BO1.1. History of Mathematics
Lecture X
The 19th-century beginnings of ‘modern algebra’

MT25 Week 5

Summary

- Lagrange's ideas (1770/71)
- Cauchy and substitutions (1815)
- 'Classical age' of theory of equations 'ends' (1799–1826)
- The invention of groups by Galois and Cauchy
- 'Symbolical algebra'
- Groups, rings, and fields: the emergence of 'modern algebra' (1854–1900)

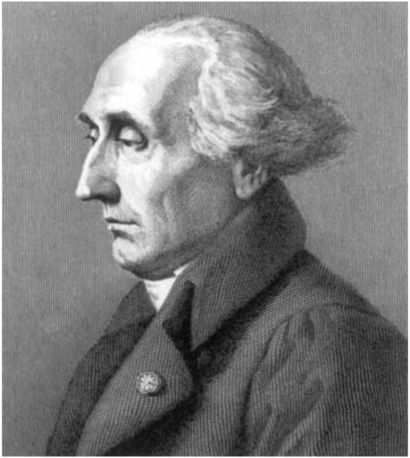
‘Modern’ or ‘abstract’ algebra

19th century: emergence of mathematics whose subject-matter is no longer space or number:

- permutations
- abstract structures (groups, rings, fields, ...)
- linear algebra [see Lecture XIV]

Lagrange's 'Réflexions' 1770/71

J.-L. Lagrange, 'Réflexions sur la résolution algébrique des équations', Berlin (1770/71):



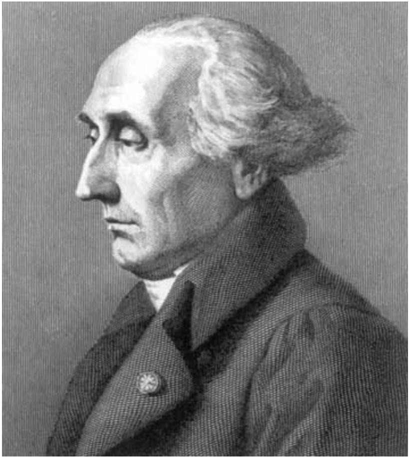
Lagrange's 'Réflexions' 1770/71

J.-L. Lagrange, 'Réflexions sur la résolution algébrique des équations', Berlin (1770/71):

Asserted that there had been little advance in equation-solving since Cardano, but that there was little left to do

Examined all known methods of solving cubics and quartics

Found that in every case the solutions of the 'reduced' (or 'resolvent') equation are 'functions' of the roots of the equation to be solved



Resolvents for cubics

For a cubic with roots x_1, x_2, x_3 there is a reduced equation whose roots are values of

$$y = \frac{1}{3}\left(x_1 + \alpha^2 x_2 + \alpha x_3\right)$$

where $\alpha^3 = 1$, $\alpha \neq 1$.

Lagrange: since y^3 takes just 2 values as x_1, x_2, x_3 are permuted, it satisfies a quadratic equation: the resolvent of the cubic

Lagrange identified this idea as a feature common to the methods for solving cubics presented by Cardano, Tschirnhaus, Bézout, and Euler

Resolvents for quartics

For a quartic with roots x_1, x_2, x_3, x_4 there is a reduced equation whose roots are values of

$$y = \frac{1}{2}\,(x_1 x_2 + x_3 x_4)$$

Lagrange: since y takes just 3 values as x_1, x_2, x_3, x_4 are permuted, it satisfies a cubic equation.

There is also reduced equation whose roots are values of

$$z = \frac{1}{2}\,[(x_1 + x_2) - (x_3 + x_4)]$$

Lagrange: since z^2 takes just 3 values as x_1, x_2, x_3, x_4 are permuted, it satisfies a cubic equation.

Resolvents in general

Let the given equation be of degree n with roots $x_1, x_2, x_3, \cdots, x_n$

Theorem: Let $y = f(x_1, x_2, x_3, \cdots, x_n)$. Then y is a root of an equation of degree m, where m is the number of values taken by y (that is, by f) under permutations of $x_1, x_2, x_3, \cdots, x_n$

Theorem: The number of values of f will always be a divisor of $n!$

Note 1: The insight is wonderful; the proof is not

Note 2: This theorem mutated several times, finally morphing into Lagrange's Theorem in group theory.

(See *Mathematics emerging*, §12.3.1, and also: Richard L. Roth, 'A history of Lagrange's Theorem on groups', *Mathematics Magazine* **74**(2) (2001), pp. 99–108)

Resolvents for equations of degree 5

For a quintic equation the general resolvent equation will be of degree 120. But if

$$y := x_1 + \varphi^4 x_2 + \varphi^3 x_3 + \varphi^2 x_4 + \varphi\, x_5$$

then y^5 takes only 24 values, so satisfies a resolvent equation of degree 24.

This can be reduced to another resolvent equation of degree 6.

Is there any hope of reducing it further?

Those influenced by Lagrange: Paolo Ruffini

Paolo Ruffini (1765–1822), *Teoria generale delle equazione* (1799) and a number of articles 1804–1819:

- showed that a function of 5 variables cannot take 3 or 4 values
- claimed to have proved that equations of degree 5 were not in general solvable by radicals
- sent book to Lagrange in 1802 and to Paris academy; no response
- further explanatory papers 1802, 1806, ...

A long, confused and confusing account, which seems to have persuaded no-one except Italian pupils and colleagues?

Those influenced by Lagrange: A.-L. Cauchy

A.-L. Cauchy (1789–1857), ‘Mémoire sur le nombre de valeurs qu’une fonction peut acquérir, lorsqu’on y permute de toutes les manières possibles les quantités qu’elle renferme’, *Journal de l’École polytechnique*, 1815:

Established notation and some theory for substitutions

Theorem: Let N be the number of values of a function of n variables. Either $N \leq 2$ or $N \geq p$ for any prime number $p \leq n$.

Conjecture: For $n \geq 5$, either $N \leq 2$ or $N \geq n$.

Proved his conjecture for $n = 6$

(See *Mathematics emerging*, §13.1.1.)

Those influenced by Lagrange: N. H. Abel

Niels Henrik Abel (1802–1829), ‘Beweis der Unmöglichkeit, algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen’, *Crelle’s Journal*, 1826:

For $n = 5$, refined Cauchy’s 1815 theorem

Used this to prove conclusively that the general equation of degree 5 is not soluble by radicals.

That is, there is no formula involving radicals for a solution of equations of degree 5.

The end of ‘classical algebra’ (?)

Évariste Galois (1811–1832)

Galois and his groups (1)

Évariste Galois (1811–1832), 'Mémoire sur les conditions de résolubilité des équations par radicaux', manuscript known as the *Premier mémoire*

Explored the question of which numerical equations are soluble by radicals, which not:

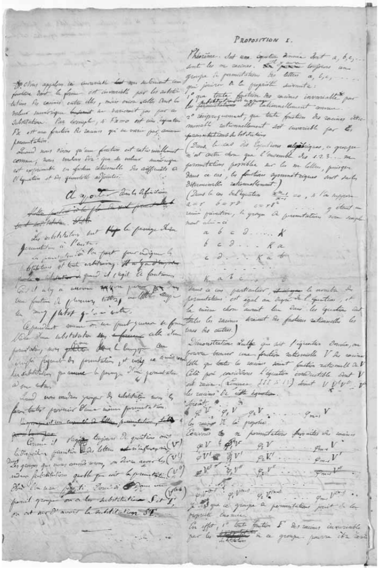
- submitted his ideas to the Academy in 1829, withdrew his articles January 1830 on Cauchy's advice
- resubmitted February 1830; lost after Fourier died in 1830
- resubmitted January 1831, rejected by Academy on Poisson's advice in July 1831
- corrected by Galois up to his death by duel in 1832
- to be read in conjunction with Galois' Testamentary Letter of 29 May 1832 to Auguste Chevalier

Galois and his groups (2)

Galois, in his writings 1829/30 (published 1846):

- invented groups (of permutations) [note: Cauchy invented groups in 1845, almost certainly independently]
- pre-invented fields (in ‘Théorie des nombres’ [published 1830] and as his ‘rationally known quantities’)
- showed how to associate a group to a polynomial (its Galois group)
- discovered a necessary and sufficient condition for solubility of an equation by radicals expressed in terms of the structure of its group
- as an application, gave a necessary and sufficient condition for solubility of an irreducible equation of prime degree by radicals

Galois and his groups (3)



PROPOSITION I.

Théorème. Soit une équation donnée dont a, b, c, ... sont les m racines. ~~On pourra~~ Il y aura toujours un groupe de permutations des lettres a, b, c, ... qui jouira de la propriété suivante:

1° que toute fonction des racines invariable* par les ~~permutations~~ substitutions de ce groupe soit rationnellement connue.

2° réciproquement, que toute fonction des racines déterminable rationnellement soit invariable par ~~les permutations~~ les substitutions.

(Dans le cas des équations algébriques, ce groupe n'est autre chose que l'ensemble des 1.2.3....m permutations possibles sur les m lettres, puisque dans ce cas, les fonctions symétriques sont seules déterminables rationnellement.)

(Dans le cas de l'équation $\frac{x^n-1}{x-1}=0$, si l'on suppose $a=r$, $b=r^g$, $c=r^{g^2}$, ..., g étant une racine primitive, le groupe de permutations sera simplement celui-ci

a b c d ..... k
b c d .... k a
c d .... k a b
....
k a b c .... b

dans ce cas particulier, ~~[illegible]~~ le nombre des permutations est égal au degré de l'équation, et la même chose aurait lieu dans les équations dont toutes les racines seraient des fonctions rationnelles les unes des autres.)

Démonstration. Quelle que soit l'équation donnée, on pourra trouver une fonction rationnelle V des racines telle que ~~toutes~~ les racines soient fonctions rationnelles de V. Cela posé, considérons l'équation irréductible dont V est racine. (Lemmes III et IV) Soient $V, V', V'', \ldots V^{(n-1)}$ les racines de cette équation.

Soient $\varphi V \quad \varphi_1 V \quad \varphi_2 V \ldots\ldots \varphi_{m-1} V$ les racines de la proposée.

Écrivons les n permutations suivantes des racines

$$\begin{array}{lllll}
(V) & \varphi V & \varphi_1 V & \varphi_2 V \ldots\ldots & \varphi_{m-1} V \\
(V') & \varphi V' & \varphi_1 V' & \varphi_2 V' \ldots\ldots & \varphi_{m-1} V' \\
(V'') & \varphi V'' & \varphi_1 V'' & \varphi_2 V'' \ldots\ldots & \varphi_{m-1} V'' \\
 & \ldots & \ldots & \ldots & \ldots \\
(V^{(n-1)}) & \varphi V^{(n-1)} & \varphi_1 V^{(n-1)} & \varphi_2 V^{(n-1)} \ldots\ldots & \varphi_{m-1} V^{(n-1)}
\end{array}$$

Je dis que ce groupe de permutations jouit de la propriété énoncée.

En effet, 1° toute fonction F des racines invariable par les ~~permutations~~ substitutions de ce groupe pourra être écrite

*Nous appelons ici invariable ~~[illegible]~~ non seulement une fonction dont la forme est invariable par les substitutions des racines entre elles, mais encore celle dont la valeur numérique ~~[illegible]~~ ne varierait pas par ces substitutions. Par exemple, si Fx=0 est une équation, Fx est une fonction des racines qui ne varie par aucune permutation.

Quand nous dirons qu'une fonction est rationnellement connue, nous voulons dire que sa valeur numérique est exprimable en fonction rationnelle des coefficients de l'équation et des quantités adjointes.

A ajouter dans les définitions

~~[illegible] toute substitution. [illegible]~~

Les substitutions sont le passage d'une permutation à l'autre.

La permutation d'où l'on part pour indiquer les substitutions est toute arbitraire, ~~[illegible]~~ quand il s'agit de fonctions. Car il n'y a aucune raison pour que, dans une fonction de plusieurs lettres, une lettre occupe un rang plutôt qu'un autre.

Cependant comme on ne peut guère se former l'idée d'une substitution sans ~~se former~~ celle d'une permutation, nous ferons dans le langage un emploi fréquent des permutations, et nous ne considérerons les substitutions que comme le passage d'une permutation à une autre.

Quand nous voudrons grouper des substitutions nous les ferons toutes provenir d'une même permutation.

~~[illegible]~~

Comme il s'agit toujours de questions où la disposition primitive des lettres n'influe en rien, dans les groupes que nous considérerons, on devra avoir les mêmes substitutions quelle que soit la permutation d'où l'on sera parti. Donc si dans un pareil groupe on a les substitutions S et T, on est sûr d'avoir la substitution ST.

Premier mémoire, dossier 1, folio 3 verso

Proposition I relates a given polynomial to a group of permutations (its Galois group)

Eleventh-hour marginal additions provide further explanation

Galois and his groups (4)

The eleventh-hour marginal addition in translation:

> *Substitutions are the passage from one permutation to another.*
>
> *The permutation from which one starts in order to indicate substitutions is completely arbitrary, ...*
>
> *... one must have the same substitutions, whichever permutation it is from which one starts. Therefore, if in such a group one has substitutions S and T, one is sure to have the substitution ST.*

Évariste Galois, 29th May 1832, published 1846

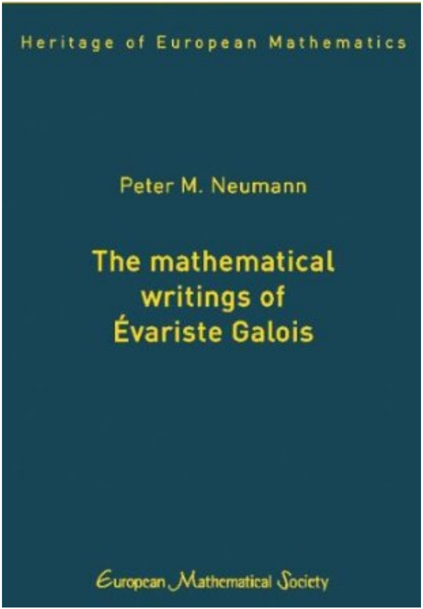
(See *Mathematics emerging*, §13.1.2.)

Galois and his groups: publication

Publication of Galois' results:

1829–30:	5 articles inc. 'Sur la théorie des nombres'
1832:	Testamentary Letter to Chevalier
1846:	letter and all other major papers by Liouville
1897:	Liouville's edition re-published by Picard
1906/07/08:	minor manuscripts published by Tannery
1962:	complete Bourgne & Azra edition
25 Oct 2011:	English/French bilingual edition by Peter Neumann

Galois in English (2011)



Heritage of European Mathematics

Peter M. Neumann

The mathematical writings of Évariste Galois

European Mathematical Society

Cauchy and his ‘groups’ (1)

Meanwhile, in 1845 . . .

Joseph Bertrand proved Cauchy’s conjecture from 1815 (subject to a Postulate) ...

and submitted a paper to the Paris Academy in March 1845;

in April 1845, Cauchy was given Bertrand’s paper for review . . .

and from September 1845 to January 1846 published a stream of papers on the same topic (and introducing a version of groups),

giving his report on Bertrand’s paper in November 1845,

which was eventually published in November 1848

(Peter M. Neumann, ‘On the date of Cauchy’s contributions to the founding of the theory of groups’, *Bull. Austral. Math. Soc.* **40** (1989), 293–302.)

Cauchy and his ‘groups’ (2)

Cauchy’s definition of a ‘group’ (1845):

Consider substitutions $\binom{A}{B}, \binom{C}{D}, \binom{E}{F}, \ldots$ and all those derived from them by multiplying them together one or more times in any order. These form a système de substitutions conjuguées (a system of conjoined substitutions).

His purpose: for any function $f(x_1, x_2, \ldots, x_n)$ the substitutions that leave it unchanged (yielding ‘valeurs égales’) form such a system. The number of values of the function (‘valeurs différentes’) is the index of this system — that is $\frac{n!}{N}$, where N is the number of its members.

Hence — a proof of his 1815 conjecture and more.

The Paris Grand Prix of 1860

Académie des Sciences, Paris, *Grand Prix de Mathématiques*, 1860: subject announced April 1857 (Cauchy on committee, he died a month later):

> *What are the possibilities for the number of values of well defined functions containing a given number of letters, and how can one form the functions for which there exist a given number of values?*

Grand Prix 1860: responses

Three competitors:

- Émile Mathieu;
- Camille Jordan

  (submitted their Paris doctoral dissertations);
- Rev. Thomas Penyngton Kirkman

  (submitted his essay 'The complete theory of groups').

None successful.

All interpreted the problem as 'find all subgroups of Sym(n)'.

The competition stimulated:

- development of theory of (finite permutation) groups;
- merger of Galois' and Cauchy's independent theories.

Meanwhile, in Britain...

A sideline in the development of algebra in the 19th century was the notion of symbolical algebra that emerged in Britain c. 1830

This was a response to an argument advanced by a (persistent) minority of British mathematicians that the notion of a negative number is invalid

It first appeared in print in the 1830 *A Treatise of Algebra* by George Peacock (1791–1858)

Symbolical algebra

In symbolical algebra, symbols are regarded initially as being without interpretation, but may be manipulated according to specified rules; interpretation comes at the end of the process.

This approach was not accepted by all mathematicians in Britain, and sparked a debate about the nature of mathematical truth: can operation really precede interpretation?

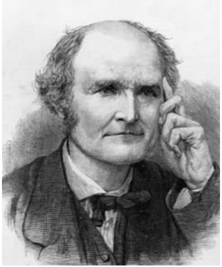
Contributors to symbolical algebra included George Peacock (1791–1858), Duncan Gregory (1813–1844), Augustus De Morgan (1806–1871), George Boole (1815–1864), and William Rowan Hamilton (1805–1865).

But the idea of symbolical algebra had largely faded away by the middle of the century: one *could* work with arbitrary operations in an entirely abstract setting, but why would one want to?

Cayley and his groups (1)

Arthur Cayley, ‘On the theory of groups, as depending on the symbolic equation $\theta^n = 1$’ (1854):

> *A set of symbols*
>
> $$1,\ \alpha,\ \beta,\ \ldots$$
>
> *all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself belongs to the set, is said to be a group.*



Cayley widely attributed with introducing ‘abstract’ theory of groups

(See *Mathematics emerging*, §13.1.4.)

Cayley and his groups (2)

Examples of groups of order 4:

- roots of $x^4 - 1 = 0$
- other examples from elliptic functions, quadratic forms
- matrices $(A, A^{-1}, A^T, (A^T)^{-1})$

Examples of groups of order 6:

- permutations of three letters
- operations from his previous paper ‘properties of a caustic’

Key question for Cayley later: how many groups of order n?

Cayley, ‘On the theory of groups’ (1878):

> *A group is defined by means of the laws of combinations of its symbols.*

Weber's axioms, 1882

A System G of h elements of any kind, Θ_1, Θ_2, $\dots$, Θ_h is called a group of degree h, if it satisfies the following conditions:

I. By some rule, which will be called composition or multiplication, from two elements of the system a new element of the system may be derived. In symbols:

$$\Theta_r \Theta_s = \Theta_t.$$

II. Always:

$$(\Theta_r\Theta_s)\Theta_t = \Theta_r(\Theta_s\Theta_t) = \Theta_r\Theta_s\Theta_t.$$

III. From $\Theta\Theta_r = \Theta\Theta_s$ and from $\Theta_r\Theta = \Theta_s\Theta$ follows $\Theta_r = \Theta_s$.

Existence of identity and inverses appear as deductions from the axioms — incorporated as axioms by later authors

On axiomatisation of groups

Peter M. Neumann, ‘What groups were: a study of the development of the axiomatics of group theory’, *Bull. Austral. Math. Soc.* **60** (1999), 285–301.

Christopher D. Hollings, ‘“Nobody could possibly misunderstand what a group is”: a study in early twentieth-century group axiomatics’, *Arch. Hist. Exact Sci.* **71**(5) (2017), 409–481.

Rings and ideals

Ernst Kummer (1844):

- concerned with Fermat's last theorem, and quadratic forms
- worked with arithmetic of 'cyclotomic integers' $a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1}$ where θ is primitive n-th root of 1
- discovered that unique factorisation need not hold
- devised the concept of 'ideal' factors

Richard Dedekind, 'Sur la théorie des nombres entiers algébriques' (1877) and famous appendices to his editions of Dirichlet's *Lectures on Number Theory*:

- changed Kummer's 'ideal numbers' to 'ideals'
- worked also with rings of numbers [domains] and fields of numbers [Körper]

‘Abstract algebra’ begins to form

Specific instances of fields studied by Galois, Kronecker, Dedekind, and others. First axiomatic definition due to Weber, 1893.

Ernst Steinitz, ‘Algebraische Theorie der Körper’, 1910: first comprehensive presentation of the theories of fields, modules, and vector spaces [to be revisited in a later lecture]

Specific rings studied by Dedekind, Hilbert, ... Early axiomatic definition given by Fraenkel in 1914: not quite the same as the modern definition.

Abstract algebra given an early boost (in the USA) via a short-lived obsession with ‘postulate analysis’: the study of systems of axioms for their own sake

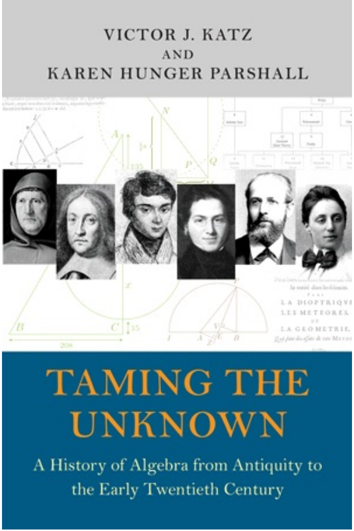
‘Abstract algebra’ takes off

Comprehensive abstract study of (commutative) rings initiated by Emmy Noether in the 1920s, sometimes mirroring the earlier ‘concrete’ work of Dedekind: ‘Es steht alles schon bei Dedekind’.

Noether’s lectures (in Göttingen) united with those of Emil Artin (Hamburg) in B. L. van der Waerden’s highly influential textbook *Moderne Algebra* (1930).

Abstract point of view now dominant, with many different objects studied: groups, fields, rings, integral domains, semigroups, algebras, lattices, semirings, quasigroups, ...

Overviews of the topics of lectures IX and X

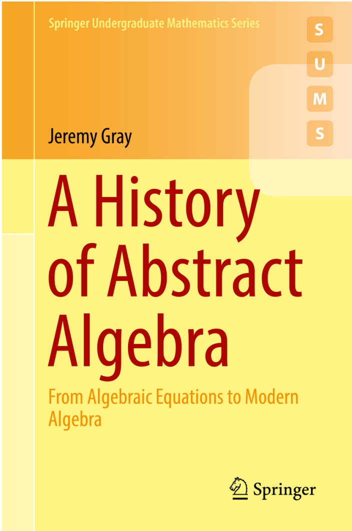


VICTOR J. KATZ
AND
KAREN HUNGER PARSHALL

TAMING THE UNKNOWN

A History of Algebra from Antiquity to the Early Twentieth Century

(Princeton Univ. Press, 2014)



Springer Undergraduate Mathematics Series

S U M S

Jeremy Gray

A History of Abstract Algebra

From Algebraic Equations to Modern Algebra

Springer

(Springer, 2018)