Introduction

The subject of Galois Theory traces back to Évariste Galois (1811–1832). He was a French mathematician whose work involved understanding the solution of polynomial equations. The standard formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

for the roots of the quadratic equation

$$ax^2 + bx + c = 0$$

is well-known. It turns out that analogous formulae exist for the roots of cubic and quartic polynomial equations. For example, the method to solve the general cubic equation was considered by mathematicians based in Bologna in the early 16th century (e.g., Scipione dal Ferro (1465–1526) and those who followed him).

What Galois did was to show that, in general, a quintic equation could not be solved by a similar formula. What he did not do was succeed in explaining it to anyone in a comprehensible way. For example, in 1830 he submitted his work to the Paris Academy of Sciences, but the final report states:

> We have made very effort to understand Galois's proof. His reasoning is not sufficiently clear, sufficiently developed, for us to judge its correctness, and we can give no idea of it in this report. The author announces that the proposition which is the special object of this memoir is part of a general theory susceptible of many applications. Perhaps it will transpire that the different parts of a theory are mutually clarifying, are easier to grasp together rather than in isolation. We would then suggest that the author should publish the whole of his work in order to form a definitive opinion. But in the state which the part he has submitted to the Academy now is, we cannot propose to give it approval.
>
> [from Stewart, *Galois Theory, Second edition*, p.xxi]

Galois's ideas were eventually understood, via the letter that he wrote to Chevalier on the eve of the duel which killed him. This theory is basically what is presented in this lecture course. As we now understand it, what Galois observed is the following:

- To every polynomial equation, $f(x) = 0$, we can associate a group, the *Galois group*, consisting of certain permutations of the roots.
- If the Galois group is *soluble*, then the polynomial equation can be solved *by radicals* (that is, by a formula of the type we are interested in).
- We can construct a polynomial whose Galois group is the symmetric group S_5, which is not soluble since it contains the non-abelian simple group A_5, and therefore we cannot solve the corresponding polynomial equation by radicals.

In fact, what we do is more general. We shall actually consider a pair of fields one inside the other ($F \subseteq K$) and then associate to this a *Galois group* $\mathrm{Gal}(K/F)$. Our work in this module will be to understand the link between the two concepts of the field extension $F \subseteq K$ and its Galois group. As a consequence of understanding these we can then establish Galois's above observations by specialising to the case when K is the field obtained by adjoining the roots of our polynomial $f(x)$ to the field F.

Structure of the lecture course

The following topics will be covered in the lectures:

- **Basic facts about fields and polynomial rings:** Mostly a review of material from MT3503, but some new information about irreducible polynomials.
- **Field extensions:** Terminology and basic properties about the situation of two fields with $F \subseteq K$.
- **Splitting fields and normal extensions:** Field extensions constructed by adjoining the roots of a polynomial, constructed so that the polynomial factorizes into linear factors over the larger field.
- **Basic facts about finite fields:** Existence and uniqueness of field of order p^n, together with the fact that the multiplicative group of a finite field is cyclic.
- **Separable extensions and the Theorem of the Primitive Element:** Separability is a technical condition to avoid repeated roots of irreducible polynomials. The Theorem of the Primitive Element applies in this circumstance and allows us to assume that our field extensions have a specific form and hence to simplify various proofs.
- **Galois groups and the Fundamental Theorem of Galois Theory:** The definition of the Galois group as the collection of invertible structure preserving maps of a field extension (this will be made more precise later). The Fundamental Theorem of Galois Theory states that the structure of the Galois group corresponds to the structure of the field extension.
- **Examples and Applications:** Including the link between solution of a polynomial equation by radicals and the solubity of the Galois groups.

Recommended texts

- Ian Stewart, *Galois Theory*, Chapman & Hall; 3rd Edition, 2004 in the library; 4th Edition, 2015.
- John M. Howie, *Fields and Galois Theory*, Springer Undergraduate Mathematics Series, Springer, 2006.
- P. M. Cohn, *Algebra, Vol. 2*, Wiley, 1977, Chapter 3. [Out of print, but available in the library.]