Math 566 - Homework 8
Due Wednesday April 10, 2024

1. Let $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, $a_n \neq 0$ be primitive, and let p be a prime number. Let
$$\overline{f} = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n \in \mathbb{Z}_p[x],$$
where $\overline{a}$ is the image of a in $\mathbb{Z}_p$ under the canonical map $\mathbb{Z} \to \mathbb{Z}_p$ from the integers to the integers modulo p.
   (i) Show that if f is monic and $\overline{f}$ is irreducible in $\mathbb{Z}_p[x]$ for some prime p, then f is irreducible in $\mathbb{Z}[x]$.
   (ii) Show the result still holds if we replace "f is monic" with "a_n is not a multiple of p".
   (iii) Give an example to show that the conclusion may fail to hold if a_n is divisible by p.

2. Prove that if F is a field, and $n \geq 2$, then $F[x_1, \ldots, x_n]$ is not a PID.

3. In $\mathbb{Z}$, given any $n > 1$, for every $a > 0$ there exist unique $r \geq 0$, and integers $a_0, \ldots, a_r$, $0 \leq a_i < n$, $a_r \neq 0$, such that
$$a = a_0 + a_1n + a_2n^2 + \cdots + a_rn^r;$$
that is, we can write every number in "base n", and the digits are uniquely determined. Prove the following analog for polynomials:

   Let F be a field, and let $g \in F[x]$, $\deg(g) \geq 1$. Prove that for every nonzero $f \in F[x]$ there exist unique $r \geq 0$ and polynomials $f_0, \ldots, f_r \in F[x]$, each f_i either equal to 0 or with $\deg(f_i) < \deg(g)$, and $f_r \neq 0$, such that
$$f = f_0 + f_1g + \cdots + f_rg^r;$$
that is, we can express every polynomial uniquely in "base g."

4. We prove **Schönemann's Irreducibility Criterion.** Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with integer coefficients, $\deg(f) = n > 0$, and assume that there exists a prime p, and integer a, and a polynomial $\mathcal{F}(x) \in \mathbb{Z}[x]$ such that
$$f(x) = (x-a)^n + p\mathcal{F}(x) \quad \text{and } \mathcal{F}(a) \not\equiv 0 \pmod{p}.$$
We will prove that if this occurs, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.
   (i) Show that the leading coefficient of f is not divisible by p.
   (ii) Assume that $f(x) = G(x)H(x)$ with $G(x)$, $H(x)$ polynomials with integer coefficients. Let $\overline{f(x)}$, $\overline{G(x)}$ and $\overline{H(x)}$ denote the images of $f(x)$, $G(x)$, and $H(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ obtained by reducing the coefficients modulo p. Prove that we have $\deg(\overline{G(x)}) = \deg(G(x))$ and $\deg(\overline{H(x)}) = \deg(H(x))$.
   (iii) Show that $\overline{G(x)} = (x-\overline{a})^i$ and $\overline{H(x)} = (x-\overline{a})^j$ for some nonnegative integers i, j with $i + j = n$.
   (iv) Show that if $i, j > 0$, then $G(a) \equiv H(a) \equiv 0 \pmod{p}$.
   (v) Show that if $i, j > 0$, then $p\mathcal{F}(a) \equiv 0 \pmod{p^2}$, and reach a contradiction.
   (vi) Conclude that $f(x)$ is irreducible in $\mathbb{Q}[x]$.