GALOIS THEORY

Fall TERM 2023

Dr. Sanhan Khasraw

1. Introduction

1.1. **Symmetry of roots of polynomials.** Galois theory arose out of attempts to understand solutions to polynomial equaltions. The underlying idea of Galois theory – expressed not very precisely – is that roots of polynomials possess certain natural symmetries.

This can be illustrated by the following example. Consider the following polynomial in a variable X:

$$f = X^5 - 2\sqrt{2}X^4 + 12X^3 + (10 - 2\sqrt{2})X^2 + (11 - 20\sqrt{2})X + 110.$$

The coefficients of f are real. As f has degree 5, it is not surprising that f has 5 complex roots, namely,

$$-2, 1+2i, 1-2i, \sqrt{2}+3i, \sqrt{2}-3i.$$

We see that the set of roots is symmetric with respect to the horizontal axis.

That is, *if $z \in \mathbb{C}$ is a root of f, then its complex conjugate $\bar{z}$ is a root of f.* In fact, this statement is true not just for the polynomial f above, but for any polynomial g with real coefficients. How can we prove this? We have

$$g = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0, \quad \text{where } a_0, \ldots, a_n \in \mathbb{R}.$$

Recall the following properties of complex conjugation: $\overline{z+w} = \overline{z} + \overline{w}$ and $\overline{zw} = \overline{z}\overline{w}$ for all $z, w \in \mathbb{C}$. We have

$$\begin{aligned} \overline{g(z)} &= \overline{a_n z^n + \cdots + a_1 z + a_0} \\ &= \bar{a}_n \bar{z}^n + \cdots + \bar{a}_1 \bar{z} + \bar{a}_0 \\ &= a_n \bar{z}^n + \cdots + \bar{a_1} + \bar{a_0} = g(\overline{z}), \end{aligned}$$

as $a_n, \ldots, a_0 \in \mathbb{R}$. Hence, if $g(z) = 0$, then $g(\bar{z}) = 0$, as claimed.

Let us look at the above proof carefully. Consider the complex conjugation map $\alpha\colon \mathbb{C} \to \mathbb{C}$, $\alpha(z) = \bar{z}$. Our argument uses only the following two facts about α:

(i) α is a field homomorphism (that is, $\alpha(z+w) = \alpha(z) + \alpha(w)$ and $\alpha(zw) = \alpha(z)\alpha(w)$ for all $z, w \in \mathbb{C}$;

(ii) $\alpha(r) = r$ for every $r \in \mathbb{R}$.

It turns out that there are only two non-zero maps satisfying these conditions: the complex conjugation α and the identity map $\mathrm{id}_{\mathbb{C}}$ given by $\mathrm{id}_{\mathbb{C}}(z) = z$. This is mainly due to the fact that $\mathbb{R}$ is “large”: it is very “difficult” for a homomorphism to satisfy condition (ii), i.e. to fix *all* real numbers. If $\mathbb{R}$ is replaced by a smaller field, for example, by $\mathbb{Q}$, we get many more symmetries and hence a much richer theory, as we will see. Indeed, the group of symmetries of the roots of a polynomial with rational coefficients may be arbitrarily large, depending on the polynomial.

Such a group is called a *Galois group* and is the main object of study in this course. (A formal definition will be given later.)

Remark. Whereas the above symmetry of the roots of f is easy to visualise pictorially, this will not be the case in general. Instead of pictures, we will need to use intuition coming mainly from Linear Algebra.

We will begin by introducing the so-called *field extensions* and looking at ways to associate a field extension with a polynomial. This is due to the fact that for many purposes it is much more convenient to look at symmetries of field extensions rather than symmetries of roots of polynomials.

1.2. **Algebraic numbers.** Our approach to numbers will be quite different to that used, say, in Analysis. Many (or most) of the fields considered in this course will lie inside the field $\overline{\mathbb{Q}}$ of algebraic numbers, which is defined below. To motivate this definition, let us consider how different number systems arose. The natural numbers

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

are the most straightforward: they are used for counting. One can add and multiply natural numbers, but one cannot always subtract: that is, the equation $x + a = b$ does not always have a solution for $a, b \in \mathbb{N}$. To allow subtraction in all cases, one has to extend $\mathbb{N}$ to

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Now one can add, subtract and multiply. But one cannot always divide: the equation

$$ax + b = 0 \tag{1.1}$$

does not necessarily have a solution for $a, b \in \mathbb{Z}$. In order to allow division in all cases, one has to "add" all solutions to (1.1), i.e. to extend $\mathbb{Z}$ to the field $\mathbb{Q}$ of rational numbers.

When we consider further extension, we are faced with a choice. The rational numbers are not very convenient for the purposes of Analysis and many applications to Physics. To this end, one defines the real numbers $\mathbb{R}$ by "completing" $\mathbb{Q}$. As a result, every Cauchy sequence in $\mathbb{R}$ converges and the Intermediate Value Theorem holds; these and other facts make $\mathbb{R}$ very suitable, say, for modelling the space we live in.

In order to expand $\mathbb{Q}$ to $\mathbb{R}$, one has to use not just the four arithmetic operations but also the fact that we are able to compare rational numbers, i.e. the usual order $<$. Indeed, it is impossible to define convergence of sequences without comparing numbers.

In Algebra and Number Theory, one doesn't necessarily use the order $<$: in this course, we will never compare two elements of the field. Instead, we consider another natural way to extend $\mathbb{Q}$. We can generalise the equation 1.1 to

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

where $a_0, \ldots, a_n \in \mathbb{Q}$ and not all of them are zero. Complex solutions to equations of this form are called *algebraic numbers*. We will see that they form a field, called $\bar{\mathbb{Q}}$. We have

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \bar{\mathbb{Q}} \subset \mathbb{C}.$$

An advantage of this approach is that much of what we will do works over any field. Indeed, many applications of Galois Theory concern fields that are very different from $\mathbb{Q}$. However, most of the examples in this course will involve $\mathbb{Q}$ and its extensions.