BO1 History of Mathematics
Lecture X
The 19th-century beginnings of ‘modern algebra’
Part 1: Resolvents and permutations

MT 2020 Week 5

Summary

Part 1

- Lagrange's ideas (1770/71)
- Cauchy and substitutions (1815)
- 'Classical age' of theory of equations 'ends' (1799–1826)

Part 2

- The invention of groups by Galois and Cauchy

Part 3

- 'Symbolical algebra'
- Groups, rings, and fields: the emergence of 'modern algebra' (1854–1900)

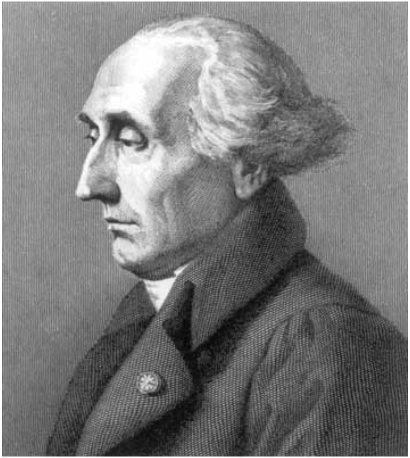
‘Modern’ or ‘abstract’ algebra

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):



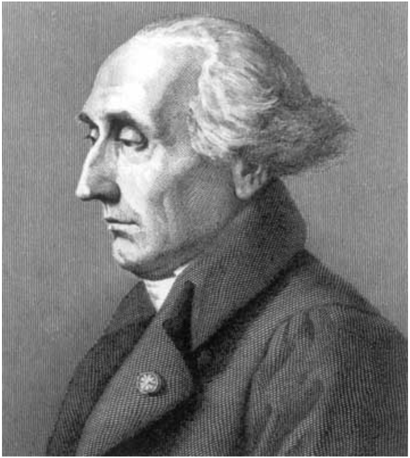
Lagrange's 'Réflexions' 1770/71

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

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

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

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

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

$$y = \frac{1}{2}(x_1x_2 + x_3x_4)$$

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

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

$$y = \frac{1}{2}(x_1x_2 + x_3x_4)$$

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

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

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 $x_1, x_2, x_3, \cdots, x_n$

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

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 $n!$

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

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.

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.

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.

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:

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

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

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

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, ...

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:

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

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 $p \leq n$.

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 $N \geq n$.

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

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:

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

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 proved conclusively that the general equation of degree 5 is not soluble by radicals.

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 proved 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.

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 proved 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’ (?)