**Shashank Singh**
**sss1@andrew.cmu.edu**
**21-373 Honors Algebraic Structures, Fall 2011**
**Assignment 6**
**Due: Monday, October 24**

**Exercise 36:** Let $R$ be an integral domain equipped with such functions $V$ and $W$. Let non-zero $\xi, \eta \in R$. Since, $\forall y \in R$, $\eta y \in R$, $\{V(\xi\eta y) \,|\, y \in R, y \neq 0\} \subseteq \{V(\xi\eta y) \,|\, y \in R, y \neq 0\}$, so $W(\xi\eta) \geq W(\xi)$.

Suppose $a, b \in R$, with $b \neq 0$. Let $y \in R$ such that $y$ minimizes $V(by)$, so that $W(b) = V(by)$. By construction of $V$, $\exists q_*, r_1 \in R$ such that $ay = byq_* + r_1$, and either $r_1 = 0$ or $r_1 \neq 0$ and $V(r_1) < V(by)$. Since $r_* = (a - qb)y$, $\exists r_* \in R$ such that $r_* = r_* y$. Thus, since $R$ is an integral domain, so that the multiplicative cancellation property holds, $a = q_* b + r_*$. Furthermore, either $r_* = 0$ or $r_* \neq 0$ and $W(r_*) \leq W(r_* y) = W(r_1) \leq V(r_1) < V(by) \leq W(b)$. ■

**Exercise 37:** Let $R$ be a commutative unital ring.

**i.** For some $n \in \mathbb{N}$, let $a_1, a_2, \ldots, a_n \in R$ be nilpotent. Then, for each $i \in \mathbb{N}$ with $1 \leq i \leq n$, letting $p_i = 0 + 0x + 0x^2 + \ldots + a_i x^i + \ldots + 0x^n = a_i x^n$, $p_i$ is also nilpotent (since $x$ commutes with the elements of the ring, so that, if, for some $m \in \mathbb{N}$ with $n \geq 1$, $a_i^m = 0$, then $p_i^m = \left(a_i x^i\right)^m = a_i^m x^{im} = 0x^{im} = 0$). Furthermore, since it was shown in the previous assignment that the sum of two nilpotent elements is also nilpotent, by a simple induction on $n$, it is shown that $a_1 x + a_2 x^2 + \ldots + a_n x^n = \sum_{i=1}^n p_i$ is also nilpotent. Furthermore, since 1 is a unit, it follows from the result of part ii. that $1 + a_1 x + \ldots a_n x^n$ is a unit. ■

**ii.** Suppose $P = a_0 + a_1 x + \ldots + a_n x^n$ is a unit in $R[x]$. Then, $\exists P^{-1} \in R[x]$ such that $PP^{-1} = P^{-1}P = 1$. Thus, $PP^{-1} = a_0 P^{-1} + x(a_1 + a_2 x + \ldots + a_n x^{n-1})P^{-1}$. Since the multiplicative identity is 1, which has no terms containing $x$, $PP^{-1} = a_0 P^{-1} = a_0 b_0 + x a_0 (b_1 + b_2 x + \ldots + b_n x^{n-1})$, where $b_0 + b_1 x + \ldots + b_n x^n = P^{-1}$, so, similarly, $PP^{-1} = a_0 b_0 = b_0 a_0 = 1$. Thus, $b_0 = a_0^{-1}$, so $a_0$ is a unit.

For $n = 0$, clearly $a_1, a_2, \ldots, a_n$ are vacuously nilpotent. Suppose, as an inductive hypothesis, that, for some $n \in \mathbb{N}$, if $P = a_0 + a_1 x + \ldots + a_n x^n$ is a unit in $R[x]$, then, $a_1, \ldots, a_n$ are nilpotent in $R$. Suppose, moreover, that $P_2 = P + a_{n+1} x^{n+1}$ is a unit in $R$. Then, $\exists P_2^{-1} \in R[x]$ such that $P_2^{-1} P_2 = P_2 P_2^{-1} = 1$. Then $P_2 P_2^{-1} = PP_2^{-1} + a_{n+1} x^{n+1} P_2^{-1}$. Since no term of $PP_2^{-1}$ can be of degree $n + 1 + deg(P_2^{-1})$, and the coefficient of $x^{n+1}$ in $P_2 P_2^{-1}$ must be 0, $a_{n+1}$ must be nilpotent. Furthermore, $a_{n+1} P_2^{-1} = 0$, so $PP_2^{-1} = 1$. Therefore, $P$ is a unit in $R[x]$, and thus, by the inductive hypothesis, $a_1, \ldots, a_n$ are nilpotent.

**Lemma:** Suppose $u$ is a unit in $R$ and $x$ is nilpotent in $R$. Then, $a = u + x$ is a unit. **Proof:** Let $u$ be a unit in $R$ and let $x$ be nilpotent in $R$. Then, $\exists u^{-1} \in R$ such that $uu^{-1} = u^{-1}u = 1$, and $\exists n \in \mathbb{N}$ such that $x^n = 0$. Let $a = u + x$, and let $a^{-1} = c^n \left(\sum_{i=0}^{n-1} (-x)^i u^{n-(i+1)}\right)$. Then, as is shown by induciton on $n$, $a^{-1}a = aa^{-1} = (u + x)c^n \left(\sum_{i=0}^{n-1} (-x)^i u^{n-(i+1)}\right) = 1$. Therefore, $a$ is a unit.

Suppose $a_0$ is a unit in $R$ and $a_1, \ldots, a_n$ are nilpotent in $R$. Then, by the result of part i., $a_1 x + a_2 x^2 + \ldots + a_n x^n$ is nilpotent in $R[x]$, so, by the above lemma, $a_0 + a_1 x + \ldots + a_n x^n$ is a unit.

Thus, $a_0 + a_1 x + \ldots + a_n x^n$ is a unit in $R[x]$ if and only if $a_0$ is a unit in $R$ and $a_1, \ldots, a_n$ are nilpotent in $R$. ■

**Exercise 39: i.** Let $x, y \in \mathbb{Z}$, such that $x^3 = y^2 + 2$. Clearly, $x$ and $y$ have the same parity (in the sense of even and odd), as, otherwise, $x^3$ and $(y^2 + 2) \equiv y^2$ would be different $\pmod 2$. Suppose, for sake of contradiction, that $x$ and $y$ are both even. Then, for some $n, m \in \mathbb{Z}$, $x^3 = 8n^3$ and $y^2 = 4m^2$, so that $x^3 \equiv 0 \pmod 4$, and yet $y^2 + 2 \equiv 2 \pmod 4$. This is impossible if indeed $x^3 = y^2 + 2$, so $x$ and $y$ are both odd. ■

**Exercise 40:** Let $R$ be a unital ring.

**i.** Let $P$ be a prime ideal, and let $A$ be an ideal. Suppose, for $n = 1$, that $A^n \subseteq P$. Then, clearly, $A = A^n \subseteq P$. Suppose, as an inductive hypothesis, that, for some $n \in \mathbb{N}$, in $A^n \subseteq P$, then $A \subseteq P$. Suppose, furthermore, that $A^{n+1} \subseteq P$. Since $P$ is a prime ideal, $A$ is an ideal, and $A^{n+1} = A^n A$, either $A^n \subseteq P$, or $A \subseteq P$. By the inductive hypothesis, in the former case, $A \subseteq P$. In the latter case, trivially, $A \subseteq P$. Thus, by induction on $n$, $\forall n \in \mathbb{N}$ with $n \geq 1$, if $A^n \subseteq P$, then $A \subseteq P$. $\blacksquare$

**Exercise 41: i.** Let $J$ be a prime ideal of a commutative ring $R$.

Suppose $j \in Rad(J)$. Then, $\exists n \in \mathbb{N}$ such that $j^n \in J$. Since $R$ is commutative, $(j) = jR$. Thus, also since $R$ is commutative, $(j)^n \subseteq j^n R$. Therefore, $(j)^n \subseteq J$. Since $(j)$ is an ideal, by the result of Exercise 40 i., then, $(j) \subseteq J$. Therefore, since $j \in (j)$, $j \in J$.

Suppose $j \in J$. Then, for $n = 1$, $n \in \mathbb{N}$ and $j^n = j \in J$, so $j \in Rad(J)$.

Thus, $Rad(J) = J$. $\blacksquare$

**ii.** Suppose $R = \mathbb{Z}$, let $J$ be an ideal of $R$, and let $I = \cap_{A \in S} A$, where $S$ is the set of prime ideals of $R$ which contain $J$. Note that it shown in class that the ideals of $\mathbb{Z}$ are precisely those subsets $I \subseteq \mathbb{Z}$ of the form $m\mathbb{Z}$, where $m \in \mathbb{N}$ (and furthermore, $I$ is a prime ideal if and only if $m$ is prime).

Suppose $j \in Rad(J)$. Then, for some $n \in \mathbb{N}$, $j^n \in J$, so that, for any $A \in S$, $j^n \in A$. Thus, $j \in Rad(A)$, so, since $A$ is a prime ideal, and thus, by the result of part i., $A = Rad(A)$, $j \in A$.

Suppose, on the other hand, that $j \in I$. Let $m \in \mathbb{N}$ such that $J = m\mathbb{Z}$, and let $p_1, p_2, \ldots, p_k$, for some $k \in \mathbb{N}$, be the prime factorization of $m$. Clearly, the prime ideals containing $J$ are $p_1\mathbb{Z}, p_2\mathbb{Z}, \ldots, p_n\mathbb{Z}$. Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be the multiplicities of $p_1, p_2, \ldots, p_k$, respectively, and let $n = \max\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$. Then, $m$ divides $j^n$, so $j^n \in m\mathbb{Z} = J$. Therefore, $j \in Rad(J)$.

Thus, $\cap_{A \in S} A = Rad(J)$. $\blacksquare$

**Exercise 42:** If an element $P = q_0 + q_1 x + \ldots \in \mathbb{Q}[[x]]$ is of the form $\frac{A}{B}$ for some $A, b \in \mathbb{Z}[[x]]$, then it is not the case that, $\forall i \in \mathbb{N}$, $q_i = \frac{1}{i!}$. For, suppose, for sake of contradiction, that it were the case that, $\forall i \in \mathbb{N}$, $q_i = \frac{1}{i!}$, so that $P \in \mathbb{Q}$, and yet $P = \frac{A}{B}$ for $A, B \in \mathbb{Z}$. Then, letting $A = a_0 + a_1 x + \ldots, B = b_0 + b_1 x + \ldots$, $BP = A$; i.e., $\forall k \in \mathbb{N}, a_k = \sum_{i=0}^{k} b_i q_{k-i} = \sum_{i=0|}^{k} \frac{b_k}{(k-i)!}$. However, multiplying by $(k-1)!$ and subtracting all but one term of the summation gives $\frac{b_0}{k} = (k-1)! a_k - \sum_{i=1}^{k} b_i \frac{(k-1)!}{(k-i)!}$. Since, for $i \geq 1$, $(k-i)!$ divides $(k-1)!$ and $b_i \in \mathbb{Z}$, every term of the summation is an integer, so that the right hand side for the equation is an integer, $\forall k \in \mathbb{N}$. However, clearly, since, for $k = b_0 + 1$, $k$ does not divide $b_0$, the left hand side is not always an integer. This is a contradiction, so $P$ is not of the form $\frac{A}{B}$ for $A, B \in \mathbb{Z}[[X]]$.

Since there exists an element $P \in \mathbb{Q}[[x]]$ (so that, consequently, $P$ is in the field of fractions of $\mathbb{Q}[[x]]$), such that $P$ is not in the field of fractions of $\mathbb{Z}[[x]]$, the field of fractions of $\mathbb{Z}[[x]]$ is strictly smaller than the field of fractions of $\mathbb{Q}[[x]]$. $\blacksquare$