Math 5031 - Homework 7

Due 10/21/05

1. **The Euclidean algorithm.** An integral domain R with 1 is called *Euclidean* if there is a function $d : R^* \to \mathbb{Z}$, with $d(r) \geq 0$ for all $r \in R^*$, such that

   (a) if $a, b \in R^*$ and $a|b$, then $d(a) \leq d(b)$, and

   (b) if $a, b \in R$, with $b \neq 0$, then there are $q, r \in R$ such that $a = bq + r$, with either $r = 0$ or $d(r) < d(b)$.

   (Examples are: $R = \mathbb{Z}$ with $d(r) = |r|$, or $R = F[x]$, where F is a field and $d(f(x))$ is the degree of $f(x)$.)

   Suppose that R is an Euclidean domain, $a, b \in R$, and $ab \neq 0$. Write

$$\begin{aligned} a &= bq_1 + r_1, & d(r_1) &< d(b), \\ b &= r_1 q_2 + r_2, & d(r_2) &< d(r_1) \\ &\vdots & &\vdots \\ r_{k-2} &= r_{k-1} q_k + r_k, & d(r_k) &< d(r_{k-1}), \\ r_{k-1} &= r_k q_{k+1}, \end{aligned}$$

   with $r_i, q_i \in R$. Show that $r_k = (a, b)$. By solving for r_k in terms of a and b, thereby expressing (a, b) in the form $ua + vb$, with $u, v \in R$, find (a, b) in the following cases:

   (a) $a = 29041, b = 23843,\ R = \mathbb{Z}$;

   (b) $a = x^3 - 2x^2 - 2x - 3,\ b = x^4 + 3x^3 + 3x^2 + 2x,\ R = \mathbb{Q}[x]$;

   (c) $a = 7 - 3i,\ b = 5 + 3i,\ R = \mathbb{Z}[i]$.

2. A ring R is said to be *simple* if the only (two-sided) ideals of R are 0 and R. If F is any field, show that the ring $M_n(F)$ of $n \times n$ matrices over F is a simple ring.

3. **The localization of R at S.** Let R be any commutative ring and let S be a subset of R^* that is a multiplicative semigroup containing no zero divisors. Let X be the Cartesian product $R \times S$ and define a relation $\sim$ on X by agreeing that $(a, b) \sim (c, d)$ if $ad = bc$.

   (a) Show that the relation $\sim$ is an equivalence relation on X.

(b) Denote the equivalence class of (a, b) by a/b and the set of all equivalence classes by R_S. Show that R_S is a commutative ring with 1. This ring is called the *localization* of R at S.

(c) If $a \in S$, show that $\{ra/a \mid r \in R\}$ is a subring of R_S and that $r \mapsto ra/a$ is a monomorphism, so that R can be identified with a subring of R_S.

(d) Show that every $s \in S$ is a unit in R_S.

(e) Give a "universal" definition for the ring R_S and show that R_S is unique up to isomorphism.

(f) Suppose for this and the next item that R is an integral domain and $P \subset R$ is a prime ideal. Show that both P and $R \setminus P$ (the set difference of R minus P) are multiplicative semigroups.

(g) If $S = R \setminus P$, show that $U(R_S) = R_S \setminus R_S P$. Conclude that $R_S P$ is the unique maximal ideal in R_S. (By definition, a ring A is called a *local ring* if it is commutative and has a unique maximal ideal. We may come to see later in the course, I hope, that local rings are important in algebraic geometry.)

4. Show that there is no ring R with 1 whose additive group is isomorphic with $\mathbb{Q}/\mathbb{Z}$.