Solutions to Math 418 Midterm Exam 1 — Feb. 19, 2025

1. (20 points) Prove that each of the following polynomials is irreducible over the given ring.

   (a) (5 points) $f(x) = x^4 + 8x + 6$ over $\mathbb{Q}$.

   This is an application of Eisenstein's criterion with the prime 2.

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

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

   (c) (5 points) $h(x) = x^3 + 2x^2 + 2025x + 16$ over $\mathbb{Q}$.

   Since $h(x) \in \mathbb{Z}[x]$, we can reduce modulo primes.
   Reducing modulo 3 gives $\overline{h(x)} = x^3 + 2x^2 + 1 \in \mathbb{F}_3[x]$, and plugging in 0, 1, and 2, we see that $\overline{h(0)} = 1, \overline{h(1)} = 1, \overline{h(2)} = 2$, so $\overline{h(x)}$ has no root in $\mathbb{F}_3$. Since it is cubic, it is irreducible over $\mathbb{F}_3$; thus over $\mathbb{Q}$.
   If you'd rather reduce modulo 5, that works too. Coincidentally, $\overline{h(x)} = x^3 + 2x^2 + 1 \in \mathbb{F}_5[x]$, and plugging in 0, 1, 2, 3, and 4 we see that $\overline{h(0)} = 1, \overline{h(1)} = 4, \overline{h(2)} = 2, \overline{h(3)} = 1, \overline{h(4)} = 2$, so $\overline{h(x)}$ has no root in $\mathbb{F}_5$. Since it is cubic, it is irreducible over $\mathbb{F}_5$; thus over $\mathbb{Q}$.
   (There are some tricks that help here, like the fact that multiples of 5 end in 5 or 0, and that multiples of 3 have digits which add up to 3. When computing powers modulo 5, note that $3 \equiv -2$ and $4 \equiv -1$; the latter elements might be easier to work with.)

   (d) (5 points) $k(x) = x^2 - 2x + \sqrt{-2}$ over $\mathbb{Q}(\sqrt{-2})$. *(You may assume that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.)*

   Since it is a Euclidean domain, $\mathbb{Z}[\sqrt{-2}]$ is a UFD (and we've seen this on the homework, too). We apply the rational root theorem to show that $k(x)$ is irreducible over $\mathbb{Z}[\sqrt{-2}]$. Any root must divide $\sqrt{-2}$, and plugging in the divisors, $\pm 1, \pm\sqrt{-2}$, shows that no such root exists. Since k has degree 2, it is irreducible. By Gauss' Lemma, $k(x)$ is also irreducible over the field of fractions $\mathbb{Q}(\sqrt{-2})$.
   (Alternatively, we can use Eisenstein's criterion with the prime $\sqrt{-2}$, along with Gauss' Lemma.)

2. (10 points) Let $f(x) = x^4 + 8x + 6 \in \mathbb{Q}[x]$. By the previous problem, it is irreducible. 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 $\theta^{-1} = a + b\theta + c\theta^2 + d\theta^3$. Then

$$1 = \theta\theta^{-1} = a\theta + b\theta^2 + c\theta^3 + d(-8\theta - 6) = -6d + (a - 8d)\theta + b\theta^2 + c\theta^3,$$

and solving for the coefficients we obtain $d = -\frac{1}{6}, a = 8d = -\frac{4}{3}, b = c = 0$, so $\theta^{-1} = -\frac{4}{3} - \frac{1}{6}\theta^3$.

3. (10 points) Let R be a Euclidean domain, with norm $N : R \to \mathbb{Z}_{\geq 0}$. Let m be the minimum integer in the set of norms of nonzero elements of R i.e.

$$m = \min\{N(a) | a \in R \setminus \{0\}\}.$$

Prove that every nonzero element of R of norm m is a unit.

Let $b \in R \setminus \{0\}$ such that $N(b) = m$. Since R is a Euclidean domain, there exist $q, r \in R$ such that $1 = qb + r$ and either $r = 0$ or $N(r) < N(b)$. Since no nonzero element of r has norm less than $N(b)$, $r = 0$, so $1 = qb$, and so b is a unit.

Note: norms don't have to be multiplicative, even Euclidean norms (e.g. the degree norm for $\mathbb{Q}[x]$). If we are dealing with a multiplicative norm, we have a sort of converse: every unit has norm 1 (or everything has norm 0). But our norm in this problem is *not* necessarily multiplicative.

4. (15 points) Let K/F be a field extension of degree 2. Suppose $f(x) \in F[x]$ is an irreducible polynomial in $F[x]$ of degree 6. Prove that in $K[x]$ either $f(x)$ is irreducible or it is the product of two irreducible cubic polynomials.

Assume without loss of generality that f is monic (otherwise, scale it to be monic, and the set of roots is preserved). Let $g(x)$ be an irreducible factor of $f(x)$ in $K[x]$, and let α be a root of g in some field extension of K. Since $g|f$, α is also a root of f. Recall that the minimal polynomial of α is the unique monic irreducible polynomial with α as a root. Since f is irreducible over F and g is irreducible over K, $f(x) = m_{\alpha,F}(x)$ and $g(x) = m_{\alpha,K}(x)$, so $[F(\alpha) : F] = \deg(f) = 6$ and $[K(\alpha) : K] = \deg(g)$.

Using the Tower Law, we compute the degree of the field extension $K(\alpha)/F$ in two ways:

$$6[K(\alpha) : F(\alpha)] = [K(\alpha) : F(\alpha)][F(\alpha) : F] = [K(\alpha) : F] = [K(\alpha) : K][K : F] = 2 \deg g,$$

so $3 | \deg g$. On the other hand, since $g|f$ and $\deg f = 6$, $\deg g \leq 6$. The only degrees which satisfy both conditions are 3 and 6, so $g(x)$ has degree 3 or 6, as desired.

5. (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.

(*The exam initially said incorrectly that this question was worth 12 points; however, further reflection has revealed that in fact* $5 \cdot 3 = 15$)

(a) (3 points) There exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ with $1/2$ as a root.

True **False**

False. This would contradict the rational root theorem.

(b) (3 points) Suppose $K/\mathbb{Q}$ is a field extension of degree 2 and $K \subseteq \mathbb{C}$. Then $K = \mathbb{Q}(\sqrt{d})$ for some $d \in F$.

True **False**

True. Since $[K : \mathbb{Q}] = 2$, by the Tower Law and the fact that 2 is prime, any element $\alpha \in K \setminus \mathbb{Q}$ must have a degree 2 minimal polynomial over $\mathbb{Q}$, and by the same reasoning, $K = \mathbb{Q}(\alpha)$. The quadratic formula tells us that the roots of this polynomial in $\mathbb{C}$ are of the form $\frac{-b \pm \sqrt{D}}{2a}$ for some rational numbers a, b, D. Therefore,

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}\left(\frac{-b \pm \sqrt{D}}{2a}\right) = \mathbb{Q}(\sqrt{D}).$$

(c) (3 points) Suppose R is a ring where every pair of non-units r, s have a gcd g. Then there exists $a, b \in R$ with $ar + bs = g$.

True **False**

False. For a counterexample, consider $F[x, y]$. $\gcd(x, y) = 1$, but 1 is not a linear combination of x and y.

(d) (3 points) The ring $\mathbb{Z}[i]/(2)$ is the field with 4 elements.

True **False**

False. This quotient ring will be a field if 2 is irreducible in $\mathbb{Z}[i]$, but it is not, since $2 = (1+i)(1-i)$, and neither $1 + i$ nor $1 - i$ are units.

(e) (3 points) Let R be an integral domain, and let a be a nonzero element of R. If (a) is a maximal ideal, then a is irreducible.

True **False**

True. Maximal ideals are prime. A principal ideal (a) is prime if and only if the element a is prime. And prime elements are irreducible. All of these facts hold in any integral domain (the reverse of the first and third implications need extra conditions on R).