MAT205 Assignment 2

You may use any result proved in the lectures or stated in Fraleigh's textbook without reproving it, provided you quote it clearly.

Problem 1. The Splitting Field of $x^4 - 2$ over $\mathbb{Q}$

Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$, let $\sqrt[4]{2}$ denote the real positive fourth root of 2, and let $i = \sqrt{-1}$. Write E for the splitting field of f over $\mathbb{Q}$ inside $\mathbb{C}$.

a. Prove that f is irreducible over $\mathbb{Q}$, and determine $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$.

b. Find all roots of f in $\mathbb{C}$, prove that the splitting field is $E = \mathbb{Q}(\sqrt[4]{2},\, i)$, and determine $[E : \mathbb{Q}]$.

c. Prove that $E/\mathbb{Q}$ is a Galois extension, and state $|\operatorname{Gal}(E/\mathbb{Q})|$.

d. Let $\sigma, \tau \in \operatorname{Gal}(E/\mathbb{Q})$ be the automorphisms determined by

$$\sigma :\ \sqrt[4]{2} \mapsto i\sqrt[4]{2},\quad i \mapsto i, \qquad\qquad \tau :\ \sqrt[4]{2} \mapsto \sqrt[4]{2},\quad i \mapsto -i.$$

Prove that σ and τ generate $\operatorname{Gal}(E/\mathbb{Q})$, determine the order of each and the power of σ equal to $\tau\sigma\tau^{-1}$, and conclude that $\operatorname{Gal}(E/\mathbb{Q}) \cong D_4$.

e. Write out the eight elements of $\operatorname{Gal}(E/\mathbb{Q})$ as $\sigma^a\tau^b$, determine the order of each, and determine the centre $Z(\operatorname{Gal}(E/\mathbb{Q}))$.

f. Determine all subgroups of $\operatorname{Gal}(E/\mathbb{Q})$.

g. For each subgroup H, determine the fixed field E^H, and present the Galois correspondence as a table listing H, E^H, and $[E^H : \mathbb{Q}]$. Then draw the subgroup lattice and the lattice of intermediate fields side by side, indicating how the correspondence matches them.

h. Determine which intermediate fields are normal over $\mathbb{Q}$. Prove that $\mathbb{Q}(\sqrt[4]{2})$ is **not** normal over $\mathbb{Q}$, and determine $\operatorname{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$.

i. Determine the commutator subgroup $[\operatorname{Gal}(E/\mathbb{Q}), \operatorname{Gal}(E/\mathbb{Q})]$, and hence determine the largest intermediate field K (with $\mathbb{Q} \subseteq K \subseteq E$) such that $K/\mathbb{Q}$ is Galois with $\operatorname{Gal}(K/\mathbb{Q})$ abelian. Identify $\operatorname{Gal}(K/\mathbb{Q})$.

Problem 2. Counting Irreducible Polynomials over Finite Fields

Let q be a prime power. You may use the following facts from the lectures without proof: for each $n \geq 1$ there is a unique field $\mathbb{F}_{q^n}$ with q^n elements; the Frobenius map $\operatorname{Fr}(\alpha) = \alpha^q$ generates the Galois group $\operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, which is cyclic of order n; and $\mathbb{F}_{q^n}$ contains a subfield with q^d elements if and only if $d \mid n$ (and the subfield is then unique).

a. For $\alpha \in \mathbb{F}_{q^n}$, prove that the $\langle \operatorname{Fr} \rangle$-orbit

$$\{\alpha,\ \operatorname{Fr}(\alpha),\ \operatorname{Fr}^2(\alpha), \dots\} = \{\alpha,\ \alpha^q,\ \alpha^{q^2}, \dots\}$$

has size $[\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ and equals the set of roots of the minimal polynomial of α over $\mathbb{F}_q$. Deduce that the monic irreducible polynomials of degree d over $\mathbb{F}_q$ are in bijection with the $\langle \operatorname{Fr} \rangle$-orbits of size d.

b. Take $n = 6$. Determine all subfields of $\mathbb{F}_{q^6}$, the possible degrees over $\mathbb{F}_q$ of the elements of $\mathbb{F}_{q^6}$, and hence the possible sizes of the $\langle \operatorname{Fr} \rangle$-orbits contained in $\mathbb{F}_{q^6} \setminus \mathbb{F}_q$.

c. By counting the elements of $\mathbb{F}_{q^6}$ of each degree over $\mathbb{F}_q$, determine the number of monic irreducible polynomials over $\mathbb{F}_q$ of degree 2, of degree 3, and of degree 6.