Jiří Bečvář

O druhém Hilbertově problému (Otázka bezespornosti aritmetiky)

Pokroky matematiky, fyziky a astronomie, Vol. 16 (1971), No. 5, 225--237

Persistent URL: http://dml.cz/dmlcz/139356

POKROKY MATEMATIKY, FYZIKY A ASTRONOMIE
ROČNÍK XVI – ČÍSLO 5

HILBERTOVY PROBLÉMY

O DRUHÉM HILBERTOVĚ PROBLÉMU

(*Otázka bezespornosti aritmetiky*)

JIŘÍ BEČVÁŘ, Praha

1. Druhý z třiadvaceti problémů, na které se David Hilbert soustředil ve své přednášce na 2. Mezinárodním matematickém kongresu v Paříži v r. 1900, je formulován jako problém důkazu bezespornosti aritmetiky ([7]). Aritmetikou přitom Hilbert rozuměl aritmetiku reálných čísel (kontinua), vybudovanou na základě vhodného axiomatického systému. (Hilbert sám navrhl takový axiomatický systém v práci [6], uveřejněné v témže roce; reálná čísla jsou zde vymezena jako soubor objektů, které tvoří archimedovsky uspořádané těleso, přičemž speciálním axiómem je navíc vysloven požadavek, aby uvažovaný soubor nebylo možno rozšířit o další objekty tak, že by zůstaly splněny ostatní axiómy.)

Problém bezespornosti aritmetiky patří svou povahou do oblasti tzv. základů matematiky a souvisí s řadou dalších problémů, které se týkají logické výstavby matematiky a obecné metodologie deduktivních věd vůbec. O některých z těchto otázek hovoří i Hilbert, a to již v úvodu své přednášky (viz překlad v [8]). Další jsou zahrnuty přímo v části, která je věnována 2. problému. Vybudovat základy nějaké vědní disciplíny znamená podle Hilberta udat systém axiómů, které „přesně a úplně" vyjadřují vztahy, jimiž jsou mezi sebou svázány objekty a základní pojmy uvažované disciplíny. Za „správné" se pak považují pouze ty její věty, které lze odvodit z axiómů konečným počtem přísně logických úsudků. Systém axiómů představuje tzv. implicitní definici základních pojmů disciplíny. Problém bezespornosti spočívá v důkazu toho, že pomocí konečně mnoha logických úsudků nelze z axiómů odvodit důsledky, které by si navzájem odporovaly (Hilbert ve své přednášce ještě nespecifikuje prostředky, kterých je dovoleno při důkazu bezespornosti použít).

Bezespornost systému axiómů je logicky nutná podmínka pro to, aby axiómy mohly vůbec něco přesně a úplně charakterizovat. Avšak pro Hilberta měly důkazy bezespornosti i jiný aktuální význam. Věřil, že pomocí důkazu bezespornosti je možno se vyhnout námitkám proti přiznání samostatné existence některých, přede-

vším transfinitních objektů a pojmů (např. i kontinua), které tehdy vyslovovali zvláště odpůrci rozvíjející se teorie množin. Podle Hilberta: Jestliže souboru objektů, resp. pojmů jsou systémem axiómů přisouzeny takové vlastnosti, že z axiómů lze odvodit spor, pak tento soubor jako celek „matematicky neexistuje". Naopak jestliže se podaří dokázat, že systém axiómů je bezesporný, je tím zároveň (z hlediska matematiky) dokázána existence souboru.

V době, kdy Hilbert formuloval své problémy, nebylo možné předvídat, jak složitý bude další vývoj v oblasti základů matematiky a jak hluboké a často nečekané výsledky přinese. V r. 1900 neexistovalo ještě striktní odlišení čistě formálních a obsahových stránek axiomatických teorií; nebyly ještě objeveny nejzávažnější paradoxy teorie množin a neexistovala axiomatická teorie množin; neexistoval přesný matematický ekvivalent pojmu algoritmu; nebyla vymezena hranice mezi jazykem, ve kterém formulujeme matematické výsledky, a mezi metajazykem, v němž o těchto výsledcích hovoříme; bylo mnohem méně jasné, než je nyní, kde vede dělicí čára mezi matematikou a logikou. Tyto otázky se vyjasňovaly postupně. Přitom Hilbertovy ideje a výsledky měly na způsob jejich řešení podstatný vliv. Ve dvacátých letech se Hilbert znovu vrátil k problému bezespornosti axiomatických teorií. Byl zejména podnícen kritikou, se kterou vystoupili intuicionisté (BROUWER, WEYL) proti nekonstruktivnímu zacházení s nekonečnými matematickými objekty, jež je typické např. pro úvahy v teorii množin a v matematické analýze, a vytyčil zpřesněný program. Jeho cílem bylo podat takové důkazy bezespornosti axiomatických systémů pro základní matematické disciplíny, při kterých mělo být použito pouze kombinatorických, ryze konstruktivních resp. „finitních" vnějších prostředků; axiomatizace byla zároveň v souhlasu s tím nahrazena tzv. formalizací. Tím měly být klasické matematické pojmy a důkazové metody nenapadnutelným způsobem zabezpečeny alespoň zevně; navíc podle Hilbertova pojetí tak měla být prokázána matematická existence příslušných objektů, resp. pojmů.

V rámci tohoto programu se úsilí Hilbertovo a jeho žáků nakonec soustředilo především na důkaz bezespornosti formálního systému pro aritmetiku přirozených čísel. Speciální výsledky, kterých přitom dosáhli ACKERMANN a VON NEUMANN, vzbudily přesvědčení, že by bylo snadné je rozšířit tak, aby daly požadovaný důkaz bezespornosti pro aritmetiku přirozených čísel v plném rozsahu (srov. k tomu [1]). Toto přesvědčení se později ukázalo mylné. Vyplynulo to z tzv. GÖDELOVY 2. věty, publikované v r. 1931 v práci [5], podle které bezespornost formálního systému, jenž stačí k vybudování aritmetiky přirozených čísel (takovým systémem je ovšem např. i formální systém teorie množin), nelze dokázat vnějšími prostředky, které by bylo možno adekvátně formalizovat v rámci systému samého. Z tohoto výsledku definitivně plyne, že pro „zabezpečení" klasických matematických disciplín nemohou mít důkazy bezespornosti ten dosah, který jim Hilbert přikládal ve formulaci svého programu.

Z Gödelovy věty na druhé straně bezprostředně neplyne, že by např. pro aritmetiku nemohl existovat „finitní" důkaz bezespornosti. Možnost takového důkazu závisí na tom, co rozumíme pod finitními prostředky. Jestliže bychom za finitní pokládali

pouze ty prostředky, které lze adekvátně vyjádřit v samotném systému formální aritmetiky (takové stanovisko se zdá být přirozené vzhledem k možnosti tzv. aritmetizace syntaxe běžných formálních teorií), pak ovšem z uvedené Gödelovy věty plyne, že finitní důkazy bezespornosti nejsou obecně možné. Ve skutečnosti však pojem finitnosti, resp. konstruktivnosti používaných prostředků nebyl v Hilbertově škole a patrně ani nikdy později zcela jednoznačně vymezen. Zbývá pak možnost, že existují důkazy bezespornosti, které sice používají prostředků přesahujících rámec možností formální aritmetiky, které však zároveň z intuitivního hlediska mají v nějakém přijatelném smyslu konstruktivní charakter. Takový důkaz bezespornosti pro formální systém aritmetiky přirozených čísel uveřejnil jako první v r. 1936 GENTZEN v práci [4]. Později byly publikovány obdobné důkazy další, mj. také pro různé částečné systémy aritmetiky reálných čísel.

V dalších odstavcích se pokusíme zjednodušenou formou osvětlit alespoň některé z otázek, které podstatně souvisí s problémem axiomatické, resp. formální charakterizace aritmetiky, a naznačit cestu, která vede jednak ke 2. Gödelově větě, jednak k důkazu bezespornosti aritmetiky. Omezíme se přitom na aritmetiku přirozených čísel, která má v okruhu těchto otázek ústřední postavení.

2. Naše matematická představa přirozených čísel, která se vyvinula na základě konkrétních operací čítání konečných souborů diskrétních objektů makrosvěta, který nás obklopuje, a na základě rozlišování těchto souborů podle jejich mohutnosti, má zdánlivě zcela neotřesitelnou intuitivní evidenci. Při unárním zápisu, kdy číslo $n \geqq 0$ je reprezentováno $n + 1$ čárkami $|||\ldots||$, je dokonce možno generovat každé přirozené číslo zcela uniformním konstruktivním procesem postupného přidávání čárky, který je věrnou paralelou procesu čítání. Jediná „potíž" u přirozených čísel na této elementární úrovni jejich chápání spočívá v tom, že jich není konečně mnoho. Uniformita jejich vytváření je tak sugestivní, že proveditelnost lokální operace připsání další čárky za předpokladu, že jsme již na konci unárního zápisu čísla, vede nezadržitelně k abstraktnímu závěru, že ke každému číslu lze utvořit jeho následníka (přitom takového, aby byl různý od všech čísel menších). Vzniká pak otázka, zda lze přirozená čísla charakterizovat jinak než pomocí fráze o „konečném počtu opakování" operace následníka.

Na trochu vyšší úrovni narazíme na komplikace další. S přirozenými čísly neprovádíme pouze operaci následníka, ale např. i operace sčítání a násobení. Zároveň kromě základního predikátu rovnosti uvažujeme také jiné jednomístné i vícemístné predikáty jako např. „$x < y$", „x dělí y", „x je prvočíslo". Z již vytvořených operací a predikátů různými typy definic konstruujeme další operace a predikáty, přičemž k jejich výstavbě navíc používáme logických částic: výrokových spojek $\neg$, $\vee$, $\&$, $\rightarrow$, $\leftrightarrow$ a kvantifikátorů $\exists$ (existuje), $\forall$ (pro všechna). Tyto částice ve spojení s operacemi a predikáty umožňují na každé dosažené úrovni tvořit věty. Na věty se můžeme dívat jako na otázky. V rámci naší intuitivní představy (kterou uplatňujeme — a rozšiřujeme — při definici každého nově zaváděného pojmu) jsme při klasické

interpretaci logických částic přesvědčeni o tom, že na každou takovou otázku existuje jednoznačná kladná nebo záporná odpověď (tj. o tom, že věta je v oboru přirozených čísel pravdivá či ne). Zároveň však naše schopnost víceméně mechanického kombinatorického tvoření otázek zdaleka přesahuje naši schopnost transformovat intuici, která provázela základní vlastnosti, resp. definice pojmů zahrnutých v otázce, do takového tvaru, který by dovolil jednoduše najít odpověď. Klasickým příkladem je Fermatova věta.

Jediný možný způsob, jak tuto obtíž obejít, spočívá v rozložení cesty za odpovědí na jednotlivé kroky, jejichž složitost odpovídá tomu, co jsme schopni v jednom kroku skutečně s porozuměním provést. To je jeden z podstatných rysů deduktivní metody. Vzniká pak otázka, zda ze souboru vět aritmetiky lze vybrat poměrně jednoduché jádro (axiómy), ze kterého by bylo možno pomocí tzv. univerzálně platných deduktivních pravidel odvodit všechny známé pravdivé věty, přitom však žádnou větu, která je v oboru přirozených čísel nepravdivá. Které věty však máme pokládat za „skutečné" věty o přirozených číslech? V aritmetice se často hovoří i o třídách podle relací ekvivalence, uvažují se libovolné množiny přirozených čísel a „obecné" aritmetické funkce. Dává naše elementární intuitivní představa o přirozených číslech dostatečný podklad pro stanovení, které z vět obsahujících tyto pojmy jsou pravdivé? V uvedených případech jsou totiž na přirozená čísla aplikovány pojmy v podstatě množinového charakteru. Je zřejmě zvlášť významné pokusit se o axiomatizaci tzv. čisté aritmetiky, tj. zhruba řečeno té části aritmetiky, v jejíchž větách se tyto pojmy explicitně nevyskytují.

Axiomatizace čisté aritmetiky by byla relativně ke svým vyjadřovacím prostředkům po obsahové stránce už velmi uspokojivá, kdyby každá věta, kterou lze v jejím jazyce formulovat, byla v ní dokazatelná právě tehdy, když je pravdivá v oboru přirozených čísel. Pak by pro každou takovou větu platilo, že buď ona, nebo její negace je dokazatelná. Dejme tomu, že bychom takovou axiomatizaci našli. Můžeme potom zpětně položit otázku, nakolik axiómy a jejich důsledky jakožto implicitní definice (viz odst. 1) „přesně a úplně" vystihují představu přirozených čísel, ze které jsme vyšli. Přitom slovům „přesně a úplně" chceme v případě aritmetiky (podobně je tomu u geometrie) rozumět v ostřejším smyslu než třeba v případě axiomatizace pojmu metrického prostoru nebo grupy, který je pro nás adekvátně vystižen právě tím, jak jsme pro něj stanovili axiómy. V případě přirozených čísel bychom totiž vzhledem k silnému dojmu o jedinečnosti matematické struktury, kterou tvoří, chtěli najít takovou axiomatizaci, která by navíc měla vlastnost tzv. kategoričnosti, tj. vlastnost, že každé dva modely axiomatického systému jsou izomorfní (a tedy všechny modely jsou izomorfní s intuitivním modelem, který je tvořen běžnými přirozenými čísly).

Aby úvahy tohoto druhu měly obvyklý matematický charakter a standard, bylo nejdříve třeba vybudovat metamatematiku, tj. matematickou teorii axiomatických teorií. Pojem intuitivní pravdivosti věty nějaké axiomatické teorie je v ní nahrazen matematicky definovaným pojmem pravdivosti věty v různých modelech této teorie. Aby při odvozování vět v axiomatických teoriích nebylo použito úsudků, resp. prostředků, které samy závisí na obsahu toho, co axiomatizujeme.

je dále do každé axiomatické teorie vložena i nějaká forma axiomatizace samotné logiky, tj. axiomatizace toho, co je univerzálně platný deduktivní úsudek. Ukazuje se pak, že při vhodném zápisu vět takové teorie má každý krok v dedukci uvnitř teorie čistě formální konstruktivní charakter, tj. závisí pouze na vnějším tvaru (syntaxi) konečně mnoha vět v něm použitých. Protože všechny věty lze vybudovat z pevného konečného počtu symbolů, lze se na celý proces dedukce v axiomatické teorii dívat jako na operování s konkrétními konečnými objekty, které má ve striktním slova smyslu finitní, konstruktivní charakter a které by za nás zásadně mohl provádět počítač. Tím nakonec dostáváme formalizovanou (axiomatickou) teorii. Takové teorie zkoumáme matematicky.

Jeden z hlavních výsledků metamatematiky spočívá ve zjištění, že jednotlivé z požadavků, které bychom (po jejich náležitém zpřesnění) chtěli klást na dokonalou axiomatizaci, už u tak základní matematické struktury, jakou tvoří přirozená čísla (tím spíš reálná čísla nebo množiny), dokazatelně nelze všechny současně splnit. Ať už si myslíme o jednoznačnosti naší intuitivní představy přirozených čísel cokoliv, nedokážeme jednoznačně charakterizovat jejich strukturu a množinu vět, které jsou pro ně pravdivé, konstruktivním deduktivním způsobem, přestože dokazování je pro nás v matematice hlavní exaktní postup. Zůstane jím zřejmě i nadále, ale musíme počítat s tím, jaké jsou hranice jeho možností.*)

Studium základů matematiky ukázalo, že u všech matematických teorií jde o souhru intuitivního a formálního, ve které oba partneři jsou nepostradatelní a ve které neexistují absolutní řešení. Nedovedeme samy sebe zvednout i se židlí, na které sedíme (fyzika je v situaci ještě obtížnější). Přesto má studium formalizovaných axiomatických teorií hluboký smysl, neboť vyjasňuje náš vztah k intuici a realitě a dovoluje nalézat možnosti a hranice závažné hry na hypotézy, kterou axiomatická metoda představuje. Ukazuje se přitom, že je třeba stále konfrontovat formalizované důkazy s obsahovými, neformalizovanými, a srovnávat výsledky dosažené s použitím klasické logiky (pro kterou je charakteristické mj. neomezené používání principu „tertium non datur") s výsledky, k nimž dospívá neaxiomatizované ryze konstruktivistické, resp. intuicionistické pojetí výstavby matematiky.

V tomto článku jsme ponechali stranou intuicionistické pojetí; poznamenejme pouze, že tam, kde metamatematika klade důraz na finitní metody, používá prostředků velmi blízkých intuicionistickým. Nechali jsme také stranou otázky, které souvisí s relativními důkazy bezespornosti a s pojmem tzv. syntaktického modelu formalizované teorie, přestože tento pojem má v kontextu snah o úplnou charakterizaci matematických objektů základní význam.

3. Ve standardních matematických textech, které se explicitně nezabývají logikou, bývá pro přirozená čísla téměř výhradně uváděn neformalizovaný axiomatický systém, založený na tzv. PEANOVÝCH axiómech. Struktura přirozených čísel je přitom

*) Např. v teorii množin, kde prvotní intuice se po nalezení paradoxů ukázala nespolehlivou, je patrné, že axiomatické pojetí musíme vzít právě za základ. (Zvlášť v takovém případě by měl alespoň důkaz bezespornosti velmi aktuální smysl. Pro teorii množin nebyl zatím důkaz podán, ale lze očekávat, že by vyžadoval použití tak mohutných prostředků, že bychom stěží dovedli interpretovat, čeho jsme přitom dosáhli.)

dána trojicí $\langle N, 0, S\rangle$, pro kterou platí:

(P0) N je množina, 0 je její prvek a S je zobrazení množiny N do sebe (funkce „následník").

(P1) Pro všechna $x \in N$ jest $S(x) \neq 0$.

(P2) Pro všechna $x, y \in N$ platí, že jestliže $S(x) = S(y)$, pak $x = y$.

(P3) Pro každou množinu $A \subseteq N$ platí: Jestliže $0 \in A$ a jestliže pro každé x platí, že z $x \in A$ plyne $S(x) \in A$, pak $A = N$.

Peano převzal tyto axiómy (uvedli jsme je v poněkud modifikovaném tvaru) od DEDEKINDA, který v práci [2] přirozená čísla v podstatě právě těmito vlastnostmi jako první skutečně matematicky definoval (vedle Fregeho, jehož zavedení přirozených čísel však vychází z jiného základu). Uvedený systém označme P.

Předpokládané matematické prostředky, pomocí kterých axiomatizujeme strukturu přirozených čísel, mohou být různé. Systém P v uvedeném tvaru představuje matematickou definici, která používá jako předpokládané výchozí prostředky intuitivní teorii množin (funkci můžeme pokládat za množinu uspořádaných dvojic). V rámci tohoto neformalizovaného(!) vnějšího pojmového lešení je možno dokázat (udělal to již Dedekind), že systém P je kategorický v následujícím smyslu: Dvě trojice $\langle N, 0, S\rangle$, $\langle N', 0', S'\rangle$, které obě splňují axiómy (P0) až (P3), jsou izomorfní, tj. existuje vzájemně jednoznačné zobrazení f množiny N na množinu N' takové, že $f(0) = 0'$ a že pro každé $x \in N$ platí $f(S(x)) = S'(f(x))$. Dosáhnout tohoto výsledku je umožněno právě zvolenou formulací axiómu indukce (P3) (který v moderní terminologii říká, že algebra $\langle N, 0, S\rangle$ nemá vlastních podalgeber). Jakkoliv se nám tato formulace dnes zdá samozřejmá, bylo velkým výkonem Dedekindovým, že na ni přišel, a dalo mu to podle jeho vlastního svědectví značnou práci (srov. Dedekindův dopis citovaný v [11]). Šlo o to vyloučit možnost, že by množina přirozených čísel obsahovala kromě prvků, které lze získat z nuly „konečným počtem kroků" (této formulace při axiomatizaci právě nechceme použít), spočívajících v tvoření následníka, ještě další nežádoucí prvky. Později se však ukázalo, že uvedený výsledek nemá (po provedení formalizace) tak absolutní platnost, jak by se zdálo.

Systém P má tu význačnou vlastnost, že i když je v něm explicitní zmínka pouze o funkci S, lze dokázat (opět s použitím obecných vlastností množin, a to za předpokladu, že nějaká trojice $\langle N, 0, S\rangle$ s vlastnostmi (P0) až (P3) existuje), že na N existují funkce „součet" a „součin" a jsou jednoznačně určeny vlastnostmi (tzv. rekursivními definicemi):

$$\text{(A)} \quad \begin{aligned} 0 + y &= y \\ S(x) + y &= S(x + y) \end{aligned} \qquad \text{(M)} \quad \begin{aligned} 0.y &= 0 \\ S(x).y &= x.y + y \end{aligned}$$

Podobně lze dokázat na množině N existenci všech funkcí běžně v aritmetice používaných. (Tyto funkce patří vesměs do třídy tzv. primitivně rekursivních funkcí.)

Chceme-li explicitně zachytit všechny matematické (množinové) prostředky, které při odvozování vět o přirozených číslech pomocí systému P používáme, můžeme

to udělat tak, že axiomatizujeme (a pak formalizujeme) teorii množin. Přitom k odvození všech běžných vět čisté aritmetiky stačí pouze fragment teorie množin. (Nepotřebujeme např. axióm výběru ani tzv. obecný axióm substituce; k důkazu samotné existence množiny přirozených čísel – tj. přesněji nějaké trojice $\langle N, 0, S\rangle$, která splňuje axiómy (P0) až (P3) – však nutně potřebujeme axióm, který říká, že existuje nějaká nekonečná množina. Vlastnosti požadované našimi axiómy bude pak mít např. množina $N = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \ldots\}$.) Formalizaci potřebné části teorie množin (dokonce celé teorie množin) je možno provést již v rámci tzv. elementární predikátové logiky. Nechceme-li přitom vůbec celou aritmetiku budovat uvnitř teorie množin a chceme-li naopak z teorie množin použít pokud možno málo, můžeme např. sestrojit formalizovaný systém P_1, ve kterém v podstatě zůstanou zachovány axiómy systému P (obohacené o vztahy (A), (M) a event. některé další) a který navíc bude obsahovat matematické axiómy, týkající se vlastností množin základních individuí systému. Množiny i „skutečná" individua (která mají představovat přirozená čísla) budou přitom v P_1 uvažovány na stejné logické úrovni, takže axióm úplné indukce (P3) bude vyjádřen jako jediná věta o všech nespočetně mnoha podmnožinách $A \subseteq N$. (Z nich však lze ve formalizované teorii skutečně „pojmenovat" – a tedy i definovat – pouze nejvýš tolik, kolik máme výrazů, tj. spočetně mnoho.) Pro systém tohoto druhu, který spolu s aritmetikou obsahuje fragment teorie množin, byl podán důkaz bezespornosti; není však konstruktivní ([10]). K systému P_1 ještě poznamenejme, že jako u všech dostatečně silných formalizací aritmetiky i v P_1 budou existovat tzv. deduktivně nerozhodnutelné aritmetické věty (viz odst. 4).

Množinové prostředky použité v systému P je alternativně možno přesunout do výstavby systému logiky, které přitom používáme. Dostaneme tak formální systém aritmetiky P_2, který používá tzv. predikátové logiky 2. stupně (v ní je dovoleno kvantifikovat predikáty) a ve kterém axióm indukce opět jakožto jedna věta bude zhruba znít: „Pro každou vlastnost (predikát) A platí: Jestliže 0 má vlastnost A atd.". Predikátová logika 2. stupně má však přitom proti elementární tu zásadní nevýhodu, že není v běžném smyslu úplná, tj. při žádné rozumné její axiomatizaci nelze dokázat všechny identicky pravdivé věty, které je možno v jejím jazyce formulovat. Systém P_2 bude sice kategorický, ale v tom omezeném smyslu, že budou navzájem izomorfní jen všechny jeho tzv. standardní modely.

4. Pojem množiny je složitější než pojem přirozeného čísla. Proto se hledala cesta, jak axiomaticky charakterizovat přirozená čísla bez explicitního použití množinových prostředků. Hilbertova metoda formalizace, která měla umožnit finitní důkazy bezespornosti, zároveň naznačovala způsob, jakým směrem takovou axiomatizaci hledat. Podstata spočívá v tom, že axióm indukce se nahradí nekonečně mnoha axiómy, které odpovídají všem těm vlastnostem objektů, jež dovedeme vyjádřit v jazyce elementární predikátové logiky. Zároveň nastanou jisté změny ohledně $N, S, ., +$. Popišme stručně nejznámější takový formalizovaný systém Z pro aritmetiku přirozených čísel.

Výrazy systému Z jsou konečné posloupnosti, sestavené z konečně mnoha symbolů, jimiž jsou 0, S, $+$, $.$, $=$, v, $|$, logické částice a závorky (,). Výrazy v, $v|$, $v||$, ... nazveme (individuové) proměnné. Pišme je obecně x, y apod. Ze symbolů 0, S, $+$, $.$, závorek a proměnných jsou utvořeny tzv. termy, např. $((v + SS0).v|)$. Speciální termy 0, $S0$, $SS0$, ... nazveme číslovky. Výrazy tvaru $u = v$, kde u, v jsou termy, nazveme primitivní formule. Z primitivních formulí jsou pak pomocí logických částic a závorek běžným způsobem vytvořeny tzv. (dobře utvořené) formule. Formuli, ve které výskyt každé proměnné je vázán nějakým kvantifikátorem, nazveme větou systému Z.

Matematickými axiómy systému Z jsou všechny formule, které jsou jednoho z následujících tvarů (s jistými licencemi v používání závorek):

(Z1) $\forall x \neg (Sx = 0)$

(Z2) $\forall x \forall y (Sx = Sy \to x = y)$

(Z3) $\forall y (0 + y = 0)$

(Z4) $\forall x \forall y (Sx + y = S(x + y))$

(Z5) $\forall y (0.y = 0)$

(Z6) $\forall x \forall y (Sx.y = x.y + y)$

(Z7) $(\mathfrak{A}(0) \,\&\, \forall x (\mathfrak{A}(x) \to \mathfrak{A}(Sx))) \to \forall x \mathfrak{A}(x)$

Přitom $\mathfrak{A}$ v (Z7) probíhá všechny formule s volnou proměnnou x, tj. (Z7) je schéma.

Logickými axiómy systému Z budou všechny formule systému Z, které mají stejný tvar jako axiómy elementární predikátové logiky s rovností při některé z jejích standardních axiomatizací.

Výběru axiomatizace logiky pak odpovídá výběr konečně mnoha tzv. odvozovacích pravidel systému Z, která stanoví, kdy lze z daných (konečně mnoha) formulí jedním krokem přejít k nové formuli. Pravidlem bývá často např. modus ponens, při kterém z formulí $\mathfrak{A}$, $\mathfrak{A} \to \mathfrak{B}$ můžeme odvodit $\mathfrak{B}$, nebo pravidlo, které říká, že z formule $\mathfrak{A} \to \mathfrak{B}$ můžeme odvodit formuli $(\exists x \mathfrak{A}) \to \mathfrak{B}$ za předpokladu, že proměnná x se nevyskytuje jako volná v $\mathfrak{B}$. S použitím odvozovacích pravidel se pak běžným způsobem definuje (v metajazyce), kdy konečná posloupnost $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ formulí je v Z důkazem formule $\mathfrak{A}_k$. Formule $\mathfrak{A}$ je v Z dokazatelná, jestliže má v Z důkaz. Pišme to (opět v metajazyce) ve tvaru $\vdash \mathfrak{A}$.

Všimněme si, že symbol, který by odpovídal množině N z odst. 3, se v Z explicitně nevyskytuje. Za model systému Z pokládáme jakoukoliv pětici $M = \langle N_M, 0_M, S_M, +_M, \cdot_M \rangle$ takovou, že N_M je množina, 0_M její prvek, S_M, $+_M$, $\cdot_M$ jsou unární, resp. binární operace na N_M a platí, že jestliže symboly 0, S, $+$, $.$ systému Z interpretujeme jakožto 0_M, S_M, $+_M$, $\cdot_M$, pak jestliže hodnoty kvantifikovaných proměnných omezíme na prvky z N_M, přejdou všechny matematické axiómy systému Z ve věty, které jsou pravdivé v N_M (logické axiómy budou přitom automaticky pravdivé při libovolném dosazení jmen prvků z N_M za event. volné proměnné v nich). Snadno se ukáže, že každá

věta, která je dokazatelná v Z, je pravdivá v každém modelu systému Z. Z úplnosti elementární predikátové logiky (kterou dokázal Gödel v r. 1930) plyne významný výsledek, že pro Z platí i obrácené tvrzení. Tedy jestliže nějaká věta $\mathfrak{A}$ systému Z je v Z nedokazatelná, existuje model M, ve kterém není pravdivá. Jestliže je $\mathfrak{A}$ v Z navíc deduktivně nerozhodnutelná, tj. jestliže ani věta $\neg\,\mathfrak{A}$ není v Z dokazatelná, pak existuje model M', ve kterém $\neg\,\mathfrak{A}$ není pravdivá, tj. ve kterém $\mathfrak{A}$ je pravdivá. Za předpokladu bezespornosti systému Z taková deduktivně nerozhodnutelná věta existuje. (To je obsahem ROSSEROVA zesílení Gödelovy tzv. 1. věty o neúplnosti, publikované v [5], které platí mj. pro systém Z a jeho axiomatizovatelná rozšíření.) Modely M, M' jsou pak neizomorfní, neboť v izomorfních modelech jsou pravdivými přesně stejné věty systému Z. Tedy je-li systém Z bezesporný, není kategorický.

Poznamenejme, že přítomnost axiómů (Z3) až (Z6) pro součet a součin je pro systém Z (na rozdíl od dříve uvažovaného systému P) podstatná. Naproti tomu všechny ostatní běžné aritmetické funkce (dokonce: rekursivní funkce) lze již v Z „reprezentovat", a to v následujícím smyslu: Pro každé přirozené číslo n nechť $\bar{n}$ značí odpovídající číslovku systému Z; tedy např. $\bar{2}$ značí $SS0$. Pak ke každé rekursivní (tj. algoritmicky vyčíslitelné) funkci f o k argumentech existuje v Z formule $\mathfrak{A}(x_1, \ldots, x_k, y)$ s $k+1$ volnými proměnnými taková, že pro každou $(k+1)$-tici $n_1, \ldots, n_k, m$ přirozených čísel platí

$$\text{jestliže } f(n_1, \ldots, n_k) = m\,, \quad \text{pak} \quad \vdash \mathfrak{A}(\bar{n}_1, \ldots, \bar{n}_k, \bar{m})\,;$$

$$\text{jestliže } f(n_1, \ldots, n_k) \neq m\,, \quad \text{pak} \quad \vdash \neg\,\mathfrak{A}(\bar{n}_1, \ldots, \bar{n}_k, \bar{m})\,.$$

V podobném smyslu lze v Z reprezentovat každou rekursivní (algoritmicky rozhodnutelnou) relaci. (Tato možnost reprezentace by zůstala v platnosti i v jistém modifikovaném systému, který by neobsahoval axióm indukce). Za zmínku stojí, že systém Z', který dostaneme ze Z odstraněním symbolu „." a axiómů pro násobení, neobsahuje deduktivně nerozhodnutelné věty (neboť se v něm dá formulovat málo vět); má však rovněž neizomorfní modely jako Z.

Pro systém Z jsou (při jeho úplné formulaci) algoritmicky rozhodnutelnými otázky, kdy posloupnost symbolů je proměnnou, termem, formulí, větou; zároveň i kdy pro danou formuli je daná posloupnost formulí jejím důkazem. (Na druhé straně podle věty dokázané CHURCHEM nelze algoritmicky pro libovolnou formuli rozhodnout, zda je v Z dokazatelná.) Protože výrazy a důkazy systému Z jsou zcela konkrétní konstruktivní objekty, je možné v metajazyce, kterého používáme, hovoříme-li o systému, zakódovat je efektivně a vzájemně jednoznačně pomocí intuitivně chápaných přirozených čísel. Přiřaďme každému objektu w, kde w je symbol, výraz nebo posloupnost výrazů, jeho numerický kód $c(w)$ např. takto: Základním symbolům 0, S, ... přiřaďme jako kódy vzájemně jednoznačně lichá čísla $1, 3, \ldots$ (potřebujeme jich pouze konečně mnoho); jestliže $w = s_1 s_2 \ldots s_k$ je výraz složený ze základních symbolů, budiž $c(w) = p_0^{c(s_1)}\, p_1^{c(s_2)} \ldots p_{k-1}^{c(s_k)}$, kde $c(s_i)$ je numerický kód symbolu s_i, $p_0 = 2$ a p_i je i-té liché prvočíslo (pro $i > 0$); jestliže w je konečná posloupnost

výrazů $u_1, \ldots, u_m$, budiž $c(w) = p_0^{c(u_1)} p_2^{c(u_2)} \ldots p_{m-1}^{c(u_m)}$. Je pak algoritmicky rozhodnutelné, kdy je přirozené číslo numerickým kódem, kdy je kódem termu, věty, důkazu (jakožto posloupnosti formulí). Zvláště pak je rozhodnutelné, zda pro dvě čísla m, n platí, že m je numerický kód nějaké věty a n je numerický kód nějakého důkazu, který je zároveň důkazem věty s kódem m. Dále se ukazuje, že je algoritmicky rozhodnutelné, zda přirozená čísla m, n jsou v takovém vztahu, že m je numerickým kódem nějaké formule $\mathfrak{A}(x)$ s jednou volnou proměnnou a zároveň pro tuto formuli n je numerickým kódem nějakého důkazu věty $\mathfrak{A}(\overline{m})$; označme tuto relaci R.

Popsaný proces aritmetizace formální struktury systému Z dovoluje na základě zmíněného výsledku o reprezentovatelnosti rekursivních funkcí a relací v Z interpretovat věty o struktuře systému Z jako věty samotného systému Z. Uvažme nejdřív relaci R. Je algoritmicky rozhodnutelná, tedy podle známé Churchovy teze rekursivní, tedy existuje formule $\mathfrak{R}(x, y)$ systému Z se dvěma volnými proměnnými x, y taková, že pro libovolná přirozená čísla m, n jsou pravdivé implikace:

$$\text{jestliže platí } R(m, n), \quad \text{pak} \quad \vdash \mathfrak{R}(\overline{m}, \overline{n}),$$

$$\text{jestliže neplatí } R(m, n), \quad \text{pak} \quad \vdash \neg\, \mathfrak{R}(\overline{m}, \overline{n}).$$

Na $\mathfrak{R}$ teď použijme variantu diagonální konstrukce. Nechť k je numerický kód formule $\forall y \neg\, \mathfrak{R}(x, y)$, kterou značme $\mathfrak{G}(x)$. Utvořme větu $\mathfrak{G}(\overline{k})$, tj. $\forall y \neg\, \mathfrak{R}(\overline{k}, y)$. *Nyní můžeme dokázat, že jestliže systém Z je bezesporný, pak $\mathfrak{G}(\overline{k})$ není v Z dokazatelná.* Nechť totiž platí opak, tj. $\vdash \mathfrak{G}(\overline{k})$. Pak $\mathfrak{G}(\overline{k})$ má v Z důkaz. Nechť d je numerický kód nějakého takového důkazu. Protože k je numerický kód formule $\mathfrak{G}(x)$, platí $R(k, d)$. Odtud vzhledem k reprezentovatelnosti relace R v Z plyne $\vdash \mathfrak{R}(\overline{k}, \overline{d})$. V souhlasu s pravidly odvozování v elementární predikátové logice, která jsou zahrnuta v Z, odtud dále plyne $\vdash \exists y\, \mathfrak{R}(\overline{k}, y)$ a nakonec $\vdash \neg\, (\forall y \neg\, \mathfrak{R}(\overline{k}, y))$, tj. $\vdash \neg\, \mathfrak{G}(\overline{k})$. Tedy je v Z dokazatelná spolu s větou $\mathfrak{G}(\overline{k})$ i její negace, což je ve sporu s předpokládanou bezesporností systému Z.

Naznačme teď důkaz 2. Gödelovy věty o nedokazatelnosti bezespornosti systému Z pomocí prostředků, které lze vyjádřit uvnitř Z. Jak jsme již uvedli, je relace D, která platí pro m, n právě když m je numerický kód nějaké věty a n je kód jejího důkazu, algoritmicky rozhodnutelná. Lze ji tedy v Z reprezentovat nějakou formulí $\mathfrak{D}(x, y)$. Nechť *Neg* je funkce, pro kterou platí, že je-li n numerický kód nějaké formule, pak $Neg(n)$ je kód negace této formule; jinak je $Neg(n) = 0$. Funkce *Neg* je algoritmicky vyčíslitelná, tedy rekursivní; proto ji lze v Z reprezentovat nějakou formulí $\mathfrak{N}(x, y)$. Vlastnost bezespornosti systému Z, tj. neexistenci dvou dokazatelných vět, z nichž jedna je negací druhé, je možno aritmeticky vyjádřit větou, která říká, že neexistují přirozená čísla m_1, m_2, n_1, n_2 taková, aby současně platilo $D(m_1, n_1)$, $D(m_2, n_2)$, $Neg(m_1) = m_2$. Tuto vlastnost pak dále můžeme vyjádřit přímo v Z, a to při vhodné volbě vázaných proměnných větou tvaru

$$\neg\, \exists x_1\, \exists x_2\, \exists y_1\, \exists y_2 (\mathfrak{D}(x_1, y_1) \,\&\, \mathfrak{D}(x_2, y_2) \,\&\, \mathfrak{N}(x_1, x_2)),$$

kterou označme $\mathfrak{B}$. Již výše jsme ukázali, že je-li systém Z bezesporný, pak věta $\mathfrak{G}(\bar{k})$ v něm není dokazatelná. Podstatné je, že tento důkaz je možno „formalizovat v Z", tj. v Z lze dokázat větu $\mathfrak{B} \to \mathfrak{G}(\bar{k})$ (viz např. [9]). Že přitom skutečně jde o formalizaci, která odpovídá obsahu původního neformálního důkazu plyne z toho, že ve smyslu použité aritmetizace říká věta $\mathfrak{G}(\bar{k})$ sama o sobě, že není v Z dokazatelná. Pak je již lehké dokázat, že věta $\mathfrak{B}$, která vyjadřuje bezespornost systému Z, není v systému Z za předpokladu jeho bezespornosti dokazatelná. V opačném případě bychom totiž měli $\vdash \mathfrak{B}$, tedy s ohledem na $\vdash \mathfrak{B} \to \mathfrak{G}(\bar{k})$ bychom v Z užitím pravidel, která dávají totéž jako modus ponens, dostali $\vdash \mathfrak{G}(\bar{k})$. Za předpokladu bezespornosti Z však, jak víme, $\vdash \mathfrak{G}(\bar{k})$ neplatí. Z tohoto sporu plyne, že nemůže být $\vdash \mathfrak{B}$.

Poznamenejme, že proveditelnost celé této úvahy nezávisí na tom, jak byla aritmetizace konkrétně provedena; stačí, aby byla provedena konstruktivně. (V souvislosti s tím však výběr formule, která vyjadřuje uvnitř systému Z jeho bezespornost, je podroben jistým omezujícím podmínkám, jak ukázal zvláště FEFERMAN [3]; při dostatečně přirozeném výběru formule jsou tyto podmínky splněny.) Gödelova 2. věta zároveň platí i pro mnohem silnější formalizované systémy, než je Z.

5. Popišme nakonec základní ideu Gentzenovy metody důkazu bezespornosti aritmetiky. Vyjděme z toho, že (jak lze dokázat) systém Z je sporný právě tehdy, jestliže v něm lze odvodit intuitivně nesprávnou větu $0 = S0$. Označme tuto větu $\mathfrak{S}$. Za důkazy v Z jsme pokládali jisté konečné posloupnosti formulí. Ve skutečnosti však toto lineární uspořádání je umělé, neboť některá odvozovací pravidla (už např. modus ponens) obsahují více formulí jakožto předpokladů, z nichž se tvoří formální závěr. Strukturu důkazu lze pak přirozeněji znázornit ve tvaru konečného pojmenovaného stromu. Kdybychom chtěli dokázat nedokazatelnost věty $\mathfrak{S}$ v Z např. indukcí podle rostoucí velikosti numerických kódů všech možných důkazů v Z, zjistili bychom, že takové uspořádání množiny všech důkazů je nevhodné, a to zhruba řečeno proto, že existují na každé úrovni složitosti důkazy s libovolně velkými kódovými čísly. Důkazy je třeba uspořádat jinak, a to v lepším souhlasu se strukturou, kterou mají jakožto stromy. Složitost důkazů lze vyjádřit pomocí tzv. ordinálních výrazů (o. v.).

Množinu Ω ordinálních výrazů definujme indukcí, a to současně s definicí relace $\succ$ mezi nimi (každý o. v. je sestaven ze symbolů $0, \omega, +$):

(1) 0 je o. v. a pro každý o. v. $\delta \neq 0$ jest $\delta \succ 0$.

(2) Jestliže $\delta_1, \delta_2, \ldots, \delta_k$ jsou o. v. $(k \geqq 1)$ a platí $\delta_1 \geqq \delta_2 \geqq \ldots \geqq \delta_k$, pak $\omega^{\delta_1} + \omega^{\delta_2} + \ldots + \omega^{\delta_k}$ je o. v.; označíme-li ho δ, pak pro každý o. v. $\lambda = \omega^{\lambda_1} + \ldots + \omega^{\lambda_m}$ $(m \geqq 1)$ jest $\delta \succ \lambda$ právě tehdy, jestliže nastává jeden z případů
   (a) $k > m$ a pro všechna $j = 1, \ldots, m$ platí $\delta_j = \lambda_j$;
   (b) pro nějaké i, $1 \leqq i \leqq \min(k, m)$, platí $\delta_i \succ \lambda_i$, přičemž pro $j = 1, \ldots, i-1$ jest $\delta_j = \lambda_j$.

Je vidět, že Ω je spočetná konstruktivní množina finitních objektů (ordinální výrazy

by bylo možno s event. použitím závorek psát lineárně) a že relace $\succ$ je na Ω algoritmicky rozhodnutelná. Lze navíc dokázat, že relace $\succ$ je dobré uspořádání množiny Ω. Důkaz je sice možno provést např. obyčejnou indukcí, ale není striktně finitní, neboť je přitom třeba uvažovat jisté třídy množin ordinálních výrazů. Z dalšího plyne, že tato okolnost je podstatná.

Pro důkaz bezespornosti systému Z (vlastně jistého ekvivalentního systému, přitom s jinou větou než $\mathfrak{S}$) sestrojil Gentzen dvě konstruktivní zobrazení ϱ: $\Delta \to \Delta$, σ: $\Delta \to \Omega$ (kde Δ je množina všech důkazů v Z) taková, že platí: Jestliže nějaké $d \in \Delta$ je důkazem věty $\mathfrak{S}$, pak $\varrho(d)$ je rovněž důkazem věty $\mathfrak{S}$ a platí $\sigma(d) \succ \sigma(\varrho(d))$. Předpokládejme nyní, že $\mathfrak{S}$ lze v Z dokázat. Nechť d je nějaký důkaz věty $\mathfrak{S}$. Pak iterací zobrazení ϱ dostáváme v Ω podle předchozího nekonečný klesající řetězec:

$$\sigma(d) \succ \sigma(\varrho(d)) \succ \sigma(\varrho(\varrho(d))) \succ \ldots$$

To je však ve sporu s tím, že $\succ$ je dobré uspořádání. Tedy systém Z je bezesporný.

Jestliže u ordinálních výrazů chápeme 0, resp. ω jako ordinální číslo prázdné množiny, resp. jako nejmenší nekonečné ordinální číslo, jestliže dále chápeme ω^0 jakožto ordinální číslo 1, ω^1 jakožto ordinální číslo ω a součet a mocninu jakožto odpovídající operace s ordinálními čísly, pak ordinální výrazy představují jednoznačné zápisy ordinálních čísel menších než ε_0, kde ε_0 je nejmenší (spočetné) ordinální číslo α takové, že $\omega^\alpha = \alpha$. Přitom relace $\succ$ mezi ordinálními výrazy splývá s relací „být větší" pro odpovídající ordinální čísla. Tedy větu o dobrém uspořádání množiny Ω lze chápat jako větu o transfinitní indukci pro ordinální čísla menší než ε_0. Uvažme dále, že ordinální výrazy je možno konstruktivně vzájemně jednoznačně zobrazit na přirozená čísla. Tím přejde $\succ$ v jistou rekursivní relaci $\succ'$ na množině přirozených čísel, která jsou touto relací dobře uspořádána. Tuto relaci lze v Z reprezentovat jistou formulí. Kdyby pro tuto formuli bylo možno v Z odpovídající větu (schéma) o dobrém uspořádání skutečně dokázat, pak by bylo možno důkaz bezespornosti systému Z formalizovat uvnitř Z. To však podle 2. Gödelovy věty není možné. Se zřetelem na zmíněný vztah k ordinálním číslům lze tedy říci, že transfinitní indukce pro ordinální typ ε_0, i když má jisté konstruktivní rysy, je prostředkem, který překračuje meze systému Z.

Literatura

[1] Bernays P.: Hilberts Untersuchungen über die Grundlagen der Arithmetik. Ve 3. svazku sebraných spisů D. Hilberta, 196–216, Springer, Berlin 1935.

[2] Dedekind R.: *Was sind und was sollen die Zahlen.* Brunswick 1888. 10. vydání v nakl. Vieweg, Braunschweig 1965.

[3] Feferman S.: Arithmetization of metamathematics in a general setting. Fundamenta Math. *49* (1960–61), 35–92.

[4] Gentzen G.: Die Widerspruchsfreiheit der reinen Zahlentheorie. Math. Ann. *112* (1936), 493–565.

[5] GÖDEL K.: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. Monatsh. Math. Phys. *38* (1931), 173—198.
[6] HILBERT D. Über den Zahlbegriff. Jber. dtsch. Math.-Ver. *8* (1900).
[7] HILBERT D.: Mathematische Probleme. Archiv f. Math. u. Phys., 3. Reihe, *1* (1901), 44—63, 213—237.
[8] HILBERT D.: Matematické problémy. Český překlad úvodní a závěrečné části předchozího článku, Pokroky mat. fyz. astr. *16* (1971), 15—22.
[9] HILBERT D., BERNAYS P : *Grundlagen der Mathematik, sv. II.* 2. vyd., Springer, Berlin 1970.
[10] SHOENFIELD J. R.: *Mathematical logic.* Addison-Wesley, Reading 1967.
[11] WANG HAO: The axiomatization of arithmetic. Jour. Symb. Logic *22* (1957), 145—157.

KRITÉRIA VĚDECKOSTI PRACÍ Z TEORIE VYUČOVÁNÍ FYZICE*)

EMIL KAŠPAR, Praha

V současné době, v době technického rozmachu, je stále naléhavější otázka, co vlastně chceme od školské fyziky. Je třeba jasně vědět, jaké úkoly má plnit, abychom si uvědomili celou šíři a rozmanitost témat, která mohou být předmětem zájmu pracovníků v teorii vyučování fyzice. Tato témata se týkají nejen fyziky na základních školách a gymnasiích, ale i na odborných a vysokých školách. Také práce z didaktiky fyziky, které až dosud u nás byly předloženy k obhajobě, tuto šířku a rozmanitost tematiky ukazovaly. Co však bylo na určitém počtu z nich negativní, byla skutečnost, že tematika nesla stopy náhodného zájmu, ať už samotného pracovníka nebo zadavatele práce. V některých případech se dokonce zdálo, že někteří pracovníci, ba i jejich vedoucí byli sami bezradní nejen snad jen v tom, jaké téma vědecké práce volit, ale dokonce i v tom, co to vůbec práce z teorie vyučování anebo jakákoli vědecká práce jest.

Je třeba proto naznačit kritéria vědeckosti práce, která by měli brát v úvahu výkonní pracovníci při sebekritice, vedoucí těchto prací při jejich vedení a posuzovatelé při jejich hodnocení.

Především si ujasněme pojem „vědecká práce". Termín „vědecká práce" má dva významy: jde jednak o činnost, jednak o písemný dokument o této činnosti. Vědecká činnost sama o sobě, byť byla sebehodnotnější, má společenskou hodnotu nulovou, není-li využita nebo aspoň sdělena. Aby výsledky vědecké činnosti mohly být využity, musí být zaprotokolovány a sděleny. Toto sdělení je podstatnou součástí jakékoli vědecké činnosti, neboť — jak praví starý reklamní slogan — „kdybys zlato za cenu hlíny prodával, neprodáš je, jestliže to neoznámíš".

*) Podle referátu přednesného dne 19. 11. 1970 na konferenci JSMF v Trenčianském Jastrabí.