Dartmouth College
Mathematics 81/111 — Homework 7

1. Consider the splitting field L of $x^4 - 2$ over $\mathbb{Q}$. The goal will be to characterize the Galois group and to write down the complete lattice of subgroups of the Galois group and the corresponding lattice of intermediate fields of the splitting field.
   (a) Start by writing down some elements of the Galois group and prove they generate the whole group. Determine the isomorphism class of this group.
   (b) Next draw (and label) the lattice of subgroups of the Galois group.
   (c) Finally for each subgroup H, find generators for the corresponding fixed field so they have the form: $L^H = \mathbb{Q}(\alpha)$ or $\mathbb{Q}(\alpha, \beta)$. Identify conjugate fields and the automorphism that relates them.

2. Suppose that $f \in \mathbb{Z}[x]$ is an irreducible quartic whose splitting field over $\mathbb{Q}$ has Galois group isomorphic to the symmetric group S_4. You may find the lattice of subgroups of A_4 given below useful in this problem.
   (a) Show that A_4 is the only subgroup of index 2 in S_4.
   (b) Let θ be a root of f, and set $K = \mathbb{Q}(\theta)$. Prove that $K/\mathbb{Q}$ is an extension of degree four which contains no proper subfields.
   (c) Are there any Galois extensions of degree four which contain no proper subfields?

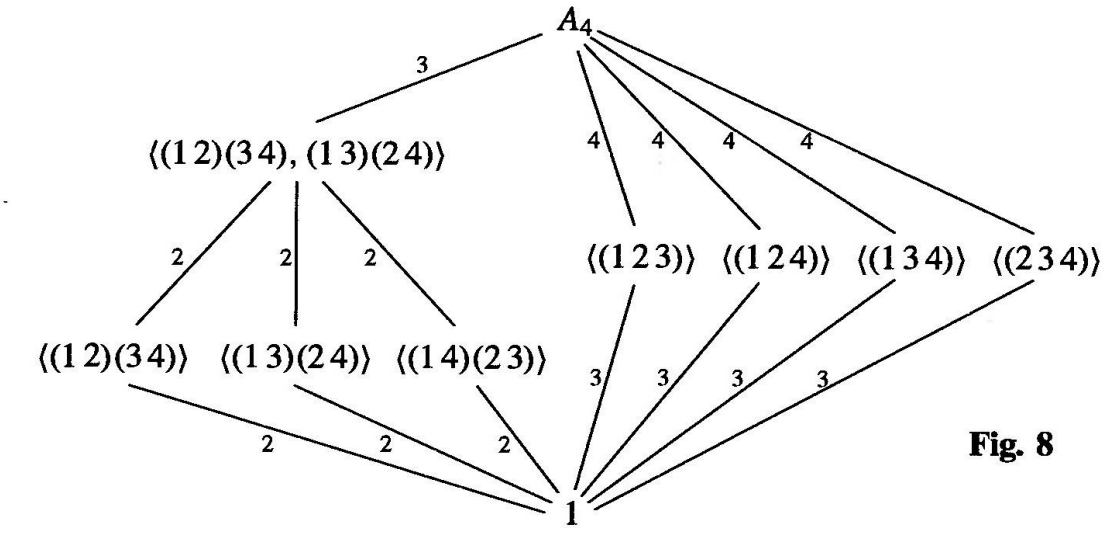

Figure 1: Lattice of Subgroups of A_4 from Dummit and Foote

3. Let L/K be a finite Galois extension of degree n, and put $G = Gal(L/K)$. Let $\alpha \in L$ and let $f = min_{\alpha,K}$ be its minimal polynomial, say of degree d. Let $h = \prod_{\sigma \in G}(x - \sigma(\alpha))$. Show that $h = f^{n/d}$.

4. Let $f \in \mathbb{Q}[x]$ be a polynomial of degree $n \geq 3$, and let K be the splitting field of f over $\mathbb{Q}$. Suppose that $\mathrm{Gal}(K/\mathbb{Q}) \cong S_n$, the symmetric group.
   (a) Show that f is irreducible.
   (b) If α is a root of f in K, show that $\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})$ is trivial.
   (c) If $n \geq 4$ and α a root of f, show that $\alpha^n \notin \mathbb{Q}$.

Some background. As preface to the next two problems, consider the following situation. Let $f \in K[x]$ be a separable polynomial of degree n, L its splitting field over K, and $G = \mathrm{Gal}(L/K)$. In the last homework set we showed that G embeds into the symmetric group via a homomorphism induced by the action of G on the n distinct roots, $\alpha_1, \ldots, \alpha_n$ of f. That is, we showed that each element $\sigma \in G$ permutes the α_i (transitively if f is irreducible) and that σ is completely determined by this action. This allows us to embed G as a subgroup of the symmetric group S_n.

Now viewing σ as a permutation, we can write σ in two useful fashions: (uniquely) as the product of disjoint cycles, or as a product of transpositions, where the only uniqueness in the later expression is that the number of transpositions always has the same parity. Permutations are called **even** or **odd** depending on the parity of this expression, and the set of even permutations forms a normal subgroup of index 2 in S_n called A_n, the alternating group.

So given $\sigma \in S_n$ consider its representation as a product of t disjoint cycles (including 1-cycles) having lengths $n_1, \ldots, n_t$. These cycle lengths form a partition of n, that is $n = n_1 + \cdots + n_t$. Also suppose that σ can be written as the product of s transpositions.

Then the **sign** of the permutation σ, $\mathrm{sign}(\sigma) = \pm 1$, can be defined equivalently as

$$\mathrm{sign}(\sigma) = (-1)^{n-t} = (-1)^s.$$

5. Now suppose that f is a monic, separable polynomial in $K[x]$, L its splitting field, and $\{\alpha_1, \ldots, \alpha_n\}$ its distinct roots. Define

$$\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j), \qquad D(f) = \Delta(f)^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

   The quantity $D(f)$ is called the **discriminant** of f.
   (a) Show that for an element $\sigma \in S_n$, $\sigma(\Delta(f)) = \mathrm{sign}(\sigma)\Delta(f)$.
   (b) Still identifying $\mathrm{Gal}(L/K)$ with its image in S_n, show that $D(f) \in K$.

(c) With the same identification of $\mathrm{Gal}(L/K) \subseteq S_n$, show that $\mathrm{Gal}(L/K) \subseteq A_n$ if and only if $\Delta(f) \in K$.

More background. If $f \in \mathbb{Z}[x]$ is a monic polynomial, then one can show $D(f) \in \mathbb{Z}$, and (as is clear from its definition) is nonzero iff f is separable. As a consequence if we consider f modulo p, it is separable iff $D(f) \not\equiv 0 \pmod{p}$, so if f is separable, so is its reduction mod p for all but the finite number of primes $p \mid D(f)$.

So suppose that $p \nmid D(f)$. Then we can write

$$f \equiv \overline{f}_1 \overline{f}_2 \dots \overline{f}_t \pmod{p},$$

where the $\overline{f}_i$ are irreducible in $\mathbb{F}_p[x]$ of degree n_i, so that the decomposition type of f modulo p $(n_1, \dots, n_t)$ is another partition of n. Note that I have purposely used the same notation n_i as well as the number t in both here and in the earlier discussion. This is justified by the theorem of Frobenius.

Theorem. (Frobenius) The density of the set of primes p for which f has decomposition type $n_1, \dots, n_t$ (modulo p) exists, and is equal to the number of $\sigma \in G$ (G the Galois group of f) with cycle type $n_1, n_2, \dots, n_t$.

So in particular, if $f \equiv \overline{f}_1 \overline{f}_2 \dots \overline{f}_t \pmod{p}$ as above, there is an element $\sigma \in G$ with cycle type $n_1, \dots, n_t$.

6. Let $f(x) = x^4 + 30x^2 + 45$. Show that the Galois group G of f over $\mathbb{Q}$ is cyclic of order 4. As a small hint, it is easy to show f is irreducible over $\mathbb{Z}$, and hence viewing G as a subgroup of S_4, it must be a transitive subgroup, and therefore one of $\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4, D_8$ (the group of order 8), A_4, or S_4. A starting point would be to show $|G| \leq 8$.