**Solutions to Homework Set 2**

1) Let $R$ be the ring of $2 \times 2$ matrices with rational entries. Prove that the only ideals of $R$ are $(0)$ and $R$.

**Solution** Suppose $I$ is an ideal of $R$ and $0 \neq A \in I$. Let $\alpha$ be a non-zero entry in $A$, and assume that it lies in row $r$ and column $s$. Let $E_1 \in R$ have all entries 0 except for the $(1, r)$ entry which is 1. Let $E_2 \in R$ have all entries 0 except for the $(s, 1)$ entry which is 1. Since $I$ is a (two sided) ideal, $B = E_1 A E_2 \in I$. But $B$ is the matrix with all entries 0 except for the $(1, 1)$ entry which is $\alpha$. Using a similar argument, we conclude that $C \in I$, where $C$ is the matrix with all entries 0 except for the $(2, 2)$ entry which is $\alpha$. Thus $B + C \in I$. Since $B + C$ is invertible, we conclude that $I = R$.

2) Let $R$ be the ring of all real valued continuous functions on $[0, 1]$. Let $M$ be a maximal ideal of $R$. Prove that there is a real number $\gamma \in [0, 1]$ such that $M = \{f(x) \in R : f(\gamma) = 0\}$. Hint: Proceed by contradiction. Use the fact that $[0, 1]$ is compact, so every open cover of it has a finite subcover.

**Solution** For each $\gamma \in [0, 1]$ we may suppose, for contradiction, that there exists $f \in M$ which does not vanish at $\gamma$ (else $M$ contains all functions that vanish at $\gamma$ and we have already shown that this is maximal, so $M$ is the desired ideal). Since $f$ is continuous, there is a neighborhood $N_\gamma$ around $\gamma$ in which $f(x) > y_\gamma > 0$. This produces a collection of open sets that cover $[0, 1]$ and by compactness, there is a finite subcover $T_1, \ldots, T_n$. We also have functions $f_1, \ldots, f_n$. Now define $g(x) = \sum_{i=1}^{n} (f(x))^2 \in M$. By definition, there exists $c > 0$ such that $g(x) > c$ for all $x \in [0, 1]$. Consequently, $1/g(x) \in M$ since it is continuous. Thus $1 \in M$ and so $M = R$.

3) Let $R$ be a Euclidean ring and $a, b \in R$. The least common multiple $c$ of $a$ and $b$ is an element of $R$ such that $a|c$ and $b|c$ and such that whenever $a|x$ and $b|x$ for $x \in R$, then $c|x$. Prove that such a $c$ exists with $c \times (a, b) = ab$, where $(a, b)$ is the gcd of $a$ and $b$.

**Solution** Clearly $ab$ is a multiple of both $a$ and $b$. Let $c$ be a multiple of both $a$ and $b$ with $d(c)$ as small as possible. Now suppose $x$ is a multiple of both $a$ and $b$. Then $x = lc + r$. If $r = 0$ then we are done. Otherwise, $d(r) < d(c)$ but $a$ and $b$ each divide both $x$ and $lc$ so they also divide $r$. This contradicts the choice of $c$. Now consider $ab/(a, b)$. Since $(a, b)|a$ we have $a = (a, b)q$ and so $ab = (a, b)qb$. Thus $b|ab/(a, b)$ and similarly $a|ab/(a, b)$. Now write $ab/(a, b) = cq + r$. Then since $a|c$ and $b|c$, the previous observation implies that $a|r$ and $b|r$. By definition of $c$, we conclude that $c|r$ and hence $c|ab/(a,b)$. Next we will show that $ab/(a,b)|c$, which is equivalent to $ab|(a,b)c$. Write $(a,b) = ax + by$. Then clearly $ab|axc$ and $ab|byc$ so $ab|(a,b)c$. We conclude that $ab/(a,b) \times u = c$ for some unit $u$. If $c$ has the property of an lcm, then certainly $cu^{-1}$ does as well, so the proof is complete.

4) Define the derivative $f'(x)$ of the polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$ as $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$. Prove that if $f(x) \in F[x]$, where $F$ is the field of rational numbers, then $f(x)$ is divisible by the square of a polynomial (of positive degree) if and only if $f(x)$ and $f'(x)$ have a gcd $d(x)$ of positive degree.

**Solution** First suppose that $h^2|f$ for some $h$ of positive degree. Then $f = h^2 g$ so using the product rule for derivatives, we have $f' = h^2 g' + 2ghh'$ and so clearly $h$ divides both $f$ and $f'$. For the other direction, we will proceed by induction on the degree of $f$. The base case $deg(f) = 1$ is vacuous, so suppose that $deg(f) > 1$. Let $d = (f, f')$ and note that $deg(d) < deg(f)$. Since $d|f$, we conclude that $f = dq$, and so $f' = dq' + qd'$. But $d|f'$ as well, and hence $d|qd'$. Now if $(d, d') = 1$, then we have that $d|q$ and so $d^2|f$. But if $(d, d')$ has positive degree, then by induction $d$ is divisible by a square and so $f$ is as well.