

Math 401 Problem Set 10 (due Friday, April 10, 2026)

Problem 1. For each of the following field extensions K/\mathbb{Q} , determine the degree $[K : \mathbb{Q}]$ of the extension, and give a basis of K over \mathbb{Q} .

- (a) $K = \mathbb{Q}[x]/(x^3 - x - 1)$.
- (b) $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.
- (c) $K = \mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/6}$.

Problem 2. Let K/\mathbb{Q} be an extension of \mathbb{Q} such that $[K : \mathbb{Q}] = 2$. Show that K is isomorphic to $\mathbb{Q}(\sqrt{d})$ for some integer d .

Problem 3. (Exercise 14.4.2 (a), (b), (d)) Determine the irreducible polynomial for $\alpha = \sqrt{3} + \sqrt{5}$ over the following fields.

- (a) \mathbb{Q} , (b) $\mathbb{Q}(\sqrt{5})$, (c) $\mathbb{Q}(\sqrt{15})$.

Problem 4.

- (a) Factor $x^3 - 2$ over $\mathbb{Q}(\sqrt[3]{2})$. Does $x^3 - 2$ split in $\mathbb{Q}(\sqrt[3]{2})$?
- (b) Let $\zeta = e^{2\pi i/5}$ be a fifth root of unity. Does $x^5 - 1$ split in $\mathbb{Q}(\zeta)$?

Problem 5. Give an explicit isomorphism $\mathbb{F}_5[x]/(x^2 + x + 1) \rightarrow \mathbb{F}_5[x]/(x^2 + 3)$.

Problem 6. Find the number of irreducible polynomials of degree 7 in $\mathbb{F}_5[x]$.

Problem 7. Let p be a prime, and let $r \geq 1$ be an integer.

- (a) Show that the map

$$\sigma: \mathbb{F}_{p^r} \rightarrow \mathbb{F}_{p^r}, \quad \sigma(x) = x^p$$

is a field automorphism, i.e., it is a ring isomorphism from \mathbb{F}_{p^r} to itself.

(You may use without proof the fact that the binomial coefficient $\binom{p}{i}$ is divisible by p for $0 < i < p$.)

- (b) Show that $\sigma(x) = x$ if and only if $x \in \mathbb{F}_p$.
- (c) For $k \geq 0$, let σ^k denote σ composed with itself k times, i.e.,

$$\sigma^k := \underbrace{\sigma \circ \cdots \circ \sigma}_{k \text{ times}}.$$

Show that σ^r is the identity map, i.e., $\sigma^r(x) = x$ for all $x \in \mathbb{F}_{p^r}$.

- (d) Show that there are exactly r automorphisms of \mathbb{F}_{p^r} , given by the powers of σ .

Problem 8. Approximately how long did you spend on this problem set? (Round to the nearest half-hour.)