Solutions to Math 418 Final Exam — May 13, 2025

1. (20 points) Let a be an even integer greater than 2. Prove that the polynomial $f(x) = x^5 - ax + 2 \in \mathbb{Q}[x]$ is not solvable by radicals.

As in the proof in class, we want to show that f is irreducible and that it has precisely two nonreal roots. Then $|\mathrm{Gal}(f)|$ is a multiple of 5, so it has a Sylow 5-subgroup, and therefore has elements of order 5, which in S_5 must be 5-cycles. In addition, complex conjugation (restricted to $Sp_{\mathbb{Q}}(f)$) fixes the three real roots and swaps the other two i.e. it is a two-cycle. In S_5, any 5-cycle and any 2-cycle generate the whole group, so $\mathrm{Gal}(f) = S_5$. Since S_5 is not solvable, by Galois' Solvability Theorem, $f(x)$ is not solvable by radicals.

$f(x)$ is irreducible by Eisenstein's criterion with $p = 2$. Since the top-degree term is odd-degree with positive coefficient, $f(x) < 0$ for $x \ll 0$ and $f(x) > 0$ for $x \gg 0$. Since $f(0) = 2 > 0$ and $f(1) = 3 - a < 0$, the Intermediate Value Theorem guarantees that $f(x)$ has at least 3 real roots.

To see that $f(x)$ doesn't have more than 3 real roots, note that $f'(x) = 5x^4 - a$. This has roots $\pm\alpha, \pm i\alpha$, where $\alpha = \sqrt[4]{a/5}$, and two of these four roots are real. By the Mean Value Theorem, $f(x)$ can't have more than $2 + 1 = 3$ real roots, so f satisfies the desired conditions and is not solvable by radicals.

2. (20 points) Let R be a commutative ring with 1, and let $a, b \in R$ be nonzero. $m \in R$ is a *least common multiple* if $a|m, b|m$, and if $a|m'$ and $b|m'$, then $m|m'$.

   (a) (10 points) Prove that if R is a UFD, then all nonzero $a, b \in R$ have a least common multiple.

Since R is a UFD, both a and b have factorizations into a finite number of irreducibles, unique up to associates. Choose a set of irreducibles $p_1, \ldots, p_n$ containing all the irreducibles in either of these factorization (again up to units). Then

$$a = up_1^{e_1} \cdots p_n^{e_n}, \qquad b = vp_1^{f_1} \cdots p_n^{f_n},$$

where $e_i, f_i \in \mathbb{Z}_{\geq 0}$ and u, v are units. Let $g_i := \max(e_i, f_i)$, and $m := p_1^{g_1} \cdots p_n^{g_n}$. Then $a|m$ since

$$m = a \cdot u^{-1} u p_1^{g_1 - e_1} \cdots p_n^{g_n - e_n},$$

and similarly, $b|m$. If $a|m'$ and $b|m'$, then consider the exponent h_i of p_i in the irreducible factorization of m'. We must have $e_i \leq h_i$ since $a|m'$ and $f_i \leq h_i$ since $b|m'$. Therefore, $h_i \geq \max(e_i, f_i) = g_i$ for all i, so $m|m'$.

   (b) (10 points) Consider the ring $\mathbb{Z}[\sqrt{-5}]$. Prove that there exist nonzero elements a and b in this ring which do not have a least common multiple. *(Hint: recall from Homework 1 that* $2, 3, 1 + \sqrt{-5}$, *and* $1 - \sqrt{-5}$ *are all irreducible, and are pairwise nonassociates)*

We show that $a = 2$ and $b = 1 + \sqrt{-5}$ do not have a least common multiple. Let $c = 2 + 2\sqrt{-5} = ab$ and $d = 6 = 3a = (1 - \sqrt{-5})b$.

Suppose a and b have a least common multiple m. Then $m|c$ and $m|d$. Since the norm $N(x + y\sqrt{-5}) = x^2 + 5y^2$ is multiplicative, $N(m)|N(c) = 24$, and $N(m)|N(d) = 36$, so $N(m)|12$. We also have $4 = N(a)|N(m)$ and $6 = N(b)|N(m)$, so $12|N(m)$ Therefore, $N(m) = 12$; however, if $m = x + y\sqrt{-5}$, then $x^2 + 5y^2 = 12$. We must have $y = 0$ or $y = 1$, but neither 12 nor 7 is a square; hence this is impossible.

3. (12 points) Recall the projective twisted cubic

$$W = \{[a^3 : a^2b : ab^2 : b^3] | a, b \in \mathbb{C}, \text{ not both } 0\} \subseteq \mathbb{P}^3(\mathbb{C}).$$

Recall also the decomposition

$$\mathbb{P}^3(\mathbb{C}) = \mathbb{C}^3 \cup \mathbb{P}^2(\mathbb{C}) = \{[1 : x : y : z]\} \cup \{[0 : x : y : z]\}.$$

(a) (6 points) Prove that $W \cap \mathbb{C}^3$ is the affine twisted cubic $V = \{(t, t^2, t^3) | t \in \mathbb{C}\}$.

Let $w \in W \cap \mathbb{C}^3$. Then w is of the form $[1 : b/a : (b/a)^2 : (b/a)^3] = [1 : t : t^2 : t^3] \mapsto (t, t^2, t^3) \in \mathbb{C}^3$, where $t = \frac{b}{a}$ (note that $a \neq 0$ since $a^3 \neq 0$). Conversely, given $t \in \mathbb{C}$, the point $[1 : t : t^2 : t^3] \in \mathbb{P}^3(\mathbb{C})$, and it's in W by setting $a = 1, b = t$.

Alternate solution: set $a^3 = 1$; the point in W becomes $[1 : a^2 b : ab^2 : b^3]$. Since a is a cube root of 1, so is a^2, say $a^2 = \zeta$. So the point is $[1 : \zeta b : (\zeta b)^2 : (\zeta b)^3]$, and set $t = \zeta b$.

(b) (6 points) Determine the affine variety $W \cap \mathbb{P}^2(\mathbb{C})$.

Let $w \in W \cap \mathbb{P}^2(\mathbb{C})$. Then we must have $a = 0$, so $w = [0 : 0 : 0 : b^3] = [0 : 0 : 0 : 1] \mapsto [0 : 0 : 1] \in \mathbb{P}^2(\mathbb{C})$.

[Note that in some sense this is the "point at infinity" of the affine twisted cubic; when t gets large, t and t^2 get very small compared to t^3. Here we are working with points up to a global scalar, so $[t : t^2 : t^3] \to [0 : 0 : 1]$. Another way to look at this is that there is a point at infinity of $\mathbb{P}^3$ for every equivalence class of parallel lines, and as t gets large, the curve (t, t^2, t^3) becomes nearly parallel with $(0, 0, 1)$.]

4. (30 points) (a) (15 points) Let K be the splitting field of $x^8 - 1$ over $\mathbb{Q}$. Compute the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ up to isomorphism, and use the Galois correspondence to compute and draw the lattice of intermediate fields $\mathbb{Q} \subseteq E \subseteq K$.

Let ζ be a primitive 8th root of 1. By Dummit and Foote Theorem 14.26, $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong V_4$. This group has three proper, nontrivial subgroups, $H_1 = \langle \zeta \mapsto \zeta^3 \rangle$, $H_2 = \langle \zeta \mapsto \zeta^5 \rangle$, $H_3 = \langle \zeta \mapsto \zeta^7 \rangle$, each of which is a cyclic group of order 2. Therefore, there are three quadratic fields lying between $\mathbb{Q}$ and K: $F_1 = \mathrm{Fix}\, H_1 = \mathbb{Q}(\zeta + \zeta^3) = \mathbb{Q}(\sqrt{-2})$, $F_2 = \mathrm{Fix}\, H_2 = \mathbb{Q}(i)$, and $F_3 = \mathrm{Fix}\, H_3 = \mathbb{Q}(\zeta + \zeta^7) = \mathbb{Q}(\sqrt{2})$. The first and third fixed fields can be obtained via a sum over the orbit, while the second needs other means (like taking a product over the orbit instead).

(b) (15 points) Let L be the splitting field of $x^8 - 1$ over $\mathbb{F}_3$. Compute the Galois group $\mathrm{Gal}(L/\mathbb{F}_3)$ up to isomorphism (no need for specific elements), and use the Galois correspondence to compute and draw the lattice of intermediate fields $\mathbb{F}_3 \subseteq F \subseteq L$.

The splitting field for $f(x) = x^8 - 1$ over $\mathbb{F}_3$ is the same as the splitting field of $x^9 - x$, which by Dummit and Foote Proposition 14.15 is the finite field $\mathbb{F}_9$. The Galois group $\mathrm{Gal}(\mathbb{F}_9/\mathbb{F}_3)$ is the cyclic group of order 2 since the degree of the extension is 2. This group has no proper nontrivial subgroups, so there are no fields strictly between $\mathbb{F}_3$ and $\mathbb{F}_9$ (which also follows from the tower law). Thus, the intermediate field lattice contains just $\mathbb{F}_3$ and $\mathbb{F}_9$.

5. (30 points) Please complete **THREE** of the following problems, some of which are on the following page. If you have work on more than three problems, **you must CLEARLY specify which three problems you would like graded**; otherwise, the first three will be graded

I would like the following three parts of this problem graded: _____

(a) (10 points) Prove that every $\alpha \in \mathbb{F}_{p^n} \setminus \mathbb{F}_p$ satisfies the equation

$$\alpha^{p^n - 3} + \alpha^{p^n - 4} + \cdots + \alpha + 1 = -\alpha^{-1}.$$

Since $\alpha \in \mathbb{F}_{p^n}$, which is the set of roots of $x^{p^n} - x$ (see Dummit and Foote, p.549-550), α is a root of that polynomial. Since $\alpha \notin \mathbb{F}_p$, $\alpha \neq 0, 1$, so we can divide by $x(x-1)$, and thus α is a root of $x^{p^n-2} + x^{p^n-3} + \cdots + x + 1$. Plugging in α, moving the 1 to the other side, and dividing by α gives the result.

(b) (10 points) Let $f(x) = x^3 + x^2 + 1 \in \mathbb{Q}[x]$. Let θ be a root of $f(x)$ in some extension field. Determine $(1+\theta)^{-1}$ in $\mathbb{Q}(\theta)$ as a polynomial in θ.

First, f is irreducible since it is degree 3 and has no roots in $\mathbb{F}_2$. This means that one obtains a well-defined solution to this equation, but showing irreducibility isn't explicitly necessary for the problem.

We have $\theta^3 + \theta^2 + 1 = 0$, so if $(1+\theta)^{-1} = a\theta^2 + b\theta + c$, then

$$\begin{aligned} 1 &= (1+\theta)(a\theta^2 + b\theta + c) \\ &= a\theta^3 + (a+b)\theta^2 + (b+c)\theta + c \\ &= a(-\theta^2 - 1) + (a+b)\theta^2 + (b+c)\theta + c \\ &= b\theta^2 + (b+c)\theta + c - a. \end{aligned}$$

Since $1, \theta, \theta^2$ form a basis for $\mathbb{Q}(\theta)/\mathbb{Q}$, we must have $b = 0, b + c = 0, c - a = 1$, and this yields $a = 0, b = 0, c = -1$, so $(1+\theta)^{-1} = -\theta^2$.

Alternate solution: we can dispense with the annoying algebra by noting that $\theta^3 + \theta^2 + 1 = 0 \implies \theta^2(\theta+1) + 1 = 0 \implies 1 = -\theta^2(\theta+1) \implies (\theta+1)^{-1} = -\theta^2$.

(c) (10 points) Let R be a PID. Prove that R is Noetherian. (That is, R doesn't have an infinite strictly ascending chain of ideals $I_1 \subsetneq I_2 \subsetneq \cdots$).

There are multiple ways to prove this.

(i) Take an infinite weakly ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$. Then $I := \cup_i I_i$ is an ideal containing every I_i. Since R is a PID, $I = (d)$ for some $d \in R$; $d \in I_k$ for some k, so choose k minimal such that $d \in I_k$. Then $I = (d) \subseteq I_k \subseteq I$, so $I_k = I$, and this chain only has finitely many strict increases.

(ii) Choose a fixed ideal $I = (r)$ in R. Since PIDs are UFD, we can write $r = p_1 p_2 \cdots p_n$ where $p_1, \ldots, p_n$ are irreducibles in R, and this factorization is unique up to order and units. Thus, $I \subseteq (d)$ if and only if $d|r$, which happens if and only if d can be expressed as $d = up_{i_1} \cdots p_{i_k}$ where $1 \leq i_1 < i_2 < \cdots i_k \leq n$, and u is a unit. There are at most 2^n such choices up to a choice of u, so I is contained in finitely many ideals, and thus cannot be part of an infinite ascending chain.

(iii) In Lecture 4, we gave essentially the proof in (i) while proving that all PIDs are UFDs. Citing this with enough specificity is acceptable.

(d) (10 points) Let $K/\mathbb{Q}$ be a Galois extension with abelian Galois group, and where $[K : \mathbb{Q}]$ is a power of 2. Prove that every $\alpha \in K$ is constructible

Suppose that $[K : \mathbb{Q}] = 2^n$, and induct on n. The Galois group $G := \mathrm{Gal}(K/\mathbb{Q})$ is abelian of order 2^n, so has a chain of subgroups $G = G_n > G_{n-1} > \cdots > G_1 > G_0 = 1$ with $|G_{i+1} : G_i| = 2$ for all i. By the Galois correspondence, taking the fixed fields of this chain gives a chain of field extensions $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$ with $[K_{i+1} : K_i] = 2$ for all i. Since every degree 2 extension is quadratic, this means every $\alpha \in K$ is constructible since $\mathbb{Q}(\alpha) \subseteq K$.

[In fact, this proof works when G is any 2-group, since (some form of) the Sylow Theorems imply that G has the necessary chain of subgroups. However, if the extension is not Galois at all, the proof fails, and indeed there are some extensions of degree a power of 2 that are not constructible.]

(e) (10 points) Let $f(x), g(x) \in \mathbb{Q}[x]$ with $\deg f = 3$, $\deg g = 4$. Let K be the splitting field of the product fg (i.e. the composite of the splitting fields of f and g). Prove that every element of $\mathrm{Gal}(K/\mathbb{Q})$ has order ≤ 12.

Note that all splitting fields over $\mathbb{Q}$ are Galois extensions. Let K_1 be the splitting field of f and K_2 be the splitting field of g. Then, $K = K_1K_2$, so by Dummit and Foote Proposition 14.21, $\mathrm{Gal}(K/\mathbb{Q})$ is a subgroup of $\mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q})$. The first group is a subgroup of S_3, and every element has order ≤ 3. The second group is a subgroup of S_4, and every element has order ≤ 4. The order of (σ_1, σ_2) in the direct product is $\mathrm{lcm}(|\sigma_1|, |\sigma_2|)$, which therefore is ≤ 12.

(f) (10 points) Let V be an irreducible nonempty variety in $\mathbb{C}^1$. Prove that either $V = \mathbb{C}^1$ or V is a point.

Let $I = I(V)$, which is an ideal in $\mathbb{C}[x]$, and note that we also have $V = V(I)$. From Lecture 37, since V is irreducible, I must be prime. If $I = (0)$, then $V = \mathbb{C}^1$, so assume henceforth that I is a nonzero prime ideal.

Since $\mathbb{C}$ is a field, $\mathbb{C}[x]$ is a Euclidean domain (hence a PID), and so all nonzero prime ideals are maximal (Lecture 3). By the Weak Nullstellensatz (Lecture 38), whenever I is a maximal ideal, $V(I)$ is a point, and putting all this together, we see that V must be a point.