Math 200b Winter 2021 Homework 8

Due 3/12/2021 by midnight on Gradescope

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 there are three possibilities for G, determined as follows:

(i) $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ if and only if $\alpha\beta \in \mathbb{Q}$.

(ii) $G \cong \mathbb{Z}_4$ if and only if $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\alpha^2)$.

(iii) $G \cong D_8$, the dihedral group of order 8, if and only if $\alpha\beta \notin \mathbb{Q}(\alpha^2)$.

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.

(b). Show that $n \mid \varphi(p^n - 1)$ for all primes p and all $n \geq 1$, where φ is the Euler phi-function.

(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.