Assignment 16

Separability, computation of automorphism groups

1. Let $f \in k[X]$ and let $E \supset k$ be a splitting field of f. We want to prove that f has no multiple root in E if and only if $\gcd_{k[X]}(f, f') = 1$.

   (a) Let F/k be a field extension and $f, g \in k[X]$. Prove that $\gcd_{k[X]}(f, g) = 1$ if and only if $\gcd_{F[X]}(f, g) = 1$.

   (b) Write $f = \prod_{i=1}^{n}(X - \alpha_i)$ in $E[X]$. Establish the formula

   $$\prod_{i=1}^{n} f'(\alpha_i) = \pm \left(\prod_{i<j} (\alpha_i - \alpha_j) \right)^2 .$$

   (c) Use the above steps in order to conclude.

2. Let p be a prime number and $\zeta := e^{\frac{2\pi i}{p}}$ a primitive p-th root of unity. Consider the polynomial $\varphi_p := \frac{X^p - 1}{X - 1} \in \mathbb{Q}[X]$ with splitting field E.

   (a) Prove that φ_p is irreducible in $\mathbb{Q}[X]$ and deduce that φ_p is the minimal polynomial of ζ over $\mathbb{Q}$.

   (b) Show that $E = \mathbb{Q}(\zeta)$.

   (c) Prove that $\mathrm{Aut}(E/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$.

3. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

   (a) Prove that $[E : \mathbb{Q}] = 4$.

   (b) Show that $\mathrm{Aut}(E/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

4. Show that the Galois group of $X^3 - 2 \in \mathbb{Q}[X]$ is isomorphic to S_3.

   Hint: Let E be the splitting field of $X^3 - 2$. Find the roots of $X^3 - 2$ in $\mathbb{C}$. Consider the intermediate extension $\mathbb{Q}(\exp(2\pi i/3))/\mathbb{Q}$ of E and show that $[E : \mathbb{Q}] > 3$.