J. H. Ewing; W. H. Gustafson; P. R. Halmos; S. H. Moolgavkar; W. H. Wheeler; W. P. Ziemer

Americká matematika od roku 1940 do předvčerejška

Pokroky matematiky, fyziky a astronomie, Vol. 24 (1979), No. 5, 258--267

Persistent URL: http://dml.cz/dmlcz/137965

potřebného kapalného vzduchu je velmi malé: na každý litr kapalného hélia je třeba dva litry kapalného vzduchu a na celý den práce s kapalným héliem ne více než 10–15 kg kapalného vzduchu.

Účinnost našeho adiabatického zkapalňovače je alespoň 10krát vyšší než dřívějších aparátů. Ale hlavní úspora je čas. Za dvě hodiny po spuštění zkapalňovače se získává dostatečné množství kapalného hélia, aby bylo možno začít experimentovat. To všechno natolik usnadňuje práci s kapalným héliem, že se stane dostupným pro většinu laboratoří.

Americká matematika od roku 1940 do předvčerejška*)

J. H. Ewing, W. H. Gustafson, P. R. Halmos, S. H. Moolgavkar, W. H. Wheeler, W. P. Ziemer

Předmluva. Jak nejlépe podat malý zlomek historie uvedený v názvu? Měla by se tato zpráva zabývat hlavně statistikou růstu časopisu Mathematical Reviews? Nebo by měla být věnována hlavně životům matematiků nebo by měla obsahovat především seznamy knih a článků? Nebo bychom měli jít v první řadě po stopách vlivů a důsledků, které vedly od königsberských mostů nejprve k analysis situs *a potom k homologické algebře? Nerozhodli jsme se pro žádný z těchto způsobů, ale místo toho chceme říci co možná nejvíce o matematice, živé matematice dneška. Aby se nám to podařilo v daném časovém a prostorovém limitu, rozhodli jsme se vykládat naši tematiku tradičním stylem historie, totiž stylem „bitev a králů". Snažíme se popsat hlavní vítězství americké matematiky od roku 1940, zmínit se o jménech vítězů a uvést — jak doufáme — dostatečné vysvětlení (ale nic víc), které ukazuje, jaký protivník byl poražen. Při popisu se obvykle omezujeme pouze na tvrzení. Vypouštíme všechny důkazy, ale někdy stručně naznačujeme jejich průběh. Takovýto náznak může být jedna věta nebo dva až tři odstavce; jeho účelem je spíše osvětlit situaci než přesvědčit.*

Pokrok v matematice znamená objevení nových pojmů, nových příkladů, nových metod nebo nových skutečností. Schwartzův pojem distribuce, Milnorův příklad exotické sféry, Cohenova metoda forcingu a Feitova-Thompsonova věta o jednoduchých grupách sem nade vší pochybnost patří. Neměli jsme potíže

---

*) Překlad 1. části článku *American Mathematics from 1940 to the Day before Yesterday*, American Mathematical Monthly *83* (1976) No. 7, pp. 503–516.

Přeložil Jiří Vanžura.

Vylepšená verze tohoto článku byla přednesena (P. R. Halmosem) ve formě pozvané přednášky na setkání Americké matematické asociace v San Antoniu 24. ledna 1976. Autoři vyjadřují svou vděčnost W. Ambrosovi, G. Benettovi, J. L. Doobovi, L. K. Durstovi, I. Kaplanskému, R. Narasimhanovi, I. Reinerovi a F. Trevesovi za jejich pomoc, rady, odkazy na literaturu a zvláště za jejich povzbuzení.

při hledání vítězství, která by měla být zahrnuta do našeho seznamu; potíž byla s rozhodnutím, která vyloučit. Formulovali jsme určitá hrubá pravidla (např.: věty, ne teorie); protože alespoň z některých hledisek byla aplikovaná matematika pokryta již v jiných článcích, omezili jsme se pouze na čistou matematiku; vyloučili jsme práce, které neměly své kořeny, ani odnože, ani plody v USA; když jsme se rozhodovali, kterého ze dvou kandidátů ponechat, přiklonili jsme se k tomu, který se těší většímu obecnému zájmu. („Obecný zájem" není přesně totéž jako „popularita", ale je jí blízký.)

Nakonec nám zůstalo deset „bitev a králů" a my si myslíme, že podávají dosti dobrý obraz o tom, co se událo. Netvrdíme, že náš seznam je důležitější než kterýkoli jiný, ani že je maximální v matematickém smyslu tohoto slova, tj. že není méně důležitý než kterýkoli jiný. Tvrdíme však, že by byl celý zahrnut a s respektem probírán v jakýchkoli odpovědných dějinách našeho místa a času. Celkový počet „nevynechatelných" vítězství je určitě větší než deset; možná je jich dvacet nebo dokonce čtyřicet. Výběr našich deseti byl ovlivněn hranicemi naší kompetence a našimi osobními zálibami; tomu se nelze vyhnout. Kdokoli jiný by pravděpodobně vybral jinou desítku. Doufáme však a myslíme, že seznam, který by byl sestaven kýmkoli jiným, by se silně překrýval s naším a že lokální rozdíly by nezměnily podstatně globální obraz.

V historii ovlivňuje každý okamžik okamžiky následující; omezit se na určitý časový interval je asi často nutné, někdy je to možné, ale zřídkakdy je to přirozené. Zcela stejně každé místo ovlivňuje všechna ostatní místa. Protože však je topologie povrchu naší zeměkoule mnohem složitější než topologie časové přímky, je omezení se na jednu zemi téměř nemožné. Historie matematiky zde není žádnou výjimkou: snažíme-li se vyličit, co se stalo zde, *velmi často musíme povolit tlaku vzdálených vlivů a hovořit o tom, co se stalo* tam. *Nicméně však jsme schopni se neodchýlit nepřiměřeně od našeho cíle. Připouštíme-li nejen celistvé položky, můžeme asi 8,25 z dosažených deseti úspěchů nazvat americkými. Je možná také zajímavé si povšimnout, že více než polovina z originálních článků, na které se odkazujeme, byla publikována v časopise* „Annals of Mathematics".

Volba pořadí může vycházet z několika hledisek (např. k čemu došlo dříve?, co bylo předpokladem k čemu?). Rozhodli jsme se pro uspořádání na základě obecnosti kategorie příslušnosti nebo — jinak zhruba řečeno — na základě vzdálenosti od základů matematiky. Na konci každého oddílu je malý seznam příslušné literatury. Je záměrně neúplný. Vše, co obsahuje, je jeden (nebo, je-li to nutné, dva nebo tři) prvotní články, ve kterých byl objev uveden, a dále nějaký novější výklad tohoto objevu, pokud jsme nějaký mohli najít.

Hypotéza kontinua. Celá matematika je odvozena z teorie množin (nebo alespoň většina z nás je o tom přesvědčena), přičemž manipulace s množinami je jednoduchý a přirozený úkon (každopádně studenti nemívají potíže s jejím zvládnutím). Vše, co aktivní matematik potřebuje vědět o množinách (včetně několika speciálních věcí, o nichž si nikdy nemyslel, že je potřebuje), se vejde na jednu tištěnou stránku (nebo na tři až čtyři tištěné strany, když chceme k formalismu přidat ještě motivaci). Na takové stránce by bylo uvedeno, jak můžeme ze známých množin vytvářet množiny nové (např. tvoření množin skládajících se ze zadaných elementů, vytváření sjednocení množin, vytvoření potenční množiny, tj. množiny všech podmnožin dané množiny); byly by tam popsány základní vlastnosti množin (např. že dvě množiny se rovnají, jestliže každá z nich je podmnožinou druhé, a že žádná množina nemá prvky, které jsou zase množinami, které mají prvky ... a tak dále až do nekonečna); bylo by tam uvedeno (jako předpoklad nebo jako důsledek, v každém případě však jakožto popis situace), že existují nekonečné množiny. Tato základní tvrzení teorie množin můžeme považovat buď za výsledky pozorování skutečnosti, nebo za axiomatický popis ZF (Zermelovy-Fraenkelovy) struktury. V obou případech by nebylo žádným problémem je zakódovat do jazyka vhodného (nepříliš složitého) počítače. Takovýto počítač bychom snadno mohli naučit všem odvozovacím

pravidlům, která matematikové používají. Kdybychom navíc k základním vstupním datům přidali dvě další tvrzení, mohl by *v principu* počítač snadno vytisknout veškerou známou matematiku (a spoustu toho, co ještě není známo).*)

Zmíněná dvě tvrzení, jimž historie věnovala zvláštní pozornost, jsou AC (axiom výběru) a GCH (zobecněná hypotéza kontinua). AC říká, že pro každou množinu X existuje zobrazení f potenční množiny množiny X do X takové, že $f(A) \in A$ pro každou neprázdnou podmnožinu A množiny X; GCH říká, že každá podmnožina potenční množiny nekonečné množiny X je ve vzájemně jednoznačné korespondenci buď s nějakou podmnožinou množiny X, nebo s celou potenční množinou množiny X — není tedy nic mezi X a její potenční množinou.

Platí axióm výběru? Tato otázka byla často srovnávána s podobným problémem týkajícím se pátého Eukleidova postulátu. V obou případech máme více méně pěkný systém axiómů a k tomu jeden méně pěkný, komplikovanější a ne zcela zřejmý dodatečný axióm. Jestliže je tento dodatečný axióm důsledkem základních axiómů, potom platí a všechno je v pořádku; jestliže důsledkem základních axiómů je jeho negace, potom neplatí a tak či onak je otázka definitivně zodpovědněna. Stejnou otázku si přirozeně můžeme klást v případě GCH. Dlouhou dobu bylo známo, že z GCH plyne AC; ve světle této skutečnosti existuje zřejmý vztah mezi oběma otázkami.

Odpovědi na tyto otázky jsou pronikavým a hlubokým úspěchem lidského ducha. GÖDEL (1940) dokázal, že AC a GCH nejsou nepravdivé (tj. že jsou konzistentní s axiómy ZF) a PAUL COHEN (1964) dokázal, že nejsou pravdivé (tj. jsou nezávislé na ZF).

Gödelův důkaz spočíval v konstrukci vhodného modelu. Gödel dokázal, že jestliže ZF je konzistentní, takže existuje třída V množin splňující základní ZF axiómy, potom existuje „podtřída", která je rovněž splňuje a v níž navíc platí AC a GCH. Podtřída, kterou Gödel zkonstruoval, je třída L „konstruovatelných" množin. (Použité přídavné jméno má prostý, ale zcela přesný význam; zhruba řečeno, konstruovatelné množiny jsou množiny, které můžeme dostat z prázdné množiny použitím transfinitní posloupnosti elementárních množinově teoretických konstrukcí.) Třída L je podstrukturou v běžném matematickém smyslu tohoto slova: objekty patřící do L jsou některé z objektů ve V a relace $\in$ mezi nimi je restrikcí množinově teoretického $\in$ ve V na objekty z L. Existence modelu typu L (zkonstruovaného na základě hypotetického konzistentního modelu V) dokazuje konzistentnost AC a GCH zcela stejně jako existence eukleidovské roviny dokazuje konzistentnost postulátu o rovnoběžkách.

Cohenův postup byl podobný, ale obtížnější. Připomíná Kleinovu konstrukci Lobačevského roviny, kdy se v eukleidovském kruhu zavádí nová metrika. Cohen vyšel od vhodného ZF-modelu a přidával k němu nové objekty. Tyto nové objekty jsou „třídy" (ale nikoli množiny) z původního modelu. Při přidávání se používá nové metody zvané „forcing", která — jakmile byla objevena — se ukázala užitečnou v mnohých partiích

*) Takto vytořená „matematická literatura" by ovšem stěží byla někomu k užitku, především ze dvou důvodů: a) Krajní primitivnost použitých vyjadřovacích prostředků by vedla k velmi neekonomickému zápisu i jednoduchých matematických pojmů a výsledků. b) Počítač sám by nebyl schopen rozlišit podstatné a obsažné pojmy a výsledky od nepodstatných a čistě formálních. (Pozn. redakce.)

teorie množin. V Cohenově důkazu se konstruuje nekonečná posloupnost lepších a lepších konečných aproximací nových objektů. Zhruba řečeno, každá vlastnost nového modelu je „vynucena" vlastnostmi starého modelu a jednou z aproximací. V závislosti na tom, jak uzpůsobíme detaily, konečným výsledkem může být ZF-model, v němž AC neplatí, nebo ZF-model, v němž AC platí, ale již klasická nezobecněná hypotéza kontinua CH neplatí. (CH je GCH pro nekonečnou spočetnou množinu.) Důsledek: AC a CH jsou nezávislé na ZF.

Literatura

[1] P. J. COHEN: *The independence of the continuum hypothesis.* Proc. N. A. S., *50* (1963) 1143—1148 and *51* (1964) 105—110.

[2] P. J. COHEN: *Set theory and the continuum hypothesis.* Benjamin, New York, 1966 (MR 38 # 999).

[3] J. B. ROSSER: *Simplified independence proofs.* Academic Press, New York, 1969 (MR 40 # 2536).

[4] T. J. JECH: *Lectures in set theory, with particular emphasis on the method of forcing.* Springer, Berlin, 1971 (MR 48 # 105).

Diofantické rovnice. Hypotéza kontinua byla obsahem prvního Hilbertova problému (z proslulého seznamu 23 problémů, které formuloval v roce 1900); Hilbertův desátý problém se týká řešitelnosti diofantických rovnic. Problémem je nalezení početního postupu-algoritmu, který by umožňoval zjistit, zda daná polynomiální rovnice s celočíselnými koeficienty má celočíselná řešení. Z jistého hlediska je přirozenější a někdy technicky jednodušší zabývat se *kladnými* celočíselnými řešeními (tj. řešeními v $\mathbf{Z}_+$) polynomiálních rovnic s *kladnými* celočíselnými koeficienty. Upozornění: nemáme na mysli pouze rovnice tvaru $p(x) = 0$. Problém zahrnuje hledání čísel x takových, že $p(x) = q(x)$; obecněji zahrnuje hledání n-tic $(x_1, \ldots, x_n)$ takových, že $p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)$; úplně obecně jde o hledání n-tic $(x_1, \ldots, x_n)$, pro něž existují m-tice $(y_1, \ldots, y_m)$ takové, že

$$p(x_1, \ldots, x_n, y_1, \ldots, y_m) = q(x_1, \ldots, x_n, y_1, \ldots, y_m) .$$

Pro polynomy p a q (v $n + m$ proměnných) se množina řešení v předchozím slova smyslu nazývá „diofantickou množinou" v $\mathbf{Z}_+^n$.

Co to znamená, jestliže řekneme, že existuje algoritmus na zjištění řešitelnosti? Vhodný způsob, jak odpovědět na tuto otázku, je nejprve zavést pojmy rekurzivní množina a rekurzivní funkce a teprve potom s jejich pomocí definovat algoritmus.

Kdy můžeme funkci ze $\mathbf{Z}_+$ do $\mathbf{Z}_+$ nebo obecněji funkci ze $\mathbf{Z}_+^n$ do $\mathbf{Z}_+$ nazvat „rekurzivní"? Podle obecné dohody dnes nazýváme rekurzivními funkcemi funkce vytvořené z určitých jednoduchých funkcí (konstanta, následník, souřadnice) pomocí tří procedur (skládání, minimalizace, primitivní rekurze). Na detailech zde nezáleží (nebudou nikde používány); je však vhodné připomenout, že vůbec nejde o obtížnou záležitost. Podmnožina (v $\mathbf{Z}_+$, nebo obecněji v $\mathbf{Z}_+^n$) se nazývá rekurzivní, jestliže je rekurzivní její charakteristická funkce. Důsledek: podmnožina (v $\mathbf{Z}_+^n$) je rekurzivní tehdy a jen tehdy, když je rekurzivní její komplement.

Uvažujme nyní všechny polynomiální rovnice (ve výše uvedeném smyslu) a napišme je do posloupnosti $\{E_1, E_2, E_3, \ldots\}$. (Abychom zůstali v souladu s intuitivním pojmem algoritmu, je třeba je sestavit v jistém smyslu slova efektivně. Ale to se dá poměrně snadno udělat.) Indexy k, pro které má rovnice E_k řešení (ve výše uvedeném smyslu), tvoří podmnožinu S množiny $\mathbf{Z}_+$. Hilbertův problém (existuje algoritmus?) můžeme nyní formulovat takto: je podmnožina S rekurzivní? Odpověď zní ne. Na tuto odpověď se čekalo dlouhou dobu a je výsledkem spojeného úsilí J. Robinsona (1952), M. Davise (1953), H. Putmana (1961) a Y. Matijaseviče (1970).

Centrálním pojmem důkazu je pojem diofantické množiny a hlavním krokem je důkaz tvrzení, že každá rekurzivní množina je diofantická. Technická část vtipně využívá elementární teorie čísel (např. tzv. Čínskou větu o zbytku a část teorie Fibonacciho čísel nebo část teorie Pellovy rovnice). V důkazu se přichází na některé zajímavé diofantické množiny, jejichž diofantický charakter není nikterak zřejmý (např. mocniny čísla 2, faktoriály a prvočísla).

Jednou z možností, jak dokázat, že podmnožina S (indexová množina řešitelných rovnic) není rekurzivní, je důkaz sporem. Kdyby S byla rekurzivní, pak by odtud vyplývalo (něco málo bychom museli ještě dokázat), že každá zmíněná diofantická množina (tj. množina řešení každé uvedené rovnice) je rekurzivní, a že tedy (na základě „hlavního kroku" z předchozího odstavce) komplement každé diofantické množiny je diofantický. Spor dostáváme nalezením diofantické množiny, jejíž komplement není diofantický.

Poslední krok používá verzi známé Cantorovy diagonální metody. Myšlenka je seřadit „efektivně" všechny diofantické podmnožiny v $\mathbf{Z}_+$ např. do posloupnosti $\{D_1, D_2, D_3, \ldots\}$, dokázat, že množina $D^* = \{n: n \in D_n\}$ je diofantická (to dá určitou práci) a konečně ukázat, že komplement $\mathbf{Z}_+ - D^* = \{n: n \notin D_n\}$ není diofantický (zde se používá Cantorova metoda).

Literatura

[1] J. Robinson: *Existential definability in arithmetic.* Trans. A. M. S., *72* (1952) 437—449 (MR 14—4)

[2] M. Davis: *Arithmetical problems and recursively enumerable predicates.* J. Symb. Logic, *18* (1953) 33—41 (MR 14—1052).

[3] M. Davis, H. Putman, and J. Robinson: *The decision problem for exponential Diophantine equations.* Ann. Math., *74*(1961) 425—436 (MR 24 # A 3061).

[4] Y. Matijasevič: *The Diophantiness of enumerable sets.* (Russian), Dokl. Akad. Nauk SSSR, *191* (1970) 279—282; improved English translation, Soviet Math. Doklady, *11* (1970, 354—358 (MR 41# 3390).

[5] M. Davis: *Hilbert's tenth problem is unsolvable.* Am. Math. Monthly *80* (1973) 233—269 (MR 47 # 6465).

Jednoduché grupy. Tolik o základech. Dalším oborem v hierarchii je algebra. V daném okamžiku teorie grup.

Každá grupa G má alespoň dvě normální podgrupy, totiž sebe samu a jako druhý extrém jednotkovou podgrupu 1. Grupa G se nazývá *jednoduchá*, jestliže tyto dvě podgrupy jsou její jediné normální podgrupy.

Jednoduché grupy se ve dvou směrech podobají prvočíslům: neobsahují netriviální části a můžeme z nich složit každou konečnou grupu. (Podle obecné konvence se kladné číslo 1 nepovažuje za prvočíslo, ale jednotková grupa 1 se zahrnuje mezi jednoduché grupy. Není to dobré, ale je tomu tak.)

Předpokládejme tedy, že grupa G je konečná a buď G_1 její maximální normální podgrupa. (G_1 se nazývá maximální, jestliže je vlastní normální podgrupou grupy G, která není obsažena v žádné jiné vlastní normální podgrupě grupy G.) Je-li G jednoduchá, potom $G_1 = 1$; obecně z maximality podgrupy G_1 plyne, že faktorgrupa G/G_1 je jednoduchá. Chceme-li vyjádřit vztah mezi grupami G, G_1 a G/G_1 (grupa, normální podgrupa, faktorgrupa), říkáme někdy, že grupa G je rozšířením grupy G/G_1 pomocí grupy G_1. V této terminologii je každá konečná grupa (s výjimkou jednotkové grupy 1) rozšířením jednoduché grupy pomocí grupy ostře menšího řádu. Toto tvrzení z teorie grup je analogií tvrzení z teorie čísel o tom, že každé kladné celé číslo (s výjimkou čísla 1) je součinem prvočísla a kladného čísla ostře menšího.

Není-li G_1 jednotková grupa, můžeme aplikovat předchozí odstavec. Výsledkem je maximální normální podgrupa G_2 grupy G_1 taková, že G_1 je rozšířením jednoduché grupy G_1/G_2 pomocí grupy G_2. Tento proces můžeme opakovat tak dlouho, dokud nedostaneme jednotkovou grupu; konečným výsledkem je řetězec

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n = 1$$

(„kompoziční řada"), ve kterém každá z grup G_i/G_{i+1} je jednoduchá ($i = 0, \ldots, n-1$). Tímto způsobem se velká část problému nalezení všech konečných grup redukuje na určení všech jednoduchých konečných grup. (Slavná Jordanova-Hölderova-Schreierova věta nám zajišťuje, že kompoziční faktory G_i/G_{i+1} jsou jednoznačně určeny až na izomorfismus a pořadí.)

Abelovské jednoduché konečné grupy určíme snadno: jsou to právě všechny cyklické grupy prvočíselného řádu. To je snadné. Co je obtížné, to je nalezení všech neabelovských jednoduchých konečných grup. Některé příklady získáme snadno, např. mezi grupami permutací jsou nejznámějšími grupy sudých permutací n prvků s $n \geqq 5$. Známé jednoduché grupy nevytvářejí žádný systém a i nejjednodušší problémy, které se jich týkají, vzdorují řešení. BURNSIDE vyslovil například domněnku, že každá neabelovská jednoduchá grupa má sudý řád, ale tato domněnka zůstala otevřeným problémem po dobu více než 50 let. Ukázkovou demonstrací síly teorie grup FEIT a THOMPSON (1963) ukázali, že Burnsideova domněnka je správná. Důkaz zabírá celé číslo (více než 250 stran) časopisu „Pacific Journal". Je to technická teorie grup a teorie charakterů. Od doby, kdy důkaz byl publikován, byla v něm provedena určitá zkrácení, ale žádný krátký nebo snadný důkaz nebyl dosud objeven. Dosažený výsledek má mnoho důsledků a použité metody byly aplikovány na mnoho jiných problémů v teorii konečných grup. Oblast, která byla mnohými prohlášena za mrtvou, se ukázala být silně životaschopnou.

Literatura

W. FEIT, J. G. THOMPSON: *Solvability of groups of odd order*. Pac. J. Math., *13* (1963) 775—1029 (MR 29 # 3538).

Odstranění singularit.*) Algebra se stává bohatší a obtížnější, když se spojí s geometrií a v ní se aplikuje; jedním z nejbohatších spojení tohoto druhu je stará, avšak velmi životaschopná disciplína známá pod názvem algebraická geometrie. Tento oddíl pojednává o řešení jednoho starého a slavného problému z této disciplíny.

Buď k algebraicky uzavřené těleso a buď k^n jako obvykle n-rozměrný souřadnicový prostor nad k. (Nejlépe pochopíme, o co dále jde, když v roli k budeme uvažovat těleso komplexních čísel.) „Afinní algebraická varieta" V v k^n je množina nulových bodů společných systému polynomů v n proměnných nad k. Protože nám jde pouze o nulové body, sám systém polynomů není důležitý; můžeme ho nahradit libovolným jiným systémem se stejnou množinou společných nulových bodů. Je-li tedy R okruh *všech* polynomů v n proměnných s koeficienty z k a je-li I ideál v R generovaný uvažovaným systémem, potom ideál I určuje tutéž varietu; proto můžeme bez újmy na obecnosti předpokládat, že uvažovaný systém polynomů tvoří ideál.

Předmětem našeho zájmu na varietách jsou jejich „singulární body". Intuitivně vzato jsou to body, v nichž „tečné vektory" nejsou takové, jaké by být měly. Uvažujme např. křivky definované rovnicemi

$$y^2 = x^3 + x^2 \quad \text{a} \quad y^2 = x^3 .$$

(Protože jsme se omezili na algebraicky uzavřená tělesa, neměli bychom si představovat *reálné* rovinné křivky zadané těmito rovnicemi. Pro představu jsou ovšem mnohem názornější než komplexní křivky, které leží v komplexní rovině. Upozornění: komplexní rovina má reálnou dimenzi čtyři. Pro algebraického geometra je „komplexní rovina" známá z analýzy komplexní *přímkou.*) První křivka přichází do počátku z prvního kvadrantu se směrnicí tečny v počátku rovnou 1, v levé polorovině vytváří smyčku a vychází z počátku do čtvrtého kvadrantu se směrnicí tečny v počátku rovnou -1; počátek je jejím dvojným bodem. Druhá křivka přichází do počátku z prvního kvadrantu se směrnicí tečny v počátku rovnou 0 a z počátku vychází stejným způsobem do čtvrtého kvadrantu; počátek je jejím bodem vratu.

Efektivní způsob práce se singulárními body začíná jejich čistě algebraickou definicí. Za tímto účelem uvažujme okruh R_V regulárních funkcí na V (tj. restrikce polynomů z R na V.) Je-li N_V ideál v R sestávající z těch polynomů, které se anulují na V, potom zřejmě $R_V = R/N_V$. Ke každému bodu $\alpha = (\alpha_1, \ldots, \alpha_n)$ z V přiřazujeme maximální ideál N_α v R (sestávající z těch polynomů, které se anulují v bodě α); zřejmě $N_V \supset N_\alpha$.

Dalším krokem (na cestě k algebraické definici singulárních bodů) je konstrukce nového okruhu, který popisuje lokální charakter funkcí v blízkosti bodu α. Myšlenka je (velmi zhruba) tato: (I) Uvažujme dvojice (U,f), kde U je „okolí" bodu α a f je racionální funkce definovaná v U, která tam nemá žádné póly. (II) Definujme relaci ekvivalence na těchto dvojicích. $(U,f) \sim (U',f')$ právě tehdy, když existuje okolí U'' bodu α obsažené v $U \cap U'$ takové, že $f = f'$ na U''. (III) Třídy ekvivalence („germy") tvoří okruh (např. sčítání definujeme předpisem

*) V originále „Resolution of singularities". Český ekvivalent v podstatě neexistuje. Byl zvolen názorný překlad. V češtině se někdy užívá termínu „rozpuštění" nebo „redukce" singularit. — Pozn. překl.

$$[(U,f)] + [(U',f')] = [(U \cap U', f + f')],$$

který se nazývá „lokální okruh" variety V v bodě α.

Z algebraického hlediska mají předchozí topologické úvahy pouze heuristický charakter; nahradíme je nyní algebraickou konstrukcí. Tato konstrukce se příhodně nazývá „lokalizace". (I) Uvažujme dvojice (f, g), kde f a g jsou z R a $g \notin N_\alpha$. (II) Definujme relaci ekvivalence na těchto dvojících. $(f, g) \sim (f', g')$ právě tehdy, když existuje h, které neleží v N_α a takové, že $h(fg' - gf') = 0$. (III) Označme symbolem f/g třídu ekvivalence dvojice (f, g). Tyto třídy ekvivalence tvoří okruh R_α (s operacemi stejného typu jako u zlomků). Okruh R_α je skutečně „lokálním okruhem" v obvyklém algebraickém smyslu: má *jediný* maximální ideál, totiž ideál tvořený prvky z R_α, které se anulují v bodě α.

Abychom motivovali následující krok, mysleme si opět, že nejsme v algebraické, nýbrž v analytické geometrii.*) V takovém případě by se okruh R_α skládal z mocninných řad se středem v bodě α, konvergujících na nějakém okolí bodu α, a ideál N_α by obsahoval mocninné řady bez konstantního členu. Lineární členy mocninné řady jsou v jistém slova smyslu diferenciály prvního řádu. Jednou z možností, jak postihnout právě tyto členy je „ignorovat" členy vyššího řádu. Přesněji: uvažujme ideál N_α^2, který se v analytickém případě skládá z mocninných řad bez konstantního a lineárního členu a vytvořme faktorprostor N_α/N_α^2.

Nyní můžeme snadno zformulovat hledanou definici. „Dimenzí" d variety V je podle definice minimum dimenzí (přirozeně nad tělesem k) všech faktorprostorů N_α/N_α^2; bod α se nazývá singulární, jestliže $\dim (N_\alpha/N_\alpha^2) > k$. Není těžké vidět, že u dvou výše uvedených příkladů křivek je počátek skutečně singulárním bodem ve smyslu této definice.

Jedním z hlavních problémů algebraické geometrie je „odstranění" singulárních bodů. Za tímto účelem se omezíme na „ireducibilní" variety, tj. na takové variety, u kterých je R_V oborem integrity, nebo ekvivalentně N_V je prvoideál. V takovém případě můžeme k R_V vytvořit podílové těleso F_V. Dvě variety V a W se nazývají „biracionálně ekvivalentní", jestliže tělesa F_V a F_W jsou izomorfní. Zhruba to znamená, že variety V a W parametrizují jedna druhou pomocí racionálních zobrazení všude až na konečný počet bodů. Problém „odstranění singularit" znamená hledání nesingulární variety, která je biracionálně ekvivalentní s V.

Celá záležitost má dlouhou historii. Křivky studoval MAX NOETHER v 19. století. Plochy byly předmětem velkého zájmu italské školy; přesný důkaz podal J. J. WALKER (1935). Pro variety libovolné dimenze bylo konečné vítězství inspirováno pracemi ZARISKÉHO; důkaz podal HIRONAKA (1964).

Literatura

H. HIRONAKA: *Resolution of singularities of an algebraic variety over a field of characteristic zero.* Ann. Math., *79* (1964) 109—326 (MR 33 # 7333).

*) Termín „analytická geometrie" se zde používá ve smyslu „teorie analytických prostorů", srv. Pokroky MFA *XX*/1975 (2), str. 71. (Pozn. red.)

Weilovy hypotézy. Práce matematika je často nejobtížnější (a nejvděčnější), jestliže matematik usuzuje podle analogií, jestliže se domnívá, že zde *tato* situace by měla být právě taková jako *tamta* situace. Uvažuje tímto způsobem vyslovil v roce 1949 A. WEIL tři hypotézy, které hluboce ovlivnily vývoj algebraické geometrie v posledních 25 letech.

Tyto hypotézy byly otištěny v článku *Numbers of solutions of equations in finite fields*, který byl vynikajícím přehledem v té době známých výsledků. Určení počtu řešení polynomiální rovnice ve více proměnných nad konečným tělesem byl klasický problém studovaný GAUSSEM, JACOBIM, LEGENDREM a dalšími. Byl to však Weil, který přišel s novým pojetím. Abychom pochopili jeho přístup, uvažujme speciální případ, totiž homogenní rovnici

$$(*) \qquad a_0 x_0^n + a_1 x_1^n + \ldots + a_r x_r^n = 0\,,$$

kde koeficienty a_i jsou z prvotělesa F obsahujícího p prvků. Základní problém je určit počet řešení v tělese F, avšak pro číselného teoretika je právě tak důležité určit počet řešení v jakémkoli konečném rozšíření tělesa F. Připomeňme, že pro každé kladné celé číslo k existuje právě jedno rozšíření F_k tělesa F mající p^k prvků. Weil udělal to, že určil počet řešení rovnice (*) v každém z těles F_k a potom zakódoval tuto informaci do generující funkce.

Abychom to udělali ekonomicky, vyšetřujme množinu řešení rovnice (*). Máme samozřejmě vždy triviální řešení, se všemi x_i rovnými nule; toto řešení se oprávněně považuje za triviální. Je-li $(x_0, x_1, \ldots, x_r)$ netriviální řešení a $0 \neq c \in F_k$, potom $(cx_0, cx_1, \ldots, cx_r)$ je rovněž netriviální řešení. Každé netriviální řešení takto vytváří $p^k - 1$ netriviálních řešení a není důvodu, proč bychom měli každé z těchto řešení počítat zvlášť. Je tedy přirozené uvažovat r-rozměrný „projektivní prostor" $P^r(F_k)$, tj. množinu netriviálních uspořádaných $(r+1)$-tic prvků z F_k, přičemž dvě $(r+1)$-tice ztotožňujeme, jestliže je jedna skalárním násobkem druhé. (To je přesně analogické známému reálnému a komplexnímu projektivnímu prostoru.) Problém v tomto pojetí je určit počet „bodů" v $P^r(F_k)$, které jsou „řešeními" rovnice (*).

Přesně toto udělal Weil. Označil symbolem N_k počet řešení rovnice (*) v $P^r(F_k)$, uvažoval generující funkci

$$G(u) = \sum_{k=1}^{\infty} N_k u^{k-1}$$

a dokázal toto pozoruhodné tvrzení: G je logaritmickou derivací *racionální* funkce. To znamená, že existuje racionální funkce Z taková, že

$$\sum_{k=1}^{\infty} N_k u^{k-1} = \frac{\mathrm{d}}{\mathrm{d}u} \log Z(u)\,,$$

nebo jinými slovy, položíme-li

$$Z(u) = \exp\left(\sum_{k=1}^{\infty} \frac{N_k}{k} u^k\right),$$

potom Z je racionální. Funkce Z vyhovuje funkcionální rovnici, která je analogická funkcionální rovnici splňované RIEMANNOVOU dzeta funkcí a je tedy vhodné ji nazývat

dzeta funkcí asociovanou s rovnicí (*). Motivován klasickými problémy, jimž dala vzniknout klasická Riemannova dzeta funkce, Weil studoval a byl schopen určit mnohé vlastnosti nulových bodů a pólů funkce Z.

Právě zde Weilův článek dosahuje svého vrcholu. Weil chce rozšířit výsledky týkající se rovnice (*) na algebraické variety v $P^r(F_k)$, tj. na řešení *systému* homogenních rovnic v r proměnných. Pojem dzeta funkce definovaný RIEMANNEM byl rozšířen DEDEKINDEM na tělesa algebraických čísel, ARTINEM na tělesa funkcí a nyní Weilem na algebraické variety. (Uvažované variety by měly být nesingulární. Nezáleží na tom, kterou obecnou definici této podmínky vezmeme; pro většinu těles ji můžeme definovat jako obvykle požadavkem, aby jakobián systému rovnic měl v každém bodě maximální hodnost.) Je-li dán systém rovnic s koeficienty v F, nechť N_k značí jako předtím počet řešení v $P^r(F_k)$. Weil vyslovil následující hypotézy. První: Funkce Z definovaná jako dříve předpisem

$$Z(u) = \exp\left(\sum_{k=1}^{\infty} \frac{N_k}{k} u^k\right)$$

je racionální. Druhá: Z vyhovuje určité funkcionální rovnici, která jako dříve se silně podobá rovnici, jíž vyhovuje Riemannova dzeta funkce. Třetí: Převrácená čísla k nulovým bodům a pólům funkce Z jsou celá algebraická čísla a jejich absolutní hodnoty jsou mocninami čísla $\sqrt{p}$. (To je tzv. zobecněná Riemannova hypotéza.)

Všechno toto by se mohlo zdát velmi vzdálené od geometrie tak, jak ji normálně chápeme, a ačkoliv bylo známo několik příkladů, mohlo by se zdát, že Weil formuloval své doměnky na základě příliš malého množství průkazného materiálu. Co však bylo ve skutečnosti za těmito hypotézami? Odpověď najdeme v poslední části Weilova článku, kde Weil připomíná analogii mezi chováním uvažovaných variet (nad tělesem charakteristiky p) a chováním klasických variet (nad tělesem komplexních čísel).

V roce 1960 DWORK dokázal, že platí hypotéza o racionalitě (bez předpokladu o nesingulárnosti). Konečný triumf přišel v roce 1974; na základě výsledků dvacetileté práce GROTHENDIECKOVY školy DELIGNE dokázal platnost všech tří Weilových hypotéz, a což je možná důležitější, ukázal, že existuje krásný vztah mezi teorií variet nad tělesy charakteristiky p a klasickou algebraickou geometrií. „Bůh vždy geometrizuje," řekl PLATON, „Bůh vždy aritmetizuje," řekl JACOBI; Weilovy hypotézy ukazují, lépe než cokoliv jiného, že „Bůh může dělat obojí současně".

Literatura

[1] A. WEIL: *Numbers of solutions of equations in finite fields.* Bull. A. M. S., *55* (1949) 497—508) (MR 10—592).

[2] P. DELIGNE: *La conjecture de Weil I.* Inst. Haute Études Sci. Publ. Math., No. *43* (1974) 273—307 (MR 49 # 5013).

[3] J. A. DIEUDONNÉ: *The Weil conjectures.* The Mathematical Intelligencer, No. 10 (September 1975) 7—21.

(Zbývající druhá část překladu bude uveřejněna v příštím čísle. Pozn. red.)