December 8, 2025

**Problem Set 12**

**Exercise 1.** Find the units and irreducible elements in the ring $\mathbb{Z}/4\mathbb{Z}$.

**Exercise 2.** (a) Let $K$ be a field and $p(X) \in K[X]$. Show that if for $\alpha \in K$, we have $p(\alpha) = 0$, then $X - \alpha$ divides $p$.

(b) Let $p(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$, $a_n \neq 0$. Suppose that $\frac{r}{s} \in \mathbb{Q}$ is a root of $p(X)$, such that $\gcd(r, s) = 1$, so that we have $p(\frac{r}{s}) = 0$. Show that $s|a_n$ and $r|a_0$ in $\mathbb{Z}$. In particular, if $p(X)$ is monic (i.e., $a_n = 1$), the only rational roots of $p(X)$ are integers. Use this property to determine which of the following polynomials are irreducible in $\mathbb{Q}[X]$.

$$X^2 - 2, \qquad X^3 + X + 1,$$
$$X^3 + 2X^2 - 3, \qquad 2X^9 - X - 1, \qquad 5X^3 - 2X^2 + 6$$

**Exercise 3.** Show that the polynomial $X^3 + 462X^2 + 2433X - 67692$ is irreducible over $\mathbb{Q}$.
*Hint:* Use the Eisenstein criterion.

**Exercise 4.** (Chinese remainder theorem for polynomial rings). Find a polynomial $f(X) \in \mathbb{Q}[X]$ such that

$$\begin{cases} f \equiv X \pmod{X^2 + 1} \\ f \equiv -1 \pmod{X - 1} \\ f \equiv X + 2 \pmod{X^2 - 4}. \end{cases}$$

**Exercise 5.** Let $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ be the field of 5 elements. Use the Euclidean algorithm in $\mathbb{F}_5[x]$ to find $F$, the monic greatest common divisor of the given polynomials $P = 3x^5 + x + 1$ and $Q = x^2 + 3x + 1$. Then use Bezout's theorem to express $F$ in the form $F = aP + bQ$, where $a, b \in \mathbb{F}_5[x]$.