Math 395 - Fall 2021
Qual problem set 12

This homework is “due” on Monday December 6 at 11:59pm.

You may also (in addition to or instead of turning this in as a homework, your choice) use this assignment as a quiz. In this case, give yourself one hour to solve two of these problems completely.

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 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: $[\mathbb{F}_q^\times : N(\mathbb{F}_q^\times)]$.

3. 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 $K = F(\sqrt{a})$?

4. (a) How many distinct roots does the polynomial $x^3 - 1$ have in $\overline{\mathbb{F}}_3$?

(b) How many distinct roots does the polynomial $x^7 - 1$ have in $\overline{\mathbb{F}}_3$?

(c) Let K be the splitting field of $x^7 - 1$ over $\mathbb{F}_3$. What is the degree of K over $\mathbb{F}_3$?

(d) Draw the lattice of all subfields of K. (You need not give generators for these subfields.)

(e) How many elements $\alpha \in K$ generate the multiplicative group $K^\times$?

(f) How many primitive elements are there for the extension $K/\mathbb{F}_3$? (In other words, how many β are there such that $K = \mathbb{F}_3(\beta)$?)