Solutions to Math 418 Midterm Exam 2 — Mar. 21, 2024

1. (12 points) **True or False**

   For each of the following, determine if the statement is (always) true. Give a proof if it is, and give a counter-example if otherwise.

   (a) (6 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 $\mathbb{Q}(\zeta_n)$.

   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) (6 points) Let $f(x) \in \mathbb{Z}[x]$, and consider the canonical projection of $f(x) \mapsto \overline{f}(x) \in \mathbb{F}_p[x]$. If f is irreducible, then $\overline{f}$ must be irreducible.

   False. One example is $f(x) = x^2 + 2$. This is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, but over $\mathbb{F}_2$, $\overline{f}(x) = x^2 = x \cdot x$ is reducible.

2. (25 points) Let $f(x) = x^3 - 23 \in \mathbb{Q}[x]$, 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 23, but do note that it is prime)*

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

   The positive real cube root of 23, $\sqrt[3]{23}$, is a root of f, and the three roots are $\sqrt[3]{23}, \zeta_3\sqrt[3]{23}, \zeta_3^2\sqrt[3]{23}$. Now, $K = \mathbb{Q}(\sqrt[3]{23}, \zeta_3)$ since the other two roots can be written in terms of $\sqrt[3]{23}$ and ζ_3, and ζ_3 can be written as a quotient of two of the roots. By the Tower Law,

   $$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{23})][\mathbb{Q}(\sqrt[3]{23}) : \mathbb{Q}].$$

   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

   $$\sigma : \begin{cases} \sqrt[3]{23} \mapsto \zeta_3\sqrt[3]{23}, \\ \zeta_3 \mapsto \zeta_3, \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{23} \mapsto \sqrt[3]{23}, \\ \zeta_3 \mapsto \zeta_3^2. \end{cases}$$

   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

   $$\sigma\tau = \tau\sigma^2 : \begin{cases} \sqrt[3]{23} \mapsto \zeta_3\sqrt[3]{23}, \\ \zeta_3 \mapsto \zeta_3^2, \end{cases}$$

(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. (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 (monic) polynomial over $\mathbb{Q}$ for $\cos 80°$ (and prove that this is indeed the minimal polynomial for $\cos 80°$ over $\mathbb{Q}$).

Note that $\cos 240° = -\cos 60° = -\frac{1}{2}$, so by the triple angle formula, $\beta := \cos 80°$ 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.

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) Similarly, reduce $g(x)$ modulo $p = 2$. if $f(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{F}_p$, then it is irreducible over $\mathbb{Q}$. This is a combination of Propositions 13.5 (Gauss' Lemma) and 13.12 in Dummit and Foote.

5) $g(x+1) = 8(x+1)^3 - 6(x+1) + 1 = 8x^3 + 24x^2 + 18x + 3$, which is irreducible by Eisenstein's criterion with the prime 3.

Therefore, g and f are both irreducible over $\mathbb{Q}$, and so f is the minimal polynomial for β.

   (b) (5 points) Prove that $\cos 80°$ is not constructible using straightedge and compass (which implies that the angle $80°$ 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.

4. (20 points) Let F be a field, and consider the polynomial $f(x) = x^5 - 10x + 5 \in F[x]$ (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 $Df = 5x^4 - 10$, and if $\mathrm{char}\, F = 5$, $Df = 0$, so $\gcd(f, Df) = f \neq 1$, and f is not separable.

So assume that $\mathrm{char}\, F \neq 5$, and do division with remainder: $x^5 - 10x + 5 = \frac{1}{5}x(5x^4 - 10) + (-8x + 5)$. If $g(x)$ is a factor of $f(x)$ and $Df(x)$, then it must also be a factor of $8x - 5$ since $8x - 5 =$

$-f(x) + \frac{1}{5}xDf(x)$. Conversely, if $g(x)$ is a factor of $8x-5$ and $Df(x)$, then it must also be a factor of $f(x)$.

So our problem now reduces to computing when $Df(x)$ and $8x-5$ have a common (nontrivial) factor. (Note: we could have used any two of $f, Df, 8x-5$; this way is easiest). If char $F = 2$, $8x-5 = -5$ is constant, so Df and $8x-5$ won't have a common root. Otherwise, the only root of $8x-5$ is $\frac{5}{8}$, so we need to see when $Df(x)$ has $\frac{5}{8}$ as a root. Plugging it in gives

$$Df\left(\frac{5}{8}\right) = 5\left(\frac{5}{8}\right)^4 - 10 = \frac{5}{8^4}(5^4 - 2^{13}),$$

which equals 0 precisely when $0 = 2^{13} - 5^4 = 7567$. Factoring into primes, $7567 = 7 \cdot 23 \cdot 47$, 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 $F \neq 5, 7, 23, 47$. (Since you don't have a calculator, fine if you say f is separable if and only if char $F | 2^{13} - 5^4$)