JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

Pedagogická fakulta

Slavní matematikové minulosti
(The famous scientists in the algebraical calculus)

Bakalářská práce

Michal Houška

České Budějovice

Duben 2008

Vedoucí bakalářské práce: Vypracoval :

Mgr. Petr Chládek, Ph.D. Michal Houška

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce pedagogickou fakultou elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

Datum.

23.4.2008 Michal Houška

Podpis studenta

Anotace

Bakalářská práce se zabývá nejslavnějšími matematiky, kteří se v historii zasloužili o největší rozkvět matematické disciplíny souhrnně nazývané algebra. Speciálně je zaměřená na hlavní objevy v oblasti lineární algebry. Matematici jsou vybíráni podle zásluh či objevů, které významně ovlivnily algebru a matematiku vůbec.

Summary

This paper reviews the life and work of some of the famous mathematicians, who greatly participated in the development of algebra throughout history.We will focus on the major breakthrough ideas concerning the field of linear algebra. Every person mentioned in this work is chosen according to his undeniable contribution to our view on algebra and on mathematics as whole.

Poděkování

Na tomto místě bych velmi rád poděkoval vedoucímu práce panu Mgr. Petru Chládkovi, Ph.D. , za pomoc při výběru a při návrhu zpracování jednotlivých částí práce, a také za individuální konzultace, které velmi přispěly ke zkvalitnění obsahu práce.

OBSAH

1. Úvod

Má bakalářská práce nese název Slavní matematikové minulosti. V této práci budou představeni nejslavnější matematici od 17. století, kteří mají největší podíl na rozvoji matematické algebry. Na začátku mé práce je charakteristika období 17. století až 19. století. Jeden z hlavních cílů práce je vhodný výběr matematiků reprezentujících danou disciplínu. Protože objem matematiků je veliký, je nutné uvést jen ty nejvýznamnější. Dalším problémem vyplývajícím z výběru je, že matematici té doby nebyli zaměřeni na jeden konkrétní matematický obor. Často se zabývali také nebeskou mechanikou, matematickou analýzou a podobně.

Každý matematik je rozdělen do dvou částí. Životopisná část je zaměřená především na studium vybraného matematika a jeho vzdělávání. Druhá část se zabývá tím, čím konkrétně matematici přispěli k rozvoji algebry.

2. Historie

2.1. 17. století

Půdu pro největší objev 17. století připravil P. de Fermat, svojí metodou určování maxima a minima funkcí.

V 17. století matematikové dostávají popud komunikovat a tak vytvářejí diskusní kroužky, ze kterých se tvoří akademie. První akademie byla založena v Neapoli roku 1560, potom Accademie dei Liencei v Římě (1603). Významní myslitelé 17.století vkládali naději do matematiky, že přinese všeobecnou metodu pro pochopení vesmíru a přírody. Proto se mnozí významní matematikové věnovali i filozofii.

V 17. století vznikla i teorie pravděpodobnosti, a to z myšlenek, které nadhodili matematikům B. Pascalovi a P. Fermatovi šlechtici, holdujícím hrám v karty a kostky.

2.2. 18. století

18. století se může pochlubit díly významných matematiků, a to Leibnize, bratrů Bernoulliových, Eulera, Lagrange a Laplace.

Počátky teorie grup sahají do posledních let 18. a počátku 19. století, kdy se začala vyvíjet jako důsledek rozvoje teorie algebraických rovnic, teorie čísel a geometrie. Prvními matematiky, kteří se zabývali touto oblastí byli Leonhard Euler, Joseph Louis Lagrange, Carl Friedrich Gauss, Niels Henrik Abel a Évariste Galois.

Z Bazilee pochází i nevýznamnější matematik 18. století L. Euler (1707 až 1783), který v letech (1741 – 1766) pracoval v Berlínské akademii pod zvláštní ochranou Fridricha 2. Předtím (1725 – 1741) se zdržoval v Petrohradě. Roku 1783 se znovu vrátil do Petrohradu, kde pracoval pod ochranou carevny Kateřiny až do své smrti.

Roku 1735 ztratil jedno oko a 1766 i druhé, ale ani to nezastavilo jeho tvorbu. Euler zanechal 886 vědeckých prací ze všech tehdy existujících disciplín matematiky.

Na Eulerovo dílo navázal Lagrange, Laplace a Gauss.

V období kdy Euler žil, neexistoval ještě přesně definovaný pojem limity, a tak mnohé jeho úvahy (například v teorii nekonečných řad) jsou z dnešního hlediska projevem jeho matematické intuice.
Z matematiků je třeba vzpomenout i na A. de Moivra, který vynikl v teorii komplexních čísel. Žil dlouho v Londýně. V Anglii spolu s Sterlingem a Landenem patřil k předním matematikům. Z francouzských matematiků tohoto období sem patří J. L. Lagrange a P. S. Laplace. K nejvýznamnějším Lagrangeovým výsledkům patří díla z oblasti variačního počtu a teorie čísel.

Vývoj matematiky v 18. století u nás charakterizuje úsilí držet krok s celosvětovým rozvojem. J. W. Pelikán vydal roku 1712 práci, ve které detailně rozpracoval aritmetické algoritmy v dvojkové soustavě a hodně pozornosti, i spolu s jinými autory věnoval i trigonometrii. Celková situace v matematice se u nás podstatně zlepšila v druhé polovině 18. století, kdy se vládní kruhy přesvědčily o potřebě podporovat matematicko – fyzikální vědy pro jejich užitečnost při zvyšování výroby.

Ke konci 18. století se na celém světě zmenšil zájem o matematické vědy, což pravděpodobně zavinil vzrůstající nezdravý pragmatismus. Typickým představitelem tohoto období je F. J. Gerstner. Byl dobrým matematikem a přednášejícím, ale nenapsal ani jednu matematickou práci. V tomto období se mezi matematiky rozšířilo pesimistické přesvědčení, že matematika v podstatě vyčerpala svou náplň. Zřejmě se předpokládalo, že vývoj matematiky úzce souvisí s rozvojem mechaniky a astronomií. Vývoj matematiky v 19. a 20. století však tento názor vyvrátil.

2.3. 19. století

Francouzská revoluce a v ní vyvolaná průmyslová revoluce příznivě působily na rozvoj matematicko-fyzikálních věd.

Vzniká „čistá“ a „aplikovaná“ matematika. Mnozí matematici působí na vysokých školách a stávají se specialisty, kteří aktivně pracují v určitých oblastech matematiky.

Na rozhraní mezi matematikou 18. a 19. století stojí jeden z nejvýznamnějších geniů matematiky K. F. Gauss (1777-1855). Od roku 1807, až do své smrti, pracoval v ústraní jako ředitel Astronomické observatoře v Gottingenu a profesor tamější univerzity. Jeho samotářský život a v neposlední řadě úsilí vyhnout se životním nepříjemnostem poznamenaly do určité míry jeho dílo.

Se jménem Gauss jsou spojené základní výsledky v teorii čísel a jeho kniha Disquisitiones arithmeticae je základním kamenem moderní teorie čísel. Gaussovy vědecké zájmy zasahovaly také do astronomie. Jeho zobrazení komplexních čísel body roviny podnítilo rozvoj teorie komplexních čísel a funkcí komplexní proměnné.

Gauss pravděpodobně už roku 1816 poznal neeuklidovskou geometrii, ale ve snaze vyhnout se osobním problémům tento poznatek ani jiné poznatky neuveřejnil.

Při rozvoji francouzské matematiky v tomto období měly významnou úlohu novodobé školy technického směru, vybavené vynikajícími učebnicemi.

V tomto období se objevují dva mladí vědci, jejichž dílo podstatně ovlivnilo další vývoj matematiky. E. Galois (1811-1832) a N. H. Abel (1802-1829).

Neúspěch snah o přímé řešení obecných algebraických rovnic vyššího, než čtvrtého stupně vedl k otázce, zda je takové řešení vůbec možné. Ruffini, Abel a Galois ukázali, že takové řešení neexistuje a postavili algebru (do té doby jen nauku o řešení rovnic) na zcela jiný základ — teorii grup.

V matematice se tak začaly z vnitřních problémů její výstavby tvořit teorie, které byly logicky správné a přitom často neodpovídaly žádné známé situaci z reálného světa. Začala nová etapa vývoje matematiky, kdy se předmětem zkoumání staly abstraktní kvantitativní vztahy a geometrické objekty, které čekaly, a mnohé čekají, na své praktické uplatnění.

Díky Galoisovu jedinečnému přístupu k práci s rovnicemi, vzniká studium základních operací v matematice. Veřejnost se s nimi seznámila až roku 1846, kdy je vydal Liouville v časopise Journal de Mathematiques. Galois zemřel ve 21 letech při souboji. Jeho matematické úvahy obsahovaly teorii grup, klíč k moderní algebře a geometrii.

Arthur Cayley položil základy algebraické geometrie a na jeho práci o maticích a lineární algebře navázal sir William Rowan Hamilton a Herman Günther Grassman. Koncem 19. století vypracoval Georg Cantor formální teorii množin, která odstranila některé neřešitelné paradoxy. Na jeho práci v teorii čísel navázali Julius Wilhelm, Richard Dedekind a Karl Theodor Wilhelm Weierstrass studiem iracionálních čísel.

Dalším významným matematikem tohoto období byl Nor N. H. Abel. Představil se krátkým spisem, uveřejněným roku 1824, ve kterém dokázal algebraické rovnice 5. a vyššího řádu řešit pomocí radikálů. Pronikavě zasáhl do teorie nekonečných řad, eliptických funkcí, teorie grup (Abelova grupa). Celý život byl vážně nemocen a zemřel v 27 letech.

1. Algebra

Algebra je odvětví matematiky, zabývající se abstraktními pojmy struktury (nějakého objektu) a vztahů (mezi nějakými objekty). Její výsledky mají významné uplatnění nejen v samotné matematice, ale také ve fyzice (teorie grup) nebo v nejrůznějších technických oborech. Veřejnosti je pod pojmem **algebra** známa takzvaná elementární algebra, což je část algebry zabývající se řešením (především polynomiálních) rovnic a jejich soustav.

3.1 Lineární algebra

Lineární algebra je odvětví matematiky, které se zabývá vektory, vektorovými prostory, soustavami lineárních rovnic a lineárními transformacemi. Jelikož vektorové prostory jsou důležitou součástí moderní matematiky, je lineární algebra důležitou součástí jak abstraktní algebry, tak funkcionální analýzy. Aplikovaná lineární algebra se využívá například v přírodních vědách nebo sociálních vědách.

Moderní lineární algebra vznikla v letech 1843 a 1844. V roce 1843 vymyslel William Rowan Hamilton kvaterniony. V roce 1844 Hermann Grassmann publikoval svou knihu *Die lineale Ausdehnungslehre*. V roce 1857 pak Arthur Cayley publikoval svou ideu matic (velikosti 2×2).

Lineární algebra má svoje počátky ve studiu vektorů v kartézském dvourozměrném a trojrozměrném prostoru. Vektor je tady směrovaná úsečka a je charakterizovaný jak svojí velikostí, která je dána délkou úsečky, tak svým směrem. Vektory mohou být používány k reprezentaci fyzikálních veličin, jako je například síla a mohou být navzájem sčítány a násobeny skalárem.

Moderní lineární algebra byla později rozšířena na prostory libovolné dimenze (i nekonečné). Vektorový prostor dimenze *n* se nazývá *n*-rozměrný prostor. Mnohé z užitečných vlastností 2 a 3-dimenzionálního prostoru mohou být rozšířeny na tyto prostory vyšší dimenze. Ačkoli si mnoho lidí nedokáže snadno představit vektory *n*-rozměrného prostoru, jsou tyto vektory neboli *n*-tice užitečné pro reprezentaci dat. Protože vektory nebo *n*-tice jsou *uspořádané* seznamy *n* komponent, je možné s daty v této podobě vhodně manipulovat. Například v ekonomii lze používat řekněme 8-dimenzionální vektory neboli osmice jako reprezentaci hrubého národního produktu 8 zemí. Mohli bychom se rozhodnout zobrazit HNP 8 zemí určitého roku, kde je dáno pořadí zemí, například (USA, Velká Británie, Francie, Německo, Španělsko, Indie, Japonsko, Austrálie), pomocí vektoru (v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8), ve kterém se HNP každé země nachází na odpovídající pozici.

Jako čistě abstraktní koncept, na kterém se dokazují věty, je vektorový prostor (nebo lineární prostor) součástí abstraktní algebry a je v této oblasti dobře integrován. Příkladem tohoto mohou být například grupy invertibilních lineárních zobrazení nebo matic a okruhy lineárních zobrazení vektorového prostoru. Lineární algebra také hraje důležitou roli v analýze, zvláště v popisu derivací vyššího řádu ve vektorové analýze a ve studiu součinu tenzorů a alternujících zobrazení.

Vektorový prostor se definuje nad polem, jako je třeba pole reálných čísel nebo pole komplexních čísel. Lineární operátory převádí prvky z jednoho lineárního prostoru do druhého (nebo do toho samého prostoru) a zachovávají přitom vektorové sčítání a násobení skalárem, dané na těchto vektorových prostorech. Množina všech takových transformací je také vektorovým prostorem. Je-li báze vektorového prostoru pevně zvolená, pak lze každou lineární transformaci zapsat ve formě matice. Detailní zkoumání vlastností matic a algoritmů prováděných na maticích, včetně výpočtu determinantu a vlastních vektorů a čísel matice, je součástí lineární algebry.

Obecná metoda, kdy je nalezen lineární způsob pohledu na nějaký problém, ten je pak vyjádřen v termínech lineární algebry a je vyřešen například pomocí matic, je jedna z nejvíce použitelných metod v matematice.

2. Seznam vybraných matematiků

Pierre de Fermat

Karl Friedrich Gauss

Niels Henrik Abel

William Rowan Hamilton

Evariste Galois

Charles Hermite

Felix Christian Klein

David Hilbert

Richard Hamming

4.1. Pierre de Fermat

Pierre de Fermat (17.srpna 1601 – 12. ledna 1665). Pocházel z francouzského šlechtického rodu, z městečka Beaumont de Lomagne. Vystudoval práva a také se jako právník živil. Matematikou se zabýval jen jako amatér pro vlastní potěšení. Přesto dosáhl vynikajících výsledků hned v několika oblastech. Podobně jako řada jeho současníků v 17. století, i Fermat nalézal inspiraci při studiu knih, které se dochovaly z antických dob. Velký obdiv budily zejména spisy tří starých řeckých matematiků – Archimeda, Apollonia a Diofanta. Při studiu Apolloniova díla o kuželosečkách Fermat vynalezl úplně nový, matematický obor - analytickou geometrii. Pro další rozvoj matematiky to byl velmi důležitý objev, neboť umožňoval vyjádřit geometrické útvary číselně a popsat křivky pomocí rovnic.

Fermat i Descartes vytvořili analytickou geometrii nezávisle a prakticky zároveň, ale Fermat své výsledky jen zřídka publikoval a tak mnohdy přišel o prvenství. Většina jeho matematických prací byla zveřejněna až posmrtně. Podobně tomu bylo i s jeho studiem křivek, při kterém se těsně přiblížil k vytvoření integrálního a diferenciálního počtu. Skutečnými zakladateli tohoto oboru se stali o něco později Newton a Leibnitz.

Další významný Fermatův přínos spočívá ve studiu pravděpodobnosti. Touto otázkou se zabýval už v mládí společně se svým přítelem, matematikem a filozofem Blaisem Pascalem. V r. 1653 Pascal narazil na tento problém znovu, když ho jeden známý požádal, aby odhadl šanci na vítězství při hře v kostky. V následujícím roce si Pascal s Fermatem vyměnili sérii dopisů, ve kterých se fakticky zrodila teorie pravděpodobnosti. Inspirovali tím řadu dalších matematiků a nový obor, u jehož počátků stojí hazardní hry, byl na světě.

Pierre de Fermat se nesmazatelně zapsal do historie matematiky především díky tzv. Velké Fermatově větě.

4.1.1. Analytická geometrie

Analytická geometrie (také souřadnicová geometrie nebo kartézská geometrie), je část geometrie, která zkoumá geometrické útvary v euklidovské geometrii pomocí algebraických a analytických metod.

V analytické geometrii jsou geometrické útvary v prostoru vyjadřovány čísly a rovnicemi ve zvolených souřadnicových soustavách.

Geometrie, používající algebraické metody v n-dimenzionálním prostoru, se nazývá algebraická geometrie a zabývá se obecnými vlastnostmi řešení těchto rovnic a jejich soustav.

4.1.2. Malá Fermatova věta

Malá Fermatova věta je matematická věta, která tvrdí, že pro každé prvočíslo p a každé celé číslo a takové, že p nedělí a, platí

$$a^{p-1} \equiv 1 \pmod{p}.$$

Věta je nazvána podle francouzského matematika a přívlastek *malá* ji odlišuje od Velké Fermatovy věty.

4.1.3. Velká Fermatova věta

Velká Fermatova věta je jedna z nejslavnějších vět v historii matematiky. Zní takto: Neexistují celá čísla x, y a z a přirozené číslo n, pro která $x^n + y^n = z^n$, kde $n>2$ a $x,y,z \neq 0$. Větu si v 17. století francouzský matematik Pierre de Fermat poznamenal na okraj knihy v této podobě:

Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exigitas non caperet.

(Je nemožné rozdělit krychli do dvou krychlí, či čtvrtou mocninu do dvou čtvrtých mocnin, nebo obecně jakoukoli mocninu, vyšší než druhou do dvou stejných mocnin. Objevil jsem opravdu tak podivuhodný důkaz, že tento okraj je příliš malý, aby se do něj vešel.)

Když zemřel, v jeho pozůstalosti nebyl zmíněný důkaz nikde nalezen. Od té doby jeho poznámka mučila nesčetné generace matematiků. Všechny ostatní Fermatovy hypotézy byly mezitím dokázány nebo vyvráceny, ale jeho velká věta vzdorovala všem pokusům. Stala se z ní jedna z největších matematických záhad a milovníky čísel přivedla k sebevraždám a soubojům. V r. 1908 slavná gottingenská univerzita v Německu vypsala odměnu 100 tisíc marek pro toho, kdo důkaz velké Fermatovy věty nalezne.
Víme, že Fermat našel důkaz pro n rovno čtyřem, ale nejspíše nikoli pro jiné exponenty.Během následujících staletí se podařilo dokázat některé další zvláštní případy věty, ovšem definitivní důkaz pokrývající Fermatovo tvrzení v celé jeho obecnosti získal britský matematik Andrew Wiles až roku 1994 a jedná se o jeden z nejsložitějších důkazů v historii matematiky.
Přestože sama Velká Fermatova věta nemá pro matematiku velký význam a fakt, na který poukazuje je zatím pouze matematickou zajímavostí a nemá dosud využití, důkaz, který Andrew Wiles vytvořil je neocenitelný pro celý matematický svět. Kvůli důkazu muselo být sjednoceno mnoho matematických myšlenek a teorií a ještě více muselo být

vytvořeno. A právě řada těchto postupů si uplatnění v moderní vědě našla a umožnila další výzkumy. Andrew Wiles dal také matematickému světu novou naději, když dokázal Tanijamovu-Šimurovu domněnku, která by spojovala Eliptické křivky a Modulární formy. Dvě odvětví matematiky s naprosto různými principy a přístupy k problémům, ale také při bližším pohledu s mnohými spojitostmi a společnými vlastnostmi. Tím, že Wiles dokázal, že Modulární formy a Eliptické křivky jsou totéž, a tedy dokázal i Tanijamovu-Šimurovu domněnku, dal matematikům šanci na splnění Langlandsova programu – tedy vytvoření velké sjednocené matematiky.

4.3.4. Fermatovo číslo

P. Fermat se domníval, že všechna čísla tvaru $2^n + 1$, kde $n = 2^m$, $m = 0,1,2,\dots$, jsou prvočísla. Toto platí však pouze pro prvních pět čísel ($F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$). V 18. století ale Leonhard Euler dokázal, že F5 je dělitelné 641, čímž jeho domněnku vyvrátil.

Přes snahy mnohých matematiků dodnes nevíme, kolik existuje Fermatových čísel složených a kolik prvočíselných. Zatím nejznámější Fermatovo prvočíslo je právě F_4. Pro čísla F_5 až F_{23} bylo dokázáno, že jde o čísla složená i když ne u všech známe úplný rozklad. Úplný rozklad známe pro čísla F_5, F_6, F_7, F_8, F_9, F_{10} a F_{11} .

4.2. Carl Friedrich Gauss

"Král matematiků"

Žil v letech (30.března 1777 - 23.února 1855). Carl (též Karl) Friedrich Gauss**,** německý matematik, astronom a fyzik, myslitel, který podal jako první důkaz tzv. základní věty algebry, přichází na svět 30. dubna roku 1777 v německém městě Braunschwein (Brunšvik) v dělnické rodině.

Kolovala spousta historek o jeho brzké genialitě a o všech se dá pochybovat. Podle jedné z nich se jeho nadání projevilo už ve věku tří let, kdy opravil chybu svého otce při počtech. Nejslavnější historka z jeho dětství hovoří o tom, že jako devítiletý školák (v roce 1786) dokázal během několika vteřin spočítat součet všech čísel od jedné do sta (5050). Gauss si uvědomil, že sečtením opačných prvků z řady čísel dostane vždy stejný výsledek: 1 + 100 = 101, 2 + 99 = 101, 3 + 98 = 101, atd., což dohromady dává 50 × 101 = 5050

V sedmnácti letech ho zaujal prastarý a dosud nezodpovězený problém, zda lze jen s pomocí pravítka a kružítka sestrojit pravidelný sedmiúhelník. Výsledek na sebe nenechal dlouho čekat. Gauss zjistil, že zkonstruovat sedmiúhelník je nemožné, a ukázal, že tímto způsobem lze sestrojit pouze ty pravidelné mnohoúhelníky s lichým počtem stran, jejichž počet stran je násobkem prvočísel 3, 5, 17, 257 nebo 65 537. Gauss byl tímto výsledkem tak nadšen, že požádal, aby pravidelný 17-úhelník byl vytesán na jeho náhrobek.

V roce 1791 Carl Friedrich Gauss získává od brunšvického vévody studijní stipendium (studuje na brunšvickém Collegium Carolinum) a v letech 1795-98 studuje s vévodovou podporou univerzitu v Göttingenu - ve své disertační práci, jíž svá studia zakončuje (v roce 1799 na univerzitě v Helmstedtu). Poté Gauss podává jako první matematik důkaz o tom, že každá algebraická rovnice má alespoň jedno možné řešení (tzv. základní věta algebry).

Během univerzitních studií Gauss „znovuobjevil“ několik vět (Bodeův zákon, Binomická věta, aritmetický a geometrický průměr, zákon kvadratické reciprocity a větu o prvočíslech).

Rok 1796 byl velice produktivní, jak pro Gausse, tak pro teorii čísel. Konstrukci 17-úhelníku objevil 30. března. Poté objevil aritmetiku zbytkových tříd a zjednodušil tak výpočty v teorii čísel. Stal se prvním, kdo dokázal platnost kvadratické reciprocity, to bylo 8. dubna. Toto pravidlo říká, že každá kvadratická rovnice má řešení v oboru zbytkových tříd. Větu o prvočíslech odhadl 31. května a říká, jak jsou prvočísla rozložena mezi celými čísly. Gauss také objevil, že každé kladné celé číslo jde vyjádřit jako součet nejvíce tří trojúhelníkových čísel.

Po studiích Gauss zůstává ve službách brunšvického vévody (má přitom i nabídky z Ruska, kde se má stát ředitelem tamní hvězdárny), po vévodově smrti pak Gauss působí jako profesor astronomie a ředitel hvězdárny v Göttingenu (v roce 1807).

Gaussovo vědecké dílo je velice obsáhlé - v matematice se, kromě již zmíněné základní věty algebry, nejvíce proslavil svými výzkumy v oblasti statistiky a počtem pravděpodobnosti (tzv. Gaussova křivka jako základní rozložení pravděpodobnosti), též se zabývá matematickou analýzou či funkcemi komplexní proměnné, významně se Gauss zabývá i teorií čísel - jeho nejznámějším dílem z oblasti matematiky je pak spis *"Disquisitones aritmeticae" (Pojednání o aritmetice, 1801).*

Jeho práce z klasické geometrie znamenaly první významný pokrok v geometrii od dob antických Řeků. Z našeho dnešního hlediska je však nejdůležitější skutečnost, že Gauss na konci 18. století objevil zcela nový typ geometrie, která se od té klasické, euklidovské zásadně liší. Euklidova geometrie je založena na pěti základních poučkách, tzv. axiomech. Po dva tisíce let nikdo z matematiků nedokázal na Euklidově systému axiomů nic opravit ani vylepšit. Avšak Gauss ke svému největšímu překvapení zjistil, že změnou pátého axiomu vznikne úplně nový systém - geometrie zakřiveného prostoru! Tento objev byl tak odvážný, že se mladý Gauss polekal a raději ho ani nezveřejnil. Později rozvinul neeuklidovskou geometrii Gaussův žák Bernhard Riemann a ve 20. století jedině díky tomu mohl Einstein vytvořit obecnou teorii relativity.

Jako astronom je Gauss slavný svými teoretickými výpočty drah asteroidů, a to především svým výpočtem (a předpovědí) dráhy planetky Ceres, objevené roku 1801 - tato planetka je poté, co se při přechodu slunce tehdejším astronomům ztratí, objevena znovu v roce 1802 jen na základě Gaussem vypočítaných souřadnic (Gauss k výpočtu využil svoji vlastní aproximační metodu nejmenších čtverců, která se dnes používá ve všech odvětvích vědy k minimalizaci chyby měření). Gaussovy astronomické objevy a výzkumy jsou shrnuty v jeho spise *"Theoria motus corporum coelestium in sectionibus conicis Solem ambientium"* (1809).

Vypracoval algebru a aritmetiku komplexních čísel a novou teorii prvočísel, v níž 3 je prvočíslo, ne však 5 neboť 5 = (1+2i).(1-2i), komplexní čísla vyjádřil jako body v rovině. Věnoval se mechanice, elektromagnetismu, astronomii a geodézii a jako jeden z prvních také zemskému magnetismu. Zavedl absolutní soustavu jednotek CGS ve fyzice. Je po něm nazvána mj. Gaussova rovina. Jeho jméno nosí nepřeberná řada matematických a fyzikálních zákonů a věd.

Roku 1799 v disertační práci, *„Nový důkaz toho, že každá racionální funkce s jednou proměnou jde rozložit na reálné faktory prvního nebo druhého stupně“*, podal Gauss důkaz základní věty algebry. Tato důležitá věta říká, že každý polynom nad komplexními čísly musí mít alespoň jeden kořen. Jiní matematici se také pokoušeli o důkaz, např. Jean le Rond d'Alembert. Gaussova disertační práce kritizovala d'Alembertův důkaz, ale jeho vlastní důkaz nebyl přijat, protože používal dosud nedokázanou Jordanovu větu. Gauss během svého života přišel ještě s třemi dalšími důkazy základní věty algebry, pravděpodobně díky odmítnutí jeho disertační práce. Poslední důkaz z roku 1849 je považován za matematicky rigorózní i z pohledu dnešních matematických standardů. Jeho důkazy značně objasnily chápání komplexních čísel.

Gauss také udělal obrovský pokrok v teorii čísel díky knize Disquisitiones Arithmeticae (1801), která obsahovala předvedení aritmetiky zbytkových tříd a také první důkaz zákona o kvadratické reciprocitě.

Ačkoliv byl Gauss do té doby zajišťován financemi vévody, pochyboval o tomto ujednání a také pochyboval o tom, že by pouhá matematika byla natolik důležitá, aby si to zasloužila. Proto usiloval o pozici v astronomii. To se mu povedlo a roku 1807 se stal profesorem astronomie a ředitelem hvězdárny v Gottingenu. Na tomto místě působil po zbytek jeho života.

4.2.1. Metoda nejmenších čtverců

Je matematická metoda, určená ke statistickému zpracování dat. Umožňuje nalézt vhodnou aproximační funkci pro dané empiricky zjištěné hodnoty. Hledaná funkce musí být lineární kombinací předem známých funkcí, metoda umožní vypočítat jejich koeficienty.

Metoda nejmenších čtverců slouží k nalezení takového řešení, aby součet druhých mocnin chyb nalezeného řešení byl minimální. (Zjednodušeně, „aby součet čtverců odchylek byl nejmenší“.)

Často je pro aproximaci užívána lineární funkce.

Pro první přiblížení uvažujme závislost jisté proměnné y na proměnné x, danou nějakým předpisem $y = f(x)$. Pokud námi uvažovaná závislost má očekávaný tvar, např. $f(x) = ax + b$ (lineární závislost), mohlo by se zdát, že postačí pouze vybrat dvě dvojice $[x,y]$ naměřených hodnot a řešením soustavy dvou rovnic (dosazením dané dvojice hodnot) získat jednoduše koeficienty a, b, které hledáme. Není tomu tak, a to z důvodu chyby měření. V kostce řečeno:

Metoda nejmenších čtverců hledá takové hodnoty koeficientů, aby součet čtverců „odchylek“ jejích funkčních hodnot od daných naměřených hodnot byl nejmenší možný.

4.2.2. Gaussova eliminační metoda (Gaussova eliminace)

Je metodou exaktního řešení soustavy lineárních algebraických rovnic.

Gaussovu eliminaci lze také použít pro výpočet inverzní matice nebo pro výpočet determinantu matice.

Obecně řečeno, Gaussova eliminace představuje řešení problému vyjádřeného pomocí matice převedením dané matice na horní trojúhelníkovou nebo na diagonální matici.

Příklad

Máme soustavu rovnic:

$$\begin{array}{rrrcr} 8x & -y & -2z & = & 0 \\ -x & +7y & -z & = & 10 \\ -2x & -y & +9z & = & 23 \end{array}$$

a hledáme čísla *x*, *y*, *z*, která jsou řešením dané soustavy.

Cílem je eliminovat jednotlivé neznámé z jednotlivých rovnic soustavy: z první rovnice eliminujeme *x* (pomocí úprav druhé a třetí rovnice), z druhé *y*, z třetí *z*.

Jsou povoleny následující operace, které nezmění hodnost soustavy:

násobení či dělení jednotlivých řádků nenulovým číslem

prohazování libovolných řádků soustavy

přičítání násobků jednotlivých řádků k jinému řádku

Postup pro výše uvedený příklad:

První krok – eliminace *x* z druhého a třetího řádku.

první řádek neupravujeme

druhý řádek násobíme 8 a přičteme první řádek

třetí řádek násobíme 4 a přičteme první řádek

$$\begin{array}{rrrcr} 8x & -y & -2z & = & 0 \\ & 55y & -10z & = & 80 \\ & -5y & +34z & = & 92 \end{array}$$

Druhý krok – eliminace *y* ze třetího řádku

první řádek neupravujeme

druhý řádek neupravujeme

třetí řádek násobíme 11 a přičteme druhý řádek

vydělíme třetí řádek 364 a získáme řešení $z = 3$

$$\begin{array}{rrrcr} 8x & -y & -2z & = & 0 \\ & 55y & -10z & = & 80 \\ & & z & = & 3 \end{array}$$

Třetí krok – zpětné dosazení

v druhém řádku dosadíme za *z* a vyřešíme *y*

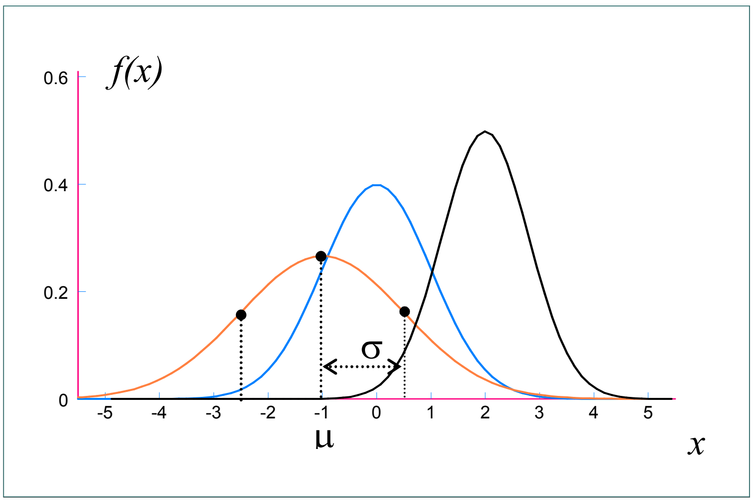
v prvním řádku dosadíme za *z* a *y* a dořešíme *x*

$x = 1,\ y = 2,\ z = 3$

4.2.3. Gaussova křivka

Rovinná křivka zvonovitého tvaru, která znázorňuje normální rozložení pravděpodobností. Vyjadřuje též rozložení náhodných chyb.

Na obrázku jsou znázorněny tři vzájemně odlišné Gaussovy křivky:



4.2.3. Gaussova rovina

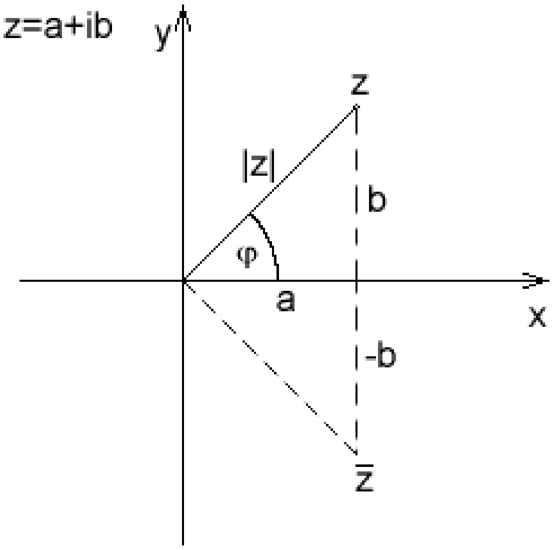
Komplexní rovina (někdy též Gaussova rovina) je v matematice způsob zobrazení komplexních čísel v rovině *xy*.

Na osu *x* se vynáší reálná část komplexního čísla *z*, tzn. $x = \Re(z)$, a proto je tato osa označována jako reálná.

Na osu *y* se vynáší imaginární část komplexního čísla *z*, tzn. $x = \Im(z)$, a proto je tato osa označována jako imaginární.

Komplexní rovinu, do níž zahrnujeme i bod $z = \infty$, označujeme jako *rozšířenou rovinu (komplexních čísel)*.

Na obrázku je zobrazen vztah mezi komplexním číslem a číslem komplexně sdruženým v komplexní rovině.



4.3. Niels Henrik Abel

(5. srpna 1802 – 6. dubna 1829). Život Nielse Abela byl poznamenán chudobou, která byla jedním z důsledků politických problémů Norska. Niels Abel vyrůstal v Gjerstadu v jihovýchodní části Norska. Abelův otec, Soren Georg Abel měl vysokoškolské vzdělání z teologie a filozofie a Abelův dědeček byl protestantským knězem v Gjerstadu nedaleko Risoru. Soren Abel byl norským nacionalistou a aktivně politicky působil v hnutí za norskou nezávislost. Jeho manželkou byla Ane Marie Simonsonová, dcera loďaře. Niels Abel byl druhým ze sedmi dětí. Jeho dědeček zemřel, když mu byl rok. Jeho otec převzal místo po svém otci v Gjerstadu. Gjerstad byl městem, kde Abel vyrůstal. Když bylo Abelovi 13 let, jeho otec kvůli ekonomické krizi nebyl schopen rodinu zaopatřit. Uvádí se, že si také rád užíval alkoholu.

Když ale v roce 1817 přišel do klášterní školy nový učitel matematiky Bernt Holmboe, Abelův přístup se od základů změnil. Předchozí učitel matematiky byl z místa odvolán kvůli hrubosti a násilí vůči žákům, které bylo příčinou úmrtí jednoho žáka. Nový učitel povzbudil žáky natolik, že Niels Abel začal studovat matematické texty na univerzitní úrovni a po roce studování práce Eulera, Newtona, Lalandeho a d'Alemberta. Holmboe rozpoznal, že Niels Abel má výrazný talent a všemožně mu pomáhal ve studiu prací Lagrange a Laplace. V roce 1820 ale Abela postihla rodinná tragédie, když jeho otec zemřel.

Rodina se ocitla po jeho smrti ve velkých problémech. Nedostávalo se peněz k tomu, aby Niels Abel dokončil školní vzdělání a nebyly peníze ke studiu na univerzitě. Abel nyní musel sám vypomáhat matce a rodině.
Abel tehdy dostal malý grant na návštěvu Degena a dalších matematiků v Kodani. Zde se setkal s Christianem Kempem. Po návratu se Abel pokusil od Univerzity v Christianii získal větší grant na návštěvu špičkových matematiků v Německu a ve Francii. V té době neuměl ani německy, ani francouzsky, ale během dvou let, kdy Abel šetřil peníze a získal grant, uměl oběma jazyky hovořit plynně. Abel začal v roce 1824 opět pracovat na rovnicích pátého stupně a dokázal, že neexistuje obecné řešení rovnice pátého stupně rozkladem na reálné kořeny. Svůj článek publikoval ve Francii na své vlastní náklady. Aby ušetřil na nákladech, zkrátil důkaz tak, aby se vešel na šest stránek.
Zhruba v této době se Abel seznámil s Ruffiniho prací, když studoval v roce 1815 Cauchyho práci, ve které byl na Ruffiniho práci odkaz. V roce 1824 Abel ve svém článku napsal, že geometři se často zabývali hledáním obecného řešení algebraických rovnic. Podle Abela ale nemohli uspět.
Abel zaslal svoji práci několika matematikům včetně Gausse, kterého chtěl navštívit v Göttingenu. V srpnu 1825 Niels Abel získal stipendium od norské vlády, aby mohl cestovat do zahraničí. Po měsíci, když uspořádal své záležitosti, navštívil nejprve matematiky v Norsku a v Dánsku. V Kodani zjistil, že Degen zemřel. Dostal zde dopis od Crelleho, který ho pozval do Berlína. Abel a Crelle se stali přáteli. Crelle začal vydávat časopis věnovaný matematickému výzkumu. Abel na radu Crelleho začal psát jasnější verzi práce o neřešitelnosti rovnic pátého stupně a výsledkem byla práce *"Recherches sur les fonctions elliptiques"*, kterou Abel publikoval v roce 1827 v Crelleho časopisu společně s dalšími šesti články.
Abelovu práci posuzovali Cauchy a Legendre. Abel zůstal v Paříži několik měsíců, vyhladovělý, sklíčený, unavený a velmi ztrápený. Mohl si dovolit jen jedno jídlo denně.
V Berlíně si Abel nějaké peníze vypůjčil a pokračoval ve své práci na eliptických funkcích. Napsal práci, která zásadně změnila teorii eliptických integrálů na teorii eliptických funkcí použitím jejich inverzních funkcí.
Bohužel zdraví Abelovi příliš nesloužilo.
O vánocích roku 1828 Abel navštívil svoji snoubenku ve Frolandu. Ale na cestě vážně onemocněl, během vánoc se trochu vzpamatoval, ale brzy znovu vážně onemocněl.

Crelle podporoval v Berlíně Abelovu práci a 8. dubna 1829 mu napsal, že pro něj získal místo. Ale Abel byl již po smrti.
Teprve po Abelově smrti Cauchy v roce 1830 nalezl jeho práci. Byla publikována teprve v roce 1841. Po Abelově smrti se také našly jeho nepublikované práce o řešení algebraických rovnic. V Abelově dopise z 18. října 1828 byl nalezen důkaz věty, kterou teprve v roce 1830 publikoval Galois. V roce 1830 Pařížská akademie ocenila Abela a Jacobiho Velkou cenou za jejich výjimečnou práci.
Objevil metodu zrychlení konvergence nekonečných řad, rozvinul teorii integrálního počtu, dokázal binomickou větu.

4.3.1. Abelova grupa

V matematice značí Abelova grupa (někdy též abelovská grupa či komutativní grupa) grupu $(G, \square)$, ve které platí $a \square b = b \square a$ pro všechna a a b z G.

Vlastnosti

Klasifikace konečných Abelových grup představovala velký úkol algebry 19. a začátku 20. století. Jejím výsledkem je základní tvrzení, které stanovuje, že každá konečná Abelova grupa je direktním součtem cyklických grup o řádech rovných mocninám prvočísel. To je jen speciální případ obecnějšího tvrzení, podle nějž každá konečně generovaná Abelova grupa je direktním součtem konečných cyklických grup o řádech rovných mocninám prvočísel, a nekonečných cyklických grup.
Součinu konečných grup z výše zmíněné věty se rovněž říká *torzní část* Abelovy grupy, součinu nekonečných cyklických grup z výše zmíněné věty se říká *beztorzní část* Abelovy grupy.

4.3.2. Algebraické řešení

Algebraické řešení rovnice vyžaduje najít postup za užití konečného počtu 5-ti operací (+,−,·,/,√), resp. 4 základních operací (+,−,·,/) a řešení binomických rovnic tvaru $x^k=a$. Algebraické řešení algebraických rovnic (jak dokázali N.H.Abel a E.Galois) pro rovnice 5-tého stupně (např. $x^5 - 10x + 2 = 0$) a vyšších stupňů neexistuje.

4.3.3. Rovnost polynomů

Uvažujme dva polynomy P(x) a R(x). Polynomy se *algebraicky* rovnají, když se rovnají všechny jejich koeficienty. Když se rovnají jejich hodnoty, říkáme, že se polynomy rovnají *funkčně*. V oborech s konečným počtem prvků může nastat případ, kdy dva polynomy s různými koeficienty dávají (pro všechna možná x) stejné hodnoty: V oboru Z3 (x=0,1,2) se *algebraicky* různé polynomy $P(x)=x^4-1$ a $Q(x)=x^4+x^3-x-1$ *funkčně* rovnají, protože dávají pro všechna x stejné hodnoty.

4.3.4. Abelova sumace

V matematice je Abelova sumace definovaná přepisem n-tého členu posloupnosti na rozdíl dvou po sobě jdoucích členech součtové řady dané touto posloupností.

Mějme dvě posloupnosti (a_n) a (b_n), kde n=1,2,3,... a definujme $A_n = \sum_{k=1}^{n} a_k$.

Tedy $a_k = A_k - A_{k-1}$.

Potom

$$\sum_{k=1}^{n} a_k b_k = \sum_{k=1}^{n} (A_k - A_{k-1}) b_k =$$

$$= \sum_{k=1}^{n} A_k b_k - \sum_{k=1}^{n} A_{k-1} b_k = \sum_{k=1}^{n} A_k b_k - \sum_{k=0}^{n-1} A_k b_{k+1}$$

A protože $A_0 = 0$, tak můžeme druhou sumu indexovat od jedničky.

$$\sum_{k=1}^{n} A_k b_k - \sum_{k=1}^{n-1} A_k b_{k+1} = \sum_{k=1}^{n} A_k (b_k - b_{k+1}) - A_n b_n$$

Což je výsledek.

Použití

Abelova sumace se používá zejména v matematických důkazech, když potřebujeme upravit součin dvou posloupností. Využíváme jí např. při důkazech kriterií konvergence součtové řady - Dirichletovo a Abelovo kriterium.

4.3.5. Abelovo kritérium

Nechť (a_n) je reálná posloupnost a (b_n) komplexní posloupnost pro které platí:

(a_n) je monotonní a konvergentní;

$\sum b_n$ je konvergentní řada.

Pak řada $\sum a_n b_n$ konverguje.

4.4. William Rowan Hamilton

Sir William Rowan Hamilton žil v letech (4. srpna 1805 – 2. září 1865)

Williamův otec, Archibald Hamilton, neměl čas učit svého syna, protože byl často na obchodních cestách. Archibald Hamilton neměl žádné univerzitní vzdělání a William zřejmě zdědil své schopnosti po své matce Sarah Huttonové. Když bylo Hamiltonovi pět let, uměl latinsky, řecky a hebrejsky. Těmto jazykům ho naučil jeho strýc James Hamilton, u něhož William bydlel po několik let. James Hamilton napsal několik článků o astronomii a byl ředitelem observatoře v Armagh.

William se brzy naučil několik dalších jazyků, ale jeho další zájem v jeho 12 letech ovlivnila návštěva Američana Zeraha Colburna, který dokázal Hamiltona zaujmout různými matematickými problémy a Hamilton s ním soutěžil ve svých matematických schopnostech.

Ve svých 13 letech začal Hamilton studovat Clairautovu knihu "Algebra", která byla ve francouzštině. Když mu bylo 15 let, začal studovat práce Newtona a Laplace. V roce 1822 objevil chybu v Laplaceově práci "Méchanique céleste", čímž vzbudil pozornost irského astronoma Johna Brinkleyho.

Ve věku 18 let Hamilton začal studovat na Trinity College v Dublinu a svoji genialitu projevil získáním vyznamenání. Přitom většinu času strávil se svým bratrancem Arthurem a nenavštěvoval všechny přednášky.

V roce 1826 Hamilton publikoval svoji práci *"Theory of Systems of Rays"* (Teorie systémů paprsků). V této práci Hamilton zavedl charakteristickou funkci pro optiku.

Hamilton 4. listopadu 1833 přečetl v Královské irské akademii svoji práci, ve které vyjádřil komplexní čísla jako algebraické uspořádané dvojice reálných čísel. Algebru pak Hamilton použil ve své práci *"On a General Method in Dynamics"* (O obecných metodách v dynamice) v roce 1834. V této práci Hamilton charakteristickou funkci použil v dynamice a následující rok napsal na toto téma další článek.

Roku 1835 Hamilton publikoval práci *"Algebra as the Science of Pure Time"* (Algebra jako věda čistého času), která byla inspirována jeho studiem Immanuela Kanta a byla zveřejněna na zasedání Britské asociace pro pokroky vědy *(the British Association for the Advancement of Science)*. Hamilton ve svém článku považoval algebraické dvojice za kroky v čase.

V roce 1835 byl Hamilton povýšen do rytířského stavu. Téhož roku se mu narodil jeho druhý syn Archibald Henry. Po objevení algebraických dvojic se Hamilton pokusil svoji teorii rozšířit na trojice a byl touto myšlenkou řadu let posedlý. Následujícího podzimu Hamilton odjel do Bristolu na zasedání Britské asociace.

Dne 16. října 1843 se Hamilton procházel se svou manželkou podél Královského kanálu, aby se připravil na zasedání Královské irské akademie. Ačkoliv s ním jeho žena rozmlouvala, byl hluboce ponořen do úvah. Uvádí se, že právě tehdy přišel na myšlenku kvaternionů, první známé nekomutativní algebry. Uvědomil si, že pro počítání s trojicemi potřebuje ještě čtvrtý rozměr. Aby svoji myšlenku nezapomněl, vyškrábal vztahy pro kvaterniony

$$i^2 = j^2 = k^2 = i.j.k = -1$$

na jeden z kamenů mostu Brougham. Hamilton se domníval, že jeho objev bude znamenat revoluci v matematické fyzice a zbytek života strávil studiem kvaternionů.

Kromě zmíněné práce o kvaternionech začal Hamilton psát další knihu o tomto tématu pod názvem *"Elements of Quaternions"* (Elementy kvaternionů), jejíž délka se odhaduje na asi 400 stránek a autor ji psal asi dva roky. Její název napovídá, že Hamilton byl do jisté míry inspirován Euklidovými "Elementy". Poslední kapitola knihy zůstala nedokončena, protože Hamilton mezitím zemřel a byla později publikována s úvodem jeho syna Williama Edwina Hamiltona.

Hamilton zemřel po několika záchvatech krátce poté, co obdržel zprávu, že byl jmenován prvním zahraničním členem Národní akademie věd Spojených států amerických.

4.4.1. Kvaterniony

V matematice se pojmem kvaternion označuje nekomutativní rozšíření komplexních čísel. Nejdříve byly považovány za nevhodný a uměle vykonstruovaný objekt, jelikož porušovaly komutativní zákon $ab = ba$, postupně ale našly uplatnění jak v teoretické fyzice, tak v aplikované matematice (přestože mnohdy se jejich použití lze za jistou cenu vyhnout s pomocí vektorů). Ve skutečnosti je však mezi kvaterniony a 4-rozměrnými vektory principiální rozdíl: Operace dělení je mezi dvěma kvaterniony definována, zatímco mezi dvěma vektory tato operace vůbec neexistuje.
Pomocí kvaternionů lze nalézt některá platónská tělesa ve čtyřrozměrném prostoru.
Zatímco komplexní čísla jsou vytvořena z reálných přidáním prvku i splňujícího $i^2 = -1$, kvaterniony jsou vytvořeny přidáním prvků i, j a k tak, že jsou splněny následující vztahy.

$$i^2 = j^2 = k^2 = ijk = -1$$

$$\begin{array}{lllllll} ij & = & k, & \quad & ji & = & -k, \\ jk & = & i, & & kj & = & -i, \\ ki & = & j, & & ik & = & -j. \end{array}$$

Každý kvaternion je lineární kombinací prvků 1, i, j a k, což znamená, že jej lze psát jako $a + bi + cj + dk$ kde a, b, c a d jsou reálná čísla.

Příklad :

Nechť

$$\begin{aligned} x &= 3+i \\ y &= 5i+j-2k \end{aligned}$$

Pak (při násobení se využívají vztahy uvedené výše)

$$x+y = 3+6i+j-2k$$

$$\begin{aligned} xy &= (3+i)(5i+j-2k) = 15i+3j-6k+5i^2+ij-2ik \\ &= 15i+3j-6k-5+k+2j = -5+15i+5j-5k \end{aligned}$$

Základní vlastnosti

Množina kvaternionů se v matematice typicky značí písmenem $\mathbb{H}$.
Kvaterniony jsou asociativní podílová algebra nad tělesem reálných čísel. Je na nich definováno (pravé a levé) dělení a jako množina spolu se sčítáním, násobením a dělením tvoří těleso. Je nekomutativní, jeho centrum je $\mathbb{R}$. Je to největší nadtěleso reálných čísel.
Pro kvaternion $h = a + bi + cj + dk$ definujeme jeho konjugaci jako $\bar{h} \equiv a - bi - cj - dk$. Platí, že součin $h\bar{h} = \bar{h}h = a^2 + b^2 + c^2 + d^2$ je nezáporné reálné číslo a je rovno nule pouze pro nulový kvaternion $h = 0$.
Inverzní prvek ke kvaternionu h je kvaternion $h^{-1} = \bar{h}/(h\bar{h})$(dělení reálným číslem $h\bar{h}$ je definováno po složkách).

Norma kvaternionu h se definuje jako $|h| \equiv \sqrt{h\bar{h}}$. Násobení zachovává normu, t.j. pro kvaterniony h,q platí $|hq| = |h||q|$.

4.4.2. Platónská tělesa ve čtyřrozměrném prostoru

Pomocí kvaternionů lze nalézt některá platónská tělesa ve čtyřrozměrném prostoru. Prvním faktem, který je potřeba si uvědomit je, že žádné platónská těleso se nezmění, pokud jej pootočíme tak, že každý vrchol přejde do vrcholu jiného. Potom je potřeba si všimnout, že pokud máme čtyřrozměrný vektor (a,b,c,d) a přiřadíme mu kvaternion $a + bi + cj + dk$, potom pokud sadu takových vektorů (kvaternionů) vynásobíme *jednotkovým kvaternionem*, tak se všechny tyto vektory pouze otočí. (Jsou násobené jednotkovým kvaternionem, takže se nezmění jejich velikost, jen směry, a to lineárně.) Pak si všimneme, že v kvaternionech existují uzavřené konečné grupy vůči násobení, které mají následující členy:

všechny permutace $(\pm 1, 0, 0, 0)$ (8 členů)
předchozí grupa + 16 čtveřic $(\pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2})$
předchozí grupa + všechny sudé permutace $\frac{1}{2}(\pm 1, \pm\varphi, \pm 1/\varphi, 0)$.

Pro každou z těchto grup tedy platí, že násobíme-li členy grupy mezi sebou, výsledkem je opět prvek dané grupy. To ovšem znamená, že každá grupa, představuje vrcholy nějakého platónského tělesa ve čtyřrozměrném prostoru! (Protože právě tehdy, když jde o platónské těleso je splněna vlastnost, že při otočení daného tělesa tak, aby se vrchol dostal do vrcholu (čemuž právě násobení jednotkovými kvaterniony z dané grupy odpovídá) zůstane těleso stejné.)

4.5. Evariste Galois

Evariste Galois žil (25. října 1811 - 31. května 1832) ve městě Bourg-la-Reine (deset kilometrů od Paříže). Jeho otec Nicolas Gabriel Galois byl starostou města. Do dvanácti let se Evariste vzdělával v rodině, a potom přešel na lyceum Ludvíka Velikého.

Budoucího velkého vědce nejprve matematika nezajímala.. V této době byli programy francouzských škol sestaveny takovým způsobem, aby daly studentům humanitní vzdělání. Matematika byla na jednom z posledních míst. Je třeba říct, že kdo chtěl, mohl se seznámit s touto vědou ve speciálních kurzech. Ale Galois se o takové kurzy nezajímal. Literatura a rétorika byly tím, co ho zajímalo. Zdálo se mu, že je jejich velký znalec. Došlo ve spor s učiteli a v důsledku toho k propadnutí ve druhém roce a Evariste začíná navštěvovat doplňkové vyučování matematiky. Brzy se před ním otevírá nový dosud neznámý svět.

Galoisovi se dostaly do rukou „Základy geometrie“ od Legendrea. Krátce po té se začíná zabývat pracemi Lagrangea o matematické analýze. Diferenciální počet, integrální, teorie analytických funkcí. S překvapivou lehkostí zvládá obtížné partie matematiky. Rétorika je zapomenuta, uskutečňuje se přerod: teď ho ovládá skutečný zájem o matematiku, který mu dovoluje zůstat nesmazatelným ve vědě.

Četl Eulera, Gausse, Jacobiho. Pevně se rozhodl, že se určitě přihlásí na Polytechnickou školu- centrum matematické Francie té doby. A tak bez přípravy, jen s naivní vírou ve svou výjimečnost, Evariste předstoupil před examinátora a propadl. Evariste zde dostal lekci a vrací se domu, do speciální matematické třídy. Jeho první učitel Richard brzy poznal že ten kdo by se měl učit od druhého je on sám. Žák Galois brzy předčil svého učitele. Richard mu pomohl publikovat první práci „Důkaz jedné věty o periodických spojitých zlomcích“. Evariste o ní nikomu neřekl a nikdo se o ni nezajímal. V každém případě to nebyla ta práce, v níž Galois formuloval své výsledky o řešitelnosti algebraických rovnic. Tyto výsledky poslal Akademii věd ve formě rukopisu, který obsahoval nejgeniálnější matematické ideje století. Doufal, že sekretář Akademie pošle rukopis Cauchymu. Ten však hodil rukopis do koše. Přece se nebude zabývat tím, co napsal student lycea. Znovu šel na Polytechnickou školu, ale neuspěl.

Pohřeb otce určil osud Evarista Galoise. Někteří zahraniční historikové se domnívají, že zvláště hořkost neúspěchů, přání pomstít se za svou neúspěšnou kariéru, z něj učinily revolucionáře.

Zdálo by se, že za jeden rok bylo dost hořkosti. Ale tento rok 1829 Evarista nešetřil . Jeho práce o spojitých zlomcích, poslaná do Akademie věd, tam byla ztracena. Ale ani tato rána nezlomila Evarista. Vstupuje na Normální školu (Ecole Normal). Zde provádí nové výzkumy, které představuje v konkurzu do Akademie věd. Teď je jeho osud v rukou stálého sekretáře Akademie Fouriera. Fourier začíná číst rukopis, ale brzy umírá. Druhý rukopis, tak jako první, mizí.

Galois napsal jedovatý dopis, kde se neomezil jen na kritiku systému vzdělávání ve škole. Informuje o politické bezprincipiálnosti jejího ředitele, popisuje výsměch, kterému jsou vystaveny vzdorovití. Za čtyři dny po zveřejnění dopisu byl Evariste Galois vyloučen ze školy. Zakázali mu nejen návštěvy přednášek, ale také ho zbavili prostředků k životu.

Věrný sám sobě, Evariste se nepoddává hořkému rozumování o svých neúspěších. Jedná. Dne 9. ledna 1831 se ve stejném listu objevuje upozornění: Bývalý student Normální školy Evariste Galois bude číst přednášky kurzu algebry. Přednášky se budou uskutečňovat každý čtvrtek ve čtvrt na dvě. Jsou určeny mladým lidem, kteří vědí, jak neúplně se studuje algebra v kolejích, mají zájem si prohloubit své znalosti v této vědě. Kurz se sestává z nových teorií, které dosud nebyly publikovány. Novou teorii je možno nazvat teorii imaginárních veličin; teorii rovnic, řešitelných v radikálech; teorii čísel a eliptických funkcí, řešitelných čistou algebrou. Vyučování začíná ve čtvrtek 13. ledna v knihovně, ulice Sorbonny 5.

To byla ohromná drzost: vyloučený student se postavil proti svým učitelům, 19ti letý matematik hodil rukavici oficiální vědě. Jak potvrzují svědectví, na první přednášku přišlo čtyřicet posluchačů, na druhé jich nebylo více než deset a na třetí (poslední) čtyři posluchači. Galois přednášel příliš složitě.
Formuloval Galoisovu teorii, jeden ze základních kamenů moderní algebry. Zemřel ve věku 20 let na následky střelného poranění ze souboje.

4.5.1. Galoisova teorie

- Idea řešitelnosti algebraických rovnic
- položeny základy teorie grup a teorie těles
- zaveden v těchto oblastech řád základních pojmů

Galoisova teorie je jeden ze základních kamenů moderní algebry. Pomocí této teorie prokázal neřešitelnost obecné polynomiální rovnice stupně většího než 4 v radikálech (tj. nemožnost zapsat obecný vzorec pro řešení jen s užitím základních aritmetických operací a odmocnin)

Galoisova teorie byla původně motivována otázkou, která je známa jako Abel-Ruffini teorém.

4.6. Charles Hermite

Charles Hermite (24. prosince 1822 – 14. ledna 1901) byl francouzský matematik. Charles Hermite se narodil jako šesté ze sedmi dětí Ferdinanda Hermita a jeho ženy Madeleine, rozené Lallemandové. Mladý Charles studoval nejprve na *Collège de Nancy* a po té v Paříži na *Collège Henri* a *Collège Louis-le-Grand*, tedy na téže škole, jako patnáct let před ním Évariste Galois. Podobně jako Galois se zajímal o řešitelnost polynomiálních rovnic v radikálech a protože nebyl obeznámen s Galoisovými výsledky v této oblasti, pokusil se dokázat neřešitelnost obecné rovnice pátého stupně. Po dokončení studia na *Collège Louis-le-Grand* a roční přípravě úspěšně složil přijímací zkoušky na *École Polytechnique* i když se mezi všemi adepty umístil až na osmašedesátém místě.

Po ročním studiu na této škole nebylo Hermitovy umožněno nastoupit do druhého ročníku kvůli postižení jeho pravé nohy, které mu velmi znesnadňovalo pohyb. I když uspěl s následným odvoláním, rozhodl se nakonce z *École Polytechnique* dobrovolně odejít. V této době (okolo roku 1843) se spřátelil s jinými významnými matematiky, zejména s Josephem Bertrandem a Carlem Gustavem Jacobim. Navzdory tomu, že se svým výzkumem zařadil mezi přední světové matematiky, jeho studijní úspěchy byly o poznání menší. V roce 1847 dokončil teprve bakalářské studium a následující rok získal místo přijímacího zkoušejícího na *École Polytechnique*.

Hermitova vědecká kariéra se v této době slibně rozvíjela a mezi lety 1848 a 1858 dosáhl svých největších výsledků (viz odstavec *Vědecká práce*). Publikoval několik článků z oblasti analytické teorie čísel a v roce 1856 se stal členem francouzské akademie věd. V tomtéž roce Hermite onemocněl pravými neštovicemi. Během doby, kdy byl nemocný, se velmi sblížil s Cauchym, který mu pomohl překonat nejtěžší fáze choroby. Pod Cauchyho vlivem Hermite konvertoval k římskokatolické církvi a stal se také, podobně jako Cauchy, přesvědčeným royalistou.

Roku 1862 získal na *École Polytechnique* místo takzvaného *maître de conférence*, které bylo vytvořeno speciálně pro něj, a o rok později se stal na téže škole zkoušejícím. Roku 1869 se stal profesorem analýzy na *École Polytechnique* a zároveň na *Sorbonně*. Na první z těchto škol zůstal do roku 1876, na druhé až do roku 1897, kdy odešel do důchodu.

Vědecká práce

Charles Hermite dosáhl významných výsledků zejména v teorii čísel a algebře. Zabýval se úspěšně také ortogonálními polynomy a eliptickými funkcemi. V roce 1848 dosáhl dobrých výsledků o dvojitě periodických funkcích a o rok později úspěšně aplikoval Cauchyovu metodu reziduí právě na tyto funkce. Zabýval se také teorií kvadratických forem a teorií invariantu. V souvislosti s tím vytvořil v roce 1855 teorii transformací. Jeho výsledky v této oblasti propojily teorii čísel, théta funkce a trasformace abelovských funkcí. Dokázal také, že obecnou algebraickou rovnici pátého stupně lze vyřešit pomocí eliptických funkcí a aplikoval tento výsledek v teorii čísel.

V roce 1873 dosáhl výsledku, který ho pravděpodobně nejvíce proslavil, když dokázal, že Eulerovo číslo e je transcendentní. Jeho metodu později zjednodušil Ferdinand von Lindemann a dokázal jejím užitím transcendentnost čísla π.

Další z jeho objevů

Symetrický, hermiteovský a sdružený operátor

Hermitovy polynomy

Hermitova normální forma

Hermitovsky sdružená matice

4.6. Felix Christian Klein

Felix Christian Klein (25. dubna 1849, Düsseldorf, Prusko – 22. června 1925, Göttingen, Německo) byl německý matematik. Zabýval se především geometrií (zejména neeukleidovskou), ale také teorií grup a teorií funkcí. Roku 1872 formuloval tzv. Erlangenský program, jehož hlavní myšlenkou je studovat jednotlivé geometrické struktury pomocí jejich symetrií a invariantů, a tak docílit hlubšího propojení geometrie s algebrou. Tento program výrazně ovlivnil rozvoj matematiky a fyziky ve dvacátém století.

Klein se narodil v Düsseldorfu do rodiny pruského vládního úředníka. Navštěvoval gymnázium v Düsseldorfu a poté studoval matematiku a fyziku na Rheinische Friedrich-Wilhelms-Universität zu Bonn am Rhein) v Bonnu. Doktorát získal v roce 1868 za práci *Über die Transformation der allgemeinen Gleichung des zweiten Grades zwischen Linien-Koordinaten auf eine kanonische Form* pod vedením Julia Plückera.

Po Plückerově smrti (1868) spolupracoval Klein s Alfredem Clebschem, který se také zasadil o to, aby Klein získal v roce 1872 místo profesora v Erlagenu v pouhých 23 letech. V roce 1875 však Klein získal místo na Technische Hochschule v Mnichově, kde vychoval řadu pozdějších vynikajících matematiků a fyziků (Adolf Hurwitz, Max Planck). Ještě v roce 1875 se oženil s Annou Hegelovou, vnučkou filosofa Georga W. F. Hegela.

V roce 1880 odešel na univerzitu v Lipsku, kde zůstal do roku 1886. V této době Klein vážně onemocněl a v letech 1883-1884 byl sužován těžkými depresemi. Charakter jeho matematické práce se poté pozvolna měnil, nepřestal však ovlivňovat vrcholnou matematiku své doby. Roku 1886 odešel do Göttingenu, kde zůstal pracovat až do odchodu do penze roku 1913. Během této doby dokázal z univerzity v Göttingenu vytvořit jedno z největších center matematiky na světě. Zasadil se také o to, že na göttingenskou univerzitu byly od roku 1889 přijímány i ženy. Od roku 1900 se Klein významně angažoval v problematice výuky matematiky na středních školách - zavedl například vyučování diferenciálního a integrálního počtu.

Ocenění

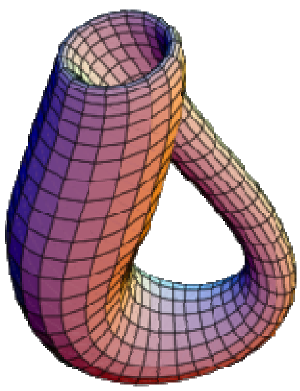
V roce 1885 byl Felix Klein zvolen členem Royal Society. Roku 1893 získal De Morganovu medaili udělovanou Londýnskou matematickou společností a v roce 1912 pak Copleyovu medaili.

Přínos matematice:

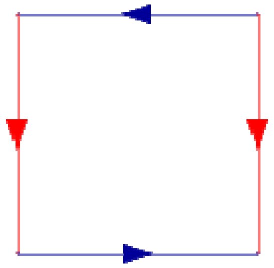
Felix Klein patří k velmi významným matematikům a vytvořil vlivné dílo nadčasové hodnoty. Jeho nejhlubší myšlenky se týkají zejména principiálních souvislostí mezi geometrií a algebrou (teorií grup). V této oblasti spolupracoval se Sophusem Liem. Oba tito vědci realizovali základy Kleinova Erlangenského programu, který výrazně ovlivnil nejen rozvoj moderní matematiky, ale velmi přispěl např. též k rozvoji teorie relativity a částicové fyziky. Klein se přitom zabýval zejména diskrétními grupami symetrií, zatímco Lie spojitými symetriemi. Při studiu neeukleidovských geometrií Klein objevil dvojrozměrnou uzavřenou plochu, která má pouze jeden povrch. Tato plocha se dnes po něm nazývá Kleinova láhev. Objevil též jeden z mimořádně významných a studovaných útvarů moderní matematiky, známým jako Kleinova kvartická křivka či Kleinova kvartika, fascinující svou symetrií a pozoruhodnými souvislostmi napříč matematikou. Kleinova kvartika představuje v jistém smyslu zobecnění Platónských těles pro případ, kdy jsou stěny tvořeny 24 pravidelnými sedmiúhelníky. Toto zobecnění je možné v prostoru s hyperbolickou geometrií. Klein ukázal, že tento útvar má právě 168 různých diskrétních symetrií (při uvažování zrcadlových symetrií 336) a tyto symetrie klasifikoval. Jde tedy o první případ tzv. Hurwitzovy plochy, dosahující maximální možný počet symetrií pro zadaný genus této plochy (v daném případě genus=3). V třírozměrném eukleidovském prostoru může být Kleinova kvartika reprezentována jako jistá plocha se třemi otvory (genus=3) a základní symetrií čtyřstěnu. Tento Kleinem objevený útvar v sobě slučuje tolik pozoruhodných vztahů a překvapivých souvislostí, že některými vlivnými matematiky bývá dokonce považován za "opravdu centrální část matematiky".

4.6.1. Kleinova láhev

Kleinova láhev je dvojrozměrný geometrický útvar, který si lze zjednodušeně představovat jako uzavřenou nádobu, která nemá vnitřek ani vnějšek. Nelze ji realizovat v trojrozměrném prostoru aniž by se protínala – to je možno nejméně v prostoru čtyřrozměrném. Pro Kleinovu láhev nelze rozhodnout, který bod prostoru je „venku“ a který „uvnitř“ (tato vlastnost se v topologii nazývá neorientovatelnost). Z toho přímo plyne, že tato plocha má jen jeden povrch.



Kleinova láhev je dvourozměrná varieta vytvořená následujícím způsobem. Vezměme uzavřený jednotkový čtverec $[0,1]^2$ s euklidovskou topologií (tj. otevřené množiny jsou právě sjednocení otevřených kruhů) a „slepme“ vždy dvě a dvě jeho protější strany tak, aby šipky v následujícím obrázku byly přilepeny na sebe.



Přesněji řečeno vytvoříme kvocientový prostor faktorizací čtverce podle ekvivalence $(0,y) \sim (1,y)$ pro $0 \le y \le 1$ a $(x,0) \sim (1-x,1)$ pro $0 \le x \le 1$. Na výsledném prostoru lze zřejmým způsobem zavést strukturu dvourozměrné variety.

4.7. David Hilbert

David Hilbert žil (23. ledna 1862 Wehlau (dnes Znamensk), Východní Prusko – 14. února 1943 Göttingen, Německo) byl jeden z největších matematiků 20. století.
Velký vliv na utváření Hilbertova charakteru měla matka. Její zájem o filozofii, astronomii a matematiku se přenášel na Davida, který od ní získával základní vzdělání. Po maturitě na gymnáziu v roce 1880 začal ve svém rodném městě studovat na univerzitě, která patřila už od poloviny století mezi nejlepší v Německu. Učili ho známí matematici Weber, Lindemann a Hurwitz. Již od gymnaziálních let ho vázala pouta přátelství s H. Minkowskim, který ho z Berlína seznamoval s nejnovějšími pracemi Kummera, Kroneckera a Weierstrasse. V 1885 obhájil Hilbert svou disertaci věnovanou vlastnostem invariantů určitých algebraických forem a odjel na studijní pobyt do Lipska, kde v té době působil F. Klein, který ho poslal ještě na rok k Ch. Hemitovi do Paříže. Po návratu až do r. 1895 přednášel Hilbert matematiku v Königsbergu. V tomto období se plně věnoval teorii invariantů. V r. 1890 podal čistě existenční důkaz věty, že každá soustava algebraických forem má konečnou bázi. Tento důkaz vyvolal značné diskuse právě z hlediska metodiky výstavby matematické teorie a byl napadán konstruktivisty.
Profesuru však Hilbert získal – tak jak bylo v té době na německých univerzitách zvykem – na jiné škole; a to když byl z iniciativy F. Kleina v r.1895 povolán do Göttingenu. V té době se Hilbert zajímal hlavně o teorii algebraických číselných těles. V letech 1898 – 1902 se věnoval práci o základech geometrie. V dalším období až do

roku 1912 se zaměřil převážně na problémy integrálních rovnic a v následujícím desetiletí do 1922 na matematickou fyziku. Poslední aktivní etapa Hilbertova života byla naplněna úvahami o obecných logických základech matematiky.

Nejvíce věhlasu si získaly dvě Hilbertovy práce z přelomu století. V letech 1889 - 1898 měl Hilbert přednášky věnované základům geometrie a v roce 1899 vyšla jeho kniha Grundlangen der Geometrie, která otevřela cestu pro jiné zaměření geometrie. Zcela nově pojal axiomatickou výstavbu teorie. Geometrie je v ní zbavena své smyslové názornosti. Kniha se stala pramenem tzv. Hilbertova formalismu – metody budování formálně abstraktních matematických teorií.

8. srpna 1900 vystoupil Hilbert v Paříži na Mezinárodním kongresu matematiků s hlavním referátem prostě nazvaným „Matematické problémy“. Formuloval 23 hlavních problémů tehdejší matematiky, o kterých se domníval, že by se jim měla věnovat badatelská pozornost. Až do současnosti reagují matematici na tyto podněty. Členský časopis JČSMF otiskoval od 3. čísla v roce 1971 informace o řešení 23 problémů.

V roce 1925 těžce onemocněl, sice se uzdravil, ale k plné tvůrčí aktivitě se přeci jenom nevrátil. Na svůj náhrobní kámen si nechal vytesat *Wir müssen wissen, wir werden wissen* (Musíme vědět, budeme vědět).

Celkem měl 69 PhD studentů, mnoho z nich se později stalo slavnými matematiky (například Otto Blumenthal (studium ukončil v roce 1898), Felix Bernstein (1901), Hermann Weyl (1908), Richard Courant (1910), Erich Hecke (1910), Hugo Steinhaus (1911), Wilhelm Ackermann (1925))

4.7.1. Hilbertovy problémy

Seznam 23 takzvaných **Hilbertových problémů** předložil David Hilbert v roce 1900 ve své přednášce *Problémy matematiky* na 2. mezinárodním kongresu matematiků v Paříži. Tyto problémy představovaly tehdy největší nevyřešené problémy. Velká část těchto problémů již dnes byla vyřešena, přičemž jejich řešení významně ovlivnilo matematiku 20. století.

Část ze seznamu řešených problémů

Existuje množina, jejíž kardinalita by byla menší než kardinalita množiny reálných čísel, ale větší než kardinalita spočetně nekonečné množiny?

Je kontinuum reálných čísel dobře uspořádaná množina?

Rigorózně podložit algebraickou geometrii, obzvláště Schubertovu výpočetní geometrii.

Nalézt způsob, jak vyjádřit definitní racionální funkci jako součet čtverců racionálních funkcí.

Jsou řešení problémů ve variačním kalkulu vždy algebraická?

Je a^b transcendentální číslo pro každé algebraické číslo $a \neq 0,1$ a iracionální číslo b?

Zobecnění teorie kvadratických forem pro libovolné algebraické těleso konečného stupně.

Zobecnění Kroneckerovy věty pro obecné algebraické těleso.

Jsou řešení problémů ve variačním kalkulu vždy algebraická?

Řešení lineárních diferenciálních rovnic při zadané charakteristické grupě.

4.7.2. Hilbertův program

Pojmem **Hilbertův program** se označuje snaha německého matematika Davida Hilberta o formalizaci matematiky až na úroveň jednoduchých axiomů, ze kterých by se daly korektně dokázat všechny matematické věty. Smyslem programu bylo redukovat složité matematické teorie (například matematickou analýzu) na jednoduché formální systémy a ty potom na jednoduchou aritmetiku, o které by se ukázalo, že je bezesporná a úplná.

Hilbert vyhlásil tento program ve 20. letech 20. století, ale již v roce 1931 dokázal Kurt Gödel své věty o neúplnosti. Jejich důsledkem je fakt, že pomocí aritmetiky nelze dokázat bezespornost a úplnost aritmetiky samotné a tedy ani bezespornost a úplnost složitějších teorií.

4.8. Richard Hamming

Professor Richard Wesley Hamming (11. února 1915 – 7. ledna 1998) byl americký matematik, známý pro svou práci na téma informativní teorie. Z jeho objevů například Hammingův kód, Hammingova vzdálenost a Hammingovo okno.

Richard Hamming získal titul bakaláře na universitě v Chicagu v roce 1937, magistra na universitě v Nebrasce v roce 1939 a Doktorát matematiky na universitě v Illinoii roku 1942. V roce 1945 se Hamming připojil k projektu *Manhattan Project* v Los Angeles.

V roce 1946, po druhé světové válce, Hamming působil v *Bell Telephone Laboratories*, kde pracoval s matematiky Shannon a Johnem Tukey. Pracoval tam do roku 1976, poté získal místo na Navalské postgraduální škole v Californii.

Hammingovo základní dílo o hledání chyb a opravování chyb objevil roku 1950.

Jeho práce v IBM 650 v roce 1956 vedla k vývoji programovacího jazyka L2.

Přestože byl nejlépe znám pro své programy, Hamming byl především číselný analytik. Pracoval na integraci diferenciálních rovnic a na svém spektrálním okně užívaném pro čistění dat. Psal učebnice, navrhoval průpovídky: " účel počítání je hlubší porozumění, nikoliv čísla“, "raději vyřešit správný problém špatně, než nesprávný problém dobře". Byl zakladatelem ACM a zastáncem *open-shop computing.*

Roku 1968 se stal členem *Institute of Electrical and Electronics Engineers* a byl oceněn tzv. Turing Prize. To je cena vydávaná *Association for Computing Machinery.*

4.8.1. Hammingův kód

V oblasti telekomunikací je **Hammingův kód** lineární kód pro opravu jedné chyby. Binární kód se nazývá *Hammingův*, jestliže má kontrolní matici, jejíž sloupce jsou všechna nenulová slova dané délky $n - k = r$ a žádné z nich se neopakuje.
Jedná se o speciální případ lineárních dvojkových (n,k) kódů. Tyto kódy opravují jednu chybu

při vzdálenosti kódových slov $d_{min}(\overrightarrow{b}_i, \overrightarrow{b}_j) = 3$ a v rozšířené variantě

$d_{min}(\overrightarrow{b}_i, \overrightarrow{b}_j) = 4$.

4.8.1.1. Algoritmus generování Hammingova kódu

1. Všechny bitové pozice, jejichž číslo je rovné mocnině 2, jsou použity pro paritní bit (1, 2, 4, 8, 16, 32, …).
2. Všechny ostatní bitové pozice náleží kódovanému informačnímu slovu (3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, …).
3. Každý paritní bit je vypočítán z některých bitů informačního slova. Pozice paritního bitu udává sekvenci bitů, které jsou v kódovém slově zjišťovány a které přeskočeny.

Pro paritní bit p_1 (pozice 1) se ve zbylém kódovém slově 1 bit přeskočí, 1 zkontroluje, 1 bit přeskočí, 1 zkontroluje, atd. Pro paritní bit p_2 (pozice 2) se přeskočí první bit, 2 zkontrolují, 2 přeskočí, 2 zkontrolují, atd. Pro p_3 (pozice 4) se přeskočí první 3 bity, 4 zkontrolují, 4 přeskočí, 4 zkontrolují, atd.

4.8.1.2. Hammingův kód (7,4)

Hammingův kód je získán pomocí konečných grup a využití zbytkových tříd při dělení dvěmi. Budeme předpokládat, že zpráva se skládá ze čtyřciferných čísel složených pouze z cifer 0, 1 .

Pro kód (7,4) platí $\overrightarrow{b} = \left(p_1^{(2^0)}, p_2^{(2^1)}, a_1^3, p_3^{(2^2)}, a_2^5, a_3^6, a_4^7\right)$

Kde $a_1, a_2, a_3, a_4, p_1, p_2, p_3 \in Z_2$. a_1, a_2, a_3, a_4 jsou čísla naší zprávy a p_1, p_2, p_3 dostaneme z výrazu :

- $p_1 \oplus a_1 \oplus a_2 \oplus a_4 = 0$ (podle bodu 3 sestaveno z b_1,b_3,b_5,b_7),
- $p_2 \oplus a_1 \oplus a_3 \oplus a_4 = 0$ (b_2,b_3,b_6,b_7),
- $p_3 \oplus a_2 \oplus a_3 \oplus a_4 = 0$ (b_4,b_5,b_6,b_7).

Generující matice $\mathbb{G}_H$ Hamming. kódu (7,4) se sestrojí tak, že se postupně zakóduje posloupnost $1000_1, 0100_2, 0010_3, 0001_4$ (proto, aby řádky byly lineárně nezávislé a tvořily bázi prostoru).

$$\mathbb{G}_H = \left(\begin{array}{cccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & p_{1_1} & p_{2_1} & 1 & p_{3_1} & 0 & 0 & 0 \\ 2 & p_{1_2} & p_{2_2} & 0 & p_{3_2} & 1 & 0 & 0 \\ 3 & p_{1_3} & p_{2_3} & 0 & p_{3_3} & 0 & 1 & 0 \\ 4 & p_{1_4} & p_{2_4} & 0 & p_{3_4} & 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{cccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 4 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

Kontrolní matice $\mathbb{H}_H$ Hamming. kódu (7,4) se určí následovně. Po přijetí kódového slova $\overrightarrow{b}$ víme, že bity b_3,b_5,b_6,b_7 obsahují informační slovo a zbylé redundantní bity jsou určeny tak, aby

$$\begin{aligned} s_1 &= b_4 \oplus b_5 \oplus b_6 \oplus b_7 = 0 \\ s_2 &= b_2 \oplus b_3 \oplus b_6 \oplus b_7 = 0 \\ s_3 &= b_1 \oplus b_3 \oplus b_5 \oplus b_7 = 0 \end{aligned} \Rightarrow \mathbb{H}_H = \left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right).$$

Vektor $\vec{s} = (s_1, s_2, s_3)$ se nazývá syndrom a pokud byla informace přijata bezchybně jeho hodnota je $\vec{s} = (0, 0, 0)$. Pokud ne, vznikla minimálně jedna chyba.

4.8.1.4. Dekódování a kontrola

Příjemce dekóduje následujícím způsobem. Nejprve se po přijetí kódového slova $\vec{b}$ určí syndrom $\vec{s} = \mathbb{H}_H \cdot \vec{b}^T$.

Pokud $\vec{s}$ vyjde nulový vektor, pak při přenosu nedošlo k žádné chybě.

Pokud ovšem $\vec{s}$ vyšlo nenulový vektor, došlo k minimálně jedné chybě.

1) Došlo-li pouze k jedné chybě. Výsledný vektor $\vec{s}$ nám ukazuje sloupec v matici $\mathbb{H}_H$. Protože všechny sloupce v $\mathbb{H}_H$ jsou navzájem různé, příjemce zjistí, kde se vyskytla chyba a může ji opravit. (pořadový sloupec v matici $\mathbb{H}_H$ určí změnu cifry pořadového řádku kódovaného slova $\vec{b}$).
2) Nastala-li více jak jedna chyba, pak nemůžeme chyby jednoznačně určit.

<u>Příklad kódování, dekódování a odstranění chyby.</u>

Chceme poslat zprávu $a_0 = (1,1,0,1)$.

Zprávu zakódujeme : $a_0 \cdot \mathbb{G}_H = \vec{b}_0 = (1,0,1,0,1,0,1)$ a odešleme

Předpokládejme že příjemce obdrží zprávu $\vec{b} = (1010111)$. Postupujeme určením syndromu

$$\vec{s} = \mathbb{H}_H \cdot \vec{b}^T$$

Tedy :

$$\mathbb{H}_H \cdot \overrightarrow{b}^T = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

Vidíme, že syndrom $\overrightarrow{s}$ je nenulový (při přenosu došlo k chybě). Syndrom, který vyšel $\overrightarrow{s} = (1, 1, 0)$ odpovídá sloupci 6 kontrolní matice $\mathbb{H}_H$ a z toho vyplývá, že je třeba opravit šestý bit kódového slova $\overrightarrow{b}' = (10101\underline{0}1)$.

(platí pouze pokud víme, že došlo k maximálně jedné chybě).

5. Závěr

Na závěr bych chtěl zhodnotit tuto práci. Myslím si, že výběr matematiků po konzultaci s vedoucím práce panem Mgr. Petrem Chládkem, Ph.D. se zdařil. Matematiky jako Pierre de Fermat, Karl Friedrich Gauss, Niels Henrik Abel , William Rowan Hamilton, Evariste Galois, Charles Hermite, Felix Christian Klein, David Hilbert a Richard Hamming lze skutečně zařadit mezi jedny z nejlepších v oboru matematické algebry, ale i mimo ni. Nejen tito matematici, ale především jejich díla a objevy poukazují na krásu a možnou využitelnost matematické algebry. A v tomto vidím využitelnost této práce, jak poukázat na tento obor jinou formou. Ukázat jeho historii, vrchní představitele a mnohdy i fantastické objevy či problémy, jako například, má oblíbená, Velká Fermatova věta.

Myslím si, že by bylo určitě zajímavé pokračování této práce, která by se zabývala například matematickou analýzou.

7. Seznam literatury

[1] Šalát, T. a kol.: *Malá encyklopédia matematiky*, Bratislava 1978

[2] Tlustý, P.: *Obecná algebra pro učitele*, Jihočeská univerzita, České Budějovice 2006

[3] Rosický, J.: *Algebra I*, Masarykova univerzita, Brno 1994

[4] http://www.sweb.cz/vladimir_ladma/czech/algebra/algebra.htm

[5] http://www.gymtc.cz/natura/2002/9/20020903.html

[6] http://www-gap.dcs.stand.ac.uk/~history/Mathematicians/Hamming.html

[7] http://vedci.wz.cz/

[8] http://cs.wikipedia.org/wiki/Port%C3%A1l:Matematika