Galois Theory Notes

Leon Lee

January 13, 2025

Contents

1 Introduction to Galois Theory

1.1 Complex Numbers over $\mathbb{R}$

Think of $\mathbb{C}$ as $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ where the only thing you know about i is that

$$i^2 + 1 = 0$$

However, this equation has two roots (no way to distinguish i and $-i$). ezample $z = i$

Definition 1.1.1: Conjugate

$z, z' \in \mathbb{Z}$ are **conjugate** over $\mathbb{R}$ if $\forall p(t) \in \mathbb{R}[t]$ (polynomials with coefficients in $\mathbb{R}$)

$$p(z) = 0 \iff p(z') = 0$$

Lemma 1.1.2: Characterising Conjugates

$z, z' \in \mathbb{C}$ are conjugate over $\mathbb{R}$ iff either $z = z'$ or $\overline{z} = z'$

Proof. Assume z, z' are conjugate.

$$z = x + iy \quad x, y \in \mathbb{R}$$

Take the equation

$$(z - x)^2 + y^2 = 0$$
$$p(t) = (t - x)^2 + y^2 \in \mathbb{R}[t]$$

□

1.2 Complex Numbers over $\mathbb{Q}$

Definition 1.2.1: Conjugacy in $\mathbb{Q}$

$z, z' \in \mathbb{C}$ are **conjugate over** $\mathbb{Q}$ if $\forall p(t) \in \mathbb{Q}[t]$

$$p(z) = 0 \iff p(z') = 0$$

Example: $\sqrt{2}$ is not conjugate to $-\sqrt{2}$ over $\mathbb{R}$. e.g.

$$p(t) = t - \sqrt{2} \in \mathbb{R}[t]$$

Example: $\sqrt{2}$ is conjugate to $-\sqrt{2}$ over $\mathbb{Q}$
Treat $\sqrt{2}$ like i

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

This is also a field.
We want the analogue of complex conjugates. Show it is well-defined:

$$a + b\sqrt{2} = a' + b'\sqrt{2}, \quad a, b, a', b' \in \mathbb{Q}, \quad a - a' = (b' - b)\sqrt{2}$$

..some more stuff

Example: $\sqrt{2}$ is not conjugate to $\sqrt{3}$ over $\mathbb{R}$

$$p(t) = t^2 - 2$$

Example: p prime, $\omega = \exp\left(\frac{z\pi i}{p}\right)$ (primitive p-th root of unity)

$$\omega^p = 1$$

ω^k is conjugate over $\mathbb{Q}$ to ω, $\forall k = 1, \dots, p-1$
ω^k is conjugate over $\mathbb{R}$ to ω iff $k \equiv 1, p-1 \mod p$

Definition 1.2.2: Conjugacy for sets

$(z_1, \dots, z_n), z_i, z_i' \in \mathbb{C}$ is conjugate over $\mathbb{Q}$ to $(z_1', \dots, z_n')$ if $\forall p(t_1, \dots, t_n) \in \mathbb{Q}[t_1, \dots, t_n]$

Additionally, if $(z_1, \dots, z_n)$ conjugate to $(z_1', \dots, z_n')$, then z_i is conjugate to z_i' for all i

Definition 1.2.3: Galois Group

If we have a $f \in \mathbb{Q}[t]$ where $\alpha_1, \dots, \alpha_n$ are roots, then the Galois group of f, $\mathrm{Gal}(f)$ is

$$\mathrm{Gal}(g) = \{\sigma \in S_n \mid (\alpha_1, \dots, \alpha_n) \text{ conjugate to } \{\alpha_{S(1)}, \dots, \alpha_{\sigma(n)}\}\}$$