Math 401 Problem Set 11 (due Wednesday, April 22, 2026)

Problem 1. According to Problem 7 on Problem Set 10, the automorphisms of $\mathbb{F}_{64}$ are given by σ^k for $0 \le k \le 5$, where

$$\sigma\colon \mathbb{F}_{64} \to \mathbb{F}_{64}, \quad \sigma(x) = x^2.$$

In view of this, determine all automorphisms of the extension $\mathbb{F}_{64}/\mathbb{F}_4$.

Problem 2. Determine the automorphism group of the extension $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})/\mathbb{Q}$. Is this extension Galois?

Problem 3. Let K/F be a Galois extension, and let $F \subseteq L \subseteq K$ be an intermediate field. For each of the following statements, either explain why it is true or provide a counterexample.

(a) The extension K/L is necessarily Galois.

(b) The extension L/F is necessarily Galois.

Problem 4. Determine the Galois group and all intermediate fields of the extension $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$.

Problem 5. For each polynomial f below, let K be the splitting field of f over $\mathbb{Q}$. Determine the Galois group of the extension $K/\mathbb{Q}$.

(a) $f(x) = x^3 - 2x + 3$.

(b) $f(x) = x^3 - 7x + 6$.

Problem 6. For each polynomial f below, let K be the splitting field of f over $\mathbb{Q}$. Determine the Galois group of $K/\mathbb{Q}$, and all intermediate fields L which are Galois over $\mathbb{Q}$.

(a) $f(x) = x^4 - 10x^2 + 1$.

(b) $f(x) = x^4 - 10x^2 + 2$.

(For this problem, you may assume that these polynomials are irreducible.)

Problem 7 (Eisenstein criterion)**. (Optional)** Let $f(x) = a_n x^n + \cdots + a_0$ be an integer polynomial such that

- p divides $a_0, \ldots, a_{n-1}$,
- p does not divide a_n,
- p^2 does not divide a_0.

(a) Show that if $f = gh$ for nonconstant polynomials $g, h \in \mathbb{Z}[x]$, then g and h both have constant term divisible by p.

(*Hint.* Consider the equation $\overline{f} = \overline{g} \cdot \overline{h}$ in $\mathbb{F}_p[x]$, where $\overline{f}$, $\overline{g}$, $\overline{h}$ denote the image of f, g, h under the reduction modulo p map $\mathbb{Z}[x] \to \mathbb{F}_p[x]$.)

(b) Conclude that f is irreducible in $\mathbb{Q}[x]$.

Problem 8. (Optional) Let p be a prime, and let $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$. Show that $f(x+1)$ is irreducible in $\mathbb{Q}[x]$, and thus f is also irreducible in $\mathbb{Q}[x]$.

(*Hint.* Use the Eisenstein criterion (Problem 7) and the fact that $f(x) = \frac{x^p-1}{x-1}$. You may use without proof the fact that $\binom{p}{i}$ is divisible by p for $0 < i < p$.)

Problem 9. (Optional) For $n \geq 1$, let $\zeta_n = e^{2\pi i/n}$. Determine all subfields of the following extensions.

(a) $\mathbb{Q}(\zeta_5)$, (b) $\mathbb{Q}(\zeta_7)$.

Problem 10. (Optional) As above, let $\zeta_n = e^{2\pi i/n}$.

(a) Show that any automorphism σ of $\mathbb{Q}(\zeta_n)$ must send ζ_n to ζ_n^k for some $k \in (\mathbb{Z}/n\mathbb{Z})^\times$.

(b) Show that the Galois group of $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/12\mathbb{Z})^\times$.

In fact, it can be shown that the Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is always isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, but you are not asked to prove this in general here.

Problem 11. Approximately how long did you spend on this problem set? (Round to the nearest half-hour.)

Bonus problem (not graded). Let K be the splitting field of $x^5 - 2$ over $\mathbb{Q}$. Show that the Galois group of $K/\mathbb{Q}$ is not isomorphic to S_5.

Bonus problem (not graded). Prove that the polynomial $x^4 - 10x^2 + 1$ is reducible in $\mathbb{F}_p[x]$ for every prime p.