Solutions to Math 418 Midterm Exam 3 — Apr. 23, 2025

1. (30 points) Let K be the splitting field of $x^4 - 3$ over $\mathbb{Q}$, and let $G = \mathrm{Gal}(K/\mathbb{Q})$.

   (a) (5 points) Determine K, and prove that $[K : \mathbb{Q}] = 8$.

   The roots of f are $\pm\sqrt[4]{3}$ and $\pm i\sqrt[4]{3}$, so $K = \mathbb{Q}(i, \sqrt[4]{3})$. Since $\sqrt[4]{3}$ is the root of an irreducible degree 4 polynomial, $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$. Since $\mathbb{Q}(\sqrt[4]{3}) \subseteq \mathbb{R}$ and $K \not\subseteq \mathbb{R}$, we must have $[K : \mathbb{Q}(\sqrt[4]{3}] > 1$. Conversely, since $[\mathbb{Q}(i) : \mathbb{Q}] = 2, [K : \mathbb{Q}(\sqrt[4]{3}] \leq 2$, so it equals 2. By the Tower Law, $[K : \mathbb{Q}] = 4 \cdot 2 = 8$.

   (b) (10 points) The dihedral group D_8 of order 8 has the following presentation:

   $$D_8 = \langle \sigma, \tau | \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle.$$

   Prove directly that $G \cong D_8$ by exhibiting automorphisms σ and τ that satisfy the above relations for D_8, and showing that they satisfy these relations.

   For any automorphism $\rho \in G$, we must have $\sqrt[4]{3} \mapsto i^a\sqrt[4]{3}$ for $a \in \{0, 1, 2, 3\}$ and $i \mapsto \pm i$. This gives a total of 8 possible automorphism, and since $|G| = 8$, all of them must be valid. Let

   $$\sigma : \begin{cases} \sqrt[4]{3} \mapsto i\sqrt[4]{3}, \\ i \mapsto i, \end{cases} \qquad \tau : \begin{cases} \sqrt[4]{3} \mapsto \sqrt[4]{3}, \\ i \mapsto -i. \end{cases}$$

   Straightforward computations show that σ has order 4 and τ has order 2. For the other relation, we have

   $$\tau\sigma : \begin{cases} \sqrt[4]{3} \mapsto i\sqrt[4]{3} \mapsto -i\sqrt[4]{3}, \\ i \mapsto i \mapsto -i, \end{cases} \qquad \text{and} \qquad \sigma^3\tau : \begin{cases} \sqrt[4]{3} \mapsto \sqrt[4]{3} \mapsto -i\sqrt[4]{3}, \\ i \mapsto -i \mapsto -i, \end{cases}$$

   and we note that this automorphisms are equal on both generators.

   (c) (15 points) Compute the subgroup lattice for D_8, and for each subgroup, compute the corresponding intermediate field. Draw both the subgroup lattice and the intermediate field lattice. *(Note: some of these subgroups/intermediate fields are more challenging than others. Finding most of the subgroups and getting their relative containments and fixed fields correct, will get most of the points for this problem.)*

   D_8 has 1 element of order 1 (the identity), 5 elements of order 2 $(\tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau, \sigma^2)$, and 2 elements of order 4 (σ, σ^3). Thus, G has one subgroup of order 1 (the trivial group), five subgroups of order two:

   $$H_1 = \langle \tau \rangle, \quad H_2 = \langle \sigma\tau \rangle, \quad H_3 = \langle \sigma^2\tau \rangle, \quad H_4 = \langle \sigma^3\tau \rangle, \quad H_5 = \langle \sigma^2 \rangle,$$

   three subgroups of order four:

   $$J_1 = \langle \sigma \rangle, \quad J_2 = \langle \sigma^2, \tau \rangle, \quad J_3 = \langle \sigma\tau, \sigma^3\tau \rangle,$$

   and one subgroup of order 8 (the whole group). We have

   $$\text{Fix id} = K, \quad \text{Fix } H_1 = \mathbb{Q}(\sqrt[4]{3}), \quad \text{Fix } H_2 = \mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3}), \quad \text{Fix } H_3 = \mathbb{Q}(i\sqrt[4]{3}),$$

   $$\text{Fix } H_4 = \mathbb{Q}(\sqrt[4]{3} - i\sqrt[4]{3}), \quad \text{Fix } H_5 = \mathbb{Q}(i, \sqrt{3}), \quad \text{Fix } J_1 = \mathbb{Q}(i),$$

   $$\text{Fix } J_2 = \mathbb{Q}(\sqrt{3}), \quad \text{Fix } J_3 = \mathbb{Q}(i\sqrt{3}), \quad \text{Fix } G = \mathbb{Q}.$$

   The most difficult fixed fields to compute are probably Fix H_2, Fix H_4, and Fix J_3. For the first two, we obtain the desired elements by summing over the orbit containing $\sqrt[4]{3}$, in a similar manner to cyclotomic extensions. For Fix J_3, if you got the fixed fields of H_2 and H_4, note that $(\sqrt[4]{3}+i\sqrt[4]{3})(\sqrt[4]{3}-i\sqrt[4]{3}) = 2i\sqrt{3}$. Another possibility is to notice that Fix $J_3 \subseteq$ Fix $H_5 = \mathbb{Q}(i, \sqrt{3})$. This is a Galois extension over $\mathbb{Q}$ with (nontrivial) intermediate fields $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(i)$, and $\mathbb{Q}(i\sqrt{3})$, and we check which one of them is fixed J_3.

To draw the diagrams, we note that

$$H_1 \subseteq J_2, \quad H_2 \subseteq J_3, \quad H_3 \subseteq J_2, \quad H_4 \subseteq J_3, \quad H_5 \subseteq J_1, J_2, J_3,$$

and both the subgroup and intermediate field lattices are drawn accordingly. See the last page of the solutions for the diagrams.

2. (15 points) Let f be a monic irreducible polynomial of degree n in $\mathbb{F}_p[x]$.
   (a) (10 points) Prove that for any $\alpha \in \mathbb{F}_{p^n}$, α is a root of f if and only if α^p is a root of f.

   This can be done directly by writing out f in coefficients and taking the pth power directly, to show that $f(\alpha^p) = f(\alpha)^p$, so if $f(\alpha) = 0$, then $f(\alpha^p) = 0^p = 0$, and if $f(\alpha^p) = f(\alpha)^p = 0$, then since $\mathbb{F}_p$ is an integral domain, $f(\alpha) = 0$.

   The slicker way is to note that $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is the cyclic group generated by the Frobenius automorphism $\phi : a \mapsto a^p$. Automorphisms always map elements to roots of the same minimal polynomial, and so since f is irreducible, α is a root of f if and only if $\phi(\alpha) = \alpha^p$ is a root of f.

   (b) (5 points) Let α be a root of f. Prove that the constant term of f must be $(-1)^n \alpha^{\frac{p^n-1}{p-1}}$.

   The constant term of any polynomial is $(-1)^n$ times the product of its roots (with multiplicity). By the previous part, the roots are $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}$, and their product is

$$\alpha^{1+p+p^2+\cdots+p^{n-1}} = \alpha^{\frac{1-p^n}{1-p}}.$$

   Not needed for the problem, but since $f \in \mathbb{F}_p[x]$, its constant term is in $\mathbb{F}_p$, so $\alpha^{\frac{p^n-1}{p-1}} \in \mathbb{F}_p$ for all $\alpha \in \mathbb{F}_{p^n}$.

3. (10 points) Let $f(x) = x^3 - 2x + 2 \in \mathbb{Q}[x]$. Determine the Galois group for f over $\mathbb{Q}$ up to isomorphism (no need for specific elements). *(Hint: recall the discriminant of $x^3 + px + q$ is $D = -4p^3 - 27q^2$)*

f is irreducible by Eisenstein's criterion, with the prime 3, so since f is degree 3 its Galois group must be either A_3 or S_3 (the only two transitive subgroups of S_3). We apply the discriminant criterion: $D = -4p^3 - 27q^2 = -4(-2)^3 - 27(2^2) = (-4)(-8) - 27 \cdot 4 = 32 - 108 = -76$. This is negative, so is not a square in $\mathbb{Q}$; therefore, by the discriminant criterion, $\text{Gal}(f) \not\subseteq A_3$, so it equals S_3.

4. (15 points) Determine the following, explaining your reasoning.
   (a) (5 points) The radical of the ideal $I = (60) \subseteq \mathbb{Z}$.

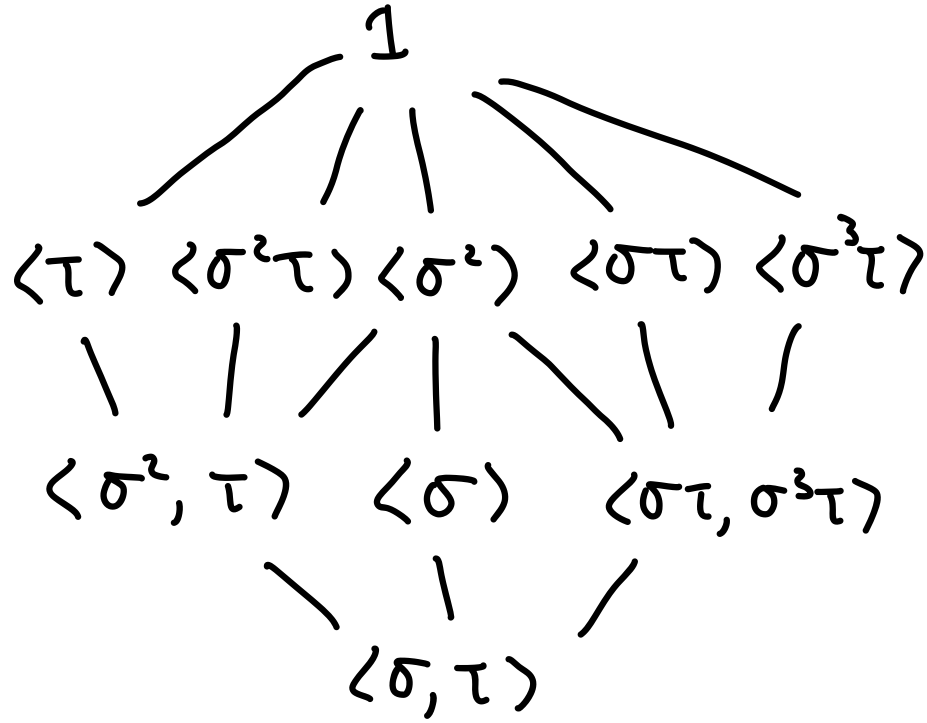
   $60 = 2^2 \cdot 3 \cdot 5$, so if a^n is a multiple of 60 for any n, a must be a multiple of 2, 3, and 5; hence, a multiple of 30. Conversely, if a is a multiple of 30, then a^2 is a multiple of $900 = 15 \cdot 60$, so $a \in \sqrt{I}$. Thus, $\sqrt{I} = (30)$.

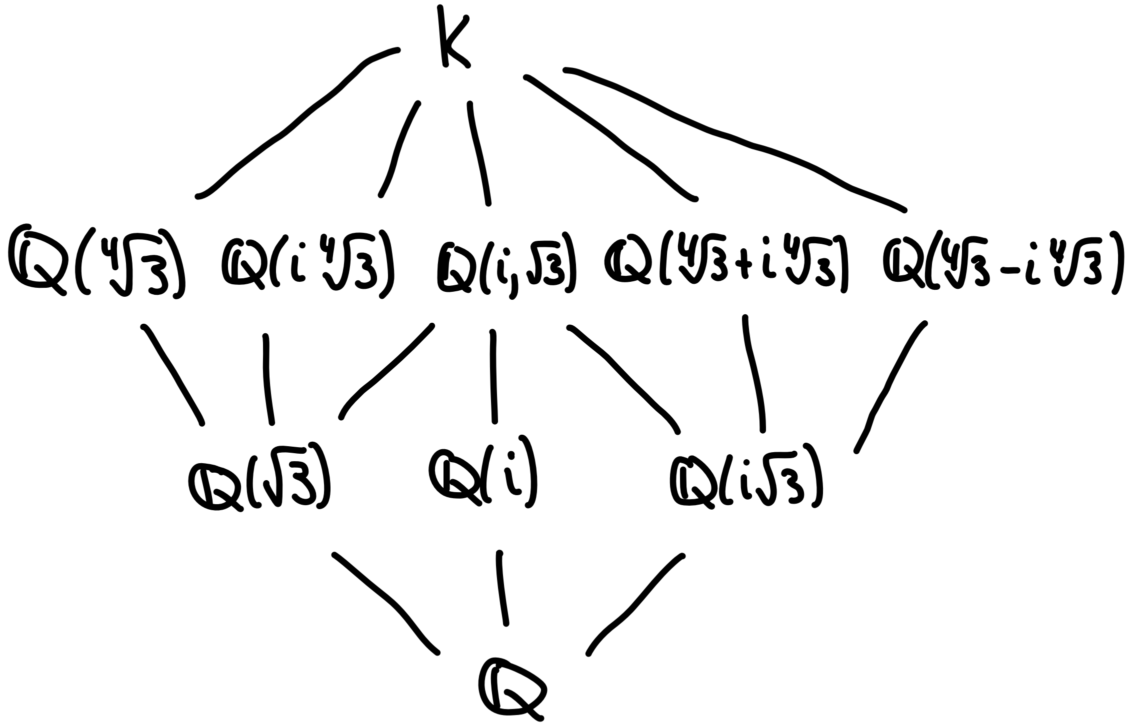
   (b) (5 points) The variety $V(I)$ corresponding to the ideal $I = (y - x^2, y - 3) \subseteq \mathbb{R}[x, y]$.

   $V(I)$ is the set of points $(x, y) \in \mathbb{R}^2$ such that $y - x^2 = 0$ and $y - 3 = 0$. Thus, $y = 3$, and so $x^2 = 3$, and therefore $V(I)$ consists of two points: $(\sqrt{3}, 3)$ and $(-\sqrt{3}, 3)$.

   (c) (5 points) The ideal $I(V)$ corresponding to the variety $V \subseteq \mathbb{R}^2$ which is the circle of radius 4 centered at $(1, 1)$.

V is the set of points $(x, y) \in \mathbb{R}^2$ such that $(x-1)^2 + (y-1)^2 = 4^2$. Moving everything to one side and expanding, $I(V) = ((x-1)^2 + (y-1)^2 - 4^2) = (x^2 - 2x + y^2 - 2y - 14)$.





All degrees/indices are 2