Motivation and Introduction

Main purpose of this course is to study Galois theory — a field that arose in trying to study roots of polynomials.

Consider $f(x) = ax^2 + bx + c$. If we want to find a general, closed-form expression for the roots of the function, we complete the square.

$$\text{roots} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

We found these roots by by the coefficients, $\mathbb{Q}$, addition, subtraction, multiplication, division, and square root (raising to the $1/2$ power: see Math 310 notes, Page 104). Naturally, this leads us to ask whether we can do this for cubic polynomials with the same operations. Obviously, we have to change from $1/2$ power to the $1/3$ power, but Cardano showed that it was possible to solve a cubic and quartic equation using these traditional operations and radicals.

Évariste Galois invented his theory to prove there is no such closed formula by radicals for any polynomial of degree 5 or above.

For example, $x^5 - x + 1$ does not have roots given by radicals.

Example: A Solvable Polynomial

Consider the polynomial $f(x) = x^2 - 2$. We know that the roots of this polynomial are $\pm\sqrt{2}$. From this, we want to create a set $K(f)$ that satisfies the following rules:

- $\mathbb{Q} \subseteq K(f)$.
- $K(f)$ must contain the roots of f.
- $K(f)$ must be closed under the traditional operations: $+, -, \times, /$
- $K(f)$ must be the smallest field that satisfies the above three requirements.

Claim: $K(f) = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

- $\mathbb{Q} \subseteq K(f)$, because we can set $b = 0$.
- $\sqrt{2} = 0 + (1)(\sqrt{2})$, $-\sqrt{2} = 0 + (-1)(\sqrt{2})$
- Let $a + b\sqrt{2}$ and $c + d\sqrt{2}$ be elements of $K(f)$. Then,
  - $(a + b\sqrt{2}) \pm (c + d\sqrt{2}) = (a \pm c) + (b \pm d)\sqrt{2}$
  - $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$
  - Set $c + d\sqrt{2} \neq 0$

$$\begin{aligned}\frac{a + b\sqrt{2}}{c + d\sqrt{2}} &= \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} \\ &= \frac{1}{c^2 - 2d^2}\left((ac - 2bd) + (bc - ad)\sqrt{2}\right) \\ &= \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}\end{aligned}$$

- $K(f)$ is indeed the smallest set.
  - Note that $K(f)$ is a $\mathbb{Q}$-vector space, with basis $\{1, \sqrt{2}\}$. Therefore, $\dim_{\mathbb{Q}} K(f) = 2$. $K(f)$ is known as the "splitting field" of f.

We want to consider a bijective function $\varphi : K(f) \to K(f)$ with the following properties:

- $\varphi(r) = r$ for every $r \in \mathbb{Q}$
- $\varphi(x+y) = \varphi(x) + \varphi(y)$
- $\varphi(xy) = \varphi(x)\varphi(y)$

We denote the collection of all such φ as $\text{Aut}(K(f)/\mathbb{Q})$. This is a group under the operation $\circ$ (composition). Specifically, we have

$$\begin{aligned}\varphi(a+b\sqrt{2}) &= \varphi(a) + \varphi(b)\varphi(\sqrt{2}) \\ &= a + b\varphi(\sqrt{2}).\end{aligned}$$

Notice

$$\begin{aligned}\left(\varphi(\sqrt{2})\right)^2 - 2 &= \varphi\left(\left(\sqrt{2}\right)^2 - 2\right) \\ &= \varphi(0) \\ &= 0.\end{aligned}$$

Therefore, $\varphi(\sqrt{2}) = \pm\sqrt{2}$. Therefore, we have that the elements of $\text{Aut}(K(f)/\mathbb{Q})$ as the following:

$$\begin{aligned}\varphi_0 : a + b\sqrt{2} &\mapsto a + b\sqrt{2} \\ \varphi_1 : a + b\sqrt{2} &\mapsto a - b\sqrt{2} \\ \varphi_1 \circ \varphi_1 &= \varphi_0\end{aligned}$$

Thus,

$$\begin{aligned}\text{Aut}(K(f)/\mathbb{Q}) &= \{\varphi_0, \varphi_1\} \\ &\cong \mathbb{Z}/2\mathbb{Z}\end{aligned}$$

Example: A Harder Polynomial

Let $f(x) = (x^2-2)(x^2-3)$. Our roots are $\{\pm\sqrt{2}, \pm\sqrt{3}\}$. We want to form $K(f)$ with the same properties. Let

$$\begin{aligned}K(f) &= \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.\end{aligned}$$

Just as with our previous example, $K(f)$ is a vector space over $\mathbb{Q}$, with basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$, so $\dim_{\mathbb{Q}} K(f) = 4$.

Now, we want $\text{Aut}(K(f)/\mathbb{Q})$. If $\varphi \in \text{Aut}(K(f)/\mathbb{Q})$, then

$$\begin{aligned}\varphi(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\varphi(\sqrt{2}) + c\varphi(\sqrt{3}) + d\varphi(\sqrt{6}) \\ &= a + b\varphi(\sqrt{2}) + c\varphi(\sqrt{3}) + d\varphi(\sqrt{2})\varphi(\sqrt{3}).\end{aligned}$$

Thus, we need to know $\varphi(\sqrt{2})$ and $\varphi(\sqrt{3})$. So,

$$\begin{aligned}f(\varphi(\sqrt{2})) &= \left(\left(\varphi(\sqrt{2})\right)^2 - 2\right)\left(\left(\varphi(\sqrt{2})\right)^2 - 3\right) \\ &= 0\end{aligned}$$

and the same is the case with $\varphi(\sqrt{3})$. So,

$$\begin{aligned}\varphi(\sqrt{2}) &\in \{\pm\sqrt{2}, \pm\sqrt{3}\} \\ \varphi(\sqrt{3}) &\in \{\pm\sqrt{2}, \pm\sqrt{3}\}.\end{aligned}$$

Suppose $\varphi(\sqrt{2}) = \sqrt{3}$. Then,

$$\begin{aligned}\left(\left(\varphi(\sqrt{2})\right)^2\right) &= (\sqrt{3}^2 - 1) \\ &= 0 \\ &= (\varphi(2) - 3) \\ &= -1. \perp\end{aligned}$$

Thus,

$$\begin{aligned}\varphi(\sqrt{2}) &\in \{\pm\sqrt{2}\} \\ \varphi(\sqrt{3}) &\in \{\pm\sqrt{3}\},\end{aligned}$$

and we have the maps as:

$$\begin{aligned}\varphi_0 &: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3} \\ \varphi_1 &: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3} \\ \varphi_2 &: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3} \\ \varphi_3 &: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}\end{aligned}$$

Example: A Cubic Polynomial

Consider the function $f(x) = x^3 - 2$. The function has one real root, $r_1 = \sqrt[3]{2}$, and two complex roots. Let's examine $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$; r_2 and r_3 are not in $Q(\sqrt[3]{2})$. We could instead consider $\mathbb{Q}(\sqrt[3]{2}, r_1, r_2)$.

$$\begin{aligned}x^3 - 2 &= (x - r_1)(x^2 + r_1 x + r_1^2) \\ r_2 &= \frac{-r_1 + \sqrt{r_1^2 - 4r_1^2}}{2} \\ &= r_1 \frac{-1 + \sqrt{-3}}{2} \\ &= r_1 \zeta_3 \\ r_3 &= r_1 \frac{-1 - \sqrt{-3}}{2} \\ &= r_1 \zeta_3^2\end{aligned}$$

However, including r_2 and r_3 is excessive — all we need is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Therefore, the basis of this vector space is $\{1, r_1, r_1^2, \zeta_3, \zeta_3 r_1, \zeta_3 r_1^2\}$ (note that $\zeta_3^2 = -1 - \zeta_3$). Therefore, $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}, \zeta_3) = 6$, and $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = K(f)$.Additionally, we have $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\varphi_0\}$, but $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$. For the full field extension, we need to find $\varphi(\sqrt[3]{2})$ and $\varphi(\zeta_3)$.

$$\begin{aligned}\varphi(\sqrt[3]{2}) &\in \{r_1, \zeta_3 r_1, \zeta_3^2 r_1\} \\ \varphi(\zeta) &\in \{\zeta_3, \zeta_3^2\} \\ \varphi_0 &: r_1 \mapsto r_1, \zeta_3 \mapsto \zeta_3 \\ \varphi_1 &: r_1 \mapsto \zeta_3 r_1, \zeta_3 \mapsto \zeta_3 \\ \varphi_2 &: r_1 \mapsto r_1, \zeta_3 \mapsto \zeta_3^2 \\ \varphi_3 &: r_1 \mapsto \zeta_3^2 r_1, \zeta_3 \mapsto \zeta_3 \\ \varphi_4 &: r_1 \mapsto \zeta_3 r_1, \zeta_3 \mapsto \zeta_3^2 \\ \varphi_5 &: r_1 \mapsto \zeta_3^2 r_1, \zeta_3 \mapsto \zeta_3^2\end{aligned}$$

Therefore,

$$\begin{aligned}\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q}) &= 6\\ &= \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{},\sqrt[3]{2})\end{aligned}$$