MAT 5173 — Problem Set 4

Due Wednesday 18 November 2026, at the start of the Q&A session.

This set covers the four meetings of 4 through 16 November: affine varieties, the correspondence $V \leftrightarrow I$, and the Nullstellensatz and Hilbert basis theorem, stated (Cox–Little–O'Shea §1.1–§1.4, Ash §8.1–§8.3), fixed fields and Galois groups (Ash §6.1), the fundamental theorem of Galois theory (§6.2), and the fundamental theorem continued, with Galois groups computed directly (§6.3). Problem 1 was Problem 5 of Problem Set 3, unchanged; if you have already written it, it counts here.

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, and Cox–Little–O'Shea in Problem 1. Every ring on this set is commutative with identity. We write $\langle a_1, \dots, a_k \rangle$ for the ideal generated by $a_1, \dots, a_k$, keeping parentheses for points of k^n. For a finite extension E/F with $G = \mathrm{Gal}(E/F)$, a subgroup $H \leq G$ and an intermediate field $F \leq K \leq E$, Ash writes $\mathcal{F}(H) = \{x \in E : \sigma(x) = x \text{ for all } \sigma \in H\}$ for the fixed field of H, and $\mathcal{G}(K) = \mathrm{Gal}(E/K)$ for the fixing group of K. Problems 2–4 continue examples from Problem Set 3, whose results you may quote; a later part may quote an earlier one.

Problem 1 (affine varieties and ideals) — Cox–Little–O'Shea §1.1–§1.4

Let k be a field. For $f_1, \dots, f_s \in k[X_1, \dots, X_n]$, the affine variety $V(f_1, \dots, f_s)$ is the set of $a \in k^n$ with $f_1(a) = \cdots = f_s(a) = 0$. For $V \subseteq k^n$, $I(V)$ is the set of $f \in k[X_1, \dots, X_n]$ with $f(a) = 0$ for every $a \in V$.

1. Prove that $I(V)$ is an ideal, and that it is *radical*: if $f^m \in I(V)$ for some $m \geq 1$, then $f \in I(V)$. Prove also that
$$V(f_1, \dots, f_s) \cup V(g_1, \dots, g_t) = V(f_i g_j : 1 \leq i \leq s,\ 1 \leq j \leq t),$$
so that a union of two varieties is a variety.

2. Let $k = \mathbb{R}$ and let $V = V(Y - X^2) \subseteq \mathbb{R}^2$, the parabola. Prove that $I(V) = \langle Y - X^2 \rangle$. (*Divide $f \in \mathbb{R}[X, Y]$ by $Y - X^2$, viewed as a monic polynomial in Y with coefficients in $\mathbb{R}[X]$, as in Set 2, Problem 3(1). What can the remainder be?*)

3. Let $h = X^2 + Y^2$. Find $V(h)$ in $\mathbb{R}^2$ and $I(V(h))$, and show that $I(V(h)) \neq \langle h \rangle$. Then find $V(h)$ in $\mathbb{C}^2$, and describe it, using part 1, as a union of two varieties.

Problem 2 (fixed fields and Galois groups) — §6.1

1. Let E/F be a finite extension with $G = \mathrm{Gal}(E/F)$.

   a. Prove that $\mathcal{F}(H)$ is a subfield of E containing F, for every $H \leq G$. Prove that $H \subseteq \mathcal{G}(\mathcal{F}(H))$ and $K \subseteq \mathcal{F}(\mathcal{G}(K))$, and that both $\mathcal{F}$ and $\mathcal{G}$ reverse inclusions.

   b. Now suppose that E/F is Galois. Using that $|\mathrm{Gal}(E/K)| = [E : K]$ for every intermediate field K (Ash 3.5.9, since E/K is again Galois), prove that $\mathcal{F}(G) = F$.

2. Let α be a real root of $g(X) = X^3 - 3X + 1$. By Set 3, Problem 4(2), the roots of g are $\alpha_1 = \alpha$, $\alpha_2 = \alpha^2 - 2$ and $\alpha_3 = 2 - \alpha - \alpha^2$, all in $\mathbb{Q}(\alpha)$, and $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \langle\sigma\rangle$ with $\sigma(\alpha) = \alpha^2 - 2$. Let $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$.

   a. Show that σ permutes the roots cyclically, $\alpha_1 \mapsto \alpha_2 \mapsto \alpha_3 \mapsto \alpha_1$, and deduce from part 1 that $\delta \in \mathbb{Q}$. Given that $\delta^2 = -4p^3 - 27q^2$ for any cubic $X^3 + px + q$, conclude that $\delta = \pm 9$.

   b. For $X^3 - 2$, the same formula gives $\delta^2 = -108$. Explain why this forces the Galois group of $X^3 - 2$ over $\mathbb{Q}$ to contain an automorphism acting on the three roots as a transposition, and name one.

Problem 3 (the fundamental theorem of Galois theory) — §6.2

1. Let E/F be a finite Galois extension with group G, let $H \leq G$, and let $K = \mathcal{F}(H)$. Prove that $\mathcal{F}(\tau H \tau^{-1}) = \tau(K)$ for every $\tau \in G$. Deduce that if $H \trianglelefteq G$, then $\tau(K) = K$ for every $\tau \in G$, so that restriction $\tau \mapsto \tau|_K$ is a homomorphism $G \to \mathrm{Gal}(K/F)$, and find its kernel. Granting that it is surjective (Ash 3.5.2), conclude that $\mathrm{Gal}(K/F) \cong G/H$.

2. Let $f(X) = X^4 - 2X^2 - 2$, with roots $\pm\alpha$ and $\pm\beta$, where $\alpha = \sqrt{1 + \sqrt{3}}$ and $\beta = \sqrt{-2}/\alpha$. By Set 3, Problem 3(2), its splitting field $E = \mathbb{Q}(\alpha, \sqrt{-2})$ has degree 8 over $\mathbb{Q}$; let $G = \mathrm{Gal}(E/\mathbb{Q})$.

   a. Explain why every $\sigma \in G$ is determined by $\sigma(\alpha)$ and $\sigma(\beta)$, and why it must map the pair $\{\pm\alpha\}$ onto one of the pairs $\{\pm\alpha\}$, $\{\pm\beta\}$. Conclude that there are exactly 8 such maps and all of them lie in G. Let $\sigma \in G$ be given by $\alpha \mapsto \beta$, $\beta \mapsto -\alpha$, and let τ be complex conjugation restricted to E. Show that σ has order 4, that $\tau\sigma\tau^{-1} = \sigma^{-1}$, and hence that $G \cong D_4$, the dihedral group of order 8.

   b. Show that $\sqrt{3} = \alpha^2 - 1$, $\sqrt{-2}$ and $\sqrt{-6}$ all lie in E. For each of the three quadratic fields $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-6})$, find the subgroup of order 4 fixing it. Which of the three subgroups is cyclic?

   c. Find the subgroups corresponding to $\mathbb{Q}(\alpha)$ and to $\mathbb{Q}(\sqrt{3}, \sqrt{-2})$. Use the fundamental theorem to decide which of these two fields is normal over $\mathbb{Q}$, and identify the Galois group of the one that is.

Problem 4 (computing Galois groups) — §6.3

1. Let $f \in F[X]$ be separable with distinct roots $\alpha_1, \dots, \alpha_n$ in a splitting field E. Prove that each $\sigma \in \mathrm{Gal}(E/F)$ permutes the roots, and that the resulting map $\mathrm{Gal}(E/F) \to S_n$ is an injective homomorphism. If f is irreducible, show that its image is *transitive*: for all i, j some σ has $\sigma(\alpha_i) = \alpha_j$. Deduce that n divides $|\mathrm{Gal}(E/F)|$, which divides $n!$, and compare Set 3, Problem 3(1).

2. Let $K = \mathbb{F}_2[X]/\langle X^4 + X + 1\rangle$, the field with 16 elements of Set 3, Problem 4(3). Show directly, without quoting Ash 6.4.2, that $\mathrm{Gal}(K/\mathbb{F}_2)$ is cyclic of order 4, generated by the Frobenius map $\varphi(z) = z^2$. (*Why is $\varphi^2 \neq \mathrm{id}$? Count the roots of $X^4 - X$.*) Then use the fundamental theorem to list every subfield of K, recovering Set 3's answer that K has exactly one subfield with 4 elements and none with 8.

3. Let $\zeta = e^{i\pi/4}$. Show that the roots of $X^4 + 1$ are $\zeta, \zeta^3, \zeta^5, \zeta^7$, that its splitting field is $\mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{2})$, of degree 4 over $\mathbb{Q}$, and that its Galois group consists of the automorphisms $\zeta \mapsto \zeta^k$ for $k \in \{1, 3, 5, 7\}$. Show that this group is isomorphic to $U(\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, and match each of its subgroups of order 2 with one of the quadratic fields $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$.