Assignment 24

Symmetric functions. Galois correspondence.

1. Let $f = X^3 - 2 \in \mathbb{Q}[X]$ and consider its splitting field E. Recall 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 with $\mathrm{char}(k) \neq 2$ and $n \geqslant 5$ an integer. Consider the field extension

$$E = k(Y_1, \ldots, Y_n)/k(e_1, \ldots, e_n) = K,$$

where $e_j \in k[Y_1, \ldots, Y_n]$ is, for each integer $1 \leqslant j \leqslant n$, the j-th elementary symmetric polynomial, so that $\mathrm{Gal}(E/K) = S_n$. Let $E/L/K$ be the unique intermediate non-trivial Galois extension. Find a polynomial $f \in K[X]$ whose splitting field is L/K. [*Hint:* What is $\mathrm{Gal}(E/L)$? And $\deg(f)$?]

3. Let k be a field and $f \in k[X]$ a polynomial with distinct roots and $E = \mathrm{Sf}(f)$. Write $R(f) = \{z_1, \ldots, z_n\}$ 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.

4. (*Artin-Schreier theory*) Let k be a field of characteristic $p > 0$ and $c \in k$ be such that $c \neq y^p - y$ for every $y \in k$. Let $f = X^p - X - c \in k[X]$ and $E = \mathrm{Sf}(f)$.

   (a) Let $x \in R(f)$. Prove that $x + \lambda \in R(f)$ for each $\lambda \in \mathbb{F}_p$.

   (b) Deduce: f is irreducible, $E = k(x)$ and $\mathrm{Gal}(E/k)$ is cyclic of order p.

   We know want to show that all p-cyclic field extensions in characteristic p are of this form. Let E/k be a finite Galois extension with $\mathrm{char}(k) = p$ and $\mathrm{Gal}(E/k) = \langle \sigma \rangle$ cyclic of order p.

   (c) Show that there exists $x \in E$ such that $\sigma(x) = x + 1$ [*Hint:* Assignment 23, Exercise 2(c)]

(d) Prove that $E = k(x)$ and that there exists $c \in k$ such that $\mathrm{irr}(E/k) = X^p - X - c$. [*Hint:* Consider $\prod_{\lambda=0}^{p-1}(X - \sigma^\lambda(x))$. How can you prove that $x^p - x \in k$?]

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

   (a) Show: there exists a minimal normal finite field extension E/k containing L.

   (b) Show: if L/k is separable, then E/k is Galois (it is called the *Galois closure of* L/k).

6. 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 want to 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 that $L = k(x)$ for some $x \in L$ and let $L/F/k$ be an intermediate extension. Let $f = \mathrm{irr}(x, F)$ and $F_0 \subset F$ the extension of k generated by the coefficients of f. Prove that $F = F_0$. [*Hint:* Notice 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 $\mathrm{irr}(x, k)$]

   (c) Let k be an infinite field and V a k-vector space. Suppose that $V_1, \ldots, V_m$ are finitely many vector subspaces of V, with $V_i \neq V$ for each i. Show that $\bigcup_{i=1}^m V_i \neq V$ [*Hint:* Induction on n]

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

7. (*Primitive Element Theorem*) Let L/k be a finite separable field extension. Prove that there exists $x \in L$ such that $L = k(x)$.

8. 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.