Solutions to Math 418 Midterm Exam 1 — Feb. 15, 2024

1. (20 points) Prove that each of the following polynomials is irreducible over the given ring.
   (a) (5 points) $f(x) = x^5 - 10x + 5$ over $\mathbb{Q}$.

   This is an application of Eisenstein's criterion with the prime 5.

   (b) (5 points) $g(x) = x^3 + 2024x^2 + 13x + 105$ over $\mathbb{Q}$.

   Reducing modulo 2 gives $\overline{g(x)} = x^3 + x + 1 \in \mathbb{F}_2[x]$, and plugging in 0 and 1, we see that this has no root. Since it is cubic, it is irreducible over $\mathbb{F}_2$; thus over $\mathbb{Q}$.

   (c) (5 points) $h(x) = x^2 + x + \sqrt{2}$ over $\mathbb{Z}[\sqrt{2}]$.

   Since $\mathbb{Z}[\sqrt{2}]$ is a UFD, we apply the rational root theorem. Any root must divide $\sqrt{2}$, and pluggin in the divisors, $\pm 1, \pm\sqrt{2}$, shows that no such root exists. Since h has degree 2, it is irreducible.

   (d) (5 points) $k(x) = x^2 - p$ over $\mathbb{Z}[i]$, where $p \in \mathbb{Z}$ is a (positive) prime number with $p \equiv 3 \mod 4$.

   We have proven that p is irreducible over the Gaussian integers $\mathbb{Z}[i]$, so in particular it is not a square in $\mathbb{Z}[i]$. Therefore, $k(x)$ doesn't have a root since this would be a square root of p, so since it is degree 2 means it's irreducible.

2. (20 points) Let $f(x) = x^5 - 10x + 5 \in \mathbb{Q}[x]$. By the previous problem, it is irreducible.
   (a) (10 points) Let $\theta \in \mathbb{Q}$ be a root of $f(x)$. Compute θ^{-1} (as a polynomial in θ) in the extension field $\mathbb{Q}(\theta)$.

   Let $\theta^{-1} = a + b\theta + c\theta^2 + d\theta^3 + e\theta^4$. Then

   $$1 = \theta\theta^{-1} = a\theta + b\theta^2 + c\theta^3 + d\theta^4 + e(10\theta - 5) = -5e + (a + 10e)\theta + b\theta^2 + c\theta^3 + d\theta^4,$$

   and solving for the coefficients we obtain $\theta^{-1} = -\frac{1}{5}\theta^4 + 2$.

   (b) (10 points) Let $\alpha, \beta \in \mathbb{C}$ be roots of f. (You may take for granted that such roots exist). Prove that $5 \leq [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leq 20$.

   By the Tower Law, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$, and the second factor on the right is 5 since the minimal polynomial for α has degree 5. Now consider the minimal polynomial $g(x)$ for β over $\mathbb{Q}(\alpha)$. Since $f(\beta) = 0$ $g|f$, but g can't equal f since the latter has a root $\alpha \in \mathbb{Q}(\alpha)$ and hence is reducible over $\mathbb{Q}(\alpha)$. Therefore, $\deg g < 5$, so it ≤ 4.

3. (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

   $$m = a \cdot u^{-1}up_1^{g_1 - e_1} \cdots p_n^{g_n - e_n},$$

   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 the homework 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.

4. (20 points) Let p and q be distinct prime numbers (i.e. positive primes in $\mathbb{Z}$).

(a) (10 points) Prove that $\sqrt{p} \notin \mathbb{Q}(\sqrt{q})$.

If $p \in \mathbb{Q}(\sqrt{q})$, then $\sqrt{p} = a + b\sqrt{q}$ for some $a, b \in \mathbb{Q}$. Then $p = a^2 + qb^2 + 2ab\sqrt{q}$. Since $p \in \mathbb{Z}$, we must have $ab = 0$, so either $p = a^2$ or $p = qb^2$. Either of these factorizations contradicts the assumption that p is a prime distinct from q.

(b) (10 points) Prove that $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = 4$.

By the Tower Law,

$$[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})][\mathbb{Q}(\sqrt{p}) : \mathbb{Q}].$$

The minimal polynomial for $\sqrt{p}$ over $\mathbb{Q}$ is $x^2 - p$, irreducible over $\mathbb{Q}$ by Eisenstein, so $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$. Now, $\sqrt{q}$ is a root of the degree-2 polynomial $x^2 - q \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\sqrt{p})[x]$, so $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})]$ is either 1 or 2. If it is 1, then $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p})$, so $\sqrt{q} \in \mathbb{Q}(\sqrt{p})$, contradicting part (a).