Math 500, Homework 5, due October 27

(1) Let R be a ring (commutative with one, as always) and $S \subset R$ a subset. The *ideal generated by* S, written (S), is the intersection of all ideals of R that contain the subset S. Prove that

$$(S) = \{a_1 s_1 + \cdots + a_n s_n \ : \ a_i \in R, s_i \in S \text{ for all } i\}.$$

(2) Prove that, if R is a UFD and $a_1, \ldots, a_n$ are elements of R, then a greatest common divisor of $a_1, \ldots, a_n$ exists.

(3) Prove that, in a UFD, an element is irreducible if and only if it is prime.

(4) If $f = \sum_{i=0}^{n} a_i x^i \in \mathbf{Z}[x]$, and p is a prime number, let $\overline{f} = \sum \overline{a}_i x^i \in (\mathbf{Z}/p\mathbf{Z})[x]$, where $\overline{a}_i$ is the image of a_i under the canonical homomorphism $\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$.
   (a) Prove that if f is monic (that is, $a_n = 1$) and $\overline{f}$ is irreducible in $(\mathbf{Z}/p\mathbf{Z})[x]$ for some prime p, then f is irreducible in $\mathbf{Z}[x]$.
   (b) Give an example to show that the conclusion does not hold without the assumption that f is monic.

(5) Suppose that R is a UFD. Prove that if $a, b \in R$ are relatively prime (that is, their gcd is 1) and, for some $c \in R$, that a divides bc, then a divides c.

(6) Prove that the polynomial $xw - yz$ is irreducible in $\mathbf{Z}[x, y, z, w]$; it then follows that $R = \mathbf{Z}[x, y, z, w]/(xw - yz)$ is a domain (why?). Prove that R is not a UFD. [Hint: prove that x, y, z, and w are irreducible elements, and use this to prove that factorizations aren't unique.]

(7) Use Zorn's Lemma to prove that every vector space (finite or infinite-dimensional) over a field has a basis.

(8) Prove that $f(x) = x^4 - 10x^2 + 1$ is irreducible in $\mathbf{Q}[x]$. [Hint: First prove that it cannot have a root in $\mathbf{Q}$. Then consider a factorization as a product of quadratics and prove that such a factorization also cannot exist.]

(9) Prove that the subring $R = \{a + b(1 + i\sqrt{19})/2 \ : \ a, b \in \mathbf{Z}\}$ of the complex numbers is a PID but is not a Euclidean domain.