Math 200b Winter 2020 Homework 8

Due 3/13/2020 in class or by 5pm in Jake Postema's mailbox.

1. Let $\pm\alpha, \pm\beta$ be the roots of the polynomial $f(x) = x^4 + ax^2 + b \in \mathbb{Z}[x]$.

(a). Prove that f is irreducible over $\mathbb{Q}$ if and only if $\alpha^2, \alpha+\beta$, and $\alpha-\beta$ are not elements of $\mathbb{Q}$.

(b). Suppose that f is irreducible and let $G = \mathrm{Gal}(K/\mathbb{Q})$ where K is the splitting field of f over $\mathbb{Q}$. Show that G is one of three possibilities, determined as follows:

1. $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ if and only if $\alpha\beta \in \mathbb{Q}$.
2. $G \cong \mathbb{Z}_4$ if and only if $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\alpha^2)$.
3. $G \cong D_8$, the dihedral group of order 8, if and only if $\alpha\beta \notin \mathbb{Q}(\alpha^2)$.

(Hint: first show there are only 8 possible ways an element of G can permute the roots of f.)

(c). Give examples of polynomials f showing that each of the three cases in part (b) can occur.

2. Let $q = p^m$ be a power of the prime p. Let $\mathbb{F}_q = \mathbb{F}_{p^m}$ be the finite field with q elements. Let $\sigma_q : \mathbb{F}_q \to \mathbb{F}_q$ be the defined by $\sigma(a) = a^q$ for all $a \in \mathbb{F}_q$. This is the mth power of the Frobenius automorphism, so it is also an automorphism.

(a). Prove that every finite extension of $\mathbb{F}_q$ of degree n is the splitting field of $x^{q^n} - x$ over $\mathbb{F}_q$, hence is unique up to isomorphism.

(b). Prove that if K is an extension of $\mathbb{F}_q$ with $[K : \mathbb{F}_q] = n$, then $\mathrm{Gal}(K/\mathbb{F}_q)$ is cyclic with σ_q as a generator.

(c). With K as in (b), prove that the intermediate fields $\mathbb{F}_q \subseteq E \subseteq K$ are exactly the subfields $E_d = \{a \in K | a^{q^d} = a\}$ as d varies over the divisors of n.

3. Let $\zeta \in \mathbb{C}$ be a primitive pth root of 1 for some prime $p > 2$. 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 be a field of characteristic $p > 0$, and let $\mathbb{F}_p$ be its prime subfield. Let K be the splitting field of F of the polynomial $f(x) = x^p - x - a \in F[x]$. Let $\alpha \in K$ be a root of f and assume that $\alpha \notin F$. Show that

(a). $\alpha + i$ is also a root of f, for all $i \in \mathbb{F}_p$.

(b). $K = F(\alpha)$.

(c). f is separable and irreducible in $F[x]$, and K/F is Galois. (hint: all roots of f have minimal polynomials over F of the same degree).

(d). There is an automorphism $\sigma \in G = \text{Gal}(K/F)$ such that $\sigma(\alpha) = \alpha + 1$. The automorphism σ has order p and G is cyclic of order p.

(Remark: an extension of the type in this problem is called an *Artin-Schreier Extension.*)