Galois Theory.

I. Introduction.

The problem at the root of Galois theory present since antiquity in special cases can be formulated as follows:

given an equation

$$x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

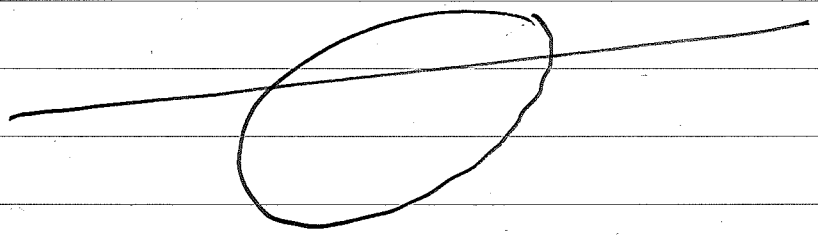
find a "formula" for its solutions in terms of the coefficients

$$a_{n-1}, \ldots, a_0.$$

Methods for solving the linear and quadratic equations, in special cases, were already found by Babylonian

mathematicians around 1700 BC.

Euklid (~ 300 BC) treated the problem using his geometry : that is, interpreting specific equations as giving solutions to a geometric problem like:



The first to present a systematic treatment on the resolution of linear and quadratic equations is the persian scholar al-Hwarizmi (780 - 850) in Baghdad in a book written in arabic that was translated into latin in the 12th century and served as standard textbook in european universities ~~in the middle age~~ until the 16th century. He is considered the

founder of algebra as an independent discipline; the name comes from "al-ğabr", which means "to fill, to complete", and appears in the title of his book.

The next big step was achieved by italian mathematicians of the late renaissance who found the solution of the equations of degree 3 (Scipione del Ferro 1515) and degree 4 (Ludovico Ferrari). These methods were exposed in the influential book by Girolamo Cardano (1501-1576) called "Ars Magna" 1545.

Let's shortly review his method since it turned out to be historically important.

Let $x^3 + ax^2 + bx + c = 0$

substitute: $z = x - \frac{a}{3}$

to get for z an equation of the form:

$$z^3 + pz + q = 0 .$$

Now set $z = y + u$.

Then $y^3 + \underbrace{3y^2u + 3yu^2}_{3yu(y+u)} + u^3 + p(y+u) + q = 0$

$$y^3 + (y+u)[3yu + p] + u^3 + q = 0 .$$

Now set $3yu + p = 0$, that is

$$u = -\frac{p}{3y}$$

to obtain the equation

$$y^3 - \left(\frac{p}{3}\right)^3 \frac{1}{y^3} + q = 0$$

or $$\boxed{y^6 + qy^3 - \left(\frac{p}{3}\right)^3 = 0 .}$$

This is now a quadratic equation in y^3

hence $$y^3 = -\left(\frac{q}{2}\right) + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

$$\begin{cases} u = -\dfrac{p}{3y} \end{cases}$$

We finally get the famous Cardano formula:

$$z = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$

This is the treatment in modern ~~langu~~ symbolism that was only introduced later by François Viète (1540-1603). In "Ars Magna" all these operations are described in words!

In terms of solving equations of higher degree nothing happened till the 19th

century. A very important step was made by Joseph Louis Lagrange (1736-1813) who observed the following:

if z_1, z_2, z_3 are the solutions of

$$z^3 + pz + q = 0$$

and $w = e^{2\pi i/3}$ (primitive) third root of 1, then the 6 solutions to the resolvent:

$$y^6 + qy^3 - \left(\frac{p}{3}\right)^3 = 0$$

are given by:

$$y_\sigma = \frac{1}{3}\left(z_{\sigma(1)} + w z_{\sigma(2)} + w^2 z_{\sigma(3)}\right)$$

where σ runs through all permutations of ~~6 elements~~ 3 elements, of which there are 6. His fundamental observation was

that $\left(z_{\sigma(1)} + \omega\, z_{\sigma(2)} + \omega^2 z_{\sigma(3)} \right)^3$

only takes 2 distinct values when σ runs through all 6 permutations.

The next step was taken by Paolo Ruffini, Medical Doctor and professor for mathematics in Modena. He focused on rational functions

$$f(z_1, z_2, \ldots, z_5)$$

in the roots of a general equation

$$z^5 + \ldots\ldots + a_0 = 0$$

and realized that the set of permutations $\sigma \in S_5$ leaving such an expression invariant is a <u>subgroup</u> of S_5.

In works began in 1799 he described all subgroups of S_5 and reduced, with a gap, that the general quintic equation ~~has no solutions~~ is not solvable by radicals. In fact the proof had a gap and it is Niels Henrik Abels (1802-1829) who published in 1824

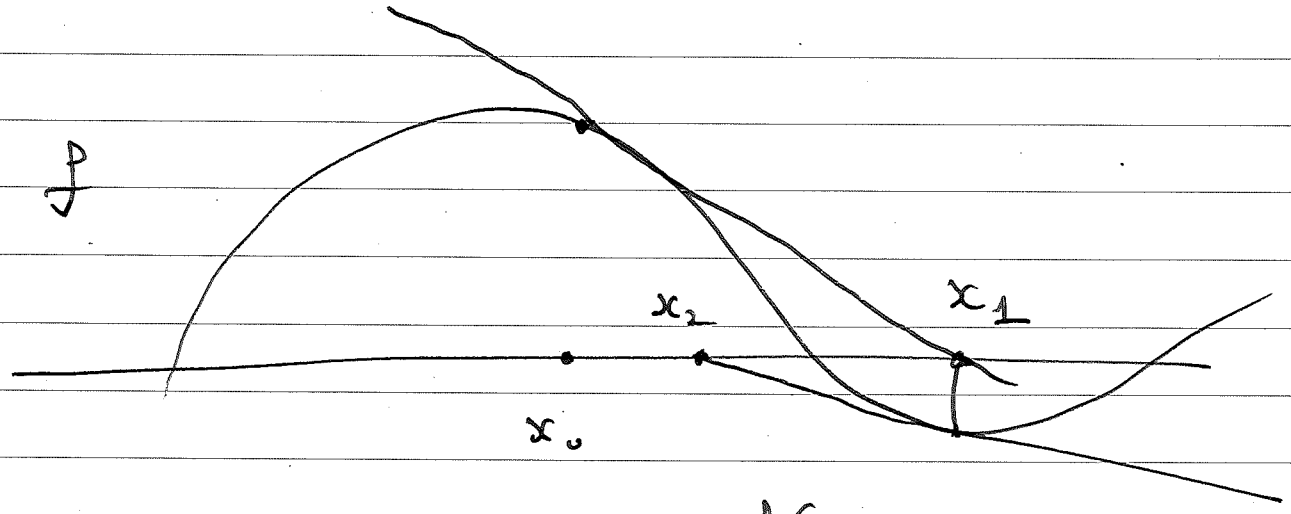
Thm. (Abel-Ruffini) The general quintic equation

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$$

is not solvable by radicals.

A solution by radicals is a formula only involving a finite number of field operations and extractions of roots.

Indeed there are methods to find real roots of any polynomial, for instance Newton's method.



Recursively $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$.

and $\lim x_n$ gives a root.

In fact, the theorem of Abel–Ruffini will be our first major goal and it will be a consequence of the following fact from Algebra I

Thm. A_5 is simple non-abelian.

More precisely the theorem of Abel-Ruffini will be a byproduct of the systematic development of Galois theory. Loosely speaking, we will for every polynomial $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k[x]$ where k is a field with good properties attach a finite group $\mathrm{Gal}(f) < S_n$ and show

Thm. (Galois) f is solvable by radicals if and only if $\mathrm{Gal}(f)$ is a solvable group.

Solvability for a finite group is a group theoretic property that is in a sense opposite to being simple. It means that

the group can be "decomposed" into finite cyclic groups in a precise way.