1 Homework 3.

1. Prove that the following polynomials are irreducible.

   (a) $f(x) := x^{p-1} + x^{p-2} + \cdots + 1$ where p is a prime number.

   (b) $g(x, y) := x^{p-1} + q_2(y)x^{p-2} + \cdots + q_{p-1}(y)$ in $\mathbb{Q}[x, y]$ where p is prime and $q_i(y)$'s are in $\mathbb{Q}[y]$ such that $q_i(1) = 1$ for all i.

   (c) $h(x) := 1 + \frac{x}{1!} + \cdots + \frac{x^p}{p!}$ in $\mathbb{Q}[x]$ where p is prime.

   (d) $k(x, y) := x^n - y$ in $F[x, y]$ where F is a field.

   (e) $p(x, y) := x^2 + y^2 - 2$ in $F[x, y]$ where F is a field and its characteristic is not 2.

   (f) $q(x) := x^4 + 12x^3 - 9x + 6$ in $\mathbb{Q}[i][x]$.

   (g) Suppose n is a positive odd integer. Prove that

   $$r(x) := (x - 1)(x - 2) \cdots (x - n) + 1$$

   is irreducible in $\mathbb{Q}[x]$.

(**Hint**. (a) Argue that $f(x)$ is irreducible precisely when $\overline{f}(x) := f(x + 1)$ is irreducible. Notice that

$$\overline{f}(x) = \frac{(x + 1)^p - 1}{x}.$$

Use Eisenstein's criterion and show that $\overline{f}(x)$ is irreducible in $\mathbb{Q}[x]$.

(b) Notice that $\mathbb{Q}[y]$ is a UFD and $\langle y - 1\rangle$ is a maximal ideal of $\mathbb{Q}[y]$. Argue that if $g(x, y)$ is not irreducible in $(\mathbb{Q}[y])[x]$, then there are monic polynomials $g_1, g_2 \in (\mathbb{Q}[y])[x]$ that are of x-degree less than $p - 1$ and $g = g_1g_2$. Look at both side modulo $\langle y - 1\rangle$; this is the same as saying that you are evaluating both sides at $y = 1$. Argue why you get a contradiction.

(c) Multiply by $p!$, and use a criterion.

(d) y is irreducible in $F[y]$ and $F[y]$ is a UFD.

(e) $y^2 - 2$ is square-free in $F[y]$ and $F[y]$ is a UFD.

(f) Think about irreducible factors of the coefficients and Eisenstein's criterion. Notice that $\mathbb{Z}[i]$ is a UFD.

(g) Suppose the contrary. Argue that there exist $r_1, r_2 \in \mathbb{Z}[x]$ of positive degree such that $r(x) = r_1(x)r_2(x)$. Consider $r(j)$ for integer j in $[1, n]$, and think about $r_1(x)^2 - 1$ and $r_2(x)^2 - 1$.)

2. Suppose p is a prime in $\mathbb{Z}$, $a \in \mathbb{Z}$, and $p \nmid a$. Prove that $x^{p^n} - x + a$ does not have a zero in $\mathbb{Q}$.

   (**Hint.** Use the rational root criterion and Fermat'a little theorem.)

3. Suppose D is an integral domain. Prove that D is a PID if and only if D is a UFD and $\langle a, b\rangle = \langle \gcd(a, b)\rangle$ for all $a, b \in D \setminus \{0\}$.

   (**Hint**. ($\Leftarrow$) Prove that every finitely generated ideal of D is principal. Argue that for every non-zero non-unit element a of D

$$\{\langle d\rangle \mid d|a\}$$

   is finite.)