Petr Vopěnka
O prvním Hilbertově problému (Hypotéza kontinua a axióm výběru)

Pokroky matematiky, fyziky a astronomie, Vol. 16 (1971), No. 3, 117--129

Persistent URL: http://dml.cz/dmlcz/139083

O PRVNÍM HILBERTOVĚ PROBLÉMU

(Hypotéza kontinua a axióm výběru)

PETR VOPĚNKA, Praha

Našim čtenářům je dostupná kniha *Problemy Gil'berta* (Moskva 1969), která byla zpracována kolektivem sovětských autorů. Připravovaný seriál v *PMFA* nemá však být podle záměrů redakce překladem tohoto sborníku, proto jsem se snažil napsat na dané téma zcela samostatný článek.

O prvním Hilbertově problému píše v uvedené knize A. S. JESENIN-VOLPIN. Uvádí formulaci problému a hlavní výsledky, které byly dosaženy při jeho řešení.

Rozhodl jsem se zvolit populárnější formu výkladu, což se nutně odrazí negativně v preciznosti formulací. Naproti tomu se na rozdíl od ruského autora pokouším seznámit čtenáře podrobněji s hlavními ideami, které byly nalezeny během řešení problému.

Literatura na konci článku obsahuje práce, které shrnují vždy určité období a z nichž je možno celou problematiku studovat.

*

Pojem množiny uvedený do matematiky CANTOREM umožnil matematikům formovat všechny do té doby známé matematické disciplíny na jednotném základě. Navíc se tento pojem stal impulsem ke vzniku dalších, velmi rozmanitých matematických oborů. Do dnešní doby si množinové pojetí zachovává v matematice své výsadní postavení v tom smyslu, že teorie množin je vlastně světem, v němž se matematika odehrává.[1])

Cantor původně definoval množinu jakožto souhrn nějakých objektů, které se nazývají prvky množiny. Jak je patrno, tato definice není vlastně žádnou definicí, ale jen intuitivním popisem toho, co bychom si měli pod pojmem množiny představovat. V definicích tohoto typu nejde o to nějaký pojem přesně vymezit, ale pouze pokud možno ho co nejvíce ozřejmit.

Více než to, co to vlastně množina je, bude nás zajímat, jaké vlastnosti množiny mají.

Jedním z nejzákladnějších požadavků kladených na množiny je to, aby ke každé vlastnosti φ, týkající se objektů, existovala množina Y, jejímiž prvky jsou právě ty objekty X, které mají vlastnost φ. Takovou množinu budeme značit $\{X; \varphi(X)\}$.

[1]) Vřele doporučujeme našim čtenářům znovu si pročíst velmi pěkný článek akademika V. KOŘÍNKA *Teorie množin, její vznik a vývoj* (*PMFA*, ročník *10*, 1965, str. 131—160). *Pozn. red.*

V intuitivní teorii množin je to v podstatě jediný požadavek, který je na množiny kladen.

To, že objekt X je prvkem množiny Y, zapíšeme $X \in Y$. Jestliže X není prvkem Y, pak píšeme $X \notin Y$.

Ve shodě se shora uvedeným požadavkem existuje množina, jejímiž prvky jsou všechny objekty X, pro které platí současně $X \in X$ a $X \notin X$. Jak je patrno, taková množina nemá žádný prvek. Množina, která nemá žádný prvek, se nazývá *prázdná.*

Dvě množiny X, Y se sobě rovnají (jsou totožné), jestliže mají tytéž prvky. *Rovnost množin* X, Y označíme $X = Y$. Jestliže φ je nějaká vlastnost, jestliže množina X má vlastnost φ a jestliže $X = Y$, pak též Y má vlastnost φ. To je přirozený požadavek, který je na rovnost kladen.

Řekneme, že množina X je *částí* nebo též *podmnožinou* množiny Y, jestliže každý prvek množiny X je též prvkem množiny Y (označíme tento fakt $X \subseteq Y$). Řekneme, že množina X je *vlastní částí* množiny Y, jestliže $X \subseteq Y$ a není $X = Y$ (značíme $X \subset Y$).

Je-li Y nějaká množina, potom *potenční množinu* množiny Y definujeme takto

$$\mathscr{P}(Y) = \{X; X \subseteq Y\} .$$

Množinu všech přirozených čísel budeme značit N. Poznamenejme, že se v tomto článku nebudeme zabývat otázkou, co je to množina přirozených čísel.

Jsou-li X, Y nějaké objekty, potom $\{X, Y\}$ značí množinu, jejímiž prvky jsou právě X a Y. Množina $\{X, Y\}$ je vlastně neuspořádanou dvojicí prvků X, Y. Uspořádanou dvojici je možno též považovat za množinu, neboť můžeme ji definovat například takto:

$$\langle XY \rangle = \{\{X\}, \{X, Y\}\} .$$

Množina F se nazývá *funkcí,* jestliže jejími prvky jsou uspořádané dvojice a jestliže platí: Je-li $\langle YX \rangle \in F$ a současně $\langle ZX \rangle \in F$, pak $Y = Z$. Jestliže F je funkce, pak je-li $\langle YX \rangle \in F$, jsme podle této definice oprávněni značit toto Y jako $F(X)$. Jestliže pro nějaké X existuje Y tak, že $\langle YX \rangle \in F$, pak říkáme, že pro toto X je $F(X)$ definováno.

Řekneme, že funkce F je vzájemně jednoznačné zobrazení množiny X na množinu Y, jestliže pro každé $Z \in X$ je $F(Z)$ definováno, $F(Z) \in Y$ a pro každé $U \in Y$ existuje právě jedno $Z \in X$ tak, že $U = F(Z)$.

Řekneme, že množiny X, Y jsou *ekvivalentní* (značíme $X \approx Y$), jestliže existuje vzájemně jednoznačné zobrazení F množiny X na množinu Y.

Snadno každý nahlédne, že když množina X je konečná a $X \approx Y$, pak též Y je konečná množina a obě množiny mají stejný počet prvků. Obráceně jestliže X, Y jsou konečné množiny a mají stejný počet prvků, pak $X \approx Y$.

Tato skutečnost nás opravňuje považovat dvě ekvivalentní množiny X, Y za stejně veliké, mající stejný počet prvků, i v případě, že jde o nekonečné množiny.

Poznamenejme, že je mnoho vlastností konečných množin, které se přenášejí i na množiny nekonečné, jsou však též vlastnosti, které se tímto způsobem nepřenesou.

Například máme-li nějakou konečnou množinu, pak žádná její vlastní část nemůže mít stejně prvků jako celá množina; v řeči ekvivalencí to znamená: je-li X konečná, $Y \subset X$, pak není $X \approx Y$. Tuto vlastnost nekonečné množiny nemají. Označme N_2 množinu všech sudých přirozených čísel. Buď F zobrazení, které každému přirozenému číslu n přiřazuje jeho dvojnásobek $2n$. Zřejmě F je vzájemně jednoznačné zobrazení množiny N na množinu N_2. Je tedy $N \approx N_2$, ačkoliv $N_2 \subset N$.

Po tomto zjištění se naskýtá přirozená otázka, zda náhodou nejsou všechny nekonečné množiny spolu ekvivalentní. Odpověď je negativní. Dokonce žádná množina X není ekvivalentní se svou potenční množinou $\mathscr{P}(X)$. Tedy pro žádné X neplatí $X \approx \mathscr{P}(X)$.

Uvedené příklady jsou popudem k tomu, abychom podrobně vyšetřovali ekvivalenci nekonečných množin, případně nalezli všechny možnosti, které v nekonečných množinách mohou nastat.

Zvláštní pozornost budeme věnovat dvěma množinám vyskytujícím se v matematice nejčastěji, a to množině N a množině všech čísel reálných. Je všeobecně známo, že množina všech reálných čísel je ekvivalentní s množinou $\mathscr{P}(N)$. (Naproti tomu množina všech čísel celých, resp. racionálních, je ekvivalentní s množinou N.)

Množiny ekvivalentní s množinou N se nazývají *spočetné množiny*, množiny ekvivalentní s množinou $\mathscr{P}(N)$ se nazývají *množiny mohutnosti kontinua*.

Jak je patrno, má množina $\mathscr{P}(N)$ podmnožiny, které jsou konečné, podmnožiny spočetné a podmnožiny mohutnosti kontinua. Naskýtá se přirozená otázka, zda uvedené typy jsou všechny, které mohou nastat. Hypotéza, že každá nekonečná podmnožina množiny $\mathscr{P}(N)$ má buď mohutnost kontinua, nebo je spočetná, se nazývá *hypotéza kontinua*. Tuto hypotézu je možné všelijak zobecňovat, například, zda všechny nekonečné podmnožiny $\mathscr{P}(\mathscr{P}(N))$ jsou buď spočetné, nebo mohutnosti kontinua, nebo ekvivalentní s $\mathscr{P}(\mathscr{P}(N))$ apod. *Zobecněnou hypotézou kontinua je* hypotéza, že pro každou nekonečnou množinu X je každá podmnožina množiny $\mathscr{P}(X)$ buď ekvivalentní s $\mathscr{P}(X)$, nebo s nějakou podmnožinou množiny X. (Pro konečnou množinu X taková hypotéza evidentně neplatí.)

Jiným závažným problémem teorie množin je *problém výběru*. Jde o to, zda existuje funkce F taková, že pro každou neprázdnou X je $F(X)$ definováno a jest $F(X) \in X$. Hypotéza, že taková funkce F existuje, se nazývá *axióm výběru*.

Je možno vyslovit řadu různých slabších nebo silnějších forem axiómu výběru. Například je otázka, zda existenci takové výběrové funkce F dokážeme ze základního principu teorie množin, to jest, zda je možno nalézt nějakou vlastnost φ takovou, že $F = \{X; \varphi(X)\}$. Axióm výběru v tomto tvaru měli patrně na mysli matematikové v době jeho formulace. Samozřejmě, že je řada možných zeslabení axiómu výběru, které spočívají v tom, že od funkce F požadujeme, aby byla výběrovou funkcí jen pro množiny, které jsou prvky nějaké konkrétní množiny. Zvlášť zajímavá je otázka, zda existuje funkce F taková, že pro každou neprázdnou množinu $X \in \mathscr{P}(\mathscr{P}(N))$ je $F(X)$ definováno a platí $F(X) \in X$. Tato slabá foma axiómu výběru má řadu důsledků pro reálná čísla a v matematické analýze se často užívá.

A. Lindenbaum a A. Tarski dokázali, že z platnosti zobecněné hypotézy kontinua plyne existence výběrové funkce na každé množině; tedy tato forma axiómu výběru je důsledkem zobecněné hypotézy kontinua.

Jak již bylo řečeno, je možno položit řadu problémů podobných problému kontinua a řadu problémů podobných axiómu výběru. Tyto problémy je možno nejrůznějším způsobem navzájem kombinovat a hledat mezi nimi různé souvislosti. Konečně v tomto století vznikla řada dalších problémů teorie množin, jejichž řešení se ukázalo stejně obtížným jako problém kontinua nebo problém výběru. Některé z těchto problémů nemají ani žádnou nápadnou souvislost s uvedenými problémy, avšak mají s nimi společný osud.

Samozřejmě, že by bylo nejjednodušší, kdyby někdo hypotézu kontinua, respektive axióm výběru, dokázal, anebo vyvrátil. Tím by nám odpadla další práce a mohli bychom ukončit tyto úvahy odkazem na příslušné práce. To se však nikomu nepodařilo. Ačkoliv byla vynaložena velká energie na řešení těchto problémů, žádný důkaz nebyl podán. To vedlo postupně matematiky k přesvědčení, že uvedené hypotézy se nedají ani dokázat, ani vyvrátit. Postupně se začal řešit jiný problém, tj. dokázat, že hypotéza kontinua, resp. axióm výběru, jsou *nedokazatelné* a zároveň *nevyvratitelné*. A právě touto problematikou se budeme v dalším zabývat.

*

Jestliže chceme řešit shora uvedenou modifikaci problému, musíme si nejprve ujasnit několik věcí.

Je všeobeně známo, že důkazy v matematice jsou v jistém smyslu relativní, jinými slovy: dokazujeme vždy nějaké tvrzení z tvrzení jiných. Na začátku každého takového důkazu jsou axiómy, tj. tvrzení, která již nedokazujeme, neboť je v dané situaci považujeme za správná.

Tedy i v případě, že dokazujeme různá tvrzení teorie množin, musíme si ujasnit, *z čeho* budeme taková tvrzení dokazovat. První úkol, který máme před sebou, je napsat *axiómy teorie množin.* Axiómy je nutno vybrat tak, abychom se všichni shodli na tom, že odpovídají našim představám o množinách, že je považujeme za správné v intuitivní teorii množin. Druhý požadavek záleží v tom, aby vše, co se dokazuje v intuitivní teorii množin, bylo již dokazatelné z našich axiómů; jinak by totiž naše axiomatická teorie byla chudá. Konečně třetím požadavkem je *bezespornost* naší soustavy axiómů. (Sporné axiómy by neměly pro naše účely žádnou cenu, neboť by z nich bylo dokazatelné každé tvrzení i jeho negace.)

Na rozdíl od jiných matematických teorií, kde se matematici celkem snadno dohodli na axiomatice, je u teorie množin situace mnohem složitější. Ukázalo se totiž, že *intuitivní teorie množin je sporná.*

Řekli jsme si již, že ke každé vlastnosti φ by měla existovat množina, jejímiž prvky jsou právě všechny objekty, které mají vlastnost φ. To znamená, že speciálně existuje množina

$$K = \{X; X \notin X\} .$$

Pro množinu K mohou nastat dva případy: buďto $K \in K$, nebo $K \notin K$. (Klasická logika jinou možnost nepřipouští.) Jestliže je $K \in K$, pak K má vlastnost, kterou mají všechny prvky X množiny K. Touto vlastností je však $K \notin K$. Jestliže na druhé straně je $K \notin K$, pak K má vlastnost, kterou mají právě všechny prvky množiny K. Je tedy $K \in K$. Tím je odvozen spor.

Tato úvaha a řada podobných vyvolala v matematice zmatek, který vedl koncem minulého století ke krizi v matematice. Nebudu zde popisovat různé směry, jimiž byla tato krize překonána; to by si vyžádalo obsáhlejší samostatné pojednání. Pro nás je důležité, že do našeho axiomatického systému nelze zahrnout axióm, který by umožňoval napodobit shora uvedený spor.

Je několik způsobů, jak základní požadavek intuitivní teorie množin zeslabit. Uveďme dva nejběžnější:

a) Požadavek existence množiny všech objektů, které mají vlastnost φ, vyslovíme jen pro *omezenou skupinu vlastností* (z této skupiny bude například vyloučena vlastnost $X \notin X$, která vedla nahoře ke sporu). Takto se postupuje v *axiomatickém systému Zermelo-Fraenkelově* (dále jen ZF). Zde například nepožadujeme existenci množiny *všech* objektů, které mají nějakou vlastnost φ, ale jen těch, které jsou navíc *prvky některé předem dané množiny.*

b) Původní množiny rozdělíme do dvou skupin. Jedna skupina bude obsahovat „rozumné" množiny, druhá tzv. *vlastní třídy*, tj. množiny, s nimiž musíme zacházet velmi opatrně, některé úvahy nejsou pro ně povoleny. Tento druhý způsob je užit v *axiomatickém systému Gödel-Bernaysově* (dále jen GB).

Axiomatický systém GB má konečně mnoho axiómů, systém ZF nekonečně mnoho. Naproti tomu v systému ZF se mnohem rychleji vybuduje základní teorie.

Otázka, který z různých axiomatických systémů teorie množin je přirozenější, nemá žádný smysl, neboť přirozený není ani jeden. Přirozený systém axiómů je, jak jsme již naznačili, sporný.

Uvedené axiomatické systémy mají tu vlastnost, že se v nich dá vybudovat celá současná matematika, takže tato praxe nás opravňuje k tomu, abychom tyto systémy považovali za dostatečně bohaté.

Proti uvedeným systémům lze namítnout, že sice odstranily konkrétní spory, které byly v intuitivní teorii množin nalezeny, že však nemáme žádnou další záruku do budoucna, že se v nich nenajde nějaký nový spor. Je tomu skutečně tak. Nemáme jinou možnost, než věřit v bezespornost uvedených axiomatických systémů. Dokonce víme, že jejich bezespornost nikdy nedokážeme, neboť populárně řečeno, jejich spornost je bezesporná. To se však již dotýká druhého Hilbertova problému, a proto nebudeme zde o těchto otázkách hovořit.

Poznamenejme ještě, že případný spor v některém z uvedených systémů by znamenal spor ve všech systémech a měl by za následek zhroucení mnohem podstatnější části matematiky, než tomu bylo v případě sporů shora uvedeného tvaru. Takový spor by asi zasáhl i do teorie čísel přirozených a vyvolal by tak všeobecnou krizi matematiky.

Nemusím jistě zvlášť zdůrazňovat, že v uvedených axiomatických systémech teorie množin je možno formulovat problém kontinua, problém výběru, různě tyto problémy modifikovat a také formulovat řadu dalších podobných problémů.

Jestliže nyní dokážeme, že hypotéza kontinua je tvrzení nedokazatelné například v axiomatickém systému ZF nebo v axiomatickém systému GB, pak musíme mít stále na paměti, že se jedná stále o *relativní nedokazatelnost*, tj. o nedokazatelnost z příslušných axiómů. Co se týče problému hypotézy kontinua v jeho *nejširším pojetí*, stále není teoreticky vyloučeno, že hypotéza *je* dokazatelná z nějakého jiného přirozeného axiómu, který všichni budeme považovat za správný a který jsme vlastně zapomněli mezi naše axiómy zahrnout. To je však málo pravděpodobné.

Konečně k axiomatickým systémům teorie množin poznamenejme, že popisují jen jakési jádro teorie množin. Zahrnují jen tu část teorie množin, která je bezpodmínečně nutná pro matematické úvahy. V axiomatických teoriích množin lze vybudovat množinu přirozených čísel, čísel reálných a podobně; nejsou zde uvažovány množiny židlí a jiné podobné množiny. Je zřejmé, že v matematických úvahách se bez takových množin snadno obejdeme. Konečně je užitečné nerozlišovat mezi objektem a množinou; v těchto teoriích je každý objekt zároveň množinou, což rovněž žádným způsobem možnosti teorie množin neomezuje.

Nyní se budeme zabývat problémem, jak dokázat, že neexistuje důkaz například hypotézy kontinua z axiómů teorie množin.

V současné době máme v podstatě dvě metody, jak takový problém řešit.

Především jde o metodu, kterou budu nazývat *metodou matematickou*, neboť byla již v matematice často použita. Přesněji řečeno, jde o metodu tzv. *relativní interpretace*.

Vzpomeňme si, jak byla podobná otázka řešena v případě neeukleidovské geometrie. Tehdy byl v geometrii eukleidovské sestrojen model geometrie neeukleidovské. Konstrukce tohoto modelu spočívá v tom, že za nové body jsme prohlásili jen body z vnitřku otevřeného kruhu, za nové přímky jen průniky přímek s tímto kruhem; nová incidence byla definována stejně jako incidence původní, nová vzdálenost jako logaritmus jistého dvojpoměru apod. Pro takto definované nové pojmy se potom dokáží všechny axiómy geometrie Lobačevského. Kdyby geometrie Lobačevského byla sporná, pak tento spor nastane i pro námi nově definované pojmy, tedy celý tento model by vedl ke sporu. To by však znamenalo spor v geometrii eukleidovské, neboť jejími prostředky jsme model sestrojili. Jinými slovy: důkaz sporu v geometrii Lobačevského by automaticky znamenal důkaz sporu v geometrii eukleidovské. Z bezespornosti geometrie eukleidovské tedy plyne i bezespornost geometrie Lobačevského.

Jak je vidět, tato metoda nám dává možnost dokazovat bezespornost jedné teorie za předpokladu, že druhá teorie je bezesporná. Aplikujeme-li tuto metodu na naši problematiku teorie množin, potom jestliže se nám podaří sestrojit v teorii množin (například ZF) model teorie množin ZF + hypotéza kontinua, pak je-li bezesporná teorie ZF, je bezesporná i po přidání dalšího axiómu, jímž je hypotéza kontinua. To však znamená, že hypotézu kontinua není možné z axiómů teorie ZF vyvrátit. Kdyby to bylo možné, pak by ZF + hypotéza kontinua byl sporný axiomatický systém; podle toho, co již bylo řečeno, by byl sporný už sám systém ZF.

Podobnou úvahu lze učinit i v ostatních případech, které se týkají jiných problémů.

Druhá metoda, jak se přesvědčit o nedokazatelnosti nějakého tvrzení z nějakých axiómů, je metoda, kterou budu nazývat metodou *matematicko-logickou.* Naším cílem je dokázat, že neexistuje nějaký důkaz. V tomto případě se pokusíme říci, co to vlastně důkaz je.

To znamená, že je nutno vytvořit matematickou teorii, která by pojem důkazu studovala, která by tento pojem matematizovala. Takovou teorií je matematická logika. Ukazuje se, že k důkazu v matematice stačí velmi chudý jazyk, který kromě základních, tzv. primitivních pojmů obsahuje už jen několik logických spojek, kvantifikátory, a několik pomocných znaků. Navíc důkazy v matematice jsou správné, jestliže jsou správné lokálně; to znamená, jestliže jednotlivé kroky důkazů jsou správně utvořeny, pak je správný i celý důkaz. Je možné popsat vlastnosti, které musí mít posloupnost znaků, aby byla důkazem nějakého tvrzení z nějakých axiómů. Jestliže tedy chceme dokázat, že neexistuje důkaz určitého tvrzení, pak dokazujeme, že neexistuje posloupnost znaků určitého tvaru. Při těchto úvahách tedy můžeme pracovat zcela matematicky a používat na důkazy neexistence takových posloupností nejrůznější matematické prostředky. (Mezi metody tohoto typu je možno zařadit též dobře známou metodu tzv. sémantických modelů.)

Použijeme-li matematicko-logickou metodu, pak ovšem mlčky předpokládáme, že neexistují jiné důkazy než ty, které jsou popsány omezenými prostředky matematické logiky; že mezi formálními důkazy a důkazy skutečnými je vzájemně jednoznačná korespondence. Tím vzniká dosti analogický vztah jako mezi intuitivní a axiomatickou teorií množin.

Navíc, jestliže dokážeme, že nějaký důkaz neexistuje, pak to dokazujeme opět z nějakých předpokladů, tedy v nějaké matematické teorii, o níž jsme nuceni předpokládat přinejmenším, že je bezesporná, neboť jinak by naše tvrzení nemělo žádnou cenu. Zde jsme dokonce nuceni předpokládat, že tato pomocná teorie dostatečně přesně odráží skutečnost.

Jak je vidět, nejsme schopni *dokázat absolutně* ani bezespornost určitého systému axiómů (až na několik triviálních případů). V každém takovém případě je nutno dodat, *jakými prostředky* byl důkaz proveden.

*

Zmíněné axiomatické systémy teorie množin vycházejí z jediného primitivního pojmu, kterým je *náležení.* Tedy vztah $X \in Y$ je jediný predikát vyskytující se v axiómech. Všechny ostatní jsou z něho již definovány.

To znamená, že budeme-li sestrojovat v axiomatické teorii množin nějaký model této teorie s nějakým dalším přidaným axiómem, pak jsme nuceni definovat nějakým způsobem nové množiny a mezi nimi nový vztah náležení, tedy nové $\in$, které často budeme značit $\in^*$.

Nejprve se budeme zabývat nedokazatelností axiómu výběru v jeho nejobecnějším tvaru.

Předpokládejme, že existuje množina x taková, že $x = \{x\}$, tedy x má jediný prvek a tím je opět x. Taková množina se nazývá *prvoelement*. Buď U množina všech prvoelementů, to jest

$$U = \{x; x = \{x\}\}.$$

Existence prvoelementů není v uvedených axiomatických systémech ani dokazatelná, ani vyvratitelná. Poměrně jednoduše se sestrojí model, kterým se dokáže bezespornost předpokladu, že U je nekonečná množina. Je možné zaručit bezespornost i jiných podobných množin, které jsou v jistém smyslu neregulární. Obecné podmínky, za jakých je možné takové modely konstruovat, nalezne čtenář v práci P. HÁJKA, uvedené v literatuře na konci tohoto článku.

Nyní tedy budeme předpokládat, že prvoelementy existují a dokonce, že množina U je nekonečná.

Vzájemné jednoznačné zobrazení množiny U na sebe budeme ve shodě s obvyklou terminologií nazývat též *permutací množiny* U. Buď p nějaká permutace množiny U. Potom je možno tuto permutaci rozšířit na vzájemné jednoznačné zobrazení $\bar{p}$, při němž *každá* množina má obraz i vzor. Je-li $x \in U$, pak $\bar{p}(x) = p(x)$ a konečně pro každé dvě množiny x, y je $x \in y$ právě tehdy, když $\bar{p}(x) \in \bar{p}(y)$. Takové zobrazení $\bar{p}$ se k dané permutaci p sestrojí transfinitní indukcí.

Množina všech permutací množiny U tvoří vzhledem k operaci skládání grupu.

Pro libovolnou množinu x definujeme *invariant množiny* x (označíme $\operatorname{Inv} x$) jako množinu všech permutací p množiny U, pro něž $\bar{p}(x) = x$. Snadno se dokáže, že pro každou množinu x je $\operatorname{Inv} x$ podgrupou grupy všech permutací množiny U.

Je-li x libovolná množina, pak *univerzum množiny* x (označení $\operatorname{Univ} x$) definujeme jako množinu všech u takových, že existuje konečná posloupnost $x_1, x_2, \dots x_n$ tak, že $u = x_1 \in x_2 \in \dots \in x_n = x$.

Řekneme, že množina x je *symetrická* (označení $\operatorname{Sym} x$), jestliže ke každému $y \in \operatorname{Univ} x$ existuje konečná $u \subset U$ taková, že každá permutace p množiny U, která je na u identická, je prvkem grupy $\operatorname{Inv} y$.

Snadno si každý ověří, že platí $\operatorname{Sym} U$. Je-li $\operatorname{Sym} x$, $y \in \operatorname{Univ} x$, pak je též $\operatorname{Sym} y$. Dále $u \subseteq U$ je symetrická právě tehdy, když je konečná, nebo když její komplement do U, tj. množina $U - u$ je konečná.

Prohlašme nyní za nové množiny pouze množiny symetrické. Nové $\in$ definujeme pro nové množiny X, Y tak, že $X \in^* Y$ právě když $X \in Y$. Tedy nové $\in$ je totožné s původním, pouze obor množin se zmenšuje.

Nyní je možno krok za krokem ověřit pro takto definované nové pojmy všechny axiómy teorie množin.

Jak jsme již řekli, množina U je symetrická, nachází se tedy mezi množinami našeho modelu, avšak v našem modelu jsou jen ty její části, které jsou konečné nebo jejichž komplementy do U jsou konečné.

Snadno se dokáže, že množina *je konečná ve smyslu modelu* právě tehdy, když je konečná. V našem modelu tedy platí věta: *Existuje nekonečná množina, jejíž každá část je buď konečná, nebo komplementem množiny konečné.* Je všeobecně známo, že pomocí axiómu výběru je možno tuto větu vyvrátit. To však znamená, že v našem modelu axióm výběru neplatí.

Pro zajímavost poznamenejme, že množina U má v našem modelu ještě další vlastnost. Není totiž ekvivalentní se žádnou svou vlastní podmnožinou. To znamená, že právě uvedená vlastnost v teorii množin, v níž nemáme axióm výběru, necharakterizuje plně konečné množiny.

Právě naznačená idea konstrukce modelu pochází od A. FRAENKELA. Tuto metodu podstatně zobecnil A. MOSTOWSKI (podstatně v tom smyslu, že jeho metodou lze dokázat řadu dalších nedokazatelností). Při definici symetrických množin (viz výše) není totiž nutné předpokládat, že množina u je konečná, ale pouze to, že náleží do ideálu jistých vlastností na Boolově algebře všech částí množiny U. Další podstatné zobecnění podal E. SPECKER, který tento ideál nahradil filtrem jistých vlastností na svazu všech podgrup grupy všech permutací. Konečně autor tohoto článku ve svém referátě na Mezinárodním matematickém kongresu v Nice 1970 naznačil ještě obecnější konstrukce modelů teorie množin za předpokladu, že množina U je nekonečná. Toto zobecnění spočívá v tom, že místo permutací množiny U se uvažují jisté imaginární permutace, které v teorii množin neexistují. O takových útvarech bude ještě v tomto článku zmínka.

*

Obraťme nyní pozornost na konstrukci modelu teorie množin, v němž axióm výběru platí, totiž k problému bezespornosti axiómu výběru.

Axiomatická teorie množin připouští množiny rozmanitého charakteru. O některých nám axiómy dají dostatek informací, jiné se mohou chovat dosti volně.

V jistém smyslu je zde podobná situace jako v některých algebraických teoriích, například v teorii algebraických těles. Zde víme zcela určitě, že existuje jednotka, nula, víme že existuje pětkrát za sebou sečtená jednotka (i když bez dalších informací nedovedeme rozhodnout, zda není náhodou rovna nule). Ovšem v takovém algebraickém tělese může nebo nemusí existovat též prvek odpovídající neurčité apod.

Položme si tedy otázku, které množiny nutně existují, neboť si je axiómy bezpodmínečně vynucují. Takovou množinou je například množina prázdná. Jestliže jsme již nějaké množiny sestrojili, pak nutně musí existovat též množina, která z nich vznikne nějakou operací, jejíž existence je zaručena axiómy. Jestliže jsme již sestrojili postupně nějaké množiny, pak axiómy teorie množin nás nutí k tomu přijmout i množinu, jejímiž prvky jsou právě všechny dříve sestrojené množiny. V tomto smyslu sestrojené množiny se nazývají *konstruktivní.*

Není jistě nutné zvlášť zdůrazňovat, že shora uvedený popis je velmi nepřesný, že se nedá v žádném případě chápat za definici konstruktivních množin. Nicméně podstata vytváření konstruktivních množin je tímto popisem znázorněna.

Operace, které vytvářejí konstruktivní množiny, umožňují to, že v našem konstruktivním procesu se žádná množina nevyskytne dříve než všechny její prvky. To znamená, že každý prvek konstruktivní množiny je opět konstruktivní množina. Rovněž se dá dokázat, že přirozená čísla a dokonce i všechna ordinální čísla, jsou konstruktivní množiny.

Samozřejmě, že se okamžitě nabízí otázka, zda každá množina je konstruktivní. Tvrzení, že každá množina je konstruktivní se nazývá *axióm konstruktivity.*

V teorii množin s axiómem konstruktivity je dokazatelný axióm výběru. To je celkem dosti přirozené, neboť výběrovou funkci F můžeme v tomto případě definovat tak, že pro X neprázdné je $F(X)$ první prvek množiny X, který se objeví v konstruktivním procesu vytváření množin.

Jestliže tedy sestrojíme model, v němž platí axióm konstruktivity, pak v něm platí též axióm výběru a bezespornost axiómu výběru s ostatními axiómy teorie množin je tím zaručena.

Takový model se sestrojí tím způsobem, že za nové množiny prohlásíme jen množiny konstruktivní; nové $\in$ definujeme pro konstruktivní množiny stejně, jako původní. Je možno též dokázat, že množina je konstruktivní ve smyslu tohoto modelu, právě když je konstruktivní v původní teorii. To znamená, že axióm konstruktivity v tomto modelu platí.

Je však možno dokázat mnohem více. *V teorii množin s axiómem konstruktivity je dokazatelná zobecněná hypotéza kontinua.* (Důkaz zde nebudeme ani naznačovat pro jeho značnou složitost.)

Autorem výsledků zde uvedených je K. Gödel. Přesné formulace a důkazy jsou obsaženy v jeho práci uvedené v seznamu literatury.

*

Jak již bylo řečeno, s axiómy teorie množin je bezesporná hypotéza kontinua a axióm výběru. Rovněž máme již prokázánu nedokazatelnost axiómu výběru, ovšem v případě, že v teorii množin existují množiny, které si jsou navzájem velmi podobné (prvoelementy). Zbývá tedy přesvědčit se o nedokazatelnosti hypotézy kontinua, respektive nedokazatelnosti existence výběrové funkce na velmi konkrétních množinách, např. $\mathscr{P}(\mathscr{P}(N))$. (Na množině $\mathscr{P}(N)$ výběrová funkce vždy existuje, neboť je-li $X \subseteq N$, X neprázdná, pak stačí zvolit $F(x) = \min X$.)

Víme již, že z bezespornosti teorie množin plyne též bezespornost teorie množin s axiómem konstruktivity. V teorii množin, obohacené o axióm konstruktivity, je potom dokazatelná hypotéza kontinua a axióm výběru. To znamená, že k řešení našeho problému je nutno především dokázat, že axióm konstruktivity není dokazatelný v teorii množin. To je jádro problému a na tuto otázku byla soustředěna pozornost.

Jde tedy o konstrukci modelu teorie množin, v němž neplatí axióm konstruktivity. Takový model je nutno opět sestrojit v teorii množin. O této teorii však předem nevíme, zda v ní náhodou axióm konstruktivity již neplatí. Jsme tedy nuceni alespoň mlčky axióm konstruktivity ve výchozí teorii množin předpokládat, neboť kdybychom udělali konstrukci, která vychází z jeho negace, nedokázali bychom nic nového.

Idea konstrukce musí tedy spočívat na adjunkci nějaké nekonstruktivní množiny, např. části množiny N k množinám konstruktivním. Taková adjunkce naráží na dvě potíže. Předně je problém, odkud adjungovanou množinu vzít, potom jak takovou adjunkci technicky provést, aby to, co nám vyjde, byl opět model teorie množin.

Zdálo by se, že konkrétní provedení adjunkce je záležitost už jen ryze technická. Pokusím se naznačit, že tomu tak není. Posloužíme si opět příkladem z algebry. Předpokládejme, že k nějakému algebraickému tělesu T chceme adjungovat neurčitou, a tím naše těleso zvětšit, tj. rozšířit do většího tělesa. Zvolíme tedy nějakou neurčitou a uvažujeme útvary, které jsou polynomy s koeficienty v základním tělese této jedné neurčité. Tyto polynomy nám už utvoří obor integrity díky komutativním, asociativním a distributivním zákonům, které platí v tělese T. Konstrukce podílového tělesa se potom už provede standardním způsobem. Kdybychom podobnou úvahu chtěli udělat pro teorii množin, pak jsme nuceni adjungované útvary brát mnohem složitější, neboť na rozdíl od oboru integrity, kde jsou nutné jen dvě operace, máme jich v teorii množin více; kromě toho nemáme k dispozici žádné jednoduché zákony, které by adjungované útvary převáděly na nějaký normální tvar, jakým jsou polynomy v případě rozšiřování tělesa. Navíc v případě, že rozšiřujeme těleso o neurčitou, nejsme nuceni brát žádný ohled na vztahy mezi touto neurčitou a prvky původního tělesa (i když takovou vazbu brát v úvahu můžeme). V případě teorie množin, kdybychom se pokoušeli adjungovat například nějakou část množiny N, pak to nemůže být neurčitá množina, neboť musí být např. číslo 1 jejím prvkem nebo prvkem jejího komplementu a podobně i pro další přirozená čísla. Přitom tato nová množina se nesmí rovnat žádné množině konstruktivní, neboť jinak by celá konstrukce neměla žádnou cenu.

První potíž, kde vzít množinu, kterou chceme adjungovat, je možno odstranit tím způsobem, že budeme v naší původní teorii předpokládat, že máme k dispozici model teorie množin, který je *spočetný*.

Je řada důvodů, které takový model ospravedlňují. Tyto důvody se zakládají v podstatě na různých modifikacích tzv. Löwenheim-Skolemovy věty. V tomto případě je poněkud rozdílná situace u axiomatického systému ZF a GB. Jak jsme již řekli, systém ZF má nekonečně mnoho axiómů. Kdyby byla v něm hypotéza kontinua dokazatelná, pak by byla dokazatelná už z konečně mnoha těchto axiómů. Stačil by nám v tomto případě jen spočetný model příslušného fragmentu, jehož existenci lze již zaručit. V případě GB existenci spočetného modelu dokázat neumíme. V tomto případě je nutno střídavě použít metodu matematicko-logickou s metodou relativní interpretace, pokud ovšem k axiómům GB nepřidáváme další axiómy týkající se existence nějakých zvláštních tříd.

Máme-li k dispozici spočetný model teorie množin, pak všech podmnožin množiny přirozených čísel, které jsou obsaženy v tomto modelu, je pochopitelně z hlediska celé teorie jen *spočetně mnoho* (i když z hlediska modelu jich spočetně mnoho není). Zbývá nám tedy dostatek množin, které se můžeme pokusit k našemu modelu adjungovat. Takový pokus se skutečně zdařil. *Bylo ukázáno, že k našemu spočetnému modelu lze adjungovat dostatečně mnoho těchto množin, takže ve výsledném modelu jejich počet přesáhne první nespočetné kardinální číslo* $\aleph_1$ (z axiómu výběru plyne existence nejmenší nespočetné množiny). Navíc se dají tyto množiny adjungovat takovým způsobem, že jejich vzájemné vazby jsou minimální, takže na výsledném modelu je možno pro ně použít podobné ideje jako v metodě Fraenkel-Mostowského pro prvoelementy (ne pro adjungované podmnožiny množiny N, ale až pro jisté množiny těchto množin).

Tímto způsobem se tedy prokazuje nedokazatelnost hypotézy kontinua a axiómu výběru.[1])

Autorem těchto výsledků je P. J. COHEN. Jeho metody jsou popsány v jeho knize uvedené v literatuře na konci tohoto článku.

Modely, které jsme dosud popisovali, měly všechny tu vlastnost, že jejich relace $\in^*$ byla totožná s původní relací $\in$. Rozhodně není bez zajímavosti otázka, zda existují také modely, jejichž relace $\in^*$ se nedá žádným izomorfismem redukovat na původní relaci $\in$. Takové modely se nazývají *nestandardní.* V nestandardních modelech se může už dosti podivně chovat množina přirozených čísel. Přirozená čísla takového modelu nemusejí nutně být izomorfní s přirozenými čísly v původní teorii. To znamená, že může existovat část těchto přirozených čísel, která je neprázdná a přitom nemá první prvek. Taková část nemůže být ovšem množinou tohoto modelu. Modely tohoto druhu je možno sestrojit tzv. metodou altraproduktu. Důležité je, že u takových modelů je teoretická možnost adjungovat k nim novou množinu přirozených čísel. (Má-li se adjunkce zdařit, pak samozřejmě tato množina musí mít první prvek a ještě řadu dalších vlastností.)

Autor tohoto článku přizpůsobil Cohenovu metodu adjunkce pro případ nestandardních modelů. Tím se podařilo z celého Cohenova důkazu odstranit mezičlánek spočetného modelu a celý důkaz nedokazatelnosti hypotézy kontinua a axiómu výběru je tedy možno provést metodou relativní interpretace tak, jako tomu je v případech bezespornosti těchto axiómů u Gödela nebo v metodě Fraenkel-Mostowského.

[1]) Dosud není známo, zda v teorii množin s axiómem výběru není přece jen dokazatelná jistá velmi slabá forma hypotézy kontinua, a to: Existuje množina X tak, že každá část množiny $\mathscr{P}(X)$ je buď ekvivalentní s $\mathscr{P}(X)$, nebo s nějakou částí X.

Navíc, poněvadž adjunkce v případě nestandardních modelů byla velmi složitá, zjistilo se, ve snaze celou konstrukci zjednodušit, že adjungované útvary lze popsat ve velmi jednoduchém normálním tvaru, který je použitelný jak na modely spočetné, tak na modely nestandardní. Tím se podstatně zjednoduší všechny důkazy.

*

Metody užité při řešení prvního Hilbertova problému podstatně obohatily matematiku. Tím význam tohoto problému přerostl jen charakter obtížné úlohy a v tom je patrně nutno v současné době vidět hlavní význam práce vykonané na této problematice.

První Hilbertův problém je možno považovat za rozřešený, i když řešení není dáno v tom smyslu, jak byl problém položen. Byla vlastně dokázána neřešitelnost původního Hilbertova problému.

Kromě problému kontinua a problému výběru bylo řešeno ještě mnoho dalších problémů teorie množin analogickým způsobem.

Vyřešením problému se sice uzavírá určitá část matematiky, ale otevírá se zároveň problematika nová. Rozšiřování teorie množin o nové množiny dalo vznik nové matematické teorii, tzv. teorii polomnožin, která rozšiřuje obor studovaných množin o nové objekty, tzv. polomnožiny, které je možno chápat jako jakési imaginární množiny; s jejich užitím je možno dokazovat věty o množinách. O polomnožinách bude vydána kniha, kterou spolu s P. Hájkem napsal autor tohoto článku.

Při rozvoji metod konstrukce modelů teorie množin i při důkazech bezespornosti různých tvrzení teorie množin odvedla kus tvrdé a poctivé práce též skupina československých matematiků.

Literatura

P. J. Cohen: *Set theory and the continuum hypothesis*, W. A. Benjamin 1966.

K. Gödel: *The consistency of the axiom of choice and the generalized continuum hypothesis*, Princeton University Press 1940.

P. Hájek: Modelle der Mengenlehre,..., Zeitschrift für Math. Logik und Grundlagen der Mathematik *11* (1965), 103—115.

A. Lindenbaum - A. Tarski: Communication sur les recherches de la Théorie des ensembles, Comptes Rendus de la Société des Sciences et de Lettres de Varsovie, Classe III. (1924) str. 314.

E. Specker: Zur Axiomatik der Mengenlehre, Zeitschrift für Math. Logik und Grundlagen der Mathematik *3* (1957), 173—210.

P. Vopěnka: General theory of ∇-models, CMUC *8* (1967), 145—170.