Pokroky matematiky, fyziky a astronomie

Garrett Birkhoff
Súčasné trendy v algebre

Pokroky matematiky, fyziky a astronomie, Vol. 21 (1976), No. 4, 199--211

Persistent URL: http://dml.cz/dmlcz/139505

Súčasné trendy v algebre*)

*Garrett Birkhoff, Harvard University***)

1. Úvod

Symbolická algebra je omnoho staršia, než sa mnohí matematici domnievajú; jej počiatky siahajú prinajmenšom k DIOFANTOVI Z ALEXANDRIE (okolo roku 250 n. l.) a k BRAHMAGUPTOVI (asi r. 598–665 n. l.). O týchto skorých prácach sa možno viac dozvedieť v diele CAJORIHO ([1], odst. 101–105) a v BALLOVEJ práci ([2], str. 154–156). Ba aj tzv. „moderná" algebra je stará už viac ako storočie.

Keď si uvedomíme tento fakt, nebude ťažké uveriť, že veľmi rýchle počítače, ktoré máme dnes k dispozícii, umožňujú vznik nových trendov v algebre. Mojím cieľom je načrtnúť vám, v čom podľa mojej mienky spočívajú tieto trendy. Urobím tak v odsekoch 17 až 23. Predtým by som však chcel podať stručný prehľad vývoja, ktorým algebra, ako ju dnes poznáme, prešla v posledných storočiach.

2. Klasická algebra

Názov *moderná algebra* mal pôvodne (v r. 1930) vyjadrovať kontrast s *klasickou algebrou*, ktorá sa všeobecne chápala ako *teória rovníc*. Klasickú algebru by sme mohli definovať tiež ako umenie riešiť *numerické problémy* pomocou *narábania so symbolmi*. Zdá sa, že vznikla zásluhou AL-CHVARIZMIHO a ďalších islamských matematikov v r. 800–1000 n. l. Ako vieme, jej hlavná idea spočíva v tom, že každé slovné tvrdenie o *číselných* veličinách nahradíme symbolickou *rovnicou*, ktorú môžeme podľa známych a dokázaných všeobecných pravidiel upravovať tak, že dostávame postupnosť ekvivalentných a dúfajme čoraz jednoduchších rovníc. Pritom pôvodnú rovnicu pokladáme za vyriešenú, ak sa nám podarilo osamostatniť na jednej strane znaku rovnosti neznámu veličinu, pričom na druhej strane je výraz obsahujúci len známe veličiny.

Hoci pôvod slova „koreň" (rovnice) možno sledovať až k sanskritu[1]) a výraz „mocnina" (čísla) sa objavuje v Al-Chvarizmiho *Algebre* (al-džebr), klasická algebra sa len

---

*) G. BIRKHOFF: *Current Trends in Algebra*, Amer. Math. Monthly *80* (1973), 760–782.

V tomto čísle otiskujeme první část článku, jehož překlad pořídili JOZEF DRAVECKÝ a PETER MEDERLY. Redakce chce překladem přiblížit čtenářům zamyšlení G. Birkhoffa o tendencích v současné algebře; článek, který je ilustrován řadou historických faktů, však není historickou studií.

**) GARRETT BIRKHOFF je profesorom čistej a aplikovanej matematiky na Harvardskej univerzite. Bol prezidentom SIAM, viceprezidentom Americkej matematickej spoločnosti (AMS), Matematickej asociácie Ameriky (MAA) a Americkej akadémie umení a vied.

[1]) Za tento fakt, ako aj za iné fakty som zaviazaný profesorovi DAVIDOVI PINGREEMU (Brown University); ďalšími veľmi užitočnými pripomienkami prispeli THOMAS HAWKINS, GIAN-CARLO ROTA, GERALD SACHS a JOHN TATE.

postupne vyvíjala k dnešnému stavu. Arabská „al-džebr“ sa v západnej Európe nerozšírila a symboly + a − nadobudli dnešný význam až tesne pred r. 1500. Potom však nastal výraznejší pokrok; CARDANOVO dielo *Ars Magna* (1545) obsahovalo už riešenie kubickej rovnice a rovnice štvrtého stupňa pomocou radikálov.

V nasledujúcich dvoch storočiach sa algebra rozvíjala hlavne[2]) v súvislosti s aplikáciami. Jednalo sa o použitie algebry v (analytickej) geometrii, ktoré dalo jasný význam záporným číslam, a tiež o aplikácie v oblasti infinitezimálneho počtu pre počítanie s nekonečnými radmi. Až do obdobia po r. 1750 význam imaginárnych koreňov a komplexných čísiel zostal hmlistý a dokonca aj úvahy o sústavách lineárnych rovníc a o determinantoch boli nesystematické a útržkovité.

Medzi rokmi 1750 a 1830 sa však klasická algebra najmä vďaka práci EULERA, LAGRANGEA a GAUSSA rýchlo vyvíjala a dostala sa takmer až na dnešnú úroveň. Tak napríklad sa zaviedla definícia exponenciálnej funkcie exp z pre všetky komplexné z ako súčet istého mocninného radu, takže bolo možné pre všetky kladné čísla a a komplexné čísla z definovať mocninu a^z vzťahom $a^z = \exp(z \ln a)$. Euler v ([3], str. 27) zaviedol tiež „Lagrangeovu rezolventu“.

Predovšetkým však bola uznaná za základnú, jasne formulovaná a dokázaná základná veta algebry. Euler sa zaoberal jej formuláciami v *reálnej* oblasti. Dve z nich, zrejme navzájom ekvivalentne, sú:

(a) Každý reálny polynóm stupňa $n > 2$ má vlastného deliteľa.

(b) Každý reálny polynóm sa dá jednoznačne rozložiť na súčin reálnych lineárnych a kvadratických polynómov.

Platnosť podmienky (a) plynie pre $n < 5$ z Cardanových úvah a pre $n = 5$ z faktu, že každý reálny polynóm nepárneho stupňa má reálny koreň. Euler sa uspokojil s konštatovaním, že podmienka (a) platí pre všetky n, ale jeho dôkaz je nejasný.

Ľahko sa dá ukázať, že podmienky (a) a (b) sú ekvivalentné aj s obvyklou formuláciou základnej vety algebry:

(c) Každý polynóm s komplexnými koeficientami sa dá rozložiť na súčin lineárnych faktorov.

Asi od r. 1800 Gauss podal viacero pomerne presných dôkazov tvrdenia (c) a tiež ukázal, že všetky polynomické rovnice majú riešenia vyjadrené pomocou komplexných čísiel $x + yi$, $i = \sqrt{(-1)}$, pričom geometrickým znázornením komplexných čísiel bodmi v (x, y) − rovine získali tieto riešenia viac než len symbolický význam. Gauss okolo r. 1825 vypracoval systematické iteračné, ako aj eliminačné metódy na riešenie sústav lineárnych rovníc, a všeobecne známymi sa stali pravidlá o determinantoch.

O niekoľko rokov neskôr GALOIS a ABEL ukázali nemožnosť riešenia všeobecnej rovnice piateho stupňa pomocou radikálov[3]) a odvtedy matematici čoraz viac obracali pozornosť z teórie rovníc na *nenumerické* aplikácie symbolickej algebry (napr. na grupy, vektory a matice).

---

[2]) Pozoruhodnou výnimkou je binomická veta, ktorú objavil PASCAL v roku 1653. O faktoch zhrnutých v tomto odseku sa píše v prácach ROUSE BALL [2] a E. T. BELL [6].

[3]) Ich výklady boli veľmi hmlisté; pozri G. BIRKHOFF, Isis *3* (1973), 260—267. GALOISOV dôkaz vyjasnil BETTI v r. 1852.

3. „Moderná“ algebra do r. 1860

Vďaka tomuto presunu pozornosti moderná algebra už pred rokom 1860 dosiahla niektoré pozoruhodné úspechy, a to aj napriek tomu, že reálna a komplexná algebra dominovala v učebnicovej literatúre cez celé storočie po r. 1830.

Skutočne už okolo r. 1770 sa Lagrange zaoberal „symetrickou grupou“ všetkých permutácií n písmen a jej podgrupami vediac, že hrajú dôležitú úlohu pri riešení všeobecnej polynomickej rovnice

$$x^n + a_1x^{n-1} + \ldots + a_n = (x-x_1)(x-x_2)\ldots(x-x_n) = 0 \tag{1}$$

pomocou radikálov. Vedľajším produktom tohoto záujmu bola Lagrangeova veta, že rád ľubovoľnej podgrupy grupy G delí rád grupy G.*)

K rozvoju teórie grúp pred r. 1845 prispeli tiež RUFFINI, GALOIS a CAUCHY ([3], str. 45–53). Galoisovým príspevkom základného významu v teórii polí je jeho konštrukcia (v r. 1830) *konečného poľa* s rádom rovným ľubovoľnej prirodzenej mocnine p^r prvočísla.**) (Formálne definície grúp a polí nájde čitateľ v odseku 4.)

O niečo skôr, v roku 1801, LEGENDRE a GAUSS dali podnet k štúdiu *komutatívnych okruhov* tým, že skonštruovali okruh Z_n celých čísel modulo n (tj. okruh, v ktorom množina všetkých celočíselných násobkov čísla n je nulou) a okruh $Z[i]$ všetkých Gaussových celých čísiel $m + ni$, kde $m, n \in Z$ sú celé čísla[4]) a $i = \sqrt{(-1)}$. Gauss naviac dokázal, že v $Z[i]$ platí veta o *jednoznačnom* rozklade na prvočinitele.

Okolo roku 1850 sa začali študovať tiež *nekomutatívne okruhy*. V r. 1843 zaviedol HAMILTON *kvaternióny*, špeciálnym prípadom ktorých sú komplexné čísla. Preto sa kvaternióny niekedy nazývajú aj *hyperkomplexnými číslami*. V prvom vydaní svojej knihy *Ausdehnungslehre* (1844) sa H. GRASSMANN zaoberá *vektorovou algebrou* (ktorá je dosť prirodzeným zovšeobecnením Descartesovej symbolickej metódy používanej v geometrii) a tiež – hoci trochu povrchne – hyperkomplexnými číslami vo všeobecnosti. Tieto pojmy upresnili (a ich spojitosť s n-rozmernou geometriou objasnili) CAYLEY, HAMILTON v úvode k svojej knihe o *kvaterniónoch* (1859) a GRASSMANN v druhom vydaní svojej knihy (1878). Cayley navyše v r. 1858 ([3], str. 84) ukázal, že teória determinantov, ktorú vypracovali VANDERMONDE a LAPLACE, je len jednou stránkou omnoho mohutnejšej teórie, a to *algebry matíc*. Algebra matíc sa podobá obvyklej algebre s tým rozdielom, že vo všeobecnosti pre matice A, B platí $AB \neq BA$, teda násobenie matíc podobne ako násobenie kvaterniónov nie je komutatívne. Matice, ktoré sú dnes ne-

---

*) Autor tu podáva dnešnú interpretáciu Lagrangeovej práce; Lagrange študoval „funkcie n písmen“ a zmeny ich hodnôt pri permutáciách. Pojem ani termín „grupa“ nepoužíval. Pozn. prekl.

**) Opät ide o modernú interpretáciu Galoisovho výsledku. Pozn. prekl.

[4]) Ako býva zvykom, označujeme písmenom Z (z nemeckého Zahl = celé číslo) množinu $\{0, \pm 1, \pm 2, \ldots\}$. Gauss prisudzuje úvahy o celých číslach modulo n („modulárnych číslach“) Legendreovi.

postrádateľné tak v čistej, ako aj v aplikovanej matematike a ktoré formálne zaviedol Cayley v r. 1858, postupne zrevolucionizovali lineárnu algebru.[5])

Krátko predtým sa otvorili dve ďalšie oblasti výskumu v modernej algebre. V roku 1854 uverejnil BOOLE svoje dielo *Introduction to the Laws of Thought* (Úvod do zákonov myslenia), v ktorom popísal podstatnú časť Aristotelovej logiky pomocou istej analógie s obvyklou algebrou, nazývanej teraz Booleovou algebrou. Táto nová „algebra logiky" okrem toho, že spĺňala väčšinu zákonov obvyklej algebry, spĺňala tiež kuriózne identity

$$a^2 = a + a = a$$

(dnes by sme to zapísali v tvare $a \wedge a = a \vee a = a$),

$$(a + b)\, a = a\,, \qquad (a + b)(a + c) = a + bc\,.$$

4. Axiomatický prístup

Ako sme práve videli, mnohé z hlavných oblastí tzv. modernej algebry (ktorú autori populárnej literatúry v posputnikovej ére prekrstili na „novú matematiku") poznali už matematici okolo r. 1860. No k axiomatickému skúmaniu základov algebry došlo až neskôr. Lagrange odvodil Lagrangeovu vetu o grupách a Galois skonštruoval Galoisove polia nemajúc ani tušenia o axiomaticky definovaných grupách a poliach; predpoklady, ktoré používali vo svojich úvahách, boli úplne intuitívne. Dokonca aj názvy „komutatívny" a „distributívny" boli zavedené pre príslušné zákony až v roku 1814 (SERVOIS)[6]). Termín „asociatívny" pochádza z roku 1835 a zaviedol ho Hamilton.

Za svoje odpútanie od výlučného záujmu o reálne a komplexné čísla vďačí algebra vo veľkej miere filozofickým bádaniam PEACOCKA, WOODHOUSEA[7]), HAMILTONA, DE MORGANA, BOOLEA a CAYLEYHO. Napriek tomu však tvrdenie E. T. BELLA, že to bol Peacock, ktorý „prvý pochopil všeobecnú algebru ako hypoteticko-deduktívnu vedu Euklidovho vzoru", je prehnané. Hoci Peacock predišiel HANKELA, čo sa týka „princípu stálosti ekvivalentných foriem", jeho kniha *Symbolical Algebra*, podobne ako H. Grassmannova *Ausdehnungslehre*,, sa zaoberá hlavne geometrickými aplikáciami a axiómy alebo postuláty sa v nej ani len nespomínajú.[8])

[5]) Podrobný historický prehľad o lineárnej a nekomutatívnej algebre nájde čitateľ v diele N. BOURBAKI ([8], str. 78—91 a 120—128). O Cayleyho príspevku si možno prečítať na str. 102—115 práce E. T. Bell [5].

[6]) GERGONNEOVE *Annales 5* (1814—15) str. 93; HAMILTONOVE idey možno nájsť v jeho *Mathematical Papers*, vol. III, Cambridge Univ. Press, 1967. LEIBNIZ a CRAMER mali veľmi útržkovité predstavy o determinantoch; pozri ([2], str. 375) a D. J. STRUIK, *A Source Book in Mathematics*, Harvard University Press, 1969, str. 180.

[7]) R. WOODHOUSE, Phil. Trans. *91* (1801), 89—119; G. PEACOCK, Reps. Brit. Assn. Adv. Sci. *3* (1834), 185—232 a *Algebra*, 2 zväzky, 1845; A. DE MORGAN, Trans. Camb. Phil. Soc., *7*, (1839), 173—187 a 287—300; G. BOOLE, Cambridge and Dublin Math. J. *3* (1848), 183—198.

[8]) F. KLEIN, *Entwicklung der Mathematik im 19ten Jahrhundert*, vol. 1, str. 175 ju charakterizoval ako takmer nečitateľnú.

Oveľa jasnejšie ozrejmujú úlohu axióm práce *Formenlehre* (R. GRASSMANN, 1872), *Operationskreis der Logikkalkul* (E. SCHRÖDER, 1877), ako aj axiomatické skúmanie grúp, polí, modulov a ideálov, ktorým sa zaoberali CAYLEY (1878), FROBENIUS a STICKELBERGER (1879), DEDEKIND[9]), WEBER (1882, 1893) a E. H. MOORE. Túto problematiku skúmali nezávisle aj BENJAMIN PEIRCE a jeho syn C. S. PEIRCE v Harvarde (1870 – 1881).[10])

Pod vplyvom týchto prác začína v roku 1888 pracovať na axiomatickom prístupe k aritmetike PEANO.[11]) Neskôr poviem o tomto probléme omnoho viac. O desať rokov neskoršie sa pokúsil HILBERT vo svojich *Grundlagen der Geometrie* [4] ďalej zdokonaliť EUKLIDA. Keď sa na jeho pokus pozeráme z hľadiska exaktnosti, môžeme konštatovať, že bol úspešný. Nedá sa to však povedať, ak berieme do úvahy hľadisko pedagogické. No jeho najdôležitejším príspevkom k axiomatike bola jasná formulácia pojmov nezávislosti, konzistencie a úplnosti axiomatického systému.

V roku 1902 E. H. Moore ukázal, že ani Hilbertove axiómy nie sú nezávislé. V ďalších desiatich rokoch E. V. HUNTINGTON, L. E. DICKSON a O. VEBLEN pracne analyzovali nezávislosť systémov postulátov pre grupy, pre polia vo všeobecnosti a špeciálne pre polia komplexných a reálnych čísel, pre algebru logiky a pre základy geometrie. Vynikajúci pohľad na túto prácu poskytujú články Moorea a Huntingtona[12]). Farbistejší, aj keď nie natoľko hodnoverný prehľad obsahuje aj ([5], kap. 3).

Čiastočne aj pod vplyvom uvedených prác sa konečne v algebre presadil axiomatický prístup. Matematici prišli na to, že aj prekvapujúco malý počet jednoduchých postulátov (oveľa menší ako v Euklidovej geometrii[13])) môže tvoriť dostatočný základ pre veľmi rozsiahle algebraické teórie. Napríklad všetky tvrdenia teórie grúp sa dajú odvodiť zo základných princípov logiky a nasledujúcich postulátov (pochádzajúcich od E. V. Huntingtona z roku 1906).

Definícia. *Grupa G* je množina prvkov (ktoré budeme označovať malými latinskými písmenami), z ktorých každé dva – povedzme x a y – majú *súčin* xy, pričom sú splnené tieto podmienky:

G1. Násobenie je *asociatívne*: $x(yz) = (xy)z$ pre všetky $x, y, z \in G$.

G2. Pre každé dva prvky $a, b \in G$ existujú $x, y \in G$ tak, že $xa = b$ a $ay = b$.

(Zápis $x \in G$, ktorý sme použili vyššie, pochádza od Peana a znamená, že x je prvkom (patrí do) množiny G.)

Dôvtipnými obratmi sa dajú z týchto postulátov odvodiť rôzne iné jednoduché tvrdenia. Napríklad: (i) každá grupa G obsahuje jediný idempotentný prvok e, t. j. prvok

---

[9]) V svojich dodatkoch k DIRICHLETOVÝM *Vorlesungen über Zahlentheorie*, 1863, 1871.

[10]) BENJAMIN PEIRCE, *Linear Associative Algebra*, Boston 1870; pozri tiež Amer. J. Math. *3* (1880), 15—57 a *4* (1881), 97—229 (prevzaté z Proc. Am. Acad. Boston, 1875).

[11]) Pozri jeho zobrané diela *Collected Papers*, vol. 2, Cremonese, Rím, 1958, str. 134. Na strane 152. zväzku *Semicentennial Addresses* Americkej matematickej spoločnosti BELL prisúdil axiomatický prístup Peanovi. Peano tiež ako prvý *čísloval* svoje teorémy.

[12]) Vo zväzkoch *3 – 6* (1902—1905), Transactions of the American Mathematical Society je tucet článkov o axiomatických systémoch od spomínaných matematikov.

[13]) EUKLIDOVE *Základy*, obsahujúce „axiómy" pre veličiny (algebra) a tiež „postuláty" geometrie, boli napísané v Alexandrii v Egypte okolo roku 300 pr. n. l.; pozri BALL [2].

spĺňajúci rovnosť $ee = e$, (ii) pre tento prvok platí $ex = xe = x$ pre všetky $x \in G$ (teda e je akousi jednotkou v G), (iii) prvky x, y v G2 sú prvkami a, b určené jednoznačne, atď.

Podobne celá teória polí sa dá odvodiť z nasledujúcej množiny postulátov, ktorá tiež pochádza od Huntingtona.

Definícia. *Pole* je množina F prvkov, z ktorých každé dva majú ***súčet*** $x + y$ a ***súčin*** xy, pričom platí:

F1. Sčítania a násobenie sú *komutatívne*:

$$x + y = y + x \quad \text{a} \quad xy = yx \quad \text{pre všetky } x, y \in F.$$

F2. Sčítanie a násobenie sú *asociatívne*:

$$x + (y + z) = (x + y) + z\,, \qquad x(yz) = (xy)z \quad \text{pre všetky } x, y, z \in F.$$

F3. Násobenie je *distributívne* vzhľadom k sčítaniu:

$$x(y + z) = xy + xz \quad \text{pre všetky } x, y, z \in F$$

F4. Pre každé $a, b \in F$ existuje $x \in F$ tak, že $a + x = b$.

F5. Ak $a + a \neq a$ tak existuje také $y \in F$, že $ay = b$.

(Huntington v skutočnosti zoslabil F5 tým, že pridal k predpokladom ešte podmienku $b + b \neq b$.)

(Prirodzene predpoklad $a + a \neq a$ je len iným spôsobom sformulované tvrdenie, že $a \neq 0$. Voliť túto cestu bolo nutné preto, lebo Huntington sa chcel vyhnúť tomu, aby musel predpokladať, že v F existuje „nula" 0.)

Použitie axiomatického prístupu v algebre spojené s uvedomením si dôležitosti všetkých druhov algebraických systémov bolo stimulom, ktorý priviedol matematikov k pokusom o nájdenie ***všetkých možných algebraických systémov*** spĺňajúcich isté podmienky. Ako príklad môže slúžiť problém nájsť všetky konečné polia (tento problém vyriešil už Galois) alebo problém nájsť všetky grupy daného rádu n atď. Pri takomto hľadaní musíme však stotožniť všetky grupy (alebo polia), ktoré sú *izomorfné*, t. j. ktorých prvky môžeme vzájomne jednoznačne priradiť pomocou *bijekcie zachovávajúcej grupové násobenie* (v poliach musí takáto bijekcia zachovávať sčítanie a násobenie). Takáto bijekcia sa nazýva *izomofirzmom*.

5. Morfizmy a podalgebry

Je užitočné poznať odpoveď na všeobecnejšiu otázku, kedy medzi dvomi algebraickými systémami A a B existuje (*homo*)*morfizmus* čiže zobrazenie $\Theta : A \to B$, ktoré zachováva všetky definujúce operácie. Konečne je tiež užitočné poznať *podalgebry* algebraického systému A, t. j. podmnožiny S množiny A, ktoré spĺňajú všetky postuláty. Ak S je podalgebrou A, nazýva sa A *rozšírením* S. (Teda pole komplexných čísiel je rozšírením poľa reálnych čísiel.) Aby sme zistili, či nejaká podmnožina je podalgebrou, stačí obvykle zistiť, či je uzavretá vzhľadom na vhodne vybraté operácie. Napríklad u grúp podgrupa musí obsahovať (i) jednotku, (ii) s každým x tiež x^{-1} a (iii) s x a y aj xy. Pri poliach zasa treba požadovať *uzavretosť* vzhľadom na sčítanie, odčítanie, násobenie a delenie.

Pojmy, ktoré sme tu spomenuli, sa dajú aplikovať na všetky bežné algebraické systémy.

6. Niektore podstatné výsledky vývoja v rokoch 1860—1914

V tom istom období, keď sa pomocou axiomatickej metody objasnili základy algebry, rozvíjala sa táto veda mohutne tak do šírky, ako aj do hĺbky. Na tomto mieste môžeme len veľmi stručne načrtnúť niekoľko veľmi významných výsledkov.

Po prvé, Galoisova teória sa objasnila nasledujúcim spôsobom (pridržím sa kvôli určitosti rozšírení poľa Q racionálnach čísel, ale výsledky možno zovšeobecniť na rozšírenie ľubovoľného poľa). Nech $F = Q\,[x_1, \ldots, x_n]$ je pole generované koreňmi polynómu

$$p(x) = (x-x_1)(x-x_2)\ldots(x-x_n) = x^n + a_1x^{n-1} + \ldots + a_n = 0$$

s koeficientmi $a_k \in Q$. Definujme *Galoisovu grupu* $G(F:Q)$ poľa F a polynómu $p(x)$ nad Q ako grupu všetkých automorfizmov α poľa F takých, že pre každé $x \in Q$ platí $\alpha(x) = x$. Galoisova veta potom tvrdí, že rovnica $p(x) = 0$ je riešiteľná *radikálmi* vyjadrenými pomocou koeficientov (čiže radikálmi nad Q) práve vtedy, keď Galoisova grupa $G(F:Q)$ je riešiteľná v nasledujúcom zmysle.

Definícia. *Kompozičným radom* konečnej grupy G sa nazýva reťazec

$$1 < S_1 < S_2 < \ldots < S_r = G$$

podgrúp grupy G, z ktorých každá je maximálnou normálnou podgrupou nasledujúcej. Vytvorme prislúchajúce faktorové grupy S_k/S_{k-1}. Potom hovoríme, že G je *riešiteľná* ak všetky tieto faktorové grupy sú *abelovské* (ekvivalentný výrok je, že všetky majú prvočíselný rád).

Po druhé, prehĺbila sa čistá teória grúp. Spomedzi mnohých význačných viet o konečných grupách dokázaných v polstoročí 1860—1914 spomeniem len niektoré. Ponajprv sa dokázalo, že množina faktorových grúp S_k/S_{k-1} je pre všetky kompozičné rady rovnaká až na izomorfizmus a prerovnanie (Jordanova-Hölderova veta). Opäť sa ukázalo, že každá grupa s rádom p^n, kde p je prvočíslo, je riešiteľná. A konečne bol podaný dôkaz, že ak p^n delí rád grupy G, tak G má podgrupu rádu p^n (Sylowova veta).

Po tretie, v oblasti algebraickej teórie čísiel Dedekind rozpracoval teóriu ideálov a pomocou nej zovšeobecnil Gaussove priekopnícke výsledky o jednoznačnom rozklade Gaussových celých čísel na skvelú vetu o jednoznačnom rozklade v ľubovoľnom poli algebraických čísiel (t. j. v ľubovoľnom podpoli poľa C komplexných čísiel, ktorého lineárna dimenzia nad podpoľom Q racionálnych čísiel je konečná). Konkrétne dokázal, že rozklad na prvoideály je jediný.[14])

[14]) Historická diskusia o teórii ideálov a DEDEKINDOVÝCH výsledkoch o algebraických číslach je v práci [6] kap. 10.

Hlbší záujem o teóriu ideálov a o rozklad na prvočinitele viedol Dedekinda aj k skúmaniu operácií najväčšieho spoločného deliteľa (n. s. d.) a najmenšieho spoločného násobku (n. s. n.) z axiomatického hľadiska. Keď si všimol ich analógiu s operáciami „a" a „alebo" v Booleovej algebre, rozvinul a využil elementárnu teóriu *zväzov* (*Dualgruppen*), *modulárnych zväzov*, *distributívnych zväzov* a *vektorových zväzov* v dvoch priekopníekych prácach (1897, 1901), čím založil nové veľké odvetvie algebry zahrnujúce Booleove algebry ako špeciálny prípad.

7. Lineárne asociatívne algebry

V roku 1870, približne v rovnakom čase keď Dedekind rozvinul teóriu ideálov na mocný matematický nástroj, Benjamin Peirce z Harvardu ako jeden z prvých skúmal systémy hyperkomplexných čísiel, ktoré zhruba načrtli už Grassmann, Hamilton a Cayley. Peirce začal definíciou lineárnej algebry nad poľom F ako množiny A, ktorej prvkami sú ľubovoľné lineárne kombinácie

$$(2) \qquad \boldsymbol{a} = (a_1, \ldots, a_r) = a_1 \boldsymbol{i}_1 + \ldots + a_r \boldsymbol{i}_r$$

$\boldsymbol{r}$ bázových prvkov $\boldsymbol{i}_k$, pričom pre násobenie platí pravidlo

$$(2') \qquad \boldsymbol{a} \,.\, \boldsymbol{b} = (\sum a_k b_m)\, \boldsymbol{i}_k \,.\, \boldsymbol{i}_m = \sum a_k b_m \gamma_{kmn} \boldsymbol{i}_n \,;$$

konštanty γ_{kmn} môžu byť ľubovoľné skaláry (prvky poľa F). Lineárnu algebru nazva *asociatívnou*, ak násobenie definované vzťahom (2') je asociatívne.

Zvlášť pozoruhodnou lineárnou asociatívnou algebrou je množina Hamiltonových kvaterniónov; táto algebra má štyri bázové prvky $\boldsymbol{1}$, $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$, a teda 64 konštát (z ktorých väčšina sa rovná nule) daných vzťahmi

$$(3) \qquad \boldsymbol{1} \,.\, \boldsymbol{a} = \boldsymbol{a} \,.\, \boldsymbol{1} = \boldsymbol{a} \text{ pre všetky } \boldsymbol{a}, \qquad \boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -\boldsymbol{1}$$

$$(3') \qquad \boldsymbol{i} \,.\, \boldsymbol{j} = -\boldsymbol{j} \,.\, \boldsymbol{i} = \boldsymbol{k}\,, \qquad \boldsymbol{j} \,.\, \boldsymbol{k} = -\boldsymbol{k} \,.\, \boldsymbol{j} = \boldsymbol{i}\,, \qquad \boldsymbol{k} \,.\, \boldsymbol{i} = -\boldsymbol{i} \,.\, \boldsymbol{k} = \boldsymbol{j}\,.$$

Identity (3') sú zrejme identitami pre vektorové súčiny. Algebra kvaterniónov $R[\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}]$ nad poľom reálnych čísel je tiež príkladom *algebry s delením*: ku každému nenulovému kvaterniónu $\boldsymbol{a} = a_0 + a_1 \boldsymbol{i} + a_2 \boldsymbol{j} + a_3 \boldsymbol{k} \neq 0$ existuje inverzný kvaternión

$$(3'') \qquad \boldsymbol{a}^{-1} = (a_0 - a_1 \boldsymbol{i} - a_2 \boldsymbol{j} - a_3 \boldsymbol{k}) / (a_0^2 + a_1^2 + a_2^2 + a_3^2)\,.$$

Peirce[15]) dokázal, že jedinými algebrami s delením nad poľom reálnych čísiel, ktorých prvky sú hyperkomplexné čísla, sú algebra komplexných čísiel a algebra kvaterniónov.

Ešte významnejšia je *algebra $M_n(F)$ všetkých štvorcových matíc $A = \|a_{km}\| = \Sigma a_{km} e_{km}$* typu $n \times n$. Bázové prvky e_{km} algebry $M_n(F)$ sa násobia podľa pravidla

$$(4) \qquad e_{km} e_{k'm'} = \begin{cases} e_{km'}\,, & \text{ak } m = k' \\ 0 & \text{inak} \end{cases}$$

---

[15]) Vyššie citované dielo, str. 216—229. Ten istý výsledok dokázal nezávisle FROBENIUS v diele citovanom nižšie.

Konštantami teda sú (v trochu zmenenom označení)

$$(4') \qquad \gamma_{km,k'm',k''m''} = \begin{cases} 1, & \text{ak } k' = m, k'' = k, m'' = m' \\ 0 & \text{inak} \end{cases}$$

Od roku 1870 sa mnoho matematikov pokúsilo klasifikovať lineárne asociatívne algebry nad poľom reálnych a komplexných čísiel, pričom vhodne používali základnú vetu algebry. Osobitne treba spomenúť práce FROBENIA (1878, 1903), MOLIENA (1893) a CARTANA (1898).[16])

V pozoruhodnom článku uverejnenom v roku 1907 WEDDERBURN ukázal, že väčšinu Cartanových a Frobeniových štruktúrnych viet možno dokázať pre lineárne asociatívne algebry nad ľubovoľným poľom. Špeciálne dokázal nasledujúci základný výsledok, ktorého presný význam vysvetlím neskôr. Podrobnosti nájde čitateľ v práci ([6], kap. 11). Wedderburn sám tvrdil, že „väčšinu výsledkov obsiahnutých v tomto článku odvodili Cartan a Frobenius pre algebry nad poľom racionálnych čísiel“.

(i) Každá lineárna asociatívna algebra je priamym súčtom (v zmysle vektorových priestorov) „polojednoduchej“ podalgebry a jednoznačne určenej „nilpotentnej“ invariantnej podalgebry.

(ii) Polojednoduchý sčítanec v (i) je priamym súčtom jednoduchých lineárnych asoasociatívnych algebier, ktoré sú jednoznačne určené.

(iii) Každý *jednoduchý* sčítanec v (ii) je pre vhodne zvolené n algebrou $M_n(D)$ všetkých matíc $A = \|a_{ij}\|$ typu $n \times n$ s prvkami a_{ij} z vhodnej algebry s delením D nad poľom F skalárov pôvodnej lineárnej asociatívnej algebry.

Na objasnenie (i) si pripomeňme, že lineárna algebra sa nazýva *nilpotentná,* ak pre niektoré prirodzené číslo n sa všetky súčiny $a_1 . a_2 . \ldots . a_n$ rovnajú nule. Podalgebra algebry je jej podmnožina uzavretá vzhľadom na sčítanie a násobenie (a tiež vzhľadom na lineárne kombinácie nad poľom skalárov); podalgebra K sa nazýva invariantná, ak pre každé $k \in K$ a ľubovoľný prvok a, ktorý nemusí byť z K, platí $a . k \in K$ a $k . a \in K$; táto podmienka znamená, že K je *ideálom* v zmysle teórie okruhov.

Nie všetky lineárne algebry sú asociatívne. Najvýznamnejšou triedou neasociatívnych algebier sú *Lieove algebry.* V nich je asociatívny zákon nahradený troma identitami:

$$[aa] = 0\,, \qquad [ab] + [ba] = 0\,,$$

$$[[ab]c] + [[bc]a] + [[ca]b] = 0\,,$$

ktoré platia pre každé a, b, c. V sedemdesiatych rokoch minulého storočia LIE ukázal, že reálne a komplexné Lieove algebry sú kľúčom k pochopeniu *spojitých grúp* konečnej dimenzie. Mimoriadne veľký význam mal preto KILLINGOV (1888–1890) a ÉLIE CARTANOV (1894) dôkaz, že pre Lieove algebry platia štruktúrne vety analogické uvedeným štruktúrnym vetám pre asociatívne algebry, a tiež stanovenie všetkých „jednoduchých“ Lieových algebier nad C. Táto práca Killingera a Cartana týkajúca sa štruktúry Lieových

[16]) G. FROBENIUS, Crelle, *84* (1878), 1–63 a Berlin Sitzb. (1903), 504–537 a 634–635. WEDDERBURNOVE *Lectures on Matrices,* Amer. Math. Soc. 1934 obsahujú úplnú bibliografiu do r. 1933.

algebier predišla analogickú Molienovu a Cartanovu prácu o lineárnych asociatívnych algebrách.[17])

Tento opis vývoja možno azda uzavrieť konštatovaním, že algebraici, ktorí sa zaoberali výskumom, vedeli v roku 1914 viac o „modernej“ algebre, ako dnes vie väčšina nositeľov titulu Ph.D. (anglosaská analógia hodnosti CSc. – pozn. prekl.). Algebra však bola stále podriadená klasickej analýze a vláde poľa komplexných čísiel. To dokumentuje aj skutočnosť, že z dvoch najrozšírenejších učebníc vyššej algebry (spracovanej mimo rámca teórie čísiel) v r. 1900 sa WEBEROVA začínala kapitolou o algebraických funkciách a SERRETOVA kapitolou o reťazových zlomkoch.

8. Symbolická logika pred Gödelom

V retrospektívnom pohľade ani veľmi neprekvapuje, že dramatické úspechy algebraikov a logikov 19. storočia dali podnet matematikom s fantáziou, aby rozpracovali *symbolickú logiku,* pomocou ktorej by sa dokazovanie viet zjednodušilo na mechanické narábanie so symbolmi podľa vopred daných pravidiel čiže axióm. História tejto idey siaha prinajmenšom k LEIBNIZOVI, ktorý už okolo roku 1700 predvídal symbolické metódy, ktoré „umožnia zväčšiť schopnosti rozumu oveľa viac, ako hociktorý optický prístroj kedy zväčšil schopnosti zraku“. Jeho plodná myseľ by bola v účinnej symbolickej algebre diferenciálneho a integrálneho počtu (z ktorého veľká časť vďačí práve jemu za svoj vznik) zaiste videla priame potvrdenie veľkých možností symbolickej metódy.

Symbolický prístup v nebývalej miere rozvinul PEANO od r. 1889. Jeho hlavné príspevky sa nachádzajú v jeho diele *Formulario Matematico* (5. vydanie, 1908), v ktorého úvode sa hovorí: „Celý pokrok v matematike je odpoveďou na zavedenie symbolov (ideografických znakov). ... Ak máme na výber, má vo všeobecnosti prednosť taký systém symbolov, ktorý má symbolov menej. Základné použitie symbolických metód spočíva v zjednodušení výpočtov.“ Úvod ďalej pojednáva o pôvode rozličných symbolov napr. $+$, $\times$, D (derivácia), $\int$ a symbolov vektorovej a Booleovej algebry. Navrhuje potom do všeobecného používania symboly $\in$ (patrí do) a $\exists$ (existuje). Peano tvrdí, že pomocou týchto a zopár ďalších symbolov a konvencií možno celú matematiku podať v symbolickej forme.[18])

V skutočnosti však Peano nebol prvým matematikom, ktorý prišiel s myšlienkou čisto symbolickej matematiky. Už v r. 1634 HÉRIGONE napísal v úvode svojho *Cursus Mathematicus*: „Vymyslel som novú metódu robenia dôkazov, ktorá je stručná, zrozumiteľná a nepoužíva žiadny jazyk“. Jeho symboliky sa pridržiaval WALLIS (1656) a BARROW (1655, 1660).[19])

Peano potom opodstatňuje svoje tvrdenie na 386 stranách textu, ktorý obsahuje

---

[17]) Pozri THOMAS HAWKINS, Archive for History of Exact Sciences *8* (1972), 243—287.

[18]) Podobný symbolický štýl použil E. H. MOORE v *Introduction to a Form of General Analysis*, New Haven Colloquium, Yale Univ. Press, 1910.

[19]) Pozri F. CAJORI, *Past struggles between symbolists and rhetoricians ...*, Proc. Int. Math. Congress Toronto (1924), vol. 2, str. 937—941.

v symbolickom prehľade (1) matematickú logiku, (2) aritmetiku, (3) algebru, (4) vektorový počet („geometriu“), (5) limity, (6) derivácie, (7) integrály. Najúspešnejšie sú časť (1) a časť (2), v ktorej sa nachádza Peanova slávna konštrukcia[20]) nezáporných celých čísel pomocou funkcie nasledovníka: $1 = 0+$, $2 = 1+$, $3 = 2+$, ..., a vynikajúce odvodenie zákonov aritmetiky z tejto funkcie. Na ďalších 70 stranách Peano rozširuje svoju čisto symbolickú metódu na skúmanie rovinných kriviek, diferenciálnych rovníc a rozličných iných objektov.

Na Peanovo *Formulario* treba hľadieť predovšetkým ako na podnetný bohatiersky čin, hoci obsahuje bohatstvo ideí a originálnych pohľadov. Nikde však nenájdeme zoznam pravidiel pre narábanie so symbolmi pri prechode od jedného vzorca k druhému; neuvádza sa ani systém axióm logiky. Podobne ako Euklidove dôkazy v geometrii možno Peanove dôkazy overiť len tak, že sa slovám priradí ich *význam*.

Tento najvážnejší nedostatok odstránili WHITEHEAD a RUSSELL v trojzväzkovom majstrovskom diele *Principia Mathematica* [7]. V ňom starostlivo špecifikovali pravidlá pre manipuláciu so symbolmi („pravidlá inferencie“), ktoré možno neomylne použiť pri odvodzovaní dôsledkov z predpokladov v symbolickej logike (v matematických úvahách).

Keď tieto pravidlá inferencie použili ako axiómy symbolickej logiky, ukázali Whitehead a Russell, že možno symbolicky prepísať aspoň konštrukciu poľa R reálnych čísiel z prirodzených čísiel a tiež veľkú časť teórie množín a aritmetiky. Tieto významné výsledky uviedli ako empirické odôvodnenie tézy, že *všetko dokazovanie matematických viet možno redukovať na mechanické narábanie so symbolmi* čiže na čistú symbolickú logiku.[21])

Nikto nepopiera Whiteheadovo a Russellovo tvrdenie, že ich pravidlá inferencie pre „peančinu“ (Peanov symbolický jazyk) (i) sú neomylné za podmienok, ktoré uvádzajú po anglicky v texte a (ii) stačia pre veľkú časť elementárnej matematiky. No skutočný matematický obsah *Principií* (ktoré majú takmer 2000 strán) je oveľa menší než obsah Peanovej knihy a nemožno povedať, že by ich symbolické metódy „zväčšili schopnosti rozumu“; myslím, že ich vlastne *zmenšujú*, a to pravdepodobne z psychologických príčin.[22])

9. Hilbert a Gödel, 1918—1931

Vďaka tomu, že Russellova axiomatizácia logiky umožnila nahradiť špeciálne axiómy rozličných oblastí matematiky teorémami (por. prvý odstavec úvodu knihy *Principia Mathematica*), HILBERT sa o nej vyjadril v r. 1918, že je korunou axiomatiky.[23]) Hilbert pritom hovoril s autoritou človeka, ktorý len pred 20 rokmi v známom diele *Grundlagen*

[20]) Po prvý raz uverejnená v roku 1889 (*Arithmetices principia nova methodo exposita*).

[21]) Túto skutočnosť naznačil už o desať rokov skôr RUSSELL vo svojich vtipných *Principles of Mathematics*, ktorých druhým zväzkom mali byť podľa pôvodného zámeru *Principia Mathematica*.

[22]) Pozri G. BIRKHOFF, *Mathematics and Psychology*, SIAM Review *11* (1969), 429—469.

[23]) *Werke*, zväzok 3, str. 153; Math. Annalen *78*, 405—415.

der Geometrie vniesol rigoróznu presnosť do Euklidových axióm. Citujem z úvodu jeho knihy:

„Geometria – podobne ako teória čísiel – vyžaduje pre svoju *deduktívnu* (*folgerichtige*) konštrukciu niekoľko základných viet (*Grundsätze*). Tieto vety sa nazývajú axiómami[24]) a počas ich súvislého vývoja od Euklida boli mnoho ráz spracované. ... Táto kniha je novým pokusom o vypracovanie najjednoduchšieho úplneho systému axióm geometrie ... aby sa tak ozrejmil význam rozličných skupín axióm a dôsledky jednotlivých axióm."

V podobnom duchu *axiomatickej analýzy* Hilbert a jeho spolupracovníci, najmä spoluautori W. Ackermann a P. Bernays[25]) venovali po r. 1918 veľké úsilie *deduktívnemu* dokázaniu (pomocou metamatematických úvah) adekvátnosti Whiteheadových a Russellových axióm (odôvodnenie v diele *Principia Mathematica* bolo len empirické). Svoju pozornosť sústredili na dve hlavné otázky:

(i) Sú tie axiómy *bezosporné*, t. j. nemožno pomocou nich dokázať výrok p aj jeho negáciu $\sim p$?

(ii) Možno rozhodnúť o pravdivosti či nepravdivosti ľubovoľného daného tvrdenia (napr. v aritmetike) v konečnom počte krokov?

Azda tieto otázky upútali Hilberta aj preto, že analógiu prvej rozriešil v *Grundlagen der Geometrie*, keď použil Descartesovu geometriu ako model euklidovskej rovinnej geometrie, a otázku analogickú druhej rozriešil pre bázu ideálov v priestore polynómov pomocou všeobecných transfinitných úvah s použitím podmienky rastúcich reťazcov.

Kladnú odpoveď na otázku (i) podal Ackermann (ktorý predtým dokázal nadbytočnosť jednej z Whiteheadových a Russellových axióm) a von Neumann v r. 1927 za *vhodných obmedzujúcich podmienok*. Tieto podmienky majú vcelku technický ráz[26]) a na prvý pohľad sa zdali celkom neškodné, čo viedlo k optimistickému prijatiu Hilbertovho programu v rokoch 1927 až 1931.

Odpoveď na otázku (ii) čiže problém rozhodnuteľnosti (*Entscheidungsproblem*) je však negatívna; podal ju Gödel v r. 1931 pre aritmetické tvrdenia. Dôvtipným použitím metamatematických úvah, ktoré vlastne spočívajú na Cantorovej diagonálnej konštrukcii, odvodil z tejto nerozhodnuteľnosti *neúplnosť* Whiteheadovho, Russellovho a Hilbertovho systému, a to v tomto zmysle: Ak sa prijme za pravdivú dodatočná *axióma konzistencie*, že „nepravdivé formuly sú nedokázateľné", možno dokázať takú formulu z teórie čísiel, ktorá by inak nebola dokázateľná. Z toho vyplýva, že nemožno dokázať bezospornosť Hilbertových axióm, takže špeciálne otázka (i) je nerozhodnuteľná.

Gödelov článok tak rozbil Hilbertove veľké nádeje; Hermann Weyl[27]) napísal: „Gödel istým spôsobom očísloval symboly, formuly a postupnosti formúl v Hilbertovom

[24]) Hilbert nedodržiava Euklidovo rozlišovanie medzi „axiómami" (pre veličiny všeobecne) a „postulátmi" (pre geometrické objekty).

[25]) Prvý je spoluautorom [9] a druhý dvojzväzkových *Grundlagen der Mathematik* (1939).

[26]) Pozri S. C. Kleene, *Introduction to Metamatemathics*, Van Nostrand, 1932, str. 204—205. (Existuje ruský preklad — pozn. prekl.)

[27]) American Mathematical Monthly *53* (1946), 1—18. Pôvodný Gödelov článok vyšiel v Monats. Math. Phys. *38* (1931), 173—198.

formalizme a tak previedol tvrdenie o konzistencii na aritmetický výrok. Vedel dokázať, že tento výrok nemožno vo vnútri toho formalizmu ani dokázať ani vyvrátiť. To môže znamenať len dve veci: buď sa v úvahách, ktorými sa dokazuje konzistencia, vyskytuje nejaký obrat, ktorý v tom systéme nemá formálny náprotivok, t. j. nepodarilo sa nám úplne sformalizovať proces matematickej indukcie; alebo sa treba vôbec vzdať nádeje na striktne „finitistický" dôkaz konzistencie. Keď sa GENTZENOVI (1936) konečne podarilo dokázať konzistenciu aritmetiky, skutočne porušil toto obmedzenie tým, že vyhlásil za zrejmé úvahy takého typu, ktoré presahujú do Cantorovej „druhej triedy ordinálnych čísiel".

Gödelovým výsledkom sa náhle skončilo polstoročie optimizmu okolo symbolickej logiky aspoň v tej forme, ako ju rozpracovali Peano, Whitehead a Russell. Tento výsledok ukázal, že ich formalizácia nie je schopná rozriešiť paradoxy a nejednoznačnosti Cantorovej teórie nekonečných množín.[28])

Literatúra

[1] F. CAJORI: *A History of Mathematical Notations*, 2 vols., Chicago, Open Court 1928—9.

[2] W. W. ROUSE BALL: *A Short History of Mathematics*, 3. vyd. New York, Macmillan 1901.

[3] U. MERZBACH: ... *Development of Modern Algebraic Structures from Leibniz to Dedekind*, dizertačná práca Ph. D. Harvard 1965.

[4] D. HILBERT: *Grundlagen der Geometrie*, 1899; 2. vyd. 1901.

[5] E. T. BELL: *Mathematics: Queen and Servant of Sciences*, New York, Mc Graw-Hill 1940.

[6] E. T. BELL: *The Development of Mathematics*, New York, McGraw-Hill 1940.

[7] A. N. WHITEHEAD and B. RUSSELL: *Principia Mathematica*, 3 vols., Cambridge Univ. Presss 1911.

[8] N. BOURBAKI: *Éléments d'Histoire des Mathématiques*, Paris, Hermann 1960.

[9] D. HILBERT, W. ACKERMANN: *Grundzüge der theoretischen Logik*, 4. vyd., 1949.

[28]) Dotýkame sa tu otázok, ktoré starostlivo historicky spracoval N. BOURBAKI ([8], kap. 1) a tiež P. BERNAYS v HILBERTOVÝCH *Werke*, zv. 3, str. 196—217; v tom istom zväzku sú aj Hilbertove práce z logiky.