Assignment 20

Galois correspondence. Simple extensions

1. Let $f = X^3 - 2 \in \mathbb{Q}[X]$ and consider its splitting field E. Recall from Assignment 16 that $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$. Write down the lattice of subgroups of S_3 and the corresponding fixed fields. Which of those are normal?

2. Let k be a field and $f \in k[X]$ a polynomial with distinct roots. Let E be the splitting field of f and enumerate the roots of f by $z_1, \ldots, z_n$ to fix an embedding $\mathrm{Gal}(E/k) \subset S_n$. Define the discriminant of f as

$$D(f) = \prod_{i<j} (z_i - z_j)^2.$$

   (a) Assume that $\mathrm{char}(k) \neq 2$. Prove that $D(f)$ is a square in k if and only if $\mathrm{Gal}(E/k) \subset A_n$.

   (b) Show that $\mathbb{F}_4/\mathbb{F}_2$ is a counterexample in characteristic 2 to the previous part.

3. Let L/k be a finite field extension and fix an embedding $L \subset \overline{k}$.

   (a) Show that there exists a minimal finite field extension E/k containing L which is the splitting field of some polynomial.

   (b) Show that if L/k is separable (i.e. the minimal polynomial over k of any element in L has distinct roots in $\bar{k}$), then E/k is Galois. In this case, E is called the *Galois closure of* L/k.

   Hint: Assignment 19, Exercise 3.

4. We say that a field extension L/k is *simple* if there exists $x \in L$ such that $L = k(x)$. In this exercise we will prove the following result:

   Lemma. A finite field extensions L/k is simple if and only if there are finitely many intermediate field extensions $L/F/k$.

   (a) Suppose $L = k(x)$ for some $x \in L$ and let $L/F/k$ be an intermediate extension. Let $f \in F[X]$ be the minimal polynomial of x over F and let $F_0 \subset F$ be the extension of k generated by the coefficients of f. Prove that $F = F_0$.

   Hint: Check that $F(x) = F_0(x)$ and compare degrees.

   (b) Conclude that if L/k is simple, then it contains only finitely many intermediate subextensions.

   Hint: In Part (a), f divides the minimal polynomial of x over k.

   (c) Let k be an infinite field and V a k-vector space. Suppose that $V_1, \ldots, V_m$ are finitely many proper subspaces of V. Prove by induction that $\bigcup_{i=1}^{m} V_i \neq V$.

   (d) Suppose that a finite field extension L/k contains only finitely many intermediate extensions. Prove that L/k is simple.

5. (*Primitive Element Theorem*) Let L/k be a finite separable field extension. Prove that there exists $x \in L$ such that $L = k(x)$, i.e. that L is simple.

   Hint: Use the preceding exercises.

6. Prove that the field extension $\mathbb{F}_p(s,t)/\mathbb{F}_p(s^p,t^p)$, where s and t are formal variables, contains infinitely many intermediate extensions.

   Hint: Use Exercise 4.