Galois Theory

Our goal will be to prove that polynomials with degree $n \geq 5$ are not always solvable using radicals.

Any polynomial $ax^2 + bx + c = 0$, $a, b, c \in \mathbb{Q}$ of degree $n = 3$ is solvable using only its coefficients a, b, c and basic mathematical operations.

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

But we will see thats not the case with quintic and higher order polynomials.

An example is

$$x^5 - 16x + 2 = 0$$

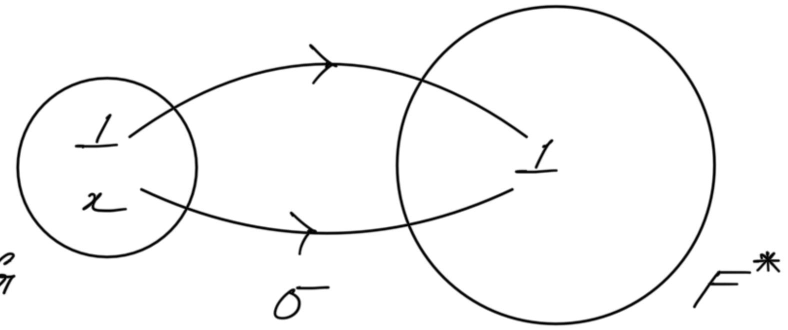
Group Characteristics

Let $(G, \cdot)$ be a group and $(F, +, \cdot)$ be a field. And $F^* = F \setminus \{0\}$.

The character of G in F is a group homomorphism $\sigma : G \to F^*$.

For example,

$G = \{1, x\}$ and $F = \mathbb{Q}$



$\sigma(1 \cdot x) = \sigma(x) = 1$

$\sigma(1) \cdot \sigma(x) = 1$

$\Rightarrow \sigma(1 \cdot x) = \sigma(1) \cdot \sigma(x)$

σ is thus a group homomorphism from G to F.

Let $\sigma_1, \ldots, \sigma_n$ be the characteristics of

G in F. They are independent if

$$a_1\sigma_1 + \cdots + a_n\sigma_n = 0 \text{ where } a_1, \ldots, a_n \in F.$$

$$\Rightarrow (a_1\sigma_1 + \cdots a_n\sigma_n)(g) = 0$$

$$\Rightarrow (a_1\sigma_1)(g) + \cdots + (a_n\sigma_n)(g) = 0$$

$$\Rightarrow \boxed{a_1 = \cdots = a_n = 0}$$

→ Any set of distinct characteristics of G in F are independent.

~~Proof~~ For $n=1$, let

$$a_1\sigma_1 = 0 \quad \Rightarrow (a_1\sigma_1)(g) = 0 \ \forall g \in G$$

$$\Rightarrow (a_1\sigma_1)(1_G) = 0$$

$$\Rightarrow a_1\{\sigma_1(1_G)\} = 0$$

$$\Rightarrow a_1 1_F = 0$$

$$\Rightarrow a_1 = 0$$

the statement holds true. Let it be true for $n = (m-1)$. Then, when

$$a_1\sigma_1 + \cdots + a_{m-1}\sigma_{m-1} = 0 \implies a_1 = \cdots = a_{m-1} = 0.$$

Now for $n = m$, when

$$(a_1\sigma_1 + \cdots + a_{m-1}\sigma_{m-1}) + a_m\sigma_m = 0$$

Let $a_m \neq 0$. Dividing by a_m,

$$\implies (a_1\sigma_1 + \cdots + a_{m-1}\sigma_{m-1}) + \sigma_m = 0$$

$$\implies (a_1\sigma_1 + \cdots + a_{m-1}\sigma_{m-1} + \sigma_m)(g) = 0 \quad \forall g \in G.$$

Since $\sigma_1 \neq \sigma_m$, $\exists\, \alpha \in G$ such that

$\sigma_1(\alpha) \neq \sigma_m(\alpha) \neq 0.$

$$(a_1\sigma_1 + \cdots + a_{m-1}\sigma_{m-1} + \sigma_m)(g\alpha) = 0 \quad \text{——— (1)}$$

$$\implies a_1\sigma_m(\alpha)^{-1}\sigma_1(\alpha)\sigma_1(g) + \cdots + a_{m-1}\sigma_m(\alpha)^{-1}\sigma_{m-1}(\alpha)$$
$$\sigma_{m-1}(g) + \sigma_m(\alpha)^{-1}\sigma_m(\alpha)\sigma_m(g) = 0$$

——— (2)

Doing (1) − (2)

$$\implies \{a_1 - a_1\sigma_m^{-1}(\alpha)\sigma_1(\alpha)\}\sigma_1(g) + \cdots +$$

$$\{a_{m-1} - a_{m-1}\sigma_m(\alpha)^{-1}\sigma_{m-1}(\alpha)\}\sigma_{m-1}(g) = 0$$

$$\left\{a_{m-1} - a_{m-1}\,\sigma_m(\alpha)\,\sigma_{m-1}(\alpha)\right\}\sigma_{m-1}(y) = 0$$

$$\Rightarrow a_1 - a_1\,\sigma_m^{-1}(\alpha)\,\sigma_1(\alpha) = 0$$

$$\Rightarrow a_1 = a_1\,\sigma_m^{-1}(\alpha)\,\sigma_1(\alpha)$$

$\Rightarrow \sigma_m(\alpha) = \sigma_1(\alpha)$ which is not possible since $\sigma_m \neq \sigma_1$. Thus $a_m = 0$. The statement holds true for $n = m$.

Let K and L be 2 fields. $\sigma_1, \dots, \sigma_n$ be field homomorphisms from K^* to L^*. Then the above statement holds true for them as well.