Math 395 - Fall 2020
Homework 11

This homework is due on Friday, November 20 to your peer reviewer, and on Friday, December 4 on Gradescope.

1. Let p be a prime, let $\mathbb{F}_p$ be the field of order p, and let $\overline{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}$. Let n be a positive integer relatively prime to p and let F_n be the splitting field of the polynomial $f_n(x)$ in $\overline{\mathbb{F}}_p$, where
$$f_n(x) = x^n - 1.$$
   (a) Explain briefly why $[F_n : \mathbb{F}_p]$ is equal to the order of p in the multiplicative subgroup $(\mathbb{Z}/n\mathbb{Z})^\times$. (You can quote without proof basic facts you need about finite fields.)
   (b) If n and m are relatively prime and neither is divisible by p, is $F_{nm} = F_n F_m$?

2. Let p be a prime, let $\mathbb{F}_p$ be the field of order p, and let $f(x)$ be a nonconstant polynomial in $\mathbb{F}_p[x]$. Assume that f factors as
$$f(x) = q_1(x)^{\alpha_1} q_2(x)^{\alpha_2} \dots q_r(x)^{\alpha_r} \tag{1}$$
for some distinct irreducible polynomials $q_1, \dots, q_r$ in $\mathbb{F}_p[x]$ and $\alpha_1, \dots, \alpha_r \in \mathbb{Z}^+$. Let E be a splitting field of f over $\mathbb{F}_p$.
   (a) Give an expression for $[E : \mathbb{F}_p]$ in terms of the q_i in equation (1). (Hint: Your answer should only involve the degrees of the q_is and not depend on the α_is.)
   (b) Fix a natural number N and assume $q_1, \dots, q_r$ are *all* the distinct irreducible polynomials of degree $\leq N$ in $\mathbb{F}_p[x]$. Find an expression for $[E : \mathbb{F}_p]$, where f is as in equation (1).

3. Let q be a power of a prime, let $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q) = \langle \sigma \rangle$ (note that σ has order 2). Let N be the usual *norm map* for this extension:
$$N \colon \mathbb{F}_{q^2}^\times \to \mathbb{F}_q^\times \quad \text{given by} \quad N(x) = x\sigma(x).$$
   (a) What is the degree of the extension $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$? Describe how the Frobenius automorphism for this extension acts on the elements of $\mathbb{F}_{q^2}$. What is its relationship to σ above?
   (b) Prove that N is surjective.
   (c) Show that $\mathbb{F}_{q^2}^\times$ has an element of order $q+1$ whose norm is 1.
   (d) Compute the following index: $[\mathbb{F}_q^\times : N(\mathbb{F}_q^\times)]$.

4. Let K be a field with 625 elements.

(a) How many elements of K are primitive (field) generators for the extension $K/\mathbb{F}_5$? (Justify.)

(b) How many nonzero elements are generators of the multiplicative group $K^\times$? (Justify.)

(c) How many nonzero elements of K satisfy $x^{75} = x$? (Justify.)

(d) Let F be the subfield of K with 25 elements. How many elements a in F are there such that $K = F(\sqrt{a})$?

5. Let K be the field $\mathbb{F}_q(t)$ and let $L = \mathbb{F}_q(t^{1/p})$. The extension L/K is inseparable, and thus not Galois. What is the degree $[L : K]$? Explain why there are no nontrivial field automorphisms of L fixing K.

6. Let $\mathbb{C}(x)$ be the field of rational functions with complex coefficients of the variable x. Thus, x is transcendental over $\mathbb{C}$. Put

$$y = x^n + x^{-n} \in \mathbb{C}(x)$$

for some $n > 0$. Prove that the field extension $\mathbb{C}(x)/\mathbb{C}(y)$ is a finite Galois extension and find its degree.