Solutions to Math 418 Midterm Exam 2 — Mar. 26, 2025

1. (15 points) Recall that to construct an angle θ using straightedge and compass, it is equivalent to construct $\cos\theta$.

   (a) (10 points) Use the triple angle formula

   $$\cos\theta = 4\cos^3(\theta/3) - 3\cos(\theta/3)$$

   to find the minimal polynomial over $\mathbb{Q}$ for $\cos 100°$ (and prove that this is indeed the minimal polynomial for $\cos 100°$ over $\mathbb{Q}$).

   Note that $\cos 300° = \frac{1}{2}$, so by the triple angle formula, $\beta := \cos 100°$ satisfies $\frac{1}{2} = 4\beta^3 - 3\beta$, so β is a root of the monic polynomial $f(x) = x^3 - \frac{3}{4}x - \frac{1}{8}$.
   We claim that $f(x)$ is the minimal polynomial for β i.e. that it is irreducible. Since f is a degree three polynomial, it suffices to show that it doesn't have a rational root. We can equivalently show that $g(x) := 8f(x) = 8x^3 - 6x - 1$ doesn't have a rational root.
   There are a few ways to show this.
   1) By the rational root theorem, the only possible rational roots of $g(x)$ are $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$. We can just plug these in directly (you actually need to do this to get full credit).
   2) Same as above, but use this trick: if one of $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$ is a root, its reciprocal (which is an integer) is a root of $-x^3 g(1/x) = x^3 + 6x^2 - 8$. But this polynomial has no integer roots, since it has no roots modulo 5, which can be checked more easily than plugging in the potential rational roots to g directly.
   3) By Gauss' Lemma, since $g(x) \in \mathbb{Z}[x]$, if $g(x)$ is irreducible over $\mathbb{Z}$, it is irreducible over $\mathbb{Q}$. However, $g(x)$ can't have an integer root since $g(a)$ is always odd if $a \in \mathbb{Z}$.
   4) $g(x-1) = 8(x-1)^3 - 6(x-1) - 1 = 8x^3 - 24x^2 + 18x - 3$, which is irreducible by Eisenstein's criterion with the prime 3.
   5) $g(x/2) = x^3 - 3x - 1$, which is irreducible by the rational root theorem with a much easier check.
   6) Modulo 5, $g(x) = 3x^3 - x - 1$, which can be checked to have no roots.
   7) Modulo 7, $g(x) = x^3 + x - 1$, which can be checked to have no roots.
   Therefore, g and f are both irreducible over $\mathbb{Q}$, and so f is the minimal polynomial for β.

   (b) (5 points) Prove that $\cos 100°$ is not constructible using straightedge and compass (which implies that the angle $100°$ isn't either).

   As we have seen in class (or Dummit & Foote Proposition 13.23), if β is constructible, then $[\mathbb{Q}(\beta) : \mathbb{Q}]$ is a power of 2. However, by the previous part, $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$, which is a contradiction.
   (Alternatively, one can bypass using part a–although I don't see why you would want to–by noting that $\zeta := e^{i(100°)}$ is a primitive 18th root of unity, so $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(18) = 6$, which is not a power of 2, and since constructing ζ is equivalent to constructing $\cos(100°)$, neither is constructible.)

2. (25 points) Let $f(x) = x^3 - 17 \in \mathbb{Q}[x]$, and let K be the splitting field for f over $\mathbb{Q}$. You may take for granted that f is irreducible over $\mathbb{Q}$. *(Hint: don't be scared by the number 17, but do note that it is prime)*

   (a) (10 points) Determine K and its degree over $\mathbb{Q}$.

   The positive real cube root of 17, $\sqrt[3]{17}$, is a root of f, and the three roots are $\sqrt[3]{17}, \zeta_3\sqrt[3]{17}, \zeta_3^2\sqrt[3]{17}$. Now, $K = \mathbb{Q}(\sqrt[3]{17}, \zeta_3)$ since the other two roots can be written in terms of $\sqrt[3]{17}$ and ζ_3, and ζ_3 can be written as a quotient of two of the roots. By the Tower Law,

   $$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{17})][\mathbb{Q}(\sqrt[3]{17}) : \mathbb{Q}].$$

The latter factor is 3 since f is irreducible, while the former is 1 or 2 since $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$, so $[K : \mathbb{Q}] = 3$ or 6. Since K contains a degree 2 element, ζ_3, it must have even degree over $\mathbb{Q}$, so $[K : \mathbb{Q}] = 6$.

(b) (5 points) Prove that the field extension $K/\mathbb{Q}$ is Galois.

f is separable because it has distinct roots (or alternatively, because it is irreducible over a characteristic zero field), so by Dummit & Foote Corollary 14.6 (splitting fields of separable polynomials are Galois), $K/\mathbb{Q}$ is Galois.

(c) (10 points) Give a presentation of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. That is, give a set of automorphisms that generate $\mathrm{Gal}(K/\mathbb{Q})$, find the relations they satisfy, and prove that the group they generate really is the full Galois group.

Let $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$ be defined by

$$\sigma : \begin{cases} \sqrt[3]{17} \mapsto \zeta_3 \sqrt[3]{17}, \\ \zeta_3 \mapsto \zeta_3, \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{17} \mapsto \sqrt[3]{17}, \\ \zeta_3 \mapsto \zeta_3^2. \end{cases}$$

It is easy to see that $\sigma^3 = \tau^2 = 1$, and so they generate a group of order at least 6. Since $K/\mathbb{Q}$ is Galois, we know that $|\mathrm{Gal}(K/\mathbb{Q})| = 6$, so $\mathrm{Gal}(K/\mathbb{Q})$ is generated by σ and τ. All that remains is to find the relations between σ and τ, and a quick computation shows that

$$\sigma\tau = \tau\sigma^2 : \begin{cases} \sqrt[3]{17} \mapsto \zeta_3 \sqrt[3]{17}, \\ \zeta_3 \mapsto \zeta_3^2, \end{cases}$$

(and note that this is equivalent to saying that $\sigma^2\tau = \tau\sigma$) so $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau | \sigma^3 = \tau^2 = 1, \sigma\tau = \tau\sigma^2 \rangle$, which equals the symmetric group S_3 (note: non-abelian).

3. (20 points) Let F be a field, and consider the polynomial $f(x) = x^4 - 8x - 2 \in F[x]$ (note that f is indeed defined over any field F since $1 = 1_F \in F$). Whether $f(x)$ is separable or not depends on F. Determine, with proof, precisely the fields F over which $f(x)$ is separable.

[Hint: This may be a challenging problem. It turns out that whether f is separable or not depends entirely on the characteristic of F. You will get partial credit for stating our general separability criterion, and for proving that f is/isn't separable in certain characteristics.]

Recall that f is separable if and only if it has distinct roots over its splitting field, and that f has a multiple root precisely when $\gcd(f, Df) = 1$. Now $Df = 4x^3 - 8$, and if char $F = 2$, $Df = 0$, so $\gcd(f, Df) = f \neq 1$, and f is not separable.

So assume that char $F \neq 2$, and do division with remainder: $x^4 - 8x - 2 = \frac{1}{4}x(4x^3 - 8) + (-6x - 2)$. If $g(x)$ is a factor of $f(x)$ and $Df(x)$, then it must also be a factor of $6x + 2$ since $6x + 2 = -f(x) + \frac{1}{4}xDf(x)$. Conversely, if $g(x)$ is a factor of $6x + 2$ and $Df(x)$, then it must also be a factor of $f(x)$.

So our problem now reduces to computing when $Df(x)$ and $6x+2$ have a common (nontrivial) factor. (Note: we could have used any two of $f, Df, 6x + 2$; this way is easiest). If char $F = 3$, $6x + 2 = 2$ is constant, so Df and $6x + 2$ won't have a common root. Otherwise, the only root of $6x + 2$ is $-\frac{1}{3}$, so we need to see when $Df(x)$ has $-\frac{1}{3}$ as a root. Plugging it in gives

$$Df\left(-\frac{1}{3}\right) = 4\left(-\frac{1}{3}\right)^3 - 8 = -\frac{4}{3^3}(1 + 2 \cdot 3^3),$$

which equals 0 precisely when $0 = 2 \cdot 3^3 + 1 = 55$. Factoring into primes, $55 = 5 \cdot 11$, so f won't be separable if the characteristic of F is one of these primes. Therefore, we conclude, f is separable if and only if char $F \neq 2, 5, 11$. (Since you don't have a calculator, fine if you say f is separable if and only if char F is not 2 and doesn't divide $2 \cdot 3^3 + 1$)

4. (15 points) **True or False**

For each of the following, determine if the statement is true or false, and **clearly circle** the correct answer. You do *not* need to justify your answers.

(a) (3 points) Recall that ζ_m denotes a primitive mth root of 1. If $d|n$ with $1 < d < n$, then $\mathbb{Q}(\zeta_d)$ is a proper subfield of $\mathbb{Q}(\zeta_n)$.

True **False**

False, and a counterexample was given by a homework exercise, Dummit & Foote Problem 13.6.3. For instance, if $d = 3, n = 6$, then $\phi(3) = \phi(6) = 2$, so the cyclotomic polynomials Φ_3 and Φ_6 are both degree 2, and the cyclotomic fields $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_6)$ are both are degree 2 extensions of $\mathbb{Q}$. Therefore, we can't have $\mathbb{Q}(\zeta_3) \subsetneq \mathbb{Q}(\zeta_6)$ (It's not necessary for the proof, but we can see that in fact they are equal. $\zeta_3 = \zeta_6^2 \in \mathbb{Q}(\zeta_6)$, and $\zeta_6 = \zeta_3 + 1 \in \mathbb{Q}(\zeta_3)$.)

(b) (3 points) Let $f(x) \in F[x]$, and let K be the splitting field for f over F. If f is not separable, then K/F is not Galois.

True **False**

False. For instance, $\mathbb{Q}(i)$ is the splitting field for $(x^2+1)^2$, which is not a separable polynomial.

(c) (3 points) Let F be a field of characteristic p such that the Frobenius map is an isomorphism. Then $x^p - a$ is reducible for all $a \in F$.

True **False**

True. Since the Frobenius map $\phi : x \mapsto x^p$ is onto, there exists an element $b := \phi^{-1}(a) \in F$, and $b^p = a$, so b is a root of $x^p - a$ contained in F, and thus $x^p - a$ (which has degree ≥ 2) is reducible.

(d) (3 points) Let H_1 and H_2 be subgroups of $\mathrm{Aut}(K)$, and let $H = H_1 \cap H_2$. Then Fix H contains the composite field (Fix H_1)(Fix H_2)

True **False**

True. Since $H \leq H_1$, reverse inclusion tells us that Fix $H_1 \subseteq$ Fix H. Similarly, since $H \leq H_2$, reverse inclusion tells us that Fix $H_2 \subseteq$ Fix H. Since Fix H is a field containing the two fields Fix H_1 and Fix H_2, it must contain their composite field, as that is the smallest field containing Fix H_1 and Fix H_2.

(e) (3 points) Let F be a field, with algebraic closure $\overline{F}$. If K is an extension field of $\overline{F}$ such that $K \neq \overline{F}$, then $[K : \overline{F}]$ is infinite.

True **False**

True. Since $\overline{F}$ is an algebraic closure, it is algebraically closed. Therefore, every element of K that is algebraic over $\overline{F}$ is contained in $\overline{F}$. Since K is strictly larger, it must contain an element which is transcendental over F, so $[K : F] = \infty$.