МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2011
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2011
Proceedings of the Fortieth Jubilee Spring Conference
of the Union of Bulgarian Mathematicians
Borovetz, April 5–9, 2011

200 ГОДИНИ ОТ РОЖДЕНИЕТО НА ЕВАРИСТ ГАЛОА

Нако Начев, Никола Зяпков, Иво Михайлов

През своя кратък жизнен път Галоа съзвава една теория, която полага основите на съвременната абстрактна математика. Понятията, които той въвежда – група, нормална подгрупа и нормално разширение на поле – дават началото на нови клонове в математиката като теория на групите, топологията, хомологичната алгебра. В наши дни тези понятия са често срещани в редица приложни науки като шумозащитното кодиране, криптографията, ядрените модели във физиката, кристалографията и много други.

Еварист Галоа

1. Биографични бележки. Целият живот на един човек е между две години, свързани с едно тире.

Еварист Галоа (1811–1832).

Какво се крие зад малкото тире?

Един кратък и бурен живот, изпълнен с героизъм и измамени надежди; едно светло име, което блести в съзвездието на най-ярките слънца на математиката ([13, 14, 16, 20, 21]).

Галоа е изключително явление в математиката. Още като юноша той полага основите на съвременната алгебра, но поради своята дълбочина, идеите му останали неразбрани за онова време. Отблъснат от официалните кръгове, той се хвърлил изцяло в политическите борби на Франция и на 20-годишна възраст паднал убит на дуел, инсцениран от полицията.

Еварист Галоа се появява като метеор на математическия небосклон и през краткия си живот създава гениални трудове, които променят коренно облика на цялата алгебра. Галоа полага основите на теорията на групите. Със създадената от него теория (сега тя се нарича теория на Галоа) той намира необходимите и достатъчни условия едно алгебрично уравнение да бъде решимо в радикали.

Еварист Галоа е роден на 26 октомври 1811 г. в парижкото предградие Бур ла Рен. Баща му Никола-Габриел Галоа бил известен със своите либерални и републикански възгледи. По време на стоте дни на Наполеон гражданите на Бур ла Рен го избрали за кмет и на този пост той останал 14 години. Майка му Аделаид-Мари Демант произхождала от семейство на прочути юристи и изиграла голяма роля в образованието и възпитанието на Еварист. Знаела отлично гръцки и латински език. В 1823 г. Галоа е записан в лицея "Луи льо Гран". Този лицей се славел, че подготвя изискани познавачи по гръцки и латински, но истинската му цел била да създава верни слуги на краля и защитници на църквата. Математиката там била слабо застъпена и не била включена в списъка на задължителните предмети. Затова Галоа се записал в допълнителна група по математика. В тази група обучението се водело по книгата на Льожандър "Начала на геометрията". Тази книга била предвидена да се изучи за две учебни години, но Галоа я завършил само за два дни. Скоро той разбрал, че не може много да разчита на г-н Верне – учителя по математика – и затова решил сам да залегне над книгите. Взел от библиотеката на лицея книгата на Лагранж "Решаване на числови уравнения", но не могъл да я прочете толкова бързо, както геометрията на Льожандър. Тази книга е тласнала Галоа да търси нови пътища за решаване на алгебричните проблеми и така да изгради своята гениална теория.

Мечтата на Еварист е била да постъпи в Политехническото училище, където ще има възможност по цял ден да се занимава с математика. Обаче, след конкурсните изпити му е отказан прием. Във връзка с това е известен цитатът: "Кандидатът с голяма интелегентност беше провален от екзаменатор с ниска интелегентност". Трябвало да остане в "Луи льо Гран". В специалния клас по математика тогава там преподавал г-н Ришар. Той давал трудни задачи за самостоятелна работа, които се опирали даже и на добрите ученици. Веднаж г-н Ришар пак диктувал три трудни задачи. Галоа ги решил само за 15 минути и дал решенията на учителя. Той много се изненадал и поощрил ученика. Той бил първият човек в "Луи льо Гран", който проявил жив интерес към Галоа.

Едно от елитните висши училища в Париж е било Нормалното училище, но в 1822 г. Бурбоните го закриват. В 1826 г. се открива Подготвителното училище, а в 1830 г. Галоа постъпва в него. На конкурсния изпит получава оценка осем по десетобалната система. Учител по математика е г-н Леруа. Веднаж той съобщил на класа за теоремата на Щурм и добавил, че доказателството още не е публикувано. Тогава той забелязал ироничната усмивка на Галоа и решил да го предизвика. Пламък проблясвал в очите на Галоа. Само след минута станал и написал доказателството на дъската. Учителят го похвалил, но злоба залегнала в душата му.

След Юлската революция Подготвителното училище било преименувано в Нормално училище. Еварист публикувал в печата остра разобличителна статия против двуличието на директора г-н Гиньо по време на Юлската революция. Затова бил изключен от Нормалното училище. Галоа си тръгнал с гордо вдигната глава. Осемдесет години по-късно проф. Жюл Танери от Нормалното училище отдал заслужена почит на Галоа [8].

Освен интереса си към математиката, Галоа активно е участвал в обществено-политическите борби на френския народ. Неговият живот протича по време на Реставрацията. На власт е династията на Бурбоните, а крал е Луи XVIII. Властта защитава интересите на роялистите и духовенството. На преследване са подложени както републиканците, така и бонапартистите. През есента на 1824 г. Луи XVIII умира и на престола се качва брат му граф Д'Артуа под името Шарл X. Новият крал е бил краен реакционер и силно ограничил правата на гражданите. На 25 юли 1830 г. той решил да извърши държавен преврат. Разпуснал Камарата на депутатите, унищожил свободата на печата, изменил конституцията в реакционен дух и насрочил избори. Това предизвикало силно негодувание сред народа. На 27 юли улиците на Париж се покрили с барикади. Галоа взел дейно участие в тази революция. На 29 юли народът победил, но от това се възползвала само едрата буржоазия. Кралят-предател избягал в Англия. Буржоазията побързала да постави на престола херцог Орлеански под името Луи Филип. Той бил крупен банкер и укрепил господството на финансовата буржоазия. Произхождал от Орлеанския клон на Бурбонската династия.

След Юлската революция Галоа се записва в дружеството "Приятели на народа" и се включва активно в неговата дейност. На един банкет на дружеството Галоа вдига тост против Луи Филип. На другия ден той е арестуван и изпратен в затвора "Света Пелагия", където е изпращан още няколко пъти. Именно там той създава своите научни трудове. От затвора Галоа съобщава на своя приятел Шевалие, че най-малката проста група е алтернативната от 5-та степен и затова общото уравнение от 5-та степен е нерешимо в радикали [7]. Галоа представя няколко пъти своите трудове в Парижката академия на науките, но винаги без резултат. Водещите математици по онова време в Парижката Академия на науките не са могли да разберат идеите на Галоа и не са ги оценили.

На 15 юни 1831 г. се е състоял процесът срещу Галоа. Той е обвинен в опит да предизвика покушение върху живота и особата на краля. По време на разпита Галоа произнася пламенна реч, наситена с революционен оптимизъм и републиканска страст. Съдът го оправдава. Много е трудно да се обясни това в тогавашна реакционна Франция, но фактът си остава факт. Полицията остава недоволна от изхода на процеса и търси нов повод да се справи с непокорния младеж. И случаят не закъснява. На 14 юли 1831 г. по случай 42-годишнината от щурма на Бастилията републиканците организират тържествен парад. Полицията успява да арестува Галоа и отново го праща в "Света Пелагия". Но и това не можало да удовлетвори блюстителите на реда. На 29 юли прокънтял изстрел в затвора, който профучал само на косъм от главата на Галоа. След излизането от затвора злонамерените полицаи го оплитат в любовна интрига и Галоа е извикан на дуел. По време на дуела Галоа не е стрелял. Секундантите са го изоставили, а те са били длъжни да му дадат първа помощ. Лекарят също избягал най-позорно. Полицаите наблюдавали всичко и потривали доволно ръце. На 31 май 1832 година в 10 часа сутринта Галоа умира в болницата на ненавършени 21 години.

Смърт и безсмъртие! Угасва една ярка звезда на небосклона на математиката, един гениален ум, един доблестен гражданин.

В своите мемоари Александър Дюма – баща (авторът на романа "Граф Монте Кристо"), който лично се е познавал с Еварист, писал, че той е бил убит на дуел от Пеше Д'Ербинвил. Този млад човек също бил член на дружеството "Приятели на народа", произхождал от аристократично семейство и бил много надменен. Промъкнал се в републиканското гнездо, за да доносничи и шпионира. Низки душици винаги се намират.

Няколко дни по-късно избухва следващата революция, но този път без Галоа. Семейството на Галоа изпраща ръкописите му на Огюст Шевалие. Още същата година той ги публикува в "Енциклопедически преглед". По-късно трудовете на Галоа попадат в ръцете на Лиувил, който добросъвестно ги проучва и публикува най-важните в "Списание за чиста и приложна математика" [8]. Бертран прави биографичен очерк за Галоа. В 1870 г. Камил Жордан написва обемиста книга, която той нарича коментар на ръкописите на Галоа – просто от скромност. Именно този труд привлича вниманието на математиците към наследството на Галоа. В края на 19 век идеите на Галоа добиват световна известност. Норвежкият математик Софус Ли в 1894 г. назовава имената на най-великите математици на 19 век. Едно от тях е Еварист Галоа.

2. Научни приноси. В края на 18 век френските математици Лагранж (1736–1813) и Вандермонд (1735–1796) въвеждат в математиката първия групов обект – субституциите [15]. Теоретико-групови разсъждения прави и Гаус (1777–1855) в своите аритметични изследвания. Галоа за първи път формулира в своите разработки групата като абстрактно понятие. Той ползва съществено това ново понятие и поставя началото на теорията на групите с въвеждането на абстрактни дефиниции за подгрупа, съседни класове по подгрупа, нормална подгрупа, разрешима група и др. Галоа пренася тази теория и върху полетата като дефинира група от автоморфизми на поле, които оставят неподвижно. Така се достига до понятията нормално разширение на поле и група на Галоа, които са широко използвани и в наши дни. Поради своята абстрактност за онова време, обаче, идеите на Галоа са били възприети с големи резерви. Голяма роля за тяхното разясняване има Камил Жордан (1838–1922), който последователно издава трудовете "Коментари към мемоара на Галоа" (1865), "Коментари към Галоа" (1869) и фундаменталната си монография "Трактат за субституциите и алгебричните уравнения" (1870). Чрез изследването на групата на дадено алгебрично уравнение, Галоа намира критерий за неговата решимост в радикали.

2.1. Разрешимост на алгебричните уравнения в радикали. Още древногръцките математици са можели да решават квадратни уравнения. Правилото за намиране корените на квадратното уравнение е описано в съчинението на Мохамед ал Хорезми (787–850) "Ал-джебр ал-мукабала". Във формулите на Мохамед ал Хорезми участват четирите рационални действия (събиране, изваждане, умножение и деление) и извличане на квадратен корен, т.е. квадратен радикал. Естествено се поставя въпросът може ли да се намерят такива формули и за уравненията от по-висока степен. Трябвало да минат почти 700 години до откриването на формули за решаване на общите уравнения от 3-та и 4-та степен. Тези открития са направени от италианските математици Сципионе дел Феро (1465–1526), Николо Тарталия (1499–1557) и Людовико Ферари (1522–1565). Резултатите им са публикувани през 1535 година от италианския лекар и математик Джироламо Кардано (1501–1576) в книгата му "Великото изкуство". След това почти три столетия математиците са правили безуспешни опити да намерят формули, които с помощта на радикали да изразяват корените на произволно уравнение от пета степен. Италианският лекар Паоло Руфини (1765–1822) през 1799 година е предположил, че такива формули не съществуват. Доказателството на Руфини имало известни пропуски. През 1826 година норвежкият математик Нилс Абел (1802–1829) публикува статия, в която доказва, че общото уравнение от степен по-висока от 4 е нерешимо в радикали. Той доказва, че не е възможно да се превърне в тъждество общото уравнение от степен по-висока от четири, ако неизвестното в него се замести с израз, съставен от коефициентите на уравнението с помощта на действията събиране, изваждане, умножение, деление и извличане на корени.

Теоремата на Абел, която сега наричаме теорема на Абел-Руфини, дава отрицателен отговор за решимост в радикали на общото уравнение от степен по-голяма от 4. Има обаче много конкретни уравнения от степен по-висока от 4, които са решими в радикали. Затова се поставя въпросът за пълно решение на задачата – намиране на критерий за решимост на уравненията в радикали. Този критерий намира Галоа, като използва гениалната идея на всяко уравнение да съпостави група от субституции на корените на уравнението. Чрез изследването на тази група, нейни подгрупи и свързаните с тях радикални разширения на полето от коефициентите, той решава тази задача. Галоа публикува някои частни случаи [2, 3], а Лиувил публикува крайния резултат на Галоа [5] през 1846 година. По-конкретно, идеите на Галоа могат да се изложат на съвременен алгебричен език по следния начин.

Нека ни е дадено уравнението $f(x) = 0$ с коефициенти от някакво поле K, което можем да считаме за простота, че е крайно разширение на $\mathbb{Q}$, получено след присъединяване на коефициентите на полинома $f(x)$ към $\mathbb{Q}$. Можем да считаме също, че $f(x)$ е неразложим полином от степен $n \geq 1$. Да означим с L полето на разлагане на $f(x)$ над K, т.е. минималното разширение на K, което съдържа корените на $f(x)$. Тогава, всеки автоморфизъм на L, който оставя неподвижни елементите на K, ще размества корените на $f(x)$. По този начин групата на Галоа на полинома $f(x)$, т.е. групата на Галоа на разширението L/K се явява транзитивна подгрупа на симетричната група S_n.

Нека да приемем, че някое решение на уравнението $f(x) = 0$ се представя във вида

$$\sqrt[k]{\cdots + \sqrt[l]{\cdots} + \sqrt[m]{\cdots} + \cdots}. \tag{1}$$

За простота ще считаме, че полето K притежава корен на единицата от степен равна на най-малкото общо кратно на всички коренни показатели на (1). Нека $p_1, p_2, \ldots$ са простите числа, които са делители на тези показатели. След това можем да присъединим последователно всяко $\sqrt[p_i]{a}$, което участва в (1). Така получаваме ред от циклични разширения от прости степени:

$$K \subset L_1 \subset L_2 \subset \cdots \subset L_K,$$

където L_K е нормално разширение на K, което съдържа поне един корен на $f(x)$.

Тогава, L_K трябва да съдържа всички корени на $f(x)$, а следователно трябва да съдържа и полето на разлагане L на $f(x)$.

Да означим с $\mathcal{G}$ и G групите на Галоа съответно на нормалните разширения L_K/K и L/K. Тогава получаваме следния ред от подгрупи:

$$\mathcal{G} \supset \mathcal{G}_1 \supset \mathcal{G}_2 \supset \cdots \supset \{e\},$$

в който всяка от тях е нормална на предходната и факторгрупите $\mathcal{G}_i/\mathcal{G}_{i+1}$ са циклични от прости редове p_i. Следователно, $\mathcal{G}$ е разрешима група, а понеже G се явява факторгрупа на $\mathcal{G}$, то и G е разрешима група. Вярно е и обратното твърдение. Така Галоа достига до следния резултат:

Едно неразложимо алгебрично уравнение с коефициенти от полето K е решимо в радикали тогава и само тогава, когато групата му на Галоа е разрешима.

Горният критерий може да бъде обобщен и за полета K с произволна характеристика, които не съдържат необходимите корени на единицата (вж. напр. [11, 17]).

От този критерий веднага се получава теоремата на Абел-Руфини за неразрешимост на общото уравнение от степен ≥ 5, тъй като то има за група на Галоа симетричната група S_n, която е неразрешима при $n \geq 5$.

2.2. Крайни полета. Галоа е положил също и основите на теорията на крайните полета, които сега наричаме полета на Галоа. В [6] Галоа разглежда полиномиалните уравнения от вида $F(x) \equiv 0 \pmod{p}$, които нямат цели корени. Той не ги записва като сравнения по $\bmod p$ (p-просто число), а като уравнения в полето на остатъците по $\bmod p$, което днес означаваме със $\mathbb{Z}_p$. Когато едно такова уравнение няма корени в $\mathbb{Z}_p$, той доказва, че те са елементи на разширение на $\mathbb{Z}_p$ и са корени на уравнението $x^{p^n} = x$. Този резултат може да се изкаже по следния начин:

За всяко просто число p и за всяко естествено число n съществува единствено поле с брой на елементите $q = p^n$, което е изоморфно на полето на разлагане на полинома $x^q - x \in \mathbb{Z}_p[x]$.

2.3. Верижни дроби. В своята първа научна публикация [1] Галоа доказва няколко резултата отнасящи се до верижните дроби. Във връзка с известната теорема, че всяка периодична верижна дроб е корен на квадратно уравнение с цели коефициенти, Галоа пише следното: *Когато някакво уравнение има два периодични корена, съответстващи на един рационален множител от втора степен, то между тези два корена съществува твърде странна връзка, която струва ми се още не е забелязана. Ако единият от корените на някакво уравнение представлява чисто периодична верижна дроб, то уравнението има и друг периодичен корен, получаващ се при деление на отрицателната единица на верижна дроб, написана в обратен ред.*

Този резултат както и всички необходими сведения за верижните дроби могат да се намерят в [18].

След доказателството на тази теорема Галоа продължава с други две твърдения: *Ако коренът на уравнение от втора степен е чисто периодична верижна дроб и е по-голям от 1, то вторият корен се намира между -1 и 0. Ако единият от корените на уравнение от втора степен е по-голям от 1, а вторият е между -1 и 0, то тези корени се представят като чисто периодични дроби.*

2.4. Производна на функция. Галоа също доказва и една теорема от анализа [4], която след известно уточнение във формулировката е известна като теорема на Коши:

Нека $F(x)$ и $f(x)$ са две функции. Тогава съществува функция $\varphi(x)$ такава, че за произволни x и h е в сила равенството

$$\frac{F(x+h)-F(x)}{f(x+h)-f(x)}=\varphi(k),$$

където k се намира между x и $x+h$.

От тази теорема се получава следствието, че

$$\lim_{h\to 0}\frac{F(x+h)-F(x)}{f(x+h)-f(x)}=\varphi(x),$$

което показва съществуването на производна на функция ако $f(x)=x$.

2.5. Абелови интеграли. Галоа излага в [5] някои резултати за интеграли, до които достига също и Риман 25 години по-късно. Галоа говори за период на абелов интеграл относно произволна алгебрична функция. Предполага се, че той е предчувствал някои понятия, отнасящи се до функциите на комплексна променлива, които са били развити няколко години след смъртта му. Той класифицира абеловите интеграли на три рода и твърди, че ако n е броят на линейно независимите интеграли от първи род, то броят на периодите е $2n$.

Галоа също така прави обобщение на класическото съотношение на Льожандър, в което участват периоди на елиптични интеграли. Това води до други важни съотношения открити по-късно от Вайерщрас и Фуко.

3. Заключение. Чрез своите открития Галоа поставя основите на съвременната алгебра. Създава се теорията на Галоа за полета, която интензивно се развива и сега. В най-общ смисъл под теория на Галоа разбираме такава теория, която изучава математически обекти на основата на техните групи от автоморфизми. Така са възникнали теорията на Галоа за пръстени, теорията на Галоа за топологични пространства и други. Един от най-значимите все още нерешени проблеми на математиката се явява обратната задача в теорията на Галоа: дали всяка крайна група се реализира като група на Галоа на някакво нормално разширение на полето на рационалните числа $\mathbb{Q}$ (вж. [9] за повече информация по този проблем).

Идеите на Галоа се използват и в геометрията. През 1872 г. немският математик Ф. Клайн (1849–1925) в своята встъпителна лекция при избирането му за професор в университета в град Ерланген (Германия) формулира предмета на геометрията по следния начин: *Геометрията е наука, изучаваща свойствата на фигурите, които са инвариантни относно някаква група от преобразувания.*

Теорията на Галоа също така дава възможност да се решават задачи за построяване с линийка и пергел. Въвеждането на квадратично достижими разширения, чиито групи на Галоа са 2-групи, води до изясняване и доразвиване идеите на Гаус и Ванцел [10] за това кога е възможно да се извърши дадено построение (за подробно изложение на този метод вж. [12, 17, 19]).

Крайните полета, които Галоа въвежда играят важна роля в много области на съвременната математика и нейните приложения. Една от тях е теорията на кодирането. Изследването на групата от автоморфизми на самодуален код C води до важни резултати при изследването на тези кодове и тяхното конструиране. Съществена роля има онази част от кода, която остава неподвижна под действието на група от автоморфизми на този код.

Накрая да цитираме следната мисъл на Галоа: *В бъдеще учените вместо да изпращат в академиите запечатани пакети, ще се обединяват в изследователски екипи.* Това още веднъж показва колко много Галоа е изпреварил своето време.

ЛИТЕРАТУРА

[1] É. Galois. Démonstration d'un théorème sur les fractions continues périodiques. *Ann. Math. Pures Appl. de M. Gergonne*, **19** (1829), 294–301.

[2] É. Galois. Analyse d'un Mémoire sur la résolution algébrique des équations. *Bulletin des Sciences mathematiques*, **XIII** (1830), 271.

[3] É. Galois. Note sur la résolution des équations numériques. *Bulletin des Sciences mathematiques*, **XIII** (1830), 413.

[4] É. Galois. Notes sur quelques points d'analyse. *Ann. Math. Pures Appl. de M. Gergonne*, **21** (1830), 182–184.

[5] É. Galois. Mémoire sur les conditions de résolubilite des équations par radicaux. (dated 6 January 1831, edited by J. Lioville) *J. Math. Pures Appl.*, **11** (1846), 417–433.

[6] É. Galois. Sur la théorie des nombres. *Bull. Sci. Math. Férussac*, **13** (1830), 428–435. (See also 40b. *J. Math. Pures Appl.*, **11** (1846), 398–407).

[7] É. Galois. Lettre de Galois á M. Auguste Chevalier. *J. Math. Pures Appl.*, **XI** (1846), 408–415.

[8] É. Galois. Œuvres mathématiques d'Évariste Galois. J. Liouville, *Jour. de Math. Pures et Appliquées*, **XI** (1846) Id. 1906-07. Manuscrits et papiers inedits de Galois. *J. Tannery, Bull. des Scie. Math.* XXX; XXXI; Id. 1962, Écrits et mémoirs mathématiques d'Évariste Galois. Azra J.-P., Paris, Bourgne.

[9] I. Michailov, N. Ziapkov. The inverse problem of Galois theory. *Math. and Education in Math.* **37** (2008), 17–28.

[10] M. L. Wantzel. Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas. *Journal de Mathématiques Pures et Appliquées*, **1** (1837), No 2, 366–372.

[11] Б. Л. ван дер Варден. Алгебра. Наука, Москва, 1979.

[12] Г. Генов, Ст. Миховски, Т. Моллов. Алгебра. Университетско издателство, Пловдив , 2006.

[13] А. Дальма. Эварист Галуа, революционер и математик, Москва, 1960 (перевод с французкого).

[14] Л. Дерелиев. Еварист Галоа, библиотека "Бележити хора на науката". ДИ "Народна просвета", София, 1961.

[15] История на математиката, том 4 (под редакцията на А. Колмогоров и А. Юшкевич), София, 1981 (превод от руски).

[16] Л. Инфельд. Эварист Галуа – Избранник богов. Москва, 1958 (перевод с английского).

[17] И. Михайлов, Н. Зяпков. Висша алгебра и теория на Галоа. Фабер, Велико Търново, 2004.

[18] Н. Обрешков. Задачи и теореми по висша алгебра (с приложение Теория на верижните дроби). София, 1966.

[19] А. Попов, П. Сидеров, К. Чакърян. Теория на Галоа. Веди, София, 2010.

[20] Э. Галуа. Сочинения, под редакцией и с примечаниями Н. Г. Чеботарева с приложением статьи П. Дюпюи "Жизнь Эвариста Галуа". Москва, 1936 (перевод с французкого).

[21] Н. Г. Чеботарев. Основы теории Галуа, том **1–2**, Москва, 1934–37.

Нако Начев
Факултет по математика и информатика
Пловдивски университет "П. Хилендарски"
бул. България № 236
4003 Пловдив
e-mail: nachev@uni-plovdiv.bg

Никола Зяпков, Иво Михайлов
Факултет по математика и информатика
Шуменски университет "Епископ К. Преславски"
ул. Университетска № 115
9712 Шумен
e-mail: ziapkov2000@yahoo.co.uk, ivo_michailov@yahoo.com

200TH ANNIVERSARY OF EVARISTE GALOIS (1811-1832)

Nako A. Nachev, Nicola P. Ziapkov, Ivo M. Michailov

During his short life path Galois invented a theory, which would set the foundations of the contemporary abstract mathematics. He introduced the definitions of groups, normal subgroups and normal field extensions, which gave birth of new branches in mathematics such as group theory, topology, homological algebra. Nowadays these objects are frequently encountered in various applied sciences – coding theory, cryptography, nuclear models in physics, crystallography and many other.