Assignment 25

Galois correspondence. Solvability by radicals.

1. In class, we stated the following result:

   Proposition. Let k be a field of characteristic 0 and E/k a finite Galois extension with solvable $\mathrm{Gal}(E/k)$. Then E is contained in a radical extension of k.

   In order to prove this result, we do an induction on $|\mathrm{Gal}(E/k)| = [E:k]$. In the case $E \neq k$ we take a normal subgroup $N \lhd \mathrm{Gal}(E/k)$ of prime index p (using Assignment 21, Exercise 3) and define k^* as the splitting field of $X^p - 1 \in k[X]$.

   (a) Prove that $k^* = k(w)$ for some root w of $X^p - 1 \in k[X]$. Define $E^* := E(w)$.

   (b) Assume that $k^* = k$. Prove that E^N/k is a pure extension and conclude.

   (c) Suppose now that $k^* \neq k$. Show that E^*/k^* is a Galois extension and that $\mathrm{Gal}(E^*/k^*)$ injects into $\mathrm{Gal}(E/k)$.

   (d) Deduce that $\mathrm{Gal}(E^*/k^*)$ is solvable and that E^*/k^* is contained in a radical field extension M/k^*.

   (e) Explain why M/k is radical as well and conclude the proof of the Lemma.

2. Let p be an odd prime number. Let $\zeta = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ and $E = \mathbb{Q}(\zeta)$. Recall that $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{F}_p^\times$. For $a \in \mathbb{F}_p^\times$, define the *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square in } \mathbb{F}_p^\times \\ -1 & \text{if } a \text{ is a not square in } \mathbb{F}_p^\times. \end{cases}$$

   Define the complex number

$$\tau = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \zeta^a.$$

   (a) Show that the map $\mathbb{F}_p^\times \longrightarrow \{\pm 1\}$ sending $a \mapsto \left(\frac{a}{p}\right)$ is a group homomorphism.

   (b) Prove that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\ p),$$

   and that this determines $\left(\frac{a}{p}\right) \in \{\pm 1\}$ uniquely.

(c) Show that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{4}$.

(d) For $b \in \mathbb{F}_p^\times$, let $\sigma_b \in \mathrm{Gal}(E/\mathbb{Q})$ be the automorphism $\sigma_b(\zeta) = \zeta^b$. Prove the equality $\sigma_b(\tau) = \left(\frac{b}{p}\right) \cdot \tau$.

(e) Prove that $\mathbb{Q}(\tau)/\mathbb{Q}$ is the unique quadratic intermediate extension of $E/\mathbb{Q}$.

We now want to determine the extension $\mathbb{Q}(\tau)$ by computing τ^2 explicitly.

(f) Let $c \in \mathbb{F}_p^\times$. Show that

$$\sum_{a \in \mathbb{F}_p^\times} \zeta^{a(1+c)} = \begin{cases} -1 & \text{if } c \neq p-1 \\ p-1 & \text{if } c = p-1 \end{cases}$$

(g) Write

$$\tau^2 = \sum_{a \in \mathbb{F}_p^\times} \sum_{b \in \mathbb{F}_p^\times} \left(\frac{ab}{p}\right) \zeta^{a+b}.$$

Substituting $b = ac$ with $c \in \mathbb{F}_p^\times$, deduce that

$$\tau^2 = -\sum_{c=1}^{p-2} \left(\frac{c}{p}\right) + \left(\frac{-1}{p}\right)(p-1).$$

(h) Conclude: if $p \equiv 1 \pmod 4$, then $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{p})$; if $p \equiv 3 \pmod 4$, then $\mathbb{Q}(\tau) = \mathbb{Q}(i\sqrt{p})$.