1. OVERVIEW

§1.1. Galois and Third Generation Mathematics

In the long history of mathematics there have been just three defining moments – when the subject underwent a profound change.

The first of these was the invention/discovery of Euclidean geometry. Previously mathematics was an experimental endeavour. Euclid, and his school, introduced the idea of proof. The second defining moment was when Newton in England, and independently Leibnitz in Germany, invented calculus.

Now most people have heard of Euclid and Isaac Newton but Évariste Galois is known to very few, which is surprising because not only was he responsible for the third defining moment (in the first half of the nineteenth century) but also because his life was much more dramatic than either of the others.

There are two branches of mathematics that owe their existence to Galois – Group Theory and Galois

Theory. But more importantly the conceptual framework that eventually proved so valuable in Group Theory became the model for most other branches of mathematics. This is the model which starts with a set of axioms and then develops the theory from there.

Of course axioms formed the basis of Euclidean geometry, but they were designed to describe just a single mathematical object – the Euclidean plane. In group theory, as in many other branches of mathematics that have followed this framework, the axioms describe a multitude of specific examples. Modern abstract mathematics owes its outlook to group theory which in turn owes its existence to Évariste Galois.

All mathematics is abstract in some way. Even counting is an abstract process. But after Galois the power of abstraction, as it moved away from the real world, began to develop strongly. An interesting thing about mathematics is that the more it moves away from the real world the more useful it becomes in understanding that real world.

Newton was more an astronomer than a mathematician and his motivation for inventing calculus was to devise a system for making calculations about the solar system. He was what you might call an applied mathematician.

Euclid was more of a pure mathematician in so far as his focus was more on the proofs than on the results. But the study of geometry itself was motivated by measurement of the earth's surface, as the word 'geometry' suggests.

By contrast, Galois Theory arose out of an esoteric problem – finding a formula for the solutions of a polynomial equation. There was no practical significance in having such a formula because calculus gives methods for solving any equation to any desired degree of accuracy. A formula gives *exact* solutions but no practical application requires that.

This is not the only thing that makes Galois' work stand out from that of Euclid and Newton, and this may account for the fact that he is much less well known than the others. Both Euclidean geometry and calculus are accessible with very little background required. True, one needs a certain amount of mathematical sophistication but given that, there isn't much required in the way of prerequisite knowledge. Also one can do just a little bit of geometry or a little bit of calculus to get the idea of what they are all about.

Galois Theory, on the other hand, requires a considerable amount of knowledge before one can even begin, which is why it is taught in the final year of a university mathematics degree. Galois Theory needs a

knowledge of polynomials and complex numbers, which Galois had, as well as a solid grounding in permutations and group theory, which Galois had to invent.

To appreciate the remarkable achievement of Galois, one has to imagine if Eiffel had built his famous tower in the middle ages. He would have had to invent the techniques of structural engineering and steel making before he even began!

Moreover, unlike Euclidean geometry and calculus, one cannot do just a taste of Galois theory. Like climbing Everest one must be prepared to commit to a long journey if one is to follow Évariste.

The story of Galois and his mathematical discoveries is one that should be better known. One of the most amazing aspects of this story is that he made his discoveries at the age of 19 and he died in a dual when he was twenty! An account of his short but eventful life is given in the book *The French Mathematician* and has even been made into a film. A short version of his life story is given in an appendix.

Also remarkable is that his discoveries were well ahead of their time. Calculus was ripe for discovery in the 17^{th} century. Had neither Newton nor Leibnitz been around it is clear that someone else would have invented calculus before very long. By contrast, had it not been for Galois, who knows how long we would have had to wait

for someone else to have made these discoveries. As it was, the notes that Galois submitted to the French Academy were lost and didn't come to light until several decades later.

§1.2. What Galois Did

So what did Galois actually prove? Loosely speaking, he proved that there is no formula for the general quintic polynomial equation, such as there is for the quadratic. In the 16^{th} century formulae were found for the cubic and quartic so it seemed only natural that there would be one for the quintic. But no.

Actually a Norwegian mathematician had proved that shortly before Galois. What Galois did was to construct a method for deciding *which* fifth (and higher) degree polynomials has zeros that could be expressed in terms of the coefficients using addition, subtraction, multiplication, division and extraction of roots.

The insolubility of the quintic is interesting enough, but not world shattering. What Galois is remembered for is the machinery that he built to solve this problem. In fact the insolubility of the quintic is not considered to be part of Galois Theory itself, but rather an interesting application. From a modern perspective Galois Theory is all about fields.

The concept of a field came long after Galois and if he were to attend a modern course in Galois Theory

he'd have a bit of catching up to do. He worked with permutations of the zeros of polynomials and constructed groups out of them. The modern approach is to form a field out of the zeros of a polynomial and then construct a group of automorphisms.

The groups that Galois worked with consisted of permutations of the zeros of a polynomial – a concept that's abstract enough. But later, group theory moved away from polynomials and dealt with groups of permutations of any objects. Finally group theory moved away from permutations and became purely axiomatic. The elements of a group could be permutations, or numbers, or even ways of rotating a mattress – indeed anything. All that's needed is a way of combining any two of these objects in a way that satisfies the four group axioms.

So while Galois went from polynomials to groups of permutations, modern Galois Theory goes from polynomials to fields and then to groups of automorphisms of fields, with the emphasis being the second part.

The true discovery that lies at the heart of Galois Theory is that, associated with every polynomial is a field, called the 'splitting field' and associated with that is a group called the 'Galois group' and a polynomial is 'soluble by radicals' (meaning that a formula of the prescribed type exists) if and only if the Galois group is soluble. [It's no accident that the word 'soluble' occurs in

both contexts. Soluble groups are called ‘soluble’ because of this connection with solubility of polynomials.] So let’s get started. Let’s consider a baby example.

§1.3. A Baby Example of Galois Theory

Consider the field $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, which we write as $\mathbb{Q}[\sqrt{2}]$. One first has to check that it is indeed a field. Most of the axioms are obvious. The only axiom that isn’t immediately obvious is the one about inverses under multiplication.

Suppose that $a + b\sqrt{2}$ is non-zero, where a, b are rational. Then $a - b\sqrt{2}$ is non-zero.

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})}$$

$$= \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

$$= \left(\frac{a}{a^2 - 2b^2}\right) + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

A **field extension** is simply a pair of fields, one inside the other. If $F \leq K$ we write the field extension as **K/F** and say that K is an extension of F. Most books write it as K:F, but I find that the analogy with fractions is useful.

Now K and F are rings, and normally in ring theory the notation K/F is used to denote the quotient ring, whose elements are cosets of F. But F would need to be an ideal

of K, and fields don't have ideals – well, only themselves and the $\{0\}$. So I'm using this notation in another sense. Also, I use the notation V/F to denote a vector space over the field F. These two uses are essentially the same because, as we'll see, whenever F is a subfield of K then K is a vector space over F.

$\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ is a field extension, as is $\mathbb{C}/\mathbb{R}$, but $\mathbb{Q}/\mathbb{Z}_p$ is not, because integers modulo a prime are not the same as ordinary integers.

An **automorphism** θ of a field F is a 1-1 and onto mapping from F to F that preserves both addition and multiplication:

$$\theta(x + y) = \theta(x) + \theta(y) \text{ and}$$
$$\theta(xy) = \theta(x)\,\theta(y).$$

[We will actually be using a different notation for functions but this will do for now.]

The Galois group of the field extension $[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}]$ is the group of all automorphisms of $\mathbb{Q}[\sqrt{2}]$ that fix the elements of the smaller field $\mathbb{Q}$. The group operation is the usual multiplication of functions, that is one function followed by the other. It's easy to check that this is indeed a group. We denote it by $\mathbf{G(\mathbb{Q}[\sqrt{2}]/\mathbb{Q})}$.

The identity element of this Galois group is the identity function $\theta(x) = x$ for all x. What else is there?

Suppose $\theta \in G(\mathbb{Q}[\sqrt{2}]/\mathbb{Q})$. If $a, b \in \mathbb{Q}$ then

$$\theta(a + b\sqrt{2}) = \theta(a) + \theta(b)\,\theta(\sqrt{2})$$

$= a + b\,\theta(\sqrt{2})$ since θ fixes every rational number.
So it all comes down to the possible values of $\theta(\sqrt{2})$.

Now $\sqrt{2}.\sqrt{2} = 2$ so $\theta(\sqrt{2}).\theta(\sqrt{2}) = \theta(2) = 2$. It follows that $\theta(\sqrt{2})$ is one of the two square roots of 2. If $\theta(\sqrt{2}) = \sqrt{2}$ then θ is just the identity automorphism. The only other automorphism is the one where $\theta(\sqrt{2}) = -\sqrt{2}$.

Let τ be the map $\tau(a + b\sqrt{2}) = a - b\sqrt{2}$. [It is easy to check that this is indeed an automorphism.]

Then $\tau^2(a + b\sqrt{2}) = \tau(a - b\sqrt{2}) = a + b\sqrt{2}$. Hence $\tau^2 = 1$, the identity automorphism. So we've seen that $G(\mathbb{Q}[\sqrt{2}]/\mathbb{Q})$ is a cyclic group of order 2.

What has this to do with polynomials? Well, consider the polynomial $x^2 - 4x + 2$. The zeros are:

$$\frac{4 \pm \sqrt{16 - 8}}{2} = \frac{4 \pm \sqrt{8}}{2} = \frac{4 \pm 2\sqrt{2}}{2} = 2 \pm \sqrt{2}.$$

The splitting field is the field we get by adjoining these to $\mathbb{Q}$, that is, the smallest field containing $\mathbb{Q}$ that also contains these zeros. Clearly this field is $\mathbb{Q}[\sqrt{2}]$.

Now Galois proved that the Galois group is soluble if and only if the polynomial is soluble by radicals. Clearly this quadratic is soluble so the Galois group must

be soluble. Of course it is. The Galois group here is cyclic and cyclic groups are abelian and abelian groups are soluble.

Here we started with the zeros and then constructed the splitting field and then the Galois group. How could we ever find a non-soluble Galois group if there is no formula for the zeros. This is done by a clever piece of indirect reasoning. Following Galois we exhibit a polynomial of degree 5 and, without finding the zeros, we can prove that the Galois group of the splitting field is $\mathbf{S}_5$, a group that is known not to be soluble.

We are now ready to roll up our sleeves and get down to some serious work. But first we must make sure that all the prerequisite knowledge is at our fingertips. It's assumed that you've seen all of the material summarised in the next chapter. That chapter serves as a compact reminder.