E. Dummit's Math 5111 ~ Algebra 1, Fall 2020 ~ Homework 11, due Fri Dec 4th.

Justify all responses with proof and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. You may use results from earlier parts of problems in later parts, even if you were unable to solve the earlier parts.

---

1. Find the number of monic irreducible polynomials over $\mathbb{F}_2$, and over $\mathbb{F}_3$, of degrees 6, 7, 8, 9, 10, 12, and 20.

---

2. Compute explicitly all of the intermediate fields of $\mathbb{Q}(\zeta_{19})/\mathbb{Q}$ and determine a generator for each. [Hint: Show that 2 generates $(\mathbb{Z}/19\mathbb{Z})^\times$.]

---

3. The goal of this problem is to identify some cyclotomic extensions containing a subgroup with Galois group isomorphic to $\mathbb{Z}/55\mathbb{Z}$.

   (a) Show there exists a subfield of $\mathbb{Q}(\zeta_{331})$ that is Galois over $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}/55\mathbb{Z}$.

   (b) Show there exists a subfield of $\mathbb{Q}(\zeta_{253})$ that is Galois over $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}/55\mathbb{Z}$. [Hint: $\mathbb{Z}/55\mathbb{Z} \cong (\mathbb{Z}/11\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$.]

---

4. Find a generator for each of the following extensions (make sure to justify why it is a generator):

   (a) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{7})/\mathbb{Q}$.

   (b) The splitting field of $x^{2019} - 2$ over $\mathbb{Q}$.

   (c) The unique subfield K of $\mathbb{Q}(\zeta_{29})$ with $[K : \mathbb{Q}] = 7$. [Hint: 2 generates $(\mathbb{Z}/29\mathbb{Z})^\times$.]

---

5. The goal of this problem is to compute the structure of $\mathrm{Gal}[\mathbb{Q}(\zeta_m)/\mathbb{Q}] \cong (\mathbb{Z}/m\mathbb{Z})^\times$. Recall that we have already shown that $(\mathbb{Z}/ab\mathbb{Z})^\times \cong (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$ when a and b are relatively prime, so it is enough to find the structure of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ when p is a prime. Let n be a positive integer.

   (a) If p is an odd prime, show that $1 + p$ is an element of order p^{n-1} in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. [Hint: Use the binomial theorem. Note that the number of factors of p in $k!$ is less than $k/(p-1)$.]

   (b) Let p be an odd prime and suppose a is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$, which we showed was cyclic of order $p - 1$. Show that the order of a in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is divisible by $p - 1$, and deduce that there is an element of order $p - 1$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

   (c) If p is an odd prime, prove that $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is a cyclic group of order $p^{n-1}(p-1)$.

   (d) If $n \geq 2$, show that 5 has order 2^{n-2} and that -1 and $1 + 2^{n-1}$ have order 2 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

   (e) If $n \geq 2$, show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is isomorphic to $(\mathbb{Z}/2^{n-2}\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

   (f) Write $(\mathbb{Z}/50\mathbb{Z})^\times$, $(\mathbb{Z}/600\mathbb{Z})^\times$, and $(\mathbb{Z}/202000\mathbb{Z})^\times$ as direct products of cyclic groups. [Hint: Combine (c) and (e).]

---

6. Let p be a prime. The goal of this problem is to determine the Galois group of $q(x) = x^p - 2$ over $\mathbb{Q}$. Let K be the splitting field of $q(x)$ over $\mathbb{Q}$ and recall that we have shown that $[K : \mathbb{Q}] = p(p-1)$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$.

   (a) Show that the automorphisms of $K/\mathbb{Q}$ are precisely the maps of the form $\sigma_{a,b}$ with $\sigma_{a,b}(\zeta_p, 2^{1/p}) = (\zeta_p^a, 2^{1/p}\zeta_p^b)$ for $a \in \mathbb{F}_p^\times$ and $b \in \mathbb{F}_p$.

   (b) Show that G is isomorphic to the group of matrices of the form $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ for $a \in \mathbb{F}_p^\times$ and $b \in \mathbb{F}_p$. [Hint: Show that the map sending $\sigma_{a,b}$ to the given matrix is a group isomorphism.]

   (c) Alternatively, we can use group theory to find the Galois group. Show that G has a subgroup K of order $p - 1$ and a normal subgroup H of order p. Deduce that G is a semidirect product $H \rtimes_\sigma K$. [Hint: Consider the subgroups corresponding to the subfields $\mathbb{Q}(2^{1/p})$ and $\mathbb{Q}(\zeta_p)$.]

---

7. Suppose $p(x) \in \mathbb{Q}[x]$ is an irreducible cubic polynomial whose Galois group is A_3. Show that all the roots of $p(x)$ are real.

---

8. Let p be a prime and $\overline{\mathbb{F}_p}$ be the algebraic closure of $\mathbb{F}_p$. Let $L = \overline{\mathbb{F}_p}(x, y)$ and $K = \overline{\mathbb{F}_p}(x^p, y^p)$ and note that $[L : K] = p^2$.

   (a) For any distinct $c, d \in \overline{\mathbb{F}_p}$ show that the fields $K(x + cy)$ and $K(x + dy)$ are distinct.

   (b) Deduce that L/K has infinitely many intermediate fields and is therefore not a simple extension.

---

9. Suppose G is a subgroup of S_n. Let F be any field and set $L = F(x_1, \cdots, x_n)$ and $E = F(s_1, \cdots, s_n)$ where s_i is the ith elementary symmetric function in the indeterminates x_j. If K is the fixed field of G inside L, show that L/K is Galois with $\mathrm{Gal}(L/K)$ is isomorphic to G. Conclude that every finite group appears as a Galois group of some field extension.
