Galois Theory
Assignment 2

Questions will be marked both on correctness and clarity of presentation. If outside resources are used in completing the assignment, references are expected.

1. The following question is from Dummit and Foote, cf. Milne 3-3. Let $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$, where we take only positive real square roots. Set $E = \mathbb{Q}(\alpha)$.

   (a) Show that $a = (2+\sqrt{2})(3+\sqrt{3})$ is not a square in $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. [Hint: Suppose $a = c^2$ for some $c \in F$. If $\phi \in Gal(F/\mathbb{Q})$ fixes $\mathbb{Q}(\sqrt{2})$, show $a\phi(a) = (c\phi(c))^2$ and that $c\phi(c) = N_{F/\mathbb{Q}(\sqrt{2})}(c) \in \mathbb{Q}(\sqrt{2})$, implying $\sqrt{6} \in \mathbb{Q}(\sqrt{2})$.]

   (b) Use (a) to conclude that $[E : \mathbb{Q}] = 8$. Prove that the roots of the minimal polynomial for α over $\mathbb{Q}$ are $\pm\sqrt{(2\pm\sqrt{2})(3\pm\sqrt{3})}$.

   (c) Show that E is a Galois extension. One way to do this is to show that if $\beta = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$ then $\alpha\beta \in F$, so $\beta \in E$, similarly for other roots. Other approaches are welcome. Explain why the elements of $Gal(E/\mathbb{Q})$ are exactly the eight automorphisms determined by sending α to one of the 8 roots in (b).

   (d) Let $\sigma \in Gal(E/\mathbb{Q})$ be the element mapping α to β, show that σ is an element of order 4. [Hint: Show that $\sigma(\alpha^2) = \sigma(\beta^2)$ and so $\sigma(\sqrt{2}) = -\sqrt{2}$, and $\sigma(\sqrt{3}) = \sqrt{3}$. Conclude $\sigma(\alpha\beta) = -\alpha\beta$ and so $\sigma(\beta) = -\alpha$.]

   (e) Define τ by $\tau(\alpha) = \sqrt{(2+\sqrt{2})(3-\sqrt{3})}$, show that τ has order four and that σ and τ generate $Gal(E/\mathbb{Q})$. Prove that $\sigma^2 = \tau^2$, and that $\sigma\tau = \tau\sigma^3$. Use these relations to show that the Galois group is Q_8, by establishing an isomorphism between the group described by the generators τ, σ with relations as above, and one of the standard presentations of Q_8.

2. Compute the Galois group of $x^4 + px + p$, where p is and odd prime [Hint: There are three cases to consider].

3. (Milne) Show that if $f(x)$ is an irreducible polynomial over $\mathbb{Q}$ with both real and nonreal roots, then its Galois group is nonabelian. Can we drop the assumption that $f(x)$ is irreducible? If not, provide a counterexample to show why not.

4. (Milne) Show that any finite extension of $\mathbb{Q}$ can contain at most finitely many roots of 1.

5. The following question is from Dummit and Foote. Show that the primitive n^{th} roots of unity form a basis over $\mathbb{Q}$ for the cyclotomic field of n^{th} roots of unity if and only if n is square-free. (Remark: You may be able to develop a shorter proof than intended by Dummit and Foote, by appealing to the normal basis theorem).

6. Suppose that G is the Galois group of L/K, a finite Galois extension. Since G acts on L, we can consider L as a KG-module. Show that L/K has a normal basis if and only if L is a free KG-module.

7. Suppose that $K = \mathbb{F}_{p^n}$, $p > 2$, and let L be a finite extension of K such that L/K is Galois. Compute the size of the kernel of $N_{L/K}$, i.e. the number of elements $\alpha \in L$ satisfying $N_{L/K}(\alpha) = 1$.