

APPENDIX A

THE LIFE OF GALOIS

Évariste Galois was born on 25th October 1811 near Paris. Until he was 12 he studied the classics at home with his mother. Then in 1823 he entered the Lycée Louis-le-Grand where at first he did well. But later he became bored and his work deteriorated. His interest in mathematics was awakened by Legendre's *Éléments de Géométrie* and by the time he was 15 his grasp of mathematics was so deep that he could read and understand the recent developments. However he continued to do poorly at school. He twice sat and failed the entrance examination at the École Polytechnique where the best mathematical brains of the country were trained.

At the age of 18 he submitted some excellent original work for the grand Prize in Mathematics of the academy of sciences. Fourier, the secretary of the Academy took the manuscript home to study it but he died before he had a chance to read it. The manuscript was not found among Fourier's papers and so Galois missed out on the prize. This was the second time some of his work had gone astray. The previous year he had submitted some work on the zeros of polynomial equations to the Academy of Sciences. Cauchy, who had published in this area himself, was appointed to consider this and another memoir that Galois submitted at about the same time. He rejected both of them and the manuscripts were subsequently lost. Galois felt that more than carelessness lay behind the loss of his manuscripts.

By this time he was studying at the École Normale. In July 1830, Charles X issued an ordinance which suppressed the freedom of the Press. during the student demonstrations that followed, the students of the École Normale, Galois among them, were locked in by the director of the institution. Galois attacked him later in a letter to the *Gazette des Écoles*. Although he signed the letter, it was published without his name. However he was found out and was expelled for having written this "anonymous letter".

Now 19 he tried, not very successfully, to earn a living as a private tutor in mathematics. He sent another memoir, *On the conditions of solubility of equations by radicals* to the academy of Sciences. The referees this time were Poisson and Lacroix. He heard nothing for two months and when he wrote enquiring about it he had no reply. Then almost six months later, he received the news that it had been rejected. Poisson wrote that it was not sufficiently developed and the reasoning was not sufficiently clear for him to judge its correctness and, referring to the fact that Galois claimed that his material was part of a more general theory, suggested that Galois publish the whole of his work as this might make it easier to understand. Galois had always been untidy and unsystematic and doing most of his mathematics in his head he found it difficult to set it down clearly on paper.

During this time, Galois joined the Republican National Guard but the organization was banned by Louis-Philippe who had succeeded Charles after the previous year's uprising. On 9th May 1831, a banquet was held in protest and during the rowdy proceedings, Galois stood up and proposed a toast to Louis-Philippe — clutching an unsheathed knife. This was taken to be a threat on the king's life and he was cheered by his Republican comrades. They poured out into the street shouting

and dancing. The next day, Galois was arrested. He admitted at his trial to having made the toast but claimed that what he had said was “To Louis-Philippe — if he turns traitor” but that because of the cheering the last phrase had not been heard. He was acquitted and freed on 15th June.

He was not to remain free for long, however, for a month later he was arrested as he led a Republican demonstration and was sentenced to six months jail. He used this time to continue his work on his mathematics. When he was freed he met and fell in love with a girl called Stephanie. Her surname appears in one of his letters but is heavily crossed out. It appears that she later rejected him, which hurt him deeply. This did not, however, prevent him from being challenged to a duel over his relationship with her. Alexandre Dumas claimed that the challenger was a political opponent, which suggests that there were political rather than private motives behind the challenge. However Galois indicated that the dispute was of a private nature as he wrote “I beg patriots and my friends not to reproach me for dying otherwise than for my country. I die the victim of an infamous coquette ... Oh! why die for so trivial a thing, for something so despicable!”

On 29th May, the day before the duel was to take place, he wrote a letter to Auguste Chevalier in which he outlined, among other things, his discoveries about the connection between groups and polynomial equations and stated that an equation is soluble by radicals when, and only when, its group is soluble. Towards the end of this pathetic document the writing became almost a scribble and was incomprehensible. He seemed conscious of the fact that time was running out and in the margin he scrawled “I have no time”. The letter ended “I hope some people will find it to their advantage to decipher all this mess”.

The duel took place the next day — pistols at 25 paces. Galois was hit in the stomach and died the following day, 31st May 1832, of an infection of the stomach lining. The world had been robbed of a great mathematician five months before he would have turned 21.

APPENDIX B

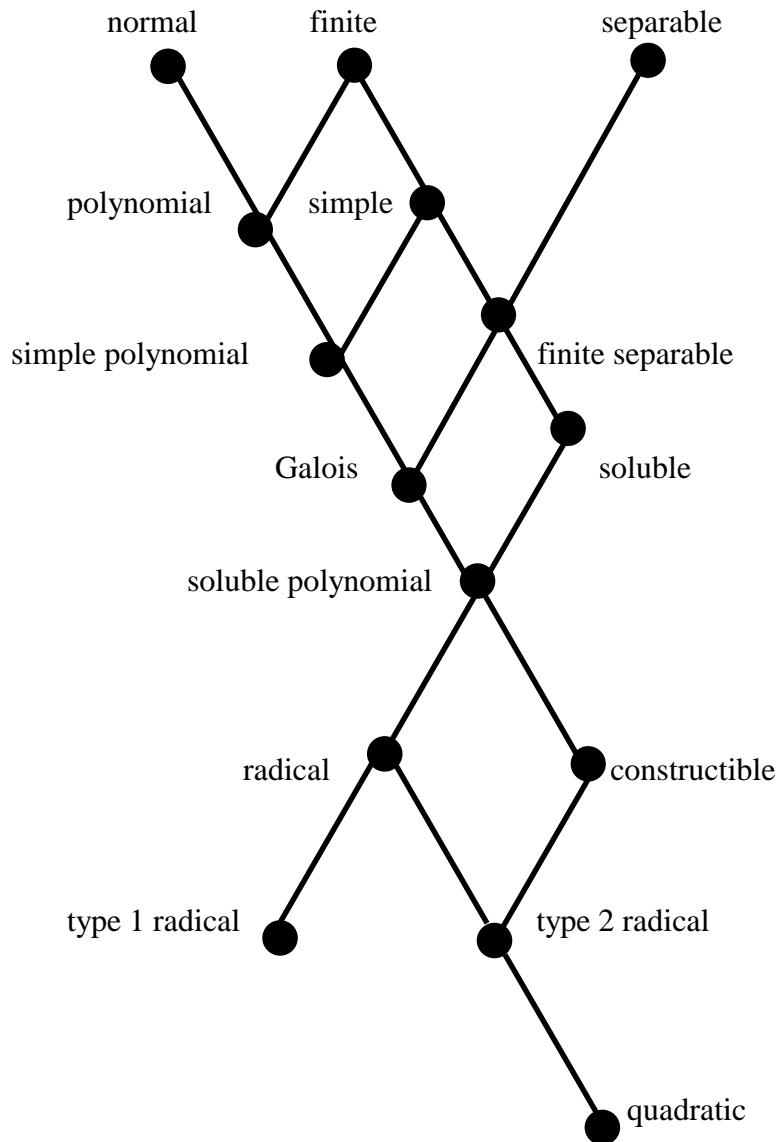
AN OVERVIEW OF GALOIS THEORY

A field extension, $[F \leq K]$ is a pair of fields. They are classified as follows:

TYPES OF FIELD EXTENSIONS

Type of extension	Definition
algebraic	every element of K is a zero of some non-zero polynomial over F
separable	every element of K is a zero of some prime polynomial over F with no repeated zeros
normal	every prime polynomial over f either has no zeros in K or splits completely in H
finite	K is finite-dimensional over F
simple	$K = F[\alpha]$ for some $\alpha \in K$
polynomial	$K = F[f(x) = 0]$ for some $f(x) \in F[x]$
radical	$K = F[x^n = \alpha]$ for some $n > 0$ and $\alpha \in F$
type 1 radical	$K = F[x^n = 1]$ for some $n > 0$
type 2 radical	$K = F[x^n = \alpha]$ for some $n > 0$ and $\alpha \in F$ where F contains all the n 'th roots of unity
quadratic	$K = F[f(x) = 0]$ for some quadratic polynomial $f(x) \in F[x]$
soluble	there is a sequence of radical extensions which reaches K from F
constructible	there is a sequence of quadratic extensions which reaches K from F
Galois	a separable polynomial extension

ALGEBRAIC EXTENSIONS OF A FIELD



For many fields, including subfields of \mathbb{C} , algebraic extensions are automatically separable. This is why we did not need the concept of separability before.

A field is said to be perfect if either it has characteristic zero or it has characteristic p and every element has a p 'th root. One can easily show that all finite fields are perfect. For a perfect field finite extensions are simple and polynomial extensions are Galois.

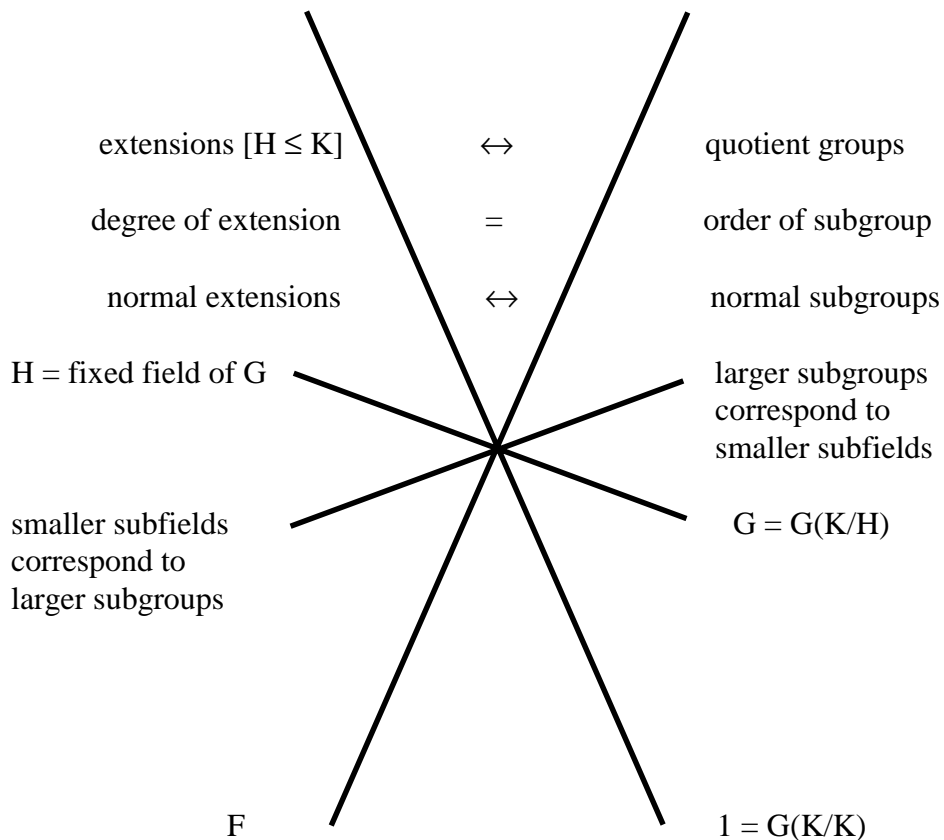
The Fundamental Theorem of Galois Theory

If K is a Galois extension of F (eg a polynomial extension of number fields) there is a 1-1, order reversing correspondence (called the Galois correspondence) between the subfields of K which contain F and the subgroups of $G(K/F)$ as illustrated by the following diagram.

GALOIS CORRESPONDANCE FOR A GALOIS EXTENSION

$K =$ Galois extension of F

$G(K/F) =$ Galois group



Galois Group of a Polynomial Extension

Let F be a field of characteristic zero and suppose that $f(x) \in F[x]$ splits in some extension of F . Then $f(x)$ is soluble by radicals over F if and only if $G(F[f(x) = 0]/F)$ is a soluble group. For all $n \geq 5$ there is a prime polynomial whose Galois group is isomorphic to S_n and which is therefore not soluble by radicals.

Every finite soluble group is the Galois group of some polynomial extension of \mathbf{Q} . Every finite group is the Galois group of some finite extension of \mathbf{Q} , but it is not known whether it must be the Galois group of some polynomial extension of \mathbf{Q} .

Galois Groups of Finite Fields

If F, K are finite fields of order p^m, p^n respectively $G(H/F)$ is a cyclic group of order $m - n$ generated by the Frobenius automorphism $x \rightarrow x^p$.

Galois Group of $\mathbf{Q}[x^n = 1]$

The minimum polynomial of $\omega = e^{2\pi i/n}$ over \mathbf{Q} is $\prod_{\substack{r=1 \\ (r,n)=1}}^{n-1} (x - \omega)^r$. It is called the n 'th

cyclotomic polynomial and has degree $\phi(n)$ = number of integers r such that:

$1 \leq r \leq n - 1$ and $\text{GCD}(r, n) = 1$.

$G(\mathbf{Q}[x^n = 1]/\mathbf{Q}) \cong \mathbf{Z}_n^\#$, the group of units of the ring \mathbf{Z}_n .

Ruler and Compass Constructibility

A complex number α is constructible by ruler and compass if and only if $|\mathbf{Q}[\alpha]:\mathbf{Q}|$ is a power of 2. Since the minimum polynomial of $\cos(\pi/9)$ has degree 3, a 60° angle cannot be trisected by ruler and compass. This also shows that a regular polygon with 18 sides is not constructible. In general, a regular n -sided polygon is constructible if and only if $\phi(n)$ is a power of 2. Gauss showed that this is the case if and only if n is a power of 2 times a product of one or more distinct Fermat primes (primes of the form $2^{2^m} + 1$). There are only 5 known Fermat primes: 3, 5, 17, 257 and 65,537. The next, if indeed there are any more, will have to exceed 10^{40000} .