Math 536 Homework 8
Spring 2008
Due: Friday, March 21

1. (Euclid's algorithm for finding the gcd.) Let a_1, a_2 be nonzero elements of a Euclidean domain R. Define a_i and q_i recursively by $a_1 = q_1 \cdot a_2 + a_3, a_i = q_i a_{i+1} + a_{i+2}$ where $\delta(a_{i+2}) < \delta(a_{i+1})$. Show that there exists an n such that $a_n \neq 0$ but $a_{n+1} = 0$, and that $\gcd(a_1, a_2) = a_n$. Also use the equations to obtain an expression for the gcd in the form $xa_1 + ya_2$.

2. Let A be a PID and $a_1, \ldots, a_n$ nonzero elements of A. Let $(a_1, \ldots, a_n) = (d)$. Show that d is a greatest common divisor for the a_i $(i = 1, \ldots, n)$.

3. (a) Let R be a commutative domain, and let a, b be nonzero elements of R. In class we defined the notion of a greatest common divisor of a and b for the domain R. Now define also a *least common multiple* of a and b so that it generalizes the usual definition over the integers.

   (b) Show that in a UFD a least common multiple of two (nonzero) elements a, b always exists.

   (c) Let a, b be two nonzero elements of a commutative domain R (with 1). Assume that $(a) \cap (b)$ is principal, $(a) \cap (b) = (v)$ for some $v \in R$. Show that v is a least common multiple of a and b.

4. (a) Is $X^6 + X^3 + 1$ irreducible in $\mathbb{Q}[X]$?

   (b) Is $X^2 + Y^2 - 1$ irreducible in $\mathbb{Q}[X, Y]$?

5. Prove that if R is a domain which is not a field, then $R[X]$ is not a PID.

6. Let F be a field, and $f(x)$ an irreducible polynomial in $F[x]$. Show that $f(x)$ is irreducible in $F(t)[x]$, t an indeterminate. Here $F(t)$ is the quotient field of $F[t]$.