

# Nepal Algebra Project (NAP) 2019

## Lecture 8

### **Historical introduction to Galois Theory**

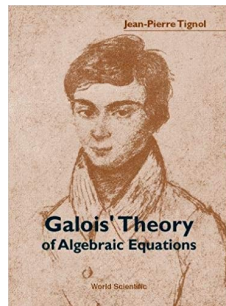
*Michel Waldschmidt*

Professeur Émérite, Sorbonne Université,

Institut de Mathématiques de Jussieu, Paris

<http://www.imj-prg.fr/~michel.waldschmidt/>

# Galois theory of algebraic equations



Jean-Pierre Tignol

[https://perso.uclouvain.be/jean-pierre.tignol/Page\\_personnelle\\_de\\_Jean-Pierre\\_Tignol.html](https://perso.uclouvain.be/jean-pierre.tignol/Page_personnelle_de_Jean-Pierre_Tignol.html)

# Quadratic equations



Simon Stevin

1548–1620



François Viète

1540–1603

<http://www-history.mcs.st-and.ac.uk/Biographies/Stevin.html>

<http://www-history.mcs.st-and.ac.uk/Biographies/Viete.html>

$$x^2 - x = b$$



Plimpton 322

1800BC

Emmanuel Peyre. Les Points Rationnels. Gazette SMF N° 159, janvier 2019, 13–22.

<https://smf.emath.fr/publications/la-gazette-des-mathematiciens-159-janvier-2019>



$$x^2 + ax = b, x^2 + b = ax, x^2 = ax + b$$

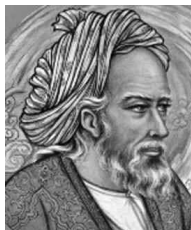


Abu Ja'far Muhammad ibn Musa Al-Khwarizmi  
780–850

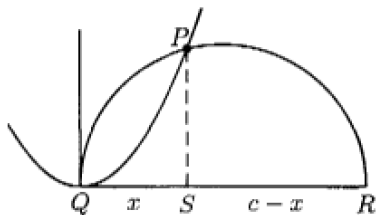
Hisab al-jabr w'al-muqabala

<http://www-history.mcs.st-and.ac.uk/Biographies/Al-Khwarizmi.htm>

# Geometric solutions to cubic equations



Omar Khayyam  
1048–1131



$$x^3 + b^2x = b^2c$$

$x^2 = by$ , the triangles  $QSP$  and  $PSR$  are similar,

$$\frac{x}{PS} = \frac{PS}{c-x}, \quad \frac{b}{x} = \frac{x}{y} = \frac{y}{c-x} = \frac{x^2}{b(c-x)}.$$

<http://www-history.mcs.st-and.ac.uk/Biographies/Khayyam.html>

# Leonardo da Pisa (Fibonacci)



Fibonacci

1170–1250

Liber Abaci (1202), Flos (1225)

In Flos, Fibonacci proves that the root of the equation  $10x + 2x^2 + x^3 = 20$  (from Omar Khayyam's algebra book) is neither an integer nor a fraction, nor the square root of a fraction and gives the approximation 1.368 808 107 5, which is correct to nine decimal places.

<http://www-history.mcs.st-and.ac.uk/Biographies/Fibonacci.html>



“The solutions of  $x^3 + mx = n$  and  $x^3 + n = mx$   
are as impossible as the quadrature of the circle”



Luca Pacioli

1445–1517

<http://www-history.mcs.st-and.ac.uk/Biographies/Pacioli.html>

$x^3 + mx = n$  – unpublished



Scipione del Ferro

1465–1526

<http://www-history.mcs.st-and.ac.uk/Biographies/Ferro.html>

# Nicolo Fontana alias Tartaglia



Nicolo Tartaglia

1500–1557

<http://www-history.mcs.st-and.ac.uk/Biographies/Tartaglia.html>

$$x^3 + mx = n$$



Girolamo Cardano

1501–1576

$$x^3 + mx = n, t - u = n, tu = (m/3)^3, x = \sqrt[3]{t} - \sqrt[3]{u}.$$

$x^3 = 15x + 4 : x = 4$ . Introduction complex numbers.

$x^2 + 2x = 48 : 1 \text{ quad } p : 2 \text{ pos aeq } 48$

<http://www-history.mcs.st-and.ac.uk/Biographies/Cardan.html>

# Algebra



Rafael Bombelli  
1526–1572

<http://www-history.mcs.st-and.ac.uk/Biographies/Bombelli.html>

# Solution of quartic equations



Lodovico Ferrari

1522–1565

Published by Cardano : “Ars Magna”.  
Resolvent cubic equation.

<http://www-history.mcs.st-and.ac.uk/Biographies/Ferrari.html>

# Negative numbers



Simon Stevin

1548–1620

<http://www-history.mcs.st-and.ac.uk/Biographies/Stevin.html>

# Letters for unknown quantities (positive numbers)



François Viète

1540–1603

<http://www-history.mcs.st-and.ac.uk/Biographies/Viete.html>



# La Géométrie, 1637



René Descartes

1596–1650

1567 :  $X - a$  divides  $P(X)$  if and only if  $P(a) = 0$ .

$$X^4 + pX^2 + qX + r = (X^2 + aX + b)(X^2 + cX + d)$$

$$a^6 + 2pa^4 + (p^2 - 4r)a^2 - q^2 = 0$$

<http://www-history.mcs.st-and.ac.uk/Biographies/Descartes.html>

# 1629 : invention nouvelle en algèbre



Albert Girard

1595–1632

The number of roots is the degree (including impossible solutions).

Relation between roots and coefficients.

[http://www-history.mcs.st-and.ac.uk/Biographies/Girard\\_Albert.html](http://www-history.mcs.st-and.ac.uk/Biographies/Girard_Albert.html)



Sir Isaac Newton

1643–1727

$$\sum \alpha_i^k.$$

Numerical methods.

<http://www-history.mcs.st-and.ac.uk/Biographies/Newton.html>

# Tschirnhaus



Ehrenfried Walter von Tschirnhaus

1651–1708

$$X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$$
$$Y = X^m + b_{m-1}X^{m-1} + \dots + b_1X + b_0$$

<http://www-history.mcs.st-and.ac.uk/Biographies/Tschirnhaus.html>

# How to solve Tschirnhaus system ?



Gottfried Wilhelm von Leibniz  
1646–1716

<http://www-history.mcs.st-and.ac.uk/Biographies/Leibniz.html>

# Réflexions sur la résolution algébrique des équations : 1772



Joseph-Louis Lagrange

1736–1813

Permutations of the roots. Number of permutations leaving invariant the polynomial. Lagrange theorem on the order of a subgroup. Lagrange resolvent.

<http://www-history.mcs.st-and.ac.uk/Biographies/Lagrange.html>

# The fundamental theorem of algebra



Albert Girard

1595–1632

1629 : invention nouvelle en algèbre

[http://www-history.mcs.st-and.ac.uk/Biographies/Girard\\_Albert.html](http://www-history.mcs.st-and.ac.uk/Biographies/Girard_Albert.html)

# The fundamental theorem of algebra : 1746



Jean Le Rond d'Alembert  
1717–1813

Analytic proof

<http://www-history.mcs.st-and.ac.uk/Biographies/DAlembert.html>



# The fundamental theorem of algebra : 1749



Leonhard Euler

1707–1783

Any irreducible polynomial over  $\mathbb{R}$  has degree 1 or 2.

<http://www-history.mcs.st-and.ac.uk/Biographies/Euler.html>

# Réflexions sur la résolution algébrique des équations : 1772



Joseph-Louis Lagrange  
1736–1813

Assumes there are  $d$  “imaginary” roots to a polynomial of degree  $d$ , proves that they are in  $\mathbb{C}$ .

<http://www-history.mcs.st-and.ac.uk/Biographies/Lagrange.html>

# The fundamental theorem of algebra : 1799, 1815



Johann Carl Friedrich Gauss

1777-1855

Corrects the proofs of d'Alembert and Lagrange, later produces two other proofs.

<http://www-history.mcs.st-and.ac.uk/Biographies/Gauss.html>

# Mémoire sur la résolution des équations 1774



Alexandre-Théophile Vandermonde  
1735–1796



Abbé Henri Grégoire  
1750–1831

Determinant

Cyclotomic polynomials

<http://www-history.mcs.st-and.ac.uk/Biographies/Vandermonde.html>

[https://fr.wikipedia.org/wiki/Henri\\_Gregoire](https://fr.wikipedia.org/wiki/Henri_Gregoire)

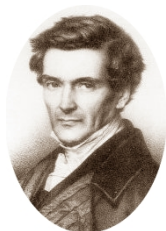
# Cyclotomic polynomials 1799



Johann Carl Friedrich Gauss  
1777-1855

<http://www-history.mcs.st-and.ac.uk/Biographies/Gauss.html>

1837



Pierre Laurent Wantzel

1814–1848

<http://www-history.mcs.st-and.ac.uk/Biographies/Wantzel.html>

# Fermat primes



Pierre de Fermat

1601?–1665

$$F_n = 2^{2^n} + 1 :$$

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65\,537$$

$$F_5 = 2^{32} + 1 \equiv 0 \pmod{641}.$$

<http://www-history.mcs.st-and.ac.uk/Biographies/Fermat.html>

# 1799 : general equation of degree 5



Paolo Ruffini

1765–1822

516 pages - non solvability of the general equation of degree 5.  
Gauss : “It appears more and more likely that this resolution is impossible”.

<http://www-history.mcs.st-and.ac.uk/Biographies/Ruffini.html>



# 1824 : non solvability of equations of degree 5



Niels Henrik Abel  
1802–1829

<http://www-history.mcs.st-and.ac.uk/Biographies/Abel.html>



Évariste Galois  
1811–1832

Necessary and sufficient condition for an equation to be solvable by radicals.

<http://www-history.mcs.st-and.ac.uk/Biographies/Galois.html>

# Referee of Galois's note



Jean Baptiste Joseph Fourier

1768–1830

<http://www-history.mcs.st-and.ac.uk/Biographies/Fourier.html>

## 1846 : publication of Galois's work



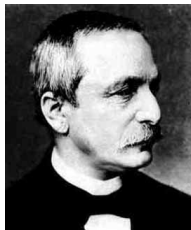
Joseph Liouville

1809–1882

Permutations which preserves the relations among the roots.  
Behavior under the extension of the base field.

<http://www-history.mcs.st-and.ac.uk/Biographies/Liouville.html>

# Field theory : constructivist



Leopold Kronecker

1823–1891

<http://www-history.mcs.st-and.ac.uk/Biographies/Kronecker.html>

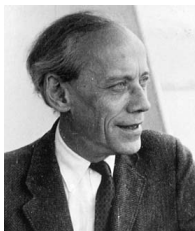
# Field theory : axiomatic



Julius Wilhelm Richard Dedekind  
1831–1916

<http://www-history.mcs.st-and.ac.uk/Biographies/Dedekind.html>

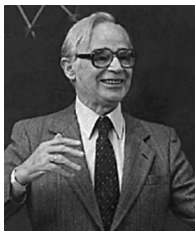
# Galois correspondence - published 1942



Emil Artin  
1898–1962

<http://www-history.mcs.st-and.ac.uk/Biographies/Artin.html>

# Moderne Algebra 1930



Bartel Leendert van der Waerden  
1903–1996

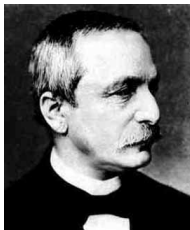
[http://www-history.mcs.st-and.ac.uk/Biographies/Van\\_der\\_Waerden.html](http://www-history.mcs.st-and.ac.uk/Biographies/Van_der_Waerden.html)



## Cyclotomic fields. Abelian extensions of $\mathbb{Q}$

Let  $\mu_n$  be the cyclic group of  $n$ -th roots of unity in  $\mathbb{C}$ . The cyclotomic field  $\mathbb{Q}(\mu_n)$  is a Galois extension of  $\mathbb{Q}$  with Galois group  $(\mathbb{Z}/n\mathbb{Z})^\times$ .

**Kronecker–Weber Theorem.** *Every finite abelian extension of  $\mathbb{Q}$  is contained in some cyclotomic field.*



Leopold Kronecker

1823–1891



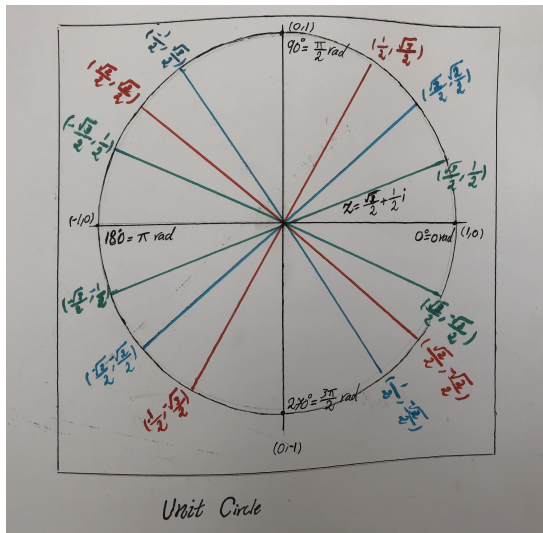
Heinrich Weber

1842–1913

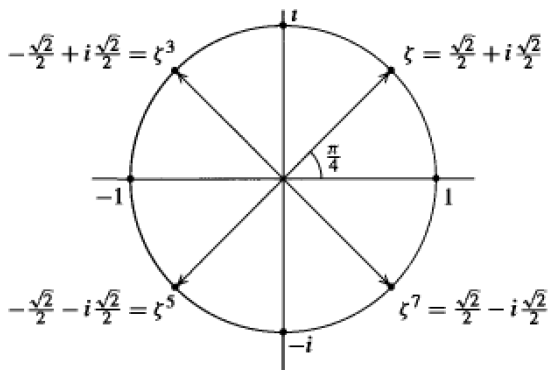
<http://www-history.mcs.st-and.ac.uk/Biographies/Kronecker.html>

[http://www-history.mcs.st-and.ac.uk/Biographies/Weber\\_Heinrich.html](http://www-history.mcs.st-and.ac.uk/Biographies/Weber_Heinrich.html)

Sixteenth roots of unity :  $\Phi_{16}(X) = X^8 + 1$ ,  
 $\zeta^{16} = 1$



Eighth roots of unity :  $\Phi_8(X) = X^4 + 1, \zeta^8 = 1$

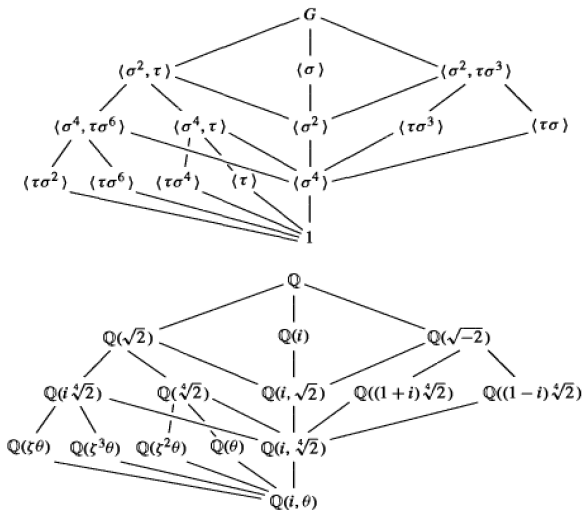


$$[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = \varphi(8) = 4, G(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = (\mathbb{Z}/8\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

David S. Dummit & Richard M. Foote, Abstract Algebra, Prentice Hall, 1991  
2nd Ed. 1999.

# Splitting field of $X^8 - 2$ and subfields

$$\theta = \sqrt[8]{2}$$



David S. Dummit & Richard M. Foote, Abstract Algebra, Prentice Hall, 1991  
2nd Ed. 1999.

# Galois theory of finite fields

If  $F$  is a finite extension of  $\mathbb{F}_q$ , then  $F/\mathbb{F}_q$  is a Galois extension and  $G(F/\mathbb{F}_q)$  is a cyclic group generated by the Frobenius  $\text{Frob}_q : x \rightarrow x^q$ .



Ferdinand Georg Frobenius  
1849–1917

<http://www-history.mcs.st-and.ac.uk/Biographies/Frobenius.html>

# Solvability of algebraic equations by radicals

Extension solvable by radicals.

In characteristic  $\neq 2$  and  $\neq 3$ , an extension of degree  $\leq 4$  is solvable by radicals.

Existence of extensions of degree  $p$  with Galois group  $\mathfrak{S}_p$ .

Example :  $X^5 + 2X^3 - 24X - 2$

# Geometric constructions with ruler and compasses

Stable subsets of  $\mathbb{R} \times \mathbb{R}$ . Stable closure  $S(E)$  of a subset  $E$  of  $\mathbb{R} \times \mathbb{R}$ . Stable closure  $S(k)$  of a subfield  $k$  of  $\mathbb{R}$ .

Let  $k$  be a subfield of  $\mathbb{R}$ .

An element  $x \in \mathbb{R}$  is in  $C(k)$  if and only if there exists a Galois extension  $K/k$  such that  $[K : k] = 2^m$  and  $x \in K$ .

- Trisection of an angle
- Squaring the circle
- Doubling the cube
- Construction of regular polygons

# References

- Jean-Pierre Tignol. Galois' theory of algebraic equations. 2nd ed. World Scientific Publishing Co. Pte. Ltd., Singapore, 2016.
- David S. Dummit & Richard M. Foote. Abstract Algebra, Prentice Hall, 1991. 2nd Ed. 1999.
- Serge Lang. Algebra. 3rd Ed. Graduate texts in mathematics **211**, 2002.  
<https://math24.files.wordpress.com/2013/02/algebra-serge-lang.pdf>
- James S. Milne, Fields and Galois Theory Version 4.52 March 17, 2017. Available at [www.jmilne.org/math/](http://www.jmilne.org/math/)
- D.J.H. Garling. A course in Galois Theory. Cambridge University Press, 1986.
- Evariste Galois. Numéro spécial de la revue d'histoire des mathématiques, SMF, 2011. <https://smf.emath.fr/node/27710>



# Nepal Algebra Project (NAP) 2019

## Lecture 8

### **Historical introduction to Galois Theory**

*Michel Waldschmidt*

Professeur Émérite, Sorbonne Université,

Institut de Mathématiques de Jussieu, Paris

<http://www.imj-prg.fr/~michel.waldschmidt/>