HW 11, due Tuesday, April 21 *Math 332*

1. Let k be a field.

   (a) Let $a_1, \ldots, a_{n+1}$ be distinct elements of k, and let $b_1, \ldots, b_{n+1}$ be any elements of k. Define
   $$f(x) = \sum_{i=1}^{n+1} \left(b_i \prod_{j \neq i} \frac{(x - a_j)}{(a_i - a_j)} \right).$$
   Show that f is the unique polynomial of degree n in $k[x]$ such that $f(a_i) = b_i$ for $i = 1, \ldots, n+1$.

   (b) Find a polynomial $f \in \mathbb{R}[x]$ of degree 3 whose graph goes through the points $(1,0)$, $(2,-1)$, $(3,0)$, and $(4,1)$.

2. Let $p \in \mathbb{Z}$ be prime.

   (a) Prove that $x^{p-1} - 1 = \prod_{i=1}^{p-1}(x - i)$ in $\mathbb{Z}_p[x]$.

   (b) Prove that $(p-2)! = 1 \bmod p$.

3. Let R be an integral domain.

   (a) Show that $p \in R$ is prime iff (p) is a prime ideal.

   (b) Elements $a, b \in R$ are *associates* if $a = ub$ for some unit $u \in R$. Prove that $a, b \in R$ are associates iff they generate the same ideals: $(a) = (b)$.

4. Find all maximal ideals $I = (f)$ in $\mathbb{Z}_5[x]$ where $f = x^2 + ax + b$ for some a, b.

5. Factor $f = x^3 + x^2 + x + 1$ completely over $\mathbb{Z}_5$, over $\mathbb{Q}$, and over $\mathbb{C}$.

6. Indicate, with justification, whether the following polynomials are reducible over $\mathbb{Q}$.

   (a) $f(x) = 23x^8 + 12x^5 - 24x^2 + 18x - 12$.

   (b) $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

   (c) $f(x) = 3x^4 + 5x + 1$.

   (d) $f(x) = x^6 + 2x^3 - 3x^2 + 1$.

7. (a) Show that $x^4 + 1$ is irreducible over $\mathbb{Q}$. (Finding the polynomials zeros in $\mathbb{C}$ does not count as a proof. You might try Eisenstein.)

   (b) Show that for every prime $p \in \mathbb{Z}$, either -1, 2, or -2 is a perfect square in $\mathbb{Z}_p$. (Hint: The set of squares in $\mathbb{Z}_p^*$ forms a multiplicative subgroup of index 2. Hence, $\mathbb{Z}_p^*$ modulo the squares is a group of order 2. Use this to show that if -1 and 2 are not perfect squares, then -2 is a perfect square.)

(c) Show that $x^4 + 1$ is reducible modulo each prime $p \in \mathbb{Z}$.

(d) Factor $x^4 + 1$ completely over $\mathbb{Z}_2$ and over $\mathbb{Z}_3$.

(e) Why don't 7a and 7c contradict Theorem 35.8 in the notes?

8. Generalized Euclidean algorithm.

   (a) Let R be a PID, and $a_1, \ldots, a_n \in R$. Show that $(a_1, \ldots, a_n) = (\gcd(a_1, \ldots, a_n))$. (For the definition of gcd, see page 59 of the notes. It follows that $\gcd(a_1, \ldots, a_n)$ can be written as an R-linear combination of $a_1 \ldots, a_n$.)

   (b) In the case of $R = k[x]$, k a field, we have the division algorithm, as we do in $\mathbb{Z}$. And just like the case of $\mathbb{Z}$, keeping track of remainders in the division algorithm allows us to write the gcd of a set of elements as an R-linear combination of those elements.

   Let $f = x^4 + 5x^3 + 5x^2 - 5x - 6$ and $g = x^3 + 4x^2 - 9x - 36$.

      i. Calculate $\gcd(f, g)$ in $R = \mathbb{R}[x]$.

      ii. Write $\gcd(f, g)$ as an R-linear combination of f and g.