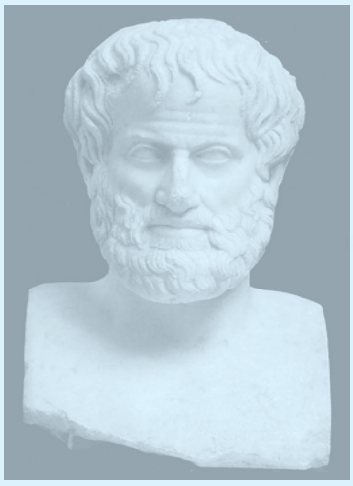
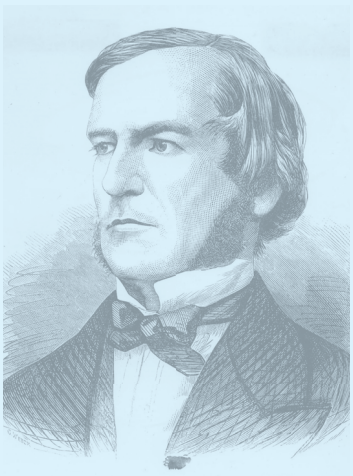
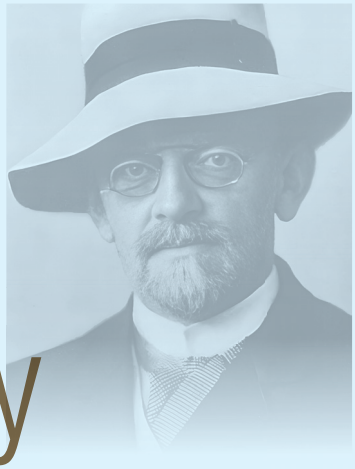
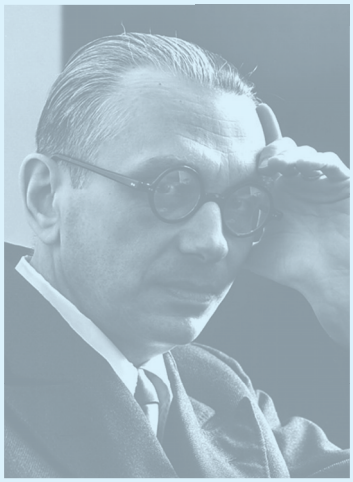
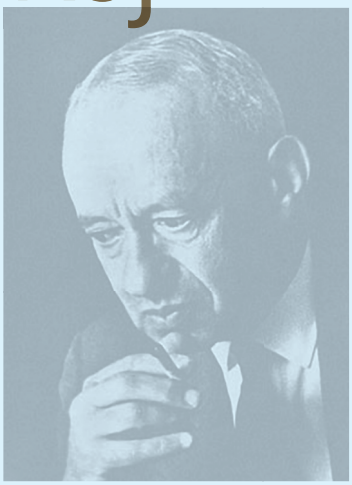






Pavol Zlatoš

Prednášky z matematickej logiky

UNIVERZITA KOMENSKÉHO V BRATISLAVE

Pavol Zlatoš

Prednášky z matematickej logiky

2025

Univerzita Komenského v Bratislave

Publikácia vychádza s podporou grantu č. K-23-002-00 slovenskej grantovej agentúry KEGA.

© prof. RNDr. Pavol Zlatoš, CSc., 2025

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky
Katedra algebry a geometrie

Recenzenti
prof. RNDr. Miroslav Haviar, CSc.
prof. RNDr. Ladislav Kvasz, DSc.

Publikácia je šírená pod licenciou Creative Commons CC BY 4.0 (vyžaduje sa: povinnosť uvádzať pôvodného autora). Viac informácií o licencii a použití diela: https://creativecommons.org/licenses/by/4.0/

https://stella.uniba.sk/texty/FMFI_PZ_matematicka_logika_prednasky.pdf

Vydavateľ
Univerzita Komenského v Bratislave

ISBN 978-80-223-6121-7 (tlač)
ISBN 978-80-223-6122-4 (online)

Obsah

Predhovor 5

1 Predmet logiky a jej postavenie v sústave vied 7

2 Letmý pohľad do histórie 13
2.1 Starovek . . . 13
2.2 Stredovek . . . 20
2.3 Renesancia a novovek . . . 21
2.4 Neeuklidovská geometria . . . 24
2.5 Logika v 19. storočí . . . 28
2.6 Koniec 19. a začiatok 20. storočia . . . 33
2.7 Teória množín . . . 36
2.8 Rozlúčka s históriou . . . 41

3 Výrokový počet 42
3.1 Výroky a výrokové formy . . . 42
3.2 Interpretácie, tabuľky pravdivostných hodnôt a logická ekvivalencia . 45
3.3 Tautológie a ďalšie triedy výrokových foriem . . . 47
3.4 Teórie vo výrokovom počte . . . 50
3.5 Axiomatizácia výrokového počtu . . . 52
3.6 Veta o korektnosti . . . 54
3.7 Veta o dedukcii a jej dôsledky . . . 55
3.8 Veta o úplnosti . . . 57
3.9 Axiomatizácia výrokového počtu pomocou štyroch logických spojok . 61

4 Logika prvého rádu 62
4.1 Jazyky prvého rádu a štruktúry prvého rádu . . . 62
4.2 Termy a formuly . . . 63
4.3 Teórie prvého rádu a ich modely . . . 66
4.4 Axiomatizácia logiky prvého rádu a veta o korektnosti . . . 75
4.5 Veta o dedukcii a jej dôsledky . . . 78
4.6 Úplné teórie . . . 79
4.7 Výsledky o rozšíreniach jazyka . . . 82
4.8 Gödelova veta o úplnosti . . . 84
4.9 Veta o kompaktnosti . . . 88
4.10 Mohutnosti modelov a Skolemov paradox . . . 90
4.11 Dôkaz vety o úplných henkinovských rozšíreniach . . . 91

5 Gödelove vety o neúplnosti 95
5.1 Paradox klamára a paradoxy Russella, Cantora a Berryho 95
5.2 Hľadanie východiska z krízy 97
5.3 Gödelove vety o neúplnosti. Prípravné úvahy 98
5.4 Prvá Gödelova veta o neúplnosti 99
5.5 Druhá Gödelova veta o neúplnosti 104
5.6 Pokusy o zúplnenie 107
5.7 Vety Tarského a Churcha-Turinga 108
5.8 Goodsteinove postupnosti 110
5.9 Filozofické dôsledky. Témy na esej 113

6 Podštruktúry a homomorfizmy 115
6.1 Podštruktúry 115
6.2 Homomorfizmy 118
6.3 Izomorfizmy a vnorenia 122
6.4 Elementárna ekvivalencia a elementárne podštruktúry 125
6.5 Diagramy štruktúr 128
6.6 Vety Löwenheima, Skolema a Tarského 130

7 Vety o zachovávaní 133
7.1 Lema o vzájomnej zlučiteľnosti a axiomatizačná lema 133
7.2 Univerzálne teórie a podštruktúry 134
7.3 Existenčné teórie a nadštruktúry 135
7.4 Univerzálno-existenčné teórie a zjednotenia reťazcov 136
7.5 Algebraický uzáver poľa 140
7.6 Pozitívne teórie a homomorfné obrazy 142

8 Ultraprodukty a axiomatické triedy 144
8.1 Priamy súčin štruktúr 144
8.2 Filtre a ultrafiltre 147
8.3 Filtrované súčiny 148
8.4 Ultraprodukty 151
8.5 Neštandardná analýza 153
8.6 Veta o kompaktnosti v jazyku ultraproduktov 157
8.7 Elementárna ekvivalencia a ultramocniny 158
8.8 Charakterizácia axiomatických a konečne axiomatizovateľných tried . 159

Vybraná literatúra 161

Zoznam symbolov 164

Vecný register 167

Menný register 173

Predhovor

Táto kniha by asi nikdy neuzrela svetlo sveta nebyť pandémie COVID-19 v rokoch 2020 – 2021. Matematickú logiku som síce prednášal dávno predtým a k prednáškam som napísal rad poznámok, ktoré som spočiatku rozdával študentom na prednáškach vo forme *hand-outs* a neskôr ich sprístupnil na sieti v elektronickej podobe. Poznámky som priebežne upravoval, dopĺňal a rozširoval, ale spracovať ich do knižnej podoby som nemal v pláne. Je predsa toľko vynikajúcich učebníc logiky všeobecne a matematickej logiky zvlášť... Napriek tomu som žiadnu z nich nepoužíval ako jediný zdroj, hoci som sa inšpiroval mnohými. Spravidla však boli na môj vkus príliš obsiahle alebo preťažené technickými detailmi, zbytočnými pre študentov, ktorí sa logike nechcú bližšie venovať. Takto som sa pri výbere tém cítil voľne a mohol ho zakaždým mierne modifikovať podľa záujmu študentov. Navyše som materiál prvého semestra zvykol na jeseň prednášať po slovensky študentom odboru *Matematika* a na jar, v trochu zjednodušenej podobe a s menej dôkazmi, po anglicky študentom odboru *Kognitívna veda*. Slovenský kurz mal pokračovanie aj v jarnom semestri, anglický bol jednosemestrový.

COVID však všetko zmenil. Samého ma zaskočilo akú zmenu (samozrejme k horšiemu) prinieslo nahradenie prednášok v triede s osobným kontaktom s poslucháčmi prednáškami *online*. Aby som účinky tejto zmeny aspoň čiastočne eliminoval, začal som si pripravovať ucelený text členený na časti zodpovedajúce podľa možnosti jednotlivým prednáškam a držať s nimi krok na týždennej báze. Text som vzápätí dával posluháčom k dispozícii v elektronickej podobe. Takto v priebehu jari 2020 vznikol prvý nástrel tejto knihy. Súčasne som totiž písal anglickú verziu prvej časti kurzu (venovanú výrokovému počtu, logike prvého rádu a Gödelovým vetám o neúplnosti) a slovenskú verziu druhej časti (venovanú vybraným kapitolám z teórie modelov). Počas jesene 2020 a jari 2021 som obe časti vlastne už len upravoval a dopĺňal. Rozhodnutie dopracovať sériu takto vzniknutých materiálov do knižnej podoby v dvoch jazykových mutáciách vo mne dozrelo až na jeseň 2021. Zároveň som pojal domýšľavý zámer odlíšiť svoj text od väčšiny matematicky koncipovaných učebníc logiky zaradením dvoch úvodných kapitol venovaných predmetu a významu logiky a jej postaveniu v sústave vied a stručnému prehľadu dejín logiky, ktorý by ju predstavil ako neodmysliteľnú a neprehliadnuteľnú súčasť ľudskej kultúry.

Obsah knihy nesie pečať okolností jej vzniku. Či to už budeme považovať za výhodu alebo za cnosť z núdze, rozsah knihy je značne obmedzený, takže sa dá bez problémov predniesť v dvojsemestrálnom kurze. Výber tém idúcich nad rámec povinných súčastí (výrokový a predikátový počet) odráža záujmy a vkus autora. Nemalo by preto prekvapiť, že viacero dôležitých tém tu čitateľ nenájde. Len námatkovo spomeňme logické obvody, neklasické, modálne a viachodnotové logiky, teóriu vypočítateľnosti, teóriu zložitosti, viaceré súčasti teórie modelov atď. Ako však už zaznelo, „je predsa

toľko vynikajúcich učebníc logiky všeobecne a matematickej logiky zvlášť…“ Ak sa chce čitateľ dozvedieť o niektorej zo spomínaných i nespomínaných, v tejto knihe spracovaných i nespracovaných tém viac, má si z čoho vyberať. Nejaké tipy nájde v zozname literatúry, no nemusí sa nechať ním obmedzovať.

Bratislava, september 2025

Pavol Zlatoš

1 Predmet logiky a jej postavenie v sústave vied

Slovo *logika* môže v závislosti na kontexte nadobúdať rôzne významy. Tieto významy síce navzájom súvisia, no určite nie sú totožné. Vo voľnom a v bežnej reči často používanom význame *logikou* rozumieme čosi ako vnútornú štruktúru, skôr tušenú než zjavnú, ktorá však danej veci (záležitosti), výkladu nejakého súboru javov, tej-ktorej oblasti poznania či argumentácii dáva zmysel alebo zaň preberá záruku. Naopak, jej narušením sa tento zmysel vytráca a jej absenciou či popretím sa prevracia v nezmysel. Takto zvykneme hovoriť o *logike veci*, *logike zákona*, *logike vývoja*, *logike deja*, *logike konfliktu*, a pod. Tento význam býva do značnej miery upresnený v kontexte vedeckých teórií, najmä ich deduktívnych súčastí. *Logika* tu splýva so súborom metodologických zásad budovania takýchto teórií, čo o. i. zahŕňa analýzu ich východzích princípov, metód spracovania experimentálnych dát a faktov, formuláciu hypotéz a metódy ich overovania.

V trochu špecifickejšom význame je *logika* súborom pravidiel a zásad správneho myslenia, usudzovania a odvodzovania, ktorými je potrebné sa pri týchto činnostiach riadiť a ktorých dodržiavanie zaručuje ich správnosť. Naopak, ich narušenie je varovným signálom poukazujúcim na chyby v tom ktorom úsudku. Treba však upozorniť, že *správnosť* nie je to isté ako *pravdivosť*. Logicky správna úvaha vedie nevyhnutne k pravdivému záveru, len ak vychádza z pravdivých predpokladov. Na druhej strane, k pravdivému záveru možno neraz dospieť aj logicky správnou úvahou vychádzajúcou z nepravdivých predpokladov, ako aj logicky chybnou úvahou bez ohľadu na pravdivosť východzích predpokladov.

Logika sa tak stáva vedeckou disciplínou na pomedzí filozofie, metodológie vedy, jazykovedy a (pretože hojne využíva matematické metódy a postupy) aj matematiky, s dôležitými uplatneniami v oblasti práva a spätne v matematike. Pre účely nášho kurzu však *logiku* budeme chápať v nasledujúcom ešte užšom význame:

> *Logika je normatívna vedecká disciplína, ktorá skúma formu, štruktúru a zákony správneho (t. j. logického) myslenia a usudzovania, tak ako sa prejavujú v jazyku, či už hovorenom alebo písanom, abstrahujúc pritom od obsahu konkrétnych myšlienok a úsudkov.*

Tento „slogan“ si však žiada podrobnejší komentár.

Zo skúsenosti vieme, že myslenie a usudzovanie sa môžu uberať po cestách rozumu i po cestách nerozumu, že môžu byť plne logické, menej logické aj celkom nelogické. Svedčia o tom napr. často používané posmešné až politicky nekorektné výrazy ako *ženská logika*, *vojenská* alebo *policajná logika* a pod. Ak je však myslenie nelogické, tým horšie pre myslenie. Podobne, chybný (nelogický) úsudok nevyvracia logiku, ale

logika vyvracia takýto úsudok. Poslaním logiky tak nie je emprický popis rôznych podôb myslenia a usudzovania, ale stanovovanie a formulácia *noriem* zaručujúcich ich správnosť. Hovoríme, že logika plní voči jazyku a mysleniu *normatívnu funkciu*.

Čitateľ si iste všimol výskyt adjektíva *logický* v našom vymedzení logiky ako vedeckej disciplíny, čo v ňom mohlo vyvolať pocit, že sa tak trochu motáme v *logickom kruhu*. Nuž, nemienime to zakrývať. Autor otvorene priznáva, že bez istej znalosti logiky, presnejšie bez schopnosti logicky uvažovať, sa logika vysvetliť ani študovať nedá. Bude teda predpokladať, že jeho čitatelia či poslucháči už vedia logicky myslieť aj logicky argumentovať, a nemá v úmysle ich to učiť, ale naopak, bude to od nich vyžadovať. Na druhej strane však štúdium logiky, zahŕňajúce zvedomenie si a reflexiu princípov logického myslenia a usudzovania, tieto schopnosti nepochybne rozvíja a kultivuje.

Pristavme sa na chvíľu pri otázke vzťahu logiky a jazyka. Hoci myslenie sa myslením v jazyku pravdepodobne nevyčerpáva – jeho súčasťou sú totiž i rôzne obrazy a neverbálne predstavy, neurčité tušenia a vhľady, ako aj rôzne nálady a emócie – jednako, ak sa chceme o obsah či výsledky svojho myslenia podeliť s inými ľuďmi, musíme im ich nejako zdeliť čiže skomunikovať. Najefektívnejší nástroj komunikácie, akým disponujeme, je náš jazyk, či už v jeho hovorenej alebo písanej podobe. Komunikácia v jazyku si však od nás žiada dodať jazykovú podobu aj tým zložkám nášho myslenia, ktoré ju pôvodne nemali. Samozrejme, je tu i možnosť vyjadriť sa prostriedkami hudby alebo výtvarného umenia, pohybom a tancom, či gestami a mimikou, a tu (s výnimkou posunkovej reči) je logika krátka. Krátka je aj na mnohé podoby literárnej tvorby, najmä na poéziu, no nielen na ňu. Avšak úvahy, v ktorých na základe nejakých prijatých východzích predpokladov logickou argumentáciou (zase ten bludný kruh) vyvodzujeme nejaké závery, prebiehajú plne, i keď nie výlučne v jazyku (v hovorenom prejave totiž hrajú istú úlohu aj intonácia, gestá a mimika) a spadajú do kompetencie logiky.

Napokon si skúsme objasniť, čo to vlastne znamená *abstrahovať od obsahu* jednotlivých myšlienok a úsudkov a sústrediť sa výlučne na ich *formu*. Je také niečo vôbec možné? Snaha vidieť v rôznorodých javoch ich obsah a formu a tieto dve zložky od seba oddeľovať tkvie hlboko v tradícii európskeho myslenia. A hoci je do veľkej miery umelá, má zároveň značný podiel na úspechoch západnej civilizácie na poli filozofickom, vedeckom a v konečnom dôsledku aj technickom. Umožňuje nám totiž rozštiepiť v myslení vnímaný úsek skutočnosti na dve zložky, ktorým pripisujeme rozličné úlohy, totiž na *obsah* a *formu*. Potlačením obsahu dostávame značne zjednodušenú vyprázdnenú formu nejakého javu, ktorú možno ľahšie podrobiť myšlienkovému skúmaniu. Navyše takáto abstraktná forma sa môže vyskytnúť aj v inej oblasti javov a umožniť, aby bola naplnená novým obsahom. Vďaka tomu sa môže podariť preniesť na túto oblasť poznatky získané v pôvodnej oblasti. To prispieva k univerzálnemu charakteru európskej vedy a tvorí jeden zo základných pilierov *redukcionizmu*, ktorý patrí k vedúcim metodologickým princípom vedeckého skúmania. Taktiež to umožňuje široké uplatnenie matematických metód a naopak, vytvára podnety pre ďalší rozvoj matematiky.

Filozofický problém oddeliteľnosti formy a obsahu sa v rozvinutej podobe po prvýkrát vynára v antickom Grécku v súvislosti s klasickou geometriou. Niektoré rovinnné, prípadne priestorové útvary nás zaujmú svojím *tvarom*, najmä jeho jednoduchosťou

a symetriou. Tieto tvary dostali osobitné pomenovania. V rovine k nim patria najmä *trojuholník* (s rôznymi prívlastkami ako *rovnostranný*, *rovnoramenný*, *pravouhlý*), *obdĺžnik*, *štvorec* ako jeho špeciálny prípad, ďalej *kruh*, *pravidelný päťuholník*, *pravidelný šesťuholník* atď. V priestore sú to predovšetkým tzv. *platónske telesá*, čiže *pravidelný štvorsten*, *kocka*, *osemsten*, *dvanásťsten* a *dvadsaťsten*, a tiež *guľa*, *pyramída* čiže *štvorboký ihlan* atď. Mnohé z týchto tvarov sa zároveň ukazujú ako účelné a žiadúce v rôznych oblastiach praktickej ľudskej činnosti: pri vymeriavaní pozemkov, stavbe obydlí, chrámov a palácov, v rôznych remeslách, a pod. Pritom tieto tvary samotné, a ešte väčšmi dômyselne skombinované, pôsobia na naše estetické cítenie, a hrajú preto dôležitú úlohu vo výtvarnom umení (v maľbe i v sochárstve) a v architektúre.

Okrem toho výtvory ľudskej činnosti využívajúcej spomínané tvary sú spravidla tým dokonalejšie, čím presnejšie a dokonalejšie sa im darí dosiahnuť či napodobniť príslušný tvar. So snahou o dokonalosť prichádza aj uvedomenie, že absolútna dokonalosť je, aspoň pre ľudského tvorcu, nedosiahnuteľná. Čisté a dokonalé geometrické tvary sa tak osamostatňujú a stávajú sa nedosiahnuteľným *ideálom*. Osamostatňuje sa aj *geometria* ako veda skúmajúca práve tieto osamostatnené ideálne tvary. Zároveň sa zoznam ideálnych geometrických tvarov rozrastá o ďalšie realite ešte vzdialenejšie objekty: k nim patria predovšetkým *body*, t. j. akési najmenšie možné miesta v rovine alebo v priestore zbavené akejkoľvek rozľahlosti, a *priamky*, resp. *úsečky*, čiže dokonale rovné čiary bez akejkoľvek hrúbky.

Uvedený výklad, podľa ktorého ideálne geometrické objekty sú výtvorom ľudského intelektu a majú svoj pôvod v skúsenosti a praktickej ľudskej činnosti, sa niesol v duchu Aristotelovom. Je však tiež možné prijať stanovisko zastávané Platónom, podľa ktorého ideálne geometrické objekty majú samostatnú existenciu a pobývajú v ideálnom geometrickom svete (niekde na polceste medzi materiálnym svetom a svetom čistých ideí), ktorý vo svojej existencii predchádza pozemský materiálny svet. Ideálne geometrické objekty majú účasť na reálnych objektoch príslušných tvarov, a to tým väčšiu, čím vernejšie ten-ktorý materiálny objekt svojím tvarom napodobňuje príslušný ideálny tvar. Čistota ideálneho geometrického objektu je však v jeho pozemskom uskutočnení vždy viac či menej „zašpinená“ jeho obsahom, presnejšie jeho materiálnou náplňou, a len tak povediac cez ňu či spoza nej presvitá.

Z nášho hľadiska nezáleží na tom, ktorému z uvedených dvoch výkladov dáme prednosť. Dôležité je si uvedomiť, že antická geometria dokazuje možnosť myšlienkového oddelenia formy a obsahu širokej triedy javov. Pritom geometria už vo svojej pôvodnej antickej podobe, a o to väčšmi vo svojich ďalších vývojových štádiách, je výrečným a nespochybniteľným dokladom plodnosti a úspešnosti takéhoto prístupu.

Ako budeme mať možnosť ešte viackrát uvidieť, podobné oddelenie formy od obsahu pripúšťa aj logika. Navyše v porovnaní s geometriou je toto oddelenie konceptuálne podstatne jednoduchšie a nenastoluje analogické problémy metafyzickej povahy. To je umožnené najmä symbolickým zápisom inšpirovaným matematikou, ktorý poskytuje konkrétnu reprezentáciu logických foriem. Ukážme si na jednoduchom príklade, čo tým máme na mysli.

Jeden zo známych sylogizmov sa zvykne ilustrovať úvahou:
Všetci ľudia sú smrteľní.
Sokrates je človek.
Preto *Sokrates je smrteľný.*

Prvé tvrdenie sa zvykne nazývať aj *veľká premisa*, druhé *malá premisa* a tretie *záver*. Uvedomme si, že záver vyplýva z premís s logickou nevyhnutnosťou. Správnosť uvedenej úvahy sa nezakladá na empirickom dôkaze Sokratovej smrteľnosti, ktorý bol podaný vykonaním rozsudku odsudzujúceho ho na trest smrti vypitím čaše odvaru z bolehlavu. Rovnakú formu má aj nasledujúca úvaha:

Všetci králi sú kone.
Alexander Veľký bol kráľ.
Preto *Alexander Veľký bol kôň.*

Hoci je svojím spôsobom absurdná, aj táto úvaha je logicky správna, i keď jej záver je očividne nepravdivý. Ďalšia úvaha podobného typu:

Všetci králi sú kone.
Alexander Veľký bol kôň.
Preto *Alexander Veľký bol kráľ.*

však logicky správna nie je, lebo jej záver – hoci je pravdivý – z jej predpokladov nevyplýva. Na druhej strane, ďalšia absurdná úvaha

Všetci králi sú kone.
Alexander Veľký nebol kôň.
Preto *Alexander Veľký nebol kráľ.*

je logicky správna, i keď jej záver je nepravdivý (rovnako ako jeden z jej predpokladov).

Podobný charakter majú aj nasledujúce dva logicky platné úsudky:

Všetci Gréci sú ľudia.
Všetci Aténčania sú Gréci.
Preto *všetci Aténčania sú ľudia.*

prípadne

Všetci Sparťania sú udatní bojovníci.
Niektorí Gréci sú Sparťania.
Preto *niektorí Gréci sú udatní bojovníci.*

Nebolo by ťažké uviesť ďalšie príklady logicky platných úsudkov spadajúcich pod rovnaké schémy ako dva posledné. Ich forma však spoza jednotlivých príkladov iba presvitá. Jej pochopenie sa dosahuje ilustrovaním na dostatočnom množstve vhodných príkladov. U Aristotela sa však po prvýkrát v histórii, vďaka použitiu subjekt-predikátových premenných, vynára jej explicitná podoba, napríklad:

Všetky M sú P.
Všetky S sú M.
Preto *všetky S sú P.*

prípadne

Všetky M sú P.
Niektoré S je M.
Preto *niektoré S je P.*

Stredný člen M vystupuje v oboch premisách, v prvej hrá úlohu subjektu, v druhej úlohu predikátu a závere sa nenachádza. Člen P sa vykytuje v prvej premise a v závere, pričom v oboch hrá úlohu predikátu; člen S sa nachádza v druhej premise a v závere, v oboch v úlohe subjektu.

Podobné formy sa objavujú v logike *stoickej školy*; v nich úlohu výrokových premenných preberajú radové číslovky:

Keď prvé, tak druhé.
Ale prvé.
Preto *druhé.*

prípadne

Keď prvé, tak druhé.
Ale nie druhé.
Preto *preto nie prvé.*

S využitím moderného symbolického jazyka, ktorý sa však vyvinul až v priebehu 19. a 20. storočia, môžeme formy uvedených úsudkov zachytiť veľmi jednoduchým a zároveň prehľadným spôsobom. Navyše pritom dokážeme odlíšiť formu prvých dvoch platných úsudkov o Sokratovi, resp. o Alexandrovi od formy úsudku o Grékoch a Aténčanoch. Nech $P(x)$, $Q(x)$, $R(x)$ označujú ľubovoľné vlastnosti (predikáty) premenného objektu x a a označuje ľubovoľný konkrétny objekt. Potom nasledujúce úsudky sú logicky platné:

$$\begin{array}{ll} (\forall x)(P(x) \Rightarrow Q(x)) & (\forall x)(P(x) \Rightarrow Q(x)) \\ P(a) & \neg Q(a) \\ \text{Preto } Q(a) & \text{Preto } \neg P(a) \end{array}$$

$$\begin{array}{ll} (\forall x)(P(x) \Rightarrow Q(x)) & (\forall x)(P(x) \Rightarrow Q(x)) \\ (\forall x)(R(x) \Rightarrow P(x)) & (\exists x)(P(x) \wedge R(x)) \\ \text{Preto } (\forall x)(R(x) \Rightarrow Q(x)) & \text{Preto } (\exists x)(Q(x) \wedge R(x)) \end{array}$$

Na záver si ešte vyjasnime, ako chápať slovné spojenie *matematická logika*. Logika môže byť matematická v zásade v dvoch významoch: jednak metódami, ktoré používa, jednak svojím predmetom. Logika môže analyzovať rôzne fragmenty prirodzených či umelých jazykov, ktoré takúto analýzu pripúšťajú. Pri tom jej môžu v rôznej miere poslúžiť matematické metódy, napr. symbolická reprezentácia jednotlivých jazykových objektov alebo ich tried a modelovanie vzťahov medzi nimi matematickými prostriedkami. Tie spravidla umožňujú spracovanie pomocou výpočtovej techniky. V tomto zmysle často používame termíny ako *formálna logika* alebo *symbolická logika*. Príkladom takejto logiky je *výrokový počet*, ktorým naše štúdium matematickej logiky začneme.

Predmetom logiky sa však môžu stať aj jazyky matematických teórií, analýza ich deduktívnej výstavby a vzťah medzi symbolikou v nich používanou a významom, aký môžu príslušné symboly nadobúdať. Sotva niekoho prekvapí, že práve jazyky matematických teórií, vďaka vysokému stupňu presnosti a jednoznačnosti, sú na podobnú

analýzu obzvlášť vhodné. Takáto logika je potom matematická svojím predmetom. Rovnako neprekvapí, že táto logika zároveň hojne používa matematické metódy. Je to teda logika matematická tak svojimi metódami ako aj svojím predmetom. Uvidíme, že takáto „dvojnásobne matematická“ logika nielenže prináša zjednocujúci pohľad na rôzne oblasti matematiky, no neraz ich aj obohacuje o nové metódy a zaujímavé matematické poznatky. Počínajúc kapitolou o *logike prvého rádu* sa budeme venovať práve takejto logike.

Značenie a jeho štruktúru v symbolickom jazyku učene nazývame *syntax*. Priraďovanie významu symbolom a ich konglomerátom je náplňou *sémantiky*. Práve skúmanie vzťahu medzi syntaxou a sémantikou bude kľúčovou témou ako aj jednotiacim prvkom štúdia rôznych odvetví matematickej logiky v našom kurze.

2 Letmý pohľad do histórie

Vopred upozorňujeme čitateľa, že náš stručný prehľad dejín logiky si nijako nečiní nárok na úplnosť a autor si je vedomý toho, že by bolo márne sa o také niečo pokúšať. Naše ciele sú podstatne skromnejšie: aspoň kaleidoskopicky predstaviť logiku v jej vývoji ako súčasť podnes živého prúdu európskej kultúry a vzdelanosti prameniaceho v časoch dávno minulých a vinúceho sa ľudskou históriou až do súčasnosti.

2.1 Starovek

Logika – podobne ako klasická geometria – je jedným z plodov gréckeho zázraku. Zárodky logiky síce možno nájsť aj v myslení starovekej Číny a Indie, ale ani zďaleka nedosahujú úroveň, na akú bola logika povznesená v antickom Grécku. Samotné slovo *logika* je odvodené z gréckeho slova *logos* ($\lambda o \gamma o \varsigma$), ktoré znamená jednak *slovo*, jednak *reč*, no taktiež *usporiadanie* či *poriadok* (česky *řád*) ako opak *chaosu*, či dokonca princíp tvoriaci svet jeho vymanením z chaosu. V podobnom význame je slovo *Slovo* použité aj v úvodnej vete Jánovho evanjelia, ktoré celé nesie zreteľnú pečať helenistického vplyvu: *Na počiatku bolo Slovo, to Slovo bolo u Boha, a to Slovo bolo Boh.*

Logika ako uvedomelá súčasť ľudského poznania reflektujúca prejavy ľudského myslenia v jazyku však nemohla vzniknúť skôr, než sa myslenie a jazyk stali logickými. Inak povedané logika sa najprv musela konštituovať v rámci jazyka ako tá „*vnútorná štruktúra, skôr tušená než zjavná, ktorá však danej veci* [...], *či argumentácii dáva zmysel alebo zaň preberá záruku,*“ a až potom mohla byť objavovaná a postupne začať nadobúdať podobu „*normatívnej vedeckej disciplíny, ktorá skúma formu, štruktúru a zákony správneho (t. j. logického) myslenia a usudzovania, tak ako sa prejavujú v jazyku,* [...] *abstrahujúc pritom od obsahu konkrétnych myšlienok a úsudkov.*“ Môžeme len špekulovať, čo všetko prispelo k objavu logiky v prvom z uvedených významov a ku vzniku logiky v druhom význame. Do akej miery to bola politická organizácia demokratických gréckych *polis*, rozvoj obchodu, právneho systému, filozofie a matematiky, v rámci ktorých sa nielen kultivuje logické myslenie a umenie argumentácie, no taktiež vzrastá úcta k týmto schopnostiam a vzniká dopyt po ľuďoch v nich zbehlých, schopných napr. zastupovať jednotlivé stránky v právnych sporoch či vyučovať iných tomuto umeniu. Zrejme to všetko malo na zrode logiky svoj podiel. Bolo by však naivné očakávať, že sa nám podarí podať dostatočne presvedčivé vysvetlenie pomocou čisto racionálnych dôvodov.

Ľuďom, ktorí sa zaoberali vyučovaním rétoriky ako rečníckeho umenia a umenia argumentácie, sa hovorilo *sofisti*, čo približne znamená *učitelia múdrosti*. Sofisti sa často nechávali najímať ako zástupcovia v právnych sporoch. Ich cieľom teda vo vše-

obecnosti bolo presvedčiť oponenta o správnosti svojho názoru. To ich viedlo k analýze jazyka a odhaľovaniu jeho vnútornej štruktúry, ktorá odlišuje všeobecne platné argumenty od tých ostatných. Sofisti takto odhalili a používali *zákon sporu*, *zákon vylúčenia tretieho* a pod. Utilitárny charakter ich profesie však spôsobuje, že ich logika sa dostáva do područia *eristiky*, čo možno voľne preložiť ako umenie viesť spor. Dôležitejším než hľadanie pravdy alebo správnosť úsudkov sa stáva vyvrátenie či aspoň spochybnenie argumentov protivníka, a taktiež tvorba zdanlivo logicky správnych argumentov, ktoré vedú k želaným záverom a je ťažké ich vyvrátiť. Zároveň, ako vedľajší produkt slúžiaci najmä na pobavenie publika, sa objavuje množstvo naoko správnych argumentov tzv. *sofizmov*, vedúcich k absurdným záverom. Niektoré sofizmy však nadobudli charakter *paradoxov*, naznačujúcich hranice možností logiky a pojmového uchopenia sveta v jazyku vôbec. Ukážme si niekoľko príkladov.

Sofizmus *Rohatý*, pripisovaný Eubulidovi z Milétu (4. stor. p. n. l.):

Čo si nestratil, máš.
Nestratil si rohy.
Teda máš rohy.

Samotná úvaha je z logického hľadiska správna. Očividne nepravdivý je však prvý predpoklad. Preto by nemalo prekvapiť, že ani záver nie je pravdivý.

Sofizmus pripisovaný bratom Euthydémovi a Dionýzodorovi (5. stor. p. n. l.):

Tento pes je tvoj.
Tento pes je otec.
Teda tvoj otec je pes.

Tu je chyba menej očividná. Slová *otec* a *pes* tu vystupujú v dvoch odlišných rolách. Jednak označujú vlastnosť „byť otcom“, resp. „byť psom“, jednak konkrétnu osobu (tvoj otec), resp. konkrétneho psa (tento pes). Trik spočíva v tom, že tieto dvojaké roly sa zámerne nerozlišujú. Označme $O(x)$ vlastnosť (predikát) „byť otcom“, $P(x)$ vlastnosť „byť psom“ a $T(x)$ a vlastnosť „patriť tebe“ (t. j. adresátovi úvahy). Nech ďalej o označuje tvojho otca a p tohto psa. Uvedená úvaha má potom tvar

$T(p)$
$O(p)$
Teda $P(o)$

Takáto úvaha nie je logický platná, lebo jej predpoklady (čo aj pravdivé) nevypovedajú nič o objekte o vyskytujúcom sa v závere. Úvahu nemožno zachrániť ani pridaním ďalších troch pravdivých premís $O(o)$, $T(o)$ a $P(p)$, ktoré sú v úvahe zamlčané, no v jej psychologickom účinku sa s nimi počíta. Žiadna z uvedených premís totiž neustanovuje akýkoľvek vzťah medzi uvažovanými predikátmi $O(x)$, $P(x)$ a $T(x)$.

Nasledujúci sofizmus, pripisovaný asi najznámejšiemu zo sofistov, Protagorovi z Abdér (okolo 485 – 410 p. n. l.), však už žiadne jednoduché riešenie nemá.

Paradox Protagorovho žiaka. Istý mladý muž nastúpil k Protagorovi do učenia. Podľa dohody mal svojmu učiteľovi zaplatiť odmenu až po ukončení štúdia, keď vyhrá svoj prvý súdny spor. Mladík štúdium ukončil, avšak žiadny spor neviedol, a tak podľa dohody ani nesplácal odmenu svojmu majstrovi. Napokon Protagorovi došla

trpezlivosť, vyzval študenta, aby zaplatil, a pohrozil mu súdnou žalobou. K tomu na vysvetlenie dodal: „Súd Ťa k zaplateniu odmeny buď odsúdi alebo neodsúdi. V prvom prípade budeš musieť zaplatiť na základe rozhodnutia súdu, v druhom podľa našej dohody, pretože si vyhral svoj prvý spor.“ Žiak dobre vyškolený samotným Protagorom sa však nezľakol a odvetil: „Nezaplatím ani v jednom prípade. Keď ma súd odsúdi k zaplateniu, tak som svoj prvý spor nevyhral, preto podľa našej dohody nezaplatím. Keď ma súd k zaplateniu neodsúdi, nezaplatím na základe rozhodnutia súdu.“

Ďaleko najslávnejším sofizmom je však *Paradox klamára*, známy aj ako *Epimenidov paradox*, pripisovaný opäť Eubulidovi. V ňom Kréťan Epimenides prednesie výrok:

„*Všetci Kréťania sú klamári.*“

Týmto paradoxom sa budeme podrobnejšie zaoberať až v kapitole venovanej Gödelovým vetám o neúplnosti.

Ďalším zdrojom logiky, spočiatku nazývanej *dialektikou*, je grécka filozofia. V jej rámci sa postupne vynára a presadzuje názor, že základným poslaním filozofie je odlíšiť zdanie od skutočnosti a získať o svete isté a nepochybné poznanie. To predovšetkým znamená spoznať poriadok sveta (*logos*), teda to, čo je vo svete stále a nemenné. Jednotlivé úkazy a veci sú naopak premenlivé, dočasné a nestále. Preto treba cez javy preniknúť k ich podstatám a za zmenami odhaliť ich zákonitosti a z nich potom spätne vyložiť i zmeny, ktorým podliehajú. Zdrojom takého poznania však nemôžu byť zmysly, ktoré nás často klamú, ani naša každodenná skúsenosť. Tá môže naše uvažovanie síce podnietiť, ale k pravému poznaniu môžeme dospieť len po ceste myslenia a rozumu.

Táto tendencia sa prejavuje už v predsokratovskej filozofii, najmä u Parmenida (okolo 540 – 470 p. n. l.) a jeho nasledovníkov, príslušníkov školy, ktorú založil v meste Elea na juhu Itálie. Parmenides vykladá svet ako jediné nemenné a večné súcno, ktorému hovorí *Bytie* alebo *Jedno*. Toto Bytie *je*, lebo Bytie nemôže nebyť, a *je* len Jedno a ne-Bytie *nie je*. Pri všetkej úcte, na súčasníka to celé pôsobí ako jedna nafúknutá znáška tautológií, až má človek problém brať to vážne.

Na podporu učenia svojho majstra vypracoval jeho žiak Zenón (okolo 490 – 430 p. n. l.) dômyselný súbor úvah, známych ako *Zenónove apórie*, dokazujúcich nemožnosť pohybu. Zenón zakaždým pripustí, že dochádza k pohybu a na základe tohto predpokladu (spolu s dodatočnými predpokladmi, na ktoré ešte upozorníme) dospieva k sporu v podobe absurdného dôsledku, z čoho vyvodzuje záver o nemožnosti pohybu. Uvedomme si, že ide o záver protirečiaci bežnej skúsenosti, jeho presvedčivosť preto spočíva výlučne na nezvratnosti použitých logických argumentov. Ide zrejme o najstarší doložený príklad argumentácie tohto druhu. Navyše svojím nástojčivým poukazom na spornosť pojmového uchopenia pohybu predstavujú Zenónove apórie permanentnú výzvu v antickom duchu zrodenej vede – matematike, fyzike a filozofii zvlášť – ktorá ani časom nestratila na aktuálnosti. Napokon, nech čitateľ posúdi sám.

Dichotómia. Nejestvuje žiaden pohyb, lebo to, čo sa pohybuje, musí najprv dospieť do polovice cesty, skôr než dospeje do konca. Ale aby to dospelo do polovice cesty, musí to ešte predtým dospieť do polovice tejto polovice atď. Takže pohyb sa ani nemôže začať.

Achilles a korytnačka. Achilles, najrýchlejší z ľudí, nemôže dobehnúť korytnačku, najpomalšiu z tvorov, ak sa vydala na cestu pred ním. Najprv by totiž prenasledovateľ musel dospieť do miesta, odkiaľ unikajúci vyrazil, potom do miesta, kde bol unikajúci v okamihu, keď prenasledovateľ dospel do východiskového bodu atď. Takže pomalá korytnačka bude pred rýchlonohým Achillom vždy o určitý úsek popredu.

Letiaci šíp. Pripusťme, že všetko v každom okamihu sa nachádza na svojom mieste a je buď v kľude alebo v pohybe. Ak sa letiaci šíp nachádza v každom okamihu na svojom mieste, tak je v každom jednotlivom okamihu nehybný, teda sa nemôže pohybovať. Ak by sa totiž v nejakom okamihu pohyboval, nebol by v tomto okamihu na svojom mieste, teda nebol by vlastne nikde.

Štadión. Nech sa dva rady, pozostávajúce z rovnakého počtu rovnako veľkých telies, pohybujú po pretekárskej dráhe štadióna oproti sebe rovnakými rýchlosťami. Ak pripustíme, že pohyb sa odohráva zmenami polohy o rovnaké malé, ďalej už nedeliteľné dĺžkové jednotky v rovnako krátkych, ďalej už nedeliteľných jednotkových okamihoch, tak v okamihu, za ktorý sa posunie prvý rad voči štadiónu o jednotku, druhý rad sa tiež posunie voči štadiónu o jednotku, lenže v opačnom smere. Jeden rad sa tak vzhľadom na druhý posunie za ten istý čas o dve jednotky. Teda dve dĺžkové jednotky sa rovnajú jednej jednotke a dva jednotkové časové okamihy sa rovnajú jednému takému okamihu.

Všimnite si, že v prvých dvoch apóriách Zenón vychádza z predpokladu neohraničenej deliteľnosti priestoru a času, kým v druhých dvoch vychádza z opačného predpokladu, že priestor a čas sa skladajú z najmenších ďalej už nedeliteľných častí (hoci explicitne je tento predpoklad vyslovený len v *Štadióne*). Zatiaľ čo prvá a tretia apória ukazujú nemožnosť absolútneho pohybu, druhá a štvrtá vyvracajú možnosť pohybu relatívneho.

Na rozdiel od sofistov, u ktorých prevláda poňatie logiky ako *eristiky*, t. j. umenia viesť spor s cieľom vyvrátiť stanovisko protivníka, rozvíja sa aj tzv. *dialektická logika* ako umenie viesť dialóg s cieľom spoločne hľadať pravdu. Neprekonateľným majstrom v tomto umení je Sokrates (469 – 399 p. n. l.), jedna z najvplyvnejších osobností západného myslenia, vynárajúca sa na jeho úsvite. V sokratovských dialógoch, tak ako nám ich podáva Sokratov žiak Platón (427 – 348 p. n. l.), sa typicky hľadá odpoveď na otázku položenú Sokratom alebo niektorým z jeho hostí, medzi ktorými je obvykle aj uznávaný odborník na daný problém. Prvá odpoveď zvykne zodpovedať všeobecne prijímanému názoru. Sokrates sa potom dožaduje podrobnejšieho vysvetlenia a žiada od návštevníkov jasné definície používaných pojmov. Ako kladie ďalšie otázky, návštevník vo svojich odpovediach obvykle dospeje k názoru, ktorý protirečí jeho pôvodnému stanovisku. Ak sa spoločnosť zhodne a prijme tento nový názor, Sokrates ho svojimi otázkami opäť spochybní. A táto schéma sa opakuje viackrát. Občas majú účastníci pocit, že sa postupne približujú k pravde, častejšie si však uvedomujú, že len hlbšie spoznávajú vlastnú nevedomosť, ku ktorej sa od začiatku hlási aj samotný Sokrates.

Prvá grécka filozofická škola zameraná na logiku vznikla v gréckom meste Megara na polceste medzi Aténami a Korintom. Jej zakladateľ, Euklides z Megary (okolo 435 – 365 p. n. l.), často zamieňaný s Euklidom z Alexandrie (okolo 300 p. n. l.), autorom *Základov*, bol žiakom Sokrata a ctiteľom Zenóna. Patril k nej aj už spomínaný Eubu-

lides z Milétu, autor viacerých známych sofizmov a paradoxov. S ňou úzko spriaznená bola aj tzv. dialektická škola reprezentovaná Diodorom Kronom (? – asi 284 p. n. l.) a Filónom z Megary (3. stor. p. n. l.). Diela megarikov ani dialektikov sa nedochovali, vieme o nich len sprostredkovane zo spisov iných autorov, napr. z Platónovho dialógu *Theaitétos*, ktorý je považovaný za pôvodne Euklidovo dielo. Vie sa, že megarici o. i. obohatili eristiku o metódu vyvodzovania absurdných záverov zo stanovísk, ktoré chceli spochybniť či vyvrátiť. Filón sa údajne dopracoval k chápaniu implikácie vo význame zhodnom so súčasným.

Základy logiky ako vedeckej disciplíny však položil až Aristoteles zo Stageiry (384 – 322 p. n. l.) vo svojom päťzväzkovom diele od stredoveku súborne označovanom ako *Organon* (t. j. *Nástroj*). Obsah jeho jednotlivých častí možno stručne a zjednodušene zhrnúť takto:

Kategórie zavádzajú klasifikáciu jednoduchých pojmov (podstatných mien), ktoré môžu byť subjektom, resp. predikátom nejakých tvrdení, do desiatich typov (kategórií).

O vyjadrovaní je rozborom kategoriálnych tvrdení na jednoduché pojmy a základné zložky ich logickej štruktúry ako negácia a protiklad, obrátenie (konverzia) ako aj znaky kvantity. S využitím subjekt-predikátových premenných je tu podaný náznak „kombinatorickej analýzy“ možných typov kategorických sylogizmov. Taktiež sa tu objavujú úvahy o možnosti, náhodilosti a nevyhnutnosti ako aj o platnosti výpovedí o budúcnosti, čiže zárodky modálnej a temporálnej logiky.

Prvé analytiky sú formálnym rozborom podmienok zaručujúcich správnosť logicky platných úsudkov (kategorických sylogizmov).

Druhé analytiky sa zaoberajú dôkazmi tvrdení, definíciami pojmov a klasifikáciou vedeckých poznatkov. Zatiaľ čo v *Prvých analytikách* sa kladie dôraz na formálny aspekt sylogistickej logiky, v *Druhých analytikách* sú logické úvahy analyzované najmä z hľadiska ich obsahu. Sú tu rozlíšené tzv. *apodiktické sylogizmy*, ktorých premisy sú isté a pravdivé, teda prinášajú aj pravdivé a isté závery, a tzv. *dialektické sylogizmy*, ktorých premisy, teda aj závery sú neisté.

Topiky podrobnejšie skúmajú dialektické dôkazy a snažia sa stanoviť stupeň ich vierohodnosti. Sylogizmy, ktoré budia klamný dojem správnosti, či už z hľadiska formy alebo obsahu, sa nazývajú sofistické. Dodatok *O sofistických dôkazoch* (často uvádzaný ako samostatný šiesty diel) je venovaný odhaľovaniu a kritike chýb, ktoré sa v nich ukrývajú. Je tu klasifikovaných trinásť typov klamných argumentov.

Z hľadiska nášho kurzu je najdôležitejšie štúdium kategorických sylogizmov, ktoré preniká celým *Organonom*. Kategorický sylogizmus je v úvode *Topikov* definovaný ako *„reč (logos), v ktorej, ak je niečo dané, niečo rôzne od toho, čo je dané, vyplýva práve tým, že dané jest“*. I keď z dnešného hľadiska je Aristotelova náuka o kategorických sylogizmoch púhym fragmentom monadickej logiky prvého rádu (t. j. logiky unárnych predikátov), tendencie označiť ju na základe toho za triviálnu, objavujúce sa z času na čas od začiatku 20. storočia, sú len dokladom nepochopenia a nedocenenia epochálneho významu kroku, ktorý tento veľký antický mysliteľ a polyhistor učinil ako prvý.

Na Aristotela nadväzujú jeho nasledovníci, príslušníci ním založenej peripatetickej školy, ktorí obohatili jeho sylogistiku napr. o štúdium foriem hypotetických úsudkov.

Z nich najvýznamnejší sú Theofrastos z Eresu na Lesbe (okolo 372 – 287 p. n. l.), považovaný za zakladateľa botaniky a dendrológie, a Eudémos z Rhodu (okolo 370 – 300 p. n. l.), známy aj ako vydavateľ Aristotelových diel a historik gréckej matematiky a astronómie.

Aristotelom a peripatetikmi je ovplyvnená aj stoická škola pôsobiaca na Cypre, ktorej najvýznamnejšími predstaviteľmi boli Zenón z Citia (okolo 334 – 262 p. n. l.) a Chrysippos zo Soloi (282 – 206 p. n. l.). Hoci stoicizmus je predovšetkým filozofia morálnych zásad a životných postojov (spomeňme napr. príslovečný stoický kľud), stoickí myslitelia vniesli nezanedbateľný vklad aj do rozvoja logiky. Kým Aristotelova logika sa primárne zaoberá analýzou vzťahu vyplývania medzi subjekt-predikátovými výpoveďami, v stoickej logike sú položené základy výrokového počtu. *Výrok* je chápaný ako zmysluplná výpoveď, ktorá je buď pravdivá alebo nepravdivá. Z daných výrokov možno tvoriť nové pomocou logických spojok negácie, konjunkcie, disjunkcie (chápanej vo vylučovacom zmysle) a implikácie. Práve *implikácia* hrá v stoickej logike zásadnú úlohu, pričom (podobne ako u Filóna) je chápaná vo význame, aký jej prisudzujeme podnes: výrok $A \Rightarrow B$ je nepravdivý jedine v tom prípade, keď jeho predpoklad A je pravdivý a záver B nepravdivý. Popri tom sa uvažuje aj o implikácii (vyplývaní) vo význame *pravdivého úsudku*, t. j. úsudku, v ktorom je z pravdivých premís logicky správne odvodený záver, čím je automaticky zaručená jeho pravdivosť. Stoici objavili a zosystematizovali viacero odvodzovacích pravidiel, ktoré formulovali s použitím radových čísloviek v úlohe výrokových premenných. Na ilustráciu uvádzame štyri ukážky pod názvami, ktoré dostali v stredoveku, kvôli prehľadnosti zapísané s použitím súčasnej notácie:

z $A \Rightarrow B$ a A odvoď B (modus ponens)

z $A \Rightarrow B$ a $\neg B$ odvoď $\neg A$ (modus tollens)

z $\neg(A \wedge B)$ a A odvoď $\neg B$ (modus ponendo tollens)

z $(A \wedge B) \Rightarrow C$, A a $\neg C$ odvoď $\neg B$ (pravidlo antilogizmu)

Pomocou svojho deduktívneho systému stoici tiež analyzovali známe antické paradoxy a sami objavili či vytvorili rad ďalších. Z pôvodných spisov gréckej stoickej školy sa toto veľa nezachovalo, vieme o nich najmä z diela Diogena Laertia (asi 180 – 240 n. l.) *Životy a názory významných gréckych filozofov* napísaného v 3. storočí n. l. Stoická škola však našla pokračovanie v starom Ríme. Hlásili sa k nej napr. Lucius Annaeus Seneca (4 p. n. l. – 65 n. l.), Marcus Aurelius (121 – 180 n. l.) a do istej miery aj Marcus Tullius Cicero (106 – 43 p. n. l.). Logika však už nebola v centre ich záujmu.

Aristotelovu sylogistiku i výrokovú logiku stoikov významne obohatil aj slávny antický lekár a anatóm Galénos (okolo 130 – 200 n. l.). Vo svojom *Úvode do logiky* Galénos rozlišuje disjunkciu vo vylučovacom zmysle (buď ... alebo ...) a alternatívu v nevylučovacom zmysle (... alebo ...), ako aj implikáciu a obojstrannú implikáciu (ekvivalenciu). Taktiež študuje otázku vzájomnej zameniteľnosti (t. j. logickej ekvivalencie) formálne rôznym spôsobom utvorených výrokov, čím vlastne predjíma pojem tautológie. Zároveň uňho nachádzame zárodky logiky dvojmiestnych predikátov, t. j. binárnych relácií, u ktorých si všíma napr. možnosť obrátenia (inverzie) a otázky symetrie. V logických úsudkoch pripúšťa tiež premisy tvorené konjunkciou viacerých jednoduchých predpokladov. Nadobudnuté logické poznatky aplikuje napr. pri svojich analýzach anatomických popisov a liečebných postupov.

Logika v staroveku sa však nerozvíjala iba v rámci antickej filozofie, na pôde ktorej sa postupne osamostatňovala. Nemenej dôležitý vklad do logiky predstavuje aj grécka matematika, v rámci ktorej sa umenie argumentácie rozvíja a kultivuje zásadným spôsobom. Toho vrcholnou ukážkou je trinásťzväzkové dielo Euklida z Alexandrie *Základy* ($\Sigma\tau o\iota\chi\varepsilon\iota\alpha$) napísané niekedy na prelome 4. a 3. storočia p. n. l. V nich sú uceleným spôsobom zhrnuté a vyložené poznatky takmer celej dovtedy známej matematiky: rovinnej i priestorovej geometrie a aritmetiky. Najmä prvých šesť dielov venovaných planimetrii sa stalo na dlhé stáročia vzorom pre výstavbu akýchkoľvek deduktívnych teórií ašpirujúcich na exaktnosť.

Euklides začína dvadsiatimi tromi *definíciami* základných pojmov (bod, čiara, priamka, uhol, kruh...), opierajúc sa pritom o geometrický názor vyostrený pohľadom do ideálneho geometrického sveta. Ďalej stanovuje päť *postulátov*. Prvé tri postuláty možno chápať ako pokyny na riešenie najjednoduchších konštrukčných úloh (spojiť dva body priamkou, ľubovoľne predĺžiť danú usečku, narysovať kružnicu s daným stredom a polomerom). Ďalšie dva postuláty majú skôr charakter axióm: všetky pravé uhly sú si rovné; slávny piaty postulát v pôvodnom znení hovorí, že dve priamky preťaté treťou priamkou sa pretnú na tej strane, kde je súčet ich uhlov s treťou priamkou menší než dva pravé. Nasleduje deväť *axióm*, ktoré majú charakter pokynov k evidencii (nahliadnutiu) či jednoduchých metodologických zásad (veličiny rovné tomu istému sú si rovné, keď sa pridajú veličiny rovné k rovným aj celky sú si rovné, ..., celok je väčší než jeho časť). Z týchto základných pojmov a predpokladov Euklides prísne logicky odvodzuje ďalšie poznatky. Logika *Základov* však nie je samostatná disciplína ale majstrovsky používaný, i keď explicitne nešpecifikovaný nástroj. Táto logika nijako nenahrádza geometrický názor, ale z neho vychádza a ďalej mu slúži tým, že ho podporuje, dopĺňa a rozvíja.

Považuje sa za nepochybné, že Euklides poznal Aristotelovo dielo, vrátane jeho sylogistiky, ako aj logické spisy stoikov. Vo svojich *Základoch* sa však na ne nijako nedvoláva. Na druhej strane, logika, ktorú používa, je zreteľne bohatšia než aristotelovská či stoická logika: pri spätnom pohľade ju možno považovať za pomerne rozsiahly fragment logiky prvého rádu, bez obmedzenia sa na jednomiestne predikáty.

Euklidove *Základy* hlboko ovplyvnili a inšpirovali Mikuláša Kopernika (1473 – 1543), Galilea Galileiho (1564 – 1642), Johannesa Keplera (1571 – 1630), René Descarta (1596 – 1650) či Isaaca Newtona (1643 – 1727). Euklidova axiomatická metóda poslúžila za vzor aj Baruchovi Spinozovi (1632 – 1677) pre jeho najvýznamnejšie filozofické dielo *Ethica ordine geometrico demonstrata*. V ňom logicky vyvodzuje metafyzické, teologické a etické závery z vopred stanovených definícií a axióm. Hneď po *Biblii* sú *Základy* najprekladanejším a najvydávanejším knižným dielom všetkých čias.

Našu galériu antických logikov uzatvára ranokresťanský rímsky filozof Anicius Manlius Severinus Boëthius (asi 480 – 524 n. l.). Boëthius sprostredkoval stredovekej Európe plody antickej filozofie prekladmi diel Platóna, Aristotela a ďalších filozofov gréckej antiky do latinčiny. K viacerým z nich, napr k Aristotelovým logickým spisom, napísal tiež podrobné komentáre. K logike prispel aj vlastnými dielami, najmä *O kategorickom sylogizme* a *O hypotetickom sylogizme*. V nich sa pokúsil o syntézu Aristotelovej kategoriálnej sylogistiky a stoickej výrokovej logiky. Taktiež v nich podáva podrobnú kombinatorickú klasifikáciu formálnej štruktúry rôznych typov úsudkov.

Jeho logika, založená na štrukturálnej analýze latinského jazyka, výrazne ovplyvnila stredoveké myslenie a položila základy vplyvu Aristotelovho diela na scholastickú filozofiu a logiku.

2.2 Stredovek

Logika v stredoveku je pestovaná ako jedno zo *siedmich slobodných umení*. Tie zahŕňali tzv. *trívium*, t. j. tri slovesné umenia [gramatika, rétorika a logika (spájaná s filozofiou a nazývaná tiež dialektikou)] a tzv. *kvadrívium*, t. j. štyri číselné umenia [aritmetika, geometria, astronómia (spolu s astrológiou) a hudba (vrátane náuky o proporciách a harmónii)]. Už z tohto jej zaradenia je zrejmé, že stredoveká logika je oddelená od matematiky a príliš sa s ňou nezbližuje.

Vo vývoji stredovekej logiky možno vyčleniť tri obdobia. Prvé obdobie, nazývané tiež *stará logika* (*logica vetus*), siahá od konca antiky približne do polovice 12. storočia. Dostupnosť antických prameňov v tomto období je obmedzená na dve Aristotelove diela (*Kategórie* a *O vyjadrovaní*) s príslušnými Boëthiovými komentármi. Najvýznamnejším predstaviteľom „starej logiky“ je francúzsky scholastický filozof, logik, teológ, básnik a hudobný skladateľ Pierre Abélard (1079 – 1142).

Druhé obdobie, nazývané *nová logika* (*logica nova*), trvá približne od polovice 12. do konca 13. storočia. V tomto období je študované a komentované celé Aristotelovo dielo a ďalšie antické zdroje. Je dovŕšená kombinatorická klasifikácia kategorických sylogizmov aj odvodzovacích pravidiel výrokovej logiky. Značná pozornosť je venovaná otázkam modálnej a temporálnej logiky. Objavuje sa tiež viacero učebníc logiky a ustaľuje sa niečo ako ich kanonická podoba. K najvýznamnejším predstaviteľom „novej logiky“ patria cirkevní učenci Albert Veľký (asi 1193 – 1280), Peter Hispánsky (1205 – 1277), John Duns Scotus (1265/6 – 1308) a ďalší.

Tretie obdobie, nazývané *moderná logika* (*logica modernorum*), zaberá približne celé 14. a 15. storočie. Je charakterizované najmä ďalším zdokonaľovaním a systematizáciou metód a výsledkov predošlého obdobia a ich využívaním pri analýze stredovekej latiny. Študujú sa tiež antické paradoxy a hľadajú sa možnosti ich riešenia; popritom sa objavujú ďalšie. K najvýznamnejším predstaviteľom „modernej logiky“ patria William Ockham (1287 – 1347), Jean Buridan (asi 1300 – 1360), Albert Saský (1320 – 1390), Paolo Venetus (1369 – 1429) a ich žiaci.

Popri rozvoji ako samostatná disciplína sa logika v stredoveku cibrí aj vo filozofických a teologických dišputách a sporoch. K typickým otázkam, ktoré sa v nich riešia, patrí napr. otázka vzťahu predurčenia a slobodnej vôle a s ňou súvisiace otázky zodpovednosti človeka za vlastné činy a jeho možnosti ovplyvniť svojím konaním vlastnú spásu. Ďalej je to otázka logickej zlučiteľnosti božských atribútov (je napr. známe, že Božia vševedúcnosť a všemohúcnosť sú v spore), otázka možnosti dokázať Božiu existenciu logickými prostriedkami z princípov čistého rozumu, otázka, ako môže dobrotivý, milosrdný a zároveň všemohúci Boh pripustiť existenciu zla v ním stvorenom svete, či otázka, čo bolo, resp. kde bol a čo robil Boh pred stvorením sveta atď. Logika hrala dôležitú úlohu aj v metafyzickom spore medzi *realizmom* a *nominalizmom* o charakter *univerzálií*. Kým realizmus zastáva stanovisko, že univerzálie (všeobecné pojmy označujúce idey či vlastnosti a vzťahy, ako napr. *dobro*, *zlo*, *krása*, *priateľstvo*,

veľkosť, a pod.) majú reálne samostatné bytie, podľa nominalizmu sú univerzálie iba mená či názvy niektorých abstraktných ideí, vlastností a vzťahov, ktorým však nezodpovedajú žiadne samostatne existujúce reálne objekty. Sotva koho prekvapí, že ani jeden zo spomínaných problémov sa k všeobecnej spokojnosti vyriešiť nepodarilo.

V protiklade k tvorivému príspevku všestranne vzdelaných stredovekých učencov k rozvoju logiky a ich brilantným dišputám stojí *výuka* logiky v stredoveku a ešte dlho potom. Tá sa do značnej miery redukuje na *memorovanie* odvodzovacích pravidiel a kategorických sylogizmov, čím popiera svoj vlastný zmysel, ktorým by mala byť kultivácia logického myslenia. A tak sa, paradoxne, najznámejšími a najrozšírenejšími výsledkami stredovekej logiky stávajú rozmanité *mnemotechnické pomôcky*: *logický štvorec*, známy aj ako *štvorec opozít*, v ktorom sú prepojené štyri typy subjekt-predikátových súdov, či mnemotechnické kódy devätnástich sylogizmov rozdelených do štyroch figúr (I: Barbara, Celarent, Darii, Ferio; II: Cesare, Camestres, Festino, Baroco; III: Darapti, Disamis, Datisi, Felapton, Bocardo, Ferison; IV: Bramalip, Camenes, Dimaris, Fesapo, Fresison).

Úloha. Vyhľadajte na internete informácie o *logickom štvorci*, štyroch základných figúrach kategorických sylogizmov a mnemotechnických kódoch jednotlivývh sylogizmov. Na základe významu kódových samohlások a, e, i, o zrekonštruujte slovnú podobu sylogizmov zodpovedajúcich uvedeným 19 kódom a zapíšte ich pomocou stredovekej i súčasnej notácie. Napr. sylogizmus Ferio má slovné vyjadrenie:

žiadne M nie je P a niektoré S sú M, preto niektoré S nie sú P

a v stredovekej, resp. v modernej notácii vyzerá nasledovne:

z $M\,e\,P$ a $S\,i\,M$ odvoď $S\,o\,P$,

resp.

z $(\forall x)(M(x) \Rightarrow \neg P(x))$ a $(\exists x)(S(x) \wedge M(x))$ odvoď $(\exists x)(S(x) \wedge \neg P(x))$.

Odhaľte tiež význam začiatočných písmen B, C, D, F a spoluhlások m, p, r, s v názvoch jednotlivých kódov (obsahujú návod, ako možno ten-ktorý kód druhej až štvrtej figúry odvodiť z príslušného kódu prvej figúry).

2.3 Renesancia a novovek

Renesančné myslenie sa stavia k scholastike a stredovekému aristotelizmu značne kriticky. Špekulatívna filozofia a teológia strácajú na význame a do popredia sa dostáva pozorovanie prírody a experiment. Postupne sa presadzuje snaha, reprezentovaná najmä Galileom Galileim, vysvetliť prírodné javy a deje kauzálnym spôsobom, odhaliť ich zákonitosti, a to nielen ich kvalitatívne no taktiež ich kvantitatívne aspekty, a tie popísať jazykom matematiky. V tejto atmosfére sa i na stredovekú logiku aspoň na istý čas hľadí s dešpektom ako na jalové mudrovanie a nekonečné omieľanie banálnych poučiek.

Zmenu pohľadu prináša až novovek, menovite René Descartes, ktorý si uvedomuje, akú dôležitú metodologickú úlohu hrá logika v racionalistickej filozofii. Dokladom toho sú najmä jeho pojednania *Rozprava o metóde* (1637) a *Pravidlá na vedenie rozumu* (napísané v r. 1628, vydané však až v r. 1701). Descartova *Rozprava* a jeho *Pravidlá*, spolu s názormi Blaise Pascala (1623 – 1662), do veľkej miery ovplyvnili aj

Antoina Arnaulda (1612 – 1694) a Pierra Nicola (1625 – 1695) pri písaní učebnice *Logika čiže umenie myslieť* (vydanej najprv anonymne v Paríži v r. 1662), známejšej pod názvom *Logika z Port-Royal*, podľa pôsobiska jej autorov, kláštora Port-Royal de Champs. Aristotelovská logika v podobe, akú nadobudla v neskorom stredoveku, je v nej vyložená v duchu karteziánskeho dualizmu. V súlade s tým je prezentáciacia materiálu verbálna, bez využitia symboliky. V sémantike autori rozlišujú *obsah* (*intenziu*) a *rozsah* (*extenziu*) pojmu. Zároveň však do logiky vnášajú psychologizujúce hľadisko. Jej zmysel vidia nie v nej samej, ale v jej osvietensky poňatej úlohe pomôcť presadiť vo svete rozum a spravodlivosť. Kniha sa v pomerne krátkom čase dočkala prekladov do viacerých jazykov. Až do 19. storočia bola najvydávanejšou učebnicou logiky v Starom aj v Novom svete.

Osobitné postavenie v našom príbehu má významný polyhistor (matematik, filozof a diplomat) Gottfried Wilhelm Leibniz (1646 – 1716). Leibniz ako matematik je (popri Newtonovi) známy najmä ako jeden z tvorcov infinitezimálneho počtu. Jeho prístup sa zakladal na využití nekonečne malých (a nekonečne veľkých) veličín; ním zavedené označenie $\frac{\mathrm{d}y}{\mathrm{d}x}$ pre deriváciu a $\int f(x)\,\mathrm{d}x$ pre integrál sa používa dodnes. Leibniz si tiež dopisoval s práve spomínaným Arnauldom. Svoj cit pre prácu so symbolmi prejavil aj pri návrhu logickej notácie, ktorá však nebola publikovaná za jeho života, a keď na prelome 19. a 20. storočia k tomu došlo, bola už prekonaná, takže dovtedajší vývoj nestihla a ďalší nedokázala ovplyvniť.

Leibniz však ovplyvnil vývoj európskeho myslenia, najmä logiky, aj svojou víziou nadväzujúcou na katalánskeho stredovekého mystika Ramóna Lulla (1232 – 1316). Lull je tvorcom systému tabuliek a diagramov *Ars Magna*, ktorý mal umožniť v symbolickej podobe zhromaždiť univerzálne východiskové princípy poznania a z nich mechanickými kombináciami podľa logických pravidiel odvodzovať ďalšie (potenciálne všetky) poznatky. V rámci toho by sa malo podariť – mimo každú pochybnosť – dokázať aj dogmy kresťanskej teológie. Leibniz zdieľal Lullovu predstavu o objavovaní právd vyčerpávajúcim spôsobom tvorbou tvrdení vhodnými kombináciami pojmov. Jeho pojednanie *De arte combinatoria* (1666) obsahuje náčrt tohto „projektu“. Podobné projekty kruto paroduje Jonathan Swift (1667 – 1745) v tretej z *Gulliverových ciest* (1726), v jednej zo scén Gulliverovej návštevy Veľkej Akadémie v Lagado.

Leibniz neskôr pojal zámer vypracovať *univerzálny charakteristický jazyk* (*lingua characteristica universalis*), v ktorom by základné pojmy boli reprezentované číslami alebo inými pre ne charakteristickými symbolmi a zložitejšie pojmy súbormi symbolov zodpovedajúcich jednoduchším pojmom, z ktorých pozostávajú, tak, aby takto vzniknuté grafické útvary boli ľahko uchopiteľné a zrozumiteľné čitateľom bez ohľadu na to, akým jazykom hovoria. Inšpiráciou mu boli egyptské hieroglyfy a čínske obrázkové písmo, ako aj algebraická symbolika, ktorú zaviedol francúzsky matematik François Viète (1540 – 1603). Ďalej hodlal rozpracovať tzv. *calculus ratiocinator*, univerzálny „rozumový kalkul“ umožňujúci výpočty s pojmami a tvrdeniami zostavenými zo znakov univerzálnej charakteristiky, ako aj tzv. *ars iudicandi*, t. j. metódu, pomocou ktorej by bolo možné rozhodnúť o pravdivosti či nepravdivosti každého takto symbolicky reprezentovaného tvrdenia.

Ciele, ktoré tým Leibniz sleduje, nie sú nijako skromné. Pokrok všetkých vied, medzi nimi i matematiky, by bol len jedným, a vôbec nie najdôležitejším dôsledkom. Všetky spory medzi jednotlivcami i vojny medzi národmi by prestali. Ak by sa aj vy-

skytli nejaké nezhody či názorové rozdiely, stačilo by si spoločne sadnúť a počítať. Tak by sa zaraz zistilo, kto má pravdu, a túto s nezvratnou jasnosťou a presvedčivosťou spoznanú pravdu by všetci, samozrejme, prijali a rešpektovali. Ľudstvo by mohlo postupne objavovať a nakoniec vyčerpať všetky pravdy. Medzi nimi miesto najpoprednejšie zaujme Pravda o Božej existencii a pravom náboženstve, „ktoré sa najväčšmi zhoduje s rozumom, a nabudúce sa bude treba obávať odpadnutia od neho práve tak málo, ako sa treba obávať odvrátenia sa ľudí od aritmetiky a geometrie, keď sa ich už raz naučili."

Akokoľvek naivne a utopicky nám môžu Leibnizove nádeje pripadať dnes, jeho projektu nemožno uprieť veľkoleposť. Pokiaľ ide o metódy, jeho génius predbehol svoju dobu o takmer tri storočia a presne predvídal smery ďalšieho rozvoja matematickej logiky: výrokový a predikátový počet, Gödelovu aritmetizáciu metamatematiky, ako aj symbolickú reprezentáciu dát a poznatkov využívanú pri počítačovej implementácii a spracovaní. Keď si zároveň uvedomíme, ako ďaleko sme napriek všetkému dosiahnutému vedeckému a technologickému pokroku od naplnenia Leibnizovho sna o večnom mieri, ťažko sa ubránime pocitu márnosti, beznádeje a sklamania z nepoučiteľného a nepolepšiteľného ľudského pokolenia.

V 18. storočí sa logikou zapodievalo viacero učencov, ktorých vedecké a filozofické záujmy mali, podobne ako u Leibniza, podstatne širší záber. Za všetkých spomeňme len z Alsaska pochádzajúceho nemeckého matematika, astronóma, fyzika a filozofa Johanna Heinricha Lamberta (1728 – 1777). Lambert ako prvý dokázal iracionalitu čísla π a svojou štúdiou *Teória rovnobežných priamok* (1766) sa stal jedným z predchodcov neeuklidovskej geometrie. Jeho práce *Photometria* (1760) a *Pyrometria* (1779) predstavujú dôležité príspevky k teórii svetla, resp. tepla. Jeho hlavné filozofické dielo *Nové Organon* (1764) prinieslo prenikavú analýzu množstva otázok týkajúcich sa o. i. formálnej logiky, pravdepodobnosti a metodológie vedy. Spolu s anglickým matematikom, astronómom a výrobcom vedeckých prístrojov Thomasom Wrightom (1711 – 1786) a nemeckým filozofom Immanuelom Kantom (1724 – 1804), s ktorými si dopisoval, patril k prvým, kto rozpoznal, že špirálovité hmloviny viditeľné hvezdárskym ďalekohľadom na nočnej oblohe sú hviezdne galaxie diskovitého tvaru podobné našej Mliečnej dráhe.

Na druhej strane bol to práve Kant, kto vo svojom najvplyvnejšom filozofickom diele *Kritika čistého rozumu* (*Kritik der reinen Vernunft*, 1781) vyslovil myšlienku, že logika je prakticky zavŕšená disciplína, ku ktorej už nemožno dodať nič podstatné. Keď uvážime, aký malý bol pokrok, ktorý dovtedy urobila logika od čias Aristotelových, nemožno sa mu ani veľmi čudovať. Už približne o polstoročie neskôr sa však malo ukázať, že to bol fatálny omyl. A nebol to jediný Kantov omyl, ktorý – podporený jeho nesporne zaslúženou autoritou – na istý čas zbrzdil prirodzený vývoj vedy. Ešte známejšou ukážkou toho je Kantova téza o absolútnom charaktere priestoru a času ako čistých apriórnych foriem nášho názoru, mimo ktorých nie je možné zmyslové vnímanie a poznávanie. Pritom tento priestor je totožný s priestorom euklidovskej geometrie a iný priestor si ani nemožno predstaviť. Táto Kantova téza bola pravdepodobne jedným z dôvodov, kvôli ktorým sa Carl Friedrich Gauss (1777 – 1855), jeden z najväčších matematikov všetkých čias, zdráhal zverejniť svoje objavy týkajúce sa neeuklidovskej geometrie. Medzitým však dozrel čas nato, aby neuklidovská geometria uzrela svetlo sveta.

2.4 Neeuklidovská geometria

Neuklidovská geometria zohrala vo vývoji logiky pozoruhodnú a nie plne docenenú úlohu. Jej vznik ide na vrub už spomínaného piateho Euklidovho postulátu. Ten býva najčastejšie formulovaný v znení, v ktorom ho uvádza novoplatónsky filozof Proklos z Lýkie (asi 410 – 485 n. l.) vo svojich *Komentároch k Euklidovi*:

> *S danou priamkou možno bodom, ktorý na nej neleží, viesť práve jednu rovnobežku.*

Toto znenie nájdeme aj u anglického klerika a matematika Williama Ludlama (1717 – 1788), pomenované je však po škótskom prírodovedcovi a matematikovi Johnovi Playfairovi (1748 – 1819), ktorý ho uvádza vo svojom diele *Základy geometrie* (*Elements of Geometry*, 1795). *Playfairova axióma* je v úplnej zhode s geometrickým názorom, stále je však formulovaná podstatne zložitejšie než zvyšné Euklidove axiómy a postuláty. To vyvoláva podozrenie, že piaty postulát – či už v pôvodnej alebo v takto modifikovanej podobe – by sa mal dať zo zvyšných axióm a postulátov dokázať, teda, že je vlastne zbytočný. O jeho dôkaz sa skutočne pokúšalo viacero učencov a niektorí z nich boli dokonca presvedčení, že sa im to naozaj podarilo. Zakaždým však vyšlo najavo, že ich „dôkaz“ sa popri zvyšných Euklidových axiómach a postulátoch opieral aj o nejaké ďalšie tvrdenie, ktoré bolo natoľko v zhode s geometrickým názorom, že ho považovali za samozrejmé. A práve toto tvrdenie bolo len inou, ekvivalentnou formuláciou piateho postulátu.

Keď sa rozhodneme poprieť piaty postulát a trváme pritom na homogénnosti priestoru, teda, že žiadny bod či priamka v ňom nemajú výsadné postavenie, tak máme len dve možnosti. Buď musíme prijať postulát, že s danou priamkou nemožno bodom, ktorý na nej neleží, viesť žiadnu rovnobežku, čo má za následok, že ľubovoľné dve rôzne priamky sa pretnú v jedinom bode. Alebo musíme prijať postulát, že s danou priamkou možno bodom, ktorý na nej neleží, viesť aspoň dve rôzne rovnobežky, čo má za následok, že takýchto rovnobežiek bude dokonca nekonečne mnoho.

V prvom prípade možno ďalej odvodiť, že všetky priamky majú konečnú dĺžku, čo protirečí druhému postulátu, podľa ktorého možno každú danú úsečku ľubovoľne predĺžiť. Tým je prvý prípad vybavený ako nemožný a ďalej sa ním netreba zapodievať. [O tom, ako si s týmto prípadom poradil Bernhard Riemann (1826 – 1866) a vytvoril tým tzv. *eliptickú geometriu*, už v našom kurze písať nebudeme.] Zostáva teda len druhý prípad; v ňom však postupne dospejeme k podivným záverom, ktoré budeme náchylní považovať za absurdné. Napríklad, že súčet vnútorných uhlov v ľubovoľnom trojuholníku je menší než dva pravé a klesá s rastúcim obsahom trojuholníka. Špeciálne keď budeme konštruovať rovnoramenný pravouhlý trojuholník, ktorého základňa leží na danej priamke p a výška na danej kolmici na túto priamku, tak oba uhly, ktoré zvierajú ramená tohto trojuholníka s priamkou p, budú menšie ako polovica pravého uhla a s rastúcou výškou bude ich veľkosť klesať. No nielen to: existuje istá medzná hodnota, ktorú keď výška dosiahne či presiahne, tak trojuholník nebude viac možné zostrojiť, lebo jeho zamýšľané ramená nikdy nepretnú priamku p; inak povedané, na seba kolmé priamky v predĺžení týchto ramien budú rovnobežné s priamkou p. Je záležitosťou osobného vkusu, kedy toho už budeme mať dosť a nejaký podobný záver prehlásime za sporný. Nebude to však spor s rozumom (t. j. logický spor), ale iba spor s naším geometrickým názorom. A – ako sa zakaždým ukázalo – popretie

príslušného „absurdného“ záveru bolo *logicky ekvivalentné* s piatym postulátom. Na druhej strane možno na tieto „absurdné“ dôsledky pozerať ako na historicky prvé teorémy novej tzv. *hyperbolickej geometrie*.

Naladenosť prieskumníkov voči podivnému svetu, ktorý sa im nenápadne otváral a oni doňho bázlivo nazerali, sa však postupne mení. Na základe jeho sporu s prirodzeným geometrickým názorom ho zavrhujú napr. islamskí učenci Thabit Ibn Qurra (asi 830 – 901), Hassan Ibn al-Haytham (asi 965 – 1040) či Omar Chajjám (1048 – 1131), aj talianski učenci 17. a začiatku 18. storočia Giovanni Alfonso Borelli (1608 – 1679), Giordano Vitale (1633 – 1711) a Giovanni Girolamo Saccheri (1667 – 1733). A tento spor podľa svojho vlastného názoru považujú za dôkaz piateho postulátu. Napríklad Saccheri vo svojom krátko pred smrťou vydanom pojednaní *Euklides každej poškvrny zbavený* (*Euclides vindicatus*, 1733) dospieva k záveru, že v rovine, v ktorej by neplatil piaty postulát, by neexistoval žiadny štvorec. Ak teda uznáme platnosť „samozrejmého faktu“, že v rovine existuje aspoň jeden štvorec, budeme na základe toho schopní dokázať piaty postulát. Saccheri napriek tomu vábeniu podivného neeuklidovského sveta očividne podlieha a váhavo ho pripúšťa ako logicky možný, avšak odporujúci skutočnému svetu. Prvý, kto otvorene priznáva, že ho svet neeuklidovskej geometrie láka, a želá si, aby bol popri euklidovskom svete tiež aspoň logicky možný, je už spomínaný Lambert v r. 1766.

V r. 1807 vydáva nemecký právnik a amatérsky matematik Ferdinand Karl Schweikart (1780 – 1857) štúdiu s veľavravným názvom *Teória rovnobežných priamok spolu s návrhom na jej vypudenie z geometrie* a v r. 1818 píše v liste Gaussovi o dvojakej geometrii. Ide jednak o geometriu v užšom zmysle (čím myslí euklidovskú geometriu) a všeobecnú, tzv. *astrálnu geometriu*, v ktorej je súčet vnútorných uhlov v trojuholníku menší než dva pravé. Jeho myšlienky ďalej rozvíja jeho synovec, matematik Franz Adolph Taurinus (1794 – 1874). Ten ešte v r. 1825 vo svojej práci *Teória rovnobežných priamok* dokazuje, že euklidovská geometria je jediná možná. No už rok na to vydáva spis *Geometriae prima elementa*, v ktorom modeluje astrálnu geometriu ako „geometriu na sfére s imaginárnym polomerom“ a nazýva ju *logaritmicko-sférickou geometriou*. V ňom Taurinus zároveň pripúšťa možnosť geometrie, v ktorej by súčet uhlov v trojuholníku bol väčší než dva pravé, čím predjíma Riemannovu eliptickú geometriu. Takúto geometriu možno (po stotožnení dvojíc antipodálnych bodov) realizovať ako geometriu na sférickom povrchu. Taurinus však stále priznáva euklidovskej geometrii výsadné postavenie a považuje ju za jedinú pravú geometriu.

Gaussovi sa neeuklidovský geometrický svet začal otvárať približne v r. 1795 a pravdepodobne okolo r. 1800 sa už v tomto svete bezpečne orientoval. Postupne si uvedomil, že tie „absurdné“ dôsledky popretia piateho postulátu nepredstavujú logický spor, ale patria k vlastnostiam novej geometrie, ktorú neskôr nazval *neeuklidovskou geometriou*. O dôvodoch, pre ktoré nič z nadobudnutých poznatkov neuverejnil, sa môžeme len dohadovať. Popri už zmienenej Kantovej téze to mohla byť obava z „kriku Bojóťanov“, čiže z hroziaceho škandálu, ktorý by mohol ohroziť jeho reputáciu. Sám Gauss totiž zastával v tom čase prevládajúce stanovisko, že geometria je vedou o štrukturálnych zákonitostiach *reálneho priestoru*, a nie skúmaním možností rôznych „priestorupodobných“ štruktúr, prípustných výlučne na základe logickej konzistentnosti. To z nej činí empirickú prírodnú vedu podobnú fyzike.

V tejto súvislosti si Gauss zároveň uvedomil, že otázka platnosti piateho postulátu by sa mohla dať rozhodnúť experimentom. Keď sa v rokoch 1821 až 1825 podieľal na geodetickej triangulácii Hanoverského kráľovstva, podrobne premeral uhly v najväčšom trojuholníku budovanej geodetickej siete, tvorenom vrcholmi kopcov Brocken, Hoher Hagen a Grosser Inselsberg so stranami 69, 85 a 107 km. Odchýlka súčtu týchto uhlov od 180° však neprevyšovala možnú chybu merania. Podstatne neskôr Gauss vyjadril názor, že na odhalenie prípadnej nezhody reálneho priestoru s euklidovskou geometriou by bolo nevyhnutné meranie uhlov v trojuholníku, ktorého strany by mnohonásobne prevyšovali zemský polomer. Zároveň si však uvedomil, že takéto meranie má šancu jedine vyvrátiť piaty postulát; aby sme ho mohli meraním bezpečne potvrdiť, museli by sme byť schopní merať uhly s absolútnou presnosťou.

Či už boli Gaussove obavy opodstatnené alebo nie a nech už boli jeho dôvody akékoľvek, nič to nemení na skutočnosti, že nič zo svojich objavov a úvah o tejto novej geometrii nezverejnil. A tak sú za objaviteľov neeuklidovskej geometrie právom považovaní až ruský matematik Nikolaj Ivanovič Lobačevskij (1792 – 1856) a maďarský dôstojník rakúskej armády a amatérsky matematik János Bolyai (1802 – 1860). Na základe toho sa hyperbolická geometria zvykne nazývať aj Lobačevského prípadne Bolyaiho-Lobačevského geometriou.

János Bolyai bol synom gymnaziálneho profesora matematiky, fyziky a chémie Farkasa Bolyaia, Gaussovho priateľa zo štúdií, ktorý sa kedysi sám nie príliš úspešne zaoberal problematikou piateho postulátu. Z toho dôvodu svojho syna odrádzal od podobných snáh. János sa však odradiť nedal a v priebehu rokov 1820 až 1823 sa mu podľa vlastných slov podarilo „objaviť obdivuhodné veci, nad ktorými žasol, [... a ...] z ničoho stvoriť podivný nový svet“. Rukopis, ktorý v r. 1826 poslal na posúdenie svojmu učiteľovi na Cisárskej a kráľovskej vojenskej akadémii vo Viedni, bol však odmietnutý. A tak jeho objavy vyšli až v r. 1832 v podobe stručného dodatku k stredoškolskej matematickej učebnici jeho otca. V ňom autor predstavil tzv. *absolútnu geometriu*, ktorá zahŕňa euklidovskú aj (vtedy ešte tak nenazývanú) *hyperbolickú geometriu* ako špeciálne prípady. Farkas Bolyai poslal synov spis na posúdenie Gaussovi. Ten mu odpísal, že k podobným výsledkom sa sám dopracoval už dávnejšie a vzápätí ho veľmi zdržanlivo pochválil. Kým otec sa cítil Gaussovou odpoveďou poctený, na mladého Jánosa zaúčinkovala deprimujúco.

Lobačevskij po prvý raz verejne predstavil svoj objav neeuklidovskej geometrie, ktorú nazýval *imaginárnou geometriou*, v r. 1826 v prednáške na univerzite v Kazani. Následne v priebehu rokov 1829 až 1855 publikoval celý rad prác venovaných jej rozpracovaniu a výkladu. V ruských akademických centrách na univerzitách v Petrohrade a v Moskve sa Lobačevskij stretol s nepochopením a odmietnutím. Uznania sa dočkal až vďaka Gaussovi po tom, ako ten čítal jeho *Geometrické skúmania k teórii rovnobežných priamok* v nemeckom preklade, ktorý vyšiel v Berlíne v r. 1840. Gauss sa dokonca začal učiť po rusky, aby mohol čítať ďalšie Lobačevského práce. Na jeho návrh bol Lobačevskij v r. 1842 prijatý za člena Götingenskej učenej spoločnosti.

Lobačevskij zastával názor, že skúmanie rôznych typov geometrií má zmysel bez ohľadu na to, ktorá z nich dáva adekvátny popis štruktúry reálneho priestoru. V tomto duchu sa nesie jeho dielo *Pangeometria* (1855), v ktorom je o. i. euklidovská geometria zrekonštruovaná v rámci hyperbolickej geometrie. Napriek tomu sa však aj on pokúšal zistiť, aká je geometria reálneho priestoru. Nemeral však uhly v trojuholníkoch

pozemských rozmerov, ale v trojuholníkoch tvorených hviezdnymi stálicami. S rovnakým cieľom analyzoval astronomické údaje získané meraním paraláx Síria a ďalších hviezd. Ani tak sa mu však významnú odchýlku, ktorá by mohla potvrdiť neeuklidovský charakter reálneho priestoru, odhaliť nepodarilo.

Ani Gaussov, Bolyaiho a Lobačevského vhľad a samozrejmosť, ba priam virtuozita, s akou sa v podivnom svete hyperbolickej geometrie orientovali, však samy o sebe nezaručujú, že nejde o prelud, ktorý sa skôr či neskôr zosype v logickom spore ako domček z karát. Úprimne si však musíme priznať, že takúto istotu nemáme ani v prípade euklidovského geometrického sveta. Tu nám to však nijako neprekáža, lebo náš geometrický vhľad, o ktorý opierame svoju vieru v jeho bezospornosť, je všeobecne zdieľaný a podporovaný tradičným vzdelaním. Preto by nám stačilo, keby sme vedeli dokázať bezospornosť hyperbolickej geometrie za predpokladu bezospornosti geometrie euklidovskej. Poznamenajme, že bezospornosť euklidovskej geometrie za predpokladu bezospornosti tej hyperbolickej je dôsledkom pred chvíľou spomínaných výsledkov Lobačevského, i keď on sám si otázku takto nekládol.

Jestvuje viacero *modelov* hyperbolickej geometrie vnútri geometrie euklidovskej. Postačí však, keď sa aspoň v náznaku zoznámime s jedným z nich. Jeho prvú podobu vytvoril v r. 1868 Eugenio Beltrami (1835 – 1900). Tú na základe jedného pozorovania Arthura Cayleyho (1821 – 1895) upravil v r. 1871 Felix Klein (1849 – 1925) do finálnej podoby známej ako *Beltramiho-Kleinov model*. Je prekvapivo jednoduchý: v tomto modeli sú bodmi hyperbolickej roviny vnútorné body nejakého kruhu v euklidovskej rovine a priamkami tetivy kružnice ohraničujúcej onen kruh bez krajných bodov.

V roku 1899 vydáva David Hilbert (1862 – 1943), považovaný za najvýznamnejšieho a najvšestrannejšieho matematika svojej doby, monografiu *Základy geometrie* (*Grundlagen der Geometrie*). Kniha nadobudne svoju finálnu podobu v druhom vydaní z r. 1902 a je považovaná za stelesnenie ideálu výstavby matematickej teórie axiomatickou metódou. Hilbert v nej dôsledne axiomaticky buduje euklidovskú geometriu roviny a priestoru, pričom dopĺňa pôvodnú Euklidovu axiomatiku matematickou formuláciou niektorých názorných princípov, ktoré sa v pôvodnej antickej verzii síce nevedome bežne používajú, avšak explicitne sformulované nie sú, lebo sú chápané ako samozrejmé. *Bezospornosť* svojej axiomatizácie euklidovskej geometrie Hilbert dokazuje metódou súradníc za predpokladu bezospornosti aritmetiky reálnych čísel. Tým je na otázku bezospornosti reálnej aritmetiky prevedená aj otázka bezospornosti geometrie hyperbolickej. Hilbert zároveň podáva dôkaz *nezávislosti* svojich axióm: žiadna z nich sa nedá odvodiť ako logický dôsledok zvyšných. Nezávislosť piateho postulátu (Playfairovej axiómy o rovnobežkách) je dokázaná práve odkazom na neeuklidovskú geometriu. Ako vyplynulo z neskorších výsledkov Alfreda Tarského (1926), Hilbertova axiomatizácia je navyše *úplná*: akékoľvek tvrdenie v jazyku euklidovskej geometrie je v nej buď dokázateľné alebo je dokázateľná jeho negácia.

Myšlienka modelovania (interpretácie) jednej teórie prostredníctvom inej bude zohrávať v 20. storočí v matematickej logike i v celej matematike len ťažko doceniteľnú úlohu. Dva spektakulárne príklady úspešného použitia tejto metódy predstavujú Gödelov model *univerza konštruktívnych množín* (1940) a Cohenova metóda *forcingu* (1963). Gödelovo konštruktívne univerzum je modelom Zermelovej-Fraenkelovej teó-

rie množín ZF rozšírenej o axiómu výberu a zovšeobecnenú hypotézu kontinua[1] vo vnútri univerza teórie ZF. Paul Cohen (1934 – 2007) pomocou forcingu zostrojil model teórie množín ZF s negáciou axiómy výberu vo vnútri univerza teórie ZF, ako aj model teórie množín ZFC (ZF s axiómou výberu) s negáciou hypotézy kontinua vo vnútri univerza teórie ZFC. To dohromady dokazuje nezávislosť axiómy výberu na axiomách teórie množín ZF, ako aj nezávislosť hypotézy kontinua na axiómach teórie ZFC.

2.5 Logika v 19. storočí

V predošlej časti sme sa už ocitli v 19. a v jej závere aj v 20. storočí, avšak na vývoj logiky sme sa zameriavali len nepriamo, prostredníctvom dramatických okolností sprevádzajúcich vznik neeuklidovskej geometrie a ich vplyvu na ňu. V tomto storočí však dochádza aj k rozvoju logiky samotnej. Deje sa to jednak na pôde filozofie, no formuje sa aj matematická logika (v podobe matematizovanej formálnej logiky) a vzniká teória množín. Postupne dozrieva predstava, že práve tieto dve disciplíny by mali zohrávať úlohu základov matematiky a tým poskytnúť už dávno pociťovanej vnútornej jednote matematiky akúsi „inštitucionalizovanú podobu“.

Pozoruhodnou postavou prvej, teda filozofickej línie v rozvoji logiky v 19. storočia je nemecky píšuci pražský rodák, katolícky kňaz Bernard Bolzano (1781 – 1848). Bolzano prednášal teológiu a filozofiu na pražskej Karlo-Ferdinandovej univerzite, zároveň sa však zaoberal aj logikou, matematikou, estetikou a etikou, no taktiež teóriou štátu a sociálnymi otázkami. Práve za svoje liberálne názory na sociálnu problematiku a antimilitaristické postoje bol v r. 1819 prepustený z univerzity, bolo mu zakázané verejne vystupovať a dve z jeho diel sa ocitli na indexe. Zvyšok života strávil v ústraní, no naďalej pôsobil a prednášal v úzkom kruhu svojich žiakov a priateľov.

Pre Bolzanovo matematické dielo je príznačná anticipácia budúcich objavov či dokonca objavy, ktoré v jeho dobe zostali nepovšimnué a boli nanovo objavené neskôr. V čase, keď topológia ako matematická disciplína ešte nejestvovala, sa Bolzano dopracoval k definícii dimenzie v zmysle blízkom malej induktívnej dimenzii, ako ju naznačil Henri Poincaré (1854 – 1912) v r. 1912 a zaviedli Pavel Samuilovič Uryson (1898 – 1924) v r. 1922 a Karl Menger (1902 – 1985) v r. 1923. Ako prvý – ešte pred Karlom Weierstrassom (1815 – 1897) – zostrojil príklad spojitej funkcie, ktorá nemá nikde deriváciu a taktiež ukázal, že každá ohraničená číselná postupnosť obsahuje konvergentnú podpostupnosť. Ešte pred Augustinom Louisom Cauchym (1789 – 1857) sformuloval kritérium konvergencie dnes známe ako Cauchyho-Bolzanova podmienka.[2] Taktiež dokázal, že spojitá funkcia nadobúdajúca v koncových bodoch intervalu hodnoty opačných znamienok, musí vnútri tohto intervalu nadobudnúť aj hodnotu 0.

To platí aj pre Bolzanov spis *Paradoxy nekonečna* (*Paradoxien des Unendlichen*), vydaný posmrtne v r. 1851. V ňom Bolzano buduje historicky prvú verziu teórie

[1] *Hypotéza kontinua* hovorí, že každá nekonečná podmnožina množiny všetkých reálnych čísel $\mathbb{R}$ je buď spočítateľná alebo má rovnakú mohutnosť ako množina $\mathbb{R}$. Podľa *zovšeobecnenej hypotézy kontinua* pre žiadnu nekonečnú množinu X neexistuje množina Y, ktorej mohutnosť $|Y|$ by spĺňala nerovnosti $|X| < |Y| < |\mathcal{P}(X)|$, kde $\mathcal{P}(X)$ je množina všetkých podmnožín množiny X.

[2] Postupnosť reálnych čísel $\{a_n\}$ spĺňa *Cauchyho-Bolzanovu podmienku*, ak pre každé kladné reálne číslo ε existuje prirodzené číslo m také, že pre každé $n > m$ platí $|a_n - a_m| < \varepsilon$.

množín (*Menge*), uvádza argumenty v prospech prijatia aktuálneho nekonečna, s prispením teológie (konkrétne s odvolaním sa na Božiu vševedúcnosť) podáva dôkaz existencie nekonečnej množiny a ukazuje, že nekonečná množina obsahuje vlastnú časť s ňou ekvivalentnú (teda v istom zmysle rovnako veľkú, čo protirečí Euklidovej axióme *„celok je väčší ako jeho časť“*). Neskôr v r. 1888 túto vlastnosť použije Richard Dedekind (1831 – 1916) ako *definíciu* nekonečnej množiny. Bolzanove *Paradoxy nekonečna* v nejednom smere inšpirovali tvorcu a zakladateľa teórie množín Cantora, ktorý sa na ne viackrát odvolával, najmä pri obhajobe svojej koncepcie aktuálneho nekonečna. Istá odlišnosť v prístupe k nekonečným množinám, ktorú Cantor považoval za Bolzanov omyl, poslúži v 70. rokoch 20. storočia ako inšpirácia českému matematikovi a filozofovi Petrovi Vopěnkovi (1935 – 2015) pri budovaní jeho *Alternatívnej teórie množín*.

No najvýznamnejším Bolzanovým príspevkom k logike je jeho monumentálne štvorzväzkové dielo *Vedoslovie, Pokus o podrobný a prevažne nový výklad logiky so stálym zreteľom na predchádzajúcich spracovateľov* (*Wissenschaftslehre, Versuch einer ausführlichen und grösstenteils neuen Darstellung der Logik mit steter Rücksicht auf deren bisherige Bearbeiter*), ktoré vyšlo v r. 1837. Logika vo *Vedosloví* je chápaná predovšetkým ako *metodológia vedy* a nie ako formálna logika – tá je v ňom prítomná len v pozadí. Zjednodušene možno povedať, že Bolzanovo *Vedoslovie* je venované analýze filozofických a epistemologických predpokladov zdôvodnenia vedeckého poznania, ako aj formulácii logických a metodologických zásad, ktorými sa treba riadiť pri poznávaní pravdy, pri členení celku poznanej pravdy na jednotlivé vedné disciplíny a pri ich spracovaní vo forme učebníc s cieľom dosiahnuť čo možno najvyššiu presvedčivosť a zrozumiteľnosť.

Bolzano je presvedčený, že pre každú jednotlivú vednú disciplínu možno stanoviť súbor základných východzích poznatkov, z ktorých všetky jej ďalšie poznatky vyplývajú ako ich dôsledky. Pritom rozlišuje pojmy *dôsledku* (*Abfolge*) a formálneho *odvodenia* (*Ableitung*). Tým implicitne dospieva k odlíšeniu sémantického a syntaktického aspektu vo vedeckých teóriách. Dôraz pritom kladie na sémantiku: napr. dobrý dôkaz by mal byť nielen logicky korektný, ale zároveň by mal obsahovať aj *zdôvodnenie* (*Begründung*) prinášajúce vhľad a pochopenie.

Bolzanov štýl výkladu a jeho argumentácia sú logicky vycibrené, detailne prepracované a vnútorne konzistentné, i keď pre dnešného čitateľa nie priam ľahko čitateľné. Bolzano zavádza originálne pojmy ako *veta o sebe* (*Satz an sich*), *pravda o sebe* (*Wahrheit an sich*) a *predstava o sebe* (*Vorstellung an sich*). *Vetou o sebe* rozumie výpoveď, ktorá niečo tvrdí, či už je to pravda alebo nie, a bez ohľadu na to, či ju niekto vyjadril slovami, ba dokonca či si ju čo len myslel v duchu. Každá jednotlivá veta o sebe sa vyskytuje takpovediac „v jedinom exemplári“ a viacnásobným vyslovením alebo napísaním sa nezmnožuje. Dnešným jazykom by sme mohli vari povedať, že taká veta o sebe je niečo, čo tvorí obsah, zmysel alebo význam nejakej výpovede, či už vyslovenej, napísanej alebo myslenej, prípadne len takej, ktorú by vôbec bolo možné vysloviť, napísať alebo myslieť. Vetu o sebe, ktorá vypovedá niečo tak, ako to skutočne je (teda je pravdivá), Bolzano nazýva *pravdou o sebe*. Časti viet o sebe, ktoré však samotné vetu netvoria, nazýva *predstavami o sebe*. Tie môžu byť jednoduché alebo zložené. Dnes by sme bolzanovskú predstavu o sebe nazvali skôr pojmom, prípadne, podľa okolností, obsahom alebo významom pojmu. Ak siahneme po príklady

do konkrétnych vied, tak predstavám, resp. vetám a pravdám osebe budú zrejme najvernejšie zodpovedať matematické pojmy, resp. matematické tvrdenia a matematické poznatky. A nie je to náhoda – matematika je Bolzanovi naozaj vzorom pre výstavbu a výklad ostatných vedných disciplín.

Bolzano priznáva svojim vetám, pravdám a predstavám o sebe istý druh existencie mimo čas a priestor, pričom varuje, že nejde o existenciu v reálnom svete. Na druhej strane priznáva reálnu existenciu nielen slovne vyjadreným predstavám a vetám, ale aj predstavám a vetám iba mysleným, ako myšlienkam toho-ktorého človeka. Takéto filozofické stanovisko sa zvykne označovať ako *moderný* alebo *sémantický platonizmus*. Zároveň je Bolzanovou zásluhou jasné oddelenie logiky od akýchkoľvek psychologizujúcich tendencii a – napriek Kanta pripomínajúcej „*an sich* terminológii" – kritické vymedzenie sa voči kantovskej metafyzike. Bolzano bol zrejme prvý, kto si uvedomil, že základom filozofie nie sú metafyzické úvahy, ale štúdium toho, čo a ako hovoríme a akým zákonom naša reč podlieha. Vo svojom *Vedosloví* tak položil základy sémantickej tradície v západnom myslení. V tomto duchu na neho podstatne neskôr nadviazali rakúski filozofi Franz Brentano (1838 – 1917), Alexius Meinong (1853 – 1920) a Edmund Husserl (1859 – 1938), zakladajúce osobnosti Poľskej logickej školy Kazimierz Twardowski (1866 – 1938), Jan Łukasiewicz (1878 – 1956) a Stanisław Lesńiewski (1886 – 1939), no najmä Alfred Tarski (1901 – 1983) svojou koncepciou logického dôsledku a pravdy vo formálnych jazykoch z 30. rokov 20. storočia, ktorá podnes zohráva v matematickej logike zásadnú úlohu.

V 19. storočí dochádza aj k intenzívnemu rozvoju algebry a k rozšíreniu tradičných oblastí jej uplatnenia. Postupne sa utvára názor, podľa ktorého algebraické výrazy a manipulácie s nimi nemusia nutne predstavovať len čísla a operácie na číselných oboroch, ani spĺňať všetky identity, ktorým podliehajú operácie s číslami. Z množstva príkladov spomeňme aspoň objav *kvaterniónov*, t. j. akejsi štvorrozmernej obdoby komplexných čísel (1843), ktorých násobenie nie je komutatívne, írskym matematikom Williamom Rowanom Hamiltonom (1805 – 1865). V tejto atmosfére dochádza na britských ostrovoch k vzniku logiky ako *matematickej disciplíny*. V roku 1847 vychádzajú dve práce *Matematická analýza logiky ako pokus o kalkulus deduktívneho uvažovania* (*The Mathematical Analysis of Logic, being an Essay towards a Calculus of Deductive Reasoning*) od Georga Boola a *Formálna logika alebo kalkulus vyvodzovania nevyhnutného a pravdepodobného* (*Formal Logic or the Calculus of Inference, Necessary and Probable*) od Augusta De Morgana.

George Boole (1815 – 1864) bol matematický samouk, ktorý však upútal na seba pozornosť vedeckej komunity niekoľkými prácami v oblasti diferenciálnych rovníc a invariantov. Za jednu z týchto prác dokonca získal zlatú medailu Kráľovskej spoločnosti v r. 1844. Vo svojej *Matematickej analýze logiky* etabloval logiku, dovtedy považovanú za súčasť filozofie, ako matematickú disciplínu a venoval sa aj teórii pravdepodobnosti. Uvedomil si, že logické spojky možno interpretovať ako algebraické operácie, či už na výrokoch, vlastnostiach alebo triedach objektov, a logickým zákonom dať podobu identít pre tieto operácie. To umožňuje zachytiť deduktívne úvahy ako *výpočty* v duchu Leibnizovej vízie *calculu ratiocinator*. Pri budovaní teórie pravdepodobnosti sa Boole pokúsil vytvoriť všeobecnú metódu, ktorá by umožnila na základe znalosti pravdepodobností istých udalostí určiť pravdepodobnosť inej udalosti určitým spôso-

bom s nimi logicky prepojenej. Ako ocenenie vedeckých zásluh bol Boole v r. 1849 s podporou De Morgana ustanovený na Queen's College v írskom Corku ako prvý profesor matematiky, hoci sám nemal univerzitný titul. Svoj prístup a názory Boole podrobnejšie systematicky vyložil v spise *Skúmanie zákonov myslenia, na ktorých sa zakladajú matematické teórie logiky a pravdepodobnosti* (*An Investigation of the Laws of Thought on which are Founded the Mathematical Theories of Logic and Probabilities*, 1854).

Boole používal pre *pravdu*, resp. *univerzálnu triedu* znak 1, *nepravdu* resp. prázdnu triedu značil 0. Negáciu značil ako doplnok vzhľadom na univerzálnu triedu $1-x$. Konjunkciu (spojku *a*) značil ako logický súčin $x \cdot y$; disjunkciu (spojku *alebo*) značil ako logický súčet $x+y$ a chápal ju vo vylučovacom význame (x alebo y, ale nie oboje). Boolovské operácie spĺňajú popri obvyklých identitách ako komutatívne zákony $xy = yx$, $x+y = y+x$, asociatívne zákony $(xy)z = x(yz)$, $(x+y)+z = x+(y+z)$, distributívny zákon $x(y+z) = xy + xz$, či zákon dvojitej negácie (doplnku) $1-(1-x) = x$, aj niekoľko „neštandardných" identít, napr. $xx = x$ či $x+x = 0$. Posledná identita, ktorá je dôsledkom chápania logickej spojky *alebo* (+) vo vylučovacom zmysle, zmiatla aj samotného autora, pretože na základe analógie s číselnými operáciami očakával, že z rovnosti $x + x = 0$ by malo vyplývať $x = 0$.

Boolove myšlienky viedli v 20. a 21. storočí k aplikáciám, o akých sa ich autorovi ani nesnívalo. Binárne kódy, boolovské hradlá a prepínače, logické obvody, prepojené do komplexných štruktúr v čipoch sú základnými jednotkami pre návrh a konštrukciu počítačov a mnohých ďalších elektronických zariadení. Boolove algebry sú zasa jednou zo základných matematických štruktúr nielen v teórii množín a v matematickej logike, ale aj v teórii miery, pravdepodobnosti a v ďalších na ne nadväzujúcich disciplínach.

Augustus De Morgan (1806 – 1871) je asi čitateľovi známy najmä ako autor *De Morganových zákonov* prepájajúcich logické spojky konjunkcie a disjunkcie (v nevylučovacom zmysle) prostredníctvom negácie, ktoré možno v modernej symbolike zapísať napr. ako tautológie

$$\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B) \qquad \neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$$

Tie sa vyskytujú v jeho práci *O štruktúre sylogismu* (*On the structure of the syllogism*, 1846) v menej priezračnom symbolickom vyjadrení, avšak vo verbálnej (t. j. nesymbolickej) podobe boli známe už Williamovi Ockhamovi v 14. storočí. De Morgan tiež zaviedol názov *matematická indukcia* pre známu metódu dôkazov tvrdení o prirodzených číslach vo svojej široko používanej učebnici *Základy aritmetiky* (*Elements of Arithmetic*, 1830). Jeho najvýznamnejší príspevok k logike však spočíva v rozšírení predmetu jej skúmania z úsudkov týkajúcich sa subjekt-predikátových tvrdení, ktoré v nej dominovali od čias antiky, na úsudky týkajúce sa tvrdení, v ktorých vystupujú dvoj- a viacmiestne vzťahy (relácie) medzi subjektmi. Tým pomohol presadiť názor, že práve relačné úsudky zohrávajú rozhodujúcu úlohu v matematickom odvodzovaní a vedeckej argumentácii. Navyše niektoré logické operácie s reláciami, ako napr. inverzia, kompozícia či projekcie, sa nedajú vyjadriť iba pomocou logických spojok, lež (s výnimkou inverzie) sa nezaobídu bez *kvantifikácie* premenných. De Morgan sa tak stáva jedným z priekopníkov štúdia úlohy kvantifikátorov v logike. Dochádza k tomu v sérii článkov so spoločným názvom *O sylogizme* (*On the Syllogism*) z obdobia rokov

1846 – 1868, ktorá zahŕňa aj obe skôr spomínané práce. De Morganovi sa tiež pripisuje anekdotický príklad logicky očividne správneho relačného úsudku, ktorý však aristotelovská subjekt-predikátová logika nedokáže zdôvodniť:

Všetky kone sú zvieratá.
Preto *každá hlava koňa je hlavou zvieraťa.*

Pod vplyvom De Morganovho a najmä Boolovho diela sa logika v druhej polovici 19. storočia stáva módnou záležitosťou medzi intelektuálmi anglofónneho sveta. Spomedzi nich vyčnievajú dve osobnosti doslova renesančného formátu pôsobiace na opačných brehoch Atlantiku.

William Stanley Jevons (1835 – 1882) je známy najmä ako popredný britský ekonóm hojne využívajúci štatistické a matematické metódy, objaviteľ tzv. *Jevonsovho paradoxu* vo vzťahu produkcie, dopytu a ceny komodít, a tiež autor *teórie marginálneho (hraničného) úžitku.*

V logike nadviazal na dielo Boola a De Morgana. Nahradil Boolov logický súčet (vylučovaciu disjunkciu) disjunkciou v nevylučovacom zmysle, systematicky pracoval s premennými a kvantifikátormi. Vo svojom spise *The Substitution of Similars* (1869) vyzdvihol leibnizovský univerzálny princíp, podľa ktorého „*čokoľvek je pravdou o nejakej veci, je pravdou o rovnakej veci*“. Ten nájde neskôr vyjadrenie v podobe logických axióm rovnosti. Jeho kniha *Elementary Lessons on Logic* (1870) sa čoskoro stala najrozšírenejšou učebnicou logiky v angličtine. V ďalšom diele *Principles of Science* (1874) sa zaoberal vzťahmi medzi logikou (dedukciou), zovšeobecňovaním na základe faktov (indukciou) a pravdepodobnosťou. Svoje úvahy ilustroval množstvom relevantných, detailne prepracovaných príkladov z prírodných vied a ekonómie. Taktiež predvídal využitie jednosmerných funcií a faktorizácie celých čísel v kryptografii. V r. 1869 zostrojil mechanický počítací stroj, pre svoj tvar nazvaný *logické piano*, ktorý ako prvý svojho druhu vykonával boolovské logické operácie rýchlejšie než človek.

Charles Sanders Peirce (1839 – 1914) je známy predovšetkým ako jeden zo zakladateľov prvého filozofického smeru, ktorý sa zrodil na americkej pôde, označovaného názvom *pragmatizmus.* Zaoberal sa však aj fyzikou, chémiou, astronómiou, geodéziou a kartografiou, a samozrejme logikou. Podieľal sa na meraní fluktuácií gravitačného poľa Zeme, ktoré prispelo k upresneniu miery elipticity zemského glóbu. Je tiež autorom tzv. *kvinkunciálnej projekcie* – kartografického zobrazenia umožnujúceho periodické dláždenie roviny na seba nadväzujúcimi priemetmi oktantov zemského glóbu v tvare rovnoramenných pravouhlých trojuholníkov.

V logike sa usiloval o prepojenie Boolovho algebraického prístupu s relačnými inferenciami De Morgana. Podobne ako Jevons nahradil Boolov logický súčet disjunkciou v nevylučovacom zmysle. Taktiež si uvedomil, že pri práci s triedami je výhodnejšie miesto rovnosti používať reláciu inklúzie, ktorá zodpovedá implikácii. Ešte pred Shefferom (1882 – 1964) prišiel na to, že všetky logické spojky možno vyjadriť pomocou jedinej, totiž spojky *not* (... *or* ...) (neskôr nazvanej *Peirce' dagger* alebo NOR), resp. spojky *not* (... *and* ...) (neskôr nazvanej *Sheffer's stroke* alebo NAND). Explicitne zaviedol kvantifikáciu premenných, pričom univerzálny kvantifikátor Π_i chápal ako nekonečný logický súčin (konjunkciu) a existenčný kvantifikátor Σ_i ako nekonečný logický súčet (disjunkciu v nevylučovacom zmysle). Zrejme ako prvý si uvedomil zá-

sadný rozdiel medzi výrokovým počtom, logikou s kvantifikáciou premenných pre individuálne objekty (logika prvého rádu) a logikou používajúcou aj kvantifikáciu vlastností individuálnych objektov (logika druhého rádu).

Peirce tiež predvídal využitie boolovskej logiky pri konštrukcii prepínačov elektrických obvodov a následnú možnosť konštrukcie elektronického počítacieho stroja. Jeho bývalý študent Allan Marquand (1854 – 1924), inšpirovaný Jevonsovým logickým pianom, zostrojil v rokoch 1881 – 1882 jeho vylepšenú, menšiu a prenosnú verziu. V r. 1887 na Peircov popud navrhol elektronickú verziu logického počítača, ktorú však už neuskutočnil.

S Peircom a Jevonsom končí obobie, počas ktorého je logika doménou prevažne polyhistorov, čiže učencov zaoberajúcich sa mnohými odvetviami ľudského poznania. Pre nich – počnúc Aristotelom cez Leibniza a Lamberta až po Jevonsa a Peirca – je logika len jednou z mnohých oblastí ich pôsobenia a záujmu. V rámci nového trendu započatého Boolom a De Morganom sa logika stáva matematickou disciplínou a jej ďalší rozvoj určujú najmä matematici, často so širokým záberom, spravidla však obmedzeným na viacero oblastí matematiky a na filozofické otázky s ňou súvisiace.

2.6 Koniec 19. a začiatok 20. storočia

Matematizácia, presnejšie, algebraizácia logiky je dovŕšená v monumentálnom trojzväzkovom diele nemeckého matematika Ernsta Schrödera (1841 – 1902) *Prednášky o algebre logiky* (*Vorlesungen über die Algebra der Logik*, 1890 – 1905). Schröder v ňom nadväzuje na Boola, De Morgana, Jevonsa, a najmä na Peirca. Systematicky využíva dualitu medzi konjunkciou a disjunkciou sprostredkovanú De Morganovými zákonmi, pracuje so vzťahom inklúzie a s kvantifikátormi a buduje algebru relácií s operáciou kompozície ako násobením. Stále je to však matematická logika iba v prvom z dvoch významov, ktoré sme spomínali na začiatku: je to *matematizácia logiky* algebraickými prostriedkami.

Na prelome 19. a 20. storočia je však už doba zrelá nato, aby sa dávno tušený potenciál logiky pre matematiku začal naplno prejavovať. Najprv je však potrebné si uvedomiť a sformulovať zámery a ciele, ktorým by takáto matematická logika mala slúžiť. V tomto vývoji možno približne od 80. rokov 19. storočia vysledovať dve odlišné línie; zjednodušene ich budeme nazývať líniou logickou a líniou množinovou. Hoci sú tesne prepletené, ich začiatky sa dajú jasne oddeliť, čo nám umožňuje sledovať ich po istý čas a do istej miery oddelene. Začneme logickou líniou.

Priekopníkom systematického využitia logiky v matematike je významný a všestranný taliansky matematik Giuseppe Peano (1858 – 1932). Zaoberal sa teóriou čísel, lineárnou algebrou, geometriou, diferenciálnymi rovnicami a tiež logikou. Ako prvý zostrojil príklad spojitej krivky vypĺňajúcej štvorec. Je tiež autorom internacionálneho jazyka *Latino sine flexione* založeného na latinčine so značne zjednodušenou gramatikou. Linguistické záujmy spolu s výskytom podobných, intuícii odporujúcich objektov v matematike ho viedli k rozhodnutiu povýšiť logiku na univerzálny jazyk umožňujúci vyjadriť všetku matematiku s dovtedy nevídanou presnosťou a jednoznačnosťou. Prvým krokom v tomto smere je Peanova axiomatizácia aritmetiky prirodzených čísel z r. 1889, využívajúca *nasledovníka* ako jedinú základnú operáciu. Pomocou nej sú

potom rekurzívne definované operácie sčítania a násobenia. To je však umožnené až *axiómou indukcie* (uvádzame ju v modernom prepise)

$$(\forall\, X \subseteq \mathbb{N})\big(0 \in X \wedge (\forall\, x \in X)(x+1 \in X) \Rightarrow X = \mathbb{N}\big)$$

v ktorej je však popri premennej x pre prirodzené čísla kvantifikovná aj premenná X pre časti (podmnožiny) množiny $\mathbb{N}$ všetkých prirodzených čísel. Pôvodná Peanova aritmetika je tak (z neskoršieho hľadiska) *teóriou druhého rádu*. Od r. 1894 začína Peano s viacerými spolupracovníkmi uverejňovať (tak trochu utopický) projekt *Matematický formulár* (*Formulario Mathematico*), ktorý mal v encyklopedickej forme zahŕňať všetky známe matematické vzorce a vety (teorémy) zapísané pomocou štandardizovanej matematickej a logickej symboliky vytvorenej na tento účel. Peanova logická a množinová symbolika sa v značnej miere (s väčšími či menšími modifikáciami) používa dodnes; príkladom je Peanom zavedený znak ε pre náležanie prvku do množiny, neskôr modifikovaný do podoby $\in$.

S ešte ambicióznejším projektom prichádza nemecký matematik, logik a filozof Gottlob Frege (1848 – 1925). Vo svojich dvoch knihách s názvami odkazujúcimi na leibnizovské dedičstvo *Pojmové písmo, podľa aritmetiky utvorený formálny jazyk čistého myslenia* (*Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens*, 1879) a *Základy aritmetiky: logicko-matematické skúmanie o pojme čísla* (*Die Grundlagen der Arithmetik: eine logisch mathematische Untersuchung über den Begriff der Zahl*, 1884), v časopiseckých článkoch *O zmysle a význame* (*Über Sinn und Bedeutung*, 1892), *O pojme a predmete* (*Über Begriff und Gegenstand*, 1892) a ďalších prácach postupne buduje svoju koncepciu logiky, vyslovuje prekvapivo moderné názory na jej úlohu vo filozofii a kladie základy toho, čo sa neskôr bude nazývať *analytický obrat vo filozofii*. Vytvára tiež vlastnú svojráznu logickú symboliku, ktorá sa však pre svoju neprehľadnosť neujme, a práve jeho ľpenie na nej zapríčiní, že sa jeho dielu nedostane od súčasníkov tej pozornosti, akú by si zaslúžilo. Zároveň dospieva k presvedčeniu, že pojem čísla i ďalšie aritmetické pojmy je možné osnovať čisto logickými prostriedkami, a postupne tak vybudovať aritmetiku aj matematickú analýzu ako odvetvia logiky. Na rozdiel od Peana, ktorý chcel využiť logiku „len“ ako univerzálny jazyk a metódu prezentácie matematiky, tak Frege ide oveľa ďalej: hodlá vyložiť matematické pojmy ako pojmy logické a následne zrekonštruovať celú kalkulatívnu matematiku v rámci sveta logických foriem. Tým sa stáva zakladateľom myšlienkového smeru v základoch matematiky známeho ako *logicizmus*. Základom logicizmu je téza, že matematiku možno v podstate zredukovať na logiku. Fregeho snaženie malo vyvrcholiť v trojzväzkovom diele *Základné zákony aritmetiky* (*Grundgesätze der Arithmetik*), ktorého prvý diel vyšiel v r. 1893 a druhý v r. 1903.

Avšak v r. 1902, v čase, keď bol druhý diel ešte len v tlači, dostal Frege list, ktorý ho upozorňoval na spor v ním navrhnutom formálnom systéme. Ten totiž pripúšťal uvažovať o vlastnosti (predikáte), ktorú majú tie vlastnosti (predikáty), ktoré sa nevzťahujú na seba, inak povedané, nemajú vlastnosť, ktorú samy označujú. Ak si túto vlastnosť označíme ako $R(x)$, tak ľubovoľný predikát $P(x)$ má vlastnosť $R(x)$ práve vtedy, keď nemá vlastnosť $P(x)$. Formálne, $R(P) \Leftrightarrow \neg P(P)$. Potom ľubovoľná z odpovedí na otázku, či predikát $R(x)$ má vlastnosť $R(x)$, má za následok svoj opak, t. j. $R(R) \Leftrightarrow \neg R(R)$. A to je spor, ktorý znamenal zrútenie Fregeho projektu v aktuálnej

podobe. Treba však dodať, že Fregemu sa podarilo v logicistickom duchu zrekonštruovať minimálne aritmetiku prirodzených čísel a dokázať Peanove axiómy, pričom táto časť jeho práce uvedeným sporom zasiahnutá nebola. Ani potom Frege neprestal obhajovať logicistickú tézu, no prácu na plánovanom treťom dieli *Grundgesätze* zanechal.

Odosielateľom onoho listu bol britský logik, matematik, filozof a politický aktivista Bertrand Russell (1872 – 1970) a spor, na ktorý v ňom Fregeho upozorňoval, dostal názov *Russellov paradox*. Russell sa v r. 1900 zúčastnil na I. Medzinárodnom filozofickom kongrese v Paríži, kde sa stretol s Peanom a jeho spolupracovníkom Alessandrom Padoom (1868 – 1937). Ich *Formulario* naňho urobilo hlboký dojem. Súznelo totiž so zámermi jeho diela *Principles of Mathematics*, na ktorom práve pracoval a ktoré vyšlo v r. 1903. Ako píše v predhovore, táto práca má dva hlavné ciele:

> *Jedným z nich je ukázať, že všetka čistá matematika sa zaoberá výlučne pojmami definovateľnými z veľmi malého počtu základných pojmov a že všetky jej tvrdenia možno odvodiť z veľmi malého počtu základných logických princípov, ... čo bude ustanovené prísne symbolickou argumentáciou... Druhý z cieľov, ... výklad základných pojmov, ktoré matematika prijíma ako nedefinovateľné, je čisto filozofická záležitosť.*

To je plne zhode s logicistickou tézou; rovnako však možno povedať, že Russel si kladie za cieľ výklad matematiky *axiomatickou metódou* s využitím symbolickej logiky.

Russell napísal svoje *Principles* skôr, ako sa zoznámil s Fregeho dielom, a mal v úmysle napísať k nim aj druhý diel. No Fregeho myšlienky ho uhranuli natoľko, že logicistickú tézu prijal za svoju a podujal sa pokračovať v napĺňaní Fregeho zámeru. Zároveň si však zoči voči vlastnému paradoxu uvedomil, že ochrana pred hroziacimi spormi si bude vyžadovať prijatie zásadných opatrení. Pre svoj nový projekt sa mu podarilo získať aj svojho priateľa a bývalého učiteľa, významného britského filozofa a matematika Alfreda North Whiteheada (1861 – 1947). Ten kvôli tomu rezignoval na druhý diel svojho podobne zameraného *Pojednania o univerzálnej algebre* (*A Treatise on Universal Algebra*, 1898). Spolu potom napísali a v priebehu rokov 1910 až 1913 vydali monumentálne trojzväzkové dielo *Principia Mathematica*, svojím titulom odkazujúce k veľkému Newtonovi. V ňom v duchu logicizmu naozaj vyložili, nie síce celú vtedajšiu matematiku, ale aspoň značne úplný súhrn jej základných pojmov a výsledkov. Aj tak sa však nezaobišli bez niektorých postulátov, ktoré sotva možno zdôvodniť čisto logicky (axiómy nekonečna, výberu a redukcie). Navyše ako ochranu pred paradoxmi zaviedli sofistikovaný systém syntaktických obmedzení zabraňujúci *autoreferencii*, teda o. i. aj aplikácii predikátu na seba (ako napr. $P(P)$, resp. $\neg P(P)$) či formulám o náležaní množiny do seba (ako $x \in x$ resp. $x \notin x$). Tento systém je známy pod názvom *rozvetvená teória typov* a jeho bližší opis nás nemusí zaujímať. Stačí povedať, že popri výrazoch zodpovedných za paradoxy, preventívne zakazuje aj mnohé vŕneškodné a robí logicistickú matematiku značne nenázornou a nadmerne komplikovanou.

Trvalým prínosom *Principia* je logická symbolika, ktorá sa do značnej miery ujala. V tom však Russell a Whitehead nenadväzujú na Fregeho lež na Peana. K Peanovmu existenčnému kvantifikátoru $(\exists x)$ pridávajú „hanblivo“ značený univerzálny kvantifikátor (x). Súčasnú podobu univerzálneho kvantifikátora $(\forall x)$ zaviedol až v r. 1935

Gerhard Gentzen (1909 – 1945), no definitívne sa presadila až v 60. rokoch 20. storočia. Dovtedy sa paralelne používalo aj „priamočiarejšie“ značenie (Ex) a (Ax).

2.7 Teória množín

Tu je vhodný čas opustiť sledovanú logickú líniu a vrátiť sa k počiatkom línie množinovej. Teóriu množín v jej prvotnej neformalizovanej podobe vytvoril jediný muž – matematik zo silným vizionárskym založením – Georg Cantor (1845 – 1918). Svoju teóriu začal budovať v 70. rokoch 19. storočia. Priviedli ho k tomu úvahy o jednoznačnosti rozvoja funkcií do trigonometrických Fourierových radov. „Prvými“ Cantorovými množinami teda boli množiny bodov na priamke. Postupne sa však dopracoval k podstatne všeobecnejšiemu chápaniu tohto pojmu. Jeho vlastnými slovami:

> *Množinou rozumieme akékoľvek zoskupenie M určitých dobre rozlíšiteľných objektov m nášho vnímania alebo myslenia (nazývaných prvkami množiny M) do jedného celku.*

Vytvorenie množiny tak predpokladá, aby všetky jej prvky už boli privedené k existencii, teda vnímané či aspoň myslené ako aktuálne existujúce. V prípade nekonečných zoskupení, ako napr. prirodzených čísel alebo bodov na priamke, tak Cantorova teória opúšťa dovtedy prevládajúce poňatie nekonečna ako *potenciálneho* a výkladom týchto zoskupení ako zavŕšených množín ho nahrádza *aktuálnym nekonečnom*.

Navyše prvky sa na množine podieľajú výlučne svojou prítomnosťou, bez ohľadu na ich usporiadanie či iné vzťahy medzi nimi. Dve množiny sa teda rovnajú práve vtedy, keď majú tie isté prvky. Tento princíp nájde neskôr svoje vyjadrenie v podobe *axiómy extenzionality*. Ďalším východzím postulátom Cantorovej teórie je všeobecný *vymedzovací princíp*:

> *Pre každú „zmysluplnú“ vlastnosť $P(x)$ možno vytvoriť množinu $\{x\colon P(x)\}$ všetkých tých prvkov x, ktoré majú túto vlastnosť.*

Uvedené dva princípy majú za následok, že teória množín zaujíma vo vzťahu k logike isté výsadné postavenie. Nie je to len jedna z teórií, ktorých výstavba ponúka logike priestor na uplatnenie. V istom zmysle je to logika sama, a to v podobe, v ktorej boli do krajnosti dovedené jej dva tesne súvisiace, viac-menej podvedomé, vedúce zámery. Prvý z nich spočíva v tendencii stotožňovať logicky ekvivalentné vlastnosti, inak povedané nahrádzať vlastnosti, bez ohľadu na ich význam a jazykový opis, ich *extenziami*, čiže zoskupeniami objektov, ktoré majú príslušnú vlastnosť. Tento zámer sa začal napĺňať už pri algebraizácii logiky napr. prostredníctvom Boolových algebier, a teória množín je iba jeho jemnejšie štrukturovaným dovŕšením. Treba si však uvedomiť, že je to zámer značne problematický. Plasticky to ilustruje príklad uvádzaný ešte De Morganom. Nech náš základný obor objektov pozostáva z ôsmich planét Slnečnej sústavy: Merkúr, Venuša, Zem, Mars, Jupiter, Saturn, Urán a Neptún. Všetkých možných vlastností týchto planét, o ktorých možno uvažovať, je nepredstaviteľné množstvo: od hmotnosti, skupenstva a povrchovej teploty, cez periódu rotácie okolo vlastnej osi, dobu obehu okolo Slnka a vzdialenosť od neho, až po počet obežníc (mesiacov), prítomnosť atmosféry, výskyt vody, či existenciu života atď. Na druhej strane, dôsledné uplatňovanie extenzionálneho hľadiska nám vnucuje absurdný záver,

že všetkých možných vlastností prvkov tohto (i ktoréhokoľvek iného) osemčlenného súboru je len $2^8 = 256$.

Druhým zo spomínaných vedúcich zámerov je výklad čo možno najviac zoskupení objektov ako samostatné objekty. Jedným z dôsledkov uplatňovania týchto zámerov je aktualizácia oboru všetkých podmnožín danej množiny, teda možnosť vytvoriť ku každej, čo aj nekonečnej množine X, množinu $\mathcal{P}(X) = \{A\colon A \subseteq X\}$ všetkých jej podmnožín. Ako neskôr uvidíme, napĺňanie týchto zámerov má svoje medze. Ich bezstarostné uplatňovanie vedie k paradoxom, či dokonca sporom v rámci Cantorovej teórie. Preto je potrebné ich uplatňovať opatrne a hľadať pravidlá, ktoré by ich uplatňovanie obmedzovali a regulovali.

Fascinujúci novátorský pohľad do sveta nekonečných množín sa Cantorovi neotvoril naraz, lež jeho osvetľovanie priebiehalo postupne, spočiatku v krokoch vcelku nenápadných. Otázky konvergencie postupností bodov na priamke a postupností funkcií ako aj otázky klasifikácie rôznych typov bodov nespojitosti funkcií si vyžiadali podrobnejšie objasnenie štruktúry reálnych čísel. V Cantorovom prístupe je každé reálne číslo určené postupnosťou racionálnych čísel, spĺňajúcej tzv. *Cauchyho-Bolzanovu podmienku*, ako jej limita. Pritom dve takéto postupnosti $\{a_n\}$, $\{b_n\}$ určujú to isté reálne číslo práve vtedy, keď postupnosť ich rozdielov $\{a_n - b_n\}$ konverguje k nule. Takto sú vlastne i jednotlivé reálne čísla reprezentované ako isté aktuálne nekonečné objekty. Ich aktualizácia tak už predpokladá aktualizáciu definičného oboru príslušných postupností, čiže nekonečnej množiny všetkých prirodzených čísel. Aktualizácia množiny všetkých reálnych čísel, ktorú stotožňujeme s množinou bodov na priamke, je potom ďalším logickým, i keď zďaleka nie samozrejmým krokom pri tomto postupe.

Pri hlbšom štúdiu trigonometrických radov a ďalších otázok matematickej analýzy svojej doby začal Cantor systematicky využívať operáciu *derivácie bodovej množiny* A, ako množiny A' všetkých hromadných bodov množiny A (t. j. takých bodov p, v ktorých ľubovoľne malom okolí sa nachádza nejaký bod a množiny A, rôzny od bodu p). Túto operáciu možno iterovať ľubovoľný konečný počet krát podľa rekurzívnej schémy

$$A^{(0)} = A \qquad\qquad A^{(n+1)} = \left(A^{(n)}\right)'$$

No nielen to, vo chvíli, keď sú k dispozícii všetky derivácie konečných rádov $A^{(n)}$, možno vytvoriť deriváciu nekonečného rádu

$$A^{(\infty)} = A^{(1)} \cap A^{(2)} \cap \ldots \cap A^{(n)} \cap \ldots = \bigcap_{n=1}^{\infty} A^{(n)}$$

a opäť pokračovať:

$$A^{(\infty+n+1)} = \left(A^{(\infty+n)}\right)' \ldots \quad A^{(2\infty)} = \bigcap_{n=1}^{\infty} A^{(\infty+n)} \ldots \quad A^{(\infty^2)} = \bigcap_{n=1}^{\infty} A^{(n\infty)} \ldots$$

$$A^{(\infty^3)} = \bigcap_{n=1}^{\infty} A^{(n\infty^2)} \ldots A^{(\infty^\infty)} = \bigcap_{n=1}^{\infty} A^{(\infty^n)} \ldots \quad A^{(\infty^{\infty^\infty})} = \bigcap_{n=1}^{\infty} A^{(\infty^{\infty^n})} \ldots$$

Zameraním sa na usporiadanie týchto po sebe vykonávaných krokov Cantor objavil nekonečné *ordinálne čísla*, ktoré nadväzujú na (konečné) prirodzené čísla. Na ordinálne čísla možno navyše prirodzeným spôsobom rozšíriť aritmetiku prirodzených

čísel s operáciami sčítania, násobenia aj umocňovania. To si však vyžiadalo zaviesť špecifickejšie značenie nekonečných ordinálnych čísel. Kvôli tomu nahradil znak ∞ znakom ω. Začiatok radu ordinálnych čísel potom pri trochu podrobnejšiom pohľade a neustále sa zrýchľujúcom postupe vyzerá približne takto:

$$0,\ 1,\ 2,\ \ldots,\ n,\ n+1,\ \ldots\ \omega,\ \omega+1,\ \omega+2,\ \ldots,\ \omega+n,\ \ldots\ 2\omega,\ 2\omega+1,\ \ldots$$
$$\omega^2,\ \omega^2+1,\ \ldots\ \omega^2+\omega,\ \ldots\ 2\omega^2,\ldots\ n\omega^2,\ \ldots\ \omega^3,\ \ldots\ \omega^n,\ \ldots\ \omega^\omega,\ \ldots\omega^{\omega^\omega},\ \ldots$$

Ďalší, odlišný typ nekonečných čísel Cantor objavil pri porovnávaní „veľkostí“ nekonečných množín, vychádzajúcom z porovnávania veľkostí konečných množín na základe počtu ich prvkov. Tento „zovšeobecnený počet prvkov“ množiny nazval jej *kardinálnym číslom* alebo *mohutnosťou*. Dve množiny A, B majú rovnaké kardinálne číslo, označenie $|A| = |B|$, ak existuje bijektívne zobrazenie $f\colon A \to B$. Hovoríme, že kardinálne číslo množiny A je menšie ako kardinálne číslo množiny B, symbolicky $|A| < |B|$, ak existuje injektívne zobrazenie $f\colon A \to B$ a neplatí $|A| = |B|$. Aj kardinálne čísla rozširujú prirodzené čísla (ktoré slúžia ako kardinálne čísla konečných množín) a taktiež na ne možno prirodzene rozšíriť aritmetiku prirodzených čísel so sčítaním, násobením aj umocňovaním. Ordinálna a kardinálna aritmetika sa však zásadne líšia: zatiaľ čo kardinálne sčítanie i násobenie sú komutatívne, pre ordinálne čísla napr. platí:

$$1+\omega = \omega < \omega+1 \qquad\qquad \omega\cdot 2 = \omega < 2\cdot\omega$$

Pre kardinálne číslo množiny $\mathbb{N}$ všetkých prirodzených čísel Cantor zaviedol označenie $\aleph_0 = |\mathbb{N}|$ ($\aleph$, čítaj *alef*, je prvé písmeno hebrejskej abecedy) a množiny mohutnosti $\aleph_0$ nazval *spočítateľnými* (*abzählbar*). Bezprostredne nasledujúce kardinálne číslo $\aleph_1 = |\Omega|$ zodpovedá množine Ω všetkých ordinálnych čísel, ktoré majú nanajvýš spočítateľne mnoho predchodcov. Kardinálne číslo množiny $\mathbb{R}$ všetkých reálnych čísel nazval Cantor *mohutnosťou kontinua* a označil ho $\mathfrak{c} = |\mathbb{R}|$. Podarilo sa mu ukázať, že $\mathfrak{c} = 2^{\aleph_0}$, kde $2^{\aleph_0} = |\mathcal{P}(\mathbb{N})|$ je mohutnosť množiny všetkých podmnožín množiny $\mathbb{N}$, ako aj nerovnosť $|X| < |\mathcal{P}(X)| = 2^{|X|}$ pre každú množinu X. Dlho sa potom snažil dokázať rovnosť $\mathfrak{c} = \aleph_1$, avšak bezvýsledne. Táto rovnosť dostala meno *hypotéza kontinua* a ocitla sa na prvom mieste v slávnom Hilbertovom zozname 23 problémov, ktorý predostrel matematickej verejnosti vo svojom vystúpení na II. Medzinárodnom matematickom kongrese v Paríži v r. 1900. O tom, ako bol tento problém vyriešený, sme sa už stručne zmienili v závere paragrafu venovaného neeuklidovskej geometrii.

Cantorovi sa však podarilo dokázať rad prekvapivých výsledkov. Ľubovoľný interval má rovnakú mohutnosť ako celá množina $\mathbb{R}$. Priamka $\mathbb{R}$ aj úsečka (t. j. interval) $[0,1]$ majú rovnakú mohutnosť ako rovina $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R}$ či štvorec $[0,1]^2 = [0,1]\times[0,1]$. Z toho možno odvodiť, že kontinuum ľubovoľnej konečnej dimenzie má rovnakú mohutnosť (čiže obsahuje „rovnako veľa bodov“) ako jednorozmerné kontinuum. To okrem iného – v protiklade s Cantorovým pôvodným očakávaním – znamená, že kardinálne číslo je príliš hrubý invariant na to, aby pomocou neho bolo možné zachytiť dimenziu bodovej množiny. Ďalej, množina $\mathbb{Q}$ všetkých racionálnych čísel aj množina $\mathbb{A}$ všetkých (reálnych) algebraických čísel[3] sú spočítateľné, teda majú mohutnosť $\aleph_0$. Na druhej strane, množina $\mathbb{R}$ všetkých reálnych čísel má mohutnosť $\mathfrak{c} > \aleph_0$. Tým Cantor podal

[3] Reálne, prípadne komplexné číslo c nazývame *algebraickým*, ak existuje polynóm $f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ s racionálnymi koeficientmi $a_1, \ldots, a_n \in \mathbb{Q}$ taký, že $f(c) = 0$.

čiste existenčný dôkaz existencie *transcendentných* (t. j. nealgebraických) reálnych čísel bez toho, aby čo i len jedno zostrojil.

Zachytenie mohutností nekonečných množín ich kardinálnymi číslami, prípadne štruktúry takzvaných *dobre usporiadaných množín*[4] ich ordinálnymi číslami, spolu s možnosťou rozšíriť na tieto čísla aritmetiku konečných prirodzených čísel, zmenili Cantorovo naladenie voči tým podobám javu nekonečna, ktoré predstavovali. Na jednej strane mu to pomohlo prekonať zábrany vykladať si toto nekonečno ako aktuálne. To viedlo v istom zmysle k zneváženiu tohto typu nekonečna prejavujúcej sa v nových názvoch ako *transfinitné množiny* či *transfinitné čísla*, ktoré mali naznačovať, že tvoria iba akýsi medzistupeň medzi konečnom a „pravým“ či „skutočným“ nekonečnom predstavovaným napr. oborom vôbec všetkých množín či obormi vôbec všetkých kardinálnych alebo ordinálnych čísel. Na druhej strane, pohľad do hĺbok týchto novootvorených oborov vyvoláva závrat, ktorý sa na formálnej rovine prejavuje nemožnosťou ich aktualizácie: ak pripustíme, že existuje množina vôbec všetkých množín alebo množina vôbec všetkých kardinálnych, resp. ordinálnych čísel, dospejeme k sporu. Cantor preto tieto obory nazýva *nekonzistentnými množinami* a pevne verí, že hroziace spory bude možné prekonať hlbším štúdiom princípov tvorby množín. Výnimkou je Russellov paradox, publikovaný až v r. 1903, ktorý sa rovnako týka Fregeho *Grundgesätze* ako Cantorovej teórie množín a práve jednoduchosťou svojej formulácie značne otriasol Cantorovou dôverou vo vlastnú teóriu.

Cantor si zároveň dobre uvedomoval, že svojím výkladom nekonečna ako aktuálneho narúša paradigmu rozhodujúcou mierou prevládajúcu v matematike aj vo filozofii od čias staroveku. Oporu nachádzal v kresťanskej teológii, podľa ktorej nekonečno aktuálne existuje, súc Božím atribútom, pokiaľ ide o mieru Jeho všemohúcnosti, vševedúcnosti, lásky a milosrdenstva. No vzápätí musel čeliť námietke, že svojou teóriou narúša Boží nárok na jedinečnosť a výlúčnosť byť nositeľom týchto atribútov. Cantor však bol presvedčený, že jeho teória množín nielen že nie je herézou, ale bola mu naopak zoslaná z nebies ako zjavenie novej hlbokej pravdy spolu s poslaním šíriť ju ďalej. Tu mu objavené paradoxy takpovediac hrali do karát, lebo vymedzovali „oblasť transfinitna“ ako prístupnú ľudskému intelektu a odeľovali ju od oblasti „pravého“, t. j. absolútneho a neaktualizovateľného nekonečna, vymykajúceho sa ľudskému rozumu a spadajúceho výlučne do Božej kompetencie. Aby však nadobudol istotu, že aktuálne nekonečno prítomné v jeho nekonečných množinách a nekonečných kardinálnych a ordinálnych číslach nie je v rozpore s cirkevným učením, obrátil sa na dvoch popredných rímsko-katolíckych mysliteľov svojej doby: na kňaza, teológa a filozofa Konstantina Gutberleta (1837 – 1928) a na jezuitského teológa zaoberajúceho sa otázkami cirkevnej dogmatiky, kardinála Johana Baptista Franzelina (1816 – 1886), s ktorými si vymenil viacero listov. Obaja teológovia reagovali na Cantorove myšlienky prívetivo a s porozumením. A po nie príliš dlhej diskusii s ním zhodne dospeli k názoru, že jeho teória množín neprotirečí učeniu cirkvi, a uznali, že aktualizácia nekonečna prítomného v nekonečných množinách a v transfinitných kardinálnych a ordinálnych číslach nie je narušením Božieho majestátu. Naopak, Cantorove objavy prispievajú k väčšej sláve Božej.

[4] Usporiadanú množinu $(X; <)$ nazývame *dobre usporiadanou*, ak každá jej neprázdna podmnožina má najmenší prvok.

V roku 1908 uverejnil nemecký matematik Ernst Zermelo (1871 – 1953) axiomatický systém teórie množín, v ktorom sa mu podarilo zachovať všetky podstatné vlastnosti Cantorovej teórie a zároveň sa vyhnúť všetkým známym množinovým paradoxom. Dosiahol to za cenu istého syntaktického obmedzenia vlastností, na ktoré možno aplikovať spomínaný vymedzovací princíp, ako aj požiadavkou, že nové množiny (až na tri výnimky) vymedzujeme ako časti vopred daných množín. Ako však sám poznamenáva, dokázať bezospornosť jeho systému (t. j. fakt, že sa v ňom nemôže vyskytnúť vôbec žiadny spor) sa mu nepodarilo. Zermelov systém neskôr doplnili Abraham Fraenkel (1891 – 1965) a samotný Zermelo. Zermelov-Fraenkelov axiomatický systém s axiómou výberu, skrátene označovaný ako ZFC, je dodnes najrozšírenejšou axiomatizáciou teórie množín.

Inú axiomatizáciu teórie množín, bližšiu duchu logicizmu v zmysle Fregeho a Russella, navrhol v r. 1937 americký filozof a logik Willard Van Orman Quine (1908 – 2000). Jeho systém nazývaný *New Foundations*, skrátene NF, pripúšťa univerzálnu množinu (t. j. množinu všetkých množín), pričom paradoxom sa vyhýba tak, že Cantorov vymedzovací princíp uplatňuje len pre vlastnosti, ktorých syntaktická forma vopred vylučuje autoreferenciu. New Foundations však majú rad bizarných znakov a v úlohe základov matematiky sa príliš neujali. Dokonca aj otázka relatívnej bezospornosti systému NF voči systému ZFC predstavuje dodnes otvorený problém.

V roku 1914, v predvečer I. svetovej vojny, vychádza kniha *Základy teórie množín* (*Grundzüge de Mengenlehre*) od Felixa Hausdorffa (1868 – 1942). Po skončení vojny sa z nej na dlhý čas stane najrozšírenejšia učebnica a zároveň referenčná monografia teórie množín. Jej druhé, prepracované a skrátené vydanie vychádza pod stručným názvom *Teória množín* (*Mengenlehre*) v r. 1927. Okrem sytematického výkladu samotnej teórie množín kniha obsahuje partie venované usporiadaným množinám, topológii (t. j. bodovým množinám), množinovému prístupu k teórii miery a pravdepodobnosti, ako aj k matematickej analýze a teórii funkcií. Hausdorff v nej uviedol do života prístup, ktorý sa v matematike v priebehu 20. storočia postupne presadí a prevládne v rozhodujúcej miere: študovať rozmanité matematické teórie prostredníctvom ich množinových modelov. Teória množín totiž nielen že poskytuje „dostatok priestoru“ na sprítomnenie možných štruktúr rôznych teórií v množinovom univerze, ale tiež dáva týmto teóriám k dispozícii univerzálny jazyk umožňujúci študovať ich jednotným spôsobom a zároveň odhaľovať vzťahy medzi nimi. Teória množín sa tak stáva zárukou vytúženej *vnútornej jednoty celej matematiky.* Podľa Hilberta je to „raj vytvorený pre nás Cantorom, z ktorého nás nikto nemôže vyhnať“. O to pálčivejšou sa tak stáva úloha dokázať bezospornosť teórie množín – podľa možnosti rovno jej axiomatického sytému ZFC, ale pre začiatok by stačilo dokázať aspoň bezospornosť nejakého jej fragmentu dostatočného na vybudovanie aritmetiky prirodzených a reálnych čísel a základov matematickej analýzy.

To sa ľahko povie, ale ťažko urobí. Vôbec totiž nie je jasné, ako by bolo treba pri takom dôkaze postupovať. Bežne sa dokazuje bezospornosť jednej teórie za predpokladu bezospornosti inej; napr. za predpokladu bezospornosti euklidovskej geometrie vieme dokázať bezospornosť geometrie hyperbolickej (a naopak). Avšak pre teóriu, ktorá má zohrať úlohu základov matematiky, už s relatívnym dôkazom bezospornosti, odvolávajúcim sa na bezospornosť nejakej inej „ešte základnejšej“, teórie nevysta-

číme. Potrebujeme nejaký „absolútny“ dôkaz. Sledujúc tento cieľ Hilbert v 20. rokoch 20. storočia navrhol a rozpracoval program *formalizácie matematiky*, ktorý umožňoval reprezentovať dôkazy v tej-ktorej teórii ako konečné postupnosti znakov s istou zreteľne rozpoznateľnou syntaktickou štruktúrou. Dokázať bezospornosť takto formalizovanej teórie potom už len vyžaduje overiť, že medzi dôkazmi v jej rámci sa nemôže vyskytnúť dvojica presne špecifikovaného tvaru, zodpovedného za spor v teórii. Ako však vyplýva z výsledkov Kurta Gödela z r. 1930, ciele Hilbertovho programu nie je možné naplniť.

2.8 Rozlúčka s históriou

Zostáva dopovedať, že v priebehu 20. a počiatkom 30. rokov 20. storočia dochádza k rozpoznaniu centrálneho postavenia *logiky prvého rádu* ako – aspoň z hľadiska matematiky – najdôležitejšej „vrstvy“ matematickej logiky. Prispeli k tomu najmä práce nórskeho matematika a logika Thoralfa Skolema (1881 – 1963) a Gödelov dôkaz *vety o úplnosti* logiky prvého rádu z r. 1929. To bolo potvrdené aj ďalším vývojom v prácach poľsko-amerického matematika a logika Alfreda Tarského a jeho žiakov v medzivojnovom Poľsku a neskôr v USA, sovietského matematika Anatolija Ivanoviča Maľceva (1909 – 1967), izraelsko-amerického logika a aplikovaného matematika Abrahama Robinsona (1918 – 1974) a mnohých ďalších, ktorí otvorili logike široké pole aplikácií v matematike. Postupne tak etablovali novú matematickú disciplínu, neskôr nazvanú *teóriou modelov*. Teóriu modelov možno do istej miery považovať za „metamatematiku algebry“. Vytvára totiž všeobecný rámec pre a poskytuje jednotiaci pohľad na rôzne algebraické disciplíny, čím umožňuje odhaliť ich často skryté vzájomné súvislosti. Ako však ukazuje príklad Robinsonovej *neštandardnej analýzy*, aplikáciami v algebre sa jej možnosti zďaleka nevyčerpávajú.

Búrlivý rozvoj matematickej logiky nastúpený v 20. a 30. rokoch sa ešte urýchlil po II. svetovej vojne a pokračoval po zvyšok 20. storočia až do súčasnosti. Je jednoducho nemožné čo i len načrtnúť jeho priebeh v rámci obmedzeného rozsahu tejto učebnice. Preto zmeníme štýl a spôsob nášho výkladu a ďalší vývoj matematickej logiky už nebudeme sledovať z historickej perspektívy. Miesto toho sa zameriame na vecný obsahový výklad jej hlavných súčastí: výrokového počtu, logiky prvého rádu a malej ukážky teórie modelov. Medzi druhú a tretiu zo spomínaných tém vložíme ešte kapitolu venovanú slávnym *Gödelovým vetám o neúplnosti* a stručnému zamysleniu sa nad ich filozofickými dôsledkami.

3 Výrokový počet

Výrokový počet, nazývaný aj *výroková logika* alebo *logika nultého rádu*, skúma štruktúru istého fragmentu spoločného pre prirodzené jazyky ako aj pre jazyky vedeckých teórií. Tento fragment tvoria abstraktné vzory alebo formy výrokov či tvrdení, ktoré sa v nich vyskytujú, ako aj vzťahy medzi nimi, na ktoré možno usudzovať na základe ich formy. To nám umožní úplný popis platných argumentov v termínoch štrukturálnych relácií medzi formami ich súčastí.

Zároveň sa budeme spoliehať na to, že naši čitatelia sú už do istej miery oboznámení s výrokovým počtom, vrátane logických spojok a ich významu, tabuliek pravdivostných hodnôt, tautológií atď. To nám umožní sústrediť sa na niektoré „filozofické" aspekty výrokového počtu a využiť túto známu a pomerne elementárnu látku ako platformu pre výklad istých tém a otázok, ktoré sa neskôr znovu objavia v náročnejšej podobe v rámci predikátového počtu.

3.1 Výroky a výrokové formy

Výrok alebo *tvrdenie* je zmysluplná výpoveď, ktorá má podobu oznamovacej gramatickej vety a je buď pravdivá alebo nepravdivá, pričom je nepodstatné, či my alebo ktokoľvek iný dokáže o jej pravdivosti rozhodnúť. Hovoríme, že *pravdivostná hodnota* výroku je 1, ak je pravdivý, a 0, ak je nepravdivý.

Z daných výrokov môžeme vytvoriť nové ich kombináciami pomocou unárnej logickej spojky *nie* a binárnych logických spojok *a*, *alebo*, *ak ... tak*, *práve vtedy keď*, *buď ... alebo*, *ani ... ani* atď. Výrokový počet sa zakladá na nasledujúcom fundamentálnom pozorovaní:

> *Ak A je výrok vytvorený určitým spôsobom z nejakých jednoduchších výrokov $p_1, \ldots, p_n$ pomocou logických spojok, tak pravdivostnú hodnotu A možno určiť len na základe pravdivostných hodnôt výrokov $p_1, \ldots, p_n$ a spôsobu ich spojenia, akým vytvárajú výrok A, bez ohľadu na význam a obsah dielčích výrokov $p_1, \ldots, p_n$.*

Inak povedané, pravdivostnú hodnotu výroku A možno *vypočítať* z pravdivostných hodnôt jeho zložiek $p_1, \ldots, p_n$ a abstraktného vzoru alebo *formy* výroku A.

V dôsledku toho predmetom výrokového počtu nie sú primárne samotné výroky ale formy, aké môžu výroky nadobúdať podľa toho, ako sú zložené z jednoduchších výrokov pomocou logických spojok. Tieto abstaktné formy nazývame *výrokovými formami*; sú to výrazy (slová) istého formálneho jazyka, ktorý teraz zavedieme. Za účelom popisu *syntaxe* jazyka výrokového počtu kodifikujeme jeho symboly a opíšeme spôsob, akým sú generované jeho slová.

Jazyk výrokového počtu má nasledujúce symboly rozdelené do troch skupín:

- Výrokové premenné: p, q, r, p_0, p_1, p_2, $\ldots$, q', q'', $\ldots$
- Logické spojky: $\neg$ (*nie*), $\wedge$ (*a*), $\vee$ (*alebo*), $\Rightarrow$ (*ak ... tak* prípadne *implikuje*), $\Leftrightarrow$ (*práve vtedy, keď*) (stačili by dve).
- Pomocné symboly: (,) (*zátvorky*) (dalo by sa zaobísť aj bez nich).

Znakom P označíme množinu všetkých výrokových premenných. Budeme predpokladať, že množina P je nekonečná aspoň v potenciálnom zmysle, to znamená, že vždy, keď máme daný akýkoľvek konečný zoznam výrokových premenných $p_1, \ldots, p_n$, môžeme nájsť nejakú novú výrokovú premennú q, ktorá sa nenachádza v tomto zozname, a zároveň že všetky výrokové premenné $p \in P$ možno zasadiť do vzájomne jednoznačnej korešpodencie s prirodzenými číslami $n \in \mathbb{N}$.

Výrokové formy sú určité konečné postupnosti, t. j. slová, pozostávajúce zo skôr uvedených symbolov. Množina $\mathrm{VF}(P)$ všetkých výrokových foriem nad množinou výrokových premenných P je definovaná rekurzívne ako najmenšia množina, ktorá obsahuje všetky výrokové premenné a je uzavretá vzhľadom na aplikáciu logických spojok. Inak povedané, je to najmenšia množina, ktorá spĺňa nasledujúce dve podmienky:

1° $P \subseteq \mathrm{VF}(P)$ (každá výroková premenná $p \in P$ je výroková forma nad množinou P).

2° Ak $A, B \in \mathrm{VF}(P)$, tak $\neg A, (A \wedge B), (A \vee B), (A \Rightarrow B), (A \Leftrightarrow B) \in \mathrm{VF}(P)$ (ak slová A, B sú výrokové formy nad množinou P, tak aj slová $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$ a $(A \Leftrightarrow B)$ sú výrokové formy nad P).

Vzhľadom na 1° výrokové premenné niekedy nazývame *atomickými výrokovými formami*. V dôsledku spočítateľnosti množiny P všetkých výrokových premenných je aj množina $\mathrm{VF}(P)$ všetkých výrokových foriem nad P spočítateľná.

Množinu $\mathrm{VF}(Q)$ všetkých výrokových foriem nad akoukoľvek neprázdnou množinou výrokových premenných $Q \subseteq P$ možno definovať analogicky. Špeciálne pre konečnú množinu $Q = \{p_1, \ldots, p_n\}$ kladieme

$$\mathrm{VF}(Q) = \mathrm{VF}(p_1, \ldots, p_n)$$

Keďže každá výroková forma $A \in \mathrm{VF}(P)$ je vytvorená z atomických výrokových foriem konečným počtom použití pravidla 2°, môžeme vždy nájsť konečný počet výrokových premenných $p_1, \ldots, p_n \in P$ takých, že $A \in \mathrm{VF}(p_1, \ldots, p_n)$.

Ak A, B sú výrokové formy, tak výrokovú formu $\neg A$ nazývame *negáciou* A, a výrokové formy $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$ a $(A \Leftrightarrow B)$ nazývame postupne *konjunkciou*, *disjunkciou* alebo *alternatívou*, *implikáciou* a *ekvivalenciou* A a B.

3.1.1 Poznámka. (a) Podľa poslednej definície sú nie všetky konečné postupnosti symbolov jazyka výrokového počtu výrokové formy. Ľahko možno rozpoznať, že napr. výrazy p, q, r, $\neg p$, $(p \wedge q)$, $(\neg p \Rightarrow r)$, $((p \wedge q) \vee (\neg p \Rightarrow r))$ sú výrokové formy, zatiaľ čo

výrazy ako $(p\neg q)$, $\neg pp\Rightarrow)(r\neg$ výrokovými formami zrejme nie sú. Už menej zrejmý je však fakt, že ani žiaden z výrazov $p\wedge q$, $\neg p\Rightarrow r$, $(p\wedge q)\vee(\neg p\Rightarrow r)$ nie je výrokovou formou, hoci sme asi náchylní ich za výrokové formy uznať. V snahe zmieriť uvedenú definíciu s našou intuíciou a obvyklou praxou prijmeme dohodu, že krajné vonkajšie zátvorky (ktoré sú očividne nadbytočné) budeme vo výrokových formách vynechávať. Takže výrazy ako napr. $p\wedge q$, $\neg p\Rightarrow r$, $(p\wedge q)\vee(\neg p\Rightarrow r)$ budeme postupne chápať ako označenia výrokových foriem $(p\wedge q)$, $(\neg p\Rightarrow r)$, $((p\wedge q)\vee(\neg p\Rightarrow r))$, a pod.

(b) Zátvorky by sme mohli úplne oželieť a miesto nich používať tzv. *poľskú notáciu*. V tom prípade by bod 2° uvedenej definície bolo treba modifikovať takto:

2* Ak $A, B\in \mathrm{VF}(P)$, tak $\neg A$, $\wedge AB$, $\vee AB$, $\Rightarrow AB$, $\Leftrightarrow AB\in \mathrm{VF}(P)$ (ak výrazy A, B sú výrokové formy nad množinou P, tak aj výrazy $\neg A$, $\wedge AB$, $\vee AB$, $\Rightarrow AB$ a $\Leftrightarrow AB$ sú výrokové formy nad P)

Napríklad zápis výrokovej formy $(p\wedge q)\vee(\neg p\Rightarrow r)$ by v poľskej notácii vyzeral takto:

$$\vee\wedge pq\Rightarrow\neg pr$$

Akokoľvek ťažkopádny a ťažko čitateľný nám uvedený zápis môže pripadať, treba si uvedomiť, že z hľadiska počítačového spracovania je tento aspekt prakticky bezvýznamný.

(c) Napriek menám, ktorými sme logické spojky nazvali v snahe poukázať na ich zamýšľané roly, zatiaľ ich treba chápať ako púhe grafické symboly zbavené akéhokoľvek významu. Svoj obvyklý význam nadobudnú až neskôr, keď vybudujeme sémantiku výrokového počtu.

(d) Ešte poznamenajme, že znaky A, B, C, ktorými označujeme ľubovoľné výrokové formy, ako aj znak P a výraz $\mathrm{VF}(P)$, ktoré označujú množinu všetkých výrokových premenných, resp. množinu všetkých výrokových foriem atď., nepatria do jazyka výrokového počtu. Sú to znaky prípadne výrazy istého metajazyka, ktorý používame pri štúdiu výrokového počtu.

Obráťme ešte pozornosť čitateľa na tú okolnosť, že $\mathrm{VF}(P)$ je *najmenšia* množina, ktorá spĺňa podmienky 1° a 2°. Táto nenápadná požiadavka nám dáva do rúk silný prostriedok na dokazovanie faktov o výrokových formách. Ide menovite o metódu dôkazov *indukciou podľa zložitosti*: Ak chceme dokázať, že všetky výrokové formy majú istú vlastnosť, stačí overiť, že množina všetkých výrokových foriem s touto vlastnosťou spĺňa skôr uvedené podmienky 1° a 2°.

3.1.2 Veta. *Nech $M\subseteq \mathrm{VF}(P)$ je ľubovoľná množina výrokových foriem, ktorá spĺňa nasledujúce dve podmienky:*

1° $P\subseteq M$
(každá výroková premenná $p\in P$ patrí do množiny M)

2° *Ak $A, B\in M$, tak $\neg A$, $A\wedge B$, $A\vee B$, $A\Rightarrow B$, $A\Leftrightarrow B\in M$ (M je uzavretá vzhľadom na tvorbu výrokových foriem pomocou logických spojok)*

Potom $M=\mathrm{VF}(P)$, čiže každá výroková forma nad P patrí do M.

Čitateľ by mal porovnať indukciu podľa zložitosti s bežnou metódou indukcie používanou pri dokazovaní, že všetky prirodzené čísla spĺňajú istú vlastnosť: Keďže množina $\mathbb{N}$ všetkých prirodzených čísel je najmenšia množina, ktorá obsahuje číslo 0 a je uzavretá vzhľadom na operáciu nasledovníka $n \mapsto n+1$, na to, aby sme dokázali, že určitá množina $M \subseteq \mathbb{N}$ obsahuje všetky prirodzené čísla, t. j. $M = \mathbb{N}$, stačí overiť, že $0 \in M$ a pre každé $n \in M$ platí $n+1 \in M$. Pri indukcii podľa zložitosti úlohu čísla 0 zohrávajú výrokové premenné $p \in P$ a úlohu operácie nasledovníka preberajú logické spojky. Už v tejto chvíli môžeme predvídať, že na účely dôkazov indukciou by bolo žiadúce minimalizovať počet logických spojok, pre ktoré treba overiť podmienku 2°. K tejto otázke sa vrátime v nasledujúcom paragrafe.

3.2 Interpretácie, tabuľky pravdivostných hodnôt a logická ekvivalencia

Vzápätí po syntaxi vybudujeme *sémantiku* výrokového počtu. Pripomeňme si, že v logike neberieme do úvahy obsah výrokov a výrokové formy sú naozaj zbavené akéhokoľvek obsahu. Jednako, stále môžeme skúmať situácie, v ktorých by boli pravdivé alebo nepravdivé. Tieto situácie, ktoré nazveme interpretáciami alebo pravdivostnými ohodnoteniami, budú predstavovať spôsob, ako možno výrokovým formám predsa len priradiť určitý, akokoľvek obmedzený význam.

Pre začiatok zavedieme boolovské algebraické operácie na dvojprvkvej množine $\{0,1\}$ pravdivostných hodnôt 0 (*nepravda*) a 1 (*pravda*) zodpovedajúce logickým spojkám a značené rovnakými symbolmi. Sú dané nasledujúcimi tabuľkami:

$\neg$	0	1
	1	0

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$\Rightarrow$	0	1
0	1	1
1	0	1

$\Leftrightarrow$	0	1
0	1	0
1	0	1

Vo výrokovom počte nazývame *interpretáciou* alebo *pravdivostným ohodnotením* ľubovoľné zobrazenie $I\colon P \to \{0,1\}$, t. j, ľubovoľné priradenie pravdivostných hodnôt 0 alebo 1 výrokovým premenným. Intuitívne taká interpretácia predstavuje možnú situáciu opísanú prostredníctvom priradenia pravdivostných hodnôt výrokovým premenným.

Každú interpretáciu $I\colon P \to \{0,1\}$ rozšírime do zobrazenia $I\colon \mathrm{VF}(P) \to \{0,1\}$, ktoré označujeme rovnakým symbolom a stále nazývame interpretáciou alebo pravdivostným ohodnotením, nasledujúcou rekurzívnou definíciou:

$$I(\neg A) = \neg I(A) \qquad I(A \wedge B) = I(A) \wedge I(B) \qquad I(A \Rightarrow B) = I(A) \Rightarrow I(B)$$
$$I(A \vee B) = I(A) \vee I(B) \qquad I(A \Leftrightarrow B) = I(A) \Leftrightarrow I(B)$$

pre všetky $A, B \in \mathrm{VF}(P)$, za predpokladu, že hodnoty $I(A)$ a $I(B)$ už boli definované. Namiesto $I(A) = 1$ hovoríme, že A je pravdivá alebo splnená v interpretácii I; $I(A) = 0$ znamená, že A je nepravdivá v interpretácii I.

Čitateľ by si mal uvedomiť nasledujúce dve skutočnosti:

- V každej vyššie z uvedených rovností symboly $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ označujú logické spojky na pravej strane, zatiaľ čo na ľavej strane označujú im zodpovedajúce boolovské operácie na množine $\{0,1\}$.

- Symbol rovnosti $=$ a znaky I, J označujúce ľubovoľné pravdivostné ohodnotenia patria do nášho metajazyka, a nie do jazyka samotného výrokového počtu.

Až od tejto chvíle a vďaka tabuľkám operácií $\neg$, $\wedge$, $\vee$, $\Rightarrow$ a $\Leftrightarrow$ na množine $\{0,1\}$ pravdivostných hodnôt môžu príslušné logické spojky oprávnene niesť svoje názvy *negácie*, resp. *konjunkcie*, *alternatívy* alebo *disjunkcie* (v nevylučovacom zmysle), *implikácie* a *ekvivalencie*.

Ľahko možno nahliadnuť, že uvedená rekurzívna definícia je v istom zmysle redundantná. Stačilo by popísať rozšírenie zobrazenia $I\colon P \to \{0,1\}$ vzhľadom na negáciu $\neg$ a ktorúkoľvek jednu z logických spojok $\wedge$, $\vee$, $\Rightarrow$; zvyšné rovnosti by už boli splnené automaticky. Inak povedané, zobrazenie $I\colon \mathrm{VF}(P) \to \{0,1\}$ je interpretáciou práve vtedy, keď spĺňa rovnosť $I(\neg A) = \neg I(A)$, a ktorúkoľvek jednu z rovností $I(A \wedge B) = I(A) \wedge I(B)$, $I(A \vee B) = I(A) \vee I(B)$, $I(A \Rightarrow B) = I(A) \Rightarrow I(B)$ pre všetky $A, B \in \mathrm{VF}(P)$. V dôsledku toho možno pojem interpretácie (pravdivostného ohodnotenia) definovať elegantnejším spôsobom: Je to zobrazenie $I\colon \mathrm{VF}(P) \to \{0,1\}$ zachovávajúce operácie algebier $(\mathrm{VF}(P); \wedge, \vee, \neg)$, $(\{0,1\}; \wedge, \vee, \neg)$, teda *homomorfizmus* $I\colon (\mathrm{VF}(P); \wedge, \vee, \neg) \to (\{0,1\}; \wedge, \vee, \neg)$.

Upresnime práve diskutovanú otázku. Dve $A, B \in \mathrm{VF}(P)$ nazveme *logicky ekvivalentými*, ak $I(A) = I(B)$ pre každú interpretáciu $I\colon P \to \{0,1\}$; v tom prípade píšeme $A \equiv B$. (Treba si uvedomiť, že znak $\equiv$, podobne ako znaky A, B, C, P, I, J alebo výraz $\mathrm{VF}(P)$, nepatrí do jazyka výrokového počtu – opäť je to znak nášho metajazyka.) Čitateľ by si mal samostatne overiť, že relácia logickej ekvivalencie je reflexívna, symetrická a tranzitívna, teda je to naozaj relácia ekvivalencie.

Je známe, že hociktorá z dvojíc $(\neg, \wedge)$, $(\neg, \vee)$, $(\neg, \Rightarrow)$ tvorí *úplný systém logických spojok*, to znamená, že každá výroková forma $A \in \mathrm{VF}(P)$ je logicky ekvivalentná s nejakou výrokovou formou A', ktorá obsahuje rovnaké výrokové premenné ako A, a vyskytujú sa v nej výlučne logické spojky z jedinej (a to ktorejkoľvek) z uvedených troch dvojíc.

Ak si za primitívne spojky zvolíme $\neg$, $\wedge$, tak zvyšné spojky možno zaviesť ako skratky za výrokové formy vpravo:

$$\begin{aligned} A \vee B &\equiv \neg(\neg A \wedge \neg B) \\ A \Rightarrow B &\equiv \neg(A \wedge \neg B) \\ A \Leftrightarrow B &\equiv \neg(A \wedge \neg B) \wedge \neg(\neg A \wedge B) \end{aligned}$$

Zvoliac $\neg$ a $\vee$ ako primitívne spojky, dostaneme

$$\begin{aligned} A \wedge B &\equiv \neg(\neg A \vee \neg B) \\ A \Rightarrow B &\equiv \neg A \vee B \\ A \Leftrightarrow B &\equiv \neg(\neg(A \vee \neg B) \vee \neg(\neg A \vee B)) \end{aligned}$$

Konečne, ak si ako primitívne spojky vyberieme $\neg$ a $\Rightarrow$, budeme mať

$$A \wedge B \equiv \neg(A \Rightarrow \neg B)$$
$$A \vee B \equiv \neg A \Rightarrow B$$
$$A \Leftrightarrow B \equiv (A \Rightarrow \neg B) \Rightarrow \neg(\neg A \Rightarrow B)$$

Z toho je jasné, že v rekurzívnej definícii pojmu výrokovej formy v predošlom paragrafe by bolo stačilo použiť unárnu spojku $\neg$ a ktorúkoľvek jednu z troch binárnych spojok $\wedge$, $\vee$, $\Rightarrow$; štvrtá binárna spojka $\Leftrightarrow$ sa stáva v každom prípade zbytočnou.

Ďalej budeme využívať logickú ekvivalenciu asociativity logických spojok $\wedge$ a $\vee$

$$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C) \qquad \text{a} \qquad (A \vee B) \vee C \equiv A \vee (B \vee C)$$

pre ľubovoľné výrokové formy $A, B, C \in \mathrm{VF}(P)$. To nám umožňuje vynechať zátvorky v konjunkciách a alternatívach ľubovoľného konečného počtu výrokových foriem a jednoducho písať $A \wedge B \wedge C$, $A \vee B \vee C$, $A_1 \wedge \ldots \wedge A_m$, $B_1 \vee \ldots \vee B_n$ atď.

Stojí za povšimnutie, že by sme mohli vystačiť aj s jedinou binárnou spojkou, menovite so *Shefferovým ťahom* $|$ (Sheffer stroke, NAND operator), ktorú možno vyjadriť pomocou $\neg$ a $\wedge$, alebo pomocou $\neg$ a $\vee$ takto:

$$A|B \ \equiv \neg(A \wedge B) \equiv \neg A \vee \neg B$$

Obrátene, štandardné logické spojky $\neg$, $\wedge$ a $\vee$ možno vyjadriť pomocou Shefferovho ťahu takto:

$$\neg A \equiv A|A$$
$$A \wedge B \equiv (A|B)|(A|B)$$
$$A \vee B \equiv (A|A)|(B|B)$$

Úlohu nájsť zodpovedajúce vyjadrenia pre $A \Rightarrow B$ a $A \Leftrightarrow B$ prenechávame čitateľovi.

Iná logická spojka, ktorá samotná stačí na vyjadrenie všetkých ostatných, známa pod názvami *Peircova šípka* alebo *Quinova dýka* $\dagger$ (Peirce arrow, Quine dagger, NOR operator), je duálna k Shefferovmu ťahu. Pomocou $\neg$ a $\wedge$, alebo $\neg$ a $\vee$ ju možno vyjadriť takto:

$$A \dagger B \equiv \neg A \wedge \neg B \equiv \neg(A \vee B)$$

Vyjadrenie obvyklých logických spojok $\neg$, $\wedge$, $\vee$, $\Rightarrow$ a $\Leftrightarrow$ pomocou Peirceovej šípky $\dagger$ prenechávame čitateľovi, rovnako ako vyjadrenie Shefferovho ťahu pomocou Peirceovej šípky a obrátene.

3.3 Tautológie a ďalšie triedy výrokových foriem

Pomocou pojmu interpretácie môžeme vymedziť viacero dôležitých tried výrokových foriem. Hovoríme, že výroková forma $A \in \mathrm{VF}(P)$ je

- *tautológia*, ak $I(A) = 1$ pre každú interpretáciu $I\colon P \to \{0,1\}$
- *kontradikcia*, ak $I(A) = 0$ pre každú interpretáciu $I\colon P \to \{0,1\}$
- *splniteľná*, ak $I(A) = 1$ pre aspoň jednu interpretáciu $I\colon P \to \{0,1\}$
- *vyvrátiteľná* ak $I(A) = 0$ pre aspoň jednu interpretáciu $I\colon P \to \{0,1\}$

Za povšimnutie stojí dvojaká dualita medzi štyrmi práve zavedenými pojmami:
vnútorná dualita

- A je tautológia práve vtedy, keď $\neg A$ je kontradikcia
- A je splniteľná práve vtedy, keď $\neg A$ je vyvrátiteľná

a *vonkajšia dualita*

- A je tautológia práve vtedy, keď A nie je vyvrátiteľná
- A je kontradikcia práve vtedy, keď A nie je splniteľná

Ľahko možno nahliadnuť, že pre ľubovoľné výrokové formy A, B platí $A \equiv B$ práve vtedy, keď výroková forma $A \Leftrightarrow B$ je tautológia.

Otázku, či daná výroková forma A patrí do tej-ktorej z uvedených tried, možno rozhodnúť algoritmicky metódou *tabuliek pravdivostných hodnôt*, výpočtom pravdivostných hodnôt $I(A)$ pre všetky interpretácie $I\colon P \to \{0,1\}$. Vzhľadom na fakt, že pre nekonečnú množinu P je takých inerpretácií nekonečne mnoho, hrá dôležitú úlohu pozorovanie, že stačí zaoberať sa len konečným počtom vhodných interpretácií.

3.3.1 Veta. *Nech $A \in \mathrm{VF}(P)$ je ľubovoľná výroková forma taká, že všetky výrokové premenné, ktoré sa v nej vyskytujú, sú zahrnuté v zozname $p_1, \ldots, p_n$. Potom $I(A) = J(A)$ pre akékoľvek pravdivostné ohodnotenia $I, J\colon P \to \{0,1\}$ také, že $I(p_k) = J(p_k)$ pre každé $k = 1, \ldots, n$.*

Inak povedané, hodnota $I(A)$ pravdivostného ohodnotenia I na výrokovej forme A závisí iba na hodnotách I na konečnej množine výrokových premenných vyskytujúcich sa v A. Akokoľvek zrejmý a intuitívne jasný nám tento fakt môže pripadať, jednako ho dokážeme, najmä preto, aby sme ilustrovali metódu dôkazu indukciou podľa zložitosti.

Ešte poznamenajme, že termín *dôkaz* budeme počnúc nasledujúcim paragrafom používať výlučne pre formálne dôkazy vo výrokovom počte. Tie budú tvoriť jednu zo súčastí predmetu nášho skúmania. Kvôli odlíšeniu budeme dôkazy výsledkov o výrokovom počte (a neskôr o predikátovom počte) vedené v našom metajazyku nazývať *demonštráciami*.

Demonštrácia. Označme $Q = \{p_1, \ldots, p_n\}$ a

$$M = \{A \in \mathrm{VF}(Q)\colon I(A) = J(A)\}$$

Treba dokázať, že $M = \mathrm{VF}(Q)$. Keďže I a J sa zhodujú na množine Q, máme $Q \subseteq M$, čo je začiatočný krok indukcie 1°. Aby sme overili indukčný krok 2°, predpokladajme, že $A, B \in M$, t. j. $A, B \in \mathrm{VF}(Q)$ a $I(A) = J(A)$ ako aj $I(B) = J(B)$. Potom, keďže I aj J zachovávajú logické spojky,

$$I(\neg A) = \neg I(A) = \neg J(A) = J(\neg A)$$
$$I(A \wedge B) = I(A) \wedge I(B) = J(A) \wedge J(B) = J(A \wedge B)$$

čiže $\neg A, A \wedge B \in M$. Podobne by sme mohli ukázať, že aj $A \vee B, A \Rightarrow B, A \Leftrightarrow B \in M$. No vzhľadom na naše predošlé úvahy, indukčný krok 2° pre spojky $\vee$, $\Rightarrow$ a $\Leftrightarrow$ už nie je potrebný.

3.3.2 Príklad. Pomocou tabuľky pravdivostných hodnôt možno ľahko overiť, že nasledujúca výroková forma je tautológia:

$$(p \Rightarrow (q \Rightarrow r)) \Leftrightarrow ((p \wedge q) \Rightarrow r)$$

Označme L výrokovú formu $p \Rightarrow (q \Rightarrow r)$ a R výrokovú formu $(p \wedge q) \Rightarrow r$. Postupne dostaneme tabuľku

p	q	r	$q \Rightarrow r$	L	$p \wedge q$	R	$L \Leftrightarrow R$
1	1	1	1	1	1	1	1
1	1	0	0	0	1	0	1
1	0	1	1	1	0	1	1
0	1	1	1	1	0	1	1
1	0	0	1	1	0	1	1
0	1	0	0	1	0	1	1
0	0	1	1	1	0	1	1
0	0	0	1	1	0	1	1

V dôsledku toho

$$A \Rightarrow (B \Rightarrow C) \equiv (A \wedge B) \Rightarrow C$$

pre ľubovoľné výrokové formy A, B, C.

Dôležitejšie a zaujímavejšie než mechanické vypĺňanie uvedenej pravdivostnej tabuľky je uvedomiť si, čo za logický zákon, nazývaný aj *zákon rozčlenenia* (law of exportation), vyjadruje príslušná tautológia alebo následná logická ekvivalencia. Forma vľavo $A \Rightarrow (B \Rightarrow C)$ hovorí: „ak A, tak z B vyplýva C“. Forma vpravo $(A \wedge B) \Rightarrow C$ hovorí: „A a B spolu implikujú C“. Tieto dve formy tvrdení su vždy ekvivalentné: ak postupujeme zľava doprava, môžeme zlúčiť predpoklady A a B do jediného predpokladu $A \wedge B$; postupujúc sprava doľava, môžeme rozčleniť predpoklad $A \wedge B$ na jeho dielčie zložky A a B a aplikovať ich jednu po druhej.

3.3.3 Úloha. (Normálne formy) Výrokovú formu nazývame *elementárnou konjunkciou*, ak má tvar $B_1 \wedge \ldots \wedge B_m$, kde každá z foriem B_i je výroková premenná alebo negácia nejakej výrokovej premennej. Hovoríme, že výroková forma je *disjunktívna normálna forma*, ak má tvar $C_1 \vee \ldots \vee C_k$, kde každá z foriem C_j je elementárna konjunkcia. Ukážte, že každá výroková forma $A \in \mathrm{VF}(p_1, \ldots, p_n)$ je logicky ekvivalentná s nejakou disjunktívnou normálnou formou $A' \in \mathrm{VF}(p_1, \ldots, p_n)$. Za tým účelom navrhnite algoritmickú metódu, ako zostrojiť disjunktívnu normálnu formu $A' \equiv A$ z pravdivostnej tabuľky formy A.

Podobne definujte duálne pojmy *elementárnej disjunkcie* a *konjunktívnej normálnej formy* a ukážte, že každá výroková forma je logicky ekvivalentná s nejakou konjunktívnou normálnou formou.

3.3.4 Úloha. (Boolovské funkcie) Nech $A \in \mathrm{VF}(p_1, \ldots, p_n)$ je výroková forma nad množinou výrokových premenných $p_1, \ldots, p_n$. Potom z A možno vytvoriť *boolovskú funkciu* $F_A \colon \{0,1\}^n \to \{0,1\}$, čiže n-árnu operáciu na dvojprvkovej množine $\{0,1\}$, danú predpisom $F_A(e_1, \ldots, e_n) = I(A)$ pre všetky $e_1, \ldots, e_n \in \{0,1\}$, kde

$I\colon \{p_1,\dots,p_n\} \to \{0,1\}$ je interpretácia na množine $\{p_1,\dots,p_n\}$ taká, že $I(p_k) = e_k$ pre $k = 1,\dots,n$.

(a) Ukážte, že pre ľubovoľné výrokové formy $A, B \in \mathrm{VF}(p_1,\dots,p_n)$ platí $F_A = F_B$ práve vtedy, keď $A \equiv B$.

(b) Dokážte, že pre dané $n \geq 1$ existuje práve 2^{2^n} boolovských funkcií $\{0,1\}^n \to \{0,1\}$. Ako je to v prípade $n = 0$?

(c) Ukážte, že pre každú boolovskú funkciu $F\colon \{0,1\}^n \to \{0,1\}$ existuje nekonečne mnoho výrokových foriem $A \in \mathrm{VF}(p_1,\dots,p_n)$ takých, že $F = F_A$.

3.3.5 Úloha. Nech $A \in \mathrm{VF}(p_1,\dots,p_n)$ je výroková forma vo výrokových premenných $p_1,\dots,\ p_n$ a $B_1,\dots,B_n \in \mathrm{VF}(P)$ sú ľubovoľné výrokové formy. Označme $A(B_1,\dots,B_n)$ výrokovú formu získanú substitúciou výrokových foriem $B_1,\dots,\ B_n$ namiesto premenných $p_1,\dots,\ p_n$ v príslušnom poradí do formy A. Napríklad, ak A je forma $(p \wedge \neg q) \Rightarrow (q \vee r)$ vo výrokových premenných p, q, r a B, C, D sú porade výrokové formy $r \vee s$, $p \Rightarrow \neg r$, q, tak $A(B,C,D)$ označuje formu

$$((r \vee s) \wedge \neg(p \Rightarrow \neg r)) \Rightarrow ((p \Rightarrow \neg r) \vee q)$$

(a) Zdôvodnite, že ak A je tautológia (kontradikcia), tak $A(B_1,\dots,B_n)$ je opäť tautológia (kontradikcia) pre ľubovoľné $B_1,\dots,\ B_n$.

(b) Uveďte príklad splniteľnej (vyvrátiteľnej) formy A a foriem $B_1,\dots,\ B_n$ takých, že $A(B_1,\dots,B_n)$ nie je splniteľná (vyvrátiteľná).

3.4 Teórie vo výrokovom počte

Slovo *teória* v bežnom jazyku zvyčajne odkazuje k nejakému systému vzájomne prepojených poznatkov, pozostávajúcemu z tvrdení o určitej oblasti javov a zahŕňajúcemu tiež metodológiu získavania a overovania alebo vyvracania týchto tvrdení. Tvrdenia alebo výroky tvoriace „telo systému“ mohli byť získané rozličnými spôsobmi: niektoré z nich vyjadrujú určité empirické fakty ustanovené pozorovaním alebo experimentmi, niektoré sú súčasťou všeobecného presvedčenia, tradície alebo kultúrneho dedičstva, niektoré z nich môžu byť púhe hypotézy čakajúce na potvrdenie alebo vyvrátenie v budúcnosti a konečne, niektoré z nich môžu byť odvodené z tých skôr spomínaných ako ich logické dôsledky.

V súlade s vedúcimi zámermi logiky budeme ignorovať obsah, metodológiu a celkový charakter nejakej teórie, rovnako nebudeme rozlišovať, ktoré z jej postulátov sú pravdivé či nepravdivé, ktoré sú pevne stanovené a ktoré sú púhymi hypotézami, ani sa nebudeme starať o to, ako k tomuto rozdeleniu došlo. Sústredíme sa na jediný aspekt všetkých takých teórií, totiž na štruktúru logického vyplývania, t. j. na spôsob, akým nové tvrdenia nevyhnutne vyplývajú alebo môžu byť odvodené z tých, ktorým sme priznali postavenie východzích postulátov alebo axióm tej-ktorej teórie.

Podľa toho budeme *teóriou vo výrokovom počte* alebo jednoducho len *teóriou* nazývať ľubovoľnú množinu $T \subseteq \mathrm{VF}(P)$ výrokových foriem; jej prvkom $A \in T$ budeme hovoriť *špecifické axiómy* alebo len krátko *axiómy* teórie T. Varujeme čitateľa pred tým, aby bral túto definíciu doslovne, dokonca ani v rámci výrokového počtu, nieto

ešte zo širšieho hľadiska. Skôr by ju mal chápať ako uznanie faktu, že nejaká teória v rámci výrokového počtu je *daná* alebo *jednoznačne určená* množinou svojich špecifických axióm. O všetko ostatné sa postará výrokový počet; štruktúra vyplývania je totiž pre všetky teórie vo výrokovom počte rovnaká.

Interpretáciu $I\colon \mathrm{VF}(P) \to \{0,1\}$ nazveme *interpretáciou teórie* T, ak $I(A) = 1$ pre každé $A \in T$, t. j. ak všetky axiómy teórie T sú pravdivé v interpretácii I. Intuitívne to znamená, že interpretácia I predstavuje situáciu, v ktorej sú všetky axiómy teórie T splnené, teda je splnená samotná T.

Hovoríme, že výroková forma B je *logickým* alebo *nevyhnutným dôsledkom* (axióm) teórie T, ak $I(B) = 1$ pre každú interpretáciu I teórie T. Alternatívne hovoríme, že B je *pravdivá* alebo *platná* alebo *splnená* v T. Symbolicky píšeme $T \vDash B$. Intuitívne $T \vDash B$ znamená, že v každej možnej siuácii, v ktorej sú splnené všetky axiómy teórie T, je splnené aj B.

Namiesto $\emptyset \vDash B$ píšeme len $\vDash B$; znamená to, že B je pravdivá v úplne každej interpretácii $I\colon P \to \{0,1\}$, inými slovami, B je tautológia.

Ako vyplýva z nasledujúcej vety, otázku, či $T \vDash B$, možno rozhodnúť algoritmicky s použitím tabuliek pravdivostných hodnôt pre každú teóriu T, ktorá má iba konečne mnoho axióm, a každú výrokovú formu $B \in \mathrm{VF}(P)$.

3.4.1 Veta. *Nech $T = \{A_1, \ldots, A_n\}$ je teória s konečne mnohými špecifickými axiómami a $B \in \mathrm{VF}(P)$. Potom $T \vDash B$ práve vtedy, keď výroková forma $(A_1 \wedge \ldots \wedge A_n) \Rightarrow B$ je tautológia.*

Demonštrácia. Predpokladajme, že $T \vDash B$. Nech $I\colon \mathrm{VF}(P) \to \{0,1\}$ je ľubovoľná interpretácia. Potom buď $I(A_k) = 0$ pre aspoň jedno $k = 1, \ldots, n$, alebo $I(A_k) = 1$ pre každé $k = 1, \ldots, n$. V prvom prípade $I(A_1 \wedge \ldots \wedge A_n) = 0$, takže

$$I((A_1 \wedge \ldots \wedge A_n) \Rightarrow B) = 1$$

V druhom prípade je I interpretáciou teórie T, teda $I(B) = 1$, lebo $T \vDash B$. Potom opäť

$$I((A_1 \wedge \ldots \wedge A_n) \Rightarrow B) = 1$$

To znamená, že $(A_1 \wedge \ldots \wedge A_n) \Rightarrow B$ je naozaj tautológia.

Obrátene, predpokladajme, že $(A_1 \wedge \ldots \wedge A_n) \Rightarrow B$ je tautológia, čiže je pravdivá v každej interpretácii I. Ak I je interpretáciou T, tak $I(A_1 \wedge \ldots \wedge A_n) = 1$. Preto

$$I((A_1 \wedge \ldots \wedge A_n) \Rightarrow B) = 1$$

može nastať jedine vtedy, keď aj $I(B) = 1$. Takže $T \vDash B$.

Vo všeobecnosti však T môže mať nekonečne mnoho špecifických axióm. Aj v tomto prípade na to, aby sme dokázali, že B nie je logickým dôsledkom teórie T, čiže $T \nvDash B$, stačí nájsť jedinú interpretáciu I teórie T takú, že $I(B) = 0$. V tom prípade hovoríme, že platnosť B v T bola *vyvrátená kontrapríkladom* I. Aby sme však potvrdili, že $T \vDash B$, potrebujeme podľa definície určiť pravdivostnú hodnotu $I(B)$ pre všetky interpretácie teórie T a tých môže byť nekonečne mnoho. Takže ide o zdanlivo neuskutočniteľnú úlohu.

Obvyklý spôsob v matematike, akým ustanovujeme platnosť nejakého tvrdenia v rámci nejakej teórie, však spočíva v tom, že toto tvrdenie *dokážeme z axióm* tejto teórie, a nie v tom, že budeme preberať všetky možné situácie, v ktorých sú tieto axiómy splnené, a v každej z nich overovať platnosť onoho tvrdenia. Aj vo výrokovom počte vybudujeme syntaktické pojmy dôkazu a dokázateľnosti s cieľom zachytiť pomocou nich sémantické pojmy platnosti či pravdivosti.

3.5 Axiomatizácia výrokového počtu

Aby sme dostali čo najstručnejšiu axiomatizáciu výrokového počtu, budeme postupovať tak, ako keby množina $\mathrm{VF}(P)$ všetkých výrokových foriem bola vybudovaná z výrokových premenných iba s použitím logických spojok $\neg$ a $\Rightarrow$. Takže zvyšné logické spojky budeme považovať za určité skratky zobrazené v predchádzajúcom paragrafe. Alternatívnu axiomatizáciu používajúcu logické spojky $\neg$, $\wedge$, $\vee$ a $\Rightarrow$ predstavíme v záverečnom paragrafe 3.9.

3.5.1 Logické axiómy. *(4 schémy axióm)*
Pre ľubovoľné výrokové formy A, B, C nasledujúce výrokové formy sú logické axiómy:

(LAx 1) $A \Rightarrow (B \Rightarrow A)$
(LAx 2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$
(LAx 3) $(A \Rightarrow B) \Rightarrow ((A \Rightarrow \neg B) \Rightarrow \neg A)$
(LAx 4) $\neg\neg A \Rightarrow A$

Navyše máme jediné odvodzovacie alebo deduktívne pravidlo:

3.5.2 Odvodzovacie pravidlo: Modus Ponens

$$\text{(MP)} \quad \frac{A,\ A \Rightarrow B}{B} \quad \textit{(z } A \textit{ a } A \Rightarrow B \textit{ odvoď } B\textit{)}$$

3.5.3 Úloha. (a) Presvedčte sa, že všetky logické axiómy sú tautológie a vysvetlite ich intuitívny význam.

(b) Ukážte, že odvodzovacie pravidlo Modus Ponens je korektné v nasledujúcom zmysle:

Ak $I\colon \mathrm{VF}(P) \to \{0,1\}$ je ľubovoľná interpretácia a $A, B \in \mathrm{VF}(P)$ sú výrokové formy také, že $I(A) = I(A \Rightarrow B) = 1$, tak aj $I(B) = 1$.

Dôkaz v teórii $T \subseteq \mathrm{VF}(P)$ je konečná postupnosť $A_0, A_1, \ldots, A_n$ výrokových foriem taká, že každý jej člen A_k je buď logická axióma alebo špecifická axióma teórie T (t. j. $A_k \in T$) alebo vyplýva z predchádzajúcich členov podľa pravidla Modus Ponens (t. j. existujú $i, j < k$ také, že A_j má tvar $A_i \Rightarrow A_k$).

Výroková forma B je *dokázateľná* v teórii T, ak existuje dôkaz $A_0, A_1, \ldots, A_n$ v T taký, že jeho posledný člen A_n je zhodný s B. Symbolicky píšeme $T \vdash B$. Namiesto $\emptyset \vdash B$ píšeme len $\vdash B$; znamená to, že B je dokázateľné výlučne z logických axióm.

3.5.4 Poznámka. Uvedená axiomatizácia výrokového počtu nie je ani zďaleka jediná možná. Ako sme už spomínali, alternatívnu axiomatizáciu možno nájsť v paragrafe 3.9. Obe tieto axiomatizácie obsahujú nekonečne mnoho axióm (uvedených v tvare konečného počtu schém axióm) a jediné odvodzovacie pravidlo. Takéto axiomatizácie sa obvykle označujú ako *axiomatizácie Hilbertovho typu*. Vyznačujú sa tým, že majú „mnoho“ axióm a „málo“ odvodzovacích pravidiel. Na druhej strane, *axiomatizácie Gentzenovho typu* obsahujú „mnoho“ odvodzovacích pravidiel a len „málo“ logických axióm (či dokonca žiadnu, nahradiac logickú axiómu A pravidlom $\frac{}{A}$ s významom *odvoď A z ničoho*). Vo všeobecnosti sú axiomatizácie Hilbertovho typu vhodnejšie na opis, štúdium a analýzu samotných formálnych logických systémov, zatiaľ čo axiomatizácie Gentzenovho typu sú efektívnejšie pri aplikáciách, napr. pri logickom programovaní alebo automatickom dokazovaní teorém. No ako axiomatizácie klasického výrokového počtu sú všetky ekvivalentné v tom zmysle, že generujú rovnaké súbory dokázateľných foriem.

3.5.5 Úloha. Overte, že pre ľubovoľné výrokové formy A, B nasledujúce výrokové formy sú tautológie, a ukážte, že všetky sú dokázateľné iba z logických axióm:

(a) $A \Rightarrow A$
(b) $A \Rightarrow \neg\neg A$
(c) $\neg A \Rightarrow (A \Rightarrow B)$
(d) $(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$
(e) $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$
(f) $(A \Rightarrow (\neg B \Rightarrow \neg(A \Rightarrow B)))$
(g) $(A \Rightarrow B) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow B)$
(h) $(\neg A \Rightarrow A) \Rightarrow A$

Ako príklad (pomerne odstrašujúci) ukážeme, že pre každú výrokovú formu A je forma v (a) dokázateľná z logických axióms.

1. $(A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$
   (LAx 2), dosadením A za A aj C a $A \Rightarrow A$ za B
2. $A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$
   (LAx 1), dosadením A za A a $A \Rightarrow A$ za B
3. $(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)$
   vyplýva z 1. a 2. podľa (MP)
4. $A \Rightarrow (A \Rightarrow A)$
   (LAx 1), dosadením A za A aj B
5. $A \Rightarrow A$
   vyplýva z 3. a 4. podľa (MP)

3.5.6 Úloha. Ukážte, že schémy axióm (LAx 3) a (LAx 4) možno nahradiť jedinou schémou axióm

(LAx 5) $(\neg A \Rightarrow B) \Rightarrow ((\neg A \Rightarrow \neg B) \Rightarrow A)$

Za tým účelom overte, že každá inštancia schémy (LAx 5) je dokázateľná z nejakých inštancií schém (LAx 1), (LAx 2), (LAx 3), (LAx 4), a obrátene, všetky inštancie schém (LAx 3), (LAx 4) sú dokázateľné z nejakých inštancií schém (LAx 1), (LAx 2), (LAx 5).

3.6 Veta o korektnosti

Vzápätí po zavedení axiomatizácie výrokového počtu vyvstáva pred nami úloha ukázať, že táto axiomatizácia je *korektná* v nasledujúcom zmysle: Pre akúkoľvek teóriu $T \subseteq \mathrm{VF}(P)$ sú všetky výrokove formy dokázateľné v T zároveň splnené v T. Inak by sa mohlo stať, že pre nejakú výrokovú formu B dokázateľnú v T nájdeme interpretáciu I teórie T takú, že $I(B) = 0$. Taká interpretácia I by predstavovala situáciu, v ktorej sú všetky axiómy teórie T splnené, jednako B v nej splnené nie je. Takže by sa mohlo stať, že z axióm teórie dokážeme dôsledky protirečiace týmto axiómam, čo by znamenalo pohromu v podobe zrútenia našej axiomatizácie. Preto je nanajvýš dôležité, že máme k dispozícii nasledujúci výsledok.

3.6.1 Veta o korektnosti. *Nech $T \subseteq \mathrm{VF}(P)$ je teória. Potom pre ľubovoľnú výrokovú formu $B \in \mathrm{VF}(P)$ z $T \vdash B$ vyplýva $T \vDash B$.*

Demonštrácia. Nech $T \vdash B$ a $A_0, A_1, \ldots, A_n$ je dôkaz B v T. Dokážeme, že $I(A_k) = 1$ pre každú interpretaciu I teórie T a *každé* $k \leq n$. Potom, samozrejme, $I(B) = 1$, lebo B je A_n. Každé A_k je buď logická axióma, v tom prípade $I(A_k) = 1$ pre vôbec každú interpretáciu I, alebo špecifická axióma teórie T, vtedy $I(A_k) = 1$, lebo I je interpretáciou T, alebo A_k vyplýva z nejakých predošlých členov A_i, A_j podľa (MP). Predpokladajúc, že sme už dokázali, že $I(A_i) = I(A_j) = 1$, možeme uzavrieť, že tiež $I(A_k) = 1$, lebo, ako sme už poznamenali v Úlohe 3.5.3 (b), pravidlo (MP) je korektné.

3.6.2 Poznámka. Obráťme teraz pozornosť k tej skutočnosti, že práve zaznamenaná argumentácia – akokoľvek jednoduchá a priezračná nám môže pripadať – nie je prostá bludného kruhu. Pri demoštrácii Vety o korektnosti sme používali logickú dedukciu v prirodzenom jazyku rozšírenom o veľmi jednoduché matematické značenie. Takže sme vlastne na neformálnej úrovni používali rovnaké logické prostriedky ako tie, ktorých správnosť sme mali ešte len ustanoviť v rámci formalizovaného výrokového počtu. Prísne vzaté, formálny proťajšok neformálnych logických prostriedkov, ktoré sme použili, presahuje rámec výrokového počtu: keďže naša argumentácia používala aj kvantifikátory, zasahovala dokonca do predikátového počtu. Je dôležité si uvedomiť, že nemôžeme dokázať Vetu o korektnosti takpovediac z ničoho, bez toho, aby sme prepokladali aspoň istý minimálny logický fragment prirodzeného jazyka. Takže to, čo sme dosiahli, nie je nič viac a nič menej než uvedomenie si, že naša formálna axiomatizácia výrokového počtu je v dobrej zhode s logickou štruktúrou vyplývania a odvodzovania v prirodzenom jazyku.

Neskôr ustanovíme aj nasledujúce obrátenie Vety o korektnosti.

3.6.3 Veta o úplnosti. *Nech $T \subseteq \mathrm{VF}(P)$ je teória. Potom pre ľubovoľnú výrokovú formu $B \in \mathrm{VF}(P)$ z $T \vDash B$ vyplýva $T \vdash B$.*

3.6.4 Poznámka. Bude poučné porovnať status Vety o úplnosti so statusom Vety o korektnosti. Ako sme videli, demonštrácia Vety o korektnosti bola dosť jednoduchá. Na druhej strane, ako uvidíme neskôr, demonštrácia Vety o úplnosti bude podstatne zložitejšia. Zatiaľ čo neplatnosť Vety o korektnosti by spôsobila zrútenie našej axiomatizácie výrokového počtu, dôsledky možnej neplatnosti Vety o úplnosti by boli aspoň na prvý pohľad menej dramatické: znamenali by iba toľko, že naša axiomatizácia výrokového počtu nie je dostatočne silná, a preto by sme sa mali poobhliadnuť po nejakých dodatočných logických axiómach a/alebo odvodzovacích pravidlách, o ktoré by sme ju mohli rozšíriť s cieľom dosiahnuť úplnosť. Vzápätí by sme však museli čeliť ďaleko jemnejšej otázke: Je vôbec možné dosiahnuť úplnosť našej axiomatizácie bez toho, aby sme narušili jej korektnosť? Až Vety o korektnosti a úplnosti vo vzájomnom spojení dávajú kladnú odpoveď na túto otázku a zaručujú, že vzťah medzi syntaxou a sémantikou výrokového počtu je starostlivo vyvážený.

Neskôr, keď sa budeme zaoberať analogickými otázkami pre predikátový počet, uvedieme príklad istého jeho značne prirodzeného fragmentu, ktorý nepripúšťa nijakú axiomatizáciu spĺňajúcu zároveň Vetu o korektnosti aj Vetu o úplnosti.

3.7 Veta o dedukcii a jej dôsledky

Cestou k dôkazu Vety o úplnosti sformulujeme rad výsledkov, ktoré sú zaujímavé aj samy osebe. Pri ich demonštrácii budeme používať označenie $A \approx B$ vyjadrujúce fakt, že písmená A a B označujú tú istú výrokovú formu. Symbol $\approx$, podobne ako symboly A, B, P, VF, I, $\equiv$ atď., patrí do nášho metajazyka, a nie do samotného jazyka výrokového počtu.

3.7.1 Veta o dedukcii. *Nech $T \subseteq \mathrm{VF}(P)$ je teória a $A, B \in \mathrm{VF}(P)$ sú výrokové formy. Potom $T \vdash A \Rightarrow B$ práve vtedy, keď $T \cup \{A\} \vdash B$.*

Demonštrácia. Nech $T \vdash A \Rightarrow B$. Tým skôr $T \cup \{A\} \vdash A \Rightarrow B$. Zrejme $T \cup \{A\} \vdash A$, z čoho dostávame $T \cup \{A\} \vdash B$ podľa (MP). Ak totiž $C_0, C_1, \ldots, C_n$ je dôkaz formy $A \Rightarrow B$ v teórii $T \cup \{A\}$, tak $C_0, C_1, \ldots, C_n, A, B$ je dôkaz formy B v $T \cup \{A\}$.

Obrátene, nech $T \cup \{A\} \vdash B$. Najskôr vybavíme nasledujúce dva triviálne prípady:

(a) B je logická axióma alebo $B \in T$. Potom B, $B \Rightarrow (A \Rightarrow B)$ (LAx 1), $A \Rightarrow B$ je dôkaz formy $A \Rightarrow B$ v T.

(b) $B \approx A$. Potom $\vdash A \Rightarrow A$ (Úloha 3.5.5 (a)), a tým skôr $T \vdash A \Rightarrow A$.

Inak musí existovať dôkaz $B_0, B_1, \ldots, B_n$ formy B v teórii $T \cup \{A\}$ taký, že $n \geq 2$ a B_n (t. j. B) vyplýva z nejakých jeho predošlých členov podľa (MP). Budeme postupovať indukciou vzhľadom na n. Predpokladajme teda, že potrebný záver je platný pre všetky dôkazy $C_0, C_1, \ldots, C_m$ v $T \cup \{A\}$, kde $m < n$. Nech $j, k < n$ sú také, že $B_j \approx (B_k \Rightarrow B_n)$. Potom $B_0, \ldots, B_j$ aj $B_0, \ldots, B_k$ sú dôkazy v $T \cup \{A\}$. Podľa indukčného predpokladu máme $T \vdash A \Rightarrow B_j$, t. j. $T \vdash A \Rightarrow (B_k \Rightarrow B_n)$, ako aj $T \vdash A \Rightarrow B_k$. Potom

$$(A \Rightarrow (B_k \Rightarrow B_n)) \Rightarrow ((A \Rightarrow B_k) \Rightarrow (A \Rightarrow B_n))$$

je (LAx 2) a s použitím (MP) postupne dostávame

$$T \vdash (A \Rightarrow B_k) \Rightarrow (A \Rightarrow B_n)$$
$$T \vdash A \Rightarrow B_n$$

čiže $T \vdash A \Rightarrow B$.

Čitateľ by si mal uvedomiť, že je to tá „ťažšia“ implikácia

$$\text{ak } T \cup \{A\} \vdash B, \text{ tak } T \vdash A \Rightarrow B$$

ktorú bežne používame pri matematických dôkazoch ako aj v mnohých deduktívnych argumentoch inde. Typický priamy dôkaz implikácie $A \Rightarrow B$ vychádzajúci z nejakého zoznamu predpokladov, t. j. z axióm nejakej teórie T, obvykle začína „rituálnou formulkou“: „*Nech* A“, prípadne „*Predpokladajme, že* A“. To neznamená nič iné ako rozšírenie zoznamu axióm T o novú axiómu A. Pokračujeme postupnosťou tvrdení $C_1, \ldots, C_n$ vytváraných podľa určtiých deduktívnych pravidiel, až kým neskončíme pri záverečnom tvrdení B. Prísne vzaté však to, čo sme takto vytvorili, je dôkaz tvrdenia B v teórii $T \cup \{A\}$ a nie dôkaz implikácie $A \Rightarrow B$ v teórii T, ako by sme si želali. Veta o dedukcii ukazuje, že tento prirodzený spôsob argumentácie je legitímne použiteľný aj vo výrokovom počte.

Iný spôsob dokazovania tvrdení vychádzajúc z nejakého zoznamu predpokladov je *dôkaz sporom*. Namiesto toho, aby sme dokazovali A v T priamo, odvodíme spor (protirečenie) s axiómami teórie T z negácie tvrdenia A. Aj tento spôsob je legitímny v rámci výrokového počtu.

Hovoríme, že teória T je *sporná* alebo *protirečivá* alebo tiež *inkonzistentná*, ak existuje výroková forma A taká, že zároveň $T \vdash A$ aj $T \vdash \neg A$. V opačnom prípade hovoríme, že T je *bezosporná* alebo *neprotirečivá* alebo tiež *konzistentná*. Z Úlohy 3.5.5 (c) vyplýva, že v spornej teórii je dokázateľná každá výroková forma B.

3.7.2 Dôsledok o dôkaze sporom. *Nech $T \subseteq \mathrm{VF}(P)$ je teória a $A \in \mathrm{VF}(P)$ je výroková forma. Potom $T \vdash A$ práve vtedy, keď teória $T \cup \{\neg A\}$ je sporná (inkonzistentná).*

Demonštrácia. Nech $T \vdash A$. Tým skôr $T \cup \{\neg A\} \vdash A$. Keďže zrejme $T \cup \{\neg A\} \vdash \neg A$, teória $T \cup \{\neg A\}$ je sporná.

Obrátene, nech $T \cup \{\neg A\}$ je sporná teória. Potom každá výroková forma je dokázateľná v T; špeciálne $T \cup \{\neg A\} \vdash A$. Potom $T \vdash \neg A \Rightarrow A$ podľa Vety o dedukcii. Podľa Úlohy 3.5.5 (h), $\vdash (\neg A \Rightarrow A) \Rightarrow A$, a tým skôr $T \vdash (\neg A \Rightarrow A) \Rightarrow A$. Pomocou (MP) dostávame $T \vdash A$.

Niekedy sa nám nedarí nájsť dôkaz tvrdenia B v teórii T, ale za istého dodatočného predpokladu A vieme B dokázať určitým spôsobom a za opačného predpokladu $\neg A$ iným spôsobom. Za týchto podmienok jednako platí, že B je dokázateľné v T. I tento spôsob argumentácie je legitímny vo výrokovom počte.

3.7.3 Dôsledok o dôkaze rozborom prípadov. *Nech $T \subseteq \mathrm{VF}(P)$ je a teória a $A, B \in \mathrm{VF}(P)$ sú výrokové formy. Potom $T \cup \{A\} \vdash B$ a $T \cup \{\neg A\} \vdash B$ práve vtedy, keď $T \vdash B$.*

Demonštrácia. Predpokladajme, že $T \cup \{A\} \vdash B$ a $T \cup \{\neg A\} \vdash B$. Podľa Vety o dedukcii z toho vyplýva $T \vdash A \Rightarrow B$ a $T \vdash \neg A \Rightarrow B$. Na základe Úlohy 3.5.5 (g) máme

$$\vdash (A \Rightarrow B) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow B)$$

a dvojnásobným použitím (MP) dostávame $T \vdash B$.

Obrátene, nech $T \vdash B$. Potom triviálne $T \cup \{A\} \vdash B$ aj $T \cup \{\neg A\} \vdash B$.

3.7.4 Úloha. *Nech $T \subseteq \mathrm{VF}(P)$ je teória a $A_1, \ldots, A_n, B \in \mathrm{VF}(P)$ sú výrokové formy také, že $T \vdash A_1 \vee \ldots \vee A_n$. Ukážte, že $T \vdash B$ práve vtedy, keď $T \cup \{A_i\} \vdash B$ pre každé $i = 1, \ldots, n$.*

3.8 Veta o úplnosti

Začneme jednou technickou lemou. Pre danú interpretáciu $I\colon \mathrm{VF}(P) \to \{0,1\}$ a výrokovú formu $A \in \mathrm{VF}(P)$ označíme

$$A^I \approx \begin{cases} A & \text{ak } I(A) = 1 \\ \neg A & \text{ak } I(A) = 0 \end{cases}$$

Inými slovami, A^I je ten člen dvojice A, $\neg A$, ktorý je pravdivý v I, čiže $I(A^I) = 1$.

3.8.1 Lema o interpretácii. (A. Church) *Nech $p_1, \ldots, p_n \in P$ a $A \in \mathrm{VF}(p_1, \ldots, p_n)$. Potom pre ľubovoľnú interpretáciu $I\colon \mathrm{VF}(P) \to \{0,1\}$ platí*

$$\{p_1^I, \ldots, p_n^I\} \vdash A^I$$

Demonštrácia. Indukciou podľa zložitosti formy A:

(a) Ak $A \approx p \in P$, tak tvrdenie hovorí, že $\{p\} \vdash p$, ak $I(p) = 1$, alebo $\{\neg p\} \vdash \neg p$, ak $I(p) = 0$. V oboch prípadoch dostávame potrebný záver.

(b) Nech $A \approx \neg B$ a náš záver platí pre B. Potom $B \in \mathrm{VF}(p_1, \ldots, p_n)$.

Ak $I(A) = 1$, tak $I(B) = 0$ a $A^I \approx A \approx \neg B \approx B^I$. Podľa indukčného predpokladu $\{p_1^I, \ldots, p_n^I\} \vdash B^I$, čiže $\{p_1^I, \ldots, p_n^I\} \vdash A^I$.

Ak $I(A) = 0$, tak $I(B) = 1$, $B^I \approx B$ a $A^I \approx \neg A \approx \neg\neg B$. Podľa indukčného predpokladu $\{p_1^I, \ldots, p_n^I\} \vdash B^I$, čiže $\{p_1^I, \ldots, p_n^I\} \vdash B$. Vzhľadom na Úlohu 3.5.5 (b) máme $\vdash B \Rightarrow \neg\neg B$, a pomocou (MP) dostaneme $\{p_1^I, \ldots, p_n^I\} \vdash \neg\neg B$, teda $\{p_1^I, \ldots, p_n^I\} \vdash A^I$.

(c) Nech $A \approx (B \Rightarrow C)$ a náš záver platí pre B, C. Potom $B, C \in \mathrm{VF}(p_1, \ldots, p_n)$. Rozlíšime tri prípady:

1. $I(B) = 0$. Potom $I(A) = I(B \Rightarrow C) = 1$, čiže $A^I \approx A$. Ďalej $B^I \approx \neg B$, takže podľa predpokladu $\{p_1^I, \ldots, p_n^I\} \vdash \neg B$. Vzhľadom na Úlohu 3.5.5 (c) platí $\vdash \neg B \Rightarrow (B \Rightarrow C)$ a pomocou (MP) dostávame $\{p_1^I, \ldots, p_n^I\} \vdash B \Rightarrow C$, t. j. $\{p_1^I, \ldots, p_n^I\} \vdash A^I$.

2. $I(C) = 1$. Potom $C^I \approx C$ a $I(A) = I(B \Rightarrow C) = 1$, preto $A^I \approx A$. Podľa indukčného predpokladu $\{p_1^I, \ldots, p_n^I\} \vdash C$. (LAx 1) dáva $\vdash C \Rightarrow (B \Rightarrow C)$, a vďaka (MP) dostávame $\{p_1^I, \ldots, p_n^I\} \vdash B \Rightarrow C$, teda $\{p_1^I, \ldots, p_n^I\} \vdash A^I$.

3. $I(B) = 1$, $I(C) = 0$. Potom $B^I \approx B$, $C^I \approx \neg C$ a $I(A) = I(B \Rightarrow C) = 0$, preto $A^I \approx \neg A$. Podľa indukčného predpokladu $\{p_1^I, \ldots, p_n^I\} \vdash B$ a $\{p_1^I, \ldots, p_n^I\} \vdash \neg C$. Podľa Úlohy 3.5.5 (f) máme $\vdash B \Rightarrow (\neg C \Rightarrow \neg(B \Rightarrow C))$. Použijúc dvakrát (MP) dostaneme $\{p_1^I, \ldots, p_n^I\} \vdash \neg(B \Rightarrow C)$, teda $\{p_1^I, \ldots, p_n^I\} \vdash A^I$.

3.8.2 Úloha. Nech $Q = \{p_1, \ldots, p_n\} \subseteq P$ je konečná množina výrokových premenných a $A \in \mathrm{VF}(Q)$. Nech ďalej

$$\mathrm{TE}(A) = \big\{I \colon Q \to \{0,1\} \colon I(A) = 1\big\} = \{I_1, \ldots, I_m\}$$

označuje množinu všetkých pravdivostných ohodnotení I na množine výrokových premenných Q takých, že A je pravdivé v I. Zrejme $m \leq 2^n$. Pre každé $I \in \mathrm{TE}(A)$ označíme

$$C_I = p_1^I \wedge \ldots \wedge p_n^I$$

elementárnu konjunkciu zodpovedajúcu I. Konečne položíme

$$A' = C_{I_1} \vee \ldots \vee C_{I_m}$$

Zdôvodnite, že $A' \in \mathrm{VF}(Q)$ je disjunktívna normálna forma logicky ekvivalentná s formou A (pozri Úlohu 3.3.3).

Špeciálny prípad Vety o úplnosti, pochádzajúci od Emila Posta, sa zaoberá dokázateľnosťou tautológií.

3.8.3 Postova veta o úplnosti. *Pre ľubovoľnú výrokovú formu $A \in \mathrm{VF}(P)$ platí $\vDash A$ práve vtedy, keď $\vdash A$. Inými slovami, A je tautológia práve vtedy, keď A je dokázateľná výhradne z logických axióm.*

Demonštrácia. Dokážeme len, že každá tautológia je dokázateľná iba z logických axióm; obrátená implikácia vyplýva z Vety o korektnosti.

Nech $A \in \mathrm{VF}(p_1, \ldots, p_n)$ je tautológia. Potom $I(A) = 1$ a $A^I \approx A$ pre každé pravdivostné ohodnotenie $I \colon \{p_1, \ldots, p_n\} \to \{0,1\}$. Podľa Lemy 3.8.1 o interpretácii

$$\{p_1^I, \ldots, p_n^I\} \vdash A$$

Pre akúkoľvek interpretáciu $J \colon \{p_1, \ldots, p_{n-1}\} \to \{0,1\}$ obe možnosti $I_1(p_n) = 1$, $I_2(p_n) = 0$, spolu s podmienkou $I_1(p_k) = I_2(p_k) = J(p_k)$ pre $k < n$, určujú interpretácie $I_1, I_2 \colon \{p_1, \ldots, p_n\} \to \{0,1\}$. Preto súčasne platí

$$\{p_1^J \ldots, p_{n-1}^J, p_n\} \vdash A$$
$$\{p_1^J \ldots, p_{n-1}^J, \neg p_n\} \vdash A$$

Podľa Dôsledku 3.7.3 o dôkaze rozborom prípadov z toho vyplýva

$$\{p_1^J, \ldots, p_{n-1}^J\} \vdash A$$

Opakovaním tohto postupu nakoniec dostaneme $\vdash A$.

Teória $T \subseteq \mathrm{VF}(P)$ sa nazýva *úplná*, ak je bezosporná a pre každú výrokovú formu $A \in \mathrm{VF}(P)$ platí $T \vdash A$ alebo $T \vdash \neg A$. Inými slovami, T je úplná práve vtedy, keď pre každú výrokovú formu A nastane práve jedna z možností $T \vdash A$, $T \vdash \neg A$.

Teraz dokážeme alternatívnu verziu Vety o úplnosti.

3.8.4 Veta o úplnosti. (Alternatívna verzia) *Každá bezosporná teória* $T \subseteq \mathrm{VF}(P)$ *má aspoň jednu interpretáciu.*

Čitateľ by si mal uvedomiť, že to platí aj obrátene: ak nejaká teória má interpretáciu, tak je nevyhnutne bezosporná. Inak povedané, sporná teória nemá žiadnu interpretáciu. (Toto je alternatívna verzia Vety o korektnosti.)

Demonštrácia. Akákoľvek interpretácia I konzistentnej teórie T musí spĺňať podmienku

$$I(A) = \begin{cases} 1 & \text{ak } T \vdash A \\ 0 & \text{ak } T \vdash \neg A \end{cases}$$

Keďže T je konzistentná, $T \vdash A$ a $T \vdash \neg A$ nemôže nastať súčasne pre žiadnu formu $A \in \mathrm{VF}(P)$. Na druhej strane, pokiaľ T nie je úplná, nemožno zaručiť, že vždy bude platiť buď $T \vdash A$ alebo $T \vdash \neg A$, teda hodnota $I(A)$ nemusí byť definovaná pre všetky $A \in \mathrm{VF}(P)$. Ale ak T je *úplná*, tak uvedená podmienka skutočne definuje interpretáciu teórie T. To znamená, že úplná teória T má práve jednu interpretáciu.

Vo všeobecnom prípade, nakoľko množina $\mathrm{VF}(P)$ všetkých výrokových foriem je spočítateľná, možno ju očíslovať prirodzenými číslami, čiže zapísať v tvare postupnosti $\mathrm{VF}(P) = \{A_0, A_1, \ldots, A_n, \ldots\}$. Teraz definujeme postupnosť teórií $T_0, T_1, \ldots, T_n, \ldots$ rekurziou:

$$T_0 = T \quad \text{a} \quad T_{n+1} = \begin{cases} T_n \cup \{A_n\} & \text{ak } T_n \cup \{A_n\} \text{ je konzistentná} \\ T_n \cup \{\neg A_n\} & \text{ak } T_n \cup \{A_n\} \text{ je sporná} \end{cases}$$

Zrejme $T_n \subseteq T_{n+1}$ pre každé n. Indukciou podľa n dokážeme, že každé T_n je konzistentná teória. Teória $T_0 = T$ je konzistentná podľa počiatočného predpokladu. Ak predpokladáme, že T_n je konzistentná, tak T_{n+1} by mohla byť sporná jedine v prípade, keby obe teórie $T_n \cup \{A_n\}$, $T_n \cup \{\neg A_n\}$ boli sporné. To by však podľa Dôsledku 3.7.2 o dôkaze sporom znamenalo, že $T_n \vdash \neg A_n$ a zároveň $T_n \vdash A_n$. To je však nemožné, lebo T_n je bezosporná.

Ďalej ukážeme, že $\widehat{T} = \bigcup_{n\in\mathbb{N}} T_n$ je úplná teória. Ľahko možno nahliadnuť, že $\widehat{T}$ je bezosporná. Keby totiž $\widehat{T}$ bola sporná, tak už niektorá z teórií T_n by musela byť sporná (toto prenechávame na premyslenie čitateľovi – pozri tiež dôkaz Vety 3.8.8 o kompaktnosti). Zostáva dokázať, že pre každé n platí buď $\widehat{T} \vdash A_n$ alebo $\widehat{T} \vdash \neg A_n$. To je ekvivalentné s tvrdením, že $\widehat{T} \nvdash \neg A_n$ implikuje $\widehat{T} \vdash A_n$. Ak $\widehat{T} \nvdash \neg A_n$, tak $\widehat{T} \cup \{A_n\}$ je konzistentná, preto aj $T_n \cup \{A_n\} \subseteq \widehat{T} \cup \{A_n\}$ je konzistentná. Potom $A_n \in T_{n+1}$, preto $T_{n+1} \vdash A_n$, a keďže $T_{n+1} \subseteq \widehat{T}$, tak aj $\widehat{T} \vdash A_n$.

Teda jediná interpretácia I úplnej teórie $\widehat{T}$ je zároveň interpretáciou teórie T.

3.8.5 Poznámka. Čitateľ by si mal uvedomiť, že skôr uvedená alternatíva nepredstavuje jedinú možnosť ako definovať postupnosť teórií $(T_n)_{n\in\mathbb{N}}$ rozširujúcich T a vedúcich k úplnej teórii $\widehat{T} = \bigcup T_n$ a k interpretácii I. V každom kroku, keď neplatí $T_n \vdash A_n$ ani $T_n \vdash \neg A_n$, si totiž môžeme slobodne vybrať z dvoch možností: $T_{n+1} = T_n \cup \{A_n\}$ alebo $T_{n+1} = T_n \cup \{\neg A_n\}$.

3.8.6 Úloha. Nech $I\colon P \to \{0,1\}$ je ľubovoľné pravdivostné ohodnotenie. Označme

$$\mathrm{Th}(I) = \{p^I : p \in P\} = \{p \in P\colon I(p) = 1\} \cup \{\neg p\colon p \in P,\ I(p) = 0\}$$

teóriu interpretácie I. Demonštrujte nasledujúce fakty:

(a) $\mathrm{Th}(I)$ je úplná teória vo výrokovom počte.

(b) Pre každú výrokovú formu $A \in \mathrm{VF}(P)$ nasledujúce podmienky sú ekvivalentné:
   (i) $I(A) = 1$
   (ii) $\mathrm{Th}(I) \vdash A$
   (iii) $\mathrm{Th}(I) \models A$

Teraz už môžeme dokázať pôvodnú formuláciu Vety o úplnosti. Uvádzame ju v podobe zahŕňajúcej zároveň Vetu o korektnosti.

3.8.7 Veta o úplnosti. *Nech $T \subseteq \mathrm{VF}(P)$ je teória. Potom pre každú výrokovú formu $B \in \mathrm{VF}(P)$ platí $T \models B$ práve vtedy, keď $T \vdash B$.*

Demonštrácia. Ak $T \vdash B$, tak $T \models B$ podľa Vety o korektnosti. Aby sme dokázali obrátenú implikáciu, pripusťme, že $T \models B$, jednako $T \nvdash B$. Podľa Dôsledku 3.7.2 o dôkaze sporom to znamená, že teória $T \cup \{\neg B\}$ je konzistentná. Potom podľa alternatívnej verzie Vety o úplnosti teória $T \cup \{\neg B\}$ má nejakú interpretáciu I. To znamená, že I je interpretácia teórie T taká, že $I(\neg B) = 1$, teda $I(B) = 0$. Ale podmienka $T \models B$ hovorí, že $J(B) = 1$ pre každú interpretáciu J teórie T; teda aj $I(B) = 1$. Tento spor dokazuje, že $T \vdash B$.

Konečne zaznamenajme ešte nasledujúci dôsledok Vety o úplnosti.

3.8.8 Veta o kompaktnosti. *Nech $T \subseteq \mathrm{VF}(P)$ je teória. Potom T má interpretáciu práve vtedy, keď každá konečná podteória T_0 teórie T má interpretáciu.*

Demonštrácia. Podľa Vety 3.8.7 o úplnosti T má interpretáciu práve vtedy, keď T je konzistentná. Podobne, každá konečná podteória $T_0 \subseteq T$ má interpretáciu práve vtedy, keď každá konečná podteória $T_0 \subseteq T$ je konzistentná. Takže si stačí uvedomiť, že T je konsistentná práve vtedy, keď každá jej konečná podteória je konzistentná. Očividne, ak T je konsistentná, tak to platí aj pre všetky jej podteórie (a nielen pre tie konečné). Obrátene, ak T je sporná, tak ľubovoľné dva dôkazy nejakej dvojice protirečiacich si výrokových foriem B, resp. $\neg B$ v T využívajú iba konečne mnoho špecifických axióm teórie T. Ak ich dáme dohromady, dostaneme konečnú podteóriu $T_0 \subseteq T$, ktorá je už sama sporná.

Vetu o kompaktnosti pre výrokový počet sme sformulovali a dokázali hlavne s cieľom pripraviť pôdu pre Vetu o kompaktnosti v predikátovom počte, ktorú uvedieme neskôr. Jednako výroková verzia Vety o kompaktnosti zďaleka nedosahuje význam jej predikátovej verzie ani neoplýva porovnateľnou hojnosťou dôsledkov.

3.9 Axiomatizácia výrokového počtu pomocou štyroch logických spojok

Kvôli úplnosti uvedieme ešte axiomatizáciu výrokového počtu pomocou všetkých štyroch obvyklých logických spojok $\neg$, $\wedge$, $\vee$ a $\Rightarrow$; zvyšnú logickú spojku $\Leftrightarrow$ zavádzame prostredníctvom logickej ekvivalencie

$$A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$$

Teda výraz vľavo slúži ako skratka za výraz vpravo. Príslušná axiomatizácia pozostáva z desiatich schém axióm. Ako jediné odvodzovacie pravidlo slúži opäť Modus Ponens.

3.9.1 Logické axiómy. (10 schém axióm)
Pre ľubovoľné výrokové formy A, B, C nasledujúce výrokové formy sú logické axiómy:

(LAx 1) $A \Rightarrow (B \Rightarrow A)$

(LAx 2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

(LAx 3) $(A \wedge B) \Rightarrow A$

(LAx 4) $(A \wedge B) \Rightarrow B$

(LAx 5) $A \Rightarrow (B \Rightarrow (A \wedge B))$

(LAx 6) $A \Rightarrow (A \vee B)$

(LAx 7) $B \Rightarrow (A \vee B)$

(LAx 8) $((A \Rightarrow C) \wedge (B \Rightarrow C)) \Rightarrow ((A \vee B) \Rightarrow C))$

(LAx 9) $((A \Rightarrow B) \wedge (A \Rightarrow \neg B)) \Rightarrow \neg A)$

(LAx 10) $A \vee \neg A$

3.9.2 Odvodzovacie pravidlo: Modus Ponens

(MP) $\dfrac{A,\ A \Rightarrow B}{B}$ *(z A a $A \Rightarrow B$ odvoď B)*

3.9.3 Úloha. Presvedčte sa, že všetky uvedené logické axiómy sú tautológie a objasnite ich intuitívny význam.

4 Logika prvého rádu

V porovnaní s výrokovým počtom v logike prvého rádu do istej miery oslabíme požiadavku abstrahovať od obsahu jednotlivých tvrdení a úsudkov a sústrediť sa len na ich formu. Konkrétne pripustíme, že tvrdenia a úsudky sa týkajú nejakých *objektov*, že tieto objekty majú nejaké *vlastnosti* alebo vstupujú do nejakých *vzťahov*, že niektoré objekty môžu byť explicitne zmienené svojimi *menami* a, konečne, že z daných objektov možno vytvárať nové objekty pomocou nejakých *operácií*. Hoci táto zmena zorného poľa dáva zmysel rovnako pre prirodzené jazyky ako aj pre jazyky vedeckých teórií, v tomto kurze zameriame svoju pozornosť výlučne na jazyky *matematických teórií*, kde je takýto prístup prirodzený a jeho plodnosť možno demonštrovať presvedčivým spôsobom. Na druhej strane, redukcia logickej štruktúry prirodzených jazykov ako aj jazykov väčšiny vedeckých teórií na ich fragment zapadajúci do rámca logiky prvého rádu by vyznela značne umelo.

Logika prvého rádu, nazývaná aj (úzky) *predikátový počet*, skúma štruktúru argumentov a dôkazov používaných v matematike, presnejšie v matematických teóriách popisujúcich triedy matematických štruktúr tvorených množinami objektov, vybavenými rôznymi finitárnymi (konečnomiestnymi) operáciami a reláciami, vymedzené prostredníctvom určitých axióm. Z toho dôvodu logika prvého rádu je matematickou logikou tak svojimi metódami ako aj svojím predmetom.

Logiku prvého rádu budeme budovať a prezentovať paralelne s našou predchádzajúcou výstavbou a výkladom výrokového počtu do tej miery, ako to len bude možné. V dôsledku toho by čitateľ mal jasne vidieť podobnosti ako aj rozdiely medzi týmito dvoma vetvami matematickej logiky.

4.1 Jazyky prvého rádu a štruktúry prvého rádu

Typická *matematická štruktúra* pozostáva z neprázdnej základnej množiny A nejakých objektov, vybavenej nejakými konečnomiestnymi operáciami, význačnými prvkami a konečnomiestnymi reláciami.

4.1.1 Príklad. Číselné systémy s operáciami sčítania $+$ a násobenia $\cdot$, význačnými prvkami 0 a 1 a (s výnimkou komplexných čísel) reláciou usporiadania $<$ tvoria matematické štruktúry bežne označované nasledujúcim spôsobom:

Prirodzené čísla: $(\mathbb{N};\, +, \cdot, 0, 1, <)$
Celé čísla: $(\mathbb{Z};\, +, \cdot, 0, 1, <)$
Racionálne čísla: $(\mathbb{Q};\, +, \cdot, 0, 1, <)$
Reálne čísla: $(\mathbb{R};\, +, \cdot, 0, 1, <)$
Komplexné čísla: $(\mathbb{C};\, +, \cdot, 0, 1)$

Jazyk prvého rádu $L = (F, C, R, \nu)$ je určený nejakými (možno i prázdnymi) množinami F funkcionálnych (operačných) symbolov, C konštantných symbolov a R relačných (predikátových) symbolov, spolu s *funkciou árnosti* (*signatúrou*) $\nu\colon F \cup R \to \mathbb{N}$, ktorá priradí každému symbolu $s \in F \cup R$ jeho *árnosť* (počet argumentov) $\nu(s) \geq 1$. Toto sú *špecifické symboly* jazyka L. Konštantné symboly niekedy považujeme za nulárne funkcionálne symboly, t. j. za prvky f množiny F také, že $\nu(f) = 0$ (v tom prípade množina C explicitne nefiguruje v opise jazyka L).

Všetky jazyky prvého rádu majú spoločné *logické symboly*:

- Objektové premenné (krátko len premenné): x, y, z, u, v, w, x_0, x_1, x_2, …, y', y'', …
- Logické spojky: $\neg$ (*nie*), $\wedge$ (*a*), $\vee$ (*alebo*), $\Rightarrow$ (*ak … tak* alebo *implikuje*), $\Leftrightarrow$ (*práve vtedy, keď*) (stačili by dve)
- Kvantifikátory: $\forall$ (*univerzálny kvantifikátor*), $\exists$ (*existenčný kvantifikátor*) (stačil by jeden)
- Znak rovnosti: $=$
- Pomocné symboly: (,) (*zátvorky*), , (*čiarka*) (dalo by sa zaobísť aj bez nich)

4.1.2 Poznámka. Na prvý pohľad by sa mohlo zdať, že od množín F, C, R by sme mali žiadať, aby boli nanajvýš spočítateľné, lebo možnosť, že by jazyk L obsahoval nespočítateľne mnoho špecifických symbolov, nedáva príliš zmysel. Takéto obmedzenie by nám však neprinieslo nijakú technickú výhodu. Čo je však dôležitejšie, ako uvidíme neskôr, napr. keď sa budeme zaoberať *diagramami* štruktúr, metódy a výsledky skúmania nespočítateľných jazykov majú aplikácie aj pre štruktúry spočítateľných jazykov prvého rádu.

Štruktúra prvého rádu, t. j. štruktúra nejakého jazyka prvého rádu $L = (F, C, R, \nu)$, stručne *L-štruktúra*, $\mathcal{A} = (A; I)$ pozostáva z neprázdnej množiny A, nazývanej *základná množina* alebo *nosič* štruktúry $\mathcal{A}$, a *interpretácie* I špecifických symbolov jazyka L v množine A:

- pre $f \in F$ také, že $\nu(f) = n$, $f^I\colon A^n \to A$
  (každý n-árny operačný symbol je interpretovaný ako n-árna operácia na množine A)
- pre $c \in C$, $c^I \in A$
  (každý konštantný symbol je interpretovaný ako nejaký význačný prvok množiny A)
- pre $r \in R$ také, že $\nu(r) = n$, $r^I \subseteq A^n$
  (každý n-árny relačný symbol je interpretovaný ako n-árna relácia na množine A)

Namiesto s^I často píšeme $s^{\mathcal{A}}$ alebo len s pre každý špecifický symbol s.

4.2 Termy a formuly

Termy jazyka prvého rádu L, stručne *L-termy*, sú zostavené z premenných, konštantných symbolov a funkcionálnych symbolov jazyka L. Množina $\mathrm{Term}(L)$ všetkých L-termov je najmenšia množina taká, že:

1° $x \in \mathrm{Term}(L)$ pre každú premennú x (každá premenná je term);

2° $c \in \mathrm{Term}(L)$ pre každé $c \in C$ (každý konštantný symbol je term);

3° ak $f \in F$, $\nu(f) = n$ a $t_1, \ldots, t_n \in \mathrm{Term}(L)$, tak $f(t_1, \ldots, t_n) \in \mathrm{Term}(L)$ (ak f je n-árny funkcionálny symbol a $t_1, \ldots, t_n$ sú termy, tak aj $f(t_1, \ldots, t_n)$ je term).

Toto je *rekurzívna definícia*. Termy v 1°, 2°, čiže premenné a konštantné symboly, sa nazývajú *atomické termy*. Aby sme dokázali, že nejaká množina L-termov obsahuje všetky L-termy, stačí overiť, že spĺňa všetky tri podmienky 1°, 2° a 3°.

Pre binárny operačný symbol f v 3° zvyčajne píšeme $t_1 f t_2$ namiesto $f(t_1, t_2)$.

Konštantné termy sú termy, ktoré neobsahujú žiadne premenné. Ak všetky premenné vyskytujúce sa v terme t sú obsiahnuté v zozname $x_1, \ldots, x_k$, píšeme $t(x_1, \ldots, x_k)$. Až na jednu výnimku: zápis t nutne neznamená, že t je konštantný term.

Ak je daná L-štruktúra $\mathcal{A} = (A; I)$ a term $t(x_1, \ldots, x_k)$, tak interpretáciou termu t v $\mathcal{A}$ je k-miestna operácia $t^I \colon A^k \to A$ definovaná pre ľubovoľnú k-ticu $(a_1, \ldots, a_k) \in A^k$ takto:

1° ak t je premenná x_i, kde $i \leq k$, tak $t^I(a_1, \ldots, a_k) = a_i$;

2° ak t je konštantný symbol $c \in C$, tak $t^I(a_1, \ldots, a_k) = c^I$;

3° ak t je tvaru $f(t_1, \ldots, t_n)$, kde $f \in F$, $\nu(f) = n$, a interpretácie t_j^I termov $t_1(x_1, \ldots, x_k)$, …, $t_n(x_1, \ldots, x_k)$ sú už definované, tak

$$t^I(a_1, \ldots, a_k) = f^I\big(t_1^I(a_1, \ldots, a_k), \ldots, t_n^I(a_1, \ldots, a_k)\big)$$

Špeciálne interpretáciou konštantného termu t je vždy nejaký prvok $t^I \in A$. Namiesto t^I často píšeme $t^{\mathcal{A}}$ alebo len t pre ľubovoľný term t.

Formuly jazyka prvého rádu L, stručne len L-formuly, sú zostavené z atomických formúl pomocou logických spojok a kvantifikátorov. *Atomické formuly* jazyka L sú výrazy tvaru $t_1 = t_2$, kde t_1, t_2 sú ľubovoľné L-termy, a $r(t_1, \ldots, t_n)$, kde $r \in R$ je relačný symbol, $\nu(r) = n$, a $t_1, \ldots, t_n$ sú ľubovoľné L-termy (namiesto $r(t_1, t_2)$ často píšeme $t_1\, r\, t_2$). Množina $\mathrm{Form}(L)$ všetkých L-formúl je najmenšia množina taká, že:

1° ak φ je atomická formula, tak $\varphi \in \mathrm{Form}(L)$ (každá atomická formula je formula);

2° ak $\varphi, \psi \in \mathrm{Form}(L)$, tak $\neg\varphi, (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \Rightarrow \psi), (\varphi \Leftrightarrow \psi) \in \mathrm{Form}(L)$ (ak φ, ψ sú L-formuly, tak nimi sú aj $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \Rightarrow \psi)$, $(\varphi \Leftrightarrow \psi)$);

3° ak $\varphi \in \mathrm{Form}(L)$ a x je premenná, tak $(\forall x)\varphi, (\exists x)\varphi \in \mathrm{Form}(L)$ (pre ľubovoľnú formulu φ a premennú x výrazy $(\forall x)\varphi$, $(\exists x)\varphi$ sú formuly).

Toto je opäť *rekurzívna definícia*. Ak chceme ukázať, že nejaká množina L-formúl obsahuje všetky L-formuly, stačí overiť že spĺňa všetky tri podmienky 1°, 2° a 3°.

Podobne ako vo výrokovom počte, aj teraz budeme vynechávať nepotrebné zátvorky. Na druhej strane, v záujme čitateľnosti občas použijeme aj zátvorky nevyžadované predchádzajúcou definíciou. Napríklad modifikované výrazy $\neg(\varphi)$, $(\varphi) \wedge (\psi)$ atď. môžu byť niekedy lepšie čitateľné ako „rigorózne“ formuly $\neg\varphi$, $\varphi \wedge \psi$ atď. Atomické formuly tvaru $t_1 = t_2$ sa nazývajú *identity*. Konjunkcia dvoch identít $(t_1 = t_2) \wedge (t_2 = t_3)$

sa často skracuje do tvaru $t_1 = t_2 = t_3$. Namiesto $\neg(t_1 = t_2)$ zvyčajne píšeme $t_1 \neq t_2$; $\neg(t_1\, r\, t_2)$ sa často skracuje na $t_1 \not r\, t_2$.

Po sebe idúce kvantifikácie s rovnakým kvantifikátorom $(\mathrm{Q}\, x_1) \dots (\mathrm{Q}\, x_n)$ budeme skracovať na tvar $(\mathrm{Q}\, x_1, \dots, x_n)$. Napríklad budeme písať $(\forall\, x_1, \dots, x_n)(\exists\, u, v)(\forall\, z)\varphi$ namiesto $(\forall\, x_1) \dots (\forall\, x_n)(\exists\, u)(\exists\, v)(\forall\, z)\varphi$.

Výskyt premennej x vo formule φ je jednoducho výskyt symbolu x v niektorej z atomických formúl, z ktorých je φ zostavená. Taký výskyt sa nazýva *viazaný*, ak spadá pod oblasť pôsobnosti nejakého kvantifikátora; inak sa nazýva *voľný*.

4.2.1 Príklad. Vo formule

$$(\forall\, x)(x + y = y + x) \wedge (\exists\, y)(\forall\, u)(x \leq y + z)$$

jazyka prvého rádu, ktorý obsahuje binárny operačný symbol $+$ a binárny predikátový symbol $\leq$, sú oba výskyty premennej x v atomickej formule $x + y = y + x$ viazané, zatiaľ čo jej výskyt v $x \leq y + z$ je voľný, oba výskyty premennej y v atomickej formule $x + y = y + x$ sú voľné, zatiaľ čo jej výskyt v $x \leq y + z$ je viazaný, výskyt premennej z v atomickej formule $x \leq y + z$ je voľný a konečne premenná u sa vo formule φ nevyskytuje.

Uzavreté formuly alebo *sentencie*, prípadne tiež *tvrdenia*, sú L-formuly, ktoré neobsahujú žiadne voľné premenné. Ak sa všetky premenné *voľne* sa vykytujúce vo formule φ nachádzajú v zozname $x_1, \dots, x_n$, píšeme $\varphi(x_1, \dots, x_n)$. Výnimka: ak napíšeme φ, nemusí to nutne znamenať, že φ je uzavretá formula.

Nasledujúca definícia *relácie spĺňania* pochádza od Alfreda Tarského. Splnenie L-formuly $\varphi(x_1, \dots, x_n)$ prvkami $a_1, \dots, a_n \in A$ nejakej L-štruktúry $\mathcal{A} = (A; I)$ sa značí $\mathcal{A} \vDash \varphi(a_1, \dots, a_n)$ a číta $\varphi(a_1, \dots, a_n)$ *je splnená* alebo *pravdivá* alebo *platí* v $\mathcal{A}$. Je definovaná rekurzívne:

- ak φ je $t_1 = t_2$, tak $\mathcal{A} \vDash \varphi(a_1, \dots, a_n)$ práve vtedy, keď $t_1^I(a_1, \dots, a_n) = t_2^I(a_1, \dots, a_n)$
- ak φ je $r(t_1, \dots, t_m)$, tak $\mathcal{A} \vDash \varphi(a_1, \dots, a_n)$ práve vtedy, keď $\big(t_1^I(a_1, \dots, a_n), \dots, t_m^I(a_1, \dots, a_n)\big) \in r^I$
- ak φ je $\neg\psi$, tak $\mathcal{A} \vDash \varphi(a_1, \dots, a_n)$ práve vtedy, keď nie je pravda, že $\mathcal{A} \vDash \psi(a_1, \dots, a_n)$
- ak φ je $\psi \wedge \chi$, tak $\mathcal{A} \vDash \varphi(a_1, \dots, a_n)$ práve vtedy, keď zároveň $\mathcal{A} \vDash \psi(a_1, \dots, a_n)$ a $\mathcal{A} \vDash \chi(a_1, \dots, a_n)$
- ak φ je $\psi \vee \chi$, tak $\mathcal{A} \vDash \varphi(a_1, \dots, a_n)$ práve vtedy, keď $\mathcal{A} \vDash \psi(a_1, \dots, a_n)$ alebo $\mathcal{A} \vDash \chi(a_1, \dots, a_n)$ (v nevylučovacom zmysle)
- ak φ je $\psi \Rightarrow \chi$, tak $\mathcal{A} \vDash \varphi(a_1, \dots, a_n)$ práve vtedy, keď z $\mathcal{A} \vDash \psi(a_1, \dots, a_n)$ vyplýva $\mathcal{A} \vDash \chi(a_1, \dots, a_n)$
- ak φ je $\psi \Leftrightarrow \chi$, tak $\mathcal{A} \vDash \varphi(a_1, \dots, a_n)$ práve vtedy, keď podmienky $\mathcal{A} \vDash \psi(a_1, \dots, a_n)$ a $\mathcal{A} \vDash \chi(a_1, \dots, a_n)$ sú ekvivalentné
- ak φ je $(\forall\, x)\psi$, tak $\mathcal{A} \vDash \varphi(a_1, \dots, a_n)$ práve vtedy, keď $\mathcal{A} \vDash \psi(a, a_1, \dots, a_n)$ pre každé $a \in A$
- ak φ je $(\exists\, x)\psi$, tak $\mathcal{A} \vDash \varphi(a_1, \dots, a_n)$ práve vtedy, keď $\mathcal{A} \vDash \psi(a, a_1, \dots, a_n)$ pre nejaké $a \in A$

Uvedenú definíciu možno prepísať do prehľadnejšej podoby, ktorá je zároveň ľahšia na zapamätanie, ak použijeme rovnaké symboly pre logické spojky, kvantifikátory a vzťah rovnosti tak v jazyku prvého rádu L, s ktorým pracujeme, ako aj v bežnej slovenčine (ktorá je súčasťou nášho metajazyka). Aby sa zabránilo nedorozumeniu, takýto prístup sa zvykne uvádzať slovným obratom „zneužitie označenia“. Čitateľ by si mal pozorne prejsť prepísanú verziu a identifikovať príslušnú úlohu každého jednotlivého výskytu logických symbolov v nej:

$$\begin{aligned}
\mathcal{A} \vDash (t_1 = t_2)(a_1, \ldots, a_n) &\Leftrightarrow \mathcal{A} \vDash t_1(a_1, \ldots, a_n) = t_2(a_1, \ldots, a_n) \\
\mathcal{A} \vDash r(t_1, \ldots, t_m)(a_1, \ldots, a_n) &\Leftrightarrow \mathcal{A} \vDash r(t_1(a_1, \ldots, a_n), \ldots, t_m(a_1, \ldots, a_n)) \\
\mathcal{A} \vDash \neg\varphi(a_1, \ldots, a_n) &\Leftrightarrow \neg(\mathcal{A} \vDash \varphi(a_1, \ldots, a_n)) \Leftrightarrow \mathcal{A} \nvDash \varphi(a_1, \ldots, a_n) \\
\mathcal{A} \vDash (\varphi \wedge \psi)(a_1, \ldots, a_n) &\Leftrightarrow \big(\mathcal{A} \vDash \varphi(a_1, \ldots, a_n) \wedge \mathcal{A} \vDash \psi(a_1, \ldots, a_n)\big) \\
\mathcal{A} \vDash (\varphi \vee \psi)(a_1, \ldots, a_n) &\Leftrightarrow \big(\mathcal{A} \vDash \varphi(a_1, \ldots, a_n) \vee \mathcal{A} \vDash \psi(a_1, \ldots, a_n)\big) \\
\mathcal{A} \vDash (\varphi \Rightarrow \psi)(a_1, \ldots, a_n) &\Leftrightarrow \big(\mathcal{A} \vDash \varphi(a_1, \ldots, a_n) \Rightarrow \mathcal{A} \vDash \psi(a_1, \ldots, a_n)\big) \\
\mathcal{A} \vDash (\varphi \Leftrightarrow \psi)(a_1, \ldots, a_n) &\Leftrightarrow \big(\mathcal{A} \vDash \varphi(a_1, \ldots, a_n) \Leftrightarrow \mathcal{A} \vDash \psi(a_1, \ldots, a_n)\big) \\
\mathcal{A} \vDash (\forall x)\varphi(x, a_1, \ldots, a_n) &\Leftrightarrow (\forall a \in A)\big(\mathcal{A} \vDash \varphi(a, a_1, \ldots, a_n)\big) \\
\mathcal{A} \vDash (\exists x)\varphi(x, a_1, \ldots, a_n) &\Leftrightarrow (\exists a \in A)\big(\mathcal{A} \vDash \varphi(a, a_1, \ldots, a_n)\big)
\end{aligned}$$

Pre $\varphi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ a $a_1, \ldots, a_n \in A$ píšeme $\mathcal{A} \vDash \varphi(a_1, \ldots, a_n, y_1, \ldots, y_m)$ práve vtedy, keď $\mathcal{A} \vDash \varphi(a_1, \ldots, a_n, b_1, \ldots, b_m)$ pre všetky $b_1, \ldots, b_m \in A$, t. j. práve vtedy, keď $\mathcal{A} \vDash (\forall y_1, \ldots, y_m)\varphi(a_1, \ldots, a_n, y_1, \ldots, y_m)$. Špeciálne $\mathcal{A} \vDash \varphi(x_1, \ldots, x_n)$ znamená, že $\mathcal{A} \vDash \varphi(a_1, \ldots, a_n)$ pre všetky prvky $a_1, \ldots, a_n \in A$, inak povedané, $\mathcal{A} \vDash (\forall x_1, \ldots, x_n)\varphi(x_1, \ldots, x_n)$. V dôsledku toho zápis $\mathcal{A} \vDash \varphi$ má jasný význam, aj keď formula φ nie je uzavretá.

4.3 Teórie prvého rádu a ich modely

Teóriu prvého rádu T, t. j. teóriu v nejakom jazyku prvého rádu L, reprezentujeme a zároveň stožňujeme s množinou jej *špecifických axióm* $T \subseteq \mathrm{Form}(L)$. Namiesto *teória prvého rádu* budeme odteraz väčšinou hovoriť len *teória*. Hovoríme, že L-štruktúra $\mathcal{A}$ *spĺňa* teóriu T alebo je *modelom* teórie T, ak $\mathcal{A}$ spĺňa všetky axiómy teórie T. V tom prípade píšeme $\mathcal{A} \vDash T$. To znamená, že

$$\mathcal{A} \vDash T \quad \text{práve vtedy, keď} \quad \mathcal{A} \vDash \varphi \text{ pre každé } \varphi \in T$$

Hovoríme, že formula ψ je *logickým* alebo *nevyhnutným dôsledkom* (axióm) teórie T, prípadne, že ψ *platí* alebo je *splnené* či *pravdivé* v T, ak ψ je splnené v každom modeli $\mathcal{A}$ teórie T. V tom prípade píšeme $T \vDash \psi$. Takže máme

$$T \vDash \psi \quad \text{práve vtedy, keď} \quad \mathcal{A} \vDash \psi \text{ pre každý model } \mathcal{A} \vDash T$$

Naším cieľom je zachytiť sémantický pojem pravdy alebo spĺňania či logického dôsledku prostredníctvom syntaktického pojmu *dokázateľnosti*. To bude náplňou nasledujúceho paragrafu. Kým však obrátime pozornosť k tejto otázke, je žiadúce, aby

sme sa aspoň letmo oboznámili s niektorými dôležitými teóriami prvého rádu a ich modelmi.

Teórie prvého rádu môžeme predbežne rozdeliť do nasledujúcich dvoch kategórií:

(a) Teórie prvého rádu popisujúce triedu rozmanitých štruktúr toho istého jazyka prvého rádu, vymedzenú nejakými spoločnými vlastnosťami formulovanými ako axiómy príslušnej teórie. Niektoré podtriedy triedy všetkých modelov tejto teórie možu byť popísané pomocou dodatočných axióm, prípadne tiež prostredníctvom podmienok, ktoré nie sú vyjadrené v onom jazyku prvého rádu. Z ďalej uvedených teórií do tejto kategórie spadajú *Teória grúp*, viaceré *Teórie okruhov* a *polí*, *vektorových priestorov, Teórie usporiadania, Boolových algebier* a *Teórie usporiadaných okruhov* a *polí*.

(b) Teórie prvého rádu kladúce si za cieľ popísať jedinú matematickú štruktúru „čo najúplnejším spôsobom“. Ako neskôr uvidíme, takéto ciele sú – až na isté triválne prípady – nedosiahnuteľné. Naším prvým príkladom tohto druhu bude *Peanova aritmetika*, usilujúca sa o úplný popis štuktúry prirodzených čísel so sčítaním a násobením. Druhý príklad zahŕňa *Zermelovu-Fraenkelovu teóriu množín* s axiómou výberu (v nie celkom presne načrtnutej podobe), ktorá by mala čo najvernejšie zachytiť univerzum množín.

4.3.1 Grupy. *Teória grúp* má niekoľko alternatívnych axiomatizácií v mierne odlišných jazykoch prvého rádu. *Grupa* je jednoducho model Teórie grúp.

(a) V jazyku prvého rádu s binárnym operačným symbolom $\cdot$ (násobenie), konštantným symbolom e (jednotka alebo neutrálny prvok) a unárnym operačným symbolom $^{-1}$ (operácia inverzného prvku) sú axiómami Teórie grúp nasledujúce identity

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$
$$x \cdot e = x = e \cdot x$$
$$x \cdot x^{-1} = e = x^{-1} \cdot x$$

vyjadrujúce asociatívnosť násobenia, úlohu e ako jednotkového prvku a fakt, že x^{-1} je inverzný prvok k x. Grupy sú potom štruktúry $\left(G;\, \cdot, e, {}^{-1}\right)$ spĺňajúce uvedené axiómy.

Grupa sa nazýva *komutatívna* alebo *abelovská*, ak spĺňa komutatívny zákon

$$x \cdot y = y \cdot x$$

Teória grúp, najmä v abelovskom prípade, sa niekedy zvykne formulovať v jazyku s binárnym operačným symbolom $+$ (sčítanie), konštantným symbolom 0 (nula) a unárnym operačným symbolom $-$ (mínus, inverzný prvok $-x$ sa nazýva opačný prvok k x).

(b) Ak z jazyka Teórie grúp vynecháme unárny operačný symbol $^{-1}$, tak poslednú axiómu vyjadrujúcu existenciu inverzných prvkov musíme formulovať trochu komplikovanejším spôsobom

$$(\forall x)(\exists y)(x \cdot y = e = y \cdot x)$$

Grupy potom chápeme ako štruktúry $(G;\, \cdot, e)$ spĺňajúce príslušné tri axiómy.

(c) V jazyku obsahujúcom iba symbol násobenia je potrebné zlúčiť axiómy vyjadrujúce existenciu jednotkového prvku a inverzných prvkov do jedinej, zato však

zložitejšej axiómy

$$(\exists\, u)(\forall\, x)\big(x \cdot u = x = u \cdot x \wedge (\exists\, y)(x \cdot y = u = y \cdot x)\big)$$

Inú možnosť predstavuje axióma

$$(\forall\, x)(\exists\, y)(\forall\, z)\big(z \cdot (x \cdot y) = z = (y \cdot x) \cdot z\big)$$

Grupa je potom štruktúra $(G; \cdot)$ spĺňajúca asociatívny zákon a jednu (teda obe) z dvoch posledných axióm.

Je jasné, že z grupy $\big(G; \cdot, e, {}^{-1}\big)$ v zmysle (a) možno dostať grupu v zmysle (b) alebo (c) vynechaním interpretácií nadbytočných symbolov. Obrátene, jazyk Teórie grúp v zmysle (c) možno rozšíriť o chýbajúce symboly a definovať jednotkový prvok a operáciu inverzného prvku formulami

$$\begin{aligned} u = e \;&\Leftrightarrow\; (\forall\, x)(x \cdot u = x = u \cdot x) \\ y = x^{-1} \;&\Leftrightarrow\; x \cdot y = e = y \cdot x \end{aligned}$$

Potom grupa $(G; \cdot)$ v zmysle (c) sa stane grupou v zmysle (b) alebo (a).

Príkladmi komutatívnych grúp (v jazyku s jedinou binárnou operáciou) sú aditívne grupy $(\mathbb{Z}; +)$ celých čísel, $(\mathbb{Z}_n; +)$ zvyškov modulo $n \geq 2$, racionálnych čísel $(\mathbb{Q}; +)$ atď. Príklady nekomutatívnych grúp poskytujú štruktúry $(S(X); \circ)$ všetkých bijektívnych zobrazení (permutácií) ľubovoľnej množiny X s viac ako dvoma prvkami do seba s operáciou kompozície, alebo štruktúry $(\mathrm{GL}(n, \mathbb{R}); \cdot)$ všetkých invertibilných reálnych matíc rozmeru $n \times n$ pre $n \geq 2$ s operáciou násobenia matíc.

4.3.2 Okruhy a polia. (a) *Teória okruhov* je formulovaná v jazyku s dvoma binárnymi operačnými symbolmi $+$ (sčítanie), $\cdot$ (násobenie) a konštantným symbolom 0 (nula). Okruh je potom štruktúra $(A; +, \cdot, 0)$ spĺňajúca axiómy Teórie okruhov. Tie vyjadrujú podmienku, že $(A; +, 0)$ je abelovská grupa, asociatívny zákon pre násobenie a dva distributívne zákony

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

obvykle zapisované v jednoduchšej podobe $x(y+z) = xy + xz$ a $(x+y)z = xz + yz$. Modely teórie okruhov sa nazývajú *okruhy*.

Okruh sa nazýva *komutatívny*, ak spĺňa komutatívny zákon pre násobenie $x \cdot y = y \cdot x$. Komutatívny okruh sa nazýva *obor integrity*, ak vyhovuje axióme

$$xy = 0 \;\Rightarrow\; (x = 0 \vee y = 0)$$

(b) *Teória okruhov s jednotkou* alebo *Teória unitárnych okruhov* je formulovaná v jazyku teórie okruhov rozšírenom o nový konštantný symbol 1, označujúci jednotku pre násobenie. Jej axiómy sú tvorené axiómami Teórie okruhov a identitami $x \cdot 1 = x = 1 \cdot x$.

(c) *Teóriu polí* dostaneme z Teórie komutatívnych okruhov s jednotkou pridaním axiómy $0 \neq 1$ a axiómy

$$(\forall\, x)(x \neq 0 \;\Rightarrow\; (\exists\, y)(x \cdot y = 1))$$

požadujúcej existenciu multiplikatívnych inverzných prvkov ku všetkým nenulovým prvkom. *Pole* je jednoducho model Teórie polí.

(d) *Teória okruhov s delením* sa dostane z Teórie unitárnych okruhov rozšírením o podmienku $0 \neq 1$ a axiómu inverzných prvkov

$$(\forall\, x)(x \neq 0 \;\Rightarrow\; (\exists\, y)(x \cdot y = 1 = y \cdot x))$$

Okruh s delením, prípadne *teleso* je jednoducho model tejto teórie.

Párne celé číslo tvoria komutatívny okruh $(2\mathbb{Z};\, +, \cdot, 0)$ bez jednotky. Štruktúra celých čísel $(\mathbb{Z};\, +, \cdot, 0, 1)$ a štruktúry $(\mathbb{Z}_n;\, +, \cdot, 0, 1)$ zvyškov modulo $n \geq 2$ tvoria komutatívne okruhy s jednotkou. Príklady nekomutatívnych okruhov s jednotkou poskytujú štruktúry $\big(\mathbb{R}^{n\times n};\, +, \cdot, 0, I\big)$ všetkých reálnych matíc rozmeru $n \times n$, kde $n \geq 2$, s operáciami sčítania a násobenia matíc, nulovou maticou 0 a jednotkovou maticou I. Príkladmi polí sú štruktúry $(\mathbb{Q};\, +, \cdot, 0, 1)$, $(\mathbb{R};\, +, \cdot, 0, 1)$, $(\mathbb{C};\, +, \cdot, 0, 1)$ všetkých racionálnych, reálnych, resp. komplexných čísel, ako aj štrukúry $(\mathbb{Z}_p;\, +, \cdot, 0, 1)$ zvyškov modulo akékoľvek prvočíslo p. Zrejme každé pole je obor inegrity, avšak celé čísla $(\mathbb{Z};\, +, \cdot, 0, 1)$ tvoria obor integrity, ktorý nie je poľom. Príkladom nekomutatívneho okruhu s delením, t. j. okruhu s delením, ktorý nie je poľom, sú *kvaternióny* $(\mathbb{H};\, +, \cdot, 0, 1)$. Kvaternióny predstavujú štvorrozmernú analógiu komplexných čísel; sú to čísla tvaru $q_0 + q_1\,\mathrm{i} + q_1\,\mathrm{j} + q_3\,\mathrm{k}$, kde $q_0, q_1, q_2, q_3 \in \mathbb{R}$ a i, j, k sú tri imaginárne jednotky spĺňajúce $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{i}\,\mathrm{j}\,\mathrm{k} = -1$. Rovnosť kvaterniónov a ich sčítanie sú definované po zložkách, zatiaľ čo ich násobenie je definované jediným možným spôsobom rozširujúcim uvedené relácie medzi generátormi i, j, k, vynúteným axiómami unitárnych okruhov.

(e) Pole $(F;\, +, \cdot, 0, 1)$ sa nazýva *algebraicky uzavreté*, ak spĺňa nekonečný zoznam axióm

$$(\forall\, u_1, \ldots, u_n)(\exists\, x)\big(x^n + u_1 x^{n-1} + \ldots + u_{n-1}x + u_n = 0\big)$$

požadujúci existenciu koreňov všetkých polynómov akéhokoľvek stupňa $n \geq 2$ s koeficientmi z F. Pole $(\mathbb{C};\, +, \cdot, 0, 1)$ všetkých komplexných čísel a pole $(\mathbb{A};\, +, \cdot, 0, 1)$ všetkých *algebraických čísel* (t. j. koreňov polynómov s racionálnymi koeficientmi) sú príkladmi algebraicky uzavretých polí.

(f) Pole $(F;\, +, \cdot, 0, 1)$ sa nazýva *formálne reálne*, ak spĺňa nekonečný zoznam axióm

$$x_1^2 + \cdots + x_n^2 = 0 \;\Rightarrow\; x_1 = \ldots = x_n = 0$$

pre každé kladné $n \in \mathbb{N}$, požadujúci, aby súčet štvorcov nenulových prvkov nebol nikdy 0. *Teória reálne uzavretých polí* je rozšírením *Teórie formálne reálnych polí* o axiómu

$$(\forall\, x)(\exists\, y)\big(y^2 = x \;\vee\; y^2 = -x\big)$$

postulujúcu existenciu druhej odmocniny z x alebo z $-x$ pre každé x, ako aj o nekonečný zoznam axióm

$$(\forall\, u_1, \ldots, u_n)(\exists\, x)\big(x^n + u_1 x^{n-1} + \ldots + u_{n-1}x + u_n = 0\big)$$

zaručujúci existenciu aspoň jedného koreňa pre každý polynóm akéhokoľvek *nepárneho* stupňa $n \geq 3$ s koeficientmi z F. Pole $(\mathbb{R};\, +, \cdot, 0, 1)$ všetkých reálnych čísel a pole

$(\mathbb{R}\cap\mathbb{A};\,+,\cdot,0,1)$ všetkých reálnych algebraických čísel sú príkladmi reálne uzavretých polí. Pole $(\mathbb{Q};\,+,\cdot,0,1)$ všetkých racionálnych čísel je formálne reálne, ale nie je reálne uzavreté.

Nasledujúci, pomerne známy príklad stojí za zmienku, lebo ukazuje, že i samotné množiny funkcionálnych alebo relačných symbolov jazyka prvého rádu môžu niesť vlastnú prvorádovú štruktúru.

4.3.3 Vektorové priestory nad daným poľom. Pre každé pevne zvolené pole $(F;\,+,\cdot,0,1)$ zavádzame jazyk prvého rádu $L(F)$ s konštantným symbolom $\mathbf{0}$, s binárnym operačným symbolom $+$ a množinou F unárnych operačných symbolov (množina relačných symbolov je prázdna). Typickú štruktúru jazyka $L(F)$ označujeme $\mathcal{V} = (V; F, +, \mathbf{0})$; prvky množiny V nazývame *vektory*. Prvky $f \in F$ v úlohe unárnych operačných symbolov nazývame *skaláry*; namiesto $f(x)$ zvykneme písať len fx a tomuto výsledku hovoríme *skalárny násobok* vektora x skalárom f. *Vektorový priestor* nad poľom F je štruktúra $\mathcal{V} = (V; F, +, \mathbf{0})$ jazyka $L(F)$ spĺňajúca axiómy vyjadrujúce fakt, že $(V; +, \mathbf{0})$ je abelovská grupa, ako aj axiómy

$$\begin{aligned} 1x &= x \\ f(x+y) &= fx + fy \\ (fg)x &= f(gx) \\ (f+g)x &= fx + gx \end{aligned}$$

pre ľubovoľné skaláry $f, g \in F$. Čitateľ by si mal uvedomiť, že posledné tri rovnosti sú vlastne *schémy axióm*, a nie jednotlivé axiómy.

4.3.4 Teórie usporiadania. *Teória čiastočného usporiadania* sa formuluje alternatívne v jazyku prvého rádu s jediným binárnym relačným symbolom $<$ (ostré čiastočné usporiadanie), resp. $\leq$ (neostré čiastočné usporiadanie). „Ostrá“ verzia je daná axiómami

$$\neg(x < x) \qquad \neg(x < y \wedge y < x) \qquad (x < y \wedge y < z) \Rightarrow x < z$$

„Neostrá“ (a častejšie používaná) verzia má axiómy

$$x \leq x \qquad (x \leq y \wedge y \leq x) \Rightarrow x = y \qquad (x \leq y \wedge y \leq z) \Rightarrow x \leq z$$

Čiastočne usporiadaná množina (*poset*) je jednoducho model $(P; <)$ alebo $(P; \leq)$ príslušnej verzie tejto teórie.

Očividne, z posetu $(P; <)$ dostaneme poset $(P; \leq)$ definíciou neostrého čiastočného usporiadania

$$x \leq y \Leftrightarrow x < y \vee x = y$$

Obrátene, z posetu $(P; \leq)$ môžeme vyrobiť poset $(P; <)$ definíciou ostrého čiastočného usporiadania

$$x < y \Leftrightarrow x \leq y \wedge x \neq y$$

Očákavame, že čitateľ bude schopný kedykoľvek prepínať medzi oboma verziami.

Teória usporiadaných množín, niekedy nazývaná aj *Teóriou lineárneho usporiadania*, alebo tiež *Teóriou totálneho usporiadania*vznikne pridaním *axiómy trichotómie*

$$x < y \vee x = y \vee y < x$$

resp. *axiómy dichotómie*

$$x \leq y \vee y \leq x$$

k príslušnej verzii Teórie čiastočného usporiadania.

4.3.5 Booleove algebry. Jazyk *Teórie Boolových algebier* má dva binárne operačné symboly $\wedge$ (priesek), $\vee$ (spojenie), jeden unárny operačný symbol $'$ (doplnok) a dva konštantné symboly 0 a 1. Takéto označenie porušuje implicitnú dohodu, že špecifické symboly akéhokoľvek jazyka prvého rádu sú odlišné od jeho logických symbolov. Nakoľko však všetky axiómy Teórie Boolových algebier sú identity a neobsahujú žiadne logické spojky, nijaké nedorozumnie z toho nehrozí. Na druhej strane toto označenie poukazuje na známu súvislosť medzi Boolovými algebrami a a výrokovým počtom. *Boolova algebra* $\mathcal{B} = (B; \wedge, \vee, ', 0, 1)$ je jednoducho model teórie s nasledujúcimi axiómami:

$x \wedge y = y \wedge x$	$x \vee y = y \vee x$	(komutatívne zákony)
$x \wedge (y \wedge z) = (x \wedge y) \wedge z$	$x \vee (y \vee z) = (x \vee y) \vee z$	(asociatívne zákony)
$x \wedge x = x$	$x \vee x = x$	(zákony idempotencie)
$x \wedge (x \vee y) = x$	$x \vee (x \wedge y) = x$	(absorbčné zákony)
$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$	$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$	(distributívne zákony)
$(x \wedge y)' = x' \vee y'$	$(x \vee y)' = x' \wedge y'$	(De Morganove zákony)
$x \wedge 0 = 0$	$x \vee 0 = x$	(zákony nuly)
$x \wedge 1 = x$	$x \vee 1 = 1$	(zákony jednotky)
$x \wedge x' = 0$	$x \vee x' = 1$	(zákony doplnku)

Tento zoznam axióm je redundantný: niektoré jeho položky sa dajú odvodiť ako dôsledky ostatných. Na ľubovoľnej Boleovej algebre možno zaviesť čiastočné usporiadanie pomocou ktorejkoľvek z nasledujúcich dvoch ekvivalentných podmienok:

$$x \leq y \Leftrightarrow x = x \wedge y \Leftrightarrow x \vee y = y$$

Potom 0 je najmenší a 1 najväčší prvok vzhľadom na toto čiastočné usporiadanie v $\mathcal{B}$.

Typickými príkladmi Boolových algebier sú potenčné množiny ľubovoľných množín. Presnejšie, pre každú množinu I jej potenčná množina $\mathcal{P}(I) = \{X \colon X \subseteq I\}$ s operáciami množinového prieniku, zjednotenia a doplnku vzhľadom na množinu I, s prázdnou množinou $\emptyset$ v úlohe nuly a množinou I v úlohe jednotky tvorí Boolovu algebru $(\mathcal{P}(I); \cap, \cup, ', \emptyset, I)$. Čiastočné usporiadanie $X \leq Y$ na $\mathcal{P}(I)$ splýva s množinovou inklúziou $X \subseteq Y$.

Iný príklad Boolovej algebry možno dostať z množiny $\mathrm{VF}(P)$ všetkých výrokových foriem nad akoukoľvek množinou výrokových premenných $P \neq \emptyset$, ak vzťah rovnosti interpretujeme ako vzťah logickej ekvivalencie $A \equiv B$, s logickými spojkami $\wedge$, $\vee$ a $\neg$ v úlohe boolovských operácií prieseku, spojenia a doplnku, a s hocakou tautológiou v úlohe 1 a hocakou kontradikciou v úlohe 0.

4.3.6 Úloha. (a) Ukážte, že obe podmienky definujúce vzťah čiastočného usporiadania $\leq$ na Boolových algebrách sú naozaj ekvivalentné, a že takto definovaný vzťah $\leq$ je naozaj (neostrým) čiastočným usporiadaním.

(b) Ukážte, že priesek $x \wedge y$ je infimum a spojenie $x \vee y$ je supremum množiny $\{x, y\}$ vzhľadom na čiastočné usporiadanaie $\leq$. To znamená, že pre ľubovoľné z platí $z \leq x$ a $z \leq y$ práve vtedy, keď $z \leq x \wedge y$, a podobne $x \leq z$ a $y \leq z$ práve vtedy, keď $x \vee y \leq z$.

(c) Dokážte *zákon dvojitého doplnku* $x'' = x$ ako aj identity $0' = 1$, $1' = 0$ z axióm Boolových algebier.

4.3.7 Usporiadané okruhy a polia. *Teóriu usporiadaných okruhov* dostaneme rozšírením jazyka Teórie okruhov o binárny relačný symbol $<$ a rozšírením zoznamu jej axióm o axiómy (totálneho) ostrého usporiadania a ďalej o axiómy

$$x < y \;\Rightarrow\; x + z < y + z$$
$$(x < y \;\wedge\; 0 < z) \;\Rightarrow\; (xz < yz \;\wedge\; zx < zy)$$

vyjadrujúce fakt, že operácie pripočítania ľubovoľného prvku z ako aj násobenia ľubovoľným kladným prvkom z sú rastúce.

Rovnaký postup možno aplikovať na Teóriu okruhov s jednotkou, Teóriu komutatívnych okruhov, Teóriu polí atď., čím získame *Teóriu usporiadaných okruhov s jednotkou*, *Teóriu usporiadaných komutatívnych okruhov*, *Teóriu usporiadaných polí* atď. Celé čísla $(\mathbb{Z}; +, \cdot, 0, 1, <)$ sú reprezentatívnym (a minimálnym) príkladom usporiadaného komutatívneho okruhu s jednotkou. Racionálne čísla $(\mathbb{Q}; +, \cdot, 0, 1, <)$ a reálne čísla $(\mathbb{R}; +, \cdot, 0, 1, <)$ tvoria usporiadané polia. Možno dokázať, že ani pole komplexných čísel $(\mathbb{C}; +, \cdot, 0, 1)$ ani žiadne konečné pole, napr. žiadne z polí $(\mathbb{Z}_p; +, \cdot, 0, 1)$ zvyškov modulo akékoľvek prvočíslo p, nemožno uporiadať reláciou $<$ tak, aby tvorili usporiadané pole.

Usporiadané pole $(F; +, \cdot, 0, 1, <)$ sa nazýva *reálne uzavreté*, ak je to formálne reálne pole spĺňajúce podmienku

$$x \geq 0 \;\Rightarrow\; (\exists\, z)\big(x = z^2\big)$$

a nekonečný zoznam podmienok požadujúcich, aby každý polynóm *nepárneho* stupňa $n \geq 3$ s koeficientmi z F mal v F aspoň jeden koreň, podobne ako v Teórii (neusporiadaných) reálne uzavretých polí. *Teória usporiadaných reálne uzavretých polí* je rozšírením *Teórie usporiadaných polí* o tieto axiómy. Jednoducho možno overiť, že z každého reálne uzavretého poľa $(F; +, \cdot, 0, 1)$ možno získať usporiadané pole $(F; +, \cdot, 0, 1, <)$ definíciou (neostrého) usporiadania podmienkou

$$x \leq y \;\Leftrightarrow\; (\exists\, z)\big(y = x + z^2\big)$$

Obrátene, pre každé usporiadané reálne uzavreté pole $(F; +, \cdot, 0, 1, <)$ je jeho redukt získaný vynechaním relácie usporiadania $<$ reálne uzavretým poľom $(F; +, \cdot, 0, 1)$.

4.3.8 Peanova aritmetika. *Peanova aritmetika* PA je najbežnejšou teóriou prvého rádu popisujúcou štruktúru prirodzených čísel. V logických textoch sa zvyčajne formuluje v jazyku prvého rádu s unárnym operačným symbolom S (operácia nasledovníka, t. j. pripočítania 1), dvomi binárnymi operáciami sčítania $+$ a násobenia $\cdot$ a konštantným symbolom 0. Pre nás je však vhodnejšie nahradiť symbol nasledovníka S konštantným symbolom 1; takto bude naša formulácia používať dôverne známy jazyk Teórie unitárnych okruhov (operáciu nasledovníka možno potom definovať ako $S(x) = x + 1$).

Axiómy teórie PA možno rozdeliť do štyroch skupín. Prvá skupina pozostáva z troch axióm pre operáciu nasledovníka (ľavý stĺpec), druhá skupina je vlastne rekurzívnou definíciou sčítania pomocu nasledovníka (stredný stĺpec) a tretia skupina je rekurzívnou definíciou násobenia pomocou sčítania (pravý stĺpec):

$$\begin{array}{lll} 0 + 1 = 1 & x + 0 = x & x \cdot 0 = 0 \\ 0 \neq x + 1 & x + (y + 1) = (x + y) + 1 & x \cdot (y + 1) = (x \cdot y) + x \\ x + 1 = y + 1 \;\Rightarrow\; x = y & & \end{array}$$

Štvrtá skupina pozostáva z nekonečne mnohých axióm zachytených v *Schéme indukcie*

$$\big(\varphi(0, \vec{u}) \;\wedge\; (\forall\, x)(\varphi(x, \vec{u}) \;\Rightarrow\; \varphi(x + 1, \vec{u}))\big) \;\Rightarrow\; (\forall\, x)\varphi(x, \vec{u})$$

kde $\varphi(x, u_1, \ldots, u_n)$ je ľubovoľná formula jazyka teórie PA, skrátená do podoby $\varphi(x, \vec{u})$.

Jazyk PA býva obvykle rozšírený o symbol usporiadania $\leq$ definovaný vzťahom

$$x \leq y \;\Leftrightarrow\; (\exists\, z)(y = x + z)$$

a z axióm PA vyplýva, že je to (neostré) lineárne usporiadanie s najmenším prvkom 0. Schému indukcie potom možno ekvivalentne vyjadriť v tvare *Princípu dobrého usporiadania*

$$(\exists\, x)\psi(x, \vec{u}) \;\Rightarrow\; (\exists\, x)\big(\psi(x, \vec{u}) \wedge (\forall\, y)(\psi(y, \vec{u}) \;\Rightarrow\; x \leq y)\big)$$

pre ľubovoľnú formulu $\psi(x, \vec{u})$ v jazyku PA. Neformálne tento princíp vyjadruje podmienku, že každá neprázdna množina prirodzených čísel tvaru $\{x\colon \psi(x, \vec{u})\}$ má najmenší prvok.

„Obvyklé“ prirodzené čísla tvoria takzvaný *štandardný model* $(\mathbb{N}; +, \cdot, 0, 1)$ Peanovej aritmetiky. Každý prvok $n \in \mathbb{N}$ je interpretáciou nejakého konštantného termu jazyka PA. Kanonické reprezentácie jednotlivých prirodzených čísel možno definovať rekurzívne:

1° Prirodzené číslo 0 splýva s konštantným symbolom 0.

2° Ak prirodzené číslo n splýva s konštantným termom t, tak prirodzené číslo $n+1$ splýva s konštantným termom $t + 1$.

„Zneužijúc označenie“ môžeme písať $0 = 0$, $1 = 0 + 1$, $2 = (0 + 1) + 1$, $3 = ((0 + 1) + 1) + 1$, $\ldots$, $n = (\ldots((0+1)+1)\cdots+1)+1$ (s n výskytmi symbolu 1) atď. Prirodzené číslo n je tak reprezentované konštantným termom, ktorý dostaneme n-tou iteráciou operácie nasledovníka aplikovanou na konštantný symbol 0.

Neskôr uvidíme, že PA má aj neštandardné modely.

4.3.9 Teória množín. Väčšina verzií *Teórie množín* je formulovaných v jazyku prvého rádu s jediným binárnym relačným symbolom $\in$ označujúcim vzťah náležania. Formula $x \in X$ znamená, že x *je prvkom (elementom)* X alebo x *patrí (náleží) do množiny* X. Spoločné jadro týchto verzií je tvorené nasledujúcimi štyrmi axiómami:

$$X = Y \;\Leftrightarrow\; (\forall z)(z \in X \;\Leftrightarrow\; z \in Y)$$
$$(\forall x, y)(\exists Z)(\forall z)(z \in Z \;\Leftrightarrow\; (z = x \vee z = y))$$
$$(\forall X)(\exists U)(\forall u)(u \in U \;\Leftrightarrow\; (\exists x \in X)(u \in x))$$
$$(\forall X)(\exists Y)(\forall y)(y \in Y \;\Leftrightarrow\; (\forall x)(x \in y \;\Rightarrow\; x \in X))$$

nazývanými *Axióma extenzionality*, *Axióma dvojice*, *Axióma zjednotenia* a *Axióma potenčnej množiny*, a nasledujúcim nekonečným zoznamom axióm

$$(\forall X)(\exists Y)(\forall x)\big(x \in Y \;\Leftrightarrow\; (x \in X \wedge \varphi(x, \vec{u}))\big)$$

pre ľubovoľnú množinovú formulu $\varphi(x, u_1, \ldots, u_n)$, nazývaným *Schémou vydelenia*.

Axióma extenzionality hovorí, že množiny X a Y sa rovnajú práve vtedy, keď obsahujú rovnaké prvky. Axióma dvojice postuluje existenciu množiny

$$Z = \{x, y\} = \{z \colon z = x \vee z = y\}$$

pre ľubovoľnú dvojicu prvkov x, y. Axióma zjednotenia zaručuje existenciu zjednotenia

$$U = \bigcup X = \{u \colon (\exists x \in X)(u \in x)\}$$

všetkých množín x z danej množiny X. Axióma potenčnej množiny postuluje existenciu potenčnej množiny (teda množiny všetkých podmnožín)

$$Y = \mathcal{P}(X) = \{y \colon y \subseteq X\} = \{y \colon (\forall x)(x \in y \;\Rightarrow\; x \in X)\}$$

ľubovoľnej množiny X. Konečne, Schéma vydelenia zaručuje možnosť vyčleniť akúkoľvek podmnožinu tvaru

$$Y = \{x \in X \colon \varphi(x, \vec{u})\} = \{x \colon x \in X \wedge \varphi(x, \vec{u})\}$$

z danej množiny X pomocou množinovej formuly $\varphi(x, u_1, \ldots, u_n)$.

Zermelova-Fraenkelova teória množín ZF vznikne rozšírením uvedeného zoznamu o *Axiómu regularity*, *Axiómu nekonečna* a *Schému nahradenia*. *Zermelova-Fraenkelova teória množín s axiómou výberu* ZFC, ktorá je najrozšírenejšou a najviac používanou verziou Teórie množín v modernej matematike, vznikne zo ZF pridaním *Axiómy výberu* (AC). Aby sme udržali náš text na elementárnej úrovni, obmedzíme sa na neformálne formulácie týchto vyšších axióm Teórie množín. Axióma regularity zabezpečuje, že každá neprázdna množina množín obsahuje ako svoj prvok množinu s ňou disjunktnú. Axióma nekonečna postuluje existenciu nekonečnej množiny a v dôsledku toho umožňuje dokázať existenciu množiny všetkých prirodzených čísel. Schéma nahradenia zovšeobecňuje Schému vydelenia tým, že dovoľuje tvoriť množiny nielen vyčleňovaním z danej množiny, ale aj ako isté obrazy podmnožín danej množiny definované pomocou množinových formúl. Konečne Axióma výberu zaručuje, že pre každú množinu X neprázdnych po dvoch disjunktných množín existuje množina, ktorá z každej z množín $x \in X$ obsahuje práve po jednom prvku.

4.4 Axiomatizácia logiky prvého rádu a veta o korektnosti

Podobne ako vo výrokovom počte aj tentokrát uprednostníme krátku a stručnú axiomatizáciu logiky prvého rádu. Preto budeme postupovať tak, ako keby množina $\mathrm{Form}(L)$ všetkých formúl akéhokoľvek jazyka prvého rádu L bola vybudovaná z atomických formúl výlučne pomocou logických spojok $\neg$ a $\Rightarrow$ a univerzálneho kvantifikátora $\forall$. Zápisom $\varphi \approx \psi$ vyjadrujeme to, že znaky φ a ψ označujú tú istú formulu. Podobne ako symboly φ, ψ, χ, L atď., ani symbol $\approx$ nepatrí do nášho jazyka prvého rádu. Napospol ide o symboly *metajazyka*, pomocou ktorého opisujeme predikátový počet.

Zostávajúce logické spojky a existenčný kvantifikátor možno zaviesť ako skratky

$$\begin{aligned}(\varphi \wedge \psi) &\approx \neg(\varphi \Rightarrow \neg\psi),\\ (\varphi \vee \psi) &\approx (\neg\varphi \Rightarrow \psi),\\ (\varphi \Leftrightarrow \psi) &\approx (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi),\\ (\exists\, x)\varphi &\approx \neg\big((\forall\, x)\neg\varphi\big).\end{aligned}$$

Logické axiómy predikátového počtu sú rozdelené do troch skupín: *axiómy výrokového počtu*, *axiómy kvantifikátorov* a *axiómy rovnosti*.

4.4.1 Axiómy výrokového počtu. (4 schémy axióm)
Pre ľubovoľné formuly φ, ψ, χ nasledujúce formuly sú axiómy:

(PrAx 1) $\varphi \Rightarrow (\psi \Rightarrow \varphi)$
(PrAx 2) $(\varphi \Rightarrow (\psi \Rightarrow \chi)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \chi))$
(PrAx 3) $(\varphi \Rightarrow \psi) \Rightarrow ((\varphi \Rightarrow \neg\psi) \Rightarrow \neg\varphi)$
(PrAx 4) $\neg\neg\varphi \Rightarrow \varphi$

Ak φ je formula a t je term, tak $\varphi(t/x)$ označuje formulu získanú *substitúciou* termu t za premennú x do formuly φ. To znamená, že každý *voľný* výskyt premennej x vo formule φ nahradíme termom t. Podobne zavádzame viacnásobné substitúcie $\varphi(t_1/x_1, \ldots, t_n/x_n)$. Keď nehrozí nedorozumenie, píšeme len $\varphi(t)$, resp. $\varphi(t_1, \ldots, t_n)$.

Substitúcia t za x do φ je *prípustná*, ak sa po nej žiadna z premenných termu t neocitne v oblasti pôsobnosti nejakého kvantifikátora. Neformálne to znamená, že „$\varphi(t/x)$ vypovedá o t to isté ako φ vypovedá o x“.

4.4.2 Príklad. V rámci celých čísel formula $\varphi(x) \approx (\exists\, y)(x = y + y)$ hovorí, že x je párne číslo. Ak t je term $u + x$, tak $\varphi(t/x)$ je formula $(\exists\, y)(u + x = y + y)$, ktorá hovorí, že $u + x$ je párne; toto je prípustná substitúcia. Ak t je term y, tak $\varphi(t/x)$ je uzavretá formula $(\exists\, y)(y = y + y)$ vyjadrujúca (pravdivý) fakt, že rovnica $y = y + y$ má riešenie; toto je neprípustná substitúcia.

4.4.3 Axiómy kvantifikátorov. (2 schémy axióm)
Pre ľubovoľné formuly φ, ψ a term t nasledujúce formuly sú axiómy:

(QAx 1) $(\forall\, x)(\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow (\forall\, x)\psi)$ (ak premenná x nemá voľný výskyt vo φ)
(QAx 2) $(\forall\, x)\varphi \Rightarrow \varphi(t/x)$ (ak substitúcia t za x do φ je prípustná)

4.4.4 Axiómy rovnosti. (3 axiómy + 2 schémy axióm)
Pre ľubovoľný n-árny funkcionálny symbol f a ľubovoľný n-árny relačný symbol r nasledujúce formuly sú axiómy:

(EAx 1) $x = x$
(EAx 2) $x = y \Rightarrow y = x$
(EAx 3) $x = y \Rightarrow (y = z \Rightarrow x = z)$
(EAx 4) $x_1 = y_1 \Rightarrow (\ldots \Rightarrow (x_n = y_n \Rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)) \ldots)$
(EAx 5) $x_1 = y_1 \Rightarrow (\ldots \Rightarrow (x_n = y_n \Rightarrow r(x_1, \ldots, x_n) \Rightarrow r(y_1, \ldots, y_n)) \ldots)$

4.4.5 Odvodzovacie pravidlá: Modus Ponens (MP)
a Pravidlo zovšeobecnenia (generalizácie) (Gen)

(MP) $\dfrac{\varphi,\ \varphi \Rightarrow \psi}{\psi}$ (z φ a $\varphi \Rightarrow \psi$ odvoď ψ)

(Gen) $\dfrac{\varphi}{(\forall x)\varphi}$ (z φ odvoď $(\forall x)\varphi$)

4.4.6 Úloha. (a) Presvedčte sa, že všetky logické axiómy sú splnené v každej L-štruktúre $\mathcal{A}$.

(b) Uvedomte si, že odvodzovacie pravidlo Modus Ponens je korektné v nasledujúcom zmysle: Pre každú L-štruktúru $\mathcal{A}$ a ľubovoľné L-formuly φ, ψ z podmienok $\mathcal{A} \vDash \varphi$ a $\mathcal{A} \vDash \varphi \Rightarrow \psi$ vyplýva $\mathcal{A} \vDash \psi$.

(c) Presvedčte sa, že Pravidlo zovšeobecnenia je korektné v nasledujúcom zmysle: Pre každú L-štruktúru $\mathcal{A}$ a ľubovoľnú L-formulu φ z podmienky $\mathcal{A} \vDash \varphi$ vyplýva $\mathcal{A} \vDash (\forall x)\varphi$ pre akúkoľvek premennú x, bez ohľadu na to, či x je voľná vo φ alebo nie.

Dôkaz v teórii prvého rádu T je konečná postupnosť formúl $\varphi_0, \varphi_1, \ldots \varphi_n$, ktorej každý člen φ_k je alebo logická axióma alebo špecifická axióma teórie T (t. j. $\varphi_k \in T$), alebo vyplýva z predchádzajúcich členov podľa pravidla Modus Ponens (MP) (t. j. pre nejaké $i, j < k$ člen φ_j má tvar $\varphi_i \Rightarrow \varphi_k$) alebo podľa Pravidla zovšeobecnenia (Gen) (t. j. pre niektoré $j < k$ člen φ_k má tvar $(\forall x)\varphi_j$ pre nejakú premennú x).

Formula ψ je *dokázateľná* v teórii T, ak existuje dôkaz $\varphi_0, \varphi_1, \ldots, \varphi_n$ v T, ktorého posledný člen φ_n splýva so ψ. Symbolicky píšeme $T \vdash \psi$. Namiesto $\emptyset \vdash \psi$ píšeme iba $\vdash \psi$; znamená to, že ψ je dokázateľné len z logických axióm.

4.4.7 Úloha. Overte, že nasledujúce prvorádové schémy sú dokázateľné len z logických axióm:
(a) všetky výrokové tautológie
(b) $\varphi(t/x) \Rightarrow (\exists x)\varphi$ (ak substitúcia t/x do φ je prípustná)
(c) $(x_1 = y_1 \wedge \ldots \wedge x_n = y_n) \Rightarrow t(x_1, \ldots, x_n) = t(y_1, \ldots, y_n)$ (pre akýkoľvek term t)
(d) $(x_1 = y_1 \wedge \ldots \wedge x_n = y_n) \Rightarrow (\varphi(x_1, \ldots, x_n) \Leftrightarrow \varphi(y_1, \ldots, y_n))$
(pre hocijakú formulu φ, ak všetky substitúcie y_i/x_i do φ sú prípustné)

4.4.8 Veta o korektnosti. *Nech T je teória v jazyku prvého rádu L. Potom pre ľubovoľnú L-formulu ψ z $T \vdash \psi$ vyplýva $T \vDash \psi$.*

Demonštrácia. Nech $T \vdash \psi$ a $\varphi_0, \varphi_1, \ldots, \varphi_n$ je dôkaz ψ v T. Ukážeme, že $\mathcal{A} \vDash \varphi_k$ pre každý model $\mathcal{A} \vDash T$ teórie T a *každé* $k \leq n$. Potom samozrejme $\mathcal{A} \vDash \psi$, keďže ψ je φ_n. Každé φ_k je logická axióma, a v tom prípade $\mathcal{A} \vDash \varphi_k$ pre každú L-štruktúru $\mathcal{A}$, alebo špecifická axióma teórie T, a v tom prípade $\mathcal{A} \vDash \varphi_k$, lebo $\mathcal{A} \vDash T$, alebo φ_k vyplýva z niektorých predchádzajúcich členov podľa (MP) alebo podľa (Gen). V prípade (MP) existujú $i, j < k$ také, že φ_j má tvar $\varphi_i \Rightarrow \varphi_k$. Teraz pre ľubovoľnú L-štruktúru $\mathcal{A}$ za predpokladu, že už máme $\mathcal{A} \vDash \varphi_i$ a $\mathcal{A} \vDash \varphi_j$, teda $\mathcal{A} \vDash \varphi_i \Rightarrow \varphi_k$, môžeme odvodiť $\mathcal{A} \vDash \varphi_k$. V prípade (Gen) existuje $j < k$ také, že φ_k má tvar $(\forall x)\varphi_j$. Opäť pre ľubovoľnú L-štruktúru $\mathcal{A}$ možno z predpokladu, že už máme $\mathcal{A} \vDash \varphi_j$, odvodiť $\mathcal{A} \vDash (\forall x)\varphi_j$, čiže $\mathcal{A} \vDash \varphi_k$. (Pozri Úlohu 4.4.6.)

V tejto chvíli by sa mal čitateľ vrátiť k Poznámke 3.6.2 nasledujúcej po demonštrácii Vety o korektnosti 3.6.1 vo výrokovom počte a uvedomiť si, že tam uvedené úvahy sa rovnakou mierou vzťahujú aj na jej prvorádovú verziu.

Neskôr ustanovíme aj nasledujúce obrátenie Vety o korektnosti.

4.4.9 Veta o úplnosti. *Nech T je teória v jazyku prvého rádu L. Potom pre ľubovoľnú L-formulu ψ z $T \vDash \psi$ vyplýva $T \vdash \psi$.*

Ako ukazuje nasledujúci príklad, jemne vyvážený vzťah medzi syntaxou a sémantikou, akého sme svedkami vo výrokovom počte aj v logike prvého rádu, nie je nijako samozrejmý ani automaticky zaručený.

4.4.10 Príklad. (Sémantika konečných modelov) Nech L je jazyk prvého rádu. Pre teóriu T v jazyku L a ľubovoľnú L-formulu φ definujeme *vzťah konečného spĺňania* $T \vDash_{\text{fin}} \varphi$ práve vtedy, keď $\mathcal{A} \vDash \varphi$ pre každý *konečný* model $\mathcal{A}$ teórie T, čiže práve vtedy, keď φ je splnené v každom *konečnom* modeli teórie T. Metódami presahujúcimi rámec nášho elementárneho kurzu možno dokázať, že túto *sémantiku konečných modelov* nemožno axiomatizovať tak, aby pre ňu súčasne platili príslušné verzie vety o korektnosti a vety o úplnosti. Presnejšie, pre každú korektnú axiomatizáciu pozostávajúcu z konečného počtu schém axióm a konečne mnohých odvodzovacích pravidiel príslušný vzťah dokázateľnosti $T \vdash_{\text{fin}} \varphi$ nikdy nevyčerpá vzťah konečného spĺňania $T \vDash_{\text{fin}} \varphi$. To znamená, že vždy možno nájsť teóriu T a uzavretú formulu φ tak, že $T \vDash_{\text{fin}} \varphi$, jednako $T \nvdash_{\text{fin}} \varphi$.

Aby sme čitateľovi pomohli utvoriť si aspoň akú-takú predstavu o tomto probléme, spomeňme hlbokú *Wedderburnovu vetu*, podľa ktorej každý konečný okruh s delením je pole. Inými slovami, komutatívny zákon $xy = yx$ je konečne splnený v teórii okruhov s delením. Na druhej strane, kvaternióny $(\mathbb{H}; +, \cdot, 0, 1)$ tvoria nekonečný okruh s delením, ktorý nie komutatívny; teda komutatívny zákon pre násobenie nie je prvorádovým dôsledkom axióm okruhov s delením.

4.4.11 Úloha. Hovoríme, že L-formula φ je *logicky platná*, ak je splnená v každej L-štruktúre $\mathcal{A}$. Dve L-formuly φ, ψ sa nazývajú *logicky ekvivalentné*, označenie $\varphi \equiv \psi$, ak formula $\varphi \Leftrightarrow \psi$ je logicky platná. Hovoríme, že formula φ je v *prenexnom normálnom tvare*, ak má podobu $(\mathrm{Q}_1 x_1) \ldots (\mathrm{Q}_n x_n)\psi$, kde $\mathrm{Q}_1, \ldots, \mathrm{Q}_n$ sú ľubovoľné kvantifikátory a ψ je formula bez kvantifikátorov.

(a) Ukážte, že pre ľubovoľné formuly φ, ψ sú nasledujúce dvojice formúl logicky ekvivalentné:

$$\begin{aligned} \neg(\forall x)\varphi &\equiv (\exists x)\neg\varphi & \qquad \neg(\exists x)\varphi &\equiv (\forall x)\neg\varphi \\ (\forall x)\varphi \wedge \psi &\equiv (\forall x)(\varphi \wedge \psi) & \qquad (\exists x)\varphi \vee \psi &\equiv (\exists x)(\varphi \vee \psi) \\ (\forall x)\varphi \Rightarrow \psi &\equiv (\exists x)(\varphi \Rightarrow \psi) & \qquad \psi \Rightarrow (\exists x)\varphi &\equiv (\exists x)(\psi \Rightarrow \varphi) \end{aligned}$$

(b) Ukážte, že pre ľubovoľné formuly φ, ψ také, že premenná x nemá voľný výskyt v ψ, sú nasledujúce dvojice formúl logicky ekvivalentné:

$$\begin{aligned} (\forall x)\varphi \vee \psi &\equiv (\forall x)(\varphi \vee \psi) & \qquad (\exists x)\varphi \wedge \psi &\equiv (\exists x)(\varphi \wedge \psi) \\ (\exists x)\varphi \Rightarrow \psi &\equiv (\forall x)(\varphi \Rightarrow \psi) & \qquad \psi \Rightarrow (\forall x)\varphi &\equiv (\forall x)(\psi \Rightarrow \varphi) \end{aligned}$$

(c) Pomocou (a) a (b) ukážte, že každá L-formula je logicky ekvivalentná s nejakou formulou v prenexnom normálnom tvare.

(d) Nahraďte v každom z prípadov v (a) a (b) logickú ekvivalenciu $\theta \equiv \chi$ formulou $\theta \Leftrightarrow \chi$ a ukážte, že všetky formuly, ktoré takto dostanete, sú dokázateľné z logických axióm (dokonca len z axióm výrokového počtu a axióm kvantifikátorov). V každom jednotlivom prípade v (b) rozhodnite, ktorá z implikácií $\theta \Rightarrow \chi$, $\chi \Rightarrow \theta$ zostáva logicky platná aj bez predpokladu, že x nemá voľný výskyt v ψ, a uveďte príklady ukazujúce, že v zostávajúcich prípadoch nemožno tento predpoklad vynechať.

4.5 Veta o dedukcii a jej dôsledky

Na ceste k demonštrácii vety o úplnosti ustanovíme niekoľko výsledkov, ktoré majú svoj význam aj samy osebe. Prvá skupina pozostáva z *Vety o dedukcii* a dvoch jej dôsledkov, menovite z *Dôsledku o dôkaze sporom* a *Dôsledku o dôkaze rozborom možností*, s ktorých analogickými verziami sme sa už stretli vo výrokovom počte.

4.5.1 Veta o dedukcii. *Nech T je teória v jazyku prvého rádu L a φ, ψ sú ľubovoľné L-formuly. Ak φ je uzavretá, tak $T \vdash \varphi \Rightarrow \psi$ práve vtedy, keď $T \cup \{\varphi\} \vdash \psi$.*

Jednoduchú skutočnosť, že z podmienky $T \vdash \varphi \Rightarrow \psi$ vyplýva $T \cup \{\varphi\} \vdash \psi$, možno overiť úplne rovnako ako v demonštrácii Vety 3.7.1 o dedukcii vo výrokovom počte, dokonca bez predpokladu, že φ je uzavretá. Oprávnenie bežného spôsobu argumentácie používaného pri dôkaze implikácie $\varphi \Rightarrow \psi$ v T, keď miesto toho dokazujeme ψ v teórii $T \cup \{\varphi\}$, si však vyžaduje úvahu v opačnom smere. To možno opäť urobiť podobným, iba trochu komplikovanejším spôsobom ako v príslušnej demonštrácii vo výrokovom počte. Musíme len navyše ošetriť prípad, keď ψ vyplýva z nejakého predchádzajúceho člena svojho dôkazu podľa Pravidla zovšeobecnenia (Gen). V našej demonštrácii zaplníme iba túto medzeru a detaily prenecháme čitateľovi.

Demonštrácia. Predpokladajme, že $\psi_0, \psi_1, \ldots, \psi_n$ je dôkaz formuly ψ v teórii $T \cup \{\varphi\}$ a ψ_n vyplýva z nejakej predošlej formuly ψ_k, kde $0 \leq k < n$, podľa (Gen). Potom ψ_k je dokázateľná v $T \cup \{\varphi\}$ a postupujúc indukciou možeme predpokladať, že implikácia $\varphi \Rightarrow \psi_k$ je dokázateľná v T. Takže ψ má tvar $(\forall x)\psi_k$ pre nejakú premennú x. Potom nasledujúce formuly sú dokázateľné v T:

(1) $\varphi \Rightarrow \psi_k$
(2) $(\forall x)(\varphi \Rightarrow \psi_k)$ vyplýva z (1) podľa (Gen)
(3) $(\forall x)(\varphi \Rightarrow \psi_k) \Rightarrow (\varphi \Rightarrow (\forall x)\psi_k)$ je inštanciou schémy axióm kvantifikátorov (QAx 1), lebo φ je uzavretá, teda x v nej nemá voľný výskyt
(4) $\varphi \Rightarrow (\forall x)\psi_k$ možno odvodiť z (2) a (3) podľa (MP)

To znamená, že $T \vdash \varphi \Rightarrow \psi$.

Ukážeme, že predpoklad o uzavretosti formuly φ nemožno vo všeobecnosti vynechať.

4.5.2 Príklad. Nech L je *jazyk čistej rovnosti*, t. j. jazyk prvého rádu bez akýchkoľvek špecifických symbolov ($F = C = R = \emptyset$) a $T = \emptyset$ je teória bez akýchkoľvek špecifických axióm v L. Označme φ formulu $x = y$ a ψ formulu $x = z$. Tvrdíme, že $T \cup \{\varphi\} \vdash \psi$, jednako $T \nvdash \varphi \Rightarrow \psi$. $T \cup \{\varphi\} = \{\varphi\}$ je teória s jedinou axiómou $x = y$. To znamená, že všetky jej modely majú len jednoprvkovú základnú množinu. Aplikujúc pravidlo (Gen) na túto axiómu vidíme, že $T \cup \{\varphi\} \vdash (\forall y)(x = y)$. Pomocou axiómy kvantifikátorov $(\forall y)(x = y) \Rightarrow x = z$ a pravidla (MP) z toho odvodíme, že $T \cup \{\varphi\} \vdash x = z$. Zároveň však implikácia $\varphi \Rightarrow \psi$, čiže $x = y \Rightarrow x = z$ nie je dokázateľná len z logických axióm, teda v teórii T. V tom prípade by totiž platila v každej L-štruktúre $\mathcal{A}$. Avšak každé $\mathcal{A}$ s aspoň dvoma prvkami $a \neq b$ porušuje túto implikáciu, lebo pri dosadení a za x aj y a b za z máme $a = a$, ale $a \neq b$.

Teória T v jazyku prvého rádu L sa nazýva *sporná* alebo *protirečivá*, prípadne *inkonzistentná*, ak pre nejakú uzavretú L-formulu φ platí $T \vdash \varphi$ a zároveň $T \vdash \neg\varphi$. V opačnom prípade hovoríme, že T je *bezosporná* alebo *neprotirečivá*, prípadne *konzistentná*. Ľahko možno nahliadnuť, že T je sporná práve vtedy, keď každá L-formula je dokázateľná v T.

Nasledujúce dva dôsledky vyplývajú z Vety 4.5.1 o dedukcii rovnako ako vo výrokovom počte.

4.5.3 Dôsledok o dôkaze sporom. *Nech T je teória v jazyku prvého rádu L a φ je uzavretá L-formula. Potom $T \vdash \varphi$ práve vtedy, keď teória $T \cup \{\neg\varphi\}$ je sporná (inkonzistentná).*

4.5.4 Dôsledok o dôkaze rozborom možností. *Nech T je teória v jazyku prvého rádu L a φ, ψ sú ľubovoľné L-formuly. Ak φ je uzavretá, tak $T \vdash \psi$ práve vtedy, keď $T \cup \{\varphi\} \vdash \psi$ a zároveň $T \cup \{\neg\varphi\} \vdash \psi$.*

4.5.5 Úloha. Na príkladoch ukážte, že predpoklad o uzavretosti formuly φ nemožno z práve uvedených dôsledkov vynechať.

4.6 Úplné teórie

Ďalšia dôležitá vlastnosť teórií prvého rádu tesne súvisiaca s bezospornosťou je ich úplnosť. Teória T v jazyku prvého rádu L sa nazýva *úplná*, ak je bezosporná a pre každú *uzavretú* L-formulu φ platí $T \vdash \varphi$ alebo $T \vdash \neg\varphi$. Inak povedané, T je úplná práve vtedy, keď pre každú uzavretú L-formulu φ nastane práve jedna z možností $T \vdash \varphi$ alebo $T \vdash \neg\varphi$. Hovoríme tiež, že T *dokáže rozhodnúť* každú uzavretú formulu φ.

4.6.1 Príklad. Čitateľ si možno kladie otázku, prečo sme v definícii úplnej teórie žiadali, aby T dokázala rozhodnúť len uzavreté formuly, a ignorovali tie ostatné. Na vysvetlenie uvažujme formulu $x = y$ a jej negáciu $x \neq y$. Keby požiadavka úplnosti teórie T zahŕňala dokázateľnosť jednej z týchto formúl, tak v prvom prípade by T mala iba jednoprvkové modely a v druhom prípade by bola sporná. V dôsledku toho by každá konzistentná v takomto zmysle „úplná“ teória mala len triviálne modely.

Úplné teórie možno s využitím Dôsledku 4.5.3 o dôkaze sporom charakterizovať ako maximálne konzistentné teórie v nasledujúcom zmysle:

4.6.2 Dôsledok o úplných teóriách. *Nech T je konzistentná teória v jazyku prvého rádu L. Potom T je úplná práve vtedy, keď pre každú uzavretú L-formulu φ platí buď $T \vdash \varphi$ alebo teória $T \cup \{\varphi\}$ je sporná.*

Inými slovami, rozšírenie zoznamu axióm úplnej teórie T o akúkoľvek uzavretú formulu φ nemá zmysel: alebo je φ dokázateľná v T (a v tom prípade množiny formúl dokázateľných v T a v $T \cup \{\varphi\}$ sú rovnaké) alebo $T \cup \{\varphi\}$ je už sporná, teda bezcenná.

Väčšina relevantných teórií vyskytujúcich sa v matematike nie je úplných. Na druhej strane mnohé z nich majú dôležité úplné rozšírenia. Na tomto mieste uvedieme niekoľko príkladov úplných teórií, ich úplnosť však už dokazovať nebudeme.

4.6.3 Deliteľné abelovské grupy. Teória grúp nie je úplná: napr. fakt, že existujú komutatívne aj nekomutatívne grupy ukazuje, že komutatívny zákon $(\forall x, y)(xy = yx)$ ani jeho negácia nie sú dokázateľné v Teórii grúp. V tejto časti popíšeme niektoré pomerne jednoduché úplné rozšírenia Teórie abelovských grúp.

Abelovská grupa $\mathcal{G} = (G; +, 0)$ je *netriviálna*, ak v nej platí $(\exists x)(x \neq 0)$; $\mathcal{G}$ sa nazýva *deliteľná*, ak je netriviálna a spĺňa podmienku

$$(\forall x)(\exists y)(n \times y = x)$$

pre každé celé číslo $n \geq 2$, kde $n \times x = x + \ldots + x$ s n-násobným výskytom x. Hovoríme, že $\mathcal{G}$ je *bez torzie*, ak spĺňa všetky podmienky

$$n \times x = 0 \;\Rightarrow\; x = 0$$

pre $n \geq 2$. Pre dané pevné $n \geq 1$ hovoríme, že $\mathcal{G}$ je *grupa s exponentom n*, ak v nej platí $(\forall x)(n \times x = 0)$. Vie sa, že *Teória deliteľných abelovských grúp bez torzie*, ako aj každá z *Teórií deliteľných abelovských grúp s exponentom p* pre pevné prvočíslo p je úplná.

4.6.4 Reálne uzavreté a algebraicky uzavreté polia. Možno ukázať, že Teória reálne uzavretých polí (tak v jej usporiadanej ako aj v jej neusporiadanej verzii) je úplná. Na druhej strane, Teória algebraicky uzavretých polí úplná nie je. Jednako, všetky jej úplné rozšírenia možno popísať vyčerpávajúcim spôsobom.

Charakteristikou unitárneho okruhu $\mathcal{A} = (A; +, \cdot, 0, 1)$ nazývame najmenšie celé číslo $\mathrm{char}(\mathcal{A}) = n \geq 1$ také, že $n \times 1 = 0$, alebo $\mathrm{char}(\mathcal{A}) = \infty$, ak $n \times 1 \neq 0$ pre každé $n \geq 1$ (niektorí autori vtedy píšu $\mathrm{char}(\mathcal{A}) = 0$). Je známe, že charakteristika

hocijakého poľa je buď prvočíslo alebo ∞. Pole $(F, +, \cdot, 0, 1)$ má prvočíselnú charakteristiku p práve vtedy, keď v ňom platí $p \times 1 = 0$, a má charakteristiku ∞ práve vtedy, keď spĺňa všetky podmienky $p \times 1 \neq 0$ pre každé prvočíslo p. Každá z Teórií algebraicky uzavretých polí pevnej prvočíselnej charakteristiky p, ako aj Teória algebraicky uzavretých polí charakteristiky ∞ je úplná.

4.6.5 Husté lineárne usporiadanie. Lineárne usporiadaná množina $(A; <)$ sa nazýva *hustá*, ak obsahuje aspoň dva prvky a spĺňa podmienku

$$(\forall\, x, y)\big(x < y \;\Rightarrow\; (\exists\, z)(x < z < y)\big)$$

Hovoríme, že $(A; <)$ je *bez koncových bodov*, ak spĺňa podmienku

$$(\forall\, x)(\exists\, y, z)(y < x < z)$$

O *Teórii hustého lineárneho usporiadania bez koncových bodov* možno dokázať, že je úplná. Ďalšie tri úplné rozšírenia Teórie hustého lineárneho usporiadania možno získať očividným spôsobom variáciou podmienky existencie koncových bodov.

4.6.6 Atomické a bezatomické Booleove algebry. Prvok $a \in B$ Boolovej algebry $\mathcal{B} = (B; \wedge, \vee, ', 0, 1)$ sa nazýva *atóm*, ak $a \neq 0$ a neexistuje prvok $b \in B$ taký, že $0 < b < a$. Formálne môžeme jazyk Boolových algebier rozšíriť o nový unárny predikát $\mathrm{At}(x)$ definovaný formulou

$$\mathrm{At}(x) \;\Leftrightarrow\; x \neq 0 \wedge (\forall\, y)\big(0 \leq y \leq x \;\Rightarrow\; (y = 0 \vee y = x)\big)$$

s použitím skôr definovaného čiastočného usporiadania $\leq$ (pozri 4.3.5). Hovoríme, že $\mathcal{B}$ je *atomická*, ak sa pod každým nenulovým prvkom v B nachádza aspoň jeden atóm, t. j., ak $\mathcal{B}$ spĺňa podmienku

$$(\forall\, x)(x \neq 0 \;\Rightarrow\; (\exists\, y)(\mathrm{At}(y) \wedge y \leq x))$$

$\mathcal{B}$ sa nazýva *bezatomická*, ak obsahuje aspoň dva prvky a neobsahuje žiadny atóm. To možno vyjadriť podmienkou netriviálnosti $0 \neq 1$ a istou formou axiómy hustoty

$$(\forall\, x)(x \neq 0 \;\Rightarrow\; (\exists\, y)(0 < y < x))$$

Teória atomických Boolových algebier s nekonečne mnohými atómami, ako aj každá z *Teórií atomických Boolových algebier s práve n atómami*, kde $n \geq 1$, je úplná. Podobne je úplná aj *Teória bezatomických Boolových algebier*. Možno dokonca podať efektívny a vyčerpávajúci popis všetkých úplných rozšírení Teórie Boolevých algebier v termínoch dvoch celočíselných invariantov. Tento popis je však pomerne náročný a presahuje rámec nášho kurzu.

4.6.7 Presburgerova aritmetika. Neskôr, keď sa budeme zaoberať Gödelovými vetami o neúplnosti, uvidíme, že Peanova aritmetika je nielen neúplná, ale ani jej úplné rozšírenia nemožno efektívne popísať. Na druhej strane PA má zaujímavú úplnú podteóriu, známu pod názvom *Presburgerova aritmetika*, ktorá opisuje štruktúru prirodzených čísel len s operáciami nasledovníka a sčítania. Jej jazyk obsahuje konštantné

symboly 0 a 1 a operačný symbol +. Jej axiómy dostaneme z axióm Peanovej aritmetiky uvedených v 4.3.8 vynechaním všetkých tých, ktoré obsahujú symbol násobenia, teda dvojice tvoriacej pravý stĺpec sedemčlenného zoznamu individuálnych axióma PA, ako aj všetkých inštancií Schémy indukcie, kde formula $\varphi(x, \vec{u})$ obsahuje operačný symbol $\cdot$.

4.7 Výsledky o rozšíreniach jazyka

Keď dokazujeme všeobecne kvantifikované tvrdenie tvaru $(\forall\, x_1, \ldots, x_k)\varphi(x_1, \ldots, x_k)$ v teórii prvého rádu T, zvyčajne začíname frázou: *„Nech x_1, …, x_n sú ľubovoľné prvky. . .“* To však znamená, že x_1, …, x_n v našom dôkaze viac nepovažujeme za premenné, ale že s nimi zaobchádzame ako s bližšie neurčenými konštantami. Nasledujúci výsledok ukazuje, že tento spôsob argumentácie je legitímny v logike prvého rádu.

4.7.1 Lema o konštantách. *Nech T je teória v jazyku prvého rádu L, $\varphi(x_1, \ldots, x_k)$ je L-formula a $c_1, \ldots, c_k$ sú navzájom rôzne konštantné symboly nevyskytujúce sa v L. Potom*

$$T \vdash \varphi(c_1, \ldots, c_k) \quad \textit{práve vtedy, keď} \quad T \vdash (\forall\, x_1, \ldots, x_k)\varphi(x_1, \ldots, x_k)$$

Demonštrácia. Predpokladajme, že $T \vdash \varphi(c_1, \ldots, c_k)$. Uvedomme si, že T je teória v jazyku L, ktorý neobsahuje konštanty $c_1, \ldots, c_k$, takže teória T „o nich nič nevie“. Preto čokoľvek, čo možno v T dokázať o týchto konštantách, možno dokázať tiež o vhodne zvolených navzájom rôznych premenných $x_1, \ldots, x_k$, ktoré sa nevyskytujú v pôvodnom dôkaze – stačí nahradiť každý výskyt symbola c_i premennou x_i. Potom $T \vdash \varphi(x_1, \ldots, x_k)$ a potrebný záver vyplýva z Pravidla zovšeobecnenia. Obrátená implikácia je triviálna.

Je jasné, že uvedená veta zostáva v platnosti aj vtedy, keď konštanty $c_1, \ldots, c_k$ patria do L, ale sa nevyskytujú v žiadnej zo špecifických axióm teórie T.

Keď rozvíjame a budujeme nejakú matematickú teóriu, len zriedka pritom fixujeme jej jazyk po celý čas. Skôr naopak, často definujeme nové pojmy zodpovedajúce nejakým operáciám, reláciám alebo významným prvkom a zavádzame pre ne nové symboly. Tieto nové symboly spravidla označujú dôležité alebo často sa vyskytujúce pojmy, skracujú inak ťažkopádne formulácie, a tým prispievajú k prehľadnosti a zrozumiteľnosti teórie. Dokonca aj v našom kurze sme takto postupovali už niekoľkokrát, keď sme sa zaoberali príkladmi rôznych teórií prvého rádu, bez toho, aby sme tejto otázke venovali zvláštnu pozornosť. Napríklad sme rozšírili jazyk Teórie grúp pozostávajúci z jedného binárneho operačného symbola $\cdot$ o konštantný symbol e pre jednotkový prvok a o unárny symbol $^{-1}$ operácie inverzného prvku. Taktiež sme rozšírili jazyk Teórie Boolových algebier, ako aj jazyk Peanovej aritmetiky o symbol relácie usporiadania $\leq$ atď. Teraz sa budeme zaoberať takouto situáciou vo všeobecnosti.

Nech $L = (F, C, R, \nu)$ a $L' = (F', C', R', \nu')$ sú dva jazyky prvého rádu. Hovoríme, že jazyk L' je *rozšírením* jazyka L, ak $F \subseteq F'$, $C \subseteq C'$, $R \subseteq R'$ a pre každý operačný alebo relačný symbol $s \in F \cup R$ platí $\nu'(s) = \nu(s)$, t. j. arity symbola s v L a v L' sa zhodujú. V takom prípade píšeme $L \subseteq L'$ alebo $L' \supseteq L$. Potom akúkoľvek teóriu T

v jazyku L možno zároveň považovať za teóriu v jazyku L'. Na druhej strane, z každej L'-štruktúry $\mathcal{A} = (A;\, I)$ možno získať L-štruktúru $\mathcal{A} \restriction L = (A;\, I \restriction L)$, nazývanú *zúženie* štruktúry $\mathcal{A}$ do jazyka L. Jej základná množina A ako aj interpretácie s^I symbolov jazyka L v nej zostávajú nezmenené, zatiaľ čo interpretácie zvyšných symbolov jazyka L' sú vynechané. V tejto chvíli sa budeme zaujímať o prípad, keď nové symboly rozširujúce L sú zavedené pomocou definícií formulami jazyka L.

Kvantifikáciu jednoznačnej existencie $(\exists!\, x)\varphi$ zavádzame ako skratku za

$$(\exists\, x)\big(\varphi \wedge (\forall\, y)(\varphi(y/x) \Rightarrow y = x)\big)$$

kde y je ľubovoľná premenná nevyskytujúca sa vo φ.

Nech T je teória v jazyku prvého rádu L. Ohľadom konštánt, funkcionálnych a relačných symbolov rozlišujeme tri možnosti:

(a) Nech $\varphi(x)$ je L-formula taká, že $T \vdash (\exists!\, x)\varphi(x)$. Jazyk L rozšírime o nový konštantný symbol d nevyskytujúci sa v L a teóriu T o axiómu

$$x = d \;\Leftrightarrow\; \varphi(x)$$

(b) Nech $\psi(x_1, \ldots, x_n, y)$ je L-formula taká, že $T \vdash (\forall\, x_1, \ldots, x_n)(\exists!\, y)\psi(\vec{x}, y)$. Jazyk L rozšírime o nový n-árny funkcionálny symbol g nevyskytujúci sa v L a teóriu T o axiómu

$$y = g(x_1, \ldots, x_n) \;\Leftrightarrow\; \psi(x_1, \ldots, x_n, y)$$

(c) Nech $\rho(x_1, \ldots, x_n)$ je ľubovoľná L-formula. Jazyk L rozšírime o nový n-árny relačný symbol q nevyskytujúci sa v L a teóriu T o axiómu

$$q(x_1, \ldots, x_n) \;\Leftrightarrow\; \rho(x_1, \ldots, x_n)$$

V každom z uvedených prípadov hovoríme, že konštantný symbol d, resp. funkcionálny symbol g resp. relačný symbol q bol zavedený príslušnou definíciou v teórii T. Čitateľ by si mal uvedomiť, že ak považujeme konštantné symboly za nulárne funkcionálne symboly, môžeme (a) považovať za špeciálny prípad (b).

Hovoríme, že teória T' v jazyku prvého rádu L' je *rozšírením* teórie T v jazyku prvého rádu L *pomocou definícií*, ak L' je rozšírením L o konečný počet špecifických symbolov a špecifické axiómy teórie T' sú získané rozširovaním teórie T postupným zavádzaním nových symbolov jazyka L' pomocou definícií. To znamená, že pri zavádzaní nového symbola v istom kroku môžeme v jeho definícii použiť nielen prostriedky pôvodného jazyka L, ale aj skôr zavedené symboly. Je jasné, že každý model $\mathcal{A} = (A;\, I)$ teórie T v jazyku L má jednoznačne určené rozšírenie do modelu $\mathcal{A}' = (A;\, I')$ teórie T' v jazyku L'. Je získané opakovanou interpretáciou každého novozavedeného symbola v $\mathcal{A}'$ s použitím jeho definujúcej formuly v jazyku L rozšírenom o skôr definované symboly.

Hoci nová teória T' umožňuje vyjadriť viaceré pojmy stručnejším a ľahšie čitateľným spôsobom, pokiaľ ide o tvrdenia v pôvodnom jazyku L, nemôže toho dokázať viac než pôvodná teória T.

Hovoríme, že teŕia T' v jazyku prvého rádu L' rozširujúca teóriu T v jazyku prvého rádu $L \subseteq L'$ je *konzervatívnym rozšírením* teórie T, ak pre každú uzavretú L-formulu φ platí

$$T' \vdash \varphi \quad \text{práve vtedy, keď} \quad T \vdash \varphi$$

Zrejme každé konzervatívne rozšírenie konzistentnej teórie je i samo konzistentné.

4.7.2 Veta o rozšírení pomocou definícií. *Predpokladajme, že teória T' v jazyku prvého rádu L' je rozšírením teórie T v jazyku prvého rádu $L \subseteq L'$ pomocou definícií. Potom T' je konzervatívnym rozšírením teórie T.*

Pri demonštrácii Vety 4.7.2 sa stačí zaoberať prípadom, keď L' a T' sú získané z L a T zavedením jediného definovaného symbola. Myšlienka dôkazu je jednoduchá: pozostáva v nahradení každej inštancie definovanej formuly $x = d$, $y = g(x_1, \ldots, x_n)$ alebo $q(x_1, \ldots, x_n)$ vhodnou inštanciou príslušnej definujúcej L-formuly. Avšak pri jej realizácii by sme museli ošetriť isté technické detaily, ktoré vynecháme, keďže by sotva prispeli k čitateľovmu porozumeniu celej veci.

4.7.3 Úloha. Rozšírenia pomocou definovaných konštánt, operácií a relácií sú časté v Teórii množín.

(a) Napíšte explicitne definujúce formuly pre prázdnu množinu, operácie neusporiadanej dvojice prvkov $\{x, y\}$, zjednotenia $\bigcup X$, ako aj pre operácie vytvárajúce podmnožiny $\{x \in X \colon \varphi(x, \vec{u})\}$ zo Schémy vydelenia.

(b) S použitím vhodných inštancií Schémy vydelenia zaveďte binárne operácie prieniku $X \cap Y = \{u \colon u \in X \wedge u \in Y\}$ a množinového rozdielu $X \setminus Y = \{u \colon u \in X \wedge u \notin Y\}$.

(c) Napíšte definujúcu formulu pre reláciu inklúzie $X \subseteq Y$ a s jej pomocou zaveďte operáciu potenčnej množiny $\mathcal{P}(X) = \{Y \colon Y \subseteq X\}$.

(d) S použitím operácie neusporiadanej dvojice $\{x, y\}$ a zjednotenia $\bigcup X$ definujte binárnu operáciu zjednotenia $X \cup Y = \{u \colon u \in X \vee u \in Y\}$.

(e) S použitím operácie neusporiadanej dvojice zaveďte operáciu usporiadanej dvojice $(x, y) = \{\{x\}, \{x, y\}\}$ a dokážte, že

$$(x, y) = (u, v) \Leftrightarrow x = u \wedge y = v$$

(f) S použitím operácií usporiadanej dvojice (x, y), binárneho zjednotenia $X \cup Y$ a potenčnej množiny $\mathcal{P}(X)$, ako aj vhodnej inštancie Schémy vydelenia zaveďte a legitimizujte operáciu karteziánskeho súčinu

$$X \times Y = \{(x, y) \colon x \in X \wedge y \in Y\}$$

4.8 Gödelova veta o úplnosti

Predpokladajme, že $L = (F, C, R, \nu)$ je jazyk prvého rádu, ktorý obsahuje aspoň jeden konštantný symbol (teda $C \neq \emptyset$). Označme K množinu všetkých konštantných termov jazyka L. Potom z K sa stane základná množina L-štruktúry $\mathcal{K} = (K; \ldots)$, ktorú získame interpretáciou špecifických symbolov jazyka L nasledujúcim prirodzeným spôsobom:

(a) pre každý n-árny funkcionálny symbol $f \in F$ a konštantné termy $t_1, \ldots, t_n \in K$ je $f^{\mathcal{K}}(t_1, \ldots, t_n)$ konštantný term $f(t_1, \ldots, t_n) \in K$;

(b) pre každý konštantný symbol $c \in C$ je $c^{\mathcal{K}}$ konštantný term $c \in K$;

(c) pre každý n-árny relačný symbol $r \in R$ a konštantné termy $t_1, \ldots, t_n \in K$ kladieme $(t_1, \ldots, t_n) \in r^{\mathcal{K}}$ práve vtedy, keď $T \vdash r(t_1, \ldots, t_n)$.

Navyše zavedieme nasledujúcu binárnu reláciu $\sim_T$ na K:

$$t_1 \sim_T t_2 \Leftrightarrow T \vdash t_1 = t_2$$

pre $t_1, t_2 \in K$. Ak nehrozí nedorozumenie, budeme namiesto $\sim_T$ písať iba $\sim$.

4.8.1 Úloha. S použitím axióm rovnosti dokážte, že

$$\begin{aligned} t &\sim t \\ t_1 \sim t_2 &\Rightarrow t_2 \sim t_1 \\ (t_1 \sim t_2 \wedge t_2 \sim t_3) &\Rightarrow t_1 \sim t_3 \\ (t_1 \sim s_1 \wedge \ldots \wedge t_n \sim s_n) &\Rightarrow f(t_1, \ldots, t_n) \sim f(s_1, \ldots, s_n) \\ (t_1 \sim s_1 \wedge \ldots \wedge t_n \sim s_n) &\Rightarrow (r(t_1, \ldots, t_n) \Leftrightarrow r(s_1, \ldots, s_n)) \end{aligned}$$

pre ľubovoľné $t, t_1, t_2, t_3 \in K$, a pre všetky n-árne symboly $f \in F$, $r \in R$ a ľubovoľné $t_1, s_1, \ldots, t_n, s_n \in K$.

Prvé tri podmienky vyjadrujú fakt, že relácia $\sim$ je reflexívna, symetrická a tranzitívna, teda je to *relácia ekvivalencie* na množine K. Pre každé $t \in K$ označíme

$$\widetilde{t} = \{s \in K \colon s \sim t\}$$

množinu všetkých konštantných termov ekvivalentných s t, čiže všetkých takých $s \in K$, pre ktoré možno rovnosť $s = t$ dokázať v T. Vždy platí $t \in \widetilde{t}$, $\widetilde{t} = \widetilde{s}$ práve vtedy, keď $t \sim s$, a $\widetilde{t} \cap \widetilde{s} = \emptyset$, ak $t \not\sim s$. Môžeme teda vytvoriť *faktorovú množinu*

$$K/{\sim} = \{\widetilde{t} \colon t \in K\}$$

čiže *rozklad* množiny K na bloky po dvoch ekvivalentných prvkov. Alternatívne sa na $K/{\sim}$ môžeme dívať ako na výsledok stotožnenia alebo splynutia každého bloku navzájom ekvivalentných prvkov z K do jediného prvku. Inak povedané, reláciu ekvivalencie $\sim$ budeme považovať za „novú rovnosť“ na K. Posledné dve *podmienky kompatibility* vyjadrujú fakt, že tak operácie ako aj relácie v $\mathcal{K}$ rešpektujú túto ekvivalenciu, čiže „novú rovnosť“ $\sim$.

Aj faktorová množina $M = K/{\sim}$ sa stane základnou množinou L-štruktúry $\mathcal{M} = (M; \ldots)$, ak interpretujeme špecifické symboly jazyka L nasledujúcim prirodzeným spôsobom:

(a) pre ľubovoľný n-árny operačný symbol $f \in F$ a bloky ekvivalencie $\widetilde{t}_1, \ldots, \widetilde{t}_n \in M$ je $f^{\mathcal{M}}(\widetilde{t}_1, \ldots, \widetilde{t}_n)$ blok $f(t_1, \ldots, t_n)^{\sim} \in M$ konštantného termu $f(t_1, \ldots, t_n) \in K$;

(b) pre ľubovoľný konštantný symbol $c \in C$ je $c^{\mathcal{M}}$ blok $\widetilde{c} \in M$ konštantného termu $c \in K$;

(c) pre ľubovoľný n-árny relačný symbol $r \in R$ a bloky ekvivalencie $\widetilde{t}_1, \ldots, \widetilde{t}_n \in M$ kladieme $(\widetilde{t}_1, \ldots, \widetilde{t}_n) \in r^{\mathcal{M}}$ práve vtedy, keď $T \vdash r(t_1, \ldots, t_n)$.

Podmienky kompatibility pre ekvivalenciu $\sim$ zaručujú, že uvedené definície interpretácií $f^{\mathcal{M}}$, $r^{\mathcal{M}}$ operačných a predikátových symbolov sú korektné, t. j. nazávisia na

jednotlivých reprezentantoch blokov ekvivalencie $\widetilde{t_i}$. Zrejme interpretáciou ľubovoľného konštantného termu $t \in K$ v štruktúre $\mathcal{M}$ je prvok $\widetilde{t} \in M$, čiže $t^{\mathcal{M}} = \widetilde{t}$.

Aby sme zdôraznili úlohu teórie T pri konštrukcii štruktúry $\mathcal{M}$, označíme ju $\mathcal{M}(T) = \mathcal{M} = (M; \dots)$ a budeme ju nazývať *kanonickou štruktúrou teórie* T.

4.8.2 Príklad. Konštantné termy v jazyku Peanovej aritmetiky PA zú zostavené z konštantných symbolov 0 a 1 pomocou operácií sčítania a násobenia. Napríklad 1, $0 + 1$, $1 + 0$, $1 \cdot 1$, $0 + (1 \cdot 1)$ je päť rozličných konštantných termov, ale každý z nich označuje to isté prirodzené číslo 1, a zároveň rovnosť medzi ktorýmikoľvek dvoma z nich je dokázateľná v PA. Inak povedané, $1 \sim_{\mathrm{PA}} 0 + 1 \sim_{\mathrm{PA}} 1 + 0 \sim_{\mathrm{PA}} 1 \cdot 1 \sim_{\mathrm{PA}} 0 + (1 \cdot 1)$. Dokonca existuje nekonečne mnoho konštantných termov t v jazyku PA takých, že $t \sim_{\mathrm{PA}} 1$. Podobne, prirodzené číslo 2 označuje blok ekvivalencie konštantného termu $1 + 1$ alebo akéhokoľvek konštantného termu dokázateľne mu rovného atď. Čitateľ by si mal uvedomiť, že kanonická štruktúra $\mathcal{M}(\mathrm{PA})$ teórie PA splýva s jej štandardným modelom $(\mathbb{N}; +, \cdot, 0, 1)$.

Bolo by pekné, keby sme vedeli zaručiť, že $\mathcal{M}(T) \vDash T$, t. j., že kanonická štruktúra $\mathcal{M}(T)$ je modelom T pre akúkoľvek bezospornú teóriu prvého rádu T (v jazyku L s aspoň jedným konštantným symbolom). Žiaľ, nie je tomu vždy tak. Jednako vieme dokázať, že $\mathcal{M}(T) \vDash T$ pre teórie spĺňajúce dve podmienky, ktoré teraz sformulujeme.

Prvá z týchto podmienok je, podobne ako vo výrokovom počte, podmienka úplnosti teórie T. Druhá podmienka však nemá výrokovú analógiu. Pre danú L-formulu $\varphi(x)$ (s jedinou voľnou premennou x) nazveme konštantný L-term t *svedkom* sentencie $(\exists\, x)\varphi(x)$ v teórii T, ak

$$T \vdash (\exists\, x)\varphi(x) \Rightarrow \varphi(t)$$

(Všimnite si, že substitúcia konštantného termu za akúkoľvek premennú je vždy prípustná.) Keďže vždy platí $T \vdash \varphi(t) \Rightarrow (\exists\, x)\varphi(x)$, t je svedkom pre $(\exists\, x)\varphi(x)$ v T práve vtedy, keď

$$T \vdash (\exists\, x)\varphi(x) \Leftrightarrow \varphi(t)$$

V tom prípade teda platí $T \vdash (\exists\, x)\varphi(x)$ práve vtedy, keď $T \vdash \varphi(t)$.

Teória T v jazyku prvého rádu L (s aspoň jedným konštantným symbolom) sa nazýva *henkinovská*, ak pre každú sentenciu tvaru $(\exists\, x)\varphi(x)$ existuje svedok v T.

4.8.3 Tvrdenie. *Nech T je úplná henkinovská teória v jazyku prvého rádu L (s aspoň jedným konštantným symbolom) Potom $\mathcal{M}(T) \vDash T$, inak povedané, kanonická štruktúra $\mathcal{M}(T)$ je modelom teórie T.*

Demonštrácia. Ukážeme, že pre každú uzavretú L-formulu φ platí

$$T \vdash \varphi \qquad \text{práve vtedy, keď} \qquad \mathcal{M}(T) \vDash \varphi \tag{$*$}$$

Z toho už vyplýva požadovaný záver $\mathcal{M}(T) \vDash T$. Budeme postupovať indukciou podľa zložitosti formuly φ.

Každá uzavretá atomická L-formula φ má tvar $t = s$ alebo $r(t_1, \dots, t_n)$, kde t, s a $t_1, \dots, t_n$ sú konštantné termy a r je n-árny relačný symbol. Teda pre atomické sentencie podmienka $(*)$ je splnená vzhľadom na definíciu štruktúry $\mathcal{M}(T)$.

Teraz už stačí vykonať indukčné kroky pre logické spojky $\neg$ a $\wedge$ a pre existenčný kvantifikátor $\exists$.

Predpokladajúc platnosť podmienky $(*)$ pre φ, overíme jej platnosť pre $\neg\varphi$ tak, že ukážeme ekvivalentnosť podmienok $T \vdash \neg\varphi$ a $\mathcal{M}(T) \vDash \neg\varphi$. Z $T \vdash \neg\varphi$ vyplýva $T \nvdash \varphi$, lebo T je konzistentná; obrátená implikácia je dôsledkom úplnosti teórie T. Teda podmienky $T \vdash \neg\varphi$ a $T \nvdash \varphi$ sú ekvivalentné. Avšak $T \nvdash \varphi$ je ekvivalentné s $\mathcal{M}(T) \nvDash \varphi$ podľa indukčného predpokladu, a to je ekvivalentné s $\mathcal{M}(T) \vDash \neg\varphi$.

Predpokladajúc platnosť podmienky $(*)$ pre φ aj ψ, overíme jej platnosť pre $\varphi \wedge \psi$. Zrejme nasledujúce podmienky sú ekvivalentné: $T \vdash \varphi \wedge \psi$; $T \vdash \varphi$ a $T \vdash \psi$; $\mathcal{M}(T) \vDash \varphi$ a $\mathcal{M}(T) \vDash \psi$; $\mathcal{M}(T) \vDash \varphi \wedge \psi$ (indukčný predpoklad potrebujeme na zabezpečenie ekvivalencie druhej a tretej podmienky).

Konečne predpokladajúc podmienku $(*)$ pre všetky sentencie $\varphi(t)$, kde t je konštantný term, overíme jej platnosť pre sentenciu $(\exists\, x)\varphi(x)$. Keďže T je henkinovská teória, sentencia $(\exists\, x)\varphi(x)$ má v T nejakého svedka t, takže podmienka $T \vdash (\exists\, x)\varphi(x)$ je ekvivalentná s existenciou nejakého konštantného termu t takého, že $T \vdash \varphi(t)$. Podľa indukčného predpokladu to je ekvivalentné s existenciou nejakého konštantného termu t takého, že $\mathcal{M}(T) \vDash \varphi(t)$, čiže $\mathcal{M}(T) \vDash \varphi\big(\widetilde{t}\,\big)$. Nakoľko $\mathcal{M}(T) = (M; \dots)$ a $M = K/\!\sim$ pozostáva výlučne z prvkov tvaru $\widetilde{t}$, kde t je konštantný term, posledná podmienka je ekvivalentá s podmienkou $\mathcal{M}(T) \vDash (\exists\, x)\varphi$.

4.8.4 Úloha. Nech S je sporná teória v jazyku prvého rádu L (s aspoň jedným konštantným symbolom). Popíšte jej kanonickú štruktúru $\mathcal{M}(S)$ a overte, že nie je modelom teórie S. Nájdite úplnú (teda bezospornú) teóriu T v L takú, že $\mathcal{M}(S) = \mathcal{M}(T) \vDash T$.

S použitím *Axiómy výberu* možno dokázať nasledujúcu vetu. Čitateľ, ktorý má záujem, nájde dôkaz v záverečnom paragrafe 4.11. Pri práci s pevne zvoleným jazykom prvého rádu, *novým symbolom* rozumieme špecifický symbol (je jedno či konštantný, funkcionálny alebo relačný), ktorý sa nevyskytuje v L.

4.8.5 Veta o úplných henkinovských rozšíreniach. *Nech T je bezosporná teória v jazyku prvého rádu $L = (F, C, R, \nu)$. Potom existuje rozšírenie jazyka L o množinu nových konštantných symbolov D do jazyka prvého rádu $L_D = (F, C \cup D, R, \nu)$ a rozšírenie teórie T do úplnej henkinovskej teórie $\widehat{T} \supseteq T$ v jazyku L_D.*

Práve vyslovenú Vetu použijeme pri demonštrácii nasledujúceho výsledku, ktorý je alternatívnou verziou Vety o úplnosti.

4.8.6 Gödelova veta o úplnosti. *Každá bezosporná teória prvého rádu T má nejaký model $\mathcal{A}$.*

Čitateľ by si mal uvedomiť, že aj obrátene, ak nejaká teória prvého rádu má model, tak je nevyhnutne bezosporná, inak povedané sporná teória prvého rádu nemôže mať nijaký model. (Toto je alternatívne znenie Vety o korektnosti.)

Demonštrácia. Nech T je bezosporná teória v jazyku prvého rádu L, jazyk L_D je rozšírením L o istú množinu D nových konštantných symbolov a teória $\widehat{T} \supseteq T$ v jazyku

L_D je úplným henkinovským rozšírením teórie T. Podľa Tvrdenia 4.8.3 je kanonická štruktúra $\mathcal{M}(\widehat{T})$ teórie $\widehat{T}$ modelom tejto teórie, t. j. $\mathcal{M}(\widehat{T}) \models \widehat{T}$. Keďže $T \subseteq \widehat{T}$, platí $\mathcal{M}(\widehat{T}) \models T$, teda $\mathcal{M}(\widehat{T})$ je zároveň modelom teórie T.

Ten, koho znepokojuje fakt, že T je teória v jazyku L, zatiaľ čo $\mathcal{M}(\widehat{T})$ je L_D-štruktúra, môže prejsť k jej zúženiu $\mathcal{A} = M(\widehat{T}) \restriction L$ do jazyka L. Potom $\mathcal{A}$ je už L-štruktúra, a samozrejme $\mathcal{A} \models T$.

Konečne sme v stave dokázať pôvodnú verziu Vety o úplnosti. Uvádzame ju v podobe zahŕňajúcej aj Vetu o korektnosti.

4.8.7 Veta o úplnosti. *Nech T je teória v jazyku prvého rádu L. Potom pre každú L-formulu ψ platí $T \models \psi$ práve vtedy, keď $T \vdash \psi$.*

Demonštrácia. Ak $T \vdash \psi$, tak $T \models \psi$ podľa Vety 4.4.8 o korektnosti. Obrátene pripusťme, že $T \models \psi$, no napriek tomu $T \nvdash \psi$. Bez ujmy na všeobecnosti môžeme predpokladať, že ψ je uzavretá. (Inak môžeme ψ nahradiť sentenciou $(\forall x_1, \ldots, x_n)\psi$, kde $x_1, \ldots, x_n$ sú všetky voľné premenné v ψ, ktorú označíme $\overline{\psi}$. Potom $T \vdash \psi$ práve vtedy, keď $T \vdash \overline{\psi}$, ako aj $T \models \psi$ práve vtedy, keď $T \models \overline{\psi}$.) Keďže ψ je uzavretá, z $T \nvdash \psi$ vyplýva, že teória $T \cup \{\neg\psi\}$ je bezosporná podľa Dôsledku 4.5.3 o dôkaze sporom. Potom podľa Gödelovej vety o úplnosti teória $T \cup \{\neg\psi\}$ má nejaký model $\mathcal{A}$. Teda $\mathcal{A}$ je model teórie T, pričom $\mathcal{A} \models \neg\psi$. No keďže $T \models \psi$, pre každý model $\mathcal{B}$ teórie T musí platiť $\mathcal{B} \models \psi$; špeciálne $\mathcal{A} \models \psi$. Tento spor dokazuje, že $T \vdash \psi$.

4.9 Veta o kompaktnosti

Keď sme už stanovili Gödelovu vetu o úplnosti, môžeme ako jej dôsledok odvodiť prvorádovú verziu Vety o kompaktnosti v zásade rovnakým spôsobom, akým sme odvodili jej zodpovedajúcu verziu vo výrokovom počte. Túto úlohu prenechávame čitateľovi ako cvičenie.

4.9.1 Veta o kompaktnosti. *Nech T je teória v jazyku prvého rádu L. Potom T má nejaký model práve vtedy, keď každá konečná podteória T_0 teórie T má nejaký model.*

No na rozdiel od jej výrokovej verzie, prvorádová verzia Vety o kompaktnosti má rad dôležitých dôsledkov. My sa obmedzíme iba na niekoľko ukážok. Aspoň pri niektorých z nich by čitateľ mal zažiť pocit, že Veta o kompaktnosti umožňuje dokázať existenciu určitých modelov niektorých teórií tak povediac – ak nie doslova – z ničoho.

Pre začiatok by si mal čitateľ uvedomiť nasledujúci bezprostredný dôsledok Vety o kompaktnosti.

4.9.2 Dôsledok. *Nech T, S sú dve teórie v jazyku prvého rádu L. Potom teória $T \cup S$ má nejaký model práve vtedy, keď pre každú konečnú podteóriu $U \subseteq S$ teória $T \cup U$ má nejaký model.*

Hovoríme, že teória T má *ľubovoľne veľké konečné modely*, ak pre každé prirodzené číslo $n \geq 1$ existuje konečný model $\mathcal{A} = (A; \ldots)$ teórie T taký, že $|A| \geq n$.

4.9.3 Veta. *Nech T je teória v jazyku prvého rádu L. Ak T má ľubovoľne veľké konečné modely, tak T má aj nejaký nekonečný model.*

Demonštrácia. Pre každé $n \geq 2$ označíme σ_n nasledujúcu sentenciu v jazyku čistej rovnosti:

$$(\exists\, x_1, \ldots, x_n)\Big(\bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \Big)$$

Potom pre každú L-štruktúru $\mathcal{A} = (A; \ldots)$ máme $\mathcal{A} \vDash \sigma_n$ práve vtedy, keď $|A| \geq n$.

Ďalej pre každé $n \geq 2$ označíme S_n teóriu prvého rádu s axiómami $\sigma_2, \ldots, \sigma_n$ a $S = \{\sigma_n \colon 2 \leq n \in \mathbb{N}\}$ teóriu tvorenú všetkými axiómami σ_n. Očividne, štruktúra prvého rádu $\mathcal{A}$ je nekonečná práve vtedy, keď $\mathcal{A} \vDash S$.

Predpokladajme, že T má ľubovoľne veľké konečné modely. To znamená, že každá z teórií $T \cup S_n$, kde $n \geq 2$, má nejaký model. Avšak pre každú konečnú podteóriu $U \subseteq S$ existuje $n \geq 2$ také, že $U \subseteq S_n$. Keďže každý model teórie $T \cup S_n$ je zároveň modelom teórie $T \cup U$, má aj $T \cup U$ nejaký model. Potom podľa Vety 4.9.1 o kompaktnosti má nejaký model $\mathcal{A}$ aj teória $T \cup S$. Toto $\mathcal{A}$ je nekonečný model teórie T.

4.9.4 Úloha. Nech T je teória prvého rádu v jazyku Teórie unitárnych okruhov φ a je uzavretá formula v tomto jazyku.

(a) Ukážte, že ak má teória T za modely unitárne okruhy ľubovoľne veľkej konečnej charakteristiky, tak má za model aj nejaký unitárny okruh charakteristiky ∞.

(b) Ukážte, že charakteristika poľa je vždy prvočíslo alebo ∞ a dokážte, že ak má teória T za modely polia ľubovoľne veľkej prvočíselnej charakteristiky, tak má za model aj nejaké pole charakteristiky ∞.

(c) Dokážte nasledujúci *Robinsonov princíp*: Ak je sentencia φ splnená v každom poli charakteristiky ∞, tak existuje prvočíslo p také, že φ je splnená v každom poli prvočíselnej charakteristiky $q \geq p$.

Ďalším pozoruhodným dôsledkom Vety o kompaktnosti je existencia neštandardných modelov Peanovej aritmetiky, ktorú ako prvý zaznamenal Thoralf Skolem.

4.9.5 Veta. *Peanova aritmetika má aj neštandardné modely.*

Demonštrácia. Rozšírme jazyk PA o nový konštantný symbol q. Nech χ_n označuje formulu $q \neq n$ v tomto rozšírenom jazyku (spomeňte si, že každé prirodzené číslo n je zároveň konštantný term $(\ldots(0+1)+\ldots+1)+1$ jazyka PA získaný n-násobným pripočítaním 1 k 0).

Zaveďme teórie $S = \{\chi_n \colon n \in \mathbb{N}\}$ a $S_n = \{\chi_0, \chi_1, \ldots, \chi_n\}$ pre každé $n \in \mathbb{N}$. Ak interpretujeme symbol q ako prirodzené číslo $q^{\mathcal{M}_n} = n+1$, dostaneme model $\mathcal{M}_n = (\mathbb{N}; +, \cdot, 0, 1, n+1)$ teórie $\mathrm{PA} \cup S_n$. Z Vety o kompaktnosti potom vyplýva, že aj teória $\mathrm{PA} \cup S$ má nejaký model $\mathcal{M} = (M; +, \cdot, 0, 1, q)$. V tomto modeli je interpretácia $q^{\mathcal{M}} \in M$ symbola q rôzna od všetkých konštantných termov $n \in \mathbb{N}$, teda $(M; +, \cdot, 0, 1)$ je neštandardný model PA.

Intuitívne možno $(M; +, \cdot, 0, 1)$ vnímať ako číselný systém rozširujúci štandardný systém prirodzených čísel $(\mathbb{N}; +, \cdot, 0, 1)$ o nejaké ideálne „nekonečné“ prirodzené čísla,

jedno z ktorých predstavuje interpretácia konštantného symbolu q. Samozrejme, potom $q-1$, $q+1$, $2q$, q^2 atď. predstavujú ďalšie navzájom rôzne nekonečné prvky M. Ba čo viac, ak $p \in M$ je akýkoľvek nekonečný prvok, tak aj prvok $p-1$ je nekonečný; keby totiž $p-1$ bol konečný, bol by konečný aj $p = (p-1)+1$. Teda neprázdna množina všetkých nekonečných prvkov v M nemá najmenší prvok, čo zdanlivo protirečí Princípu dobrého uporiadania, ktorý je dôsledkom Schémy indukcie v PA. Jednako, tento paradox má jednoduché vysvetlenie: Množiny všetkých konečných, resp. nekonečných prvkov v $\mathcal{M}$ sa nedajú vyjadriť v jazyku prvého rádu. To znamená, že neexistujú formuly $\varphi(x, u_1, \ldots, u_n)$, $\psi(x, u_1, \ldots, u_n)$ v jazyku PA a (konečné či nekonečné) prvky $p_1, q_1, \ldots, p_n, q_n \in M$ také, že

$$\{a \in M\colon a \text{ je konečné}\} = \{a \in M\colon \mathcal{M} \vDash \varphi(a, p_1, \ldots, p_n)\}$$
$$\{a \in M\colon a \text{ je nekonečné}\} = \{a \in M\colon \mathcal{M} \vDash \psi(a, q_1, \ldots, q_n)\}$$

Podobnými úvahami sa možno dopracovať k záveru, že existujú aj neštandardné číselné systémy $({}^*\mathbb{R}; +, \cdot, 0, 1)$ rozširujúce štandardný číselný systém $(\mathbb{R}; +, \cdot, 0, 1)$ všetkých reálnych čísel a spĺňajúce všetky axiómy teórie reálne uzavretých polí, vyznačujúce sa rovnakými prvorádovými vlastnosťami ako $(\mathbb{R}; +, \cdot, 0, 1)$. Takéto systémy obsahujú popri štandardných reálnych číslach aj nekonečné (nekonečne veľké) a infinitezimálne (nekonečne malé) číselné veličiny. S ich využitím možno (popri ďalších veciach) vybudovať infinitezimálny (t. j. diferenciálny a integrálny) počet intuitívne pôsobivým spôsobom, blízkym jeho historicky pôvodnej podobe v duchu Newtona, Leibniza, Eulera a ďalších, a tým legalizovať a rehabilitovať tento prístup, ktorý bol v 19. storočí opustený a nahradený technikou limít a $\varepsilon\delta$-analýzou.

4.10 Mohutnosti modelov a Skolemov paradox

Pri podrobnejšom preskúmaní dôkazu Gödelovej vety o úplnosti (tak v paragrafe 4.8 ako aj v paragrafe 4.11) vyjde najavo, že zostrojený model spĺňa navyše istú podmienku týkajúcu sa jeho mohutnosti.

Mohutnosť jazyka prvého rádu $L = (F, C, R, \nu)$ je definovaná ako kardinálne číslo

$$\|L\| = |\operatorname{Form}(L)| = \max(|F|, |C|, |R|, \aleph_0)$$

Jazyk prvého rádu L sa nazýva *spočítateľný*, ak $\|L\| = \aleph_0$. Zrejme každý jazyk s konečne mnohými špecifickými symbolmi je spočítateľný.

Je jasné, že množina K všetkých konštantných termov akéhokoľvek jazyka prvého rádu má mohutnosť $|K| \leq |\operatorname{Term}(L)|$. Nosičom M kanonickej štruktúry $\mathcal{M}(T) = (M; \ldots)$ ľubovoľnej teórie T v jazyku L je faktorová množina $M = K/{\sim_T}$, preto $|M| \leq |K|$. Takže kanonická štruktúra $\mathcal{M}(T) = (M; \ldots)$ akejkoľvek teórie v jazyku prvého rádu L má mohutnosť

$$|M| \leq |K| \leq |\operatorname{Term}(L)| \leq |\operatorname{Form}(L)| = \|L\|$$

Podobne množina D nových konštantných symbolov, pridaná k jazyku L za účelom konštrukcie úplného henkinovského rozšírenia $\widehat{T} = T_H^+$ teórie T, má opäť mohutnosť $\|L\|$. Takže nový jazyk L_D má rovnakú mohutnosť ako pôvodný jazyk L. Ak

to všetko dáme dohromady, vidíme, že i kanonická štruktúra $\mathcal{M}(\widehat{T}) = (M; \dots)$ má mohutnosť $|M| \leq \|L\|$. V dôsledku toho dostávame nasledujúce zosilnenie Gödelovej vety o úplnosti 4.8.6.

4.10.1 Veta. *Nech T je bezosporná teória v jazyku prvého rádu L mohutnosti $\|L\| = \alpha$. Potom T má model $\mathcal{M} = (M; \dots)$ mohutnosti $|M| \leq \alpha$.*

4.10.2 Dôsledok. *Každá bezosporná teória v spočítateľnom jazyku prvého rádu má spočítateľný model, t. j. model $\mathcal{M} = (M; \dots)$ mohutnosti nanajvýš $\aleph_0$.*

Ak si uvedomíme, že obvyklý jazyk Teórie množín obsahuje jediný špecifický symbol, menovite binárny symbol $\in$ relácie náležania prvku do množiny, okamžite dostávame:

4.10.3 Dôsledok. *Každá z teórií* ZF, ZFC *(ak je konzistentná) má nejaký spočítateľný model $\mathcal{M} = \big(M; \in^{\mathcal{M}}\big)$.*

Navyše na základe *Mostowského vety o kolapse* možno zariadiť, že pre všetky $a, b \in M$ platí $a \subseteq M$, ako aj $a \in^{\mathcal{M}} b$ práve vtedy, keď $a \in b$. Potom podľa Vety o korektnosti 4.4.8 všetko, čo možno dokázať v Teórii množín, musí byť splnené v $\mathcal{M}$. Špeciálne musia existovať množiny $\mathbb{N}^{\mathcal{M}}, \mathbb{R}^{\mathcal{M}} \in M$, ktoré zohrávajú úlohu množín všetkých prirodzených, resp. všetkých reálnych čísel v $\mathcal{M}$. Nakoľko však $\mathbb{N}^{\mathcal{M}} \subseteq M$, $\mathbb{R}^{\mathcal{M}} \subseteq M$, obe množiny $\mathbb{N}^{\mathcal{M}}$, $\mathbb{R}^{\mathcal{M}}$ sú spočítateľné, teda (keďže je jasné, že ani jedna z nich nemôže byť konečná) existuje bijektívne zobrazenie $f\colon \mathbb{N}^{\mathcal{M}} \to \mathbb{R}^{\mathcal{M}}$. Na druhej strane, Cantorova veta „*množina $\mathbb{R}$ všetkých reálnych čísel je nespočítateľná*," ktorú možno dokázať v Teórii množín, musí rovnako platiť v $\mathcal{M}$. To znie ako protirečenie.

Tento paradox objavil nórsky matematik Thoralf Skolem v r. 1922. Skolem ho však odvodil z *Löwenheimovej-Skolemovej vety „zhora nadol"* (ktorou sa budeme zaoberať neskôr), a nie z Gödelovej vety o úplnosti (hoci mu bola známa ešte skôr, ako ju Gödel dokázal a uverejnil v r. 1930, no on sám ju nedokázal ani explicitne nesformuloval). Skolemov paradox nie je žiaden spor, ktorý by dokazoval nekonzistentnosť Teórie množín. Možno ho objasniť nasledujúcim spôsobom: Bijekcia $f\colon \mathbb{N}^{\mathcal{M}} \to \mathbb{R}^{\mathcal{M}}$ nepatrí do modelu $\mathcal{M}$; v skutočnosti neexistuje funkcia $f \in M$ stanovujúca bijektívnu korešpondenciu $f\colon \mathbb{N}^{\mathcal{M}} \to \mathbb{R}^{\mathcal{M}}$. Teda Cantorova veta stále platí v $\mathcal{M}$. Neformálne, množina $\mathbb{R}^{\mathcal{M}}$ sa javí ako nespočítateľná iba pri pohľade znútra (t. j. ako množina patriaca do modelu $\mathcal{M}$), zatiaľ čo pri pohľade zvonka je len spočítateľná. Jednako Skolemov paradox naznačuje, že pojmy ako spočítateľnosť alebo nespočítateľnosť, podobne ako viaceré ďalšie množinovo teoretické pojmy týkajúce sa nekonečných kardinálnych čísel, nemajú absolútny, ale iba relatívny charakter.

4.11 Dôkaz vety o úplných henkinovských rozšíreniach

Nech $(A; \leq)$ je čiastočne usporiadaná množina. Prvok $m \in A$ sa nazýva *maximálny*, ak neexistuje prvok $a \in A$ taký, že $m < a$.

Akúkoľvek neprázdnu podmnožinu $\mathcal{T} \subseteq \mathcal{P}(X)$ potenčnej množiny ľubovoľnej množiny X budeme nazývať *systémom podmnožín* množiny X a automaticky považovať

za čiastočne usporiadanú množinu $(\mathcal{T}; \subseteq)$ s reláciou množinovej inklúzie. Hovoríme, že systém $\mathcal{T} \subseteq \mathcal{P}(X)$ podmnožín množiny X má *konečný charakter*, ak pre každé $T \subseteq X$ platí $T \in \mathcal{T}$ práve vtedy, keď $U \in \mathcal{T}$ pre každú konečnú množinu $U \subseteq T$.

Bez dôkazu zaznamenáme nasledujúci dôsledok Axiómy výberu; poznamenajme na okraj, že je s ňou dokonca ekvivalentný.

4.11.1 Teichmüllerova-Tukeyho lema. *Nech X je ľubovoľná množina a $\mathcal{T} \subseteq \mathcal{P}(X)$ je nejaký systém konečného charakteru podmnožín množiny X. Potom pre každé $T \in \mathcal{T}$ existuje maximálny prvok $M \in \mathcal{T}$ taký, že $T \subseteq M$.*

Vezmime za X množinu $\Phi = \mathrm{Form}(L)$ všetkých formúl nejakého jazyka prvého rádu L a označme $\mathcal{T} \subseteq \mathcal{P}(\Phi)$ systém všetkých bezosporných teórií v L. Ako sme už zaznamenali pri dôkaze Vety o kompaktnosti, teória T je bezosporná práve vtedy, keď každá jej konečná podteória $T_0 \subseteq T$ je bezosporná. Inak povedané, systém $\mathcal{T} \subseteq \mathcal{P}(\Phi)$ všetkých bezosporných teórií v jazyku L má konečný charakter. Teda podľa Teichmüllerovej-Tukeyho lemy možno každú bezospornú teóriu T v jazyku prvého rádu L rozšíriť do maximálnej bezospornej teórie $M \supseteq T$ v jazyku L.

4.11.2 Úloha. Nech T je teória v jazyku prvého rádu L. Označme

$$T^{\vdash} = \{\varphi \in \mathrm{Form}(L) \colon T \vdash \varphi\}$$

množinu všetkých L-formúl dokázateľných v T. Ukážte, že T je úplná práve vtedy, keď $T^{\vdash}$ je maximálna bezosporná teória.

Úloha 4.11.2 nám dáva k dispozícii posledný poznatok potrebný na ustanovenie nasledujúceho výsledku.

4.11.3 Lindenbaumova veta. *Každú bezospornú teóriu T v jazyku prvého rádu L možno rozšíriť do úplnej teórie $T^{+} \supseteq T$ v L.*

4.11.4 Poznámka. Hoci Axióma výberu (v istej s ňou ekvivalentnej alternatívnej formulácii) hrala v dôkaze Lindenbaumovej vety kľúčovú úlohu, je známe, že táto veta je slabšia než AC, to znamená, že AC nemožno dokázať v Zermelovej-Fraenkelovej teórii množín za predpokladu Lindenbaumovej vety.

Adolf Lindenbaum Teraz pristúpime k dôkazu výsledku o henkinovských rozšíreniach bezosporných teórií.

4.11.5 Veta o konzervatívnych henkinovských rozšíreniach. *Nech T je bezosporná teória v jazyku prvého rádu $L = (F, C, R, \nu)$. Potom existuje rozšírenie jazyka L o množinu D nových konštantných symbolov do jazyka prvého rádu $L_D = (F, C \cup D, R, \nu)$ a konzervatívne rozšírenie teórie T do henkinovskej teórie $T_H \supseteq T$ v jazyku L_D.*

Demonštrácia. Naším cieľom je vybaviť každú sentenciu $(\exists\, x)\varphi(x)$ novou svedeckou konštantou d_φ a rozšíriť teóriu T o dosvedčujúcu axiómu $(\exists\, x)\varphi(x) \Rightarrow \varphi(d_\varphi)$. No keď to urobíme pre všetky L-formuly $\varphi(x)$, tak zároveň rozšírime aj jazyk L a vzniknú

nové sentencie $(\exists x)\varphi(x)$ dožadujúce sa svojich vlastných svedkov. Preto je potrebné proces rozširovania rekurzívne iterovať.

Označme $L_0 = L$ pôvodný jazyk a Φ_0 množinu všetkých L_0-formúl s jedinou voľnou premennou x. Pre každú formulu $\varphi \in \Phi_0$ zavedieme nový konštantný symbol d_φ tak, že rôznym formulám $\varphi, \psi \in \Phi_0$ zodpovedajú rôzne symboly d_φ, d_ψ. Označíme $D_0 = \{d_\varphi \colon \varphi \in \Phi_0\}$ množinu všetkých týchto konštánt, L_1 rozšírenie jazyka L_0 o množinu nových konštánt D_0 a

$$W_0 = \{(\exists x)\varphi(x) \Rightarrow \varphi(d_\varphi) \colon \varphi \in \Phi_0\}$$

množinu všetkých dosvedčujúcich axióm pre sentencie $(\exists x)\varphi(x)$, kde $\varphi \in \Phi_0$.

Predpokladajúc, že množina formúl Φ_n, množina konštánt $D_n = \{d_\varphi \colon \varphi \in \Phi_n\}$, jazyk L_{n+1} a množina dosvedčujúcich axióm $W_n = \{(\exists x)\varphi(x) \Rightarrow \varphi(d_\varphi) \colon \varphi \in \Phi_n\}$ už boli definované, označíme Φ_{n+1} množinu všetkých formúl jazyka L_{n+1} s jedinou voľnou premennou x, ktoré nepatria do zjednotenia $\bigcup_{k=0}^{n} \Phi_k$. Pre každé $\varphi \in \Phi_{n+1}$ zavedieme nový (t. j. nevyskytujúci sa v jazyku L_{n+1}) konštantný symbol d_φ, pričom rôznym formulám φ, ψ zodpovedajú rôzne symboly d_φ, d_ψ. Ďalej označíme $D_{n+1} = \{d_\varphi \colon \varphi \in \Phi_{n+1}\}$ množinu práve dodaných konštánt, L_{n+2} rozšírenie jazyka L_{n+1} o množinu D_{n+1} týchto konštánt a

$$W_{n+1} = \{(\exists x)\varphi(x) \Rightarrow \varphi(d_\varphi) \colon \varphi \in \Phi_{n+1}\}$$

množinu všetkých dosvedčujúcich axióm pre sentencie $(\exists x)\varphi(x)$, kde $\varphi \in \Phi_{n+1}$.

Nakoniec položíme $D = \bigcup_{n\in\mathbb{N}} D_n$, $W = \bigcup_{n\in\mathbb{N}} W_n$ a označíme L_D rozšírenie jazyka L o množinu nových konštantných symbolov D. Tvrdíme, že $T_H = T \cup W$ je henkinovská teória v jazyku L_D a zároveň konzervatívne rozšírenie teórie T.

Ľahko nahliadneme, že každá L_D-sentencia tvaru $(\exists x)\varphi(x)$ má svedka v teórii T_H. Keďže φ obsahuje len konečne mnoho konštantných symbolov z D (ak vôbec nejaké), existuje najmenšie $n \in \mathbb{N}$ také, že φ neobsahuje žiadny symbol z D_m pre $m \geq n$. Potom $\varphi \in \Phi_n$ a sentencia $(\exists x)\varphi(x) \Rightarrow \varphi(d_\varphi)$ patrí do W_n, teda do T_H. To znamená, že konštantný symbol $d_\varphi \in D$ je svedkom sentencie $(\exists x)\varphi(x)$ v T_H.

Aby sme dokázali, že T_H je konzervatívnym rozšírením T, stačí overiť, že každá L-sentencia ψ dokázateľná v T_H je dokázateľná už v T. Ak $T_H \vdash \psi$, tak existuje konečne veľa dosvedčujúcich axióm θ_i tvaru $(\exists x)\varphi_i(x) \Rightarrow \varphi_i(d_i)$, kde $1 \leq i \leq k$, pričom píšeme d_i namiesto d_{φ_i}, takých, že $T \cup \{\theta_1, \ldots, \theta_k\} \vdash \psi$. Ak $k = 0$, tak $T \vdash \psi$ a sme hotoví; takže môžeme predpokladať, že $k \geq 1$. Zrejme stačí ukázať, že počet k dosvedčujúcich axióm možno vždy znížiť o 1.

Opäť možno nájsť najmenšie n také, že žiadna z formúl $\varphi_1, \ldots, \varphi_k$ neobsahuje žiaden konštantný symbol z D_m pre $m \geq n$. Potom $\varphi_j \in \Phi_n$ pre nejaké $j \in \{1, \ldots, k\}$ a žiadna z dosvedčujúcich sentencií θ_i, kde $i \neq j$, neobsahuje symbol d_j. Kvôli stručnosti označme φ_j ako φ, d_j ako d a $\Theta = \{\theta_i \colon 1 \leq i \leq k,\ i \neq j\}$. Z Vety 4.5.1 o dedukcii dostávame

$$T \cup \Theta \vdash \big((\exists x)\varphi(x) \Rightarrow \varphi(d)\big) \Rightarrow \psi$$

Uvedomme si, že pre ľubovoľné výrokové formy A, B, C nasledujúce výrokové formy

$$((A \Rightarrow B) \Rightarrow C) \Rightarrow (\neg A \Rightarrow C) \qquad \text{a} \qquad ((A \Rightarrow B) \Rightarrow C) \Rightarrow (B \Rightarrow C)$$

sú tautológie, takže podľa Postovej vety o úplnosti 3.8.3 sú dokázateľné výlučne z výrokových logických axióm. Špeciálne obe formuly

$$\big(\big((\exists\, x)\varphi(x) \Rightarrow \varphi(d)\big) \Rightarrow \psi\big) \Rightarrow \big(\neg(\exists\, x)\varphi(x) \Rightarrow \psi\big)$$
$$\big(\big((\exists\, x)\varphi(x) \Rightarrow \varphi(d)\big) \Rightarrow \psi\big) \Rightarrow (\varphi(d) \Rightarrow \psi)$$

sú dokázateľné len z výrokových axióm predikátového počtu. Potom na základe Modus Ponens máme

$$T \cup \Theta \vdash \neg(\exists\, x)\varphi(x) \Rightarrow \psi \qquad \text{ako aj} \qquad T \cup \Theta \vdash \varphi(d) \Rightarrow \psi$$

Nakoľko symbol d sa nevyskytuje v žiadnej zo špecifických axióm teórie $T \cup \Theta$, aplikáciou Lemy 4.7.1 o konštantách na druhý z uvedenej dvojice vzťahov dostávame

$$T \cup \Theta \vdash (\forall\, x)(\varphi(x) \Rightarrow \psi)$$

Keďže ψ je uzavretá, premenná x nie je voľná v ψ, teda podľa (d) a tretej ekvivalencie v (b) Úlohy 4.4.11 o prenexnom normálnom tvare

$$T \cup \Theta \vdash (\exists\, x)\varphi(x) \Rightarrow \psi$$

Toto spolu s prvým z uvedenej dvojice vzťahov na základe Dôsledku 4.5.4 o dôkaze rozborom možností dáva $T \cup \Theta \vdash \psi$. Nakoľko množina Θ pozostáva iba z $k-1$ dosvedčujúcich axióm, sme hotoví.

4.11.6 Úloha. Ukážte priamo, teda bez odvolávania sa na Vetu 4.11.5, že henkinovské rozšírenie T_H bezospornej teórie T zostrojené v jej demonštrácii, je bezosporné. (Možno to urobiť podobným, len trochu jednoduchším spôsobom ako pri demonštrácii konzervatívnosti rozšírenia T_H.)

Kombináciou oboch práve stanovených viet môžeme konečne dokázať avizovaný výsledok.

4.8.5. Veta o úplných henkinovských rozšíreniach. *Nech T je bezosporná teória v jazyku prvého rádu $L = (F, C, R, \nu)$. Potom existuje rozšírenie jazyka L o množinu nových konštantných symbolov D do jazyka prvého rádu $L_D = (F, C \cup D, R, \nu)$ a rozšírenie teórie T do úplnej henkinovskej teórie $\widehat{T} \supseteq T$ v jazyku L_D.*

Demonštrácia. Nech T_H je konzervatívne henkinovské rozšírenie teórie T v jazyku $L_D = (F, C \cup D, R, \nu)$ zostrojené v predchádzajúcej demonštrácii. Potom podľa Lindenbaumovej vety existuje úplná teória $\widehat{T} = T_H^+ \supseteq T_H$ v rovnakom jazyku L_D. Je zrejmé, že $\widehat{T}$ je takisto henkinovská teória.

5 Gödelove vety o neúplnosti

Gödelove vety o neúplnosti patria k najpozoruhodnejším matematickým výsledkom dosiahnutým v 20. storočí, vrhajúcim svetlo na obmedzenia formálnych metód a vyvolávajúcim filozofické otázky o povahe ľudského myslenia, jeho možnostiach a vzťahu k našim mozgom, k počítačom atď.

> *Výsledok Kurta Gödela je v modernej logike ojedinelý a monumentálny – nie je to len monument, je to medzník, ktorý zostane zďaleka viditeľný v priestore a v čase.* [...] *Predmet logiky určite úplne zmenil svoju povahu aj možnosti vďaka Gödelovmu výsledku.*
>
> (John von Neumann)

5.1 Paradox klamára a paradoxy Russella, Cantora a Berryho

Pripomeňme si slávny antický *Paradox klamára*, známy tiež ako *Epimenidov paradox*, zvyčajne pripisovaný Eubulidovi z Milétu. V ňom Kréťan Epimenides vysloví nasledujúcu vetu:

„Všetci Kréťania sú klamári.“

pričom sa mlčky predpokladá, že slovo „klamár“ označuje osobu, ktorá vždy klame. Ak sú vyslovená veta aj zamlčaný predpoklad pravdivé, tak Epimenides musí byť klamár a jeho tvrdenie musí byť tiež lož. Potom však aspoň jeden Kréťan nie je klamár (vo význame, že nie vždy klame). Teda vyslovená veta je nepravdivá, takže Epimenides nám klamal. Toto nie je protirečenie, ale fakt, že vyslovenie jedinej nepravdivej vety nám môže zaručiť existenciu človeka, ktorý nie vždy klame, je stále dosť paradoxný. Silná verzia *Paradoxu klamára* pochádza od stredovekého francúzskeho učenca Jeana Buridana:

„To, čo Vám práve hovorím, je lož.“

Ešte jednoduchšiu formuláciu predstavuje nasledujúca autoreferenčná veta:

„Táto veta je nepravdivá.“

Veta na prvý pohľad vyzerá ako výrok, teda sa zdá byť na mieste spýtať sa: „Je pravdivá alebo nepravdivá?“ Ak je nepravdivá, tak musí byť pravdivá. Podobne, ak je pravdivá, tak nemôže byť pravdivá, teda musí byť nepravdivá. Môžeme uzavrieť, že je pravdivá práve vtedy, keď je nepravdivá. Toto máme na mysli, keď ju nazývame *silnou verziou Paradoxu klamára.*

V bežnom živote nás Paradox klamára príliš trápiť nemusí. Jednoducho ho môžeme odbaviť tým, že spomínanú vetu prehlásime za nezmyselnú a viac sa ňou nebudeme zaoberať. Situácia sa však radikálne zmení, keď sa taká autoreferenčná veta vyskytne

v rámci nejakého formálneho deduktívneho systému, napr. v nejakej axiomatickej teórii prvého rádu. Taká teória bude nevyhnutne protirečivá. A práve to sa stalo v pôvodnej verzii Cantorovej „naivnej“ Teórie množín.

Cantorova teória množín používala pri tvorbe množín neohraničenú verziu *vymedzovacieho princípu*:

Pre každú „rozumnú“ vlastnosť $P(x)$ možno vytvoriť množinu $\{x\colon P(x)\}$ všetkých objektov x s touto vlastnosťou.

Akokoľvek sa nám tento princíp môže zdať intuitívne prijateľný, v skutočnosti je značne nejasný, pokiaľ nevyjasníme, aké vlastnosti považujeme za „rozumné“. Čo je však ešte horšie, tento princíp dovoľuje sformulovať množinovú verziu Paradoxu klamára, menovite *Russellov paradox*, pomenovaný podľa britského logika a filozofa Bertranda Russella:

Cantorov vymedzovací princíp dovoľuje vytvoriť množinu

$$R = \{x\colon x \text{ je množina a } x \notin x\}$$

všetkých množín, ktoré nie sú prvkami samých seba.

Potom otázka: „Je množina R prvkom samej seba?“ vedie okamžite k sporu. Ľahko totiž nahliadneme, že platí $R \in R \Leftrightarrow R \notin R$.

Teda pôvodná verzia Cantorovej Teórie množín je sporná; neohraničený vymedzovací princíp umožňuje zreprodukovať Paradox klamára vnútri tejto teórie.

Paradoxu klamára sa možno vyhnúť zúžením Cantorovho vymedzovacieho princípu do nasledujúcej ohraničenej podoby:

Pre každú množinu M a každú „rozumnú“ vlastnosť $P(x)$ možno vytvoriť množinu $\{x \in M\colon P(x)\}$ všetkých tých objektov x z množiny M, ktoré majú túto vlastnosť.

Tento princíp viac neumožňuje vytvoriť množinu R a Russellov paradox zanikne. Miesto toho nadobudne podobu nasledujúceho faktu:

Neexistuje množina všetkých množín.

Keby totiž množina V všetkých množín existovala, mohli by sme „legálne“ vytvoriť množinu

$$R = \{x \in V\colon x \notin x\}$$

všetkých množín, ktoré nie sú prvkami samých seba, a opäť dostať spor $R \in R \Leftrightarrow R \notin R$.

Ďalší množinový paradox objavil samotný Cantor. Podľa jednej z jeho slávnych viet je mohutnosť akejkoľvek množiny X menšia než mohutnosť jej potenčnej množiny

$$\mathcal{P}(X) = \{A\colon A \subseteq X\}$$

symbolicky $|X| < |\mathcal{P}(X)|$. Ak za X vezmeme množinu V všetkých množín, dostaneme $|V| < |\mathcal{P}(V)|$. Na druhej strane, keďže každý prvok A potenčnej množiny $\mathcal{P}(V)$ je i sám množinou, platí $\mathcal{P}(V) \subseteq V$, a preto $|\mathcal{P}(V)| \leq |V|$, čo je spor. Aj tomuto paradoxu sa možno vyhnúť a zvrátiť ho v tvrdenie, že totalita V všetkých množín netvorí množinu.

Podľa Cantorových vlastných slov, V je „nekonzistentná množina“. Preto na ňu ani nemožno aplikovať konštrukciu potenčnej množiny.

Berryho paradox demonštruje potrebu vyjasniť vágny pojem „rozumnej vlastnosti“, a tým vniesť svetlo do otázky, aké vlastnosti možno používať dokonca aj v ohraničenom vymedzovacom princípe.

Uvažujme množinu A všetkých prirodzených čísel, ktoré možno definovať nejakým slovným spojením slovenského jazyka pozostávajúcim z menej než dvadsiatich slov. Nakoľko slovenčina má konečný slovník, aj slovných spojení v tomto jazyku pozostávajúcich z menej než dvadsiatich slov je len konečne mnoho. Množina A je preto konečná, no keďže prirodzených čísel je nekonečne veľa, existujú prirodzené čísla, ktoré nepatria do množiny A. Inak povedané, jej doplnok $\mathbb{N} \setminus A$ je neprázdny, preto podľa Princípu dobrého usporiadania obsahuje najmenší prvok. Toto prirodzené číslo možno teraz definovať nasledujúcim slovným spojením slovenského jazyka:

„Najmenšie prirodzené číslo, ktoré nemožno definovať žiadnym slovným“ spojením slovenského jazyka pozostávajúcim z menej než dvadsiatich slov.

Uvedené slovné spojenie však má iba sedemnásť slov. Teda najmenší prvok množiny $\mathbb{N} \setminus A$ zároveň patrí do množiny A. Ale to je spor, lebo $A \cap (\mathbb{N} \setminus A) = \emptyset$.

5.2 Hľadanie východiska z krízy

Objavenie sa paradoxov v Cantorovej Teórii množín na prelome 19. a 20. storočia uvrhlo vtedajšiu matematiku do hlbokej krízy. Navyše sa to stalo krátko potom, ako sa Teória množín stala široko akceptovanou a uznávanou ako univerzálna teória poskytujúca celej matematike všeobecný jazyk umožňujúci formulovať rozmanité matematické disciplíny jednotným spôsobom, ako aj spoločné pevné základy, na ktorých by sa mohli ďalej rozvíjať. Nájsť východisko z tejto krízy sa preto stalo takpovediac úlohou dňa.

Niektorí matematici reagovali úplným odmietnutím koncepcie aktuálneho nekonečna, predstavujúcej jeden z uhoľných kameňov Teórie množín (H. Poincaré, L. E. J. Brouwer). Menovite Brouwer sa stal zakladateľom doktríny *intuicionizmu*, podľa ktorej o nekonečne možno uvažovať iba ako o potenciálnom a nikdy nezavŕšenom procese rastu či úbytku za ľubovoľnú hranicu. Taktiež navrhol revíziu logiky, pričom odmietol niektoré klasické logické zákony (napr. zákon vylúčenia tretieho $\varphi \vee \neg\varphi$ alebo zákon kvantifikácie $\neg(\forall x)\neg\varphi(x) \Rightarrow (\exists x)\varphi(x)$) ako nepoužiteľné v oblasti potenciálneho nekoenčna. Konkurenčná doktrína *logicizmu* navrhovala rozvíjať matematiku ako odvetvie logiky (G. Frege, B. Russell, A. N. Whitehead) a vyhnúť sa fenoménu autoreferencie, ktorému sa pripisovala zodpovednosť za protirečenia, pomocou značne zložitej hierarchie *Teórie typov*. No žiadna z týchto koncepcií nemohla súťažiť s prístupmi ponúkanými Teóriou množín, ktorá naplno využívala klasickú logiku, pričom sa dokázala vyhnúť ťažkopádnej hierarchii Teórie typov a zároveň zachovať koncepciu aktuálne nekonečných množín.

Ako sme už spomínali, axiomatický systém teórie množín, ktorý navrhol Ernst Zermelo a neskôr vylepšil Abraham Fraenkel, postupne prevzal úlohu všeobecne akceptovaných základov rozhodujúcej časti modernej matematiky. Paradoxom Russella,

Cantora či Berryho (ako aj ďalším podobným paradoxom) sa podarilo vyhnúť opatrnou formuláciou Schémy vydelenia, povoľujúcej vydeľovať nové množiny iba ako *podmnožiny vopred daných množín* prostredníctvom *množinových formúl*. Ako tri výnimky sa objavujú množiny vymedzené pomocou množinových formúl, nie však z vopred danej množiny, zaručené Axiómami dvojice, zjednotenia a potenčnej množiny. (Pozri 2.7 a 4.3.9.)

Nikomu sa nepodarilo zreprodukovať známe paradoxy ani nájsť akýkoľvek spor vnútri Zermelovho-Fraenkelovho axiomatického systému s Axiómou výberu ZFC. To, žiaľ, nevylučuje možnosť, že nejaké protirečenia v ňom zostávajú ukryté hlboko pod povrchom. To pred nás stavia úlohu *dokázať* bezospornosť ZFC, prípadne nejakého iného axiomatického systému Teórie množín schopného prevziať na seba úlohu základov matematiky. Projekt dokázať bezospornosť základov matematiky sformuloval David Hilbert, vedúca osobnosť vtedajšej matematiky, a zároveň s tým navrhol ústredné pojmy a metódy potrebné na tento účel. Projekt je známy pod názvom *Hilbertov program*.

> *Hilbertov program bol ambiciózny a ďalekosiahly projekt vo filozofii a základoch matematiky. S cieľom „vysporiadať sa s otázkami základov matematiky raz a navždy“, Hilbert v r. 1921 navrhol dvojbodový prístup: po prvé, klasická matematika má byť formalizovaná v axiomatických systémoch; po druhé, bezospornosť týchto axiomatických systémov treba dokázať len s použitím obmedzených „finitných“ prostriedkov. Hoci Gödelova veta o neúplnosti ukazuje, že tento projekt tak, ako bol pôvodne zamýšľaný, nie je uskutočniteľný, Hilbertov program i tak zaznamenal rad dielčích úspechov v logickej teórii aj v metateórii od tých čias až podnes.*
>
> (Richard Zach, *Hilbert's Program Then and Now*, arXiv:math/0508572)

5.3 Gödelove vety o neúplnosti Prípravné úvahy

Uvažujme nasledujúcu autoreferenčnú vetu:

„Táto veta je nedokázateľná.“

mlčky predpokladajúc, že každá dokázateľná veta je nevyhnutne pravdivá. Opäť raz považujeme za oprávnenú otázku: „Je oná veta pravdivá alebo nepravdivá?“ Ak je nepravdivá, tak je dokázateľná, teda musí byť pravdivá. Tento spor ukazuje, že nemôže byť nepravdivá, takže je pravdivá. Tým sme práve dokázali, že oná veta je pravdivá, inak povedané, *dokázali sme* tú vetu. Takže je dokázateľná, a keďže tvrdí svoju vlastnú nedokázateľnosť, je nepravdivá. Zdá sa, že sme opäť dospeli k sporu, nápadne pripomínajúcemu Paradox klamára.

Tomuto záveru sa však môžeme vyhnúť upresnením pojmu dokázateľnosti. Keby znamenal *dokázateľnosť v rámci nejakého formálneho axiomatického systému* (napr. v nejakej teórii prvého rádu), tak náš dôkaz uvedenej vety by bol iba neformálnym intuitívnym zdôvodnením jej pravdivosti, a nie dôkazom v rámci onoho systému. Navyše tvrdenia o dokázateľnosti v rámci daného formálneho systému vo všeobecnosti *nepatria* do toho systému, takže otázka ich dokázateľnosti v jeho rámci vôbec nedáva zmysel. Zdá sa teda, že hroziaci paradox možno zmiesť zo stola od samého začiatku.

Jednako pripusťme, že nejaký formálny systém by mohol spĺňať nasledujúce dve podmienky:

(1) Možno vymedziť dostatočne rozsiahlu význačnú triedu tvrdení sformulovaných v jazyku tohto systému takú, že všetky tvrdenia z tejto triedy, ktoré sú v tom systéme dokázateľné, sú pravdivé v istom intuitívne prijateľnom význame tohto slova.

(2) V tejto význačnej triede sa nachádza tvrdenie, deklarujúce svoju vlastnú nedokázateľnosť v rámci onoho systému.

Potom príslušný systém je nevyhnutne neúplný v nasledujúcom zmysle:

(3) Existujú intuitívne pravdivé tvrdenia sformulované v jazyku tohto systému (dokonca náležiace do onej význačnej triedy), ktoré sú v rámci tohto systému nedokázateľné.

Menovite tvrdenie patriace do onej význačnej triedy a deklarujúce svoju vlastnú nedokázateľnosť v rámci systému je príkladom intuitívne pravdivého tvrdenia, ktoré nie je dokázateľné v rámci tohto systému.

V tejto chvíli asi čitateľ sotva dokáže potlačiť v sebe pocit, že existencia takých formálnych systémov (teórií prvého rádu) je čisto hypotetická a v skutočnosti by sa malo dať dokázať, že niečo také nemôže existovať. Takže to, čo v roku 1930 dokázal mladý rakúsky matematik, logik a filozof Kurt Gödel (1906, Brno – 1978, Princeton), sa môže javiť ako dosť prekvapivé. Podľa jeho *Prvej vety o neúplnosti* sú totiž Peanova aritmetika, ako aj akákoľvek teória prvého rádu schopná na seba prevziať úlohu základov matematiky, ako napr. ZF alebo ZFC, či Principia Mathematica, príkladmi takých axiomatických systémov. Podľa jeho *Druhej vety o neúplnosti* sú takéto systémy v stave sformulovať tvrdenie deklarujúce ich vlastnú bezospornosť, jednako, pokiaľ sú naozaj bezosporné, nie sú schopné toto tvrdenie dokázať, i keď v tom prípade je samotné toto tvrdenie pravdivé. Ako jeden z dôsledkov Gödelových objavov sa ukázalo, že ciele Hilbertovho programu nie je možné naplniť.

5.4 Prvá Gödelova veta o neúplnosti

Stojí za zmienku, že Gödel pracoval v intenciách Hilbertovho programu a jeho Vety o neúplnosti sa vynorili takpovediac po ceste, bez toho aby boli vopred plánované alebo očakávané. V našom výklade preskočíme väčšinu technických podrobností Gödelovho dôkazu a začneme rovno niektorými finálnymi výsledkami jeho kódovania formúl a dôkazov prirodzenými číslami a reprezentáciou vzťahu dokázateľnosti istým aritmetickým predikátom. Upozorňujeme, že naša prezentácia sa značne líši od Gödelovho pôvodného prístupu.

Neformálne Prvá Gödelova veta o neúplnosti hovorí, že každý konzistentný formálny systém, ktorý je dosť obsiahly na to, aby v sebe zahŕňal Peanovu aritmetiku, je nevyhnutne neúplný, či už v tom zmysle, že obsahuje nejaké pravdivé tvrdenia o prirodzených číslach, ktoré nevie dokázať (sémantická verzia), alebo v tom zmysle, že obsahuje nejaké aritmetické tvrdenia, ktoré nevie dokázať ani vyvrátiť (syntaktická verzia).

Začnime s pojmami nevyhnutnými na presnejší opis variety teórií prvého rádu, na ktoré sa Gödelove výsledky vzťahujú. Teória prvého rádu T v jazyku s konečným

počtom špecifických symbolov sa nazýva *rekurzívne axiomatizovateľná*, ak má len konečne mnoho axióm alebo jej axiómy možno efektívne rozpoznať nejakým algoritmom (napr. počítačovým programom). Teória prvého rádu T sa nazýva *aritmetická*, ak existuje nejaká interpretácia Peanovej aritmetiky v tejto teórií. To znamená, že máme k dispozícii nejaké formuly $\mathrm{Nat}(x)$, $\mathrm{Add}(x,y,z)$, $\mathrm{Mult}(x,y,z)$, $\mathrm{Zero}(x)$, $\mathrm{One}(x)$ v jazyku teórie T, definujúce pojem prirodzeného čísla, operácie sčítania a násobenia a význačné prvky 0 a 1 takým spôsobom, že pre takto získanú štruktúru prirodzených čísel možno v teórii T dokázať platnosť všetkých axióm teórie PA. Ak T je aritmetická teória, tak formulu φ v jej jazyku nazveme *aritmetickou*, ak je vybudovaná z „nových" atomických formúl tvaru $x = y$, $\mathrm{Add}(x,y,z)$, $\mathrm{Mult}(x,y,z)$, $\mathrm{Zero}(x)$, $\mathrm{One}(x)$ pomocou logických spojok a *ohraničených kvantifikácií* $(\forall\, x)(\mathrm{Nat}(x) \Rightarrow \varphi)$, $(\exists\, x)(\mathrm{Nat}(x) \wedge \varphi)$. Aritmetická teória T sa nazýva *aritmeticky korektná*, ak všetky aritmetické sentencie dokázateľné v T sú splnené v $(\mathbb{N}; +, \cdot, 0, 1)$.

Príkladom rekurzívne axiomatizovanej aritmeticky korektnej teórie je zrejme samotná Peanova aritmetika. Ďalšími paradigmatickými príkladmi takých teórií sú rekurzívne rozšírenia PA pomocou axióm splnených v $(\mathbb{N}; +, \cdot, 0, 1)$, ako aj rozmanité teórie množín, napr. ZF alebo ZFC.

Budeme hovoriť, že daná aritmetická sentencia θ je *pravdivá* alebo *platná* alebo *splnená*, ak je splnená v štandardnom modeli Peanovej aritmetiky $(\mathbb{N}; +, \cdot, 0, 1)$. Pre aritmetickú sentenciu tvaru $\psi(k_1, \ldots, k_n)$, kde $\psi(x_1, \ldots, x_n)$ je aritmetická formula a $k_1, \ldots, k_n$ sú konkrétne prirodzené čísla (konštantné aritmetické termy), v tom prípade zvykneme hovoriť, že $\psi(k_1, \ldots, k_n)$ *platí* alebo jednoducho $\psi(k_1, \ldots, k_n)$.

Gödel vypracoval metódu *kódovania* alebo *enumerácie*, pomocou ktorej všetky aritmetické formuly v jazyku aritmetickej teórie T s jednou voľnou premennou x možno zoradiť do postupnosti $\varphi_0(x), \varphi_1(x), \ldots, \varphi_n(x), \ldots$ takým spôsobom, že pre každé n možno formulu $\varphi_n(x)$ efektívne zostrojiť (napr. programom), a tiež naopak pre každú aritmetickú formula $\psi(x)$ možno efektívne určiť jej číslo n také, že $\psi(x)$ splýva s $\varphi_n(x)$. Ak T je navyše rekurzívne axiomatizovateľná, tak aj všetky dôkazy v T možno zoradiť do postupnosti $\Delta_0, \Delta_1, \ldots, \Delta_k, \ldots$ takým spôsobom, že korešpondenciu $k \leftrightarrow \Delta_k$ možno efektívne popísať (napr. pomocou nejakého programu) v oboch smeroch. Navyše v tom prípade Gödel zostrojil dva efektívne rozhodnuteľné ternárne aritmetické predikáty $P(x,y,z)$ a $R(x,y,z)$ dokázateľnosti (provability), resp. vyvrátiteľnosti (refutability) také, že pre ľubovoľné prirodzené čísla k, m, n sú splnené nasledujúce podmienky:

$P(m,n,k)$ práve vtedy, keď Δ_k je dôkaz sentencie $\varphi_n(m)$ v T

$R(m,n,k)$ práve vtedy, keď Δ_k je dôkaz sentencie $\neg\varphi_n(m)$ v T

Algoritmická rozhodnuteľnosť predikátov $P(x,y,z)$ a $R(x,y,z)$ zároveň zaručuje, že pre akúkoľvek voľbu $m, n, k \in \mathbb{N}$ je platnosť ľubovoľného z tvrdení $P(m,n,k)$, $\neg P(m,n,k)$, $R(m,n,k)$, $\neg R(m,n,k)$ v $(\mathbb{N}; +, \cdot, 0, 1)$ ekvivalentná jeho dokázateľnosti v PA, teda aj v T. Totiž algoritmus, ktorý rozhodne, či $P(m,n,k)$ platí alebo nie, zároveň poskytuje dôkaz tvrdenia $P(m,n,k)$ alebo jeho negácie, a podobne pre $R(m,n,k)$. Takže môžeme zhrnúť:

5.4.1 Veta. *Predpokladajme, že T je konzistentná rekurzívne axiomatizovateľná aritmetická teória. Potom pre ľubovoľné prirodzené čísla m, n, k sú tri podmienky*

v každom z nasledujúcich štyroch riadkov navzájom ekvivalentné:

$$\begin{array}{rll} P(m,n,k), & T \vdash P(m,n,k), & \Delta_k \text{ je dôkaz sentencie } \varphi_n(m) \text{ v } T \\ R(m,n,k), & T \vdash R(m,n,k), & \Delta_k \text{ je dôkaz sentencie } \neg\varphi_n(m) \text{ v } T \\ \neg P(m,n,k), & T \nvdash P(m,n,k), & T \vdash \neg P(m,n,k) \\ \neg R(m,n,k), & T \nvdash R(m,n,k), & T \vdash \neg R(m,n,k) \end{array}$$

Špeciálne T rozhodne každé z tvrdení $P(m,n,k)$ a $R(m,n,k)$ pre ľubovoľné m, n, k.

Teraz už máme k dispozícii všetky ingrediencie potrebné na formuláciu Gödelových výsledkov. Uvažujme formulu $\neg(\exists\, z)P(x,x,z)$. Obsahuje jedinú voľnú premennú x, teda sa vyskytuje v postupnosti $\{\varphi_n(x)\}_{n\in\mathbb{N}}$ pod nejakým číslom – označme ho g. Potom $\varphi_g(x)$ je uvedená forrmula, a keď do nej dosadíme prirodzené číslo g miesto premennej x, dostaneme tvrdenie $\varphi_g(g)$, t. j. $\neg(\exists\, z)P(g,g,z)$, ktoré hovorí, že pre žiadne $z = k$ nie je Δ_k dôkaz tvrdenia $\varphi_g(g)$. Inak povedané, význam tohto tvrdenia je:

$$\varphi_g(g)\colon \quad \textit{„Tvrdenie } \varphi_g(g) \textit{ nie je dokázateľné v } T.\text{“}$$

Teda $\varphi_g(g)$ je príkladom autoreferenčného tvrdenia v jazyku teórie T vyhlasujúceho svoju vlastnú nedokázateľnosť. Na druhej strane by si čitateľ mal uvedomiť, že $\varphi_g(g)$ je aritmetické tvrdenie, ako napr. $\neg(\exists\, x,y,z)\big((x+1)^2+(y+2)^3=(z+3)^4\big)$, ktoré tvrdí, že diofantická rovnica $(x+1)^2+(y+2)^3=(z+3)^4$ nemá riešenie v obore všetkých prirodzených čísel.

Naše prípravné úvahy (pozri 5.3) nás teraz oprávňujú vysloviť sémantickú verziu Prvej Gödelovej vety o neúplnosti.

5.4.2 Prvá Gödelova veta o neúplnosti. [Sémantická verzia] *Ak T je rekurzívne axiomatizovateľná aritmeticky korektná teória prvého rádu, tak Gödelovo tvrdenie $\varphi_g(g)$ je splnené v $(\mathbb{N};+,\cdot,0,1)$, jednako však nie je dokázateľné v T. Takže T nie je v stave dokázať všetky pravdivé aritmetické tvrdenia o prirodzených číslach.*

Teda špeciálne PA ani žiadna z teórií množín, ako napr. ZF alebo ZFC, nemôžu dokázať všetky pravdivé aritmetické tvrdenia o prirodzených číslach.

Keďže k nekonečnému oboru $\mathbb{N}$ všetkých prirodzených čísel nemáme priamy prístup, sémantický pojem aritmetickej pravdy, ktorý hrá kľúčovú úlohu v sémantickej verzii Prvej Gödelovej vety o neúplnosti, „zaváňa metafyzikou“ a môže v čitateľovi vyvolať isté rozpaky. Zakladá sa na našej viere, že $(\mathbb{N};+,\cdot,0,1)$ je model PA, čo však možno sotva považovať za zrejmý či pevne a nespochybniteľne ustanovený fakt. Jednako, táto viera je dokonca silnejšia než viera v bezospornosť PA, ktorá sa však rovnako nezakladá na priamej, bezprostrednej evidencii. Každopádne bude zaujímavé vidieť, čo môžeme odvodiť z tohto slabšieho syntaktického predpokladu.

5.4.3 Prvá Gödelova veta o neúplnosti. [Syntaktická verzia] *Nech T je rekurzívne axiomatizovateľná aritmetická teória.*

(a) *Ak T je bezosporná, tak Gödelovo tvrdenie $\varphi_g(g)$ nie je dokázateľné v T.*

(b) *Ak T je ω-konzistentná, tak ani tvrdenie $\neg\varphi_g(g)$ nie je dokázateľné v T.*

Takže z predpokladu ω-konzistentnosti teórie T vyplýva, že T je neúplná.

Poznamenajme, že ω-konzistentnosť je technická podmienka, silnejšia než púha konzistentnosť (bezospornosť), ktorú sformulujeme počas demonštrácie časti (b).

Demonštrácia. (a) Predpokladajme, že tvrdenie $\varphi_g(g)$ je dokázateľné v T. Z tohto bodu môžeme postupovať dvoma spôsobmi. Predvedieme si ich oba.

Po prvé, dokázateľnosť $\varphi_g(g)$ znamená, že táto sentencia má nejaký dôkaz v T, povedzme Δ_k. Potom platí $P(g,g,k)$, a v dôsledku algoritmického charakteru predikátu $P(x,y,z)$, je tvrdenie $P(g,g,k)$ dokázateľné v T. Preto aj $(\exists\, z)P(g,g,z)$, čo je ekvivalentné s $\neg\varphi_g(g)$, je dokázateľné v T. Takže máme $T \vdash \varphi_g(g)$ a zároveň $T \vdash \neg\varphi_g(g)$, čo protirečí bezospornosti teórie T.

Druhý argument začína uvedomením si tvaru tvrdenia $\varphi_g(g)$: vlastne predpokladáme, že $T \vdash \neg(\exists\, z)P(g,g,z)$, čiže $T \vdash (\forall\, z)\neg P(g,g,z)$, keďže druhé tvrdenie je ekvivalentné s prvým. Preto $T \vdash \neg P(g,g,k)$ pre každé $k \in \mathbb{N}$. Podľa Vety 5.4.1 potom $\neg P(g,g,k)$ platí pre každé k. To znamená, že žiaden z dôkazov Δ_k nie je dôkazom sentencie $\varphi_g(g)$ v T, inak povedané, tvrdenie $\varphi_g(g)$ nie je dokázateľné v T. To protirečí nášmu pôvodnému predpokladu, ktorý je z toho dôvodu chybný. Takže $\varphi_g(g)$ je nedokázateľné v T.

(b) Predpokladajme, že tvrdenie $\neg\varphi_g(g)$, ktoré je ekvivalentné s $(\exists\, z)P(g,g,z)$, je dokázateľné v T. Keby existovalo nejaké $k \in \mathbb{N}$ také, že $P(g,g,k)$, mohli by sme usúdiť, že Δ_k je dôkaz tvrdenia $\varphi_g(g)$ v T. Potom by obe tvrdenia $\varphi_g(g)$ ako aj $\neg\varphi_g(g)$ boli dokázateľné v T, a mohli by sme vyvrátiť náš počiatočný predpoklad $T \vdash \neg\varphi_g(g)$ iba na základe bezospornosti teórie T (a zaobísť sa bez predpokladu jej ω-konzistentnosti).

Vyplýva teda z dokázateľnosti aritmetickej sentencie $(\exists\, z)P(g,g,z)$ existencia nejakého $k \in \mathbb{N}$ takého, že $P(g,g,k)$? Súhlasná odpoveď na túto otázku sa na prvý pohľad zdá samozrejmou. Keby sme mali konštruktívny dôkaz tvrdenia $(\exists\, z)P(g,g,z)$, ten by nám dal konkrétne k také, že $P(g,g,k)$. Bohužiaľ nevieme vylúčiť, že dôkaz tvrdenia $(\exists\, z)P(g,g,z)$ postupuje nepriamym nekonštruktívnym spôsobom, iba vyvodením sporu z predpokladu $\neg(\exists\, z)P(g,g,z)$, a nedáva nám ani žiaden návod, ako by sme nejaké také k, pre ktoré platí $P(g,g,k)$, mali hľadať. Musíme konštatovať, že náš optimizmus bol predčasný a naša pôvodná predstava o demonštrácii tejto časti nefunguje. Ak sa chceme dostať ďalej, potrebujeme čosi viac.

Aritmetická teória T sa nazýva *ω-konzistentná*, ak pre žiadnu aritmetickú formulu $\psi(z)$ nemôžu byť v T zároveň dokázateľné tvrdenie $(\exists\, z)\psi(z)$ ako aj všetky tvrdenia $\neg\psi(0)$, $\neg\psi(1)$, …, $\neg\psi(k)$, …. Zrejme každá ω-konzistentná aritmetická teória musí byť konzistentná.

Ak teraz predpokladáme, že T je ω-konzistentná a $T \vdash (\exists\, z)P(g,g,z)$, môžeme z toho vyvodiť, že $T \nvdash \neg P(g,g,k)$ pre nejaké k. Pre toto k podľa Vety 5.4.1 platí $P(g,g,k)$. V tejto chvíli už môžeme použiť náš pôvodný argument.

Nasledujúci príklad ilustruje rozdiel medzi čisto existenčným a konštruktívnym dôkazom nejakého existenčného tvrdenia.

5.4.4 Príklad. Dokážeme nasledujúcu vetu:

„Existujú iracionálne čísla $a, b > 0$ také, že číslo a^b je racionálne.“

Dôkaz. Je známe (a ľahko sa dokáže), že $\sqrt{2}$ je iracionálne číslo. Potom číslo $\sqrt{2}^{\sqrt{2}}$ je buď racionálne alebo iracionálne. Ak je racionálne, sme hotoví: stačí položiť $a = b = \sqrt{2}$. Ak $\sqrt{2}^{\sqrt{2}}$ je iracionálne, položíme $a = \sqrt{2}^{\sqrt{2}}$ a $b = \sqrt{2}$. Potom a aj b sú iracionálne a platí

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\left(\sqrt{2}\,\sqrt{2}\right)} = \left(\sqrt{2}\right)^2 = 2$$

Keďže $a^b = 2$ je očividne racionálne číslo, opäť sme hotoví.

Čitateľ by si mal uvedomiť, že náš dôkaz je čisto existenčný a využíva Zákon vylúčenia tretieho. Nevieme, či číslo $\sqrt{2}^{\sqrt{2}}$ je racionálne alebo iracionálne, takže nevieme, ktorá z oboch možností naozaj funguje. Z intuicionistického alebo konštruktivistického hľadiska sú také dôkazy neprijateľné. Konštruktívny dôkaz by si vyžadoval rozhodnúť, či je číslo $\sqrt{2}^{\sqrt{2}}$ racionálne alebo iracionálne, a urobiť explicitnú, jednoznačnú voľbu dvojice a, b.

V skutočnosti sa vie že číslo $\sqrt{2}^{\sqrt{2}}$ je iracionálne (no nie je to také ľahké dokázať), teda v uvedenom dôkaze nastáva druhá možnosť.

5.4.5 Úloha. Predpokladajte, že Peanova aritmetika je bezosporná a henkinovská teória. Dokážte, že potom je už nevyhnutne ω-konzistentná. (*Pomôcka*: Vychádzajte z toho, že každý konštantný term v jazyku teórie PA sa v PA dokázateľne rovná niektorému termu tvaru $(\ldots(0+1)+\cdots+1)+1$ (n jednotiek), t. j. štandardnému prirodzenému číslu n.)

Neskôr Barkley Rosser sformuloval modifikáciu Gödelovho tvrdenia $\neg(\exists\, z)P(g,g,z)$ umožňujúcu zaobísť sa bez predpokladu ω-konzistentnosti a dokázať neúplnosť rekurzívne axiomatizovateľných aritmetických teórií iba na základe predpokladu ich púhej konzistentnosti.

Uvažujme aritmetickú formulu $(\forall\, z)(P(x,x,z) \Rightarrow (\exists\, u \leq z)R(x,x,u))$ a označme r jej číslo v zozname $\{\varphi_n(x)\}_{n\in\mathbb{N}}$. Dosadením r za x do formuly $\varphi_r(x)$ dostaneme autoreferenčné tvrdenie $\varphi_r(r)$, čiže

$$(\forall\, z)(P(r,r,z) \Rightarrow (\exists\, u \leq z)R(r,r,u))$$

Jeho zmysel možno dešifrovať takto:

$\varphi_r(r)$: „*Ak je tvrdenie $\varphi_r(r)$ dokázateľné v T nejakým dôkazom s daným číslom, tak medzi dôkazmi s číslom menším alebo rovným tomuto číslu sa nachádza dôkaz jeho negácie $\neg\varphi_r(r)$ v T.*“

Snáď ani netreba zvlášť zdôrazňovať, že nasledujúca verzia Prvej vety o neúplosti má syntaktický charakter.

5.4.6 Gödelova-Rosserova veta o neúplnosti. *Nech T je ľubovoľná rekurzívne axiomatizovateľná aritmetická teória. Ak T je bezosporná, tak ani Rosserovo tvrdenie $\varphi_r(r)$ ani jeho negácia $\neg\varphi_r(r)$ nie sú dokázateľné v T. Preto ak T je bezosporná, tak je neúplná.*

Demonštrácia. Predpokladajme, že tvrdenie $\varphi_r(r)$ je dokázateľné a Δ_k je jeho dôkaz v T. Potom obe tvrdenia $P(r,r,k)$ aj $(\exists\, u \leq k)R(r,r,u)$ sú dokázateľné v T. Druhé z nich je ekvivalentné s alternatívou

$$R(r,r,0) \vee R(r,r,1) \vee \ldots \vee R(r,r,k)$$

Potom však stačí prebrať dôkazy Δ_0, Δ_1, ..., Δ_k a máme zaručené, že sa medzi nimi nachádza dôkaz tvrdenia $\neg\varphi_r(r)$ v teórii T, čo protirečí jej bezospornosti.

Teraz predpokladajme, že tvrdenie $\neg\varphi_r(r)$ je dokázateľné v T dôkazom Δ_l. Potom platí $R(r,r,l)$, a algoritmus potvrdzujúci tento fakt poskytuje dôkaz tvrdenia $R(r,r,l)$ v T. Ak si uvedomíme, že $\neg\varphi_r(r)$ je ekvivalentné s tvrdením

$$(\exists\, z)\big(P(r,r,z) \wedge (\forall\, u)(R(r,r,u) \Rightarrow z < u)\big)$$

môžeme usúdiť, že tvrdenie $(\exists\, z < l)P(r,r,z)$ je dokázateľné v T. Potom nevyhnutne $l > 0$, a posledné tvrdenie je ekvivalentné s alternatívou

$$P(r,r,0) \vee P(r,r,1) \vee \ldots \vee P(r,r,l-1)$$

To znamená, že medzi dôkazmi Δ_0, Δ_1, ..., Δ_{l-1} sa nachádza dôkaz tvrdenia $\varphi_r(r)$ v T, čo opäť odporuje bezospornosti teórie T.

5.5 Druhá Gödelova veta o neúplnosti

Neformálne Druhá Gödelova veta o neúplnosti hovorí, že žiadny formálny systém dosť bohatý na to, aby v sebe zahŕňal Peanovu aritmetiku, nie je schopný dokázať vlastnú bezospornosť. Treba si však uvedomiť, že tvrdenie o bezospornosti nejakého formálneho systému je tvrdením *o tomto systéme*, ktoré nie je ani formulované v jeho jazyku, takže otázka dokázateľnosti tohto tvrdenia v rámci systému vôbec nedáva zmysel. Preto je nanajvýš dôležité poznanie, že niektoré formálne systémy, špeciálne všetky rekurzívne axiomatizovateľné aritmetické teórie prvého rádu, formuláciu takýchto tvrdení umožňujú.

Ak máme danú aritmetickú teóriu T, tak aritmetickú sentenciu θ nazveme *prehlásením o bezospornosti* teórie T, ak bezospornosť teórie T je ekvivalentná s platnosťou tvrdenia θ v $(\mathbb{N};\, +, \cdot, 0, 1)$. Ak T je navyše rekurzívne axiomatizovateľná, tak máme viacero možností ako formulovať prehlásenie o jej bezospornosti.

(1) Pripomeňme, že teória T v jazyku prvého rádu L je sporná práve vtedy, keď existuje uzavretá formula ψ jazyka L taká, že ψ aj $\neg\psi$ sú dokázateľné v T. Vzhľadom na to možno prehlásenie o bezospornosti rekurzívne axiomatizovateľnej aritmetickej teórie T formulovať nasledujúcim sugestívnym spôsobom

$$\mathrm{Cons}_1(T)\colon \neg(\exists\, x, y, z, u)(P(x,y,z) \wedge R(x,y,u))$$

vylučujúcim existenciu akejkoľvek sentencie tvaru $\varphi_n(m)$, ktorá by bola dokázateľná v T zároveň so svojou negáciou $\neg\varphi_n(m)$.

(2) Ekvivalentne, T je sporná práve vtedy, keď *každá* L-sentencia je dokázateľná v T. Teda T je bezosporná práve vtedy, keď aspoň jedna L-sentencia ψ nie je dokázateľná v T. Pri výbere takejto sentencie máme značnú voľnosť. Môžeme si napríklad zvoliť úspornú cestu navrhnutú Johnom von Neumannom a vybrať na ten účel Gödelovo tvrdenie $\varphi_g(g)$. Skutočne, ak $\varphi_g(g)$ je dokázateľné v T, tak, ako sme už videli, T je sporná. Naopak, ak $\varphi_g(g)$ je nedokázateľné v T, tak T je samozrejme konzistentná. Takže T je konzistentná práve vtedy, keď $\varphi_g(g)$ nie je dokázateľné v T. To nám dáva prehlásenie o bezospornosti

$$\mathrm{Cons}_2(T)\colon \neg(\exists\, z)P(g,g,z),$$

ktoré sa zhoduje so skôr zavedeným Gödelovým tvrdením $\varphi_g(g)$.

(3) Nakoniec si môžeme zvoliť nejakú logickú axiómu alebo axiómu teórie PA; potom požiadavka nedokázateľnosti jej negácie je zrejme ekvivalentná s bezospornosťou teórie T. Nech napr. $s \in \mathbb{N}$ je číslo formuly $x \neq x$. Potom $\varphi_s(0)$ je sentencia $0 \neq 0$. Takto dostávame ďalšie prehlásenie o bezospornosti

$$\mathrm{Cons}_3(T)\colon \neg(\exists\, z)P(0,s,z)$$

vyjadrujúce nedokázateľnosť tvrdenia $0 \neq 0$ v T.

5.5.1 Úloha. (a) Keď sme sa zaoberali syntaktickou verziou Prvej Gödelovej vety o neúplnosti, ukázali sme, že z dokázateľnosti Gödelovho tvrdenia $\varphi_g(g)$ v T vyplýva dokázateľnosť jeho negácie $\neg\varphi_g(g)$ v T. Považujte za zaručené, že implikácia

$$(\exists\, z)P(g,g,z) \Rightarrow (\exists\, u)R(g,g,u)$$

ktorá formalizuje túto úvahu, je dokázateľná v T, a dokážte, že potom aj implikácia

$$\neg(\exists\, x,y,z,u)(P(x,y,z) \wedge R(x,y,u)) \Rightarrow \neg(\exists\, z)P(g,g,z)$$

je dokázateľná v T. To znamená, že dokázateľnosť prehlásenia o bezospornosti $\mathrm{Cons}_1(T)$ z (1) v T by mala za následok dokázateľnosť Gödelovho tvrdenia $\varphi_g(g)$.

(b) Podobne ako v (a), môžeme odvodiť, že dokázateľnosť Gödelovho tvrdenia $\varphi_g(g)$ by mala za následok dokázateľnosť tvrdenia $0 \neq 0$ v T. Považujte za zaručené, že implikácia

$$(\exists\, z)P(g,g,z) \Rightarrow (\exists\, u)P(0,s,u)$$

ktorá formalizuje túto úvahu, je dokázateľná v T, a dokážte, že potom dokázateľnosť prehlásenia o bezospornosti $\mathrm{Cons}_3(T)$ z (3) v T by mala opäť za následok dokázateľnosť Gödelovho tvrdenia $\varphi_g(g)$.

To znamená, že pre rekurzívne axiomatizovateľnú aritmetickú teóriu T s predikátom dokázateľnosti $P(x,y,z)$, prípadne aj s predikátom vyvrátiteľnosti $R(x,y,z)$, možno sformulovať prehlásenie o bezospornosti $\mathrm{Cons}(T)$ v jej jazyku v tvare ktorejkoľvek z uvedených troch sentencií $\mathrm{Cons}_1(T)$, $\mathrm{Cons}_2(T)$, $\mathrm{Cons}_3(T)$ (ako aj mnohých ďalších). Zároveň predpoklad o dokázateľnosti ktoréhokoľvek z týchto prehlásení v T má za následok dokázateľnosť Gödelovho tvrdenia $\varphi_g(g)$ v T. Keď si to všetko zhrnieme, dostávame:

5.5.2 Druhá Gödelova veta o neúplnosti. *Nech T je rekurzívne axiomatizovateľná aritmetická teória. Potom T umožňuje sformulovať prehlásenie o svojej vlastnej bezospornosti* $\mathrm{Cons}(T)$. *Ak je však T bezosporná, tak žiadne z prehlázení o jej bezospornosti* $\mathrm{Cons}_1(T)$, $\mathrm{Cons}_2(T)$, $\mathrm{Cons}_3(T)$ *z uvedeného zoznamu nie je dokázateľné v T.*

Ak T je konzistentná rekurzívne axiomatizovateľná aritmetická teória, tak podľa Druhej Gödelovej vety o neúplnosti tvrdenie $\mathrm{Cons}(T)$ nie je dokázateľné v T, preto podľa Dôsledku 4.5.3 o dôkaze sporom je konzistentné aj jej rozšírenie $T\cup\{\neg\,\mathrm{Cons}(T)\}$. Nakoľko však T je konzistentná, nová axióma $\neg\,\mathrm{Cons}(T)$ nie je splnená v $(\mathbb{N};\,+,\cdot,0,1)$, teda $T\cup\{\neg\,\mathrm{Cons}(T)\}$ nemôže byť aritmeticky korektná, aj keby T bola. Ďalej kvôli určitosti označíme $\mathrm{Cons}(T)$ Gödelovo tvrdenie $\varphi_g(g)$. Potom tvrdenie $(\exists\,z)P(g,g,z)$, logicky ekvivalentné s negáciou $\neg\,\mathrm{Cons}(T)$, je dokázateľné v $T\cup\{\neg\,\mathrm{Cons}(T)\}$. Nakoľko však T je bezosporná, žiaden z dôkazov Δ_k nemôže byť dôkazom tvrdenia $\varphi_g(g)$, t. j. $\mathrm{Cons}(T)$, v T, takže všetky tvrdenia $\neg P(g,g,k)$ pre $k\in\mathbb{N}$ sú splnené v $(\mathbb{N};\,+,\cdot,0,1)$, teda dokázateľné v T, a tým skôr v $T\cup\{\neg\,\mathrm{Cons}(T)\}$. To znamená, že $T\cup\{\neg\,\mathrm{Cons}(T)\}$ je príkladom konzistentnej teórie, ktorá nie je ω-konzistentná. Na druhej strane, ak T je aritmeticky korektná, tak aj $T\cup\{\mathrm{Cons}(T)\}$ má túto vlastnosť.

V nasledujúcich dvoch úlohách T označuje rekurzívne axiomatizovateľnú aritmetickú teóriu s predikátom dokázateľnosti $P(x,y,z)$ a predikátom vyvrátiteľnosti $R(x,y,z)$.

5.5.3 Úloha. Úvodná úvaha v (2) ponúka nasledujúcu formalizáciu prehlásenia o bezospornosti teórie T

$$\mathrm{Cons}_4(T)\colon (\exists\,x,y)(\forall\,z)\neg P(x,y,z)$$

deklarujúcu existenciu nejakej uzavretej formuly $\varphi_n(m)$ nedokázateľnej v T. Avšak skutočnosť, že syntaktická zložitosť formuly je (v dôsledku prefixu kvantifikátorov $\exists\,\forall$) o stupeň vyššia než u troch predchádzajúcich prehlásení o bezospornosti, spôsobuje, že nie je také ľahké odvodiť akékoľvek závery z predpokladu dokázateľnosti tvrdenia $\mathrm{Cons}_4(T)$ v T.

(a) Dokážte, že tvrdenie $\mathrm{Cons}_4(T)$ je prehlásením o bezospornosti teórie T.

(b) Preskúmajte status dokázateľnosti prehlásenia o bezospornosti $\mathrm{Cons}_4(T)$ v T. Uvedomte si, že púhy predpoklad, že T je bezosporná, neumožňuje odvodiť, že $\mathrm{Cons}_4(T)$ je dokázateľné, ani že $\mathrm{Cons}_4(T)$ je nedokázateľné v T.

(c) Všimnite si, že implikácia $\varphi_g(g)\Rightarrow\mathrm{Cons}_4(T)$ je logicky platná. Následne odvoďte, že z predpokladu ω-konzistentnosti teórie T vyplýva, že negácia $\neg\,\mathrm{Cons}_4(T)$ nie je dokázateľná v T.

5.5.4 Úloha. (a) Ukážte, že Rosserovo tvrdenie $\varphi_r(r)$ nie je prehlásením o bezospornosti teórie T. Ako je to s jeho negáciou $\neg\varphi_r(r)$?

(b) Ukážte, že obe tvrdenia $\neg(\exists\,z)P(r,r,z)$, $\neg(\exists\,u)R(r,r,u)$ sú prehláseniami o bezospornosti teórie T. Ako je to s ich dokázateľnosťou?

Vo svetle Gödelových výsledkov je možno prekvapivé, no každopádne stojí za zmienku, že Solomon Feferman v roku 1960 zostrojil za cenu vyššej zložitosti prehlásenie o bezospornosti $\mathrm{Cons}^*(\mathrm{PA})$ Peanovej aritmetiky, ktoré je napriek tomu *dokázateľné* v PA. Jednako pre takéto prehlásenie o bezospornosti nemožno v PA dokázať

ekvivalenciu $\mathrm{Cons}^*(\mathrm{PA}) \Leftrightarrow \mathrm{Cons}_i(\mathrm{PA})$, ba ani implikáciu $\mathrm{Cons}^*(\mathrm{PA}) \Rightarrow \mathrm{Cons}_i(\mathrm{PA})$, pre žiadne $i = 1, 2, 3$ (samozrejme, pokiaľ samotná PA nie je sporná).

Na druhej strane možno bezospornosť Peanovej aritmetiky (a nielen niektoré prehlásenie o jej bezospornosti) dokázať v rámci niektorých teórií silnejších než PA (ktorých bezospornosť je z toho dôvodu pochybnejšia než bezospornosť PA). Zoznam zrejme zahŕňa akúkoľvek rozumnú verziu Teórie množín, keďže tie dovoľujú zostrojiť štandardný model $(\mathbb{N}; +, \cdot, 0, 1)$ Peanovej aritmetiky. No už i niektoré pomerne skromné rozšírenia PA zvládnu túto úlohu. Gerhard Gentzen v roku 1936 dokázal bezospornosť PA *transfinitnou indukciou* cez ordinálne čísla menšie než spočítateľný ordinál $\varepsilon_0 = \omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}$. (S náznakom tejto metódy sa stretneme v paragrafe 5.8 venovanom Goodsteinovým postupnostiam. Pri konštrukcii algebraického uzáveru poľa transfinitnou rekurziou v dôkaze Vety 7.5.2 sa vyskytne dokonca aj pre iné ordinálne ohraničenia ako ε_0.) Samotný Gödel podal dôkaz bezospornosti PA pomocou *rekurzívnych funkcionálov* v roku 1958.

5.6 Pokusy o zúplnenie

Prirodzene sa natíska otázka, či by nebolo možné zúplniť Peanovu aritmetiku pridaním nejakých nových axióm, o ktorých vieme, že sú splnené v štandardnom modeli $(\mathbb{N}; +, \cdot, 0, 1)$. Jedného možného kandidáta ponúka nasledujúca rekurzívna konštrukcia: Nech T_0 je samotná PA. Ak je daná teória T_q pre $q \in \mathbb{N}$, zostrojíme postupnosť $\Delta_0^q, \Delta_1^q, \ldots, \Delta_k^q, \ldots$ všetkých dôkazov v T_q, ako aj predikát $P_q(x, y, z)$ dokázateľnosti v T_q taký, že pre všetky $k, m, n \in \mathbb{N}$ platí:

$$P_q(m, n, k) \text{ práve vtedy, keď } \Delta_k^q \text{ je dôkaz sentencie } \varphi_n(m) \text{v } T_q\,.$$

Vzápätí položíme

$$T_{q+1} = T_q \cup \{\mathrm{Cons}(T_q)\}$$

kde $\mathrm{Cons}(T_q)$ je niektoré z prehlásení o bezospornosti $\mathrm{Cons}_i(T_q)$ pre pevné $i = 1, 2, 3$. Inak povedané, T_{q+1} je rozšírením T_q o axiómu $\mathrm{Cons}(T_q)$ prehlasujúcu bezospornosť teórie T_q. Zrejme každé T_q je rekurzívne axiomatizovateľná aritmeticky korektná teória. Preto vytvorením zjednotenia

$$\widehat{T} = \bigcup_{q \in \mathbb{N}} T_q$$

dostaneme opäť aritmeticky korektnú teóriu, v ktorej sú dokázateľné všetky prehlásenia o bezospornosti $\mathrm{Cons}(T_q)$. Avšak aj $\widehat{T}$ je rekurzívne axiomatizovateľná, preto sa na ňu vzťahujú všetky predchádzajúce výsledky o neúplnosti. To okrem iného znamená, že $\widehat{T}$ je neúplná, dokáže sformulovať prehlásenie o svojej vlastnej bezospornosti $\mathrm{Cons}\big(\widehat{T}\,\big)$, ktoré však nie je schopná dokázať. Navyše, ako ukázal Alan Turing v roku 1939, Peanovu aritmetiku nemožno zúplniť ani transfinitnou iteráciou procedúry jej rozširovania o postupné prehlásenia o bezospornosti.

Jeden z aspektov neúplnosti Peanovej aritmetiky a príbuzných teórií sa prejavuje ako fenomén *ω-neúplnosti*, t. j. istého druhu „nerovnomernosti“ dokázateľnosti v nich.

Napríklad, ak $\psi(x)$ je formula v jazyku PA, tak z dokázateľnosti všetkých sentencií $\psi(m)$ pre ľubovoľné $m \in \mathbb{N}$ v PA ešte nevyplýva, že v PA je dokázateľný aj univerzálny uzáver $(\forall x)\psi(x)$. Môže sa totiž stať, že dôkazy jednotlivých inštancií $\psi(0)$, $\psi(1)$, ..., $\psi(m)$, ... sa líšia do takej miery, že zostaviť na ich základe jednotný dôkaz univerzálne kvantifikovaného tvrdenia $(\forall x)\psi(x)$ je jednoducho nemožné. Aritmetická teória T sa nazýva *ω-úplná*, ak sa také niečo nemôže stať, teda ak pre každú aritmetickú formulu $\psi(x)$ z dokázateľnosti všetkých jednotlivých inštancií $\psi(m)$ pre $m \in \mathbb{N}$ v T vyplýva, že aj jej univerzálny uzáver $(\forall x)\psi(x)$ je dokázateľný v T.

Konštrukciu úplného rozšírenia Peanovej aritmetiky založenú na odstránení javu ω-neúplnosti navrhol S. Feferman v r. 1962. Aby však mohol rozšíriť PA do úplnej a zároveň ω-úplnej teórie, musel obetovať podmienku rekurzívnej axiomatizovateľnosti. Transfinitnou rekurziou cez ordinálne čísla menšie než istý limitný ordinál $\zeta \leq \omega^{\omega^\omega}$ zostrojil postupnosť aritmetických teórií $\{T_\alpha\}_{\alpha<\zeta}$ a postupnosť predikátov dokázateľnosti $\{P_\alpha(x,y,z)\}_{\alpha<\zeta}$ v týchto teóriách takých, že

$$\begin{aligned} T_0 &= \mathrm{PA} \\ T_{\alpha+1} &= T_\alpha \cup \{(\forall x)(\exists z)P_\alpha(x,n,z) \Rightarrow (\forall x)\varphi_n(x)\colon n \in \mathbb{N}\} \quad \text{pre každé } \alpha < \zeta \\ T_\lambda &= \bigcup_{\alpha<\lambda} T_\alpha \quad \text{pre každý limitný ordinál } \lambda < \zeta \end{aligned}$$

Pridanie nových axióm

$$(\forall x)(\exists z)P_\alpha(x,n,z) \Rightarrow (\forall x)\varphi_n(x)$$

pre $n \in \mathbb{N}$ k axiómam teórie T_α zaručuje dokázateľnosť každého univerzálne kvantifikovaného tvrdenia $(\forall x)\varphi_n(x)$ v teórii $T_{\alpha+1}$, akonáhle sú všetky jeho jednotlivé inštancie $\varphi_n(m)$ pre $m \in \mathbb{N}$ dokázateľné v T_α.

Napokon možno dokázať, že aritmetická teória

$$\widetilde{T} = \bigcup_{\alpha<\zeta} T_\alpha$$

nie je len ω-úplná, ale aj úplná a ω-konzistentná. Aby sme však mohli odvodiť tento záver, musíme predpokladať, že PA je konzistentná. Ak predpokladáme, že PA je aritmeticky korektná, môžeme usúdiť, že aj $\widetilde{T}$ má túto vlastnosť.

5.7 Vety Tarského a Churcha-Turinga

Aby sme čitateľovi poskytli úplný obraz, sformulujeme ešte dva ďalšie výsledky o neúplnosti pochádzajúce od Alfreda Tarského z r. 1933, resp. od Alonza Churcha a Alana Turinga z r. 1936. *Tarského veta o nedefinovateľnosti pravdy* neformálne hovorí, že vlastnosť aritmetických sentencií „byť pravdivými“ nemožno definovať žiadnou formulou v jazyku týchto sentencií. Presnejšie to znamená, že *reláciu spĺňania* pre aritmetické formuly v štandardnom modeli $(\mathbb{N}; +, \cdot, 0, 1)$ nemožno vyjadriť žiadnou aritmetickou formulou. V ďalších dvoch vetách sa opäť odvolávame na postupnosť $\{\varphi_n(x)\}_{n\in\mathbb{N}}$ aritmetických formúl.

5.7.1 Tarského veta o nedefinovateľnosti pravdy. *Nech T je ľubovoľná konzistentná aritmetická teória. Potom neexistuje aritmetická formula $\sigma(x, y)$ v jazyku teórie T taká, aby pre všetky $m, n \in \mathbb{N}$ platilo*

$$(\mathbb{N}; +, \cdot, 0, 1) \vDash \varphi_n(m) \Leftrightarrow \sigma(m, n)$$

Demonštrácia. Pripusťme, že taká formula $\sigma(x, y)$ existuje. Potom $\neg\sigma(x, x)$ je aritmetická formula s jedinou voľnou premennou x, teda sa nachádza v postupnosti $\{\varphi_n(x)\}_{n\in\mathbb{N}}$ pod nejakým číslom $t \in \mathbb{N}$. Potom nasledujúce tvrdenia sú ekvivalentné v $(\mathbb{N}; +, \cdot, 0, 1)$: $\sigma(t, t)$, $\varphi_t(t)$, $\neg\sigma(t, t)$. Takže

$$(\mathbb{N}; +, \cdot, 0, 1) \vDash \sigma(t, t) \Leftrightarrow \neg\sigma(t, t)$$

čo je spor.

Tarského veta kladie výrazné obmedzenia na možnosti autoreprezentácie aritmetických teórií. Aby sme mohli definovať formulu spĺňania $\sigma(x, y)$ pre takú teóriu T, je potrebné rozšíriť ju do nejakej teórie T' v „metajazyku“, ktorého expresívna sila presahuje možnosti pôvodnej teórie T. Napríklad formulu spĺňania pre Peanovu aritmetiku možno definovať v Aritmetike druhého rádu alebo v Zermelovej-Fraenkelovej teórii množín.

Pri svojich skúmaniach otázok rozhodnuteľnosti boli A. Church aj A. Turing značne ovplyvnení prácou K. Gödela o úplnosti Logiky prvého rádu a ešte väčšmi jeho prácou o neúplnosti Peanovej aritmetiky a ďalších aritmetických teórií. Zatiaľ čo Church rozpracoval tzv. *λ-kalkulus* a použil ho ako paradigmatický model všeobecných výpočtov, Turing navrhol ideálne modely výpočtových zariadení, ktoré sa stali známymi ako *Turingove stroje*. Krátko nato sa ukázalo, že oba prístupy sú ekvivalentné. Dôkaz nasledujúcej vety presahuje rámec nášho kurzu.

5.7.2 Churchova-Turingova veta o nerozhodnuteľnosti. *Nech T je ľubovoľná konzistentná rekurzívne axiomatizovateľná aritmetická teória. Potom neexistuje algoritmus schopný rozhodnúť, či je daná aritmetická sentencia v jej jazyku dokázateľná v T. Špeciálne neexistuje algoritmus schopný rozhodnúť otázku dokázateľnosti sentencie $\varphi_n(m)$ v T pre každý vstup $(m, n) \in \mathbb{N} \times \mathbb{N}$.*

Church tiež dokázal, že neexistuje algoritmus, ktorý by dokázal rozhodnúť, či je daná sentencia v jazyku prvého rádu L s aspoň jedným binárnym alebo relačným symbolom alebo s aspoň dvoma unárnymi operačnými symbolmi „tautológia prvého rádu“, t. j. či je splnená v každej L-štruktúre (alebo, čo je to isté, či je dokázateľná iba z logických axióm). To znamená, že Logika prvého rádu sa zásadne líši od Výrokového počtu, v ktorom sú tautológie efektívne rozpoznateľné algoritmom tabuliek pravdivostných hodnôt.

Zatiaľ čo Tarského veta kladie určité obmedzenia na to, čo možno *vyjadriť* formálnymi jazykmi, Churchova-Turingova veta vymedzuje hranice toho, čo možno *vypočítať* s použitím akéhokoľvek mechanického alebo elektronického zariadenia alebo *efektívne rozhodnúť* prostredníctvom akejkoľvek algoritmickej výpočtovej procedúry. No obe, samozrejme, spolu s Gödelovými vetami o neúplnosti, vyvolávajú rad otázok o vzťahu počítačov, ľudských mozgov a ľudskej mysle alebo ducha.

5.8 Goodsteinove postupnosti

Možno namietať, že pravdivé aritmetické tvrdenia nedokázateľné v PA, ktoré zostrojili Gödel a Rosser, ako napr. $\varphi_g(g)$, $\varphi_r(r)$, Cons(PA) (bez ohľadu na to, ktorú možnosť si vyberieme), sú značne umelé a nemajú „skutočný“ matematický obsah a zmysel. Možno však uviesť viacero známych aritmetických viet kombinatorického či číselne teoretického charakteru, ktoré sú pravdivé (t. j. splnené v $(\mathbb{N}; +, \cdot, 0, 1)$) a napriek tomu nedokázateľné v PA. Tie spravidla zároveň ilustrujú fenomén ω-neúplnosti. Príklady univerzálne kvantifikovaných tvrdení tvaru $(\forall x)\psi(x)$ nedokázateľných v PA, no splnených v $(\mathbb{N}; +, \cdot, 0, 1)$ v tom zmysle, že všetky jednotlivé inštancie $\psi(m)$ pre $m \in \mathbb{N}$ sú dokonca dokázateľné v PA, poskytujú napr. *Parisovo-Harringtonovo* zosilnenie *Ramseyho vety* alebo *Goodsteinove postupnosti*. Oba výsledky sú v skutočnosti ekvivalentné s bezospornosťou Peanovej aritmetiky. Stručne si vysvetlíme povahu druhého z týchto výsledkov.

Ak je dané prirodzené číslo $b \geq 2$, tak *dedičný rozvoj pri základe* b ľubovoľného prirodzeného čísla m dostaneme z jeho obvyklého rozvoja pri základe b rozvojom všetkých jeho exponentov pri základe b, následným rozvojom exponentov týchto exponentov pri základe b, a opakovaním tohto postupu tak dlho, až pokým všetky čísla väčšie než b nie sú eliminované z príslušného výrazu. Napríklad dedičný rozvoj pri základe 2 čísla $m = 357$ vyzerá takto:

$$\begin{aligned} 357 &= 2^8 + 2^6 + 2^5 + 2^2 + 1 = 2^{2^3} + 2^{2^2+2} + 2^{2^2+1} + 1 \\ &= 2^{2^{2+1}} + 2^{2^2+2} + 2^{2^{2+1}} + 2^{2^2+1} + 1 \end{aligned}$$

Jeho dedičný rozvoj pri základe 3 je

$$357 = 3^5 + 3^4 + 3^3 + 2 \cdot 3 = 3^{3+2} + 3^{3+1} + 3^3 + 2 \cdot 3$$

Podobne, dedičný rozvoj pri základe 2 čísla $m = 1\,000$ je

$$\begin{aligned} 1\,000 &= 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3 \\ &= 2^{2^3+1} + 2^{2^3} + 2^{2^2+2+1} + 2^{2^2+2} + 2^{2^2+1} + 2^{2+1} \\ &= 2^{2^{2+1}+1} + 2^{2^{2+1}} + 2^{2^2+2+1} + 2^{2^2+2} + 2^{2^2+1} + 2^{2+1} \end{aligned}$$

Na druhej strane, jeho dedičný rozvoj pri základe 5 sa zhoduje s jeho jednoduchým rozvojom pri tomto základe:

$$1\,000 = 5^4 + 3 \cdot 5^3$$

Pre ľubovoľné prirodzené číslo m zostrojíme *Goodsteinovu postupnosť* prirodzených čísel

$$G(m,0),\ G(m,1),\ G(m,2),\ \ldots,\ G(m,n),\ G(m,n+1),\ \ldots$$

prislúchajúcu k prirodzenému číslu m, ktorá začína číslom $G(m,0) = m$ a po dosiahnutí čísla $G(m,n)$ pokračuje takto: Ak $G(m,n) > 0$, tak nasledujúci člen $G(m,n+1)$ získame z dedičného rozvoja pri základe $n+2$ čísla $G(m,n)$ nahradením každého výskytu čísla $n+2$ číslom $n+3$ a odpočítaním 1 od výsledku; ak $G(m,n) = 0$, tak aj

$G(m,n+1)=0$. Napríklad pre $m=29$ dostávame:

$$\begin{aligned}
G(m,0) &= 2^4+2^3+2^2+1 = 2^{2^2}+2^{2+1}+2^2+1\\
G(m,1) &= 3^{3^3}+3^{3+1}+3^3+1-1 = 3^{3^3}+3^{3+1}+3^3 = 7\,625\,597\,485\,095\\
G(m,2) &= 4^{4^4}+4^{4+1}+4^4-1 = 4^{4^4}+4^{4+1}+3\cdot 4^3+3\cdot 4^2+3\cdot 4+3 \approx 134\cdot 10^{152}\\
G(m,3) &= 5^{5^5}+5^{5+1}+3\cdot 5^3+3\cdot 5^2+3\cdot 5+3-1\\
&= 5^{5^5}+5^{5+1}+3\cdot 5^3+3\cdot 5^2+3\cdot 5+2 \sim 10^{2\,200}\\
G(m,4) &= 6^{6^6}+6^{6+1}+3\cdot 6^3+3\cdot 6^2+3\cdot 6+2-1\\
&= 6^{6^6}+6^{6+1}+3\cdot 6^3+3\cdot 6^2+3\cdot 6+1 \sim 10^{36\,305}\\
G(m,5) &= 7^{7^7}+7^{7+1}+3\cdot 7^3+3\cdot 7^2+3\cdot 7+1-1\\
&= 7^{7^7}+7^{7+1}+3\cdot 7^3+3\cdot 7^2+3\cdot 7 \sim 10^{696\,000}\ \ldots
\end{aligned}$$

Uvedené výpočty naznačujú, že Goodsteinove postupnosti $\{G(m,n)\}_{n=0}^{\infty}$ veľmi rýchlo rastú pre každé m, a nielen pre jednotlivú hodnotu $m=29$. Preto nasledujúci výsledok R. L. Goodsteina z r. 1944 je značne prekvapivý a neočakávaný.

5.8.1 Goodsteinova veta. *Pre každé prirodzené číslo m existuje prirodzené číslo n také, že $G(m,n)=0$.*

V skutočnosti pre $m\le 3$ postupnosť $\{G(m,n)\}_{n=0}^{\infty}$ nadobudne hodnotu 0 veľmi rýchlo. Čiatateľ si ľahko overí, že $G(0,n)=0$ pre každé n, $G(1,0)=1$, $G(1,n)=0$ pre $n\ge 1$, $G(2,0)=G(2,1)=2$, $G(2,2)=1$ a $G(2,n)=0$ pre $n\ge 3$. Pre $m=3$ máme

$$\begin{aligned}
&G(3,0)=3=2+1, \quad G(3,1)=3+1-1=3, \quad G(3,2)=4-1=3,\\
&G(3,3)=3-1=2, \quad G(3,4)=2-1=1, \qquad G(3,5)=0=G(3,n) \quad \text{pre } n>5
\end{aligned}$$

Pre $m=4$ má prvé n, pre ktoré $G(4,n)=0$, nesmierne veľkú hodnotu $3\big(2^{402\,653\,211}-1\big)$.

Formálne využíva dôkaz Goodsteinovej vety transfinitnú indukciu cez spočítateľnú dobre usporiadanú množinu všetkých ordinálnych čísel menších než ordinál

$$\varepsilon_0=\omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}$$

t. j. prvý ordinál α, ktorý spĺňa podmienku $\omega^\alpha=\alpha$. No základnú myšlienku tohto dôkazu možno vysvetliť jednoducho. Spočíva v dominovaní každej postupnosti $\{G(m,n)\}_{n=0}^{\infty}$ pri pevnom m postupnosťou $\{\Gamma(m,n)\}_{n=0}^{\infty}$ ordinálnych čísel $\Gamma(m,n)<\varepsilon_0$ takou, že pre každé n platí $G(m,n)\le\Gamma(m,n)$ a $\Gamma(m,n)>\Gamma(m,n+1)$ vždy, keď $\Gamma(m,n)>0$. Keďže množina všetkých ordinálov $<\varepsilon_0$ je dobre usporiadaná reláciou $<$, nemôže obsahovať žiadnu nekonečnú ostro klesajúcu postupnosť. Preto každá z postupností $\{\Gamma(m,n)\}_{n=0}^{\infty}$ sa musí nakoniec ustáliť na hodnote $\Gamma(m,n)=0$ pre nejaké n. Potom tiež $G(m,n)=0$.

Ordinálne číslo $\Gamma(m,n)$ dostaneme nahradením každého výskytu termu $n+2$ v dedičnom rozvoji pri základe $n+2$ čísla $G(m,n)$ ordinálom ω. V prípade $m=29$ máme

$$\begin{aligned}
G(m,0) &= 2^{2^2} + 2^{2+1} + 2^2 + 1 \\
&< \omega^{\omega^\omega} + \omega^{\omega+1} + \omega^\omega + 1 = \Gamma(m,0) \\
G(m,1) &= 3^{3^3} + 3^{3+1} + 3^3 \\
&< \omega^{\omega^\omega} + \omega^{\omega+1} + \omega^\omega = \Gamma(m,1) \\
G(m,2) &= 4^{4^4} + 4^{4+1} + 3\cdot 4^3 + 3\cdot 4^2 + 3\cdot 4 + 3 \\
&< \omega^{\omega^\omega} + \omega^{\omega+1} + 3\cdot\omega^3 + 3\cdot\omega^2 + 3\cdot\omega + 3 = \Gamma(m,2) \\
G(m,3) &= 5^{5^5} + 5^{5+1} + 3\cdot 5^3 + 3\cdot 5^2 + 3\cdot 5 + 2 \\
&< \omega^{\omega^\omega} + \omega^{\omega+1} + 3\cdot\omega^3 + 3\cdot\omega^2 + 3\cdot\omega + 2 = \Gamma(m,3) \\
G(m,4) &= 6^{6^6} + 6^{6+1} + 3\cdot 6^3 + 3\cdot 6^2 + 3\cdot 6 + 1 \\
&< \omega^{\omega^\omega} + \omega^{\omega+1} + 3\cdot\omega^3 + 3\cdot\omega^2 + 3\cdot\omega + 1 = \Gamma(m,4) \\
G(m,5) &= 7^{7^7} + 7^{7+1} + 3\cdot 7^3 + 3\cdot 7^2 + 3\cdot 7 \\
&< \omega^{\omega^\omega} + \omega^{\omega+1} + 3\cdot\omega^3 + 3\cdot\omega^2 + 3\cdot\omega = \Gamma(m,5) \ \ldots
\end{aligned}$$

Postupnosť ordinálov

$$\begin{aligned}
&\Gamma(m,0) = \omega^{\omega^\omega} + \omega^{\omega+1} + \omega^\omega + 1 \\
&> \Gamma(m,1) = \omega^{\omega^\omega} + \omega^{\omega+1} + \omega^\omega \\
&> \Gamma(m,2) = \omega^{\omega^\omega} + \omega^{\omega+1} + 3\cdot\omega^3 + 3\cdot\omega^2 + 3\cdot\omega + 3 \\
&> \Gamma(m,3) = \omega^{\omega^\omega} + \omega^{\omega+1} + 3\cdot\omega^3 + 3\cdot\omega^2 + 3\cdot\omega + 2 \\
&> \Gamma(m,4) = \omega^{\omega^\omega} + \omega^{\omega+1} + 3\cdot\omega^3 + 3\cdot\omega^2 + 3\cdot\omega + 1 \\
&> \Gamma(m,5) = \omega^{\omega^\omega} + \omega^{\omega+1} + 3\cdot\omega^3 + 3\cdot\omega^2 + 3\cdot\omega \\
&> \ldots
\end{aligned}$$

však nemôže klesať naveky, takže sa musí napokon ustáliť na hodnote $\Gamma(m,n) = 0$ pre nejaké gigantické, nepredstaviteľne veľké n. Pre toto n je tiež $G(m,n) = 0$.

Ako ukázali L. Kirby a J. Paris v r. 1982, Goodsteinovu vetu nemožno dokázať iba prostriedkami samotnej Peanovej aritmetiky.

5.8.2 Kirbyho-Parisova veta. *V* PA *možno dokázať, že z Goodsteinovej vety vyplýva prehlásenie o bezospornosti* Cons(PA). *V dôsledku toho ak* PA *je bezosporná, tak Goodsteinova veta nie je dokázateľná v* PA.

Na druhej strane, pre jednotlivé $m \in \mathbb{N}$ sú existenčné tvrdenia $(\exists\, y)(G(m, y) = 0)$ dokázateľné v PA. Vieme to, hoci už pre pomerne malé hodnoty m nielen že nepoznáme presné hodnoty príslušných $y = n$, ale ani nedisponujeme žiadnym explicitným dôkazom týchto tvrdení v PA. Vieme len, že primitívne výpočty krok za krokom musia nakoniec priniesť potrebný výsledok. Taký výpočet sa však nemusí skončiť, nielen v čase existencie ľudského druhu, no ani celého vesmíru. Zároveň si na ilustráciu fenoménu ω-neúplnosti spomínaného v súvislosti s Fefermanovou konštrukciou treba uvedomiť, že je nemožné extrahovať z týchto jednotlivých dôkazov – výpočtov akúkoľvek všeobecnú spoločnú myšlienku, na základe ktorej by sa z nich dal zostaviť jednotný dôkaz univerzálno-existenčného tvrdenia $(\forall\, x)(\exists\, y)(G(x, y) = 0)$ v PA.

5.9 Filozofické dôsledky. Témy na esej

Existuje rozsiahla literatúra zaoberajúca sa matematickými, filozofickými, metafyzickými a ďalšími mimomatematickými dôsledkami Gödelových viet o neúplnosti a niektorých podobných výsledkov. Obmedzíme sa len na stručný zoznam niektorých tradične vyvodzovaných záverov:

(1) Ľudské poznanie je nevyhnutne neúplné a my si nikdy nemôžeme byť istí, že neobsahuje protirečenia.

(2) Ľudské poznanie nemožno zredukovať na žiaden formálny systém. Uvedomiac si javy neúplnosti vlastné takým systémom, môžeme prekonať ich obmedzenia.

(3) Počítače môžu počítať a dokazovať vždy len v rámci určitého formálneho systému. No ľudia sú schopní pochopiť a odhaliť aj pravdy nedokázateľné v rámci akéhokoľvek formálneho systému. V dôsledku toho ľudský mozog – napriek tomu, že vzhľadom na niektoré parametre (ako napr. rýchlosť výpočtu) ďaleko zaostáva za počítačmi – stále disponuje určitými schopnosťami, ktoré ho činia nadradeným akémukoľvek počítaču.

Je extrémne zaujímavé zoznámiť sa s niektorými Gödelovými myšlienkami na uvedené témy. Gödel totiž šiel o krok ďalej za (3). Podľa neho sa všetci asi zhodneme na tom, že počítače môžu počítať a dokazovať výlučne v rámci nejakého vopred daného formálneho systému. Podobne aj činnosť ľudkého mozgu možno v zásade simulovať nejakým počítačom (i keď takými počítačmi zatiaľ nedisponujeme). No ľudské bytosti sú schopné nazerať a zmocniť sa aj určitých právd nedokázateľných v rámci akéhokoľvek formálneho systému. Z toho vyplýva, že ľudská myseľ, ľudský intelekt či ľudský duch, akokoľvek to nazveme, je obdarený nielen schopnosťami, ktoré ho činia nadradeným akémukoľvek počítaču, ale tiež určitými schopnosťami, ktoré nemožno vysvetliť ako púhe prejavy fungovania ľudského mozgu.[5]

[5] Voľne citované podľa Hao Wang [1996].

Skúste sa zamyslieť nad uvedenými závermi a názormi. Do akej miery súhlasíte či nesúhlasíte s každým z nich a prečo? Do akej miery možno uvedené závery zdôvodniť výsledkami o neúplnosti, ktorými sme sa zaoberali? Rozdiskutujte tieto otázky a skúste ich upresniť a nakoniec sa dopracovať k formuláciám, s ktorými by ste mohli súhlasiť. Do akej miery vyplývajú Vaše závery z výsledkov Gödela, Rossera, Tarského, Churcha a Turinga? Skúste tieto otázky zasadiť do kontextu najnovšieho búrlivého rozvoja v oblasti umelej inteligencie.

6 Podštruktúry a homomorfizmy

Touto kapitolou začíname časť venovanú *teórii modelov*. Z rozsiahleho materiálu, ktorý zahŕňa táto matematická disciplína, sa obmedzíme iba na malú ukážku jej základných pojmov a metód, zovšeobecňujúcich rad výsledkov, s ktorými sa čitateľ pravdepodobne už mal možnosť zoznámiť v kurze algebry. I keď teóriu modelov možno v istom zmysle chápať ako „metamatematiku algebry“, náš prístup bude – na rozdiel od predošlých troch kapitol – väčšmi matematický než metamatematický. To sa okrem iného prejaví v tom, že dôkazy stanovených výsledkov budeme väčšinou uvádzať pod obvyklým názvom „dôkaz“ namiesto doteraz používaného názvu „demonštrácia“.

V celej kapitole $L = (F, R, \nu)$ označuje nejaký pevne zvolený, no inak ľubovoľný jazyk prvého rádu, pričom jeho konštantné symboly chápeme ako nulárne funkcionálne symboly. Pokiaľ nebude hroziť nedorozumenie alebo výslovne nepovieme inak, tak pod pojmom „štruktúra“, prípadne „štruktúra prvého rádu“, budeme rozumieť štruktúru jazyka L a „teóriou“, resp. „teóriou prvého rádu“ budeme rozumieť teóriu v jazyku L. Podobne budeme pod slovami ako „term“ alebo „formula“ rozumieť term, resp. formulu jazyka L.

6.1 Podštruktúry

Nech $\mathcal{A} = (A; \dots)$, $\mathcal{B} = (B; \dots)$ sú dve štruktúry prvého rádu. Hovoríme, že štruktúra $\mathcal{B}$ je *podštruktúrou* štruktúry $\mathcal{A}$, označenie $\mathcal{B} \subseteq \mathcal{A}$, ak $B \subseteq A$ a pre ľubovoľný n-árny funkcionálny symbol $f \in F$, resp. relačný symbol $r \in R$ a všetky $b_1, \dots, b_n \in B$ platí

$$f^{\mathcal{B}}(b_1, \dots, b_n) = f^{\mathcal{A}}(b_1, \dots, b_n)$$
$$(b_1, \dots, b_n) \in r^{\mathcal{B}} \;\Leftrightarrow\; (b_1, \dots, b_n) \in r^{\mathcal{A}}$$

Inak povedané, $f^{\mathcal{B}} = f^{\mathcal{A}} \restriction B^n$ a $r^{\mathcal{B}} = r^{\mathcal{A}} \cap B^n$. Špeciálne pre konštantný symbol $f \in F$ to znamená, že $f^{\mathcal{B}} = f^{\mathcal{A}}$. Hovoríme tiež, že štruktúra $\mathcal{A}$ je *nadštruktúrou* alebo *rozšírením* štruktúry $\mathcal{B}$ a píšeme $\mathcal{A} \supseteq \mathcal{B}$.

Vzťah „byť podštruktúrou“ je zrejme tranzitívny, čiže pre ľubovoľné štruktúry $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ platí

$$\mathcal{A} \subseteq \mathcal{B} \wedge \mathcal{B} \subseteq \mathcal{C} \;\Rightarrow\; \mathcal{A} \subseteq \mathcal{C}$$

Základná množina B podštruktúry $\mathcal{B} \subseteq \mathcal{A}$ musí byť uzavretá vzhľadom na všetky operácie v nadštruktúre $\mathcal{A}$. Teda pre každý n-árny funkcionálny symbol $f \in F$ a všetky $b_1, \dots, b_n \in B$ platí $f^{\mathcal{A}}(b_1, \dots, b_n) \in B$. Špeciálne $f^{\mathcal{A}} \in B$ pre každý konštantný symbol $f \in F$.

Naopak, každá neprázdna podmnožina $M \subseteq A$ základnej množiny štruktúry $\mathcal{A}$, ktorá je uzavretá vzhľadom na všetky operácie štruktúry $\mathcal{A}$, už jednoznačne určuje

podštruktúru $\mathcal{M} = (M; \dots)$ štruktúry $\mathcal{A}$ s nosičom M. Operácie a relácie v $\mathcal{M}$ sú potom korektne definované jediným možným spôsobom:

$$f^{\mathcal{M}} = f^{\mathcal{A}} \restriction M^n$$
$$r^{\mathcal{M}} = r^{\mathcal{A}} \cap M^n$$

pre každý n-árny operačný, resp. relačný symbol $f \in F$, $r \in R$. Uvedené rovnosti vyjadrujeme slovným obratom, že operácie a relácie štruktúry $\mathcal{M}$ sú *zdedené* zo štruktúry $\mathcal{A}$. Toto pozorovanie nám poskytuje istú voľnosť vo vyjadrovaní: pod pojmom podštruktúry štruktúry $\mathcal{A}$ môžeme podľa okolností rozumieť niekedy štruktúru $\mathcal{M}$ takú, že $\mathcal{M} \subseteq \mathcal{A}$, inokedy zas neprázdnu podmnožinu $M \subseteq A$ uzavretú vzhľadom na operácie v $\mathcal{A}$ (príslušná štruktúra $\mathcal{M} = (M; \dots)$ má potom operácie a relácie zdedené z $\mathcal{A}$).

6.1.1 Príklad. Vektorové priestory nad daným poľom F možno chápať ako štruktúry $\big(V; F \cup \{+\}\big)$ jazyka prvého rádu s binárnou operáciou sčítania $+$, unárnymi operáciami násobenia skalármi $f \in F$ a bez relačných symbolov (pozri Príklad 4.3.3). Potom podštruktúry vektorového priestoru $\big(V; F \cup \{+\}\big)$ sú práve všetky jeho lineárne podpriestory.

6.1.2 Úloha. Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry prvého rádu, pričom $\mathcal{A} \subseteq \mathcal{B}$, $t(x_1, \dots, x_n)$ je term a $\varphi(x_1, \dots, x_n)$ je atomická formula. Potom pre všetky $b_1, \dots, b_n \in B$ platí

$$t^{\mathcal{A}}(b_1, \dots, b_n) \in B$$
$$\mathcal{B} \vDash \varphi(b_1, \dots, b_n) \;\Leftrightarrow\; \mathcal{A} \vDash \varphi(b_1, \dots, b_n)$$

Dokážte.

Upozornenie. Čitateľ s istými znalosťami z teórie grafov by si mal uvedomiť, že pojem podštruktúry zodpovedá pojmu *indukovaného podgrafu* daného grafu $G = (V; E)$, a nie pojmu jeho ľubovoľného podgrafu.

Vlastnosti podštruktúr vykazujú istú citlivosť voči jazyku. Nasledujúca úloha ukazuje, čo tým máme na mysli.

6.1.3 Úloha. Už sme spomínali tri možné definície grúp ako štruktúr $(G; \cdot)$, $(G; \cdot, e)$, resp. $\big(G; \cdot, e, {}^{-1}\big)$ v rôzne bohatých jazykoch.

(a) Nájdite niekoľko príkladov grúp $\mathcal{G} = (G; \cdot)$, resp. $\mathcal{G} = (G; \cdot, e)$ a ich podštruktúr, ktoré samy nie sú grupy. Na základe toho si uvedomte, že v oboch týchto jazykoch podštruktúra grupy nemusí byť jej podgrupou.

(b) Dokážte, že každá podštruktúra grupy $\mathcal{G} = \big(G; \cdot, e, {}^{-1}\big)$ je i sama grupou. V tomto prípade ju teda možno oprávnene nazývať podgrupou danej grupy.

V súvislosti s podštruktúrami grúp, ktoré nie sú podgrupami, sa vynára všeobecná otázka, ktoré vlastnosti danej štruktúry, vyjadrené formulami prvého rádu, sa prenášajú na jej podštruktúry, prípadne na jej rozšírenia. Isté triedy takýchto formúl môžeme opísať pomerne ľahko.

Hovoríme, že formula φ je *otvorená*, ak neobsahuje nijaké kvantifikátory. Hovoríme, že φ je *univerzálna* formula, ak φ má tvar $(\forall x_1, \ldots, x_n)\psi$, kde ψ je otvorená formula. Podobne hovoríme, že φ je *existenčná* formula, ak φ má tvar $(\exists x_1, \ldots, x_n)\psi$, kde ψ je otvorená formula. Zrejme negácia univerzálnej (existenčnej) formuly je logicky ekvivalentná s existenčnou (univerzálnou) formulou.

6.1.4 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry prvého rádu a $\mathcal{B} \subseteq \mathcal{A}$.*

(a) *Ak $\varphi(x_1, \ldots, x_n)$ je otvorená formula, tak pre všetky $b_1, \ldots, b_n \in B$ platí*
$$\mathcal{B} \vDash \varphi(b_1, \ldots, b_n) \;\Leftrightarrow\; \mathcal{A} \vDash \varphi(b_1, \ldots, b_n)$$

(b) *Ak $\varphi(x_1, \ldots, x_n)$ je univerzálna formula, tak pre všetky $b_1, \ldots, b_n \in B$ platí*
$$\mathcal{A} \vDash \varphi(b_1, \ldots, b_n) \;\Rightarrow\; \mathcal{B} \vDash \varphi(b_1, \ldots, b_n)$$

(c) *Ak $\varphi(x_1, \ldots, x_n)$ je existenčná formula, tak pre všetky $b_1, \ldots, b_n \in B$ platí*
$$\mathcal{B} \vDash \varphi(b_1, \ldots, b_n) \;\Rightarrow\; \mathcal{A} \vDash \varphi(b_1, \ldots, b_n)$$

Dôkaz. (a) Tvrdenie možno jednoducho dokázať indukciou podľa zložitosti vzhľadom na logické spojky $\neg$ a (napríklad) $\wedge$. Pre atomickú formulu φ sa stačí odvolať na Úlohu 6.1.2. Indukčné kroky pre $\neg$ a $\wedge$ prenechávame čitateľovi.

(b) Univerzálna formula φ má tvar $(\forall y_1, \ldots, y_m)\psi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ pre nejakú otvorenú formulu ψ. Podmienka $\mathcal{A} \vDash \varphi(b_1, \ldots, b_n)$ znamená, že

$$(\forall a_1, \ldots, a_m \in A)\big(\mathcal{A} \vDash \psi(b_1, \ldots, b_n, a_1, \ldots, a_m)\big)$$

Keďže $B \subseteq A$, tak tým skôr

$$(\forall a_1, \ldots, a_m \in B)\big(\mathcal{A} \vDash \psi(b_1, \ldots, b_n, a_1, \ldots, a_m)\big)$$

Potrebný záver vyplýva z (a).

(c) možno dokázať analogicky ako (b), alebo odvodiť z (b) s využitím faktu, že každá existenčná formula je logicky ekvivalentná s negáciou univerzálnej.

6.1.5 Dôsledok. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry prvého rádu a $\mathcal{B} \subseteq \mathcal{A}$.*

(a) *Ak φ je uzavretá univerzálna formula, tak z $\mathcal{A} \vDash \varphi$ vyplýva $\mathcal{B} \vDash \varphi$.*

(b) *Ak φ je uzavretá existenčná formula, tak z $\mathcal{B} \vDash \varphi$ vyplýva $\mathcal{A} \vDash \varphi$.*

Inak povedané, univerzálne vlastnosti sa prenášajú na podštruktúry a existenčné vlastnosti sa prenášajú na nadštruktúry. Z toho naopak vyplýva, že vlastnosti, ktoré sa neprenášajú na podštruktúry (nadštruktúry), nemožno vyjadriť univerzálnymi (existenčnými) formulami. V nasledujúcej úlohe si predvedieme niekoľko využití tohto poznatku.

6.1.6 Úloha. (a) Pomocou formuly v jazyku, ktorého jediným špecifickým symbolom je znak binárnej operácie $\cdot$, vyjadrite podmienku existencie neutrálneho prvku tejto operácie. Dokážte, že táto podmienka sa nedá vyjadriť ani univerzálnou ani existenčnou formulou v tomto jazyku.

(b) Pomocou formuly v jazyku, ktorého jedinými špecifickými symbolmi sú znak binárnej operácie $\cdot$ a konštantný symbol e vyjadrite univerzálnou formulou podmienku, že e je neutrálny prvok tejto operácie. Dokážte, že táto podmienka sa nedá vyjadriť existenčnou formulou.

(c) V rovnakom jazyku ako v (b) (a za podmienky, že e plní úlohu neutrálneho prvku operácie $\cdot$) vyjadrite podmienku existencie inverzného prvku tejto operácie k ľubovoľnému prvku. Dokážte, že táto podmienka sa nedá vyjadriť ani univerzálnou ani existenčnou formulou v tomto jazyku.

(d) Nájdite samostatne ďalšie príklady vlastností, ktoré sa nedajú vyjadriť univerzálnymi, resp. existenčnými formulami istého jazyka.

6.1.7 Úloha. Uvažujme pole všetkých reálnych čísel ako štruktúru $(\mathbb{R};\, +, \cdot, 0, 1)$.

(a) Nájdite príklady podštruktúr tejto štruktúry, ktoré sú okruhmi, no nie sú poľami. Nájdite tiež príklady jej podštruktúr, ktoré nie sú ani okruhmi.

(b) Ako vyzerá vôbec najmenšie podpole poľa $(\mathbb{R};\, +, \cdot, 0, 1)$ a ako vyzerá jeho najmenšie podpole, ktoré obsahuje všetky celé čísla? Ako vyzerá najmenšie podpole poľa $(\mathbb{R};\, +, \cdot, 0, 1)$, ktoré obsahuje číslo $\sqrt{2}$, prípadne číslo $\sqrt[3]{5}$, resp. číslo π ?

(c) Ako vyzerá vôbec najmenšia podštruktúra poľa $(\mathbb{R};\, +, \cdot, 0, 1)$? Je to pole (okruh)?

V tejto súvislosti sa prirodzene vynárajú otázky, či možno všetky vlastnosti, ktoré sa prenášajú na podštruktúry (nadštruktúry), vyjadriť pomocou univerzálnych (existenčných) formúl. *A priori* sa totiž nedá vylúčiť, že by sa takto mohli prenášať aj niektoré vlastnosti vyjadrené formulami iného syntaktického tvaru. Prezradíme už vopred, že odpoveď na obe uvedené otázky je kladná, no na dôkazy týchto výsledkov si budeme musieť ešte nejakú chvíľu počkať.

6.2 Homomorfizmy

Homomorfizmom (zo) štruktúry $\mathcal{A} = (A;\, \dots)$ do štruktúry $\mathcal{B} = (B;\, \dots)$ nazývame zobrazenie $h\colon A \to B$ také, že pre ľubovoľný n-árny funkcionálny symbol $f \in F$, resp. relačný symbol $r \in R$ a všetky $a_1, \dots, a_n \in A$ platí

$$h\big(f^{\mathcal{A}}(a_1, \dots, a_n)\big) = f^{\mathcal{B}}(h(a_1), \dots, h(a_n))$$
$$(a_1, \dots, a_n) \in r^{\mathcal{A}} \;\Rightarrow\; (h(a_1), \dots, h(a_n)) \in r^{\mathcal{B}}$$

Špeciálne pre konštantný symbol $f \in F$ to znamená, že $h\big(f^{\mathcal{A}}\big) = f^{\mathcal{B}}$. Skutočnosť, že zobrazenie $h\colon A \to B$ je homomorfizmom z $\mathcal{A}$ do $\mathcal{B}$ symbolicky zapisujeme v tvare $h\colon \mathcal{A} \to \mathcal{B}$, resp. $h\colon (A;\, \dots) \to (B;\, \dots)$. Jednoducho povedané, homomorfizmy sú zobrazenia medzi štruktúrami, ktoré zachovávajú ich základné operácie (vrátane nulárnych) a relácie.

6.2.1 Úloha. Nech $h\colon \mathcal{A} \to \mathcal{B}$ je homomorfizmus, $t(x_1, \dots, x_n)$ je term a $\varphi(x_1, \dots, x_n)$ je atomická formula. Potom pre všetky $a_1, \dots, a_n \in A$ platí

$$h\big(t^{\mathcal{A}}(a_1, \dots, a_n)\big) = t^{\mathcal{B}}(h(a_1), \dots, h(a_n))$$
$$\mathcal{A} \vDash \varphi(a_1, \dots, a_n) \;\Rightarrow\; \mathcal{B} \vDash \varphi(h(a_1), \dots, h(b_n))$$

Dokážte.

Čitateľ sa už zrejme stretol s homomorfizmami grúp či homomorfizmami okruhov. Taktiež lineárne zobrazenia medzi vektorovými priestormi nad daným poľom F nie sú vlastne ničím iným ako homomorfizmami medzi štruktúrami tvaru $\big(V; F \cup \{+\}\big)$ s binárnou operáciou sčítania $+$ a unárnymi operáciami násobenia skalármi $f \in F$.

Stojí za povšimnutie, že na rozdiel od podštruktúr, vykazujú homomorfizmy medzi grupami značnú nezávislosť na jazyku. S vysvetlením tohto faktu sa zoznámime ešte v tomto paragrafe.

6.2.2 Úloha. Nech $\big(G; \cdot, e, {}^{-1}\big)$, $\big(H; \cdot, e, {}^{-1}\big)$ sú grupy a $h\colon G \to H$ je ľubovoľné zobrazenie. Dokážte, že nasledujúce podmienky sú ekvivalentné:

(i) h je homomorfizmus $\big(G; \cdot, e, {}^{-1}\big) \to \big(H; \cdot, e, {}^{-1}\big)$;

(ii) h je homomorfizmus $(G; \cdot, e) \to (H; \cdot, e)$;

(iii) h je homomorfizmus $(G; \cdot) \to (H; \cdot)$.

Kompozícia homomorfizmov je opäť homomorfizmus. Ďalej, homomorfizmy zachovávajú podštruktúry daných štruktúr „oboma smermi“. Jednoduché dôkazy týchto faktov ponechávame ako cvičenie čitateľovi.

6.2.3 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ sú štruktúry prvého rádu a $h\colon \mathcal{A} \to \mathcal{B}$, $g\colon \mathcal{B} \to \mathcal{C}$ sú homomorfizmy. Potom aj zložené zobrazenie $g \circ h\colon \mathcal{A} \to \mathcal{C}$ je homomorfizmus.*

6.2.4 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry prvého rádu a $h\colon \mathcal{A} \to \mathcal{B}$ je homomorfizmus.*

(a) *Ak $M \subseteq A$ je podštruktúra štruktúry $\mathcal{A}$, tak množina*

$$h[M] = \{h(a)\colon a \in M\} \subseteq B$$

je podštruktúrou štruktúry $\mathcal{B}$.

(b) *Ak $N \subseteq B$ je podštruktúra štruktúry $\mathcal{B}$, pričom množina*

$$h^{-1}[N] = \{a \in A\colon h(a) \in N\} \subseteq A$$

je neprázdna, tak $h^{-1}[N]$ je podštruktúra štruktúry $\mathcal{A}$.

Krátko povedané, homomorfný obraz podštruktúry je podštruktúra a homomorfný vzor podštruktúry, pokiaľ je neprázdny, je tiež podštruktúra. Uvedomme si, že v prípade, keď jazyk L obsahuje aspoň jeden konštantný symbol, je podmienka $h^{-1}[N] \neq \emptyset$ automaticky splnená pre každú podštruktúru N štuktúry $\mathcal{B}$.

Hovoríme, že štruktúra $\mathcal{B}$ je *homomorfným obrazom* štruktúry $\mathcal{A}$, ak existuje surjektívny homomorfizmus $h\colon \mathcal{A} \to \mathcal{B}$. Zaujíma nás, aké vlastnosti sa prenášajú na homomorfné obrazy. Hovoríme, že formula φ je *pozitívna*, ak je vytvorená z atomických formúl výlučne pomocou logických spojok $\wedge$, $\vee$ a kvantifikátorov $\forall$, $\exists$.

6.2.5 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry prvého rádu a $h\colon \mathcal{A} \to \mathcal{B}$ je surjektívny homomorfizmus. Potom pre ľubovoľnú pozitívnu formulu $\varphi(x_1, \ldots, x_n)$ a všetky $a_1, \ldots, a_n \in A$ platí*

$$\mathcal{A} \vDash \varphi(a_1, \ldots, a_n) \;\Rightarrow\; \mathcal{B} \vDash \varphi(h(a_1), \ldots, h(a_n))$$

Dôkaz. Budeme postupovať indukciou podľa zložitosti. Pre atomickú formulu φ sa stačí odvolať na Úlohu 6.2.1. Indukčné kroky vzhľadom na obe logické spojky, resp. oba kvantifikátory vykonáme naraz. Nech $*$ označuje ktorúkoľvek z logických spojok $\wedge$, $\vee$ a Q označuje ktorýkoľvek z kvantifikátorov $\forall$, $\exists$ (tak v jazyku L ako aj v prirodzenom jazyku).

Predpokladajme, že dokazovaná implikácia platí pre každú z formúl $\varphi(x_1, \ldots, x_n)$, $\psi(x_1, \ldots, x_n)$, a zvoľme ľubovoľné $a_1, \ldots, a_n \in A$. Potom podmienka

$$\mathcal{A} \vDash (\varphi * \psi)(a_1, \ldots, a_n)$$

je ekvivalentná s podmienkou

$$\mathcal{A} \vDash \varphi(a_1, \ldots, a_n) \ * \ \mathcal{A} \vDash \psi(a_1, \ldots, a_n)$$

Z toho podľa indukčného predpokladu vyplýva

$$\mathcal{B} \vDash \varphi(h(a_1), \ldots, h(a_n)) \ * \ \mathcal{B} \vDash \psi(h(a_1), \ldots, h(a_n))$$

čo je ekvivalentné s podmienkou

$$\mathcal{B} \vDash (\varphi * \psi)(h(a_1), \ldots, h(a_n))$$

Predpokladajme, že uvedená implikácia platí pre formulu $\varphi(x, x_1, \ldots, x_n)$, a zvoľme ľubovoľné $a_1, \ldots, a_n \in A$. Potom podmienka

$$\mathcal{A} \vDash (\mathrm{Q}\, x)\varphi(x, a_1, \ldots, a_n)$$

je ekvivalentná s podmienkou

$$(\mathrm{Q}\, a \in A)\big(\mathcal{A} \vDash \varphi(a, a_1, \ldots, a_n)\big)$$

Z toho podľa indukčného predpokladu vyplýva

$$(\mathrm{Q}\, a \in A)\big(\mathcal{B} \vDash \varphi(h(a), h(a_1), \ldots, h(a_n))\big)$$

Z uvedenej podmienky vyplýva

$$(\mathrm{Q}\, b \in B)\big(\mathcal{B} \vDash \varphi(b, h(a_1), \ldots, h(a_n))\big)$$

Pre existenčný kvantifikátor $\exists$ je to zrejmé: stačí položiť $b = h(a)$. Analogický záver pre univerzálny kvantifikátor $\forall$ platí vďaka surjektívnosti zobrazenia h: každé $b \in B$ má totiž tvar $b = h(a)$ pre nejaké $a \in A$. V oboch prípadoch tak dostávame

$$\mathcal{B} \vDash (\mathrm{Q}\, x)\varphi(x, h(a_1), \ldots, h(a_n))$$

6.2.6 Dôsledok. *Nech štruktúra $\mathcal{B}$ je homomorfným obrazom štruktúry $\mathcal{A}$. Potom pre ľubovoľnú uzavretú pozitívnu formulu φ z $\mathcal{A} \vDash \varphi$ vyplýva $\mathcal{B} \vDash \varphi$.*

Inak povedané, pozitívne vlastnosti sa prenášajú na homomorfné obrazy.

Pri podrobnejšom pohľade na dôkaz Tvrdenia 6.2.5 vyjde najavo, že podmienku surjektívnosti zobrazenia φ sme použili iba v indukčnom kroku pre univerzálny kvantifikátor. Tým sme vlastne zároveň dokázali nasledujúci výsledok.

6.2.7 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry prvého rádu a $h\colon \mathcal{A} \to \mathcal{B}$ je homomorfizmus. Potom pre ľubovoľnú existenčnú pozitívnu formulu $\varphi(x_1, \ldots, x_n)$ a všetky $a_1, \ldots, a_n \in A$ platí*

$$\mathcal{A} \vDash \varphi(a_1, \ldots, a_n) \;\Rightarrow\; \mathcal{B} \vDash \varphi(h(a_1), \ldots, h(a_n))$$

6.2.8 Úloha. Uvažujme o grupách ako o štruktúrach $(G; \cdot)$ v jazyku s jediným binárnym operačným symbolom $\cdot$. Vyjadrite formulami tohto jazyka vlastnosť $\varepsilon(u)$: „u je neutrálny prvok operácie $\cdot$“, resp. vzťah $\iota(x, y)$: „y je inverzný prvok k prvku x vzhľadom na operáciu $\cdot$“. Presvedčte sa, že $\varepsilon(u)$ aj $\iota(x, y)$ sú (univerzálne) pozitívne formuly. Stačí samotný tento fakt na vysvetlenie implikácie (iii) $\Rightarrow$ (i) z Úlohy 6.2.2? Za akých okolností áno a za akých nie? Premyslite si, ako možno v našom prípade „zachrániť situáciu“.

Z Tvrdenia 6.2.5 okrem iného vyplýva, že vlastnosti, ktoré sa neprenášajú na homomorfné obrazy, nemožno vyjadriť pomocou pozitívnych formúl.

6.2.9 Úloha. Okruh $(A; +, \cdot, 0)$ sa nazýva *obor integrity*, ak je komutatívny a spĺňa podmienku

$$(\forall\, x, y)(x \cdot y = 0 \;\Rightarrow\; (x = 0 \;\vee\; y = 0))$$

Dokážte, že vlastnosť okruhov „byť oborom integrity“ nemožno vyjadriť pozitívnou formulou. Nájdite ďalšie príklady vlastností štruktúr prvého rádu, ktoré nemožno vyjadriť pozitívnymi formulami.

Neskôr uvidíme, že aj, naopak, vlastnosti prvého rádu, ktoré sa prenášajú na homomorfné obrazy možno vyjadriť pomocou pozitívnych formúl.

Formula φ sa nazýva *negatívna*, ak je negáciou pozitívnej formuly. Dôkazy nasledujúcich výsledkov o spätnom prenose negatívnych vlastností z homomorfných obrazov na pôvodnú štruktúru prenechávame ako cvičenie čitateľovi.

6.2.10 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry prvého rádu a $h\colon \mathcal{A} \to \mathcal{B}$ je surjektívny homomorfizmus. Potom pre ľubovoľnú negatívnu formulu $\varphi(x_1, \ldots, x_n)$ a všetky prvky $a_1, \ldots, a_n \in A$ platí*

$$\mathcal{B} \vDash \varphi(h(a_1), \ldots, h(a_n)) \;\Rightarrow\; \mathcal{A} \vDash \varphi(a_1, \ldots, a_n)$$

Ak φ je navyše uzavretá, tak z $\mathcal{B} \vDash \varphi$ vyplýva $\mathcal{A} \vDash \varphi$.

6.2.11 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry prvého rádu a $h\colon \mathcal{A} \to \mathcal{B}$ je homomorfizmus. Potom pre ľubovoľnú univerzálnu negatívnu formulu $\varphi(x_1, \ldots, x_n)$ a všetky prvky $a_1, \ldots, a_n \in A$ platí*

$$\mathcal{B} \vDash \varphi(h(a_1), \ldots, h(a_n)) \;\Rightarrow\; \mathcal{A} \vDash \varphi(a_1, \ldots, a_n)$$

Ak φ je navyše uzavretá, tak z $\mathcal{B} \vDash \varphi$ vyplýva $\mathcal{A} \vDash \varphi$.

6.3 Izomorfizmy a vnorenia

Homomorfizmus $h\colon \mathcal{A} \to \mathcal{B}$ sa nazýva *izomorfizmus*, ak h je bijektívne zobrazenie a aj k nemu inverzné zobrazenie $h^{-1}\colon B \to A$ je homomorfizmus $h^{-1}\colon \mathcal{B} \to \mathcal{A}$. Fakt, že h je izomorfizmus štruktúry $\mathcal{A}$ na štruktúru $\mathcal{B}$ značíme $h\colon \mathcal{A} \xrightarrow{\sim} \mathcal{B}$. Hovoríme, že štruktúry $\mathcal{A}$, $\mathcal{B}$ sú *izomorfné*, ak existuje aspoň jeden izomorfizmus $h\colon \mathcal{A} \xrightarrow{\sim} \mathcal{B}$; píšeme $\mathcal{A} \cong \mathcal{B}$.

Nasledujúce pozorovanie je očividné.

6.3.1 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ sú štruktúry prvého rádu.*

(a) *Identické zobrazenie $\mathrm{Id}_A\colon A \to A$ je izomorfizmus $\mathrm{Id}_A\colon \mathcal{A} \xrightarrow{\sim} \mathcal{A}$.*

(b) *Ak $h\colon \mathcal{A} \xrightarrow{\sim} \mathcal{B}$ je izomorfizmus, tak aj k nemu inverzné zobrazenie $h^{-1}\colon \mathcal{B} \to \mathcal{A}$ je izomorfiznus.*

(c) *Ak $h\colon \mathcal{A} \xrightarrow{\sim} \mathcal{B}$, $g\colon \mathcal{B} \xrightarrow{\sim} \mathcal{C}$ sú izomorfimy, tak aj zložené zobrazenie $g \circ h\colon \mathcal{A} \xrightarrow{\sim} \mathcal{C}$ je izomorfizmus.*

V dôsledku toho pre ľubovoľné štruktúry $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ platí

$$\mathcal{A} \cong \mathcal{A}$$
$$\mathcal{A} \cong \mathcal{B} \;\Rightarrow\; \mathcal{B} \cong \mathcal{A}$$
$$\mathcal{A} \cong \mathcal{B} \wedge \mathcal{B} \cong \mathcal{C} \;\Rightarrow\; \mathcal{A} \cong \mathcal{C}$$

čiže vzťah izomorfnosti je *reflexívny*, *symetrický* a *tranzitívny*; jedným slovom, je to vzťah *ekvivalencie* na triede všetkých štruktúr jazyka L.

Čitateľ by si mal uvedomiť, že každý izomorfizmus je síce bijektívny homomorfizmus, no nie každý bijektívny homomorfizmus je izomorfizmus.

6.3.2 Príklad. Nech jazyk L obsahuje jediný špecifický symbol – unárny predikátový symbol P. Nech ďalej $\mathcal{A}_1 = (A; P_1)$, $\mathcal{A}_2 = (A; P_2)$ sú dve štruktúry jazyka L s tou istou základnou množinou A a podmnožiny $P_1, P_2 \subseteq A$ slúžia ako interpretácie symbola P v štruktúre $\mathcal{A}_1$, resp. $\mathcal{A}_2$. Potom identické zobrazenie $\mathrm{Id}_A\colon A \to A$ je určite bijektívne. Homomorfizmus $\mathrm{Id}_A\colon \mathcal{A}_1 \to \mathcal{A}_2$ je to zrejme práve vtedy, keď $P_1 \subseteq P_2$, a izomorfizmus $\mathrm{Id}_A\colon \mathcal{A}_1 \xrightarrow{\sim} \mathcal{A}_2$ je to práve vtedy, keď $P_1 = P_2$. Ak teda P_1 je vlastnou podmnožinou P_2, tak $\mathrm{Id}_A\colon \mathcal{A}_1 \to \mathcal{A}_2$ je príkladom bijektívneho homomorfizmu, ktorý nie je izomorfizmom.

Za určitých dodatočných podmienok je však už každý bijektívny homomorfizmus naozaj izomorfizmom.

6.3.3 Tvrdenie. *Predpokladajme, že jazyk L neobsahuje žiadne relačné symboly. Potom každý bijektívny homomorfizmus $h\colon \mathcal{A} \to \mathcal{B}$ medzi štruktúrami jazyka L je izomorfizmus.*

Dôkaz. Nech $h\colon \mathcal{A} \to \mathcal{B}$ je bijektívny homomorfizmus. Stačí overiť, že pre každý n-árny operačný symbol $f \in F$ a všetky $b_1, \ldots, b_n \in B$ platí

$$h^{-1}\big(f^{\mathcal{B}}(b_1, \ldots, b_n)\big) = f^{\mathcal{A}}\big(h^{-1}(b_1), \ldots, h^{-1}(b_n)\big)$$

Označme $a_i = h^{-1}(b_i)$ pre $1 \leq i \leq n$; potom $b_i = h(a_i)$. Ďalej, keďže h je homomorfizmus a $h^{-1} \circ h = \mathrm{Id}_A$,

$$\begin{aligned} h^{-1}\big(f^{\mathcal{B}}(b_1, \ldots, b_n)\big) &= h^{-1}\big(f^{\mathcal{B}}(h(a_1), \ldots, h(a_n))\big) \\ &= \big(h^{-1} \circ h\big)\big(f^{\mathcal{A}}(a_1, \ldots, a_n)\big) \\ &= f^{\mathcal{A}}\big(h^{-1}(b_1), \ldots, h^{-1}(b_n)\big) \end{aligned}$$

6.3.4 Dôsledok. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry prvého rádu. Potom zobrazenie $h\colon A \to B$ je izomorfizmus $h\colon \mathcal{A} \xrightarrow{\sim} \mathcal{B}$ práve vtedy, keď je bijektívne a pre každý n-árny funkcionálny symbol $f \in F$, resp. relačný symbol $r \in R$ a všetky $a_1, \ldots, a_n \in A$ platí*

$$\begin{aligned} &h\big(f^{\mathcal{A}}(a_1, \ldots, a_n)\big) = f^{\mathcal{B}}(h(a_1), \ldots, h(a_n)) \\ &(a_1, \ldots, a_n) \in r^{\mathcal{A}} \;\Leftrightarrow\; (h(a_1), \ldots, h(a_n)) \in r^{\mathcal{B}} \end{aligned}$$

Zobrazenie $h\colon A \to B$ medzi základnými množinami štruktúr $\mathcal{A}$, $\mathcal{B}$ nazývame *vnorením* štruktúry $\mathcal{A}$ do štruktúry $\mathcal{B}$, ak h je izomorfizmom štruktúry $\mathcal{A}$ na podštruktúru $h[A]$ štruktúry $\mathcal{B}$. V tom prípade píšeme $h\colon \mathcal{A} \hookrightarrow \mathcal{B}$.

Základným a najjednoduchším príkladom vnorenia je vnorenie podštruktúry $\mathcal{B} \subseteq \mathcal{A}$ do štruktúry $\mathcal{A}$ prostredníctvom identického zobrazenia $\mathrm{Id}_B\colon B \hookrightarrow A$. Taktiež je zrejmé, že kompozícia vnorení $h\colon \mathcal{A} \hookrightarrow \mathcal{B}$, $g\colon \mathcal{B} \hookrightarrow \mathcal{C}$ je sama vnorením $g \circ h\colon \mathcal{A} \hookrightarrow \mathcal{C}$.

Z predošlého Dôsledku 6.3.4 okamžite vyplýva nasledujúca podrobnejšia charakterizácia vnorení.

6.3.5 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry prvého rádu. Potom zobrazenie $h\colon A \to B$ je vnorením $h\colon \mathcal{A} \hookrightarrow \mathcal{B}$ práve vtedy, keď je injektívne a pre každý n-árny funkcionálny symbol $f \in F$, resp. relačný symbol $r \in R$ a všetky $a_1, \ldots, a_n \in A$ platí*

$$\begin{aligned} &h\big(f^{\mathcal{A}}(a_1, \ldots, a_n)\big) = f^{\mathcal{B}}(h(a_1), \ldots, h(a_n)) \\ &(a_1, \ldots, a_n) \in r^{\mathcal{A}} \;\Leftrightarrow\; (h(a_1), \ldots, h(a_n)) \in r^{\mathcal{B}} \end{aligned}$$

Z toho vyplýva, že ak jazyk L neobsahuje žiadne relačné symboly, tak každý injektívny homomorfizmus je vnorenie.

Ešte si uvedomme, že i samotná vlastnosť injektívnosti zobrazenia h

$$a = b \;\Leftrightarrow\; h(a) = h(b)$$

pre všetky $a, b \in A$, nie je ničím iným ako podmienkou obojsmerného zachovávania relácie rovnosti. Kým implikácia $\Rightarrow$ je triviálne splnená „vždy“, injektívnosť je daná práve obrátenou implikáciou $\Leftarrow$.

6.3.6 Úloha. Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry prvého rádu. Dokážte, že zobrazenie $h\colon A \to B$ je vnorením $h\colon \mathcal{A} \hookrightarrow \mathcal{B}$ práve vtedy, keď pre ľubovoľnú atomickú formulu $\varphi(x_1, \ldots, x_n)$ a všetky $a_1, \ldots, a_n \in A$ platí

$$\mathcal{A} \vDash \varphi(a_1, \ldots, a_n) \;\Leftrightarrow\; \mathcal{B} \vDash \varphi(h(a_1), \ldots, h(a_n))$$

6.3.7 Tvrdenie. *Nech $(A; <)$, $(B; <)$ sú čiastočne usporiadané množiny. Ak $(A; <)$ je lineárne usporiadaná, tak každý homomorfizmus $h\colon (A; <) \to (B; <)$ je zároveň vnorením. Ak h je navyše surjektívny, tak je to izomorfizmus $h\colon (A; <) \xrightarrow{\sim} (B; <)$.*

Dôkaz. Nech $h\colon (A; <) \to (B; <)$ je homomorfizmus. Najprv ukážeme, že h je injektívne zobrazenie. Zvoľme dva rôzne prvky $a, b \in A$. Keďže usporiadanie $<$ množiny A je lineárne, platí $a < b$ alebo $b < a$. V prvom prípade z toho dostávame $h(a) < h(b)$, v druhom $h(b) < h(a)$, teda každopádne $h(a) \neq h(b)$. Ďalej treba overiť, že pre ľubovoľné $a, b \in A$ z podmienky $h(a) < h(b)$ vyplýva $a < b$. Keďže h je injektívny, z $h(a) < h(b)$ vyplýva $a \neq b$. Potom $a < b$ alebo $b < a$. Druhá možnosť by však mala za následok $h(b) < h(a)$, čo je v spore s predpokladom $h(a) < h(b)$. Z toho okamžite vyplýva aj druhá časť tvrdenia.

6.3.8 Úloha. Sformulujte a dokážte analogické tvrdenie pre homomorfizmy a vnorenia čiastočne usporiadaných množín s neostrým usporiadaním $\leq$.

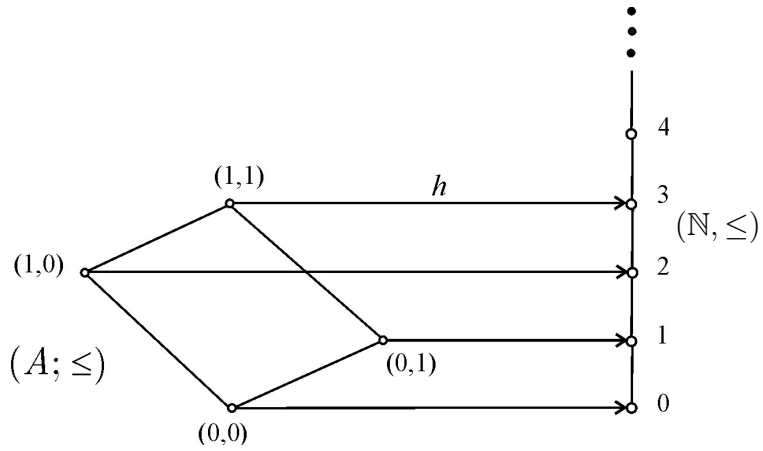
6.3.9 Príklad. Nech $(A; \leq)$ je množina $A = \{0, 1\} \times \{0, 1\}$ s čiastočným usporiadaním po zložkách, čiže

$$(a_1, b_1) \leq (a_2, b_2) \;\Leftrightarrow\; a_1 \leq a_2 \wedge b_1 \leq b_2$$

pre $(a_1, b_1), (a_2, b_2) \in A$. Nech ďalej $(\mathbb{N}; \leq)$ je množina všetkých prirodzených čísel s obvyklým (lineárnym) usporiadaním. Zobrazenie $h\colon A \to B$ je dané predpisom

$$h(a, b) = 2a + b$$

pre $(a, b) \in A$ (pozri obrázok).



Na prvý pohľad je zrejmé, že $h\colon (A; \leq) \to (\mathbb{N}; \leq)$ je injektívny homomorfizmus, no nie je to vnorenie. V $(\mathbb{N}; \leq)$ platí $h(0, 1) = 1 \leq 2 = h(1, 0)$, no v $(A; \leq)$ neplatí $(0, 1) \leq (1, 0)$ – prvky $(0, 1)$, $(1, 0)$ sú totiž neporovnateľné.

Z Dôsledku 6.1.5 okamžite vyplýva jeho nasledujúce zovšeobecnenie.

6.3.10 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry prvého rádu a $h\colon \mathcal{A} \hookrightarrow \mathcal{B}$ je vnorenie.*
(a) *Ak φ je uzavretá univerzálna formula, tak z $\mathcal{B} \models \varphi$ vyplýva $\mathcal{A} \models \varphi$.*
(b) *Ak φ je uzavretá existenčná formula, tak z $\mathcal{A} \models \varphi$ vyplýva $\mathcal{B} \models \varphi$.*

6.3.11 Úloha. (a) Sformulujte (a ak pociťujete potrebu, tak aj dokážte) analogické zovšeobecnenie Tvrdenia 6.1.4.
(b) Aké vlastnosti prvého rádu sa prenášajú prostredníctvom izomorfizmov?

6.4 Elementárna ekvivalencia a elementárne podštruktúry

Izomorfné L-štruktúry $\mathcal{A}$, $\mathcal{B}$ možno považovať za „úplne rovnaké“ a v prípade potreby ich pomocou príslušného izomorfizmu dokonca stotožniť. Na mnohé účely teórie modelov je však ekvivalencia izomorfnosti „príliš prísna“. Z istého hľadiska možno štruktúry $\mathcal{A}$, $\mathcal{B}$ považovať za „rovnaké“ už vtedy, keď majú rovnaké vlastnosti vyjadrené v jazyku L.

Hovoríme, že štruktúry $\mathcal{A}$, $\mathcal{B}$ sú *elementárne ekvivalentné*, označenie $\mathcal{A} \equiv \mathcal{B}$, ak pre každú uzavretú formulu φ platí

$$\mathcal{A} \models \varphi \;\Leftrightarrow\; \mathcal{B} \models \varphi$$

Okamžite je zrejmé, že vzťah elementárnej ekvivalencie je reflexívny, symetrický a tranzitívny, t. j. pre ľubovoľné štruktúry $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ platí

$$\mathcal{A} \equiv \mathcal{B}$$
$$\mathcal{A} \equiv \mathcal{B} \;\Rightarrow\; \mathcal{B} \equiv \mathcal{A}$$
$$\mathcal{A} \equiv \mathcal{B} \wedge \mathcal{B} \equiv \mathcal{C} \;\Rightarrow\; \mathcal{A} \equiv \mathcal{C}$$

teda je naozaj vzťahom ekvivalencie na triede všetkých štruktúr jazyka L. Rovnako je jasné, že izomorfné štruktúry sú elementárne ekvivalentné, čiže

$$\mathcal{A} \cong \mathcal{B} \;\Rightarrow\; \mathcal{A} \equiv \mathcal{B}$$

pre ľubovoľné $\mathcal{A}$, $\mathcal{B}$. O existencii elementárne ekvivalentných štruktúr, ktoré nie sú izomorfné (napr. z dôvodu rôznych mohutností), sa budeme môcť presvedčiť zakrátko.

6.4.1 Úloha. Nech aspoň jedna zo štruktúr $\mathcal{A}$, $\mathcal{B}$ je konečná. Potom $\mathcal{A} \equiv \mathcal{B}$ práve vtedy, keď $\mathcal{A} \cong \mathcal{B}$. Dokážte. (*Pomôcka*: Najprv dokážte, že ak je napr. štruktúra $\mathcal{A}$ konečná a $|A| = n$, tak z $\mathcal{A} \equiv \mathcal{B}$ vyplýva $|B| = n$. Ďalej skúste dokázať implikáciu $\mathcal{A} \equiv \mathcal{B} \Rightarrow \mathcal{A} \cong \mathcal{B}$ za dodatočného predpokladu, že jazyk L má len konečne mnoho špecifických symbolov. Nakoniec skúste všeobecný prípad previesť na túto situáciu.)

Teóriou štruktúry $\mathcal{A}$ nazývame množinu

$$\mathrm{Th}(\mathcal{A}) = \{\varphi \in \mathrm{Form}(L)\colon \varphi \text{ je uzavretá a } \mathcal{A} \models \varphi\}$$

všetkých uzavretých formúl jazyka L, ktoré platia v štruktúre $\mathcal{A}$. Zrejme pre ľubovoľné štruktúry $\mathcal{A}$, $\mathcal{B}$ platí

$$\mathcal{A} \equiv \mathcal{B} \;\Leftrightarrow\; \mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$$

Keďže pre každú štruktúru $\mathcal{A}$ je $\mathrm{Th}(\mathcal{A})$ úplná teória, pre ľubovoľné štrutúry $\mathcal{A}$, $\mathcal{B}$ sú nasledujúce tri podmienky ekvivalentné:

$$\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B}), \quad \mathrm{Th}(\mathcal{A}) \subseteq \mathrm{Th}(\mathcal{B}), \quad \mathrm{Th}(\mathcal{A}) \supseteq \mathrm{Th}(\mathcal{B})$$

To však znamená, že logickú ekvivalenciu v definícii elementárnej ekvivalencie možno nahradiť ktoroukoľvek z implikácií $\Rightarrow$, $\Leftarrow$.

6.4.2 Tvrdenie. *Pre ľubovoľné štruktúry $\mathcal{A}$, $\mathcal{B}$ sú nasledujúce podmienky ekvivalentné:*

(i) $\mathcal{A} \equiv \mathcal{B}$;

(ii) *pre každú uzavretú formulu φ platí* $\mathcal{A} \vDash \varphi \Rightarrow \mathcal{B} \vDash \varphi$;

(iii) *pre každú uzavretú formulu φ platí* $\mathcal{B} \vDash \varphi \Rightarrow \mathcal{A} \vDash \varphi$.

K rovnakému záveru možno dospieť aj na základe skutočnosti, že systém všetkých uzavretých formúl jazyka L je uzavretý vzhľadom na negáciu. Rozmyslite si ako.

Ešte tesnejší vzťah podobnosti štruktúr je vzťah elementárnej podštruktúry. Hovoríme, že štruktúra $\mathcal{A}$ je *elementárnou podštruktúrou* štruktúry $\mathcal{B}$, prípadne, že štruktúra $\mathcal{B}$ je *elementárnym rozšírením* štruktúry $\mathcal{A}$, ak $A \subseteq B$ a pre *každú* formulu $\varphi(x_1, \ldots, x_n)$ jazyka L a všetky $a_1, \ldots, a_n \in A$ platí

$$\mathcal{A} \vDash \varphi(a_1, \ldots, a_n) \;\Leftrightarrow\; \mathcal{B} \vDash \varphi(a_1, \ldots, a_n)$$

Tento fakt zapisujeme symbolicky v tvare $\mathcal{A} \prec \mathcal{B}$, prípadne $\mathcal{B} \succ \mathcal{A}$. Rozmyslite si, že z podmienky $\mathcal{A} \prec \mathcal{B}$ už vyplýva $\mathcal{A} \subseteq \mathcal{B}$, teda každá elementárna podštruktúra štruktúry $\mathcal{B}$ je naozaj jej podštruktúrou.

6.4.3 Úloha. Overte, že pre ľubovolné štruktúry $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ platí

$$\mathcal{A} \prec \mathcal{A}$$
$$\mathcal{A} \prec \mathcal{B} \;\Rightarrow\; \mathcal{A} \equiv \mathcal{B}$$
$$\mathcal{A} \prec \mathcal{B} \wedge \mathcal{B} \prec \mathcal{C} \;\Rightarrow\; \mathcal{A} \prec \mathcal{C}$$
$$\mathcal{A} \prec \mathcal{C} \wedge \mathcal{B} \prec \mathcal{C} \wedge \mathcal{A} \subseteq \mathcal{B} \;\Rightarrow\; \mathcal{A} \prec \mathcal{B}$$

Kedže aj systém všetkých L-formúl je uzavretý vzhľadom na negáciu, možno i v definícii elementárnej podštruktúry nahradiť logickú ekvivalenciu ktoroukoľvek z implikácií $\Rightarrow$, $\Leftarrow$.

6.4.4 Tvrdenie. *Pre ľubovoľné štruktúry $\mathcal{A}$, $\mathcal{B}$ také, že $A \subseteq B$, sú nasledujúce podmienky ekvivalentné:*

(i) $\mathcal{A} \prec \mathcal{B}$

(ii) *pre ľubovoľnú L-formulu $\varphi(x_1, \ldots, x_n)$ a všetky $a_1, \ldots, a_n \in A$ platí*

$$\mathcal{A} \vDash \varphi(a_1, \ldots, a_n) \;\Rightarrow\; \mathcal{B} \vDash \varphi(a_1, \ldots, a_n)$$

(iii) *pre ľubovoľnú L-formulu $\varphi(x_1, \ldots, x_n)$ a všetky $a_1, \ldots, a_n \in A$ platí*

$$\mathcal{B} \vDash \varphi(a_1, \ldots, a_n) \;\Rightarrow\; \mathcal{A} \vDash \varphi(a_1, \ldots, a_n)$$

6.4.5 Príklad. Pole $\mathcal{Q} = (\mathbb{Q}; +, \cdot, 0, 1)$ všetkých racionálnych čísel je podštruktúrou poľa $\mathcal{R} = (\mathbb{R}; +, \cdot, 0, 1)$ všetkých reálnych čísel. Tieto polia však nie sú elementárne ekvivalentné. Keďže v $\mathbb{Q}$ neexistuje odmocnina z dvoch, máme

$$\mathcal{Q} \vDash \neg(\exists\, x)(x \cdot x = 1 + 1)$$

zatiaľ čo $\sqrt{2} \in \mathbb{R}$, teda

$$\mathcal{R} \vDash (\exists\, x)(x \cdot x = 1 + 1)$$

Preto nemôže platiť $\mathcal{Q} \prec \mathcal{R}$. Skúste analogicky zdôvodniť, že pole $\mathcal{R}$ nie je elementárne ekvivalentné s poľom $(\mathbb{C}; +, \cdot, 0, 1)$ všetkých komplexných čísel, teda nemôže byť jeho elementárnou podštruktúrou. Na druhej strane, ako dokázal Alfred Tarski v r. 1930, pole $(\mathbb{A}; +, \cdot, 0, 1)$ všetkých algebraických čísel (t. j. riešení polynomických rovníc s racionálnymi koeficientmi) je elementárnou podštruktúrou poľa $(\mathbb{C}; +, \cdot, 0, 1)$. Podobne, pole $(\mathbb{A} \cap \mathbb{R}; +, \cdot, 0, 1)$ všetkých reálnych algebraických čísel je elementárnou podštruktúrou poľa $\mathcal{R}$. A keďže množiny $\mathbb{R}$ aj $\mathbb{C}$ majú mohutnosť kontinua, zatiaľ čo množiny $\mathbb{A} \cap \mathbb{R}$ a $\mathbb{A}$ sú spočítateľné, elementárne ekvivalentné polia $(\mathbb{A}; +, \cdot, 0, 1) \equiv (\mathbb{C}; +, \cdot, 0, 1)$, ani $(\mathbb{A} \cap \mathbb{R}; +, \cdot, 0, 1) \equiv (\mathbb{R}; +, \cdot, 0, 1)$ nemôžu byť izomorfné.

Nasledujúci výsledok, známy pod názvom Tarského alebo tiež Tarského-Vaughtovo kritérium, takpovediac lokalizuje otázku, či $\mathcal{A} \prec \mathcal{B}$, výlučne do „väčšej“ z oboch štruktúr $\mathcal{B} \supseteq \mathcal{A}$.

6.4.6 Veta. *Nech $\mathcal{A}$, $\mathcal{B}$ sú ľubovoľné štruktúry, pričom $\mathcal{A} \subseteq \mathcal{B}$. Potom nasledujúce podmienky sú ekvivalentné:*

(i) $\mathcal{A} \prec \mathcal{B}$

(ii) *Pre ľubovoľnú formulu $\varphi(x, x_1, \ldots, x_n)$ a všetky $a_1, \ldots, a_n \in A$ platí:*

$$(\exists\, b \in B)\big(\mathcal{B} \vDash \varphi(b, a_1, \ldots, a_n)\big) \;\Rightarrow\; (\exists\, a \in A)\big(\mathcal{B} \vDash \varphi(a, a_1, \ldots, a_n)\big)$$

Podmienka (ii) vlastne hovorí: ak má úloha „nájdi x také, že $\mathcal{B} \vDash \varphi(x, a_1, \ldots, a_n)$“ s parametrami $a_1, \ldots, a_n \in A$ aspoň jedno riešenie $b \in B$, tak táto úloha má aj nejaké riešenie $a \in A$.

Dôkaz (i) $\Rightarrow$ (ii): Nech $\mathcal{A} \prec \mathcal{B}$. Predpokladajme, že $\varphi(x, x_1, \ldots, x_n)$ je formula a pre $a_1, \ldots, a_n \in A$ platí $(\exists\, b \in B)\big(\mathcal{B} \vDash \varphi(b, a_1, \ldots, a_n)\big)$, čiže $\mathcal{B} \vDash (\exists\, x)\varphi(x, a_1, \ldots, a_n)$. Potom aj $\mathcal{A} \vDash (\exists\, x)\varphi(x, a_1, \ldots, a_n)$, t. j. $(\exists\, a \in A)\big(\mathcal{A} \vDash \varphi(a, a_1, \ldots, a_n)\big)$. Pre také a máme $\mathcal{B} \vDash \varphi(a, a_1, \ldots, a_n)$, teda $(\exists\, a \in A)\big(\mathcal{B} \vDash \varphi(a, a_1, \ldots, a_n)\big)$.

(ii) $\Rightarrow$ (i): Predpokladajme (ii). Indukciou podľa zložitosti dokážeme, že pre každú formulu $\varphi(x_1, \ldots, x_n)$ a všetky $a_1, \ldots, a_n \in A$ platí

$$\mathcal{A} \vDash \varphi(a_1, \ldots, a_n) \;\Leftrightarrow\; \mathcal{B} \vDash \varphi(a_1, \ldots, a_n)$$

Pre atomickú φ je to tak, lebo $\mathcal{A} \subseteq \mathcal{B}$. Indukčné kroky pre logické spojky $\neg$ a $\wedge$ sú priamočiare – prenechávame ich čitateľovi. Takže sa obmedzíme iba na indukčný krok pre existenčný kvantifikátor $\exists$. Predpokladajme teda, že uvedená ekvivalencia platí

pre formulu $\varphi(x, x_1, \dots, x_n)$ a všetky $a, a_1, \dots, a_n \in A$. Potrebujeme overiť jej platnosť pre formulu $(\exists\, x)\varphi(x, x_1, \dots, x_n)$ a všetky $a_1, \dots, a_n \in A$. Pre ne sú nasledujúce podmienky ekvivalentné:

$$\mathcal{A} \vDash (\exists\, x)\varphi(x, a_1, \dots, a_n) \tag{1}$$

$$(\exists\, a \in A)\big(\mathcal{A} \vDash \varphi(a, a_1, \dots, a_n)\big) \tag{2}$$

$$(\exists\, a \in A)\big(\mathcal{B} \vDash \varphi(a, a_1, \dots, a_n)\big) \tag{3}$$

$$(\exists\, b \in B)\big(\mathcal{B} \vDash \varphi(b, a_1, \dots, a_n)\big) \tag{4}$$

$$\mathcal{B} \vDash (\exists\, x)\varphi(x, a_1, \dots, a_n) \tag{5}$$

Na vysvetlenie dodávame, že ekvivalencie (1) $\Leftrightarrow$ (2) a (4) $\Leftrightarrow$ (5) vyplývajú z definície spĺňania formúl v štruktúrach, ekvivalencia (2) $\Leftrightarrow$ (3) je dôsledkom indukčného predpokladu, implikácia (3) $\Rightarrow$ (4) je triviálna, zatiaľ čo obrátená implikácia (4) $\Rightarrow$ (3) je priamo podmienka (ii) dokazovanej vety.

Zobrazenie $h\colon A \to B$ medzi základnými množinami štruktúr $\mathcal{A}$, $\mathcal{B}$ nazývame *elementárnym vnorením* štruktúry $\mathcal{A}$ do štruktúry $\mathcal{B}$, ak h je izomorfizmom štruktúry $\mathcal{A}$ na *elementárnu* podštruktúru $h[A]$ štruktúry $\mathcal{B}$. V tom prípade píšeme $h\colon \mathcal{A} \xrightarrow{\prec} \mathcal{B}$.

Najjednoduchším príkladom elementárneho vnorenia je vnorenie elementárnej podštruktúry $\mathcal{B} \prec \mathcal{A}$ do štruktúry $\mathcal{A}$ prostredníctvom identického zobrazenia $\mathrm{Id}_B : B \to A$. Taktiež je zrejmé, že kompozícia elementárnych vnorení $h\colon \mathcal{A} \xrightarrow{\prec} \mathcal{B}$, $g\colon \mathcal{B} \xrightarrow{\prec} \mathcal{C}$ je sama elementárnym vnorením $g \circ h\colon \mathcal{A} \xrightarrow{\prec} \mathcal{C}$.

6.4.7 Úloha. (a) Sformulujte a dokážte zovšeobecnenia Tvrdenia 6.4.4 a Vety 6.4.6 z elementárnych podštruktúr na elementárne vnorenia.

(b) Nech $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ sú štruktúry, $h\colon \mathcal{A} \hookrightarrow \mathcal{B}$ je vnorenie a $g\colon \mathcal{B} \xrightarrow{\prec} \mathcal{C}$ je elementárne vnorenie také, že zložené zobrazenie $g \circ h\colon \mathcal{A} \xrightarrow{\prec} \mathcal{C}$ je tiež elementárne vnorenie. Dokážte, že potom aj $h\colon \mathcal{A} \xrightarrow{\prec} \mathcal{B}$ je elementárne vnorenie. Ktorý skôr uvedený fakt o elementárnych podštruktúrach zovšeobecňuje toto tvrdenie?

6.5 Diagramy štruktúr

V tomto paragrafe sa zbežne zoznámime s tzv. *metódou diagramov*, založenou na rozširovaní základného jazyka o nové konštantné symboly. Táto metóda nám umožní konštruovať z daných štruktúr nové štruktúry predpísaných vlastností, ktoré reflektujú isté vlastnosti pôvodných štruktúr, ako modely vhodných teórií v rozšírenom jazyku.

Nech L je jazyk prvého rádu, $\mathcal{A} = (A; \dots)$ je L-štruktúra a $M \subseteq A$. Jazyk, ktorý vznikne z jazyka L jeho rozšírením o množinu nových konštánt $\{c_a\colon a \in M\}$ (pričom konštantné symboly c_a prislúchajúce rôznym prvkom množiny M sú rôzne), budeme značiť L_M. Štruktúru jazyka L_M, ktorá vznikne zo štruktúry $\mathcal{A}$ tak, že interpretácie symbolov pôvodného jazyka L ponecháme nezmenené a každú z nových konštánt c_a budeme interpretovať ako prvok $a \in M$, označíme

$$\mathcal{A}_M = (\mathcal{A}, a)_{a \in M}$$

Najdôležitejší pre nás bude špeciálny prípad, keď $M = A$; vtedy $\mathcal{A}_A = (\mathcal{A}, a)_{a\in A}$. Podobne, ak $\mathcal{B}$ je ďalšia L-štruktúra a $h\colon A \to B$ je nejaké zobrazenie, tak $\big(\mathcal{B}, h(a)\big)_{a\in A}$ označuje štruktúru jazyka L_A, v ktorej sú jednotlivé konštanty c_a interpretované prvkami $h(a)$ (a pôvodné symboly jazyka L interpretované rovnako ako v $\mathcal{B}$).

Kvôli stručnosti budeme negácie atomických formúl nazývať *negatomickými* formulami. *Atomickým diagramom*, alebo len krátko *diagramom* L-štruktúry $\mathcal{A}$, nazývame množinu formúl

$$\mathrm{D}(\mathcal{A}) = \{\varphi \in \mathrm{Form}(L_A)\colon \varphi \text{ je uzavretá atomická alebo negatomická a } \mathcal{A}_A \vDash \varphi\}$$

Uvedomte si, že každá uzavretá formula φ jazyka L_A má tvar $\psi(c_{a_1}, \dots, c_{a_n})$ pre istú formulu $\psi(x_1, \dots, x_n)$ pôvodného jazyka L. V takom prípade je podmienka $\mathcal{A}_A \vDash \varphi$, t. j.

$$\mathcal{A}_A \vDash \psi(c_{a_1}, \dots, c_{a_n})$$

ekvivalentná s podmienkou

$$\mathcal{A} \vDash \psi(a_1, \dots, a_n)$$

takže si môžeme dovoliť nerozlišovať medzi predposledným a posledným zápisom.

Pozitívnym atomickým diagramom L-štruktúry $\mathcal{A}$ nazývame množinu formúl

$$\mathrm{D}^+(\mathcal{A}) = \{\varphi \in \mathrm{Form}(L_A)\colon \varphi \text{ je uzavretá atomická a } \mathcal{A}_A \vDash \varphi\}$$

Zrejme plati $\mathrm{D}^+(\mathcal{A}) \subseteq \mathrm{D}(\mathcal{A})$, pričom „menší“ z oboch diagramov $\mathrm{D}^+(\mathcal{A})$ je tvorený všetkými atomickými formulami z „väčšieho“ diagramu $\mathrm{D}(\mathcal{A})$. Zdá sa teda, že „väčší“ diagram $\mathrm{D}(\mathcal{A})$ obsahuje viac informácie ako ten „menší“ $\mathrm{D}^+(\mathcal{A})$. Nie je však tomu tak – v skutočnosti obsahujú oba diagramy rovnaké množstvo informácie. Z „menšieho“ diagramu $\mathrm{D}^+(\mathcal{A})$ možno totiž „väčší“ diagram $\mathrm{D}(\mathcal{A})$ jednoducho zrekonštruovať. Z dvojice formúl $\varphi(a_1, \dots, a_n)$, $\neg\varphi(a_1, \dots, a_n)$, kde $\varphi(x_1, \dots, x_n)$ je atomická L-formula a $a_1, \dots, a_n \in A$, patrí totiž do diagramu $\mathrm{D}(\mathcal{A})$ práve jedna. Ak $\varphi(a_1, \dots, a_n) \in \mathrm{D}^+(\mathcal{A})$, tak je to $\varphi(a_1, \dots, a_n)$; ak $\varphi(a_1, \dots, a_n) \notin \mathrm{D}^+(\mathcal{A})$, je to $\neg\varphi(a_1, \dots, a_n)$. Dôvody, pre ktoré závadzame aj redundantný a zdanlivo zbytočne veľký diagram $\mathrm{D}(\mathcal{A})$, vyjdú najavo o chvíľu.

6.5.1 Príklad. Nech $\mathcal{A} = (A; \cdot)$ je konečná množina s jednou binárnou operáciou $\cdot$. Potom diagramy $\mathrm{D}(\mathcal{A})$, $\mathrm{D}^+(\mathcal{A})$ obsahujú rovnakú informáciu ako Cayleyho multiplikatívna tabuľka štruktúry $\mathcal{A}$. Prvok $c \in A$ sa v tejto tabuľke nachádza v riadku prvku $a \in A$ a v stĺpci prvku $b \in A$ práve vtedy, keď v $\mathcal{A}$ platí $a \cdot b = c$.

Nasledujúce tvrdenia vyjadrujú niektoré nám už známe vzťahy medzi štruktúrami pomocou práve zavedených diagramov.

6.5.2 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry jazyka L.*

(a) *Nech $A \subseteq B$. Potom $\mathcal{A} \subseteq \mathcal{B}$ práve vtedy, keď $\mathcal{B}_A \vDash \mathrm{D}(\mathcal{A})$.*

(b) *Nech $h\colon A \to B$. Potom h je vnorenie $\mathcal{A}$ do $\mathcal{B}$ práve vtedy, keď $\big(\mathcal{B}, h(a)\big)_{a\in A} \vDash \mathrm{D}(\mathcal{A})$.*

6.5.3 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry jazyka L a $h\colon A \to B$. Potom h je homomorfizmus z $\mathcal{A}$ do $\mathcal{B}$ práve vtedy, keď $\big(\mathcal{B}, h(a)\big)_{a\in A} \vDash \mathrm{D}^+(\mathcal{A})$.*

Z oboch práve vyslovených tvrdení zároveň jasne vidno rozdielne úlohy, ktoré plnia oba diagramy $\mathrm{D}(\mathcal{A})$ a $\mathrm{D}^+(\mathcal{A})$.

Ak sa nezameriame iba na atomické formuly, môžeme zaviesť ešte jeden typ diagramov. *Elementárnym* alebo tiež *úplným diagramom* L-štruktúry $\mathcal{A}$ nazývame množinu formúl

$$\mathrm{Th}(\mathcal{A}_A) = \{\varphi \in \mathrm{Form}(L_A)\colon \varphi \text{ je uzavretá a } \mathcal{A}_A \vDash \varphi\}$$

Nasledujúce tvrdenie je priamou analógiou Tvrdenia 6.5.2.

6.5.4 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry jazyka L.*

(a) *Nech $A \subseteq B$. Potom $\mathcal{A} \prec \mathcal{B}$ práve vtedy, keď $\mathcal{B}_A \vDash \mathrm{Th}(\mathcal{A}_A)$.*

(b) *Nech $h\colon A \to B$. Potom h je elementárne vnorenie $\mathcal{A}$ do $\mathcal{B}$ práve vtedy, keď $\big(\mathcal{B}, h(a)\big)_{a\in A} \vDash \mathrm{Th}(\mathcal{A}_A)$.*

Pre úplnosť si ešte uvedomme, že aj *teóriu štruktúry* $\mathcal{A}$ jazyka L

$$\mathrm{Th}(\mathcal{A}) = \{\varphi \in \mathrm{Form}(L)\colon \varphi \text{ je uzavretá a } \mathcal{A} \vDash \varphi\}$$

možno považovať za istý typ diagramu, pomocou ktorého možno vyjadriť vzťah elementárnej ekvivalencie.

6.5.5 Tvrdenie. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry jazyka L. Potom $\mathcal{A} \equiv \mathcal{B}$ práve vtedy, keď $\mathcal{B} \vDash \mathrm{Th}(\mathcal{A})$.*

6.5.6 Úloha. S využitím rozšírenia jazyka L o vhodné konštantné symboly zostručnite formuláciu podmienky (ii) v Tarského-Vaughtovom kritériu pre elementárne podštruktúry a zjednodušte zápis niektorých častí jeho dôkazu.

6.6 Vety Löwenheima, Skolema a Tarského

V tomto paragrafe dokážeme dva výsledky – vety Löwenheima, Skolema a Tarského „zhora nadol“ (downward) a „zdola nahor“ (upward) –, ktoré pre ľubovoľnú nekonečnú štruktúru $\mathcal{A}$ zaručujú existenciu mnohých jej elementárnych podštruktúr, resp. elementárnych rozšírení vopred danej mohutnosti spĺňajúcej isté minimálne obmedzenia dané mohutnosťami jazyka L a samotnej štruktúry $\mathcal{A}$. Využijeme pri tom rozšírenia pôvodného jazyka o vhodné konštantné symboly a v dôkaze druhej z týchto viet sa zároveň po prvýkrát stretneme s jednoduchou aplikáciou metódy diagramov (konkrétne elementárneho diagramu $\mathrm{Th}(\mathcal{A}_A)$ štruktúry $\mathcal{A}$).

Pripomeňme, že *mohutnosťou jazyka* $L = (F, R, \nu)$ nazývame kardinálne číslo

$$\|L\| = |\,\mathrm{Form}(L)| = \max(|F|, |R|, \aleph_0)$$

6.6.1 Veta Löwenheima, Skolema a Tarského „zhora nadol“. *Nech $\mathcal{A}$ je štruktúra nekonečnej mohutnosti $|A| = \alpha \geq \|L\|$ a β je kardinálne číslo také, že $\|L\| \leq \beta \leq \alpha$. Potom pre každú množinu $M \subseteq A$ mohutnosti $|M| \leq \beta$ existuje elementárna podštruktúra $\mathcal{B} \prec \mathcal{A}$ štruktúry $\mathcal{A}$ mohutnosti $|B| = \beta$ taká, že $M \subseteq B$.*

Dôkaz. Bez ujmy na na všeobecnosti môžeme predpokladať, že $|M| = \beta$ (inak môžeme množinu M nahradiť množinou M' mohutnosti β takou, že $M \subseteq M' \subseteq A$). Rekurziou zostrojíme istú postupnosť $B_0 \subseteq B_1 \subseteq \ldots \subseteq B_n \subseteq B_{n+1} \subseteq \ldots$ podmnožín množiny A. Na začiatok položíme $B_0 = M$ a pre každé n množinu B_{n+1} vytvoríme tak, že pre ľubovoľnú formulu $\varphi(x)$ jazyka L_{B_n}, pre ktorú platí

$$\mathcal{A} \vDash (\exists\, x)\varphi(x)$$

vyberieme jeden prvok $b \in A$ taký, že $\mathcal{A} \vDash \varphi(b)$, a pridáme ho k prvkom množiny B_n. Ľahko možno overiť, že množina

$$B = \bigcup_{n\in\mathbb{N}} B_n$$

má mohutnosť β a tvorí podštruktúru štruktúry $\mathcal{A}$. Na základe konštrukcie postupnosti (B_n) je podľa Tarského-Vaughtovho kritéria (Veta 6.4.6) zrejmé, že podštruktúra $\mathcal{B} = (B; \ldots)$ štruktúry $\mathcal{A}$ s nosičom B je jej elementárnou podštruktúrou. (Samostatne si doplňte vynechané kroky. Rozmyslite si, kde sme v dôkaze použili axiómu výberu.)

V prípade $\|L\| \leq \beta < \alpha$ je elementárna podštruktúra $\mathcal{B}$ štruktúry $\mathcal{A}$, ktorej existenciu zaručuje práve dokázaná veta, nevyhnutne vlastná. V prípade $\|L\| \leq \beta = \alpha$ to však len na základe tejto vety nevieme zaručiť.

6.6.2 Veta Löwenheima, Skolema a Tarského „zdola nahor". *Nech $\mathcal{A}$ je štruktúra nekonečnej mohutnosti $|A| = \alpha$ a β je kardinálne číslo také, že $\|L_A\| = \max(\alpha, \|L\|) \leq \beta$. Potom existuje elementárne rozšírenie $\mathcal{B} \succ \mathcal{A}$ štruktúry $\mathcal{A}$ mohutnosti $|B| = \beta$.*

Dôkaz. Utvorme jazyk L_A a rozšírme ho o ďalšiu množinu nových konštantných symbolov D mohutnosti $|D| = \beta$. Toto rozšírenie jazyka L (a zároveň jazyka L_A) označíme $L^+ = (L_A)_D$. Ďalej označme U teóriu v jazyku L^+ požadujúcu, aby všetky konštanty $d \in D$ označovali rôzne prvky. Inak povedané, axiómami teórie U sú práve všetky nerovnosti $d_1 \neq d_2$ pre ľubovoľné dva rozličné koštantné symboly $d_1, d_2 \in D$. Keďže $|D| = \beta$, bude mať každý model teórie U mohutnosť aspoň β. Tvrdíme, že teória $\mathrm{Th}(\mathcal{A}_A) \cup U$ v jazyku L^+ má nejaký model $\mathcal{M}$. Podľa vety o kompaktnosti stačí overiť, že pre ľubovoľnú konečnú podteóriu $U_0 \subseteq U$ teória $\mathrm{Th}(\mathcal{A}_A) \cup U_0$ má nejaký model. Nech D_0 je množina všetkých konštantných symbolov $d \in D$ vyskytujúcich sa v axiómach teórie U_0. Zrejme D_0 je konečná množina. Vezmime si štruktúru $\mathcal{A}_A$ jazyka L_A a rozšírme ju do štruktúry $\mathcal{A}^+$ jazyka L^+ tak, že interpretácie symbolov jazyka L_A ponecháme nezmenené, konštanty $d \in D_0$ interpretujeme navzájom rôznymi prvkami množiny A (čo je vždy možné, lebo A je nekonečná) a zvyšné konštanty $d \in D \setminus D_0$ interpretujeme ľubovoľnými prvkami množiny A. Je zrejmé, že $\mathcal{A}^+ \vDash \mathrm{Th}(\mathcal{A}_A) \cup U_0$.

Nech teda $\mathcal{M}$ je štruktúra jazyka L^+ taká, že $\mathcal{M} \vDash \mathrm{Th}(\mathcal{A}_A) \cup U$. Keďže $\mathcal{M} \vDash U$, platí $|M| \geq \beta$. Pretože $\mathcal{M} \vDash \mathrm{Th}(\mathcal{A}_A)$, zúženie $\mathcal{M}^- = \mathcal{M} \restriction L$ na štruktúru jazyka L (vynechaním interpretácií konštánt c_a a $d \in D$) je podľa Tvrdenia 6.5.4 elementárnym rozšírením (izomorfnej kópie) štruktúry $\mathcal{A}$. Podľa Vety 6.6.1 Löwenheima, Skolema

a Tarského „zhora nadol“, $\mathcal{M}^-$ obsahuje elementárnu podštruktúru $\mathcal{B} \prec \mathcal{M}^-$ mohutnosti $|B| = \beta$ takú, že $A \subseteq B$. Potom $\mathcal{A} \prec \mathcal{M}^-$, $\mathcal{B} \prec \mathcal{M}^-$ a $\mathcal{A} \subseteq \mathcal{B}$, preto tiež $\mathcal{A} \prec \mathcal{B}$ (pozri Úlohu 6.4.3).

V prípade $\alpha < \beta$ je $\mathcal{B}$ opäť vlastným elementárnym rozšírením štruktúry $\mathcal{A}$. V prípade $\alpha = \beta$ to však len na základe práve dokázanej vety nevieme zaručiť. Otázka existencie vlastných elementárnych podštruktúr $\mathcal{B} \prec \mathcal{A}$, resp. vlastných elementárnych rozšírení $\mathcal{B} \succ \mathcal{A}$ danej štruktúry $\mathcal{A}$ s rovnakou mohutnosťou $|B| = |A| = \alpha$ je podstatne náročnejšou záležitosťou. Za určitých okolností možno existenciu vlastného elementárneho rozšírenia $\mathcal{B}$ štruktúry $\mathcal{A}$ rovnakej mohutnosti $|B| = |A|$ dokázať pomocou konštrukcie *ultramocniny* (pozri Úlohu 8.4.4).

7 Vety o zachovávaní

V tejto kapitole sa budeme podrobnejšie zaoberať súvisom medzi syntaktickým tvarom axióm teórií prvého rádu a zachovávaním týchto teórií pri základných konštrukciách s ich modelmi. Konkrétne budeme charakterizovať teórie, ktoré sa zachovávajú pri prechode k podštruktúram, resp. nadštruktúram, teórie, ktoré sa zachovávajú pri zjednoteniach reťazcov, a teórie, ktoré sa prenášajú na homomorfné obrazy, ako teórie, ktoré sa dajú axiomatizovať pomocou axióm určitého dobre popísateľného syntaktického tvaru.

Naše úvahy začneme „inventarizáciou“ najdôležitejších prostriedkov, ktoré budeme pritom používať. Sú to najmä Gödelova veta o úplnosti 4.8.6, Veta 4.9.1 o kompaktnosti spolu s jej Dôsledkom 4.9.2, ako aj Lema 4.7.1 o konštantách. S ďalšími sa zoznámime v nasledujúcom paragrafe.

7.1 Lema o vzájomnej zlučiteľnosti a axiomatizačná lema

Nech T a S sú bezosporné teórie v jazyku prvého rádu L. Hovoríme, že T a S sú *zlučiteľné*, ak teória $T \cup S$ je bezosporná. V opačnom prípade hovoríme, že T a S sú *nezlučiteľné*.

7.1.1 Lema o vzájomnej zlučiteľnosti. *Nech T a S sú teórie v jazyku prvého rádu L. Potom T a S sú nezlučiteľné práve vtedy, keď existujú axiómy $\sigma_1(x_1, \ldots, x_k)$, $\ldots$, $\sigma_n(x_1, \ldots, x_k)$ teórie S také, že*

$$T \vdash (\exists\, x_1, \ldots, x_k)\big(\neg\sigma_1(x_1, \ldots, x_k) \vee \ldots \vee \neg\sigma_n(x_1, \ldots, x_k)\big)$$

Demonštrácia. Ak existujú také formuly σ_1, $\ldots$, σ_n, tak

$$S \vdash (\forall\, x_1, \ldots, x_k)\big(\sigma_1(x_1, \ldots, x_k) \wedge \ldots \wedge \sigma_n(x_1, \ldots, x_k)\big)$$

v dôsledku čoho je $T \cup S$ zrejme sporná.

Naopak, ak $T \cup S$ je sporná, tak je sporná už nejaká teória tvaru $T \cup S_0$, kde $S_0 = \{\sigma_1, \ldots, \sigma_n\}$ je konečná podteória teórie S. Nech $x_1, \ldots, x_k$ sú všetky premenné, ktoré su voľné v niektorej z formúl σ_i. Potom aj teória

$$T \cup \big\{(\forall\, x_1, \ldots, x_k)(\sigma_1(x_1, \ldots, x_k) \wedge \ldots \wedge \sigma_n(x_1, \ldots, x_k))\big\}$$

je sporná, čo znamená, že v T je dokázateľná negácia tejto formuly.

Triedu všetkých modelov teórie T v jazyku L budeme značiť $\mathrm{Mod}(T)$. Hovoríme, že množina formúl Γ jazyka L je *množinou axióm teórie* T, ak $\mathrm{Mod}(T) = \mathrm{Mod}(\Gamma)$, t. j. pre každú L-štruktúru $\mathcal{A}$ platí $\mathcal{A} \models T$ práve vtedy, keď $\mathcal{A} \models \Gamma$.

7.1.2 Axiomatizačná lema. *Nech T je bezosporná teória v jazyku L a Δ je množina sentencií jazyka L uzavretá vzhľadom na konečné disjunkcie. Nasledujúce podmienky sú ekvivalentné:*

(i) *T má množinu axióm $\Gamma \subseteq \Delta$.*

(ii) *Pre ľubovoľné štruktúry $\mathcal{A}$, $\mathcal{B}$ jazyka L platí:*

$$\mathcal{A} \models T \ \wedge\ \mathcal{B} \models \mathrm{Th}(\mathcal{A}) \cap \Delta \ \Rightarrow\ \mathcal{B} \models T$$

Na množinu Δ sa treba dívať ako na množinu formúl (logicky ekvivalentných s formulami) určitého syntaktického tvaru, napr. univerzálne formuly, existenčné formuly, pozitívne formuly atď.

Dôkaz. (i) $\Rightarrow$ (ii): Predpokladajme, že T má množinu axióm $\Gamma \subseteq \Delta$. Nech ďalej platí $\mathcal{A} \models T$ a $\mathcal{B} \models \mathrm{Th}(\mathcal{A}) \cap \Delta$. Potom zrejme $\mathcal{B} \models \Gamma$, teda $\mathcal{B} \models T$.

(ii) $\Rightarrow$ (i): Nech platí (ii). Označme Γ množinu všetkých sentencií φ jazyka L takých, že $\varphi \in \Delta$ a $T \vdash \varphi$. Ukážeme, že Γ je množina axióm pre T. Zrejme stačí dokázať inklúziu $\mathrm{Mod}(\Gamma) \subseteq \mathrm{Mod}(T)$ (obrátená inklúzia je totiž zrejmá – prečo?). Nech teda $\mathcal{B} \in \mathrm{Mod}(\Gamma)$. Ak máme s využitím podmienky (ii) dokázať, že $\mathcal{B} \in \mathrm{Mod}(T)$, čiže $\mathcal{B} \models T$, potrebujeme nájsť nejakú štruktúru $\mathcal{A} \models T$ takú, že $\mathcal{B} \models \mathrm{Th}(\mathcal{A}) \cap \Delta$. Poslednú podmienku možno ekvivalentne zapísať v tvare $\mathcal{A} \models \Sigma$, kde

$$\Sigma = \{\neg\delta \colon \delta \in \Delta,\ \mathcal{B} \models \neg\delta\}$$

(rozmyslite si prečo). Potrebujeme teda zaručiť, že teória $T \cup \Sigma$ má nejaký model $\mathcal{A}$. Na to stačí dokázať, že je bezosporná. Inak by podľa Lemy 7.1.1 o vzájomnej zlučiteľnosti existovali nejaké formuly $\delta_1, \ldots, \delta_n \in \Delta$ také, že $\neg\delta_1, \ldots, \neg\delta_n \in \Sigma$ a $T \vdash \delta_1 \vee \ldots \vee \delta_n$. Označme δ poslednú formulu. Zrejme $\delta \in \Delta$, preto tiež $\delta \in \Gamma$, a keďže $\mathcal{B} \models \Gamma$, tak aj $\mathcal{B} \models \delta$. To je však v spore s tým, že $\mathcal{B} \models \neg\delta_1, \ldots, \mathcal{B} \models \neg\delta_n$, teda $\mathcal{B} \models \neg\delta$.

7.2 Univerzálne teórie a podštruktúry

Hovoríme, že *teória T sa prenáša na podštruktúry*, ak ľubovoľná podštruktúra modelu teórie T je tiež modelom T.

7.2.1 Veta. *Nech T je bezosporná teória. Potom nasledujúce podmienky sú ekvivalentné:*

(i) *T má množinu univerzálnych axióm.*

(ii) *T sa prenáša na podštruktúry.*

Dôkaz. Sústredíme sa iba na netriválnu implikáciu (ii) $\Rightarrow$ (i). Nech platí (ii). Označme Π^0_1 množinu všetkých sentencií jazyka L ekvivalentných s univerzálnymi formulami. Zrejme Π^0_1 je uzavretá vzhľadom na konečné disjunkcie. Pomocou Axiomatizačnej lemy 7.1.2 dokážeme, že T má množinu axióm $\Gamma \subseteq \Pi^0_1$. Nech teda $\mathcal{A} \models T$

a $\mathcal{B} \models \mathrm{Th}(\mathcal{A}) \cap \Pi_1^0$. Ukážeme, že za týchto podmienok existuje L-štruktúra $\mathcal{C}$ taká, že $\mathcal{A} \equiv \mathcal{C}$ a $\mathcal{B} \subseteq \mathcal{C}$. Tým budeme hotoví, lebo potom $\mathcal{C} \models T$ a – keďže sa T prenáša na podštruktúry – aj $\mathcal{B} \models T$.

Inak povedané, potrebujeme nájsť štruktúru $(\mathcal{C}, b)_{b\in B}$ jazyka L_B, ktorá je modelom teórie $\mathrm{Th}(\mathcal{A}) \cup \mathrm{D}(\mathcal{B})$. Stačí teda overiť, že táto teória v jazyku L_B je bezosporná. V opačnom prípade by pre nejaké $n \geq 1$ existovali formuly $\theta_1(\vec{b}), \ldots, \theta_n(\vec{b}) \in \mathrm{D}(\mathcal{B})$ také, že $\theta_i(x_1, \ldots, x_k)$ sú atomické alebo negatomické formuly jazyka L, $\vec{b} = (b_1, \ldots, b_k) \in B^k$ a

$$\mathrm{Th}(\mathcal{A}) \vdash \neg\theta_1(\vec{b}) \vee \ldots \vee \neg\theta_n(\vec{b})$$

No $\mathrm{Th}(\mathcal{A})$ je teória v jazyku L, v ktorom sa konštanty $b_1, \ldots, b_k$ nevyskytujú. Preto podľa Lemy 7.1.2 o konštantách

$$\mathrm{Th}(\mathcal{A}) \vdash (\forall \vec{x})\big(\neg\theta_1(\vec{x}) \vee \ldots \vee \neg\theta_n(\vec{x})\big)$$

kde $\vec{x} = (x_1, \ldots, x_k)$. Posledná formula je však uzavretá, univerzálna a platí v $\mathcal{A}$. Preto je splnená i v $\mathcal{B}$. To je však v spore s tým, že

$$\mathcal{B} \models (\exists \vec{x})(\theta_1(\vec{x}) \wedge \ldots \wedge \theta_n(\vec{x}))$$

Skrátené „vektorové“ označenie ako $\vec{x} = (x_1, \ldots, x_k)$ alebo $\vec{b} = (b_1, \ldots, b_k)$ pre usporiadané k-tice premenných, resp. prvkov množín budeme ďalej používať bez zvláštneho upozornenia.

7.3 Existenčné teórie a nadštruktúry

Hovoríme, že *teória T sa prenáša na nadštruktúry*, ak ľubovoľná nadštruktúra modelu teórie T je tiež modelom teórie T.

7.3.1 Veta. *Nech T je bezosporná teória. Potom nasledujúce podmienky sú ekvivalentné:*

(i) *T má množinu existenčných axióm.*

(ii) *T sa prenáša na nadštruktúry.*

Dôkaz. Opäť sa sústredíme len na netriválnu implikáciu (ii) $\Rightarrow$ (i). Nech platí (ii). Označme Σ_1^0 množinu všetkých sentencií jazyka L ekvivalentných s existenčnými formulami. Zrejme Σ_1^0 je uzavretá na konečné disjunkcie. Pomocou Axiomatizačnej lemy 7.1.2 dokážeme, že T má množinu axióm $\Gamma \subseteq \Sigma_1^0$. Nech teda $\mathcal{A} \models T$ ako aj $\mathcal{B} \models \mathrm{Th}(\mathcal{A}) \cap \Sigma_1^0$. Z toho vyplýva, že $\mathcal{A} \models \mathrm{Th}(\mathcal{B}) \cap \Pi_1^0$ (rozmyslite si prečo). To je však rovnaká situácia ako v dôkaze predchádzajúcej vety, iba úlohy štruktúr $\mathcal{A}$ a $\mathcal{B}$ sú zamenené. Preto existuje štruktúra $\mathcal{C}$ taká, že $\mathcal{A} \subseteq \mathcal{C}$ a $\mathcal{B} \equiv \mathcal{C}$. Potom – keďže T sa prenáša na nadštruktúry – platí $\mathcal{C} \models T$ a taktiež $\mathcal{B} \models T$.

7.4 Univerzálno-existenčné teórie a zjednotenia reťazcov

Pripomeňme, že pod *usporiadanou množinou* $(I;\leq)$ rozumieme množinu $I \neq \emptyset$ s binárnou reláciou $\leq$ spĺňajúcou nasledujúce podmienky:

$$(\forall\, x)(x \leq x)$$
$$(\forall\, x,y)(x \leq y \ \wedge\ y \leq x \ \Rightarrow\ x = y)$$
$$(\forall\, x,y,z)(x \leq y \ \wedge\ y \leq z \ \Rightarrow\ x \leq z)$$
$$(\forall\, x,y)(x \leq y \ \vee\ y \leq x)$$

Reťazcom štruktúr nad usporiadanou množinou $(I;\leq)$ rozumieme systém štruktúr $(\mathcal{A}_i)_{i\in I}$ nejakého jazyka prvého rádu L taký, že pre ľubovoľné prvky $i \leq j$ množiny I štruktúra $\mathcal{A}_i$ je podštruktúrou štruktúry $\mathcal{A}_j$, t.j. $\mathcal{A}_i \subseteq \mathcal{A}_j$. *Zjednotením reťazca* $(\mathcal{A}_i)_{i\in I}$ nazývame L-štruktúru $\bar{\mathcal{A}} = \bigcup_{i\in I} \mathcal{A}_i$ so základnou množinou $\bar{A} = \bigcup_{i\in I} A_i$, na ktorej sú operačné a relačné symboly jazyka L interpretované nasledujúcim spôsobom:

Pre ľubovoľný n-árny operačný symbol f, resp. relačný symbol r jazyka L a prvky $a_1,\ldots,a_n \in \bar{A}$ kladieme

$$f^{\bar{\mathcal{A}}}(a_1,\ldots,a_n) = f^{\mathcal{A}_i}(a_1,\ldots,a_n)$$
$$(a_1,\ldots,a_n) \in r^{\bar{\mathcal{A}}} \ \Leftrightarrow\ (a_1,\ldots,a_n) \in r^{\mathcal{A}_i}$$

kde i je ľubovoľný prvok množiny I taký, že $a_1,\ldots,a_n \in A_i$.

(Samostatne si premyslite, že aspoň jeden taký prvok $i \in I$ vždy existuje a ak $i,j \in I$ sú dva také prvky, tak uvedené interpretácie $f^{\bar{\mathcal{A}}}$, $r^{\bar{\mathcal{A}}}$ nezávisia na tom, ktorý z nich použijeme pri ich definícii.)

Zrejme ak množina $(I;\leq)$ má najväčší prvok m (špeciálne ak I je konečná), tak $\bigcup_{i\in I} \mathcal{A}_i = \mathcal{A}_m$, teda uvedená konštrukcia môže priniesť niečo nové, len ak $(I;\leq)$ je nekonečná a nemá najväčší prvok. Typickým príkladom reťazcov štruktúr sú reťazce $(\mathcal{A}_n)_{n\in\mathbb{N}}$ nad množinou $(\mathbb{N},\leq)$ všetkých prirodzených čísel s obvyklým usporiadaním. Také reťazce možno tiež zapísať v tvare

$$\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq\ \ldots\ \subseteq \mathcal{A}_n \subseteq \mathcal{A}_{n+1}\ \subseteq \ldots$$

prípadne v tvare $(\mathcal{A}_n)_{n<\omega}$.

Jednoduchý dôkaz nasledujúceho tvrdenia ponechávame ako cvičenie čitateľovi.

7.4.1 Tvrdenie. *Nech $(\mathcal{A}_i)_{i\in I}$ je reťazec štruktúr nad usporiadanou množinou $(I;\leq)$. Potom pre každé $j \in I$ platí $\mathcal{A}_j \subseteq \bigcup_{i\in I} \mathcal{A}_i$, čiže zjednotenie reťazca štruktúr je rozšírením každej zo štruktúr tohto reťazca. Navyše ak štruktúra $\mathcal{B}$ je rozšírením každej zo štruktúr reťazca $(\mathcal{A}_i)_{i\in I}$, tak $\bigcup_{i\in I} \mathcal{A}_i \subseteq \mathcal{B}$; inak povedané, zjednotenie reťazca $(\mathcal{A}_i)_{i\in I}$ je najmenšia štruktúra, ktorá je rozšírením každej zo štruktúr $\mathcal{A}_i$.*

Reťazec $(\mathcal{A}_i)_{i\in I}$ štruktúr nad usporiadanou množinou $(I;\leq)$ nazývame *elementárnym reťazcom*, ak pre všetky dvojice prvkov $i \leq j$ z množiny I platí $\mathcal{A}_i \prec \mathcal{A}_j$, t. j. $\mathcal{A}_i$ je elementárnou podštruktúrou štruktúry $\mathcal{A}_j$.

7.4.2 Veta. *Nech $(\mathcal{A}_i)_{i\in I}$ je elementárny reťazec štruktúr nad usporiadanou množinou $(I;\leq)$. Potom pre každé $j \in I$ platí $\mathcal{A}_j \prec \bigcup_{i\in I}\mathcal{A}_i$, čiže zjednotenie elementárneho reťazca štruktúr je elementárnym rozšírením každej zo štruktúr tohto reťazca.*

Dôkaz. Označme $\bar{\mathcal{A}} = \bigcup_{i\in I}\mathcal{A}_i$. Máme dokázať, že $\mathcal{A}_j \prec \bar{\mathcal{A}}$ pre každý člen $\mathcal{A}_j$ elementárneho reťazca $(\mathcal{A}_i)_{i\in I}$. To vyplýva z nasledujúceho tvrdenia:

Pre všetky L-formuly $\varphi(x_1,\ldots,x_n)$, každé $j \in I$ a ľubovoľné prvky $a_1,\ldots,a_n \in A_j$

$$\mathcal{A}_j \vDash \varphi(a_1,\ldots,a_n) \;\Leftrightarrow\; \bar{\mathcal{A}} \vDash \varphi(a_1,\ldots,a_n)$$

Dôkaz urobíme indukciou podľa zložitosti formuly φ. Ak φ je atomická, tak podmienka je triviálne splnená, lebo $\mathcal{A}_j \subseteq \bar{\mathcal{A}}$. Podobne, z platnosti uvedenej podmienky pre formuly φ, ψ očividne vyplýva jej platnosť pre konjunkciu $\varphi\wedge\psi$ aj pre negáciu $\neg\varphi$ (detaily prenechávame čitateľovi). Predpokladajme teda, že uvedená podmienka je splnená pre formulu $\varphi(x_0,x_1,\ldots,x_n)$ a overme jej platnosť pre formulu $(\exists\, x_0)\varphi(x_0,x_1,\ldots,x_n)$. Nech $j \in I$ a $a_1,\ldots,a_n \in A_j$. Potom nasledujúce podmienky sú ekvivalentné:

(1) $\bar{\mathcal{A}} \vDash (\exists\, x_0)\varphi(x_0,a_1,\ldots,a_n)$

(2) existuje $a_0 \in \bar{A}$ také, že $\bar{\mathcal{A}} \vDash \varphi(a_0,a_1,\ldots,a_n)$

(3) existujú $k \in I$ a $a_0 \in A_k$ také, že $k \geq j$ a $\bar{\mathcal{A}} \vDash \varphi(a_0,a_1,\ldots,a_n)$

(Rozmyslite si, prečo si v (3) môžeme bez ujmy na všeobecnosti dovoliť predpoklad $k \geq j$.) Pre také $k \in I$ a $a_0 \in A_k$ je podmienka $\bar{\mathcal{A}} \vDash \varphi(a_0,a_1,\ldots,a_n)$ na základe indukčného predpokladu ekvivalentná s podmienkou $\mathcal{A}_k \vDash \varphi(a_0,a_1,\ldots,a_n)$, teda podmienka (3) je postupne ekvivalentná s podmienkami

(4) existujú $k \in I$ a $a_0 \in A_k$ také, že $k \geq j$ a $\mathcal{A}_k \vDash \varphi(a_0,a_1,\ldots,a_n)$

(5) existuje $k \in I$ také, že $k \geq j$ a $\mathcal{A}_k \vDash (\exists\, x_0)\varphi(x_0,a_1,\ldots,a_n)$

Napokon, kedže pre $j \leq k$ platí $\mathcal{A}_j \prec \mathcal{A}_k$, podmienka (5) je ekvivalentná s podmienkou

(6) $\mathcal{A}_j \vDash (\exists\, x_0)\varphi(x_0,a_1,\ldots,a_n)$

ku ktorej sme chceli dospieť.

7.4.3 Tvrdenie. *Nech $(\mathcal{A}_i)_{i\in I}$ je reťazec štruktúr nad usporiadanou množinou $(I;\leq)$ a $\varphi(x_1,\ldots,x_m,y_1,\ldots,y_n)$ je otvorená formula. Predpokladajme, že*

$$\mathcal{A}_i \vDash (\forall\,\vec{x}\,)(\exists\,\vec{y}\,)\varphi(\vec{x},\vec{y}\,)$$

v každej zo štruktúr $\mathcal{A}_i$. Potom tiež

$$\bigcup_{i\in I}\mathcal{A}_i \vDash (\forall\,\vec{x}\,)(\exists\,\vec{y}\,)\varphi(\vec{x},\vec{y}\,)$$

Dôkaz. Za uvedeného predpokladu zvoľme ľubovoľné prvky $a_1,\ldots,a_m \in \bigcup_{i\in I}A_i$. Potrebujeme dokázať existenciu nejakých prvkov $b_1,\ldots,b_n \in \bigcup_{i\in I}A_i$ takých, že

$$\bigcup_{i\in I}\mathcal{A}_i \vDash \varphi\big(\vec{a},\vec{b}\,\big)$$

Za daných podmienok možno nájsť $j \in I$ také, že $a_1, \ldots, a_m \in A_j$. Keďže

$$\mathcal{A}_j \vDash (\forall \vec{x}\,)(\exists \vec{y}\,)\varphi(\vec{x}, \vec{y}\,)$$

existujú prvky $b_1, \ldots, b_n \in A_j$ také, že $\mathcal{A}_j \vDash \varphi\big(\vec{a}, \vec{b}\,\big)$. Nakoľko $\mathcal{A}_j \subseteq \bigcup_{i\in I} \mathcal{A}_i$ a φ neobsahuje žiadne kvantifikátory, podľa Tvrdenia 6.1.4 (a) platí

$$\bigcup_{i\in I} \mathcal{A}_i \vDash \varphi\big(\vec{a}, \vec{b}\,\big)$$

Hovoríme, že *teória T sa zachováva pri zjednoteniach reťazcov*, ak zjednotenie ľubovoľného reťazca modelov teórie T je tiež modelom T. Podobne možno definovať aj zachovávanie teórií pri zjednoteniach reťazcov nad usporiadanou množinou $(\mathbb{N}; \leq)$.

Formulu tvaru $(\forall x_1, \ldots, x_m)(\exists y_1, \ldots, y_n)\varphi$, kde φ je otvorená formula, nazývame *univerzálno-existenčnou formulou.*

7.4.4 Veta. *Nech T je bezosporná teória. Potom nasledujúce podmienky sú ekvivalentné:*

(i) *T má množinu univerzálno-existenčných axióm.*

(ii) *T sa zachováva pri zjednoteniach reťazcov.*

(iii) *T sa zachováva pri zjednoteniach reťazcov nad $(\mathbb{N}; \leq)$.*

Dôkaz. Platnosť implikácie (i) $\Rightarrow$ (ii) vyplýva z predchádzajúceho tvrdenia a implikácia (ii) $\Rightarrow$ (iii) je triviálna. Stačí sa teda sústrediť na implikáciu (iii) $\Rightarrow$ (i).

Nech platí (iii). Označme Π^0_2 množinu všetkých sentencií jazyka L ekvivalentných s univerzálno-existenčnými formulami. Zrejme Π^0_2 je uzavretá na konečné disjunkcie. Pomocou Axiomatizačnej lemy 7.1.2 dokážeme, že T má množinu axióm $\Gamma \subseteq \Pi^0_2$. Nech teda $\mathcal{A} \vDash T$ a platí

(0) $\mathcal{B} \vDash \mathrm{Th}(\mathcal{A}) \cap \Pi^0_2$

Za týchto podmienok zostrojíme dve postupnosti štruktúr $(\mathcal{A}_n)_{n<\omega}$, $(\mathcal{B}_n)_{n<\omega}$ jazyka L také, že $\mathcal{A}_0 = \mathcal{A}$, $\mathcal{B}_0 = \mathcal{B}$, pre každé n platí $\mathcal{A}_n \equiv \mathcal{A}_{n+1}$, preto tiež $\mathcal{A}_n \equiv \mathcal{A}$, ako aj $\mathcal{B}_n \prec \mathcal{B}_{n+1}$, pričom obe postupnosti dohromady tvoria striedavo vzájomne poprekladaný reťazec

$$\mathcal{B}_0 \subseteq \mathcal{A}_1 \subseteq \mathcal{B}_1 \subseteq \mathcal{A}_2 \subseteq \ldots \subseteq \mathcal{B}_n \subseteq \mathcal{A}_{n+1} \subseteq \mathcal{B}_{n+1} \subseteq \ldots$$

Označme $\mathcal{C}$ jeho zjednotenie. Potom zároveň platí

$$\mathcal{C} = \bigcup_{1\leq n<\omega} \mathcal{A}_n = \bigcup_{n<\omega} \mathcal{B}_n$$

Keďže teória T sa zachováva pri zjednoteniach reťazcov nad $(\mathbb{N}; \leq)$ a všetky $\mathcal{A}_n$ sú jej modelmi, platí $\mathcal{C} \vDash T$. Pretože reťazec $(\mathcal{B}_n)_{n<\omega}$ je elementárny, dostávame $\mathcal{B} \prec \mathcal{C}$, teda konečne $\mathcal{B} \vDash T$. Tým podľa Axiomatizačnej lemy 7.1.2 zabezpečíme, že T má množinu univerzálno-existenčných axióm.

Ukážeme, že za podmienky (0) platí nasledujúce tvrdenie:

(1) Existujú štruktúry $\mathcal{A}'$, $\mathcal{B}'$ také, že $\mathcal{A} \equiv \mathcal{A}'$, $\mathcal{B} \prec \mathcal{B}'$ a $\mathcal{B} \subseteq \mathcal{A}' \subseteq \mathcal{B}'$.

Keďže každá univerzálna formula je zároveň univerzálno-existenčná, z podmienky (0) vyplýva, že $\mathcal{B} \vDash \mathrm{Th}(\mathcal{A}) \cap \Pi_1^0$. Ako sme videli v dôkaze Vety 7.2.1, za tejto podmienky je teória $\mathrm{Th}(\mathcal{A}) \cup \mathrm{D}(\mathcal{B})$ bezosporná a existuje štruktúra $\mathcal{A}'_B = (\mathcal{A}', b)_{b\in B}$, ktorá je modelom teórie $\mathrm{Th}(\mathcal{A}) \cup \mathrm{D}(\mathcal{B})$ v jazyku L_B. Potom $\mathcal{A}' \equiv \mathcal{A}$ a $\mathcal{B} \subseteq \mathcal{A}'$.

Hľadanú štruktúru $\mathcal{B}'$ získame zo štruktúry $(\mathcal{B}', b, a)_{b\in B, a\in A'}$ jazyka $L_{B,A'} = (L_B)_{A'}$, od ktorej budeme požadovať, aby bola modelom teórie $\mathrm{Th}(\mathcal{B}_B) \cup \mathrm{D}(\mathcal{A}')$ v tomto jazyku. Stačí teda overiť, že uvedená teória je bezosporná. Inak by podľa Lemy 7.1.1 o vzájomnej zlučiteľnosti existovali formuly $\theta_1(\vec{a}), \ldots, \theta_n(\vec{a}) \in \mathrm{D}(\mathcal{A}')$, kde $\theta_i(x_1, \ldots, x_k)$ sú atomické alebo negatomické formuly jazyka L a $\vec{a} = (a_1, \ldots, a_k) \in (A')^k$, také, že

$$\mathrm{Th}(\mathcal{B}_B) \vdash \neg\theta_1(\vec{a}) \vee \ldots \vee \neg\theta_n(\vec{a})$$

Keďže $\mathrm{Th}(\mathcal{B}_B)$ je teória v jazyka L_B, v ktorom sa konštanty $a_1, \ldots, a_k$ nevyskytujú, podľa Lemy 4.7.1 o konštantách z toho vyplýva, že

$$\mathrm{Th}(\mathcal{B}_B) \vdash (\forall \vec{x})(\neg\theta_1(\vec{x}) \vee \ldots \vee \neg\theta_n(\vec{x}))$$

Nakoľko to je formula jazyka L, znamená to, že musí byť splnená v $\mathcal{B}$. Zároveň však

$$\mathcal{A}' \vDash (\exists \vec{x})(\theta_1(\vec{x}) \wedge \ldots \wedge \theta_n(\vec{x}))$$

a keďže $\mathcal{A}' \equiv \mathcal{A}$, tak posledná formula platí aj v $\mathcal{A}$. Nakoľko to však je existenčná, teda tým skôr univerzálno-existenčná formula, tak podľa predpokladu (0) je splnená tiež v $\mathcal{B}$. Tento spor dokazuje (1).

Na záver si uvedomme, že pre takto získané čiarkované štruktúry opäť platí podmienka (0), t. j. $\mathcal{B}' \vDash \mathrm{Th}(\mathcal{A}') \cap \Pi_2^0$, takže celú konštrukciu možno iterovať. Postupne tak dostávame štruktúry $\mathcal{A}_1 = \mathcal{A}'$, $\mathcal{B}_1 = \mathcal{B}'$ zo štruktúr $\mathcal{A}_0 = \mathcal{A}$, $\mathcal{B}_0 = \mathcal{B}$, ako aj štruktúry $\mathcal{A}_{n+1} = \mathcal{A}'_n$, $\mathcal{B}_{n+1} = \mathcal{B}'_n$ zo štruktúr $\mathcal{A}_n$, $\mathcal{B}_n$ pre $n \geq 1$.

7.4.5 Úloha. Uvažujme grupy ako štruktúry $(G; \cdot)$ s jednou binárnou operáciou. Potom teória grúp je daná dvoma axiómami: asociatívnym zákonom

$$(\forall x, y, z)\big(x \cdot (y \cdot z) = (x \cdot y) \cdot z\big)$$

a axiómou vyjadrujúcou existenciu jednotkového prvku ako i inverzných prvkov

$$(\exists u)(\forall x)\big(x \cdot u = x = u \cdot x \ \wedge\ (\exists y)(x \cdot y = u = y \cdot x)\big)$$

ktorú možno nahradiť axiómou

$$(\forall x)(\exists y)(\forall z)\big(z \cdot (x \cdot y) = z = (y \cdot x) \cdot z\big)$$

Ani jedna z uvedených dvoch axióm však nie je univerzálno-existenčná. Preto možno prekvapí, že teória grúp (v takomto jazyku) sa zachováva pri zjednoteniach reťazcov. Inak povedané, ak $\big((G_i; \cdot)\big)_{i\in I}$ je reťazec grúp nad usporiadanou množinou $(I; \leq)$, tak aj jeho zjednotenie $\left(\bigcup_{i\in I} G_i\,;\, \cdot\right)$ je grupa. Dokážte si to samostatne.

Z Vety 7.4.4 potom vyplýva, že teória grúp musí mať množinu univerzálno-existenčných axióm v jazyku s jediným binárnym operačným symbolom $\cdot$. Nájdite takúto axiomatizáciu teórie grúp.

7.5 Algebraický uzáver poľa

Axiómy teórie polí ako štruktúr $(F;+,\cdot,0,1)$ jazyka s dvomi binárnymi operáciami $+$ a $\cdot$ a dvomi konštantami 0 a 1 sú našim čitateľom určite dobre známe, takže ich tu nebudeme explicitne vypisovať. Stačí, ak si uvedomíme, že popri univerzálnych axiómach (identitách) vyjadrujúcich komutatívne a asociatívne zákony pre obe operácie, úlohách prvkov 0 a 1 ako neutrálnych prvkov týchto operácií a distributívnom zákone, k nim patria ešte dve univerzálno-existenčné axiómy

$$(\forall x)(\exists y)(x+y=0) \quad \text{a} \quad (\forall x)(\exists y)(x\neq 0 \Rightarrow x\cdot y=1)$$

zaručujúce existenciu inverzných prvkov oboch operácií. Z vety o zachovávaní teórií pri zjednoteniach reťazcov potom vyplýva, že aj teória polí sa zachováva pri zjednoteniach reťazcov, to znamená, že zjednotením ľubovoľného reťazca polí $\big((F_i;+,\cdot,0,1)\big)_{i\in I}$ nad usporiadanou množinou $(I;\leq)$ dostaneme opäť pole $\Big(\bigcup_{i\in I} F_i\,;+,\cdot,0,1\Big)$.

Zjednotenia reťazcov sa v teórii polí hojne využívajú. Ich najdôležitejším uplatnením je konštrukcia *algebraického uzáveru poľa*, s ktorou sa teraz zoznámime.

Ďalej už budeme, ako je bežne zvykom, pole $(F;+,\cdot,0,1)$ značiť väčšinou iba F, teda rovnako ako jeho základnú množinu. Hovoríme, že pole K je *algebraickým rozšírením* poľa F, ak F je podpoľom poľa K a každý prvok poľa K je algebraický nad F, t. j. je koreňom nejakého polynómu $p(x)$ s koeficientmi z poľa F.

Čitateľ by si mal z prednášok z algebry pamätať niekoľko výsledkov o algebraických rozšíreniach polí, ktoré tu stručne zrekapitulujeme. Ak $p(x)\in F[x]$ je ireducibilný polynóm stupňa ≥ 2 nad poľom F, tak faktorový okruh $F[x]/(p(x))$ okruhu polynómov $F[x]$ podľa hlavného ideálu $(p(x))$ generovaného polynómom $p(x)$ je opäť pole, ktoré je navyše rozšírením poľa F. V tomto poli už polynóm $p(x)$ má koreň (je ním rozkladová trieda $x+(p(x))$), teda nie viac je ireducibilný. Takéto rozšírenia poľa F nazývame jeho *jednoduchými rozšíreniami*. Zrejme každé jednoduché rozšírenie poľa F je algebraické. Taktiež možno ľahko nahliadnuť, že pre ľubovoľné polia F, H, K platí: ak H je algebraickým rozšíremím poľa F a K je algebraickým rozšírením poľa H, tak K je algebraickým rozšírením poľa F.

Jednoduchý dôkaz nasledujúceho pomocného tvrdenia prenechávame ako cvičenie čitateľovi.

7.5.1 Lema. *Nech $(F_i)_{i\in I}$ je reťazec polí nad usporiadnou množinou $(I;\leq)$, z ktorých každé je algebraickým rozšírením poľa F. Potom aj zjednotenie tohto reťazca $\bigcup_{i\in I} F_i$ je algebraickým rozšírením poľa F.*

Hovoríme, že pole K je *algebraicky uzavreté*, ak každý polynóm $p\in K[x]$ stupňa ≥ 2 má v K aspoň jeden koreň. Ľahko nahliadneme, že pole K je algebraicky uzavreté práve vtedy, keď jedinými ireducibilnými normovanými polynómami stupňa ≥ 1 nad K sú lineárne polynómy tvaru $x-a$, kde $a\in K$. Z toho ďalej vyplýva, že v algebraicky uzavretom poli má každý polynóm stupňa $n\geq 1$ práve n koreňov, ak každý koreň počítame toľkokrát, aká je jeho násobnosť. Pole K nazývame *algebraickým uzáverom* poľa F, ak K je algebraicky uzavreté pole, ktoré je algebraickým rozšírením poľa F.

7.5.2 Veta. *Ku každému poľu existuje jeho algebraický uzáver.*

Dodávame, že algebraický uzáver ľubovoľného poľa je navyše určený jednoznačne až na izomorfizmus. Dôkaz tohto výsledku však už nie je náplňou nášo kurzu.

Dôkaz. Nech F je ľubovoľné pole. Najprv zostrojíme algebraické rozšírenie $\widehat{F}$ poľa F, v ktorom má každý ireducibilný polynóm $p(x) \in F[x]$ stupňa ≥ 2 koreň. Inak povedané, neexistuje polynóm $p(x) \in F[x]$ stupňa ≥ 2 ireducibilný nad poľom $\widehat{F}$. Nech $(p_\alpha(x))_{\alpha<\rho}$ je ľubovoľné očíslovanie množiny všetkých normovaných ireducibilných polynómov stupňa ≥ 2 z okruhu $F[x]$ ordinálnymi číslami menšími ako nejaké ordinálne číslo ρ. Transfinitnou rekurziou cez ordinály $\alpha < \rho$ zostrojíme transfinitnú postupnosť $(F_\alpha)_{\alpha<\rho}$ rozšírení poľa F takú, že

$$F_0 = F$$

$$F_{\alpha+1} = \begin{cases} F_\alpha[x]/(p_\beta(x)), & \text{kde } \beta < \rho \text{ je prvý ordinál taký, že polynóm} \\ & p_\beta(x) \text{ je ireducibilný nad poľom } F_\alpha \\ F_\alpha, & \text{ak taký ordinál } \beta \text{ neexistuje} \end{cases}$$

$$F_\lambda = \bigcup_{\alpha<\lambda} F_\alpha$$

pre ľubovoľný ordinál $\alpha < \rho$, resp. pre limitný ordinál $\lambda < \rho$. Zrejme pre ľubovoľné $\alpha \leq \beta < \rho$ je pole F_β rozšírením poľa F_α, teda $(F_\alpha)_{\alpha<\rho}$ je reťazec polí nad usporiadanou množinou $(\{\alpha\colon \alpha < \rho\}; \leq)$.

Transfinitnou indukciou dokážeme, že každé z polí F_α je algebraickým rozšírením poľa F. Pre $\alpha = 0$ je to zrejmé. Nech $\alpha < \rho$ je ľubovoľný ordinál; predpokladajme, že F_α je algebraickým rozšírením poľa F. Potom $F_{\alpha+1}$ je buď jednoduché (teda algebraické) rozšírenie $F_\alpha[x]/(p_\beta(x))$ poľa F_α, alebo je to samotné pole F_α. Teda v oboch prípaoch ide o algebraické rozšírenie poľa F. Konečne, nech $\lambda < \rho$ je limitný ordinál. Predpokladajme, že všetky polia F_α, pre $\alpha < \lambda$, sú algebraické rozšírenia poľa F. Potom aj F_λ, ako zjednotenie reťazca $(F_\alpha)_{\alpha<\lambda}$, je jeho algebraickým rozšírením na základe Lemy 7.5.1.

Teraz položíme $\widehat{F} = \bigcup_{\alpha<\rho} F_\alpha$. Potom aj pole $\widehat{F}$, ako zjednotenie reťazca $(F_\alpha)_{\alpha<\rho}$ algebraických rozšírení poľa F, je samo algebraickým rozšírením poľa F. Zrejme každý ireducibilný polynóm stupňa ≥ 2 nad poľom F má koreň v niektorom z polí F_α, teda aj v poli $\widehat{F}$.

S využitím práve opísanej konštrukcie zostrojíme ešte jeden reťazec $\left(F^{(n)}\right)_{n\in\mathbb{N}}$ algebraických rozšírení poľa F nad usporiadanou množinou $\mathbb{N}$ všetkých prirodzených čísel taký, že

$$F^{(0)} = F \qquad \text{a} \qquad F^{(n+1)} = \widehat{F^{(n)}}$$

pre $n \in \mathbb{N}$. Potom aj zjednotenie tohto reťazca $\widetilde{F} = \bigcup_{n\in\mathbb{N}} F^{(n)}$ je algebraickým rozšírením poľa F. Dokážeme, že je to zároveň algebraicky uzavreté pole. Na to stačí overiť, že neexistujú normované ireducibilné polynómy $p(x) \in \widetilde{F}[x]$ stupňa ≥ 2. Predokladajme teda, že

$$p(x) = x^k + a_1x^{k-1} + \ldots + a_{k-1}x + a_k \in \widetilde{F}[x]$$

je normovaný ireducibilný polynóm stupňa $k \geq 2$. Potom existuje $n \in \mathbb{N}$, také, že pole $F^{(n)}$ obsahuje všetky jeho koeficienty $a_1, \ldots, a_k$, teda $p(x) \in F^{(n)}[x]$ je normovaný

ireducibilný polynóm nad poľom $F^{(n)}$. Potom však $p(x)$ má koreň v poli $F^{(n+1)} = \widehat{F^{(n)}}$, preto aj v poli $\widetilde{F}$. Ale to znamená, že – navzdory pôvodnému predpokladu – polynóm $p(x)$ nie je ireducibilný nad poľom $\widetilde{F}$. Tým sme dokázali, že pole $\widetilde{F}$ je algebraický uzáver poľa F.

7.6 Pozitívne teórie a homomorfné obrazy

Hovoríme, že *teória T sa prenáša na homomorfné obrazy*, ak každý homomorfný obraz ľubovoľného modelu teórie T je tiež modelom T.

7.6.1 Veta. *Nech T je bezosporná teória. Potom nasledujúce podmienky sú ekvivalentné:*

(i) *T má množinu pozitívnych axióm.*

(ii) *T sa prenáša na homomorfné obrazy.*

Dôkaz. Opäť sa sústredíme len na implikáciu (ii) $\Rightarrow$ (i). Nech platí (ii). Pre ľubovoľné rozšírenie L_C jazyka L o nové konštanty označíme $\mathrm{Pos}(L_C)$, resp. $\mathrm{Neg}(L_C)$ množinu všetkých uzavretých formúl jazyka L_C ekvivalentných, s pozitívnymi, resp. negatívnymi formulami. Zrejme $\mathrm{Pos}(L)$ je uzavretá na konečné disjunkcie. Pomocou Axiomatizačnej lemy 7.1.2 dokážeme, že T má množinu axióm $\Gamma \subseteq \mathrm{Pos}(L)$. Nech teda $\mathcal{A} \models T$ a platí

(0) $\mathcal{B} \models \mathrm{Th}(\mathcal{A}) \cap \mathrm{Pos}(L)$.

Za tohto predpokladu dokážeme nasledujúce tvrdenia:

(1) Existuje elementárne rozšírenie $\mathcal{B}' \succ \mathcal{B}$ a homomorfizmus $h\colon \mathcal{A} \to \mathcal{B}'$ také, že $(\mathcal{B}', h(a))_{a\in A} \models \mathrm{Th}(\mathcal{A}_A) \cap \mathrm{Pos}(L_A)$.

(2) Existuje elementárne rozšírenie $\mathcal{A}' \succ \mathcal{A}$ a zobrazenie $g\colon B \to A'$ také, že $(\mathcal{B}, b)_{b\in B} \models \mathrm{Th}(\mathcal{A}', g(b))_{b\in B} \cap \mathrm{Pos}(L_B)$.

(1): Uvažujme teóriu $\mathrm{Th}(\mathcal{B}_B) \cup \big(\mathrm{Th}(\mathcal{A}_A) \cap \mathrm{Pos}(L_A)\big)$ v jazyku $L_{A,B}$. Z predpokladu (0) možno odvodiť, že je bezosporná, rutinným použitím Lemy 7.1.1 o vzájomnej zlučiteľnosti a Lemy 4.7.1 o konštantách. Nech $(\mathcal{B}', h(a), b)_{a\in A, b\in B}$ je jej model, kde $\mathcal{B}$ je štruktúra jazyka L. Potom $\mathcal{B} \prec \mathcal{B}'$, a platí $(\mathcal{B}', h(a))_{a\in A} \models \mathrm{Th}(\mathcal{A}_A) \cap \mathrm{Pos}(L_A)$, z čoho okrem iného vyplýva, že $h\colon \mathcal{A} \to \mathcal{B}$ je homomorfizmus.

(2): Podobne ako v (1) možno na základe predpokladu (0) dokázať bezospornosť teórie $\mathrm{Th}(\mathcal{A}_A) \cup \big(\mathrm{Th}(\mathcal{B}_B) \cap \mathrm{Neg}(L_B)\big)$ v jazyku $L_{A,B}$ s použitím rovnakých prostriedkov. Nech $(\mathcal{A}', a, g(b))_{a\in A, b\in B}$ je jej model, kde $\mathcal{A}'$ je štruktúra jazyka L. Potom $\mathcal{A} \prec \mathcal{A}'$ a pre zobrazenie $g\colon B \to A'$ platí $(\mathcal{A}', g(b))_{b\in B} \models \mathrm{Th}(\mathcal{B}_B) \cap \mathrm{Neg}(L_B)$, teda $(\mathcal{B}, b)_{b\in B} \models \mathrm{Th}(\mathcal{A}', g(b))_{b\in B} \cap \mathrm{Pos}(L_B)$.

Striedavou iteráciou konštrukcií (1), (2) teraz zostrojíme dve postupnosti $(\mathcal{A}_n)_{n<\omega}$, $(\mathcal{B}_n)_{n<\omega}$ štruktúr jazyka L, spolu so zobrazeniami $g_n\colon B_n \to A_{n+1}$ a homomorfizmami $h_{n+1}\colon \mathcal{A}_{n+1} \to \mathcal{B}_{n+1}$ v nasledujúcich krokoch:

0° Na začiatok položíme $\mathcal{A}_0 = \mathcal{A}$, $\mathcal{B}_0 = \mathcal{B}$.

1° Štruktúru $\mathcal{A}_{n+1}$ a zobrazenie $g_n\colon B_n \to A_{n+1}$ také, že platí

$$(\mathcal{B}_n, b)_{b\in B_n} \vDash \mathrm{Th}(\mathcal{A}_{n+1}, g_n(b))_{b\in B_n} \cap \mathrm{Pos}(L_{B_n})$$

zostrojíme zo štruktúr $\mathcal{A}_n$, $\mathcal{B}_n$ jazyka L podľa (2).

2° Štruktúru $(\mathcal{B}_1, b)_{b\in B_0}$ a homomorfizmus $h_1\colon (\mathcal{A}_1, g_0(b))_{b\in B_0} \to (\mathcal{B}_1, b)_{b\in B_0}$ také, že platí

$$(\mathcal{B}_1, b, h_1(a))_{b\in B_0, a\in A_1} \vDash \mathrm{Th}(\mathcal{A}_1, g_0(b), a)_{b\in B_0, a\in A_1} \cap \mathrm{Pos}(L_{B_0,A_1})$$

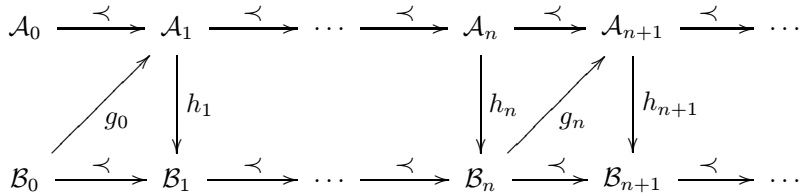
dostaneme zo štruktúr $(\mathcal{A}_1, g_0(b))_{b\in B_0}$, $(\mathcal{B}_0, b)_{b\in B_0}$ jazyka L_{B_0} podľa (1).

3° Konečne pre $n \geq 1$ štruktúru $(\mathcal{B}_{n+1}, h_n(a), b)_{a\in A_n, b\in B_n}$ spolu s homomorfizmom $h_{n+1}\colon (\mathcal{A}_{n+1}, a, g_n(b))_{a\in A_n, b\in B_n} \to (\mathcal{B}_{n+1}, h_n(a), b)_{a\in A_n, b\in B_n}$ tak, že platí

$$(\mathcal{B}_{n+1}, h_n(a), b, h_{n+1}(a'))_{a\in A_n, b\in B_n, a'\in A_{n+1}} \vDash \mathrm{Th}(\mathcal{A}_{n+1}, a, g_n(b), a')_{a\in A_n, b\in B_n, a'\in A_{n+1}} \cap \mathrm{Pos}(L_{A_n,B_n,A_{n+1}})$$

zostrojíme podľa (1) zo štruktúr $(\mathcal{A}_{n+1}, a, g_n(b))_{a\in A_n, b\in B_n}$,$(\mathcal{B}_n, h_n(a), b)_{a\in A_n, b\in B_n}$ jazyka L_{A_n,B_n}.

Pritom si treba uvedomiť, že práve splnenie uvedených podmienok, t. j. predpokladov typu (0), zakaždým zabezpečuje uskutočniteľnosť nasledujúceho kroku. Takto dostaneme dva vzájomne prepojené elementárne reťazce



Krok 3° o. i. zaručuje, že pre $n \geq 1$ a ľubovoľné $a \in A_n$ platí $h_n(a) = h_{n+1}(a)$, t. j. $h_n = h_{n+1} \restriction A_n$. Podobne, kroky 2° a 3° zaručujú, že pre každé n a ľubovoľné $b \in B_n$ platí $h_{n+1}(g_n(b)) = b$, preto tiež $B_n \subseteq h_{n+1}(A_{n+1})$.

Utvorme zjednotenia elementárnych reťazcov

$$\mathcal{A}_\omega = \bigcup_{n<\omega} \mathcal{A}_n \qquad\qquad \mathcal{B}_\omega = \bigcup_{n<\omega} \mathcal{B}_n$$

a položme

$$h_\omega = \bigcup_{1\leq n<\omega} h_n$$

Potom $\mathcal{A} \prec \mathcal{A}_\omega$, $\mathcal{B} \prec \mathcal{B}_\omega$ a $h_\omega\colon \mathcal{A}_\omega \to \mathcal{B}_\omega$ je zrejme surjektívny homomorfizmus. Z podmienky $\mathcal{A} \vDash T$ vyplýva, že $\mathcal{A}_\omega \vDash T$, a keďže T sa prenáša na homomorfné obrazy, tiež $\mathcal{B}_\omega \vDash T$, teda konečne $\mathcal{B} \vDash T$. Podľa Axiomatizačnej lemy 7.1.2 má T množinu pozitívnych axióm.

7.6.2 Úloha. Za predpokladu (0) z dôkazu Vety 7.6.1 dokážte bezospornosť oboch teórií $\mathrm{Th}(\mathcal{B}_B) \cup (\mathrm{Th}(\mathcal{A}_A) \cap \mathrm{Pos}(L_A))$ a $\mathrm{Th}(\mathcal{A}_A) \cup (\mathrm{Th}(\mathcal{B}_B) \cap \mathrm{Neg}(L_B))$ v jazyku $L_{A,B}$, vyskytujúcich sa v (1), resp. (2).

8 Ultraprodukty a axiomatické triedy

Naša záverečná kapitola je venovaná konštrukciám modelov vychádzajúcim z konštrukcie priameho súčinu. Pôjde o tzv. *filtrované súčiny* a *filtrované mocniny*. Z nich najdôležitejší prípad predstavujú tzv. *ultraprodukty*, ktoré zachovávajú všetky vlastnosti prvého rádu, a *ultramocniny*, pomocou ktorých možno jednotným a elegantným spôsobom vytvárať elementárne rozšírenia štruktúr. Taktiež predvedieme niekoľko aplikácií týchto konštrukcií, no čitateľ by si mal byť vedomý toho, že ide len o malú ukážku, ktorou sa možnosti využitia ultraproduktov zďaleka nevyčerpávajú.

8.1 Priamy súčin štruktúr

Priamym alebo *karteziánskym súčinom* systému množín $(A_i)_{i\in I}$ nazývame množinu $\prod_{i\in I} A_i$ všetkých funkcií $\alpha\colon I \to \bigcup_{i\in I} A_i$ takých, že $\alpha(i) \in A_i$ pre každé $i \in I$. Tvrdenie, že pre ľubovoľný systém $(A_i)_{i\in I}$ *neprázdnych* množín A_i je aj ich karteziánsky súčin neprázdny, je ekvivalentné s axiómou výberu, ktorej platnosť budeme automaticky predpokladať.

8.1.1 Úloha. Rozmyslite si, že pre *konečný* systém $(A_i)_{i=1}^n$ existuje prirodzená bijekcia medzi „dvoma verziami“ karteziánskeho súčinu $A_1 \times \ldots \times A_n$ a $\prod_{i=1}^n A_i$ a explicitne ju popíšte.

Priamou alebo *karteziánskou mocninou* množiny A s množinou indexov I nazývame priamy súčin

$$A^I = \prod_{i\in I} A_i$$

v ktorom $A_i = A$ pre každé $i \in I$. Ak $I \neq \emptyset$, tak máme k dispozícii prosté *diagonálne zobrazenie* $A \to A^I$, ktoré zobrazí každý prvok $a \in A$ na konštantnú funkciu $\overline{a} \in A^I$, čiže $\overline{a}(i) = a$ pre všetky $i \in I$.

Nech $(\mathcal{A}_i)_{i\in I}$ je systém štruktúr prvého rádu nad množinou I. *Priamym súčinom* týchto štruktúr nazývame štruktúru

$$\widetilde{\mathcal{A}} = \prod_{i\in I} \mathcal{A}_i$$

so základnou množinou $\widetilde{A} = \prod_{i\in I} A_i$, v ktorej sú operačné a relačné symboly interpretované po zložkách, čiže pre ľubovoľný n-árny funkcionálny symbol f, resp. n-árny

relačný symbol r jazyka L a všetky $\alpha_1, \dots, \alpha_n \in \widetilde{A}$ platí

$$f^{\widetilde{\mathcal{A}}}(\alpha_1, \dots, \alpha_n)(i) = f^{\mathcal{A}_i}(\alpha_1(i), \dots, \alpha_n(i)) \qquad \text{pre každé } i \in I$$
$$(\alpha_1, \dots, \alpha_n) \in r^{\widetilde{\mathcal{A}}} \;\Leftrightarrow\; (\alpha_1(i), \dots, \alpha_n(i)) \in r^{\mathcal{A}_i} \quad \text{pre každé } i \in I$$

Uvedené definície sa jednoducho prenesú aj na ľubovoľné termy, resp. atomické formuly. Samostatne si overte, že pre ľubovoľný term $t(x_1, \dots, x_n)$, resp. atomickú formulu $\varphi(x_1, \dots, x_n)$ a prvky $\alpha_1, \dots, \alpha_n \in \widetilde{A}$ platí

$$t^{\widetilde{\mathcal{A}}}(\alpha_1, \dots, \alpha_n)(i) = t^{\mathcal{A}_i}(\alpha_1(i), \dots, \alpha_n(i)) \qquad \text{pre každé } i \in I$$
$$\widetilde{A} \vDash \varphi(\alpha_1, \dots, \alpha_n) \;\Leftrightarrow\; \mathcal{A}_i \vDash \varphi(\alpha_1(i), \dots, \alpha_n(i)) \quad \text{pre každé } i \in I$$

Pre úplnosť ešte definujeme priamy súčin prázdneho systému štruktúr (zodpovedajúci prípadu $I = \emptyset$) ako jednoprvkovú štruktúru s operačnými symbolmi interpretovanými jediným možným spôsobom a s plnými reláciami.

Ak je indexová množina I zrejmá z kontextu, píšeme len $\prod A_i$, resp. $\prod \mathcal{A}_i$.

Priamou mocninou štruktúry $\mathcal{A}$ s množinou indexov I nazývame priamy súčin

$$\mathcal{A}^I = \prod_{i \in I} \mathcal{A}_i$$

v ktorom $\mathcal{A}_i = \mathcal{A}$ pre každé $i \in I$. Zrejme ak $I \neq \emptyset$, tak diagonálne zobrazenie $A \to A^I$ je vnorením štruktúry $\mathcal{A}$ do jej priamej mocniny $\mathcal{A}^I$, čiže $\mathcal{A} \hookrightarrow \mathcal{A}^I$.

Pre ľubovoľnú formulu $\varphi(x_1, \dots, x_n)$ jazyka L definujeme jej *boolovskú pravdivostnú hodnotu* na prvkoch $\alpha_1, \dots, \alpha_n \in \prod A_i$ ako množinu

$$[\varphi(\alpha_1, \dots, \alpha_n)] = \big\{ i \in I \colon \mathcal{A}_i \vDash \varphi(\alpha_1(i), \dots, \alpha_n(i)) \big\}$$

Zrejme $[\varphi(\alpha_1, \dots, \alpha_n)] \subseteq I$, teda boolovská pravdivostná hodnota $[\varphi(\alpha_1, \dots, \alpha_n)]$ je prvkom Boolovej algebry $\mathcal{P}(I)$ všetkých podmnožín množiny I.

Všimnite si, že v priamej mocnine nadobúda boolovská pravdivostná hodnota na konštantných funkciách len dve hodnoty.

8.1.2 Tvrdenie. *Nech I je neprázdna množina, $\mathcal{A}$ je štruktúra a $\varphi(x_1, \dots, x_n)$ je formula. Potom pre všetky $a_1, \dots, a_n \in A$ platí*

$$[\varphi(\overline{a}_1, \dots, \overline{a}_n)] = \begin{cases} I & \text{ak } \mathcal{A} \vDash \varphi(a_1, \dots, a_n) \\ \emptyset & \text{ak } \mathcal{A} \nvDash \varphi(a_1, \dots, a_n) \end{cases}$$

Boolovská pravdivostná hodnota formúl zachováva prirodzený súvis medzi logickými spojkami a boolovskými operáciami v Boolovej algebry $\mathcal{P}(I)$. Jednoduchý dôkaz nasledujúceho tvrdenia prenechávame ako cvičenie čitateľovi.

8.1.3 Tvrdenie. *Nech $(\mathcal{A}_i)_{i \in I}$ je systém štruktúr a $\varphi(x_1, \dots, x_n)$, $\psi(x_1, \dots, x_n)$ sú formuly. Potom pre ľubovoľné $\alpha_1, \dots, \alpha_n \in \prod A_i$ platí*

$$[\neg\varphi(\alpha_1, \dots, \alpha_n)] = I \smallsetminus [\varphi(\alpha_1, \dots, \alpha_n)]$$
$$[(\varphi \wedge \psi)(\alpha_1, \dots, \alpha_n)] = [\varphi(\alpha_1, \dots, \alpha_n)] \cap [\psi(\alpha_1, \dots, \alpha_n)]$$
$$[(\varphi \vee \psi)(\alpha_1, \dots, \alpha_n)] = [\varphi(\alpha_1, \dots, \alpha_n)] \cup [\psi(\alpha_1, \dots, \alpha_n)]$$

Pre boolovskú pravdivostnú hodnotu existenčne kvantifikovaných formúl platí tzv. *princíp maximality.*

8.1.4 Tvrdenie. *Nech $(\mathcal{A}_i)_{i\in I}$ je systém štruktúr a $\varphi(x,x_1,\dots,x_n)$ je formula. Potom pre ľubovoľné $\alpha_1,\dots,\alpha_n \in \prod A_i$ existuje $\alpha_0 \in \prod A_i$ také, že pre ľubovoľné $\alpha \in \prod A_i$ platí*

$$[\varphi(\alpha,\alpha_1,\dots,\alpha_n)] \subseteq [\varphi(\alpha_0,\alpha_1,\dots,\alpha_n)] = [(\exists\, x)\varphi(x,\alpha_1,\dots,\alpha_n)]$$

Dôkaz. Označme

$$J = [(\exists\, x)\varphi(x,\alpha_1,\dots,\alpha_n)] = \big\{i \in I\colon (\exists\, a_i \in A_i)\big(\mathcal{A}_i \vDash \varphi(a_i,\alpha_1(i),\dots,\alpha_n(i))\big)\big\}$$

S použitím axiómy výberu definujeme funkciu $\alpha_0 \in \prod A_i$ takto:

$$\alpha_0(i) = \begin{cases} a_i & \text{kde pre prvok } a_i \in A_i \text{ platí } \varphi(a_i,\alpha_1(i),\dots,\alpha_n(i)), \text{ ak } i \in J \\ a_i & \text{kde } a_i \text{ je ľubovoľný prvok množiny } A_i, \text{ ak } i \notin J \end{cases}$$

Overenie, že funkcia α_0 spĺňa všetky požadované podmienky, prenechávame čitateľovi.

Nasledujúce dve tvrdenia ukazujú, že boolovská pravdivostná hodnota spĺňa podmienky analogické axiómam rovnosti. A s použitím týchto axióm ich naozaj možno jednoducho overiť – skúste samostatne.

8.1.5 Tvrdenie. *Nech $(\mathcal{A}_i)_{i\in I}$ je systém štruktúr. Potom pre ľubovoľné $\alpha,\beta,\gamma \in \prod A_i$ platí*

$$[\alpha=\alpha] = I$$
$$[\alpha=\beta] = [\beta=\alpha]$$
$$[\alpha=\beta] \cap [\beta=\gamma] \subseteq [\alpha=\gamma]$$

8.1.6 Tvrdenie. *Nech $(\mathcal{A}_i)_{i\in I}$ je systém štruktúr, $t(x_1,\dots,x_n)$ je term a $\varphi(x_1,\dots,x_n)$ je formula jazyka L. Potom pre ľubovoľné $\alpha_1,\beta_1,\dots,\alpha_n,\beta_n \in \prod A_i$ platí*

$$[\alpha_1=\beta_1]\cap\ldots\cap[\alpha_n=\beta_n] \subseteq [t(\alpha_1,\dots,\alpha_n) = t(\beta_1,\dots,\beta_n)]$$
$$[\alpha_1=\beta_1]\cap\ldots\cap[\alpha_n=\beta_n]\cap[\varphi(\alpha_1,\dots,\alpha_n)] \subseteq [\varphi(\beta_1,\dots,\beta_n)]$$

Všimnite is, že pre atomickú fomulu $\varphi(x_1,\dots,x_n)$ platí

$$\prod_{i\in I}\mathcal{A}_i \vDash \varphi(\alpha_1,\dots,\alpha_n) \;\Leftrightarrow\; [\varphi(\alpha_1,\dots,\alpha_n)] = I$$

čiže na jej splnenie je potrebné, aby „platila všade“. Na druhej strane pre jej negáciu $\neg\varphi(x_1,\dots,x_n)$ máme

$$\prod_{i\in I}\mathcal{A}_i \vDash \neg\varphi(\alpha_1,\dots,\alpha_n) \;\Leftrightarrow\; [\neg\varphi(\alpha_1,\dots,\alpha_n)] \neq \emptyset$$

teda na jej splnenie postačuje, aby platila aspoň v jednej zo štruktúr $\mathcal{A}_i$. Inak povedané, naša definícia štruktúry $\prod\mathcal{A}_i$ má za následok, že pre spĺňanie formúl rôzneho syntaktického tvaru platia rôzne kritéria na ich boolovskú pravdivostnú hodnotu. V nasledujúcich troch paragrafoch sa pokúsime v tejto situácii trochu zorientovať.

8.2 Filtre a ultrafiltre

Filtrom na množine I nazývame ľubovoľnú neprázdnu množinu $\mathcal{D} \subseteq \mathcal{P}(I)$ takú, že pre ľubovoľné $X, Y \subseteq I$ platí
(a) ak $X \in \mathcal{D}$ a $X \subseteq Y$, tak $Y \in \mathcal{D}$;
(b) ak $X, Y \in \mathcal{D}$, tak aj $X \cap Y \in \mathcal{D}$.
Miesto názvu *filter* sa niekedy používa názov *duálny ideál*. Podmienky (a), (b) majú za následok, že pre ľubovoľné $X, Y \subseteq I$ platí $X \cap Y \in \mathcal{D}$ práve vtedy, keď zároveň $X \in \mathcal{D}$ a $Y \in \mathcal{D}$.

Zrejme každý filter obsahuje celú množinu I a jednoprvková množina $\mathcal{D} = \{I\}$ je najmenší zo všetkých filtrov na množine I – hovoríme mu *triviálny filter*. Aj systém $\mathcal{P}(I)$ všetkých podmnožín množiny I tvorí filter na I – hovoríme mu *nevlastný filter*. Ostatné filtre nazývame *vlastné*. Zrejme filter $\mathcal{D}$ je vlastný práve vtedy, keď $\emptyset \notin \mathcal{D}$. Niektorí autori pod pojmom *filter* rozumejú iba vlastný filter. Trochu všeobecnejšie, pre každú množinu $J \subseteq I$ je

$$\mathcal{P}_J(I) = \{X \subseteq I : J \subseteq X\}$$

filtrom na množine I; takéto filtre nazývame *hlavné filtre*. Zrejme na konečnej množine I sú všetky filtre hlavné. Na nekonečnej množine však existujú aj *nehlavné filtre*, t. j. také, ktoré nemajú najmenší prvok. Príkladom je tzv *Fréchetov filter*

$$\mathcal{F}(I) = \{X \subseteq I : \text{množina } I \setminus X \text{ je konečná}\}$$

Zrejme pre konečnú množinu I splýva Fréchetov filter $\mathcal{F}(I)$ s nevlastným filtrom $\mathcal{P}(I)$. Ak je však I nekonečná, tak $\mathcal{F}(I)$ je netriviálny, vlastný a nehlavný filter na I.

Ďalšie príklady filtrov poskytujú topologické, resp. merateľné priestory. V topologickom priestore $(X, \mathcal{T})$ tvorí pre každý bod $x \in X$ množina

$$\mathcal{V}(x) = \{V \subseteq X : (\exists U \in \mathcal{T})(x \in U \subseteq V)\}$$

filter na množine X nazývaný *filtrom okolí* bodu x.

Podobne, ak $\mathbf{X} = (X, \mathcal{B}, \mu)$ je merateľný priestor s úplnou mierou μ (t. j. pre ľubovoľné $A, B \subseteq X$ z podmienok $A \subseteq B \in \mathcal{B}$ a $\mu(B) = 0$ vyplýva $A \in \mathcal{B}$ a $\mu(A) = 0$), tak množina

$$\mathcal{Z}(\mathbf{X}) = \{A \subseteq X : \mu(X \setminus A) = 0\}$$

tvorí filter na X.

Intuitívne sa na (vlastný) filter $\mathcal{D}$ na množine I pozeráme ako na systém jej podmnožín, ktoré sú z istého hľadiska „veľké“, preto ich príslušný filter „zachytí“. Pritom takýchto hľadísk môže byť mnoho – každý (vlastný) filter predstavuje jednu z možností. Ak má byť však takéto hľadisko „rozumné“, určite musí spĺňať podmienku (a); podmienka (b) vyjadruje idealizujúcu požiadavku, že doplnok „veľkej“ množiny musí byť „malý“, pričom zjednotenie dvoch „malých“ množín by mala byť opäť „malá“ množina.

Filter $\mathcal{D}$ na množine I nazývame *ultrafiltrom*, ak $\mathcal{D}$ je vlastný filter a pre ľubovoľnú množinu $X \subseteq I$ platí $X \in \mathcal{D}$ alebo $I \setminus X \in \mathcal{D}$ (pre vlastný filter môže nastať iba jedna z týchto dvoch možností). Zrejme pre ľuboľný prvok $i \in I$ je hlavný filter

$$\mathcal{P}_{\{i\}}(I) = \{X \subseteq I : i \in X\}$$

ultrafiltrom na množine I. Nás však zaujímaju najmä nehlavné ultrafiltre – také však môžu existovať len na nekonečných množinách. Zrejme to musia byť ultrafiltre, ktoré rozširujú Fréchetov filter $\mathcal{F}(I)$.

Samostatne si premyslite, že filter $\mathcal{D}$ na množine I je ultrafilter práve vtedy, keď je to maximálny vlastný filter na I. Z axiómy výberu, presnejšie z jej ekvivalentnej formulácie v tvare Zornovej lemy alebo Hausdorffovho princípu maximality tak vyplýva nasledujúci výsledok. Systém podmnožín $\mathcal{S} \subseteq \mathcal{P}(I)$ množiny I nazývame *centrovaný*, ak pre ľubovoľný konečný počet množín $X_1, \ldots, X_n \in \mathcal{S}$ platí $X_1 \cap \ldots \cap X_n \neq \emptyset$.

8.2.1 Tvrdenie. *Nech $\mathcal{S}$ je ľubovoľný centrovaný systém podmnožín množiny I. Potom existuje ultrafilter $\mathcal{E}$ na I taký, že $\mathcal{S} \subseteq \mathcal{E}$. Špeciálne pre ľubovoľný vlastný filter $\mathcal{D}$ na množine I existuje ultrafilter $\mathcal{E}$ na I taký, že $\mathcal{D} \subseteq \mathcal{E}$.*

8.3 Filtrované súčiny

Základná myšlienka konštrukcie filtrovaného súčinu spočíva v istom oslabení požiadaviek na rovnosť funkcií v priamom súčine a na ich zaradenie do relácií zodpovedajúcich relačným symbolom príslušného jazyka. Funkcie z priameho súčinu, ktoré sa rovnajú na „veľkej“ podmnožine indexovej množiny, stotožníme, a na zaradenie nejakej n-tice funkcií do príslušnej relácie postačí, ak sú jednotlivé zložky prvkov tejto n-tice v príslušných reláciách na jednotlivých činiteľoch pre „veľkú“ množinu indexov. Presnejší popis celej konštrukcie nasleduje.

Nech $(A_i)_{i\in I}$ je systém množín a $\mathcal{D}$ je filter na množine I. Pre ľubovoľné funkcie $\alpha, \beta \in \prod A_i$ položíme

$$\alpha \equiv_{\mathcal{D}} \beta \;\Leftrightarrow\; [\alpha = \beta] \in \mathcal{D}$$

Z vlastností filtra a boolovskej pravdivostnej hodnoty okamžite vyplýva, že $\equiv_{\mathcal{D}}$ je relácia ekvivalencie na množine $\prod_{i\in I} A_i$. Faktorovú množinu $\prod_{i\in I} A_i/{\equiv_{\mathcal{D}}}$ budeme značiť

$$\prod_{i\in I} A_i \Big/ \mathcal{D} \quad \text{alebo len} \quad \prod A_i \Big/ \mathcal{D}$$

a nazývať *filtrovaným* alebo *redukovaným súčinom* systému množín $(A_i)_{i\in I}$ podľa filtra $\mathcal{D}$. Triedu ekvivalencie funkcie $\alpha \in \prod A_i$ značíme $\alpha^{\mathcal{D}}$. Zrejme priradením $\alpha \mapsto \alpha^{\mathcal{D}}$ je určené kanonické surjektívne zobrazenie $\prod_{i\in I} A_i \to \prod_{i\in I} A_i/\mathcal{D}$ priameho súčinu $\prod A_i$ na filtrovaný súčin $\prod A_i/\mathcal{D}$.

Ak $(\mathcal{A}_i)_{i\in I}$ je systém štruktúr prvého rádu, tak *filtrovaným* alebo tiež *redukovaným súčinom* tohto systému nazývame štruktúru

$$\widetilde{\mathcal{A}}/\mathcal{D} = \prod_{i\in I} \mathcal{A}_i \Big/ \mathcal{D}$$

so základnou množinou $\prod_{i\in I} A_i/\mathcal{D}$, na ktorej sú špecifické symboly príslušného jazyka L interpretované takto:

$$f^{\widetilde{\mathcal{A}}/\mathcal{D}}\big(\alpha_1^{\mathcal{D}}, \ldots, \alpha_n^{\mathcal{D}}\big) = f^{\widetilde{\mathcal{A}}}(\alpha_1, \ldots, \alpha_n)^{\mathcal{D}}$$
$$\big(\alpha_1^{\mathcal{D}}, \ldots, \alpha_n^{\mathcal{D}}\big) \in r^{\widetilde{\mathcal{A}}/\mathcal{D}} \;\Leftrightarrow\; [r(\alpha_1, \ldots, \alpha_n)] \in \mathcal{D}$$

pre ľubovoľný n-árny funkcionálny symbol n, resp. n-árny relačný symbol r a všetky $\alpha_1, \dots, \alpha_n \in \prod A_i$.

Vlastnosti filtrov a boolovskej pravdivostnej hodnoty zaručujú, že uvedené definície sú korektné, teda nezávisia od jednotlivých reprezentantov α_k tried ekvivalencie $\alpha_k^{\mathcal{D}}$ pre $k = 1, \dots, n$. (Rozmyslite si samostatne.) Kanonické zobrazenie $\prod A_i \to \prod A_i/\mathcal{D}$ dané priradením $\alpha \mapsto \alpha^{\mathcal{D}}$ je potom homomorfizmom priameho súčinu $\prod \mathcal{A}_i$ na redukovaný súčin $\prod \mathcal{A}_i/\mathcal{D}$.

Ak $J \subseteq I$ a $\mathcal{D} = \mathcal{P}_J(I)$ je hlavný filter, tak priradenie $\alpha \mapsto \alpha \restriction J$, ktoré každú funkciu $\alpha \in \prod_{i\in I} A_i$ zobrazí na jej zúženie $\alpha \restriction J \in \prod_{i\in J} A_i$, má tu vlastnosť, že

$$\alpha \restriction J = \beta \restriction J \;\Leftrightarrow\; J \subseteq [\alpha = \beta] \;\Leftrightarrow\; \alpha \equiv_{\mathcal{D}} \beta$$

pre ľubovoľné $\alpha, \beta \in \prod A_i$. Teda priradením $\alpha^{\mathcal{D}} \mapsto \alpha \restriction J$ je definované bijektívne zobrazenie $\prod_{i\in I} A_i/\mathcal{D} \to \prod_{i\in J} A_i$. Čitateľ by si mal samostatne premyslieť, že to je dokonca izomorfizmus filtrovaného súčinu $\prod_{i\in I} \mathcal{A}_i/\mathcal{D}$ na priamy súčin $\prod_{i\in J} \mathcal{A}_i$. V niektorých špeciálnych prípadoch dostávame

$$\prod_{i\in I} \mathcal{A}_i \Big/ \mathcal{D} \cong \prod_{i\in I} \mathcal{A}_i \qquad \text{pre triviálny filter } \mathcal{D} = \{I\}$$

$$\prod_{i\in I} \mathcal{A}_i \Big/ \mathcal{D} \cong \mathcal{A}_j \qquad \text{pre hlavný ultrafilter } \mathcal{D} = \{X \subseteq I \colon j \in X\}$$

$$\prod_{i\in I} \mathcal{A}_i \Big/ \mathcal{D} \cong \prod_{i\in \emptyset} \mathcal{A}_i \qquad \text{pre nevlastný filter } \mathcal{D} = \mathcal{P}(I)$$

Každopádne je však jasné, že redukované súčiny možu priniesť niečo nové v porovnaní s priamymi súčinmi jedine v prípade nehlavných filtrov.

Filtrovanou alebo *redukovanou mocninou* štruktúry $\mathcal{A}$ s množinou indexov I podľa filtra $\mathcal{D}$ na I nazývame filtrovaný súčin

$$\mathcal{A}^I/\mathcal{D} = \prod_{i\in I} \mathcal{A}_i \Big/ \mathcal{D}$$

v ktorom $\mathcal{A}_i = \mathcal{A}$ pre každé $i \in I$. Priradenie $a \mapsto \overline{a}^{\mathcal{D}}$, ktoré zobrazí každý prvok $a \in A$ na triedu ekvivalencie $\overline{a}^{\mathcal{D}} \in A^I/\mathcal{D}$ konštantnej funkcie $\overline{a} \in A^I$, nazývame *diagonálnym zobrazením* množiny A do jej filtrovanej mocniny $A^I/\mathcal{D}$. Z vlastností filtrov a boolovskej pravdivostnej hodnoty okamžite vyplýva nasledujúce pozorovanie. Dôkaz prenechávame čitateľovi.

8.3.1 Tvrdenie. *Nech $\mathcal{A}$ je štruktúra a $\mathcal{D}$ je vlastný filter na neprázdnej množine I. Potom diagonálne zobrazenie $A \to A^I/\mathcal{D}$ je vnorením štruktúry $\mathcal{A}$ do jej filtrovanej mocniny $\mathcal{A}^I/\mathcal{D}$, čiže $\mathcal{A} \hookrightarrow \mathcal{A}^I/\mathcal{D}$.*

8.3.2 Príklad. (a) Filtrovaná mocnina $\mathbb{R}^{\mathbb{N}}/\mathcal{F}$ podľa Fréchetovho filtra $\mathcal{F} = \mathcal{F}(\mathbb{N})$ pozostáva z tried ekvivalencie $\alpha^{\mathcal{F}}$ všetkých reálnych postupností $\alpha \colon \mathbb{N} \to \mathbb{R}$, pričom postupnosti α, β predstavujú tú istú triedu ekvivalencie práve vtedy, keď sa rovnajú

„skoro všade“, t. j. všade nanajvýš s výnimkou prvkov $n \in J$ nejakej konečnej množiny $J \subseteq \mathbb{N}$.

(b) Nech $\mathbf{X} = (X, \mathcal{B}, \mu)$ je merateľný priestor s úplnou mierou μ a $\mathcal{Z} = \mathcal{Z}(\mathbf{X})$ je filter na X pozostávajúci zo všetkých množín $A \subseteq X$, ktorých doplnok má mieru 0. Potom filtrovaná mocnina $\mathbb{R}^X\big/\mathcal{Z}$ pozostáva z tried ekvivalencie $\alpha^{\mathcal{Z}}$ všetkých reálnych funkcií $\alpha\colon X \to \mathbb{R}$, pričom funkcie α, β predstavujú tú istú triedu ekvivalencie práve vtedy, keď sa rovnajú „skoro všade“, t. j. všade nanajvýš s výnimkou prvkov $x \in B$ nejakej množiny $B \in \mathcal{B}$ miery 0.

8.3.3 Úloha. (Frayne-Morel-Scott) (a) Nech $K \neq \emptyset$, $(I_k)_{k\in K}$ je systém neprázdnych po dvoch disjunktných množín a $I = \bigcup_{k\in K} I_k$. Nech ďalej $(A_i)_{i\in I}$ je systém neprázdnych množín. Zobrazenie h z priameho súčinu $\prod_{i\in I} A_i$ do iterovaného priameho súčinu $\prod_{k\in K}\Big(\prod_{i\in I_k} A_i\Big)$ je dané predpisom

$$h(\alpha)(k) = \alpha \restriction I_k$$

pre $\alpha \in \prod_{i\in I} A_i$, $k \in K$. Dokážte, že h je bijektívne zobrazenie. Za predpokladu, že $(\mathcal{A}_i)_{i\in I}$ je systém štruktúr jazyka prvého rádu L dokážte, že

$$h\colon \prod_{i\in I} \mathcal{A}_i \longrightarrow \prod_{k\in K}\Big(\prod_{i\in I_k} \mathcal{A}_i\Big)$$

je izomorfizmus L-štruktúr.

(b) Nech ďalej $\mathcal{E}$ je filter na množine K a pre každé $k \in K$ nech $\mathcal{D}_k$ je filter na množine I_k. Položme

$$\mathcal{D} = \big\{X \subseteq I\colon \{k \in K\colon X \cap I_k \in \mathcal{D}_k\} \in \mathcal{E}\big\}$$

Dokážte, že $\mathcal{D}$ je filter na množine I.

(c) Dokážte, že $\mathcal{D}$ je ultrafilter práve vtedy, keď $\mathcal{E}$ je ultrafilter a

$$\{k \in K\colon \mathcal{D}_k \text{ je ultrafilter}\} \in \mathcal{E}$$

(d) S využitím zobrazenia h z (a) zostrojte prirodzenú bijekciu medzi filtrovaným súčinom $\prod_{i\in I} A_i/\mathcal{D}$ a iterovaným filtrovaným súčinom

$$\prod_{k\in K}\Big(\prod_{i\in I_k} A_i\Big/\mathcal{D}_k\Big)\Big/\mathcal{E}$$

(e) Dokážte, že bijekcia popísaná v (d) je izomorfizmom L-štruktúr

$$\prod_{i\in I} \mathcal{A}_i\Big/\mathcal{D} \longrightarrow \prod_{k\in K}\Big(\prod_{i\in I_k} \mathcal{A}_i\Big/\mathcal{D}_k\Big)\Big/\mathcal{E}$$

8.4 Ultraprodukty

Ultraproduktom systému $(\mathcal{A}_i)_{i\in I}$ štruktúr prvého rádu nazývame redukovaný súčin

$$\prod_{i\in I}\mathcal{A}_i\Big/\mathcal{D}$$

tohto systému podľa nejakého ultrafiltra $\mathcal{D}$ na množine I. Filtrovanú mocninu $\mathcal{A}^I/\mathcal{D}$ štruktúry $\mathcal{A}$ podľa ultrafiltra $\mathcal{D}$ nazývame *ultramocninou* štruktúry $\mathcal{A}$.

Keďže pre hlavný ultrafilter $\mathcal{D}=\mathcal{P}_{\{j\}}(I)$ platí $\prod\mathcal{A}_i/\mathcal{D}\cong\mathcal{A}_j$, budeme sa zaujímať hlavne o ultraprodukty podľa nehlavných ultrafiltrov. Také môžu existovať iba na nekonečných množinách. Zrejme ultrafilter $\mathcal{D}$ na nekonečnej množine I je nehlavný práve vtedy, keď je rozšírením Fréchetovho filtra, t. j. platí preň $\mathcal{F}(I)\subseteq\mathcal{D}$.

Spĺňanie formúl v ultraproduktoch možno plne charakterizovať pomocou ich boolovských pravdivostných hodnôt.

8.4.1 Łošova veta. *Nech $(\mathcal{A}_i)_{i\in I}$ je systém štruktúr a $\mathcal{D}$ je ultrafilter na množine I. Potom pre ľubovoľnú formulu $\varphi(x_1,\dots,x_n)$ a prvky $\alpha_1,\dots,\alpha_n\in\prod A_i$ platí*

$$\prod_{i\in I}\mathcal{A}_i\Big/\mathcal{D}\vDash\varphi\big(\alpha_1^{\mathcal{D}},\dots,\alpha_n^{\mathcal{D}}\big)\ \Leftrightarrow\ [\varphi(\alpha_1,\dots,\alpha_n)]\in\mathcal{D}$$

Inak povedané, n-tica prvkov $\alpha_1^{\mathcal{D}},\dots,\alpha_n^{\mathcal{D}}\in\prod A_i/\mathcal{D}$ spĺňa formulu φ v ultraprodukte $\prod_{i\in I}\mathcal{A}_i/\mathcal{D}$ práve vtedy, keď boolovská pravdivostná hodnota $[\varphi(\alpha_1,\dots,\alpha_n)]$ je „veľká“ v zmysle ultrafiltra $\mathcal{D}$, to znamená práve vtedy, keď n-tica funkcií $\alpha_1,\dots,\alpha_n\in\prod A_i$ spĺňa po zložkách formulu φ pre „veľkú“ množinu indexov $i\in I$.

Dôkaz. Dôkaz možno vykonať jednoducho indukciou podľa zložitosti formuly φ. Ak φ je atomická, tak platnosť uvedenej ekvivalencie vyplýva z definície operácií a relácií vo filtrovaných súčinoch. Predpokladajme teda, že uvedená ekvivalencia platí pre formuly $\varphi(x_1,\dots,x_n)$, $\psi(x_1,\dots,x_n)$ a ľubovoľné prvky $\alpha_1,\dots,\alpha_n\in\prod A_i$. Za tohto predpokladu overíme jej platnosť aj pre formuly $\neg\varphi$ a $\varphi\wedge\psi$.

Za uvedených predpokladov pre ľubovoľné $\alpha_1,\dots,\alpha_n\in\prod A_i$ nasledujúce podmienky sú ekvivalentné:

$$\prod\mathcal{A}_i\Big/\mathcal{D}\vDash\neg\varphi\big(\alpha_1^{\mathcal{D}},\dots,\alpha_n^{\mathcal{D}}\big)$$
$$\prod\mathcal{A}_i\Big/\mathcal{D}\nvDash\varphi\big(\alpha_1^{\mathcal{D}},\dots,\alpha_n^{\mathcal{D}}\big)$$
$$[\varphi(\alpha_1,\dots,\alpha_n)]\notin\mathcal{D}$$
$$[\neg\varphi(\alpha_1,\dots,\alpha_n)]=I\smallsetminus[\varphi(\alpha_1,\dots,\alpha_n)]\in\mathcal{D}$$

Pritom ekvivalencia podmienok v druhom a treťom riadku je zaručená indukčným predpokladom a ekvivalencia podmienok v treťom a štvrtom riadku vlastnosťami boolovskej pravdivostnej hodnoty a ultrafiltrov.

Podobne, pre ľubovoľné $\alpha_1, \dots, \alpha_n \in \prod A_i$ nasledujúce podmienky sú ekvivalentné:

$$\prod \mathcal{A}_i \Big/ \mathcal{D} \vDash (\varphi \wedge \psi)\big(\alpha_1^{\mathcal{D}}, \dots, \alpha_n^{\mathcal{D}}\big)$$
$$\prod \mathcal{A}_i \Big/ \mathcal{D} \vDash \varphi\big(\alpha_1^{\mathcal{D}}, \dots, \alpha_n^{\mathcal{D}}\big) \ \wedge \ \prod \mathcal{A}_i \Big/ \mathcal{D} \vDash \psi\big(\alpha_1^{\mathcal{D}}, \dots, \alpha_n^{\mathcal{D}}\big)$$
$$[\varphi(\alpha_1, \dots, \alpha_n)] \in \mathcal{D} \ \wedge \ [\psi(\alpha_1, \dots, \alpha_n)] \in \mathcal{D}$$
$$[(\varphi \wedge \psi)(\alpha_1, \dots, \alpha_n)] = [\varphi(\alpha_1, \dots, \alpha_n)] \cap [\psi(\alpha_1, \dots, \alpha_n)] \in \mathcal{D}$$

Pritom ekvivalencia podmienok v druhom a treťom riadku je zaručená indukčným predpokladom a ekvivalencia podmienok v treťom a štvrtom riadku vlastnosťami boolovskej pravdivostnej hodnoty a ľubovoľných filtrov.

Predpokladajme ďalej, že uvedená ekvivalencia platí pre formulu $\varphi(x, x_1, \dots, x_n)$ a ľubovoľné prvky $\alpha, \alpha_1, \dots, \alpha_n \in \prod A_i$. Za tohto predpokladu overíme jej platnosť aj pre formulu $(\exists\, x)\varphi(x, x_1, \dots, x_n)$. Za uvedených predpokladov pre ľubovoľné $\alpha_1, \dots, \alpha_n \in \prod A_i$ sú nasledujúce podmienky ekvivalentné:

$$\prod \mathcal{A}_i \Big/ \mathcal{D} \vDash (\exists\, x)\varphi\big(x, \alpha_1^{\mathcal{D}}, \dots, \alpha_n^{\mathcal{D}}\big)$$
$$\Big(\exists\, \alpha \in \prod A_i\Big)\Big(\prod \mathcal{A}_i \Big/ \mathcal{D} \vDash \varphi\big(\alpha^{\mathcal{D}}, \alpha_1^{\mathcal{D}}, \dots, \alpha_n^{\mathcal{D}}\big)\Big)$$
$$\Big(\exists\, \alpha \in \prod A_i\Big)\big([\varphi(\alpha, \alpha_1, \dots, \alpha_n)] \in \mathcal{D}\big)$$
$$[(\exists\, x)\varphi(x, \alpha_1, \dots, \alpha_n)] \in \mathcal{D}$$

Pritom ekvivalencia podmienok v druhom a treťom riadku je zaručená indukčným predpokladom a ekvivalencia podmienok v treťom a štvrtom riadku princípom maximality pre boolovskú pravdivostnú hodnotu a vlastnosťami ľubovoľných filtrov.

Všimnite si, že indukčné kroky pre konjunkciu a existenčný kvantifikátor by prešli pre ľubovoľný filter $\mathcal{D}$; podmienku, že $\mathcal{D}$ je ultrafilter, sme potrebovali iba v indukčnom kroku pre negáciu.

Bezprostredným dôsledkom Łošovej vety je fakt, že ultraprodukt modelov ľubovoľnej teórie prvého rádu je sám modelom tejto teórie.

8.4.2 Dôsledok. *Nech T je teória prvého rádu, $\mathcal{D}$ je ultrafilter na množine I a $(\mathcal{A}_i)_{i\in I}$ je systém štruktúr taký, že $\mathcal{A}_i \vDash T$ pre každé $i \in I$. Potom tiež*

$$\prod_{i\in I} \mathcal{A}_i \Big/ \mathcal{D} \vDash T$$

8.4.3 Dôsledok. *Nech $\mathcal{A}$ je štruktúra prvého rádu a $\mathcal{D}$ je ultrafilter na množine I. Potom diagonálne zobrazenie $a \mapsto \overline{a}^{\mathcal{D}}$ je elementárnym vnorením $\mathcal{A} \xrightarrow{\prec} \mathcal{A}^I/\mathcal{D}$ štruktúry $\mathcal{A}$ do jej ultramocniny $\mathcal{A}^I/\mathcal{D}$.*

Dôkaz. Stačí overiť, že pre ľubovoľnú formulu $\varphi(x_1, \dots, x_n)$ a prvky $a_1, \dots, a_n \in A$ z podmienky $\mathcal{A} \vDash \varphi(a_1, \dots, a_n)$ vyplýva, že $\mathcal{A}^I/\mathcal{D} \vDash \varphi\big(\overline{a}_1^{\mathcal{D}}, \dots, \overline{a}_n^{\mathcal{D}}\big)$. Za uvedeného predpokladu však platí $[\varphi(\overline{a}_1, \dots, \overline{a}_n)] = I \in \mathcal{D}$, teda požadovaný záver vyplýva z Łošovej vety.

8.4.4 Úloha. Nech $\mathcal{A} = (A; \dots)$ je štruktúra nekonečnej mohutnosti $|A| = \alpha$ takej, že $\alpha^{\aleph_0} = \alpha$ (túto podmienku spĺňa napr. mohutnosť kontinua $\alpha = 2^{\aleph_0}$). Nech ďalej I je nekonečná spočítateľná množina (napr. $I = \mathbb{N}$) a $\mathcal{D}$ je nehlavný ultrafilter na I. Dokážte, že ultramocnina $\mathcal{A}^I/\mathcal{D}$ je vlastným elementárnym rozšírením štruktúry $\mathcal{A}$ rovnakej mohutnosti $\left|A^I/\mathcal{D}\right| = \alpha$.

8.5 Neštandardná analýza

Konštrukcia ultramocniny umožňuje rozšíriť obor reálnych čísel do číselného systému, ktorý obsahuje „nekonečne malé“ aj „nekonečne veľké“ veličiny a využiť ich pri budovaní infinitezimálneho, t. j. diferenciálneho a integrálneho počtu v poňatí blízkom jeho historicky pôvodnej podobe, akú mu vtlačili jeho zakladatelia Isaac Newton a Gottfried Wilhelm Leibniz. Matematická disciplína, ktorá s využitím metód matematickej logiky a teórie modelov skúma rôzne klasické matematické štruktúry pomocou ich elementárnych rozšírení, kde sú obohatené o rôzne typy ideálnych prvkov, sa nazýva *neštandardná analýza*. Jej základy položil v 60. rokoch 20. storočia Abraham Robinson. „Neštandardné metódy“ sa v súčasnosti používajú v rôznych oblastiach matematiky, napr. v teórii miery a pravdepodobnosti, v topológii, funkcionálnej analýze, v ergodickej teórii, dynamických systémoch atď., takže rehabilitáciou pôvodného infinitezimálneho počtu sa význam neštandardnej analýzy ani zďaleka nevyčerpáva. V tejto krátkej ukážke však naznačíme iba niekoľko jej základnych myšlienok, týkajúcich sa práve infinitezimálneho počtu reálnych funkcií jednej reálnej premennej.

Kvôli konkrétnosti si za indexovú množinu I zvolíme množinu všetkých kladných celých čísel, teda $I = \{1, 2, 3, \dots\}$; jej úlohu by však mohla zohrať ľubovoľná nekonečná množina. Ďalej nech $\mathcal{D}$ je ľubovoľný nehlavný ultrafilter na množine I; to znamená, že platí $\mathcal{F}(I) \subseteq \mathcal{D}$. Pre ľubovoľnú štruktúru $\mathcal{A}$ akéhokoľvek jazyka prvého rádu L budeme jej ultramocninu $\mathcal{A}^I/\mathcal{D}$ značiť ${}^*\mathcal{A}$. Špeciálne pre množinu A kladieme ${}^*A = A^I/\mathcal{D}$ a každý prvok $a \in A$ stotožníme s jeho obrazom $\overline{a}^{\mathcal{D}}$ v diagonálnom vnorení $A \to {}^*A$.

Množinu ${}^*\mathbb{R} = \mathbb{R}^I/\mathcal{D}$ nazývame množinou všetkých *hyperreálnych čísel*. Podobne možno zaviesť *hyperprirodzené, hypercelé, hyperracionálne* či *hyperkomplexné čísla*. Dohodneme sa, že $L = (F, R, \nu)$ je jazyk prvého rádu, ktorého špecifické symboly zahŕňajú typické znaky pre operácie sčítania $+$ a násobenia $\cdot$, konštanty 0 a 1, relácie usporiadania $<$ aj $\leq$, ako aj obvyklé znaky pre všetky funkcie, operácie, konštanty a relácie bežne používané v matematickej analýze, napr. funkcie absolútna hodnota $|x|$, exponenciála e^x, sínus $\sin x$, kosínus $\cos x$, operácie delenia x/y, umocňovania x^y, konštanty π, e, jednomiestne predikáty $\mathbb{Z}(x)$ „byť celým číslom“, $\mathbb{Q}(x)$ „byť racionálnym číslom“, $\mathbb{R}^+(x)$ „byť kladným (reálnym) číslom“ a pod. Potom $\mathcal{R}$ označuje L-štruktúru so základnou množinou $\mathbb{R}$, v ktorej sú všetky špecifické symboly jazyka L interpretované prirodzeným (t. j. štandardným) spôsobom. Ultramocninu

$$ {}^*\mathcal{R} = \mathcal{R}^I/\mathcal{D} $$

nazývame *neštandardným rozšírením* štruktúry $\mathcal{R}$. Kým interepretácie špecifických symbolov jazyka L v štruktúre $\mathcal{R}$ budeme značiť príslušným symbolom samotným, interpretáciu symbola s v štruktúre ${}^*\mathcal{R}$ budeme značiť ${}^*s$. Keď nehrozí nedorozumenie,

budeme najmä pri symboloch s ustáleným významom, ako napr. $+$, $\cdot$, 0, 1, π, e, $|x|$, $\sin x$, $\cos x$, $<$ a pod., túto hviezdičku vynechávať. O každej funkcii $f\colon P \to \mathbb{R}$, ktorú hodláme študovať, budeme predpokladať, že f aj jej definičný obor $P \subseteq \mathbb{R}$ „majú mená“ vyjadrené špecifickými symbolmi, či aspoň termami alebo formulami jazyka L. Takejto funkcii potom zodpovedá funkcia ${}^*f\colon {}^*P \to {}^*\mathbb{R}$, ktorá spĺňa podmienky $P \subseteq {}^*P \subseteq {}^*\mathbb{R}$ a ${}^*f(x) = f(x)$ pre $x \in P$. Keďže $\mathcal{R} \prec {}^*\mathcal{R}$, ${}^*f$ má v istom dobre definovanom zmysle „rovnaké vlastnosti“ ako pôvodná funkcia f.

Zúžením štruktúr $\mathcal{R}$ a ${}^*\mathcal{R}$ do jazyka so špecifickými symbolmi $+$, $\cdot$, 0, 1 a $<$ dostávame usporiadané polia $\mathcal{R}_0 = (\mathbb{R}; +, \cdot, 0, 1, <)$ a ${}^*\mathcal{R}_0 = ({}^*\mathbb{R}; +, \cdot, 0, 1, <)$, pričom stále platí $\mathcal{R}_0 \prec {}^*\mathcal{R}_0$. Usporiadané pole ${}^*\mathcal{R}_0$ však obsahuje „nekonečne veľké“ a „nekonečne malé“ čísla (veličiny). Hovoríme, že hyperreálne číslo $x \in {}^*\mathbb{R}$ je *konečne veľké*, prípadne tiež *ohraničené* alebo len *konečné*, ak existuje kladné reálne číslo $r \in \mathbb{R}$ také, že $|x| < r$. V opačnom prípade hovoríme, že x je *nekonečne veľké*, prípadne tiež *neohraničené* alebo len *nekonečné* hyperreálne číslo. Hovoríme, že hyperreálne číslo $x \in {}^*\mathbb{R}$ je *nekonečne malé* alebo tiež *infinitezimálne*, ak pre každé kladné reálne číslo $r \in \mathbb{R}$ platí $|x| < r$. Ľahko možno nahliadnuť, že množina

$$\mathbb{F}^*\mathbb{R} = \bigl\{x \in {}^*\mathbb{R}\colon (\exists\, r \in \mathbb{R}^+)(|x| < r)\bigr\}$$

všetkých konečných hyperreálnych čísel tvorí *konvexný podokruh*[6] usporiadaného poľa ${}^*\mathcal{R}_0$. Množina

$$\mathbb{I}^*\mathbb{R} = \bigl\{x \in {}^*\mathbb{R}\colon (\forall\, r \in \mathbb{R}^+)(|x| < r)\bigr\}$$

všetkých nekonečne malých hyperreálnych čísel tvorí *konvexný ideál* usporiadaného okruhu $(\mathbb{F}^*\mathbb{R}; +, \cdot, 0, 1, <)$.

Čitateľ by si mal samostatne rozmyslieť, že pre postupnosť $\alpha = (1, 2, 3, \dots) \in \mathbb{R}^I$, t. j. $\alpha(i) = i$ pre $i \in I$, platí $\alpha^{\mathcal{D}} \in {}^*\mathbb{R} \setminus \mathbb{F}^*\mathbb{R}$, to znamená, že $\alpha^{\mathcal{D}}$ je kladné nekonečne veľké hyperreálne číslo. Na druhej strane, pre postupnosť $\beta = (1, 1/2, 1/3, \dots) \in \mathbb{R}^I$, t. j. $\beta(i) = 1/i$ pre $i \in I$, platí $0 \neq \beta^{\mathcal{D}} \in \mathbb{I}^*\mathbb{R}$, teda $\beta^{\mathcal{D}}$ je kladné nekonečne malé hyperreálne číslo. Vo všeobecnosti platí, že hyperreálne číslo x je nekonečne veľké práve vtedy, keď jeho prevrátená hodnota $1/x$ je nekonečne malá.

Keďže množina $\mathbb{I}^*\mathbb{R}$ nekonečne malých čísel tvorí zároveň podgrupu abelovskej grupy $({}^*\mathbb{R}; +, 0)$, vzťahom

$$x \approx y \;\Leftrightarrow\; x - y \in \mathbb{I}^*\mathbb{R}$$

je definovaná relácia ekvivalencie na množine ${}^*\mathbb{R}$ nazývaná *reláciou* alebo *ekvivalenciou nekonečnej blízkosti* prípadne *ekvivalenciou nerozlíšiteľnosti*. Množinu

$$\mu(x) = x + \mathbb{I}^*\mathbb{R} = \{y \in {}^*\mathbb{R}\colon y \approx x\}$$

všetkých hyperreálnych čísel nekonečne blízkych k číslu (bodu) $x \in {}^*\mathbb{R}$ nazývame zhodne s Leibnizom *monádou* čísla (bodu) x. Zrejme $\mu(0) = \mathbb{I}^*\mathbb{R}$ a každá monáda $\mu(x)$ je konvexná podmnožina množiny ${}^*\mathbb{R}$.

Ku každému *konečnému* hyperreálnemu číslu x existuje práve jedno (štandardné) reálne číslo r také, že $x \approx r$; toto reálne číslo nazývame *štandardnou časťou* alebo *tieňom* čísla x a značíme ho

$$r = \operatorname{st} x = {}^\circ x$$

[6] Podmnožinu X čiastočne usporiadanej množiny $(A; <)$ nazývame *konvexnou*, ak pre ľubovoľné $x, y, z \in A$ platí $(x, z \in X \wedge x < y < z) \Rightarrow y \in X$.

Pre čitateľa s istými vedomosťami z topológie dodávame, že pre $x \in \mathbb{F}^*\mathbb{R}$ určené postupnosťou $\xi \in \mathbb{R}^I$, t. j. $x = \xi^{\mathcal{D}}$, platí $^\circ x = r$ práve vtedy, keď postupnosť ξ konverguje k bodu r *podľa ultrafiltra* $\mathcal{D}$.[7] Z toho vyplýva, že konvergencia

$$\lim_{i\to\infty} \xi(i) = r$$

v „bežnom“ význame (t. j. podľa Fréchetovho filtra $\mathcal{F}(I)$) je postačujúcou (nie však nutnou) podmienkou pre rovnosť $^\circ x = r$.

Z našich úvah vyplýva, že faktorová množina $\mathbb{F}^*\mathbb{R}/\mathbb{I}^*\mathbb{R} = \mathbb{F}^*\mathbb{R}/{\approx}$ je tvorená monádami $\mu(x)$ ohraničených hyperreálnych čísel $x \in \mathbb{F}^*\mathbb{R}$. Faktorizáciou usporiadaného okruhu $(\mathbb{F}^*\mathbb{R}; +, \cdot, 0, 1, <)$ podľa jeho konvexného ideálu $\mathbb{I}^*\mathbb{R}$ tak opäť dostaneme usporiadaný okruh $(\mathbb{F}^*\mathbb{R}/\mathbb{I}^*\mathbb{R}; +, \cdot, 0, 1, <)$. Špeciálne pre usporiadanie v tomto okruhu platí

$$\mu(x) < \mu(y) \;\Leftrightarrow\; (x < y \wedge x \not\approx y)$$
$$\mu(x) \leq \mu(y) \;\Leftrightarrow\; (x < y \vee x \approx y)$$

Navyše priradením $\mu(x) \mapsto \operatorname{st} x$ je korektne definovaný izomorfizmus usporiadaných okruhov $(\mathbb{F}^*\mathbb{R}/\mathbb{I}^*\mathbb{R}; +, \cdot, 0, 1, <) \cong (\mathbb{R}; +, \cdot, 0, 1, <)$, z ktorého okrem iného vyplýva, že $(\mathbb{F}^*\mathbb{R}/\mathbb{I}^*\mathbb{R}; +, \cdot, 0, 1, <)$ je usporiadané pole.

8.5.1 Úloha. Podobne možno zaviesť aj množiny všetkých konečných hyperracionálnych čísel $\mathbb{F}^*\mathbb{Q}$ a nekonečne malých hyperracionálnych čísel $\mathbb{I}^*\mathbb{Q}$ a vytvoriť faktorový usporiadaný okruh $(\mathbb{F}^*\mathbb{Q}/\mathbb{I}^*\mathbb{Q}; +, \cdot, 0, 1, <)$. Samostatne si premyslite, ktorá z dvoch možností

$$(\mathbb{F}^*\mathbb{Q}/\mathbb{I}^*\mathbb{Q}; +, \cdot, 0, 1, <) \cong (\mathbb{Q}; +, \cdot, 0, 1, <)$$

resp.

$$(\mathbb{F}^*\mathbb{Q}/\mathbb{I}^*\mathbb{Q}; +, \cdot, 0, 1, <) \cong (\mathbb{R}; +, \cdot, 0, 1, <)$$

skutočne nastáva, a zdôvodnite prečo.

Skutočnosť, že usporiadané polia $\mathcal{R}_0 = (\mathbb{R}; +, \cdot, 0, 1, <)$ a ${}^*\mathcal{R}_0 = ({}^*\mathbb{R}; +, \cdot, 0, 1, <)$ sú elementárne ekvivalentné, ktorá vyplýva z elementárnej inklúzie $\mathcal{R}_0 \prec {}^*\mathcal{R}$, znamená len toľko, že $\mathcal{R}_0$ a ${}^*\mathcal{R}_0$ majú rovnaké vlastnosti vyjadriteľné v jazyku usporiadaných polí. Pokiaľ však ide o iné vlastnosti, môžu sa výrazne líšiť. Napr. v $\mathcal{R}_0$ platí veta o supreme, teda každá zhora ohraničená množina $X \subseteq \mathbb{R}$ má supremum v $\mathbb{R}$. Na druhej strane, množiny $\mathbb{I}^*\mathbb{R} \subseteq {}^*\mathbb{R}$, $\mathbb{F}^*\mathbb{R} \subseteq {}^*\mathbb{R}$ sú obe ohraničené v ${}^*\mathbb{R}$ (prvá ľubovoľným kladným číslom $r \in \mathbb{R}$, druhá ľubovoľným nekonečným kladným číslom $z \in {}^*\mathbb{R}$). Ľahko sa však možno presvedčiť, že ani jedna z nich nemá v ${}^*\mathbb{R}$ supremum. Z faktu, že štruktúra ${}^*\mathcal{R}_0$ je elementárnym rozšírením štruktúry $\mathcal{R}_0$ vyplýva existencia suprema len pre všetky zhora ohraničené množinu tvaru $X = \{x \in {}^*\mathbb{R} \colon \varphi(x, a_1, \ldots, a_n)\}$, kde $\varphi(x, x_1, \ldots, x_n)$ je formula v jazyku usporiadaných polí a $a_1, \ldots, a_n \in {}^*\mathbb{R}$. V dôsledku toho vidíme, že množiny $\mathbb{I}^*\mathbb{R}$, $\mathbb{F}^*\mathbb{R}$ sa v takomto tvare vyjadriť nedajú. Podobné úvahy sa vzťahujú aj na bohatší jazyk L a L-štruktúry $\mathcal{R} \prec {}^*\mathcal{R}$.

Nasledujúce tri vety, ktoré uvádzame bez dôkazov, charakterizujú tri základné pojmy matematickej analýzy (spojitosť, deriváciu a určitý integrál) pomocou nekonečne

[7] Postupnosť $\alpha \colon I \to \mathbb{R}$ konverguje k reálnemu číslu a podľa filtra $\mathcal{D}$ na množine I, ak pre každé reálne číslo $\varepsilon > 0$ existuje množina $X \in \mathcal{D}$ taká, že $|\alpha(k) - a| < \varepsilon$ pre každé $k \in X$.

malých a nekonečne veľkých veličín. Zároveň ich však možno chápať ako *definície* uvedených pojmov. V tom prípade by sa však opäť patrilo dokázať, že zodpovedajúce štandardné definície týchto pojmov sú s nimi ekvivalentné. Ponechávame na osobné posúdenie čitateľa, či považuje za intuitívne názornejšie štandardné alebo neštandardné formulácie.

8.5.2 Veta. *Nech $P \subseteq \mathbb{R}$ a $f\colon P \to \mathbb{R}$ je ľubovoľná funkcia pomenovaná v jazyku L. Potom*

(a) *f je spojitá v bode $a \in P$ práve vtedy, keď pre všetky $x \in {}^*P$ platí $x \approx a \Rightarrow {}^*f(x) \approx f(a)$;*

(b) *f je spojitá na množine P práve vtedy, keď pre všetky $a \in P$, $x \in {}^*P$ platí $x \approx a \Rightarrow {}^*f(x) \approx f(a)$;*

(c) *f je rovnomerne spojitá na množine P práve vtedy, keď pre všetky $x, y \in {}^*P$ platí $x \approx y \Rightarrow {}^*f(x) \approx {}^*f(y)$.*

Pripomíname, že bod $a \in P$ množiny $P \subseteq \mathbb{R}$ nazývame jej *vnútorným bodom*, ak existuje kladné číslo $\varepsilon \in \mathbb{R}$ také, že $(a - \varepsilon, a + \varepsilon) \subseteq P$. Možno dokázať, že $a \in P$ je vnútorným bodom tejto množiny práve vtedy, keď $\mu(a) \subseteq {}^*P$.

8.5.3 Veta. *Nech $P \subseteq \mathbb{R}$ a $f\colon P \to \mathbb{R}$ je ľubovoľná funkcia pomenovaná v jazyku L a $a \in P$ je vnútorný bod množiny P. Potom funkcia f má v bode a konečnú deriváciu práve vtedy, keď existuje reálne číslo r také, že pre každé nekonečné malé číslo $d \neq 0$ platí*

$$\frac{{}^*f(a+d) - f(a)}{d} \approx r$$

V takom prípade píšeme

$$f'(a) = \frac{\mathrm{d}f(a)}{\mathrm{d}x} = r = \mathrm{st}\left(\frac{{}^*f(a+d) - f(a)}{d}\right)$$

a toto číslo nazývame *deriváciou funkcie f v bode a*.

Riemannovský určitý integrál možno definovať pomocou „nekonečných integrálnych súčtov“ zodpovedajúcich *infinitezimálnym deleniam* daného intervalu. Rigorózne zavedenie takýchto súčtov by si vyžiadalo ešte niekoľko jemnejších úvah navyše, ktoré si tentokrát odpustíme. Prvotné predstavy, na ktorých spočívajú nasledujúce pojmy a na nich založená konštrukcia, sú však do značnej miery intuitívne jasné. Stačí, ak poznamenáme, že množinu, resp. postupnosť nazývame *hyperkonečnou*, ak jej možno zmysluplne priradiť nejaké hyperprirodzené číslo $n \in {}^*\mathbb{N}$ ako počet jej prvkov, resp. členov. Pritom ak $n \in {}^*\mathbb{N} \setminus \mathbb{N}$, tak táto množina, resp. postupnosť je v štandardnom zmysle nekonečná. Čísla tvoriace hyperkonečnú postupnosť $(c_1, \ldots, c_n) \in {}^*\mathbb{R}^n$ možno navyše sčítať a s ich súčtom $\sum_{i=1}^{n} c_n$ možno narábať v istom dobre definovateľnom zmysle rovnako ako s konečnými súčtami.

Nech $a < b$ sú (štandardné) reálne čísla. *Delením intervalu* $[a, b]$ nazývame hyperkonečnú postupnosť $(c_0, c_1, \ldots, c_n)$, kde $n \in {}^*\mathbb{N}$, takú, že $a = c_0 < c_1 < \ldots < c_n = b$. Hovoríme, že $(c_0, c_1, \ldots, c_n)$ je *infinitezimálne delenie* intervalu $[a, b]$, ak $c_{k-1} \approx c_k$ pre každé $1 \leq k \leq n$. Zrejme ak $(c_0, c_1, \ldots, c_n)$ je infinitezimálne delenie intervalu

$[a,b]$, tak $n \in {}^*\mathbb{N} \setminus \mathbb{N}$, čiže n je nekonečne veľké hyperprirodzené číslo. *Integrálnym súčtom* prislúchajúcim k deleniu $(c_0, c_1, \ldots, c_n)$ nazývame každý súčet tvaru

$$\sum_{k=1}^{n} {}^*f(x_k)(c_k - c_{k-1})$$

kde $(x_1, \ldots, x_n)$ je hyperkonečná postupnosť vybraných bodov $x_k \in [c_{k-1}, c_k]$ z jednotlivých dielčích intervalov $[c_{k-1}, c_k] \subseteq [a,b]$.

8.5.4 Veta. *Nech $a < b$ sú reálne čísla a $f\colon [a,b] \to \mathbb{R}$ je ľubovoľná funkcia pomenovaná v jazyku L. Potom funkcia f je riemannovsky integrovateľná na intervale $[a,b]$ práve vtedy, keď existuje reálne číslo S také, že pre všetky infinitezimálne delenia $(c_0, c_1, \ldots, c_n)$ intervalu $[a,b]$ a vybrané body $x_k \in [c_{k-1}, c_k]$ pre $1 \le k \le n$ platí*

$$\sum_{k=1}^{n} {}^*f(x_k)(c_k - c_{k-1}) \approx S$$

V takom prípade píšeme

$$\int_a^b f(x)\,\mathrm{d}x = S = \mathrm{st}\left(\sum_{k=1}^{n} {}^*f(x_k)(c_k - c_{k-1})\right)$$

a toto číslo nazývame *určitým integrálom funkcie f na intervale $[a,b]$*. Špeciálne ak $n \in {}^*\mathbb{N} \setminus \mathbb{N}$, $d = (b-a)/n \approx 0$ a $c_k = a + kd$ pre $0 \le k \le n$, tak $(c_0, c_1, \ldots, c_n)$ je *rovnomerné* infinitezimálne delenie intervalu $[a,b]$. V tom prípade pre riemannovsky integrovateľnú funkciu $f\colon [a,b] \to \mathbb{R}$ a ľubovoľný výber bodov $x_k \in [c_{k-1}, c_k]$ platí

$$\int_a^b f(x)\,\mathrm{d}x = S = \mathrm{st}\left(\sum_{k=1}^{n} {}^*f(x_k)\,d\right) = (b-a)\,\mathrm{st}\left(\frac{1}{n}\sum_{k=1}^{n} {}^*f(x_k)\right)$$

čiže štandardná časť aritmetického priemeru $\frac{1}{n}\sum_{k=1}^{n} {}^*f(x_k)$ predstavuje *strednú hodnotu* funkcie f na intervale $[a,b]$.

Na záver ešte poznamenajme, čo si niektorí pozorní čitatelia všimli možno aj sami. Skutočnosť, že sme štruktúru ${}^*\mathcal{R}$ nad množinou hyperreálnych čísel ${}^*\mathbb{R}$ zostrojili ako ultramocninu ${}^*\mathcal{R} = \mathcal{R}^I/\mathcal{D}$ štruktúry $\mathcal{R}$ nad množinou reálnych čísel $\mathbb{R}$, nehrala totiž v našich úvahách nijako dôležitú úlohu. Dôležitý bol iba fakt, že štruktúra ${}^*\mathcal{R}$ je elementárnym rozšírením štruktúry $\mathcal{R}$, a intuícia a názorné predstavy spojené s pojmami nekonečne malých a nekonečne veľkých čísel. Konštrukcia ultramocniny im poskytla iba akúsi počiatočnú oporu tým, že ich tak povediac „zlegalizovala“ v rámci univerza množín, ktoré sme si zvykli považovať za svet prakticky celej súčasnej matematiky.

8.6 Veta o kompaktnosti v jazyku ultraproduktov

Náš pôvodný dôkaz Vety 4.9.1 o kompaktnosti vychádzal z Vety 4.8.6 o úplnosti a bol nekonštruktívny v tom zmysle, že nedával žiadny návod, ako možno z modelov

konečných podteórií danej teórie prvého rádu T zostrojiť model samotnej teórie T. Nasledujúca veta nám poskytuje istú predstavu o takejto konštrukcii. Treba si však uvedomiť, že nehlavné ultrafiltre nevieme explicitne popísať a axiómy teórie množín nám zaručujú iba ich existenciu, preto „konštruktívnosť“ dôkazu nasledujúcej vety zostáva aj naďalej značne iluzórna.

8.6.1 Veta o kompaktnosti. *Nech Σ je množina sentencií jazyka L uzavretá vzhľadom na konečné konjunkcie a pre každé $\sigma \in \Sigma$ nech $\mathcal{A}_\sigma$ je štruktúra jazyka L taká, že $\mathcal{A}_\sigma \vDash \sigma$. Potom existuje ultrafilter $\mathcal{D}$ na množine Σ taký, že*

$$\prod_{\sigma\in\Sigma} \mathcal{A}_\sigma \Big/ \mathcal{D} \vDash \Sigma$$

Dôkaz. Pre každé $\sigma \in \Sigma$ označíme $J_\sigma = \{\varrho \in \Sigma \colon \mathcal{A}_\varrho \vDash \sigma\}$. Množina $J_{\sigma_1} \cap \ldots \cap J_{\sigma_n}$ zrejme obsahuje formulu $\sigma_1 \wedge \ldots \wedge \sigma_n$, takže $\{J_\sigma \colon \sigma \in \Sigma\}$ je centrovaný systém podmnožín množiny Σ. Preto existuje ultrafilter $\mathcal{D}$ na Σ taký, že $J_\sigma \in \mathcal{D}$ pre každé $\sigma \in \Sigma$. Dokážeme, že

$$\prod_{\varrho\in\Sigma} \mathcal{A}_\varrho \Big/ \mathcal{D} \vDash \sigma$$

pre ľubovoľné $\sigma \in \Sigma$. Stačí si uvedomiť, že

$$[\sigma] = \{\varrho \in \Sigma \colon \mathcal{A}_\varrho \vDash \sigma\} = J_\sigma \in \mathcal{D}$$

Požadovaný záver vyplýva z Łošovej vety 8.4.1.

8.7 Elementárna ekvivalencia a ultramocniny

Práve dokázaná verzia Vety o kompaktnosti umožňuje charakterizovať vzťah elementárnej ekvivalencie štruktúr prostredníctvom elementárnej vnoriteľnosti jednej z nich do ultramocniny druhej z nich.

8.7.1 Veta. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry jazyka L. Potom $\mathcal{A} \equiv \mathcal{B}$ práve vtedy keď existuje ultramocnina $\mathcal{A}^I/\mathcal{D}$ štruktúry $\mathcal{A}$ a elementárne vnorenie $h \colon \mathcal{B} \xrightarrow{\prec} \mathcal{A}^I/\mathcal{D}$.*

Dôkaz. Nech $\mathcal{A} \equiv \mathcal{B}$. Položme $\Sigma = \mathrm{Th}(\mathcal{B}_B)$. Zrejme Σ je množina sentencií jazyka L_B uzavretá na konečné konjunkcie. Ľubovoľné $\sigma \in \Sigma$ má tvar $\varphi(b_1, \ldots, b_n)$ pre vhodnú formulu $\varphi(x_1, \ldots, x_n)$ jazyka L a $b_1, \ldots, b_n \in B$. Potom $\mathcal{B} \vDash \varphi(b_1, \ldots, b_n)$, a keďže $\mathcal{A} \equiv \mathcal{B}$, tak aj

$$\mathcal{A} \vDash (\exists\, x_1, \ldots, x_n)\varphi(x_1, \ldots, x_n)$$

Nech $g_\sigma \colon B \to A$ je zobrazenie také, že pre štruktúru $\mathcal{A}_\sigma = \big(\mathcal{A}, g_\sigma(b)\big)_{b\in B}$ jazyka L_B platí

$$\mathcal{A} \vDash \varphi\big(g_\sigma(b_1), \ldots, g_\sigma(b_n)\big)$$

t. j. $\mathcal{A}_\sigma \vDash \sigma$. Podľa Vety 8.6.1 o kompaktnosti existuje ultrafilter $\mathcal{D}$ na Σ taký, že

$$\prod_{\sigma\in\Sigma} \mathcal{A}_\sigma \Big/ \mathcal{D} \vDash \Sigma$$

Potom zúženie tohto ultraproduktu do jazyka L je ultramocnina $\mathcal{A}^\Sigma/\mathcal{D}$ a zobrazenie $h\colon B \to A^\Sigma/\mathcal{D}$, dané predpisom $h(b)(\sigma) = g_\sigma(b)$ pre $b \in B$, $\sigma \in \Sigma$, je elementárnym vnorením $\mathcal{B} \xrightarrow{\prec} \mathcal{A}^\Sigma/\mathcal{D}$.

Obrátená implikácia je triviálna.

Poznamenajme, že prostriedkami presahujúcimi rámec nášho kurzu možno dokázať aj podstatne silnejší výsledok.

8.7.2 Keislerova-Shelahova veta. *Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry prvého rádu. Potom $\mathcal{A} \equiv \mathcal{B}$ práve vtedy keď existuje množina I a ultrafilter $\mathcal{D}$ na I také, že $\mathcal{A}^I/\mathcal{D} \cong \mathcal{B}^I/\mathcal{D}$.*

8.8 Charakterizácia axiomatických a konečne axiomatizovateľných tried

Triedu všetkých štruktúr jazyka L označujeme $\mathrm{Mod}(L)$. Ak T je teória v jazyku L, tak triedu všetkých jej modelov označujeme $\mathrm{Mod}(T)$, teda

$$\mathrm{Mod}(T) = \{\mathcal{A} \in \mathrm{Mod}(L)\colon \mathcal{A} \vDash T\}$$

Hovoríme, že trieda $\mathbf{K} \subseteq \mathrm{Mod}(L)$ štruktúr jazyka L je *axiomatická trieda*, ak existuje teória T v jazyku L taká, že $\mathbf{K} = \mathrm{Mod}(T)$. Hovoríme, že trieda $\mathbf{K}$ štruktúr jazyka L je *konečne axiomatizovateľná*, ak existuje konečná teória v jazyku L taká, že $\mathbf{K} = \mathrm{Mod}(T)$.

Teóriou triedy $\mathbf{K} \subseteq \mathrm{Mod}(L)$ nazývame množinu $\mathrm{Th}(\mathbf{K})$ všetkých uzavretých formúl jazyka L splnených v každej štruktúre $\mathcal{A} \in \mathbf{K}$, teda

$$\mathrm{Th}(\mathbf{K}) = \big\{\varphi \in \mathrm{Form}(L)\colon \varphi \text{ je uzavretá a } (\forall\, \mathcal{A} \in \mathbf{K})(\mathcal{A} \vDash \varphi)\big\}$$

Nasledujúce dve vety charakterizujú axiomatické a konečne axiomatizovateľné triedy v termínoch ich uzavretosti vzhľadom na vzťahy izomorfizmu, elementárnej ekvivalencie, resp. elementárnej podštruktúry a konštrukciu ultraproduktu.

8.8.1 Veta. *Nech $\mathbf{K}$ je ľubovoľná trieda štruktúr jazyka L. Nasledujúce podmienky sú ekvivalentné:*

(i) $\mathbf{K}$ *je axiomatická trieda.*

(ii) $\mathbf{K}$ *je uzavretá vzhľadom na izomorfizmus, elementárne podštruktúry a ultraprodukty.*

(iii) $\mathbf{K}$ *je uzavretá vzhľadom na elementárnu ekvivalenciu a ultraprodukty.*

Dôkaz. (i) $\Rightarrow$ (ii) je triválne, (ii) $\Rightarrow$ (iii) vyplýva z predchádzajúcej Vety 8.7.1. Zostáva dokázať jedine (iii) $\Rightarrow$ (i).

Nech $\mathbf{K}$ je uzavretá vzhľadom na elementárnu ekvivalenciu a ultraprodukty. Položme $T = \mathrm{Th}(\mathbf{K})$. Zrejme $\mathbf{K} \subseteq \mathrm{Mod}(T)$. Dokážeme obrátenú inklúziu. Nech $\mathcal{B} \in \mathrm{Mod}(T)$. Potom $\Sigma = \mathrm{Th}(\mathcal{B})$ je množina uzavretých formúl jazyka L uzavretá na konečné konjunkcie. Taktiež pre každé $\sigma \in \Sigma$ existuje $\mathcal{A}_\sigma \in \mathbf{K}$ také, že $\mathcal{A}_\sigma \vDash \sigma$. V opačnom prípade by totiž platilo $\neg\sigma \in T$, a preto $\mathcal{B} \vDash \neg\sigma$. Podľa Vety 8.6.1 o kompaktnosti potom existuje ultrafilter $\mathcal{D}$ na množine Σ taký, že $\prod_{\sigma\in\Sigma} \mathcal{A}_\sigma/\mathcal{D} \vDash \Sigma$, teda $\prod \mathcal{A}_\sigma/\mathcal{D} \equiv \mathcal{B}$. Preto $\mathcal{B} \in \mathbf{K}$.

8.8.2 Veta. *Nech* $\mathbf{K}$ *je ľubovoľná trieda štruktúr jazyka* L*. Nasledujúce podmienky sú ekvivalentné:*

(i) $\mathbf{K}$ *je konečne axiomatizovateľná trieda.*

(ii) $\mathbf{K}$ *aj* $\mathrm{Mod}(L) \setminus \mathbf{K}$ *sú axiomatické triedy.*

(iii) $\mathbf{K}$ *je axiomatická trieda a trieda* $\mathrm{Mod}(L) \setminus \mathbf{K}$ *je uzavretá vzhľadom na ultraprodukty.*

Dôkaz. (i) $\Rightarrow$ (ii) je takmer očividná. Ak je totiž $\mathbf{K}$ konečne axiomatizovateľná trieda, tak existuje uzavretá L-formula σ (univerzálny uzáver konjunkcie všetkých axióm definujúcich triedu $\mathbf{K}$) taká, že $\mathbf{K} = \mathrm{Mod}(\sigma)$. Potom pre doplnok $\mathbf{K}' = \mathrm{Mod}(L) \setminus \mathbf{K}$ triedy $\mathbf{K}$ v triede všetkých L-štruktúr platí $\mathbf{K}' = \mathrm{Mod}(\neg\sigma)$, čiže aj $\mathbf{K}'$ je konečne axiomatizovateľná trieda.

Nakoľko (ii) $\Rightarrow$ (iii) je triviálne, dokážeme už len (iii) $\Rightarrow$ (i). Označme $\Sigma = \mathrm{Th}(\mathbf{K})$. Zrejme Σ je množina sentenecií jazyka L uzavretá na konečné konjunkcie. Keďže $\mathbf{K}$ je axiomatická trieda, platí $\mathbf{K} = \mathrm{Mod}(\Sigma)$. Dokážeme, že existuje $\sigma \in \Sigma$ také, že $\mathbf{K} = \mathrm{Mod}(\sigma)$. V opačnom prípade by pre každé $\sigma \in \Sigma$ existovala štruktúra $\mathcal{A}_\sigma \in \mathbf{K}'$ taká, že $\mathcal{A}_\sigma \models \sigma$. Podľa Vety 8.6.1 o kompaktnosti existuje ultrafilter $\mathcal{D}$ na množine Σ taký, že $\prod_{\sigma\in\Sigma} \mathcal{A}_\sigma/\mathcal{D} \models \Sigma$, čiže $\prod \mathcal{A}_\sigma/\mathcal{D} \in \mathbf{K}$. Nakoľko trieda $\mathbf{K}'$ je uzavretá na ultraprodukty, zároveň platí $\prod \mathcal{A}_\sigma/\mathcal{D} \in \mathbf{K}'$, čo je spor.

8.8.3 Úloha. Nech S, T sú teórie (ktorých axiómy sú uzavreté formuly) v jazyku L a $\mathbf{J}$, $\mathbf{K}$ sú triedy L-štruktúr.

(a) Dokážte nasledujúce vzťahy:

$$S \subseteq T \;\Rightarrow\; \mathrm{Mod}(T) \subseteq \mathrm{Mod}(S) \qquad T \subseteq \mathrm{Th}(\mathrm{Mod}\, T)$$
$$\mathbf{J} \subseteq \mathbf{K} \;\Rightarrow\; \mathrm{Th}(\mathbf{K}) \subseteq \mathrm{Th}(\mathbf{J}) \qquad \mathbf{K} \subseteq \mathrm{Mod}(\mathrm{Th}\, \mathbf{K})$$

(b) Odvoďte z (a) rovnosti

$$\mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}\, T)) = \mathrm{Mod}(T) \qquad \mathrm{Th}(\mathrm{Mod}(\mathrm{Th}\, \mathbf{K})) = \mathrm{Th}(\mathbf{K})$$

(c) Dokážte, že množina $\mathrm{Th}(\mathrm{Mod}\, T)$ pozostáva práve zo všetkých uzavretých L-formúl φ takých, že $T \vdash \varphi$.

(d) Dokážte, že $\mathrm{Mod}(\mathrm{Th}\, \mathbf{K})$ je najmenšia axiomatická trieda $\mathbf{M} \subseteq \mathrm{Mod}(L)$ taká, že $\mathbf{K} \subseteq \mathbf{M}$.

(e) Dokážte, že trieda $\mathrm{Mod}(\mathrm{Th}\, \mathbf{K})$ pozostáva práve zo všetkých L-štruktúr $\mathcal{B}$, ktoré sú izomorfné s elementárnymi podštruktúrami ultraproduktov všetkých možných systémov $(\mathcal{A}_i)_{i\in I}$ štruktúr $\mathcal{A}_i \in \mathbf{K}$.

Vybraná literatúra

Balcar, B., Štěpánek, P. [2000], *Teorie množin*, Academia, Praha (2. vyd.).

Barwise, J. (ed.) [1977], *Handbook of Mathematical Logic*, North Holland, Amsterdam – New York – Oxford.

Bukovský, L. [1985], *Množiny a všeličo okolo nich*, Alfa, Bratislava.

Chang, C. C., Keisler, H. J. [1990], *Model Theory*, Studies in Logic and the Foundations of Mathematics, Elsevier, North Holland, Amsterdam (3^{rd} ed.).

Čechák, V., Berka, K., Zapletal, I. [1981], *Co víte o moderní logice*, Horizont, Praha.

Dauben, J. W. [1979], *Georg Cantor: His Mathematics and Philosophy of the Infinite*, Harvard University Press, Cambridge, Mass.

Davis, M. (ed.) [1965], *The Undecidable. Basic Papers on Undecidable Propositions, Unsolvable Problems and Computable Functions*, Raven Press, Hewlett, N. Y.

Davis, M. [1977], *Applied Nonstandard Analysis*, John Wiley & Sons, New York – London.

Davis, M. [2018], *Pragmatic Platonism, Mathematics and the Infinite*, in Hellman, G., Cook, R. T. (eds.), *Hillary Putnam on Mathematical Logic*, Springer-Verlag, Cham (Switzerland), pages 145 – 159;
`https://www.researchgate.net/publication/329449494%_Pragmatic_Platonism_Mathematics_and_the_Infinite`

Davis, M. [2005], *What Did Gödel Believe and When Did He Believe It?* Bull. Symbolic Logic **11**, 194 – 206;
`https://www.jstor.org/stable/1556749?seq=1%#metadata_info_tab_contents`

Ebbinghaus, H.-D., Flum, J. [1999], *Finite Model Theory*, Perspectives in Mathematical Logic, Springer, Berlin – Heidelberg – New York (2^{nd} ed.).

Enderton, H. B. [1977], *Elements of Set Theory*, Aacademic Press, New York.

Enderton, H. B. [2001], *A Mathematical Introduction to Logic*, Academic Press, New York (2^{nd} ed.).

Feferman, S. [2006], *The Impact of the Incompleteness Theorems on Mathematics*, Notices Amer. Math. Soc. **53** (April), 434 – 439;
`https://www.ams.org/notices/200604/fea-feferman.pdf`

Franzen, T. [2005], *Gödel's Theorem: An Incomplete Guide to Its Use and Abuse*, A K Peters, Wellesley, Mass.

Gaifman, H., *What Gödel's Incompleteness Result Does and Does Not Show*; `https://pdfs.semanticscholar.org/1efb/5896951d8c20984f558c1e4ab4d6d029143d.pdf`

Goldblatt, R. [1998], *Lectures on the Hyperreals. An Introduction to Nonstandard Analysis*, Springer-Verlag, New York.

Hills, M., Loeser, F. [2019], *A First Journey through Logic*, Student Mathematical Library vol. 89, Amer. Math. Soc., Providence, Rhode Island.

Hodges, W. [1993], *Model Theory*, Cambridge University Press, Cambridge – New York.

Hodges, W. [1997], *A Shorter Model Theory*, Cambridge University Press, Cambridge – New York.

Jech, T. [1978], *Set Theory*, Academic Press, New York.

Kneale, W., Kneale, M. [1984], *The Development of Logic*, Clarendon Press, Oxford.

Kolář, J., Štepánková, O., Chytil, M. [1989], *Logika, algebry a grafy* (Kap. 2. Výroková logika, Kap. 3. Predikátová logika), SNTL, Praha.

Kolman, V. [2008], *Filosofie čísla. Základy logiky a aritmetiky v zrcadle analytické filosofie*, FILOSOFIA – Nakladatelství Filosofického ústavu AV ČR, Praha.

Kolman, V., Punčochář, V. [2015], *Formy jazyka: Úvod do logiky a její filosofie*, Filosofia, Praha.

Kossak, R. [2024], *Mathematical Logic. On Numbers, Sets, Structures and Symmetry*, Springer Graduate Texts in Philosophy, vol. 4, Springer, Cham, Switzerland (2^{nd} ed.).

Manin, Yu. I. [2010], *A Course in Mathematical Logic for Mathematicians*, Graduate Texts in Mathematics, Springer, New York – Heidelberg – London (2^{nd} ed. with collaboration by B. Zilber).

Marker, D. [2002], *Model Theory, An Introduction*, Graduate Texts in Mathematics, Springer, New York – London.

Mendelson, E. [1964], *Introduction to Mathematical Logic*, D. Van Nostrand, Princeton, New Jersey.

Raatikainen, P. [2020], *Gödel's Incompleteness Theorems*, Stanford Encyclopedia of Philosophy; `https://plato.stanford.edu/entries/goedel-incompleteness/`

Restall, G. [2005], *Logic, An Introduction*, Routlege, Taylor & Francis Group, London – New York.

Robinson, A. [1963], *Introduction to Model Theory and to the Metamathematics of Algebra*, North Holland, Amsterdam.

Robinson, A. [1966], *Non-Standard Analysis*, North Holland, Amsterdam.

Shoenfield, J. R. [1967], *Mathematical Logic*, Addison-Wesley, Reading, Mass.; reprinted by Assoc. Symb. Logic, Urbana, Illinois and A K Peters, Natick, Mass. 2001.

Smith, P. [2013], *An Introduction to Gödel's Theorems*, Cambridge University Press, Cambridge – New York.

Smullyan, R. M. [1992], *Gödel's Incompleteness Theorems*, Oxford University Press, Oxford – New York.

Smullyan, R. M. [2014], *A Beginner's Guide to Mathematical Logic*, Dover Publications, New York.

Smullyan, R. M. [2017], *A Beginner's Further Guide to Mathematical Logic*, World Scientific, Singapore.

Sochor, A. [2001], *Klasická matematická logika*, Univerzita Karlova, Nakladatelství Karolinum, Praha.

Sochor, A. [2011], *Logika pro všechny ochotné myslet*, Univerzita Karlova, Praha.

Šalát, T., Smítal, J. [1986], *Teória množín*, Alfa, Bratislava.

Štěpánek, P. [1982], *Matematická logika*, skriptá MFF UK, SPN, Praha.

Švejdar, V. [2002], *Logika – neúplnost, složitost, nutnost*, Academia, Praha.

Tarski, A. [1965], *Introduction to Logic and to the Methodology of Deductive Sciences*, Oxford University Press (3rd ed.); český preklad *Úvod do logiky a metodologie deduktivních věd*, Academia, Praha 1966.

van Heijenoort, J. (ed.) [1967], *From Frege to Gödel. A Source Book in Mathematical Logic, 1879–1931*, Harvard University Press, Cambridge, Mass.

Vopěnka, P. [2000], *Úhelný kámen evropské vzdělanosti a moci. Souborné vydání rozprav s geometrií*, Práh, Praha.

Vopěnka, P. [2004], *Vyprávění o kráse novobarokní matematiky. Souborné vydání rozprav o teorii množin*, Práh, Praha.

Wang, Hao [1987], *Reflections on Kurt Gödel*, MIT Press, Cambridge, Mass.

Wang, Hao [1996], *A Logical Journey: From Gödel to Philosophy*, MIT Press, Cambridge, Mass.

Zach, R. [2003], *Hilbert's Program*, Stanford Encyclopedia of Philosophy; `http://plato.stanford.edu/archives/fall2003/entries/hilbert-program/` `(2003)`

Zlatoš, P. [1995], *Ani matematika si nemôže byť istá sama sebou. Úvahy o množinách, nekonečne, paradoxoch a Gödelových vetách*, IRIS, Bratislava; `http://thales.doa.fmph.uniba.sk/zlatos/animat/animat.pdf`ti

Zlatoš, P. [1999], *O dobrom usporiadaní a axióme výberu I*, Obzory matematiky, fyziky a informatiky, **58**, 1 – 9.

Zlatoš, P. [2000], *O dobrom usporiadaní a axióme výberu II*, Obzory matematiky, fyziky a informatiky, **1**, 14 – 24.

Zoznam symbolov

$\aleph_0$	38	$A \approx B$	55
$\aleph_1$	38	A^I	57
$\mathfrak{c}$	38	$\mathrm{TE}(A)$	58
$\mathrm{VF}(P)$	43	C_I	58
$\neg A$	43	$\mathrm{Th}(I)$	60
$A \wedge B$	43	$(\mathbb{N};\, +, \cdot, 0, 1, <)$	62
$A \vee B$	43	$(\mathbb{Z};\, +, \cdot, 0, 1, <)$	62
$A \Rightarrow B$	43	$(\mathbb{Q};\, +, \cdot, 0, 1, <)$	62
$A \Leftrightarrow B$	43	$(\mathbb{R};\, +, \cdot, 0, 1, <)$	62
$\mathrm{VF}(p_1, \ldots, p_n)$	43	$(\mathbb{C};\, +, \cdot, 0, 1)$	62
$I \colon P \to \{0,1\}$	45	$L = (F, C, R, \nu)$	63
$I \colon \mathrm{VF}(P) \to \{0,1\}$	45	$\mathcal{A} = (A;\, I)$	63
$A \equiv B$	46	$f^I \colon A^n \to A$	63
$A \vert B$	47	$c^I \in A$	63
$A \dagger B$	47	$r^I \subseteq A^n$	63
$F_A \colon \{0,1\}^n \to \{0,1\}$	49	s^I, $s^{\mathcal{A}}$	63
$T \vDash B$	51	$\mathrm{Term}(L)$	63
$\vDash B$	51	t^I, $t^{\mathcal{A}}$	64
(LAx 1)	52	$t_1 = t_2$	64
(LAx 2)	52	$r(t_1, \ldots, t_n)$	64
(LAx 3)	52	$\mathrm{Form}(L)$	64
(LAx 4)	52	$\neg\varphi$	64
(MP)	52	$\varphi \wedge \psi$	64
$T \vdash B$	52	$\varphi \vee \psi$	64
$\vdash B$	52	$\varphi \Rightarrow \psi$	64
(LAx 5)	53	$\varphi \Leftrightarrow \psi$	64

$(\forall x)\varphi$	64	$T \vdash \psi$	76
$(\exists x)\varphi$	64	$\vdash \psi$	76
$\mathcal{A} \vDash \varphi(a_1, \ldots, a_n)$	65	$T \vDash_{\mathrm{fin}} \varphi$	77
$\mathcal{A} \vDash \varphi$	66	$\varphi \equiv \psi$	77
$\mathcal{A} \vDash T$	66	$\mathrm{char}(\mathcal{A})$	80
$T \vDash \psi$	66	$\mathrm{At}(x)$	81
$(\mathbb{Z}_n; +, \cdot, 0, 1)$	69	$L \subseteq L'$	82
$(\mathbb{H}; +, \cdot, 0, 1)$	69	$\mathcal{A} \restriction L$	83
$(\mathbb{A}; +, \cdot, 0, 1)$	69	$(\exists! x)\varphi$	83
$(P; <)$, $(P; \leq)$	70	$t_1 \sim_T t_2$	85
PA	73	$\widetilde{t}$	85
$(\mathbb{N}; +, \cdot, 0, 1)$	73	$\mathcal{M}(T)$	86
$\{x, y\}$	74	$\|L\|$	90
$\bigcup X$	74	$\varphi_0(x), \varphi_1(x), \ldots, \varphi_n(x), \ldots$	100
$\mathcal{P}(X)$	74	$\Delta_0, \Delta_1, \ldots, \Delta_k, \ldots$	100
$\{x \in X \colon \varphi(x, \vec{u})\}$	74	$P(x, y, z)$	100
ZF	74	$R(x, y, z)$	100
ZFC	74	$\varphi_g(g)$	101
AC	74	$\varphi_r(r)$	103
(PrAx 1)	75	$\mathrm{Cons}_1(T)$	104
(PrAx 2)	75	$\mathrm{Cons}_2(T)$	105
(PrAx 3)	75	$\mathrm{Cons}_3(T)$	105
(PrAx 4)	75	$\mathrm{Cons}_4(T)$	106
$\varphi(t/x)$, $\varphi(t)$	75	$G(m, n)$	110
$\varphi(t_1/x_1, \ldots, t_n/x_n)$, $\varphi(t_1, \ldots, t_n)$	75	ε_0	111
		$\Gamma(m, n)$	111
(QAx 1)	75	$\mathcal{B} \subseteq \mathcal{A}$	115
(QAx 2)	75	$h \colon \mathcal{A} \to \mathcal{B}$	118
(EAx 1)	76	$h[M]$	119
(EAx 2)	76	$h^{-1}[N]$	119
(EAx 3)	76	$h \colon \mathcal{A} \xrightarrow{\sim} \mathcal{B}$	122
(EAx 4)	76	$\mathcal{A} \cong \mathcal{B}$	122
(EAx 5)	76	$\mathrm{Id}_A \colon A \to A$	122
(MP)	76	$h \colon \mathcal{A} \hookrightarrow \mathcal{B}$	123
(Gen)	76	$\mathcal{A} \equiv \mathcal{B}$	125

$\mathrm{Th}(\mathcal{A})$	125
$\mathcal{A} \prec \mathcal{B}$	126
$h\colon \mathcal{A} \xrightarrow{\prec} \mathcal{B}$	128
$\mathcal{A}_M = (\mathcal{A}, a)_{a\in M}$	128
$\mathcal{A}_A = (\mathcal{A}, a)_{a\in A}$	129
$\big(\mathcal{B}, h(a)\big)_{a\in A}$	129
$\mathrm{D}(\mathcal{A})$	129
$\mathrm{D}^+(\mathcal{A})$	129
$\mathrm{Th}(\mathcal{A}_A)$	130
$\mathrm{Th}(\mathcal{A})$	130
Π^0_1	134
Σ^0_1	135
$(I; \leq)$	136
$(\mathcal{A}_i)_{i\in I}$	136
$\bigcup_{i\in I} \mathcal{A}_i$	136
$\bigcup_{i\in I} A_i$	136
$\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \ldots \subseteq \mathcal{A}_n \subseteq \ldots$	136
Π^0_2	138
$\mathrm{Pos}(L_C)$	142
$\mathrm{Neg}(L_C)$	142
$\prod_{i\in I} A_i$	144
A^I	144
$\overline{a}$	144
$\prod_{i\in I} \mathcal{A}_i$	144
$\mathcal{A}^I$	145
$[\varphi(\alpha_1, \ldots, \alpha_n)]$	145
$\mathcal{D}$	147
$\mathcal{P}_J(I)$	147
$\mathcal{F}(I)$	147
$(X, \mathcal{T})$	147
$\mathcal{V}(x)$	147
$\mathbf{X} = (X, \mathcal{B}, \mu)$	147
$\mathcal{Z}(\mathbf{X})$	147
$\alpha \equiv_{\mathcal{D}} \beta$	148
$\prod_{i\in I} A_i \big/ \mathcal{D}$, $\prod A_i \big/ \mathcal{D}$	148
$\alpha^{\mathcal{D}}$	148
$\prod_{i\in I} \mathcal{A}_i \big/ \mathcal{D}$	148
$\mathcal{A}^I \big/ \mathcal{D}$	149
$a \mapsto \overline{a}^{\mathcal{D}}$	149
${}^*\mathbb{R}$	153
${}^*\mathcal{A}$	153
${}^*A$	153
${}^*\mathcal{R} = \mathcal{R}^I \big/ \mathcal{D}$	153
${}^*f\colon {}^*P \to {}^*\mathbb{R}$	154
$\mathcal{R}_0 = (\mathbb{R}; +, \cdot, 0, 1, <)$	154
${}^*\mathcal{R}_0 = ({}^*\mathbb{R}; +, \cdot, 0, 1, <)$	154
$\mathbb{F}^*\mathbb{R}$	154
$\mathbb{I}^*\mathbb{R}$	154
$x \approx y$	154
$\mu(x)$	154
$\mathrm{st}\, x = {}^\circ x$	154
$\mathbb{F}^*\mathbb{R}/\mathbb{I}^*\mathbb{R}$	155
$\mathbb{F}^*\mathbb{Q},\ \mathbb{I}^*\mathbb{Q},\ \mathbb{F}^*\mathbb{Q}/\mathbb{I}^*\mathbb{Q}$	155
$\mathrm{Mod}(L)$	159
$\mathrm{Mod}(T)$	159
$\mathrm{Th}(\mathbf{K})$	159

Vecný register

algebraické rozširenie poľa, 140
algebraický uzáver poľa, 140
alternatíva, 46
aritmetická sentencia
    platná, 100
    pravdivá, 100
atóm, 81
axiomatická trieda, 159
axióma
    dvojice, 74
    extenzionality, 74
    potenčnej množiny, 74
    regularity, 74
    výberu, 74, 148
    zjednotenia, 74
axióma nekonečna, 74
axiómy
    kvantifikátorov, 75
    rovnosti, 76
    teórie, 50
        špecifické, 50, 66
    výrokového počtu, 52, 75

Boolova algebra, 71
    atomická, 81
    bezatomická, 81
boolovská pravdivostná hodnota, 145

číslo
    algebraické, 69
    hypercelé, 153
    hyperkomplexné, 153
    hyperprirodzené, 153
    hyperracionálne, 153
    hyperreálne, 153

De Morganove zákony, 31
delenie intervalu, 156
    infinitezimálne, 156
demonštrácia, 48
derivácia funkcie, 156
diagram štruktúry, 129
    atomický, 129
    elementárny, 130
    pozitívny atomický, 129
    úplný, 130
dialektika, 15
disjunkcia, 46
dôkaz, 52, 76
    rozborom prípadov, 56
    sporom, 56
dôsledok
    logický, 51, 66
    nevyhnutný, 51, 66
    o dôkaze rozborom možností, 79
    o dôkaze sporom, 79
    o úplných teóriách, 80
duálny ideál, 147

ekvivalencia, 46
    nekonečnej blízkosti, 154
    nerozlíšiteľnosti, 154
erisitika, 16

filter, 147
    Fréchetov, 147
    hlavný, 147
    nehlavný, 147
    nevlastný, 147
    okolí, 147
    triviálny, 147
    vlastný, 147

filtrovaná mocnina
štruktúry, 149
filtrovaný súčin
množín, 148
štruktúr, 148
formula
aritmetická, 100
atomická, 64
dokázateľná, 76
existenčná, 117
jazyka L, 64
logicky platná, 77
negatomická, 129
negatívna, 121
otvorená, 117
pozitívna, 119
pravdivá, 66
splnená, 66
univerzálna, 117
univerzálno-existenčná, 138
uzavretá, 65
v prenexnom normálnom tvare, 77
formuly
logicky ekvivalentné, 77
funkcia
boolovská, 49
árnosti, 63

Gödelova veta o neúplnosti
druhá, 104, 106
prvá, 99
syntaktická verzia, 101
sémantická verzia, 101
Gödelova-Rosserova veta o neúplnosti, 103
grupa, 67
abelovská, 67
bez torzie, 80
deliteľná, 80
komutatívna, 67
s exponentom n, 80

Hilbertov program, 98
homomorfizmus, 118
homomorfný obraz, 119

hyperreálne číslo
infinitezimálne, 154
konečne veľké, 154
konečné, 154
nekonečne malé, 154
nekonečné, 154
neohraničené, 154
ohraničené, 154

charakteristika unitárneho okruhu, 80

identita, 64
implikácia, 46
indukcia podľa zložitosti, 44
interpretácia, 45
termu, 64
teórie, 51
špecifických symbolov, 63
intuicionizmus, 97
izomorfizmus, 122

jazyk
prvého rádu, 63
spočítateľný, 90
výrokového počtu, 43
čistej rovnosti, 79

kanonická štruktúra teórie, 86
karteziánska mocnina
množiny, 144
karteziánsky súčin
množín, 144
konečne axiomatizovateľná trieda, 159
konjunkcia, 46
kontradikcia, 47
kvantifikácia jednoznačnej existencie, 83
kvantifikátory, 63
kvaternióny, 30, 69

lema
axiomatizačná, 134
o konštantách, 82
o vzájomnej zlučiteľnosti, 133
Teichmüllerova-Tukeyho, 92
logické axiómy
predikátového počtu, 75
výrokového počtu, 52

logické spojky, 43, 63
logika, 7, 13
  dialektická, 16
  formálna, 11
  matematická, 11, 12
  modálna, 17
  nultého rádu, 42
  prvého rádu, 62
  sylogistická, 17
  symbolická, 11
  temporálna, 17
  výroková, 42
L-formula, 64
L-term, 63
L-štruktúra, 63

matematická štruktúra, 62
maximálny prvok, 91
množina
  axióm teórie, 134
  faktorová, 85
  hyperkonečná, 156
  lineárne usporiadaná
    bez koncových bodov, 81
    hustá, 81
  potenčná, 71
  usporiadaná, 136
  základná, 63
  čiastočne usporiadaná, 70
model
  teórie, 66
modus ponens, 52, 76
mohutnosť jazyka, 90, 130
monáda
  čísla (bodu), 154

nadštruktúra, 115
negácia, 46
neštandardná analýza, 153
normálna forma
  disjunktívna, 49
  konjunktívna, 49
nosič, 63

objektová premenná, 63
obor integrity, 68, 121
okruh, 68
  komutatívny, 68
  s delením, 69
operácia
  nasledovníka, 73
  násobenia, 73
  sčítania, 73
Organon, 17

paradox, 14
  Berryho, 97
  Epimenidov, 15, 95
  klamára, 15, 95
    silná verzia, 95
  Russellov, 96
  Skolemov, 91
Peanova aritmetika, 73
Peircova šípka, 47
podštruktúra, 115
  elementárna, 126
pole, 69
  algebraicky uzavreté, 69, 140
  formálne reálne, 69
  reálne uzavreté, 69
poset, 70
postupnosť
  hyperkonečná, 156
poľská notácia, 44
pravdivostná hodnota, 42
pravdivostné ohodnotenie, 45
pravidlo zovšeobecnenia, 76
predikátový počet, 62
prehlásenie o bezospornosti, 104
Presburgerova aritmetika, 81
priama mocnina
  množiny, 144
  štruktúry, 145
priamy súčin
  množín, 144
  štruktúr, 144
princíp dobrého usporiadania, 73
princíp maximality, 146

Quinova dýka, 47

redukovaná mocnina
štruktúry, 149
redukovaný súčin
množín, 148
štruktúr, 148
relácia
ekvivalencie, 85
nekonečnej blízkosti, 154
spĺňania, 65
reťazec štruktúr, 136
elementárny, 136
rozšírenie
jazyka, 82
neštandardné, 153
štruktúry, 115
elementárne, 126
rozšírenie teórie
konzervatívne, 83
pomocou definícií, 83

schéma
indukcie, 73
nahradenia, 74
vydelenia, 74
sentencia, 65
Shefferov ťah, 47
signatúra, 63
skalár, 70
skalárny násobok, 70
sofisti, 13
sofizmus, 14
stredná hodnota funkcie, 157
substitúcia
prípustná, 75
termu do formuly, 75
svedok sentencie v teórii, 86
sylogizmus
apodiktický, 17
dialektický, 17
kategorický, 17
symbol
funkcionálny (operačný), 63
konštantný, 63
logický, 63
nový, 87
relačný (predikátový), 63
špecifický, 63
symboly
pomocné, 43, 63
syntax, 12
výrokového počtu, 42
systém
centrovaný, 148
systém podmnožín, 91
konečného charakteru, 92
sémantika, 12
výrokového počtu, 45
súčet
integrálny, 157

štandardná časť hyperreálneho čísla, 154
štandardný model Peanovej aritmetiky, 73
štruktúra
jazyka L, 63
prvého rádu, 63
štruktúry
elementárne ekvivalentné, 125
izomorfné, 122

tabuľka pravdivostných hodnôt, 48
Tarského kritérium, 127
tautológia, 47
teleso, 69
term, 63
atomický, 64
konštantný, 64
teória, 66
aritmeticky korektná, 100
aritmetická, 100
ω-konzistentná, 102
ω-úplná, 108
bezosporná, 56, 79
Boolových algebier, 71
grúp, 67
henkinovská, 86
inkonzistentná, 56, 79
konzistentná, 56, 79
lineárneho usporiadania, 71
množín, 74
neprotirečivá, 56, 79
okruhov, 68

s delením, 69
s jednotkou, 68
polí, 68
protirečivá, 56, 79
prvého rádu, 66
rekurzívne axiomatizovateľná, 100
sa prenáša na homomorfné obrazy, 142
sa prenáša na nadštruktúry, 135
sa prenáša na podštruktúry, 134
sa zachováva pri zjednoteniach reťazcov, 138
sporná, 56, 79
triedy, 159
unitárnych okruhov, 68
usporiadaných komutatívnych okruhov, 72
usporiadaných množín, 71
usporiadaných okruhov, 72
usporiadaných okruhov s jednotkou, 72
usporiadaných polí, 72
usporiadaných reálne uzavretých polí, 72
vo výrokovom počte, 50
štruktúry, 125
čiastočného usporiadania, 70
úplná, 58, 79
teória množín
ZF, 74
ZFC, 74
teórie
nezlučiteľné, 133
zlučiteľné, 133
tieň hyperreálneho čísla, 154
tvrdenie, 65

ultrafilter, 147
ultramocnina štruktúry, 151
ultraprodukt štruktúr, 151
určitý integrál funkcie, 157
usporiadanie
čiastočné, 70
neostré, 70
ostré, 70
usporiadané pole
reálne uzavreté, 72

vektor, 70
vektorový priestor, 70
veta
Łošova, 151
Churchova-Turingova, 109
Goodsteinova, 111
Keislerova-Shelahova, 159
Kirbyho-Parisova, 113
Lindenbaumova, 92
Löwenheima, Skolema, Tarského
„zdola nahor“, 131
„zhora nadol“, 130
o dedukcii, 55, 78
o kompaktnosti, 60, 88, 158
o korektnosti, 54, 76
o rozšírení pomocou definícií, 84
o úplnosti, 54, 59, 60, 77, 88
Gödelova, 87
Postova, 58
o úplných henkinovských rozšíreniach, 94
Tarského, 108
vnorenie, 123
elementárne, 128
vymedzovací princíp, 96
výroková forma, 42, 43
dokázateľná, 52
platná, 51
pravdivá, 51
splnená, 51
splniteľná, 47
vyvrátiteľná, 47
výrokové formy
logicky ekvivalené, 46
výrokové premenné, 43
výrokový počet, 42
výskyt premennej, 65
viazaný, 65
voľný, 65

Zenónove apórie, 15
Zermelova-Fraenkelova teória množín, 74
s axiómou výberu, 74

znak rovnosti, 63
zobrazenie
    diagonálne, 144, 149
zúženie štruktúry do jazyka L, 83

Menný register

Abélard, Pierre, 20
Albert Saský, 20
Albert Veľký, 20
Aristoteles, 17, 19, 23, 33
Arnauld, Antoine, 22

Beltrami, Eugenio, 27
Berry, George Godfrey, 97
Boëthius, Anicius Manlius Severinus, 19
Bolyai, Farkas, 26
Bolyai, János, 26
Bolzano, Bernard, 28
Boole, George, 30, 33
Borelli, Giovanni Alfonso, 25
Brentano, Franz, 30
Brouwer, Luitzen Egbertus Jan, 97
Buridan, Jean, 20, 95

Cantor, Georg, 36, 40, 96
Cauchy, Augustin Louis, 28
Cayley, Arthur, 27
Chajjám, Omar, 25
Chrysippos zo Soloi, 18
Church, Alonzo, 57, 108, 109, 114
Cicero, Marcus Tulius, 18
Cohen, Paul J., 28

De Morgan, Augustus, 30, 31, 33, 36
Dedekind, Richard, 29
Descartes, René, 19, 21
Diodoros Kronos, 17
Diogenes Laertios, 18
Dionýzodoros, 14

Epimenides, 15, 95
Eubulides z Milétu, 14, 17, 95
Eudémos z Rhodu, 18
Euklides, 16, 19, 24, 27
Euklides z Megary, 16
Euthydémos, 14

Feferman, Solomon, 106, 108, 113
Filón z Megary, 17
Fraenkel, Abraham, 40, 97
Franzelin, Johan Baptist, 39
Frayne, Thomas, 150
Frege, Gottlob, 34, 40, 97
Fréchet, Maurice, 147

Galileo Galilei, 19
Galénos, 18
Gauss, Carl Friedrich, 23, 25
Gentzen, Gerhard, 36, 107
Goodstein, Reuben Luis, 110, 111
Gödel, Kurt, 23, 27, 41, 91, 95, 99, 100, 107, 109, 110, 113
Gutberlet, Konstantin, 39

Hamilton, William Rowan, 30
Harrington, Leo, 110
Hausdorff, Felix, 40
Henkin, Leon, 86
Hilbert, David, 27, 38, 40, 98
Husserl, Edmund, 30

Ibn al-Haytham, Hassan, 25
Ibn Qurra, Thabit, 25

Jevons, William Stanley, 32, 33

Kant, Immanuel, 23
Keisler, H. Jerome, 159

Kepler, Johannes, 19
Kirby, Laurie, 112
Klein, Felix, 27
Koperník, Mikuláš, 19

Lambert, Johann Heinrich, 23, 25, 33
Leibniz, Gottfried Wilhelm, 22, 33, 153
Lesńiewski, Stanisław, 30
Lindenbaum, Adolf, 92
Lobačevskij, Nikolaj Ivanovič, 26
Löwenheim, Leopold, 91, 130
Ludlam, William, 24
Lull, Ramón, 22
Łoś, Jerzy, 151
Łukasiewicz, Jan, 30

Marcus Aurelius, 18
Marquand, Allan, 33
Maľcev, Anatolij Ivanovič, 41
Meinong, Alexius, 30
Menger, Karl, 28
Morel, Anne C., 150
Mostowski, Andrzej, 91

Neumann, John von, 95, 105
Newton, Isaac, 19, 35, 153
Nicole, Pierre, 22

Ockham, William, 20, 31

Padoa, Alessandro, 35
Paris, Jeff, 110, 112
Parmenides, 15
Pascal, Blaise, 21
Peano, Giuseppe, 33, 34
Peirce, Charles Sanders, 32, 33, 47
Peter Hispánsky, 20
Platón, 16, 19
Playfair, John, 24
Poincaré, Henri, 28, 97
Post, Emil, 58
Presburger, Mojżesz, 81
Proklos z Lýkie, 24
Protagoras z Abdér, 14

Quine, Willard Van Orman, 40, 47

Ramsey, Frank, 110
Riemann, Bernhard, 24
Robinson, Abraham, 41, 153
Rosser, Barkley, 103, 110, 114
Russell, Bertrand, 35, 40, 97

Saccheri, Giovanni Girolamo, 25
Schröder, Ernst, 33
Schweikart, Ferdinand Karl, 25
Scott, Dana, 150
Scotus, John Duns, 20
Seneca, Lucius Annaeus, 18
Sheffer, Henry Maurice, 32, 47
Shelah, Saharon, 159
Skolem, Thoralf, 41, 89, 91, 130
Sokrates, 16
Spinoza, Baruch, 19
Swift, Jonathan, 22

Tarski, Alfred, 27, 30, 41, 65, 108, 114, 127, 130
Taurinus, Franz Adolph, 25
Teichmüller, Oswald, 92
Theofrastos z Eresu, 18
Tukey, John W., 92
Turing, Alan, 108, 109, 114
Twardowski, Kazimierz, 30

Uryson, Pavel Samuilovič, 28

Vaught, Robert, 127
Venetus, Paolo, 20
Viète, François, 22
Vitale, Giordano, 25
Vopěnka, Petr, 29

Wang, Hao, 114
Wedderburn, Joseph, 77
Weierstrass, Karl, 28
Whitehead, Alfred North, 35, 97
Wright, Thomas, 23

Zach, Richard, 98
Zenón, 15
Zenón z Citia, 18
Zermelo, Ernst, 40, 97

Pavol Zlatoš

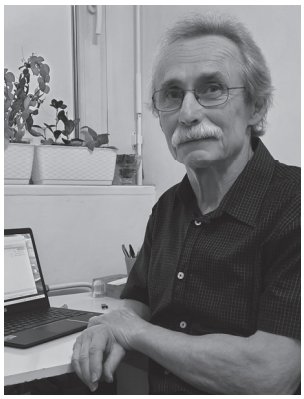
Prednášky z matematickej logiky

Vydala Univerzita Komenského v Bratislave, 2025
Grafická úprava: Mária Benešová
Návrh obálky: Pavol Zlatoš, Marián Sekela

Rozsah 175 strán, 11,98 AH, prvé vydanie,
vyšlo ako elektronická publikácia

ISBN 978-80-223-6121-7 (tlač)
ISBN 978-80-223-6122-4 (online)

9 788022 361224



Pavol Zlatoš (1955)
je profesorom na Fakulte matematiky, fyziky a informatiky Univerzity Komenského v Bratislave. Jeho vedecké záujmy siahajú od algebry, topológie a matematickej logiky cez neštandardnú analýzu a jej aplikácie v iných oblastiach matematiky až k farmakokinetike a filozofii matematiky.
Je autorom rozsiahlej učebnice monografického charakteru *Lineárna algebra a geometria. Cesta z troch rozmerov s presahmi do príbuzných odborov* a knihy esejí *Ani matematika si nemôže byť istá sama sebou. Úvahy o množinách, nekonečne, paradoxoch a Gödelových vetách*.
Za svoj najvýznamnejší vedecký výsledok považuje dôkaz troch Gordonových hypotéz, ktoré prostriedkami neštandardnej analýzy prepájajú dualitu pre konečné abelovské grupy a Pontriaginovu dualitu pre lokálne kompaktné abelovské grupy, ako aj diskrétnu Fourierovu transformáciu a harmonickú analýzu na istých nekonečnorozmerných fukcionálnych priestoroch nad takýmito grupami.

ISBN 978-80-223-6122-4