání* $<_L$ *a* $<_H$ *jsou rovněž dobrá.*

Důkaz. Tvrzení dokážeme pouze pro uspořádání $<_L$, argument pro druhé uspořádání je symetrický. Nechť m je daná podmnožina součinu $r \times s$ (tj. vlastně relace z r do s). Množina $\mathrm{dom}(m) \subseteq r$ má nejmenší prvek x. Nechť y je nejmenší prvek obrazu $m[\{x\}]$. Pak $\langle x, y\rangle$ je nejmenší prvek množiny m v uspořádání $<_L$. □

Začneme definicí součtu a součinu dobře uspořádaných množin $(r, <)$ a $(s, \lhd)$, přičemž výsledkem je v obou případech opět dobře uspořádaná množina. ***Součet*** $(r, <) + (s, \lhd)$ je definován jako disjunktní sjednocení

$$(\{0\} \times r) \cup (\{1\} \times s)$$

s dobrým uspořádáním, které je restrikcí lexikografického uspořádání na součinu $\{0, 1\} \times (r \cup s)$.

Součin $(r, <) \cdot (s, \lhd)$ je kartézský součin

$$r \times s$$

s hebrejským lexikografickým uspořádáním $<_H$.

Nyní již můžeme snadno definovat součet $\alpha + \beta$ a součin $\alpha \cdot \beta$ ordinálních čísel α, β:

$$\alpha + \beta = \mathrm{typ}((\alpha, \in) + (\beta, \in))$$
$$\alpha \cdot \beta = \mathrm{typ}((\alpha, \in) \cdot (\beta, \in))$$

Tvrzení 11.18. *Sčítání a násobení ordinálních čísel mají následující vlastnosti:*

(i) sčítání i násobení jsou asociativní,

(ii) 0 je oboustranný neutrální prvek pro sčítání, 1 pro násobení,

(iii) $0 \cdot \alpha = \alpha \cdot 0 = 0$.

Důkaz. Cvičení 11.4.1. □

Jak ukazuje následující příklad, ordinální součet není komutativní:

$$1 + \omega = \omega$$
$$\omega + 1 = \omega^+$$

Komutativní není ani ordinální součin:

$$2 \cdot \omega = \omega$$
$$\omega \cdot 2 = \omega + \omega \neq \omega$$

Cvičení

► **11.4.1.** Dokažte tvrzení 11.18.

► **11.4.2.** Dokažte pro $\alpha, \beta, \gamma \in \mathrm{On}$:

$$\alpha(\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma.$$

Ukažte na příkladu, že analogická rovnost pro výraz $(\beta + \gamma) \cdot \alpha$ neplatí.

► **11.4.3.** Dokažte, že v ordinálních číslech platí věta o dělení se zbytkem: Pro každé dva ordinály $\beta > 0$ a α existují jednoznačně určené ordinály κ, ρ tak, že

$$\alpha = \beta \cdot \kappa + \rho.$$

11.5 Transfinitní indukce a rekurze

Věta 11.19 (Věta o transfinitní indukci)**.** *Nechť $\varphi(x)$ je množinová formule, splňující pro každý ordinál α podmínku:*

$$\Big((\forall \beta < \alpha)\ \varphi(\beta)\Big) \to \varphi(\alpha). \tag{11.2}$$

Pak je φ splněna pro každý ordinál.

Důkaz. Sporem. Nechť μ je nejmenší ordinál takový, že $\neg\varphi(\mu)$. Ovšem φ platí pro každé $\beta < \alpha$, takže podle předpokladu musí platit i pro μ. To je spor. □

Věta 11.20 (Věta o konstrukci transfinitní rekurzí)**.** *Nechť G je třídové zobrazení a α je ordinál. Pak existuje právě jedno (množinové) zobrazení f_α s vlastnostmi:*

(i) $\mathrm{dom}(f_\alpha) = \alpha$,

(ii) pro každé $\beta < \alpha$ je

$$f_\alpha(\beta) = G(f_\alpha \mid \beta).$$

Důkaz. Předpokládejme, že zobrazení f_α neexistuje. Můžeme také předpokládat, že α je nejmenší ordinál s touto vlastností.

Tvrdíme především, že pro každé $\gamma < \delta < \alpha$ platí

$$f_\delta(\gamma) = G(f_\gamma). \tag{11.3}$$

Nechť tento vztah neplatí. Zvolme nejmenší možný ordinál γ, pro který existuje nějaký ordinál δ v rozmezí $\gamma < \delta < \alpha$ tak, že (11.3) neplatí.

Protože platí

$$G(f_\delta \mid \gamma) = f_\delta(\gamma) \neq G(f_\gamma),$$

musí být $f_\delta \mid \gamma \neq f_\gamma$. Existuje tedy ordinál $\mu < \gamma$, pro který platí

$$f_\delta(\mu) \neq f_\gamma(\mu).$$

Z minimality ordinálu γ však obě strany této nerovnosti jsou rovny $G(f_\mu)$, což je spor. Tím je dokázána platnost vztahu (11.3).

Položme tedy v souladu s (11.3) pro každé $\delta < \alpha$

$$f_\alpha(\delta) := G(f_\delta).$$

Takto definované zobrazení f_ϵ splňuje podmínku (i) a dokážeme, že i podmínku (ii). Dejme tomu, že pro nějaké $\delta < \alpha$ je

$$f_\alpha(\delta) \neq G(f_\alpha \mid \delta).$$

S ohledem na definici zobrazení f_α musí být $f_\delta \neq f_\alpha \mid \delta$, takže pro nějaké $\mu < \delta$ musí platit

$$f_\delta(\mu) \neq f_\alpha(\mu).$$

Obě strany této nerovnosti však mají hodnotu f_μ, což je spor. Podmínky (i) a (ii) jsou tedy dokázány.

Zbývá dokázat jednoznačnost. Kdyby zobrazení f_1, f_2 měla obě požadovanou vlastnost, pak nechť δ je nejmenší ordinál, ve kterém se obě funkce liší. Potom platí

$$f_1 \mid \delta = f_2 \mid \delta$$

a podle podmínky (ii) také $f_1(\delta) = f_2(\delta)$. To je spor. □

Kapitola 12

Kardinály a axiom výběru

12.1 Kardinály

Kardinál je ordinál κ s vlastností, že pro každé $\alpha < \kappa$ je $\alpha \not\approx \kappa$.

Tvrzení 12.1. *Pro každou dobře uspořádanou množinu* r *s nějakým dobrým uspořádáním existuje právě jeden kardinál* κ *s vlastností* $r \approx \kappa$.

Důkaz. Nechť $<$ je dobré uspořádání na množině r. Podle důsledku 11.16 existuje právě jeden ordinál α s vlastností

$$(r, <) \cong (\alpha, \in).$$

Nechť κ je nejmenší ordinál, pro který platí $\kappa \approx \alpha$. Pak κ je kardinál s požadovanou vlastností.

Pokud pro kardinál λ rovněž platí $r \approx \lambda$, pak $\kappa \approx \lambda$. Jsou-li κ a λ různé kardinály, jeden z nich je menší a dostáváme spor s definicí kardinálu. Proto $\kappa = \lambda$, čímž je dokázána jednoznačnost. □

Existuje-li pro množinu r kardinál κ s vlastností $r \approx \kappa$, označujeme jej jako ***mohutnost*** množiny r a píšeme $|r| = \kappa$.

Tvrzení 12.2. *Neexistuje největší kardinál.*

Důkaz. Nechť κ je největší kardinál. Podle věty 11.15 existuje ordinál α s vlastností $\alpha \not\preceq \kappa$. Podle tvrzení 11.13 je dobře uspořádaná množina $(\kappa, \in)$ isomorfní s nějakou dolní podmnožinou uspořádané množiny $(\alpha, \in)$, takže $\kappa \prec \alpha$. Lze tedy najít nejmenší ordinál λ, pro který platí $\kappa \prec \lambda$. Ten je ale zjevně kardinálem, což je spor s maximalitou kardinálu κ. □

Třídu všech kardinálů označujeme symbolem Cn.

Tvrzení 12.3. Cn *není množina.*

Důkaz. Dejme tomu, že Cn je množina. Podle tvrzení 11.10 je pro množinu $x \subseteq \mathrm{On}$ množina $\bigcup x$ jejím supremem, tj. nejmenším ordinálem větším než každý prvek množiny x. Ordinál $\kappa = \bigcup \mathrm{Cn}$ je tedy zjevně kardinálem. Pak ale κ je největší kardinál, který podle tvrzení 12.2 neexistuje. To je spor. □

12.2 Axiom výběru

Selektor na množině s je funkce $\sigma : \mathcal{P}(s) \to s$ s vlastností, že pro každou neprázdnou množinu $r \subseteq s$ je

$$\sigma(r) \in r.$$

Axiom 12.4 (Axiom výběru)**.**

$$(\forall s)\ (\exists \sigma)\ \sigma \textit{ je selektor na množině } s.$$

Věta 12.5. *Axiom výběru je ekvivalentní s tvrzením, že pro každou množinu s existuje dobré uspořádání na s.*

Důkaz. Existuje-li na množině s dobré uspořádání, můžeme selektor σ na s definovat předpisem

$$\sigma(r) = \text{nejmenší prvek množiny } r \text{ vzhledem k } \lhd.$$

Předpokládejme naopak platnost axiomu výběru. Pomocí transfinitní rekurze zkonstruujeme dobré uspořádání $\lhd$ na množině s. Zvolme selektor σ na s a množinu $m \notin s$. Definujme třídové zobrazení G předpisem

$$G(h) = \begin{cases} \sigma(s \setminus \mathrm{rng}(h)) & \text{pokud } h \text{ je zobrazení a } s \setminus \mathrm{rng}(h) \neq \emptyset, \\ m & \text{jinak.} \end{cases}$$

Nechť α je ordinál, pro který platí $\alpha \not\preceq s$, který existuje podle věty 11.15. Z věty o transfinitní rekurzi plyne existence zobrazení $f : \alpha \to s \cup \{m\}$, splňujícího pro $\beta < \alpha$ podmínku

$$f(\beta) = G(f \mid \beta) = \begin{cases} \sigma(s \setminus f[\beta]) & \text{pokud } f[\beta] \subsetneq s, \\ m & \text{jinak.} \end{cases}$$

Platí-li pro nějaké $\delta \leq \alpha$ podmínka $f[\delta] \subsetneq s$, pak restrikce $f \mid \delta$ je prosté zobrazení, neboť její hodnota v každém bodě $\beta < \delta$ je vybírána z množiny $s \setminus f[\beta]$. Z předpokladu $\alpha \not\preceq s$ plyne existence nejmenšího ordinálu γ s vlastností, že $f[\gamma] = s$. Zobrazení $g = f \mid \gamma$ je bijekcí mezi γ a s. Zbývá jen pro $x, y \in s$ definovat dobré uspořádání

$$x \lhd y \quad \text{právě když} \quad g^{-1}(x) \in g^{-1}(y).$$

□

Tvrzení 12.6. *Pokud existuje zobrazení* f *množiny* r *na množinu* s*, pak* $s \preceq r$.

Důkaz. Nechť σ je selektor na množině $\mathcal{P}(r)$. Definujme zobrazení $g : s \to r$ předpisem

$$g(x) = \sigma(f^{-1}[\{x\}]).$$

Zobrazení g je prosté, neboť pro $x \in s$ je $f(g(x)) = x$, takže pro $x \neq y$ je $g(x) \neq g(y)$. □

Věta 12.7. *Je-li* s *spočetná množina a každé* $x \in s$ *rovněž, pak sjednocení* $\bigcup s$ *je spočetné.*

Důkaz. Nechť $f : s \to \omega$ je prosté zobrazení. Pomocí axiomu výběru najdeme zobrazení g, které každému $x \in s$ přiřazuje prosté zobrazení

$$g(x) : x \to \omega$$

(podrobně viz cvičení 12.2.1).

Pro $y \in \bigcup s$ definujme m_y jako prvek $x \in s$, pro který je hodnota $f(x)$ nejmenší. (V tomto bodě již axiom výběru nepotřebujeme, stačí nám dobré uspořádání na množině ω.) Konečně definujme zobrazení $h : \bigcup s \to \omega \times \omega$ předpisem

$$h(y) = \langle f(m_y), g(m_y)(y) \rangle .$$

Zobrazení h je zjevně prosté, takže

$$\bigcup s \preceq \omega \times \omega \preceq \omega,$$

kde poslední nerovnost plyne z tvrzení 10.7. □

Zobecnění věty 12.7 na větší mohutnosti dokážeme ve cvičení 12.2.2.

Cvičení

► **12.2.1.** Vysvětlete podrobně, jak se v důkazu věty 12.7 k nalezení zobrazení g používá axiom výběru. (*Návod:* použijte selektor na množině $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(s))))$.)

► **12.2.2.** Nechť množina r i každý její prvek mají mohutnost menší nebo rovnou nekonečnému kardinálu κ. Dokažte, že

$$|\bigcup r| \leq \kappa.$$

12.3 Kardinální aritmetika

• • •

Kapitola 13

Regularita

13.1 Axiom regularity

. . .

13.2 Hodnost

. . .

Literatura

. . .