Math 395 - Fall 2020
Homework 10

This homework is due on Friday, November 13 to your peer reviewer, and on Friday, November 20 on Gradescope.

1. Let ζ be a primitive 24th root of unity in $\mathbb{C}$, and let $K = \mathbb{Q}(\zeta)$.
   (a) Describe the isomorphism type of the Galois group of $K/\mathbb{Q}$.
   (b) Determine the number of quadratic extensions of $\mathbb{Q}$ that are subfields of K. (You need not give generators for these subfields.)
   (c) Prove that $\sqrt[4]{2}$ is not an element of K.

2. Let F be a field of characteristic zero and suppose that $F[x]$ contains a polynomial $f(x)$ of degree 6 whose roots are not expressible by radicals over F. Let E be a splitting field of f over F. Prove that $[E : F]$ is divisible by 10.
   (State clearly what facts you are quoting from either group theory or field theory. Do not assume that f is irreducible.)

3. Let $f(x)$ be an irreducible polynomial in $\mathbb{Q}[x]$ of degree n and let K be the splitting field of $f(x)$ in $\mathbb{C}$. Assume that $G = \mathrm{Gal}(K/\mathbb{Q})$ is *abelian*.
   (a) Prove that $[K : \mathbb{Q}] = n$ and that $K = \mathbb{Q}(\alpha)$ for every root α of $f(x)$.
   (b) Prove that G acts regularly on the set of roots of $f(x)$. (A group acts regularly on a set if it is transitive and the stabilizer of any point is the identity.)
   (c) Prove that either all the roots of $f(x)$ are real numbers or none of its roots are real.
   (d) Is the converse of (a) true? That is, if K is the splitting field of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ and $\alpha \in K$ is a root of f such that $K = \mathbb{Q}(\alpha)$, must $\mathrm{Gal}(K/\mathbb{Q})$ be abelian?

4. Let n be a given positive integer and let E_{2^n} be the elementary abelian group of order 2^n (the direct product of n copies of the cyclic group of order 2). Show that there is some positive integer N such that the cyclotomic field $\mathbb{Q}(\zeta_N)$ contains a subfield F that is Galois over $\mathbb{Q}$ with $\mathrm{Gal}(F/\mathbb{Q}) \cong E_{2^n}$, where ζ_N is a primitive Nth root of 1 in $\mathbb{C}$.

5. Put $\alpha = e^{\frac{2\pi i}{7}}$, and consider the field $K = \mathbb{Q}(\alpha)$. Find an element $x \in K$ such that $[\mathbb{Q}(x) : \mathbb{Q}] = 2$. (Proving that such x exists will earn you partial credit; for full credit, express x explicitly as a polynomial in α, such as $42\alpha^3 - 1337\alpha^5$, for example.)

6. Let F be a field of characteristic 0 and let $f \in F[x]$ be an irreducible polynomial of degree > 1 with splitting field $E \supset F$. Define $\Omega = \{\alpha \in E : f(\alpha) = 0\}$.

(a) Let $\alpha \in \Omega$ and let m be a positive integer. If $g \in F[x]$ is the minimal polynomial of α^m over F, show that $\{\beta^m : \beta \in \Omega\}$ is the set of roots of g.

(b) Now fix $\alpha \in \Omega$ and suppose that $\alpha r \in \Omega$ for some $r \in F$. Show that, for all $\beta \in \Omega$ and integers $i \geq 0$, we have $\beta r^i \in \Omega$. Conclude that r is a root of unity.

(c) If α and r are as in (b) and if m is the multiplicative order of the root of unity r, show that $f(x) = g(x^m)$, where g is the minimal polynomial of α^m over F.