Solutions to Math 418 Midterm Exam 3 — Apr. 18, 2024

1. (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: $F_1 = \text{Fix } H_1 = \mathbb{Q}(\zeta + \zeta^3) = \mathbb{Q}(\sqrt{-2})$, $F_2 = \text{Fix } H_2 = \mathbb{Q}(i)$, and $F_3 = \text{Fix } H_3 = \mathbb{Q}(\zeta + \zeta^7) = \mathbb{Q}(\sqrt{2})$.

   (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 $\mathbb{F}_9$.

2. (15 points) Let $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$. 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 since its reduction mod 2 has no roots $\overline{f}(x) = x^3 + x + 1, \overline{f}(0) = \overline{f}(1) = 1$ (or by the rational root theorem, since $f(1) = -1, f(-1) = -3$).

   Since f is irreducible, its Galois group $\mathrm{Gal}(f)$ is a transitive subgroup of S_3, so $\mathrm{Gal}(f) = A_3$ or S_3. By the discriminant criterion, $\mathrm{Gal}(f) \subseteq A_3 \iff \sqrt{D} \in \mathbb{Q}$, so $\mathrm{Gal}(f) = A_3$ if $\sqrt{D} \in \mathbb{Q}$, and $\mathrm{Gal}(f) = S_3$ otherwise. Computing, we have $D = -4p^3 - 27q^2 = 81$, which is a square in $\mathbb{Q}$, so $\mathrm{Gal}(f) = A_3$.

3. (15 points) Prove that the polynomial $f(x) = x^5 - 4x^2 + 2 \in \mathbb{Q}[x]$ 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 $x << 0$ and $f(x) > 0$ for $x >> 0$. Since $f(-1) = 1 > 0$ and $f(0) = -2 < 0$, 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 $f'(x) = 5x^4 - 8x = x(5x^3 - 8)$. This has precisely 2 real roots, 0 and the unique real root of $5x^3 - 8$ (which is a scaled, shifted version of x^3, and therefore has the same number of real roots). By the Mean Value Theorem, $f(x)$ can have more than $2 + 1 = 3$ real roots, so f satisfies the desired conditions and is not solvable by radicals.

4. (20 points) Miscellaneous problems.

   (a) (10 points) Give an example of fields $F \subseteq K \subseteq L$ such that K/F and L/K are both Galois, but L/F is not (and prove your claims).

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt[4]{2})$. K/F is Galois because K is the splitting field for $x^2 - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$. L/K is Galois because L is the splitting field for $x^2 - \sqrt{2} \in K[x]$ over K. However, $L/\mathbb{Q}$ is not Galois. To see this, consider the polynomial $f(x) = x^4 - 2 \in \mathbb{Q}[x]$, which is irreducible by Eisenstein's criterion, and since $\sqrt[4]{2}$ is a root of f, f is the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$. L contains two roots, $\pm\sqrt[4]{2}$ of f, but $L \subseteq \mathbb{R}$ and so L does not contain the other two roots, $\pm i\sqrt[4]{2}$. Any automorphism of L is determined by its action on $\sqrt[4]{2}$ since this is a primitive element for the extension. But this means that $|\mathrm{Aut}_{L/\mathbb{Q}}| = 2$ since any such automorphism must send $\sqrt[4]{2} \mapsto \pm\sqrt[4]{2}$. Since $[L : \mathbb{Q}] = 4 > 2 = |\mathrm{Aut}_{L/\mathbb{Q}}|$, the extension is not Galois.

(b) (10 points) Let $K/\mathbb{Q}$ be a Galois extension with abelian Galois group such that $[K : \mathbb{Q}]$ 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 $\mathbb{Q}(\alpha) \subseteq K$.