

MAT 5173 — Problem Set 3

Due Monday 2 November 2026, at the start of the Q&A session.

This set covers the five meetings of 14 through 28 October: principal ideal domains, Euclidean domains and irreducible polynomials (Ash §2.7–§2.9), field extensions, degree and simple extensions (§3.1), splitting fields and algebraic closures (§3.2–§3.3), and separability, normal extensions and finite fields (§3.4–§3.5, §6.4; two meetings). Affine varieties now begin on 4 November, so the problem on them has moved to Problem Set 4.

Maximum six pages. Each problem is scored on *completeness* alone, not on correctness: **2** for a nominally complete solution, **1** for a clearly partial one, **0** for nothing submitted or for filler with no substance. Any submission containing non-human-readable content, stray characters, or unproofread AI output scores 0 for that item.

Sources. AI assistance, solution keys (Ash prints them at the back), collaboration and the internet are all permitted, without restriction. Include one line naming what you used. Note that at the Q&A session we name the problem you are to explain; you do not choose, so be ready on every problem on this set.

Notation. We follow Ash throughout. Every ring on this set is commutative with identity. For fields $F \leq E$, $[E : F]$ is the degree of the extension, $F(\alpha)$ the subfield of E generated by F and α , $\min(\alpha, F)$ the minimal polynomial of α over F , and $\text{Gal}(E/F)$ the group of F -automorphisms of E ; $\mathbb{F}_p$ is the field with p elements. We write $\langle a_1, \dots, a_k \rangle$ for the ideal generated by $a_1, \dots, a_k$. Problems 1, 2 and 4 share the polynomial $x^3 - 3x + 1$; a later part may quote an earlier one.

Problem 1 (principal ideal domains, Euclidean domains, irreducible polynomials) — §2.7, §2.9

1. Let R be a principal ideal domain. Prove that every nonzero prime ideal of R is maximal. Deduce, from Problem 2(2) of Set 2, that $\mathbb{Z}[x]$ is not a principal ideal domain, and show likewise that $F[x, y]$ is not one for any field F .
2. In the Gaussian integers $\mathbb{Z}[i]$, a Euclidean domain with $\Psi(a + bi) = a^2 + b^2$ (Ash 2.7.5), run the Euclidean algorithm on

$$\alpha = 21 + 8i \quad \text{and} \quad \beta = 9 - 3i.$$

Find a greatest common divisor δ of α and β , write $\delta = \mu\alpha + \nu\beta$ with $\mu, \nu \in \mathbb{Z}[i]$, and show that δ is irreducible in $\mathbb{Z}[i]$. (*At each step, divide in $\mathbb{Q}(i)$ and round both coordinates to a nearest integer.*)

3. Let $g(x) = x^3 - 3x + 1$. Prove that if $g(x + c)$ is irreducible in $\mathbb{Z}[x]$ for some $c \in \mathbb{Z}$, then so is $g(x)$. Find such a c for which Eisenstein's criterion applies to $g(x + c)$, and conclude, naming the result you use, that g is irreducible in $\mathbb{Q}[x]$ as well.

Problem 2 (field extensions and simple extensions) — §3.1

1. Let $F \leq E$ be fields, and let $\alpha \in E$ be algebraic over F with minimal polynomial $m(x)$. Prove that evaluation $\varphi: F[x] \rightarrow E$, $\varphi(f) := f(\alpha)$, is a ring homomorphism with kernel $\langle m \rangle$ and image $F[\alpha]$. Deduce that $F[\alpha] \cong F[x]/\langle m \rangle$, that $F[\alpha]$ is a field, and hence that $F[\alpha] = F(\alpha)$.
 2. Let $\alpha \in \mathbb{R}$ be a root of $g(x) = x^3 - 3x + 1$. Explain why $1, \alpha, \alpha^2$ is a basis of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Then express α^4 and $(\alpha + 1)^{-1}$ in that basis.
 3. Let $F \leq K \leq L$ be fields, with $[K : F] = m$ finite, and let $\alpha \in L$ be algebraic over F of degree n , with $\gcd(m, n) = 1$. Prove that $[K(\alpha) : K] = n$; that is, $\min(\alpha, F)$ remains irreducible over K . Deduce, without any computation, that $x^3 - 2$ is irreducible over $\mathbb{Q}(i)$.
-

Problem 3 (splitting fields and algebraic closures) — §3.2–§3.3

1. Let $f \in F[x]$ be irreducible of degree n , and let K be a splitting field for f over F . Prove that n divides $[K : F]$, and that $[K : F] \leq n!$. Conclude that the splitting field of an irreducible cubic has degree 3 or 6.
 2. Let $f(x) = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$. Show that f is irreducible, and find its four complex roots. Let $\alpha = \sqrt{1 + \sqrt{3}}$, the positive real root. Show that the splitting field of f is $K = \mathbb{Q}(\alpha, \sqrt{-2})$, and that $[K : \mathbb{Q}] = 8$, neither 4 nor $4! = 24$. (*Multiply a real root by an imaginary one.*)
 3. Prove that an algebraically closed field is infinite. (*Given a finite field F , write down a polynomial over F with no root in F .*) Conclude that an algebraic closure of $\mathbb{F}_p$ is an algebraic extension of $\mathbb{F}_p$ that is not finite.
-

Problem 4 (separability, normal extensions, finite fields) — §3.4–§3.5, §6.4

1. Let p be prime, $q = p^n$ with $n \geq 1$, and let L be a splitting field of $f(x) = x^q - x$ over $\mathbb{F}_p$.
 - a. Using the derivative, show that f has q distinct roots in L .
 - b. Prove that the set of roots of f in L is a subfield of L . Conclude that a field with exactly q elements exists.
 2. Let $\alpha \in \mathbb{R}$ be a root of $g(x) = x^3 - 3x + 1$, as in Problem 2(2).
 - a. Verify that $\alpha^2 - 2$ and $2 - \alpha - \alpha^2$ are also roots of g . Conclude that $\mathbb{Q}(\alpha)$ is a splitting field of g over $\mathbb{Q}$, hence a normal extension of degree 3.
 - b. Show that $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ has order 3 and is generated by the automorphism σ with $\sigma(\alpha) = \alpha^2 - 2$. Contrast this with $\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ (Ash 3.5.10), and say which hypothesis of Ash 3.5.9 fails there.
 3. Let $K = \mathbb{F}_2[x]/\langle x^4 + x + 1 \rangle$, and let $\beta \in K$ be the class of x .
 - a. Show that $x^4 + x + 1$ is irreducible over $\mathbb{F}_2$, so that K is a field with 16 elements.
 - b. Show that β generates the cyclic group K^* of order 15.
 - c. Show that $\{0, 1, \beta^5, \beta^{10}\}$ is a subfield of K with 4 elements, and write β^5 in the basis $1, \beta, \beta^2, \beta^3$. Does K contain a subfield with 8 elements?
-