Math 200b Winter 2022 Homework 7

Complete before final exam, but no need to hand in

1. (a). Suppose that K/F is a Galois extension with $[K : F] = p^n$ for some prime p and $n \geq 1$. Show that there are intermediate fields $F \subseteq E_1 \subseteq K$, $F \subseteq E_2 \subseteq K$ such that E_i/F is Galois for $i = 1, 2$ and $[E_1 : F] = p$, $[E_2 : F] = p^{n-1}$.

(b). Suppose that $f \in \mathbb{Q}[x]$ is irreducible of degree 4 over $\mathbb{Q}$, and that its splitting field K over $\mathbb{Q}$ satisfies $\mathrm{Gal}(K/\mathbb{Q}) \cong S_4$. Show that there is a field $\mathbb{Q} \subseteq E \subseteq K$ such that $[E : \mathbb{Q}] = 4$ and there are no proper intermediate fields between $\mathbb{Q}$ and E.

2. Let p be prime and let $\mathbb{F}_{p^n}$ be a field with p^n elements. Let S be the set of generators (as a group) of the multiplicative group $(\mathbb{F}_{p^n})^*$.

(a). Let $f \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree n. Show that f splits in $\mathbb{F}_{p^n}$ and that either all of its roots are in S or none of them is. (hint: for any two roots of f, there is an automorphism sending one to the other).

(b). Show that $n \,|\, \varphi(p^n - 1)$ for all primes p and all $n \geq 1$, where φ is the Euler phi-function. (hint: use part (a)).

(c). Consider the explicit case of the field $\mathbb{F}_{16}$. Find all irreducible polynomials of degree 4 over $\mathbb{F}_2$. Which ones have roots in S?

3. Let $\zeta \in \mathbb{C}$ be a primitive pth root of 1 for some prime $p \geq 3$. Let $K = \mathbb{Q}(\zeta)$ be the splitting field of $x^p - 1$ inside $\mathbb{C}$.

(a). Let $\alpha = \sum_{i=0}^{p-1} \zeta^{i^2}$. This is called a *Gauss sum*. Prove that $E = \mathbb{Q}(\alpha)$ is the unique subfield of K such that $[E : \mathbb{Q}] = 2$.

(b). Show that $L = \mathbb{Q}(\zeta + \zeta^{-1})$ is the unique subfield of K such that $[K : L] = 2$. Show that in fact $L = K \cap \mathbb{R}$. (Hint: note that complex conjugation restricts to an automorphism of K).

4. Let $f = x^p - 2$ for some prime $p \geq 3$. Consider the splitting field K of f over $\mathbb{Q}$. Show that $K/\mathbb{Q}$ is Galois with $[K : \mathbb{Q}] = p(p-1)$. Prove that $G = \mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the semidirect product $\mathbb{Z}_p^* \ltimes_\psi \mathbb{Z}_p$, where $\psi : \mathbb{Z}_p^* \to \mathrm{Aut}(\mathbb{Z}_p)$ is the natural isomorphism.