Assignment 18

Radical extensions, Transitive group actions

1. Let $f = X^3 + pX + q \in \mathbb{Q}[X]$ be an irreducible polynomial. Let $R(f) = \{z_1, z_2, z_3\}$ and $E = \mathrm{Sf}(f)$.

   (a) Define the *discriminant* of f as
   $$D(f) := \prod_{i<j} (z_i - z_j)^2.$$
   Prove that $D(f) = -4p^3 - 27q^2 \neq 0$. [*Hint:* $f = (X - z_1)(X - z_2)(X - z_3)$]

   (b) Notice that E contains the square roots of $D(f)$.

   (c) Suppose that $D(f)$ is not a square in $\mathbb{Q}$. Show that $\mathrm{Gal}(E/\mathbb{Q}) = S_3$.

   (d) Suppose that $D(f)$ is a square in $\mathbb{Q}$. Show that there exists no automorphism $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ switching z_1 and z_2 and deduce that $\mathrm{Gal}(E/\mathbb{Q}) = A_3$.

   (e) Prove that the roots of f are all real if and only if $D(f) > 0$. Else, f has one real root and two non-real conjugated roots.

2. Let $f = X^3 + X^2 + 2X + \frac{7}{27} \in \mathbb{Q}[X]$. Construct a radical extension of $\mathbb{Q}$ containing the splitting field of f. [*Hint:* Look at Cardano's formula from the first lecture]

3. Let k be a field of characteristic 2 and K/k a quadratic extension such that $\mathrm{Card}(\mathrm{Gal}(K/k)) = 2$. Show that there exist $\beta \in K$ and $a \in k$ such that β is a root of $X^2 - X + a \in k[X]$ and $K = k(\beta)$.

4. Let G be a group acting on a set X with at least two elements. We say that the action is *doubly transitive* if for each $x_1, x_2, y_1, y_2 \in X$ with $x_1 \neq x_2$ and $y_1 \neq y_2$ there exists $g \in G$ such that $g \cdot x_i = y_i$ for $i = 1, 2$. Show that the following statements hold:

   (a) S_n acts doubly transitively on $\{1, \ldots, n\}$ for each $n \geqslant 2$.

   (b) A_n acts doubly transitively on $\{1, \ldots, n\}$ for each $n \geqslant 4$.

   (c) For each $n \geqslant 4$ the group D_n does *not* act doubly transitively on the vertices of an n-gon (see Assignment 8, Exercise 7).