The Galois Theorem

Let us recall our setup from last lecture. For simplicity we will work with field extensions over $F \subset \mathbb{C}$, although much of what we will say holds in greater generality. Let E be a finite extension of F. Recall that E is a *Galois* extension, or a *splitting field*, if there is some polynomial $f(x) \in F[x]$ such that over the complex numbers, say, we have

$$f(x) = a(x - \alpha_1)\cdots(x - \alpha_n)$$

where $a \in F$, and $E = F(\alpha_1, \ldots, \alpha_n)$. We introduced for any extension E over F the automorphism group $\mathrm{Aut}(E/F)$ consisting of field isomorphisms $\sigma : E \to E$ which fix F in the sense that $\sigma(a) = a$ for all $a \in F$. In case E is Galois, we write

$$\mathrm{Gal}(E/F) = \mathrm{Aut}(E/F)$$

and call this the *Galois group* of the field extension. The main result from last lecture gives us an isomorphism from $\mathrm{Gal}(E/F)$ to a subgroup of the symmetric group S_n, where n is the number of roots as above.

Example: Consider the field $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We saw last lecture that this is a Galois extension over $\mathbb{Q}$: it is the splitting field for the polynomial $f(x) = (x^2 - 2)(x^2 - 3)$ with roots $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$. The Galois group $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. In fact

$$\mathrm{Gal}(E/\mathbb{Q}) = \{\mathrm{id}_E, \sigma_1, \sigma_2, \sigma_3\}$$

where σ_1 has the effect of interchanging $\sqrt{2}$ with $-\sqrt{2}$, but fixes $\sqrt{3}$; σ_2 has the effect of interchanging $\sqrt{3}$ with $-\sqrt{3}$, but fixes $\sqrt{2}$; and $\sigma_3 = \sigma_1 \circ \sigma_2$.

Note that $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ can also be viewed as an extension of $\mathbb{Q}(\sqrt{2})$ and of $\mathbb{Q}(\sqrt{3})$, and also $\mathbb{Q}(\sqrt{6})$. We can write all these extensions in a diagram (below on the left); in general, if a line connects E and F and E appears above F, then E is an extension field of F.

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
& \{\mathrm{id}_E, \sigma_1, \sigma_2, \sigma_3\} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\{\mathrm{id}_E, \sigma_1\} \arrow[dr, dash, "2"'] & \{\mathrm{id}_E, \sigma_2\} \arrow[d, dash, "2"] & \{\mathrm{id}_E, \sigma_3\} \arrow[dl, dash, "2"] \\
& \{\mathrm{id}_E\} &
\end{tikzcd}$$

We have also indicated the degrees of the extensions; in this case they are all 2. On the right we have drawn instead the diagram of subgroups of the group $\mathrm{Gal}(E/\mathbb{Q}) = \{\mathrm{id}_E, \sigma_1, \sigma_2, \sigma_3\}$. Each subgroup has index 2, as indicated at the lines.

The fundamental theorem of Galois theory states the precise relationship between these two situations, and gives a correspondence between certain field extensions and subgroups.

▶ **(The Galois Theorem) Let E be a finite Galois extension of $F \subset \mathbb{C}$. Then**

$$[E : F] = |\mathbf{Gal}(E/F)|$$

For each field K with $F \subset K \subset E$ we have that E is Galois over K. The assignment $K \mapsto \mathbf{Gal}(E/K)$ induces a 1-1 and onto correspondence

$$\{\textbf{fields } K : \; F \subset K \subset E\} \longrightarrow \{\textbf{subgroups of } \mathbf{Gal}(E/F)\}$$

Further, we have $F \subset K \subset L \subset E$ if and only if we have the sequence of inclusions

$$\{e\} = \mathbf{Gal}(E/E) \subset \mathbf{Gal}(E/L) \subset \mathbf{Gal}(E/K) \subset \mathbf{Gal}(E/F)$$

Finally, a field K with $F \subset K \subset E$ is Galois over F if and only if $\mathbf{Gal}(E/K)$ is a normal subgroup of $\mathbf{Gal}(E/F)$, and if this is the case, we have

$$\mathrm{Gal}(K/F) \cong \frac{\mathrm{Gal}(E/F)}{\mathrm{Gal}(E/K)}$$

Due to a lack of time we will unfortunately omit the proof.

Consider the following problem: given a polynomial $f(x) \in \mathbb{Q}[x]$, we know it has some complete set of roots in the complex numbers, say $\alpha_1, \ldots, \alpha_n$. Thus over $\mathbb{C}$ we can write

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$$

where $a \in \mathbb{Q}$ and each α_i is some complex number. Can we obtain each root α_i from the rational numbers by taking successive radicals? That is to say, can we write each α_i as an expression involving only the coefficients of $f(x)$, the operations of addition, multiplication, subtraction and division, and also k^{th} roots? The quadratic formula says the answer is “yes” when $f(X)$ is degree 2, and in fact the answer is “yes” for $\deg(f(x)) \leqslant 4$. However, it is not always possible beyond these cases:

▶ **(Abel–Ruffini Theorem) For any $n \geqslant 5$ there are polynomials of degree n such the roots cannot be solved in terms of radicals.**

We sketch a proof of this theorem by exhibiting a quintic which is not solvable in terms of radicals. We begin by recasting what we mean by solvable in terms of field theory: if we can solve for the roots of $f(x)$ in terms of radicals, then there is a chain of field extensions

$$\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_{k-1} \subset F_k = E$$

such that E is the splitting field of $f(x)$ and each extension

$$F_i \subset F_{i+1}$$

is obtained by appending a radical, in the sense that $F_{i+1} = F_i(\beta_i)$ where $\beta_i^{n_i} \in F_i$. It can be shown that the special structure of this chain of field extensions along with the Galois Theorem implies that $\mathrm{Gal}(E/\mathbb{Q})$ is a *solvable group*. In general, a solvable group is a group G that admits a sequence of subgroups $H_i \subset G$ as depicted below

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_{k-1} \subset H_k = G$$

such that each H_i is normal in H_{i+1} and the factor group H_{i+1}/H_i is abelian. One can prove:

▸**The symmetric group S_n is solvable if and only if $n \leqslant 4$.**

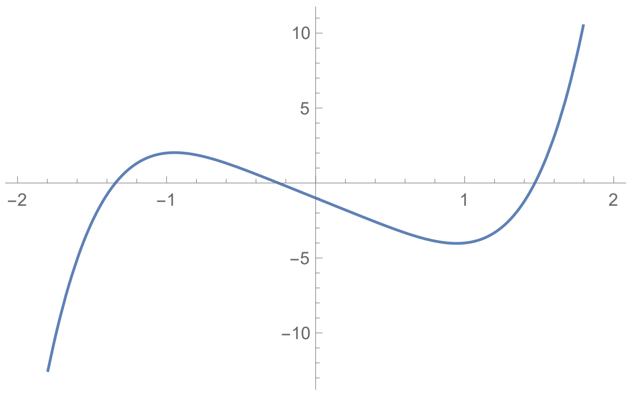
Thus to prove the Abel–Ruffini theorem for quintics, it suffices to find an irreducible polynomial $f(x)$ of degree 5 whose Galois group is isomorphic to S_5.

We know in this case that $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to a subgroup G of S_5. Furthermore, from last lecture we know that this subgroup $G \subset S_5$ is *transitive*, that is, given any $i, j \in \{1, 2, 3, 4, 5\}$ we can find $g \in G$ such that $g(i) = j$. A direct computation shows:

▸**If $G \subset S_5$ is transitive and contains a transposition, then $G = S_5$.**

It remains then to show that we can find an irreducible quintic $f(x) \in \mathbb{Q}[x]$ whose Galois group, viewed as a permutation group of the 5 roots, contains a transposition. For this it suffices to find an irreducible quintic with rational coefficients that has exactly 2 complex roots, for then complex conjugation will provide the corresponding transposition!

Example: Consider $f(x) = x^5 - 4x - 1$. One can check this is irreducible.



From its graph, we see that there are exactly 3 real roots. Thus there are 2 complex roots, and complex conjugation gives an element of the Galois group which acts as a transposition on the roots. Thus the Galois group, being a transitive subgroup of S_5 with a transposition, must be all of S_5. This is not solvable, and so the roots of this quintic are not expressible in terms of radicals.