Katolícka univerzita v Ružomberku, Pedagogická fakulta

Evariste Galois

– práca k predmetu História matematiky (RNDr. Štefan Tkačik, PhD.)

3.5.2009 Pavol Druska, Ma – Nv, 1.Mgr

Stručný životopis

Tento geniálny francúzsky matematik sa narodil 25. októbra 1811, blízko Paríža. Už ako sedemnásťročný vypracoval originálnu matematickú teóriu grúp, ktorá sa vyučuje dodnes. V devätnástich sa zapojil do odboja proti Bourbonovcom, za čo ho vylúčili zo školy a uväznili. Keď ochorel, prepustili ho. V nemocnici sa šialene zamiloval, no jeho láska ho o niekoľko dní priviedla do hrobu. V súboji mu ako dvadsaťročnému prestrelili brucho.

Rodičia boli zameraní humanitne, vyznali sa v literatúre, filozofii a náboženstve. Keď mal Evariste 10 rokov, komponoval kuplety, študoval rétoriku a literatúru. Nebol však zázračným dieťaťom, o čom svedčí aj vyjadrenie jeho učiteľa literatúry z roku 1829: „Toto je jediný študent, ktorý nevie absolútne nič. Povedali mi o jeho mimoriadnom matematickom nadaní, čo ma veľmi prekvapilo, pretože pri skúške z literatúry neprejavil nijakú inteligenciu.“

Učitelia mu vytýkali uzavretosť a nejasné vyjadrovanie a to, že je príliš vzdialený od praktických problémov. „Tento študent je ochotný zaoberať sa iba najvyššími sférami matematiky,“ napísal jeden z nich. Evariste mal vtedy už naštudovaného Eulera, Gaussa a Jacobiho. Napísal svoju životnú prácu, ktorú poslal na zverejnenie Parížskej akadémii vied. Tam ju zamietli a rýchlo stratili. To sa opakovalo dvakrát. Nie je isté, či ju vôbec uznali za hodnú ich akademickej pozornosti, keďže vedec, ktorý nebol známy, nemal vtedy veľké slovo.

Galois vnímal odmietnutie po svojom. „Vedecké funkcie nemôžu byť odmenou za tie alebo iné politické či náboženské názory,“ myslel si a nijako sa s tým netajil. Narážal na to, že akademici a učitelia boli poplatní režimu, ktorý potieral prívržencov republiky a podporoval priemernosť. Matematik Ian Stewart o ňom napísal: „V skutočnosti to mohla byť jeho vlastná chyba, pretože nemal vo zvyku vysvetľovať svoje nápady práve najzrozumiteľnejšie. A novátorstvo plus nezrozumiteľnosť je samovražedná kombinácia, najmä vtedy, ak ide o niekoho úplne neznámeho.“

Stewart zrejme trochu pozabudol, že každý tínedžer, nielen matematický génius, môže mať problémy s dodržiavaním pravidiel a sotva sa bude formálne vyjadrovať na úrovni predsedu vlády či akadémie. Dôležité je, že jeho originálna práca bola a zostáva jedným z kľúčov, ktorým sa odomyká tajomná skrinka modernej matematiky.

Galoisovým odkazom sú tieto slová: „Požiadajte verejne Jacobiho alebo Gaussa, aby vyslovili svoj názor ani nie tak na pravdivosť, ale na dôležitosť týchto viet. Dúfam, že sa časom nájdu ľudia, ktorým bude lúštenie tohto zmätku na prospech.“ Dnes je isté, že tento zmätok pomohol a pomáha „vytvoriť matematický odbor, ktorý poskytuje náhľad do takých rôznych oblastí, ako je aritmetika, kryštalografia, časticová fyzika a možné pozície Rubikovej kocky.“ (T. Rothman)

Jeho život však vyhasol veľmi skoro, a to kvôli milovanej Stéphanie, pre ktorú sa dal na súboj. Poznal ju veľmi krátko a je ťažké zistiť, aký mali vlastne vzťah. Vie sa, že si navzájom písavali listy a to je všetko. V danom súboji vraj Galois ani nevystrelil. Všetci si svoje tajomstvo odniesli na večnosť. Francúzsky génius príliš skoro - 31. mája 1832. Koho vraj bohovia milujú, chcú ho mať čím skôr pri sebe na Olympe. A on na ňom určite sedí, aspoň na tom matematickom. Ak sú bohovia spravodliví, nepochybne veľmi vysoko.

Galoisova teória

V matematike, presnejšie v abstraktnej algebre, **Galoisova teória**, pomenovaná po Evariste Galoisovi, poskytuje spojenie medzi teóriou polí a teóriou grúp. Použitím Galoisovej teórie, určité problémy v teórii polí sa môžu zredukovať do teórie grúp, ktorá je v istom zmysle jednoduchšia a zrozumiteľnejšia.

Pôvodne Galois použil grupy permutácií, aby opísal, ako rôzne korene danej polynomickej rovnice navzájom súvisia. Moderný prístup ku Galoisovej teórii, ktorý vyvinul Richard Dedekind, Leopold Kronecker a Emil Artin, zahŕňa okrem iného štúdium automorfizmu polí.

Aplikácia na klasické prolémy

Zrod Galoisovej teórie bol pôvodne motivovaný nasledujúcou otázkou, ktorej odpoveď je známa ako Abel-Ruffíniova veta.

> *"Prečo neexistuje formula pre korene piateho (alebo vyššieho) stupňa polynomickej rovnice pokiaľ ide o koeficienty mnohočlena, pri použití iba bežných algebraických operácií (sčítanie, odčítanie, násobenie, delenie) a aplikáciou odmocnín (druhá odmocnina,tretia odmocnina, atď.)?"*

Galoisova teória nielenže poskytuje krásnu odpoveď na túto otázku, ale tiež vysvetľuje do detajlov, prečo *je* možné vyriešiť rovnice štvrtého stupňa alebo nižšieho horeuvedeným spôsobom a prečo ich výsledky majú takú formu ako majú. Okrem toho dáva jasné a často praktické prostriedky počítania, keď niektoré jednotlivé rovnice vyššieho stupňa sa môžu vyriešiť týmto spôsobom.

Vzťah permutácie grúp k Galoisovej teórii

Keď máme daný polynóm, môže sa stať, že niektoré korene toho polynómu sú spojené rôznymi algebraickými rovnicami. Napríklad, môže sa ukázať, že pre dva korene, povedzme A a B, rovnica $A^2 + 5B^3 = 7$ platí. Centrálnou myšlienkou Galoisovej teórie je predpoklad, že tieto permutácie (alebo preskupenia) koreňov majú také vlastnosti, že ak akejkoľvek algebraickej rovnici vyhovujú tieto korene, vyhovujú jej aj permutované korene. Dôležitou podmienkou je, že my sa obmedzujeme na algebraické rovnice, ktorých koeficientmi sú racionálne čísla.

Tieto permutácie spoločne tvoria permutačnú grupu, volanú tiež Galoisovu grupu polynómu Objasníme to prostredníctvom príkladu.

príklad — kvadratická rovnica

Uvažujme o kvadratickej rovnici

$$x^2 - 4x + 1 = 0.$$

Použitím kvadratickej formuly zistíme, že tie dva korene sú

$$A = 2 + \sqrt{3}$$
$$B = 2 - \sqrt{3}.$$

Príklady algebraických rovníc, ktorým vyhovuje A a B zahŕňajú

$$A + B = 4, \quad \text{a}$$
$$AB = 1.$$

Pochpiteľne, v ktorejkoľvek z týchto rovníc, ak vymeníme A a B, získame ďalší pravdivý výrok. Napríklad, rovnica $A + B = 4$ sa stáva jednoducho $B + A = 4$. Okrem toho, je pravdivé, ale oveľa menej bežné, že toto platí pre *každú* možnú algebraickú rovnicu s racionálnymi koeficientmi, ktorej riešením sú korene A a B; aby sme to dokázali, potrebujeme teóriu symetrických polynómov.

Uzavrieme to tým, že Galoisova grupa polynómu $x^2 - 4x + 1$ pozostáva z dvoch permutácií: identická permutácia, ktorá necháva A a B nedotknuté, a transpozičná permutácia, ktorá vymieňa A a B. Je to cyklická grupa druhéhé rádu. Niekto by mohol vyjadriť námietku že A a B súvisia navzájom prostredníctvom ešte jednej algebraickej rovnice,

$$A - B - 2\sqrt{3} = 0$$

čo neostane pravdou, keď A a B sa vymenia. Avšak, táto rovnica sa nás netýka, pretože nemá racionálne koeficienty; hlavne, $-2\sqrt{3}$ nie je racionálny.

Podobnú diskusiu možno aplikovať na akékoľvek kvadratické polynómy $ax^2 + bx + c$, kde a, b a c sú racionálne čísla.

- Ak má polynóm len jeden koreň, napríklad $x^2 - 4x + 4 = (x-2)^2$, potom Galoisova grupa je triviálna; to je, obsahuje len identické permutácie.
- Ak má dva rôzne *racionálne korene*, napríklad $x^2 - 3x + 2 = (x-2)(x-1)$, Galoisova grupa je zase triviálna.
- Ak má *iracionálne* korene (vrátane prípadu, kde sú komplexné korene), potom Galoisova grupa obsahuje dve permutácie, práve tak, ako je v hore uvedenom príklade.

Zdroje:

1.) http://www.sme.sk/c/2969930/evariste-galois-a-kratky-vystup-na-matematicky-olymp.html
2.) http://en.wikipedia.org/wiki/Galois_theory
3.) http://www-history.mcs.st-and.ac.uk/