Math 516 **Fall 2006** **Radford**

Written Homework # 4 Solution

12/10/06

You may use results form the book in Chapters 1–6 of the text, from notes found on our course web page, and results of the previous homework.

---

1. (**20 total**) Let R be a ring with unity (identity). Show that every element of R is either a unit or a zero divisor if

(a) (**10**) R is finite or

Solution: Let $0 \neq a \in R$. Since R is finite the list $1 = a^0, a, a^2, \ldots$ must contain a repetition. Thus $a^\ell = a^n$ for some $0 \leq \ell < n$. We may assume that n is the smallest such integer. Note that $n - 1 \geq 0$.

Suppose $\ell = 0$. Then $1 = a^0 = a^n = aa^{n-1} = a^{n-1}a$ which means a^{n-1} is an inverse for a.

Suppose $\ell > 0$. Then $0 \leq \ell - 1 < n - 1$ and we deduce $0 = a(a^{n-1} - a^{\ell-1})$ from $a^\ell = a^n$. But $a^{\ell-1} \neq a^{n-1}$ by the minimality of n; thus $a^{n-1} - a^{\ell-1} \neq 0$. We have shown that a is a zero divisor. (Note that $0 = (a^{n-1} - a^{\ell-1})a$ also.)

(b) (**10**) $R = \mathrm{M}_n(k)$, where k is a field.

Solution: Let $0 \neq a \in R$. Since R is finite-dimensional the set of vectors $\{1 = a^0, a, a^2, \ldots\}$ can not be independent. Since $1 \neq 0$ there is a an $n > 0$ such that $\{1, \ldots, a^{n-1}\}$ is independent and $\{1, a, \ldots, a^n\}$ is dependent. In particular

$$\alpha_0 1 + \cdots + \alpha_n a^n = 0,$$

where $\alpha_0, \ldots, \alpha_n \in k$ and $\alpha_n \neq 0$.

Suppose that $\alpha_0 \neq 0$. Since $n-1 \geq 0$ we can write

$$a(-\alpha_0^{-1}(\alpha_1 1 + \cdots + \alpha_n a^{n-1})) = 1 = (-\alpha_0^{-1}(\alpha_1 1 + \cdots + \alpha_n a^{n-1}))a.$$

Thus a has an inverse.

Suppose that $\alpha_0 = 0$. Then $a(\alpha_1 1 + \cdots + \alpha_n a^{n-1}) = 0$. Since $\{1, \ldots, a^{n-1}\}$ is independent and $\alpha_n \neq 0$, $\alpha_1 1 + \cdots + \alpha_n a^{n-1} \neq 0$. We have shown that a is a zero divisor. (Note that $(\alpha_1 1 + \cdots + \alpha_n a^{n-1})a = 0$ also.)

[Hint: Let $a \in R$ and consider the sequence $1, a, a^2, a^3, \ldots$, noting that its terms belong to a finite set or a finite-dimensional vector space.]

2. (**20 total**) Let R be a commutative ring with unity and let N be the set of nilpotent elements of R.

(a) (**8**) Show that N is an ideal of R. [Hint: Let $a, b \in R$. You may assume that the binomial theorem holds for a, b and that $(ab)^n = a^n b^n$ for all $n \geq 0$.]

Solution: $0 \in N$ since $0^1 = 0$. Thus $N \neq \emptyset$. Suppose that $a \in N$ and $r \in R$. Since $a^n = 0$ for some $n > 0$, the calculation $(ra)^n = r^n a^n = r^n 0 = 0$ shows that $ar = ra \in N$. It remains to show that N is an additive subgroup of R.

Suppose $b \in N$ also. Then $b^m = 0$ for some $m > 0$. Now $n+m-1 \geq 1$ since $n, m \geq 1$. By the binomial theorem

$$(a-b)^{n+m-1} = (a+(-b))^{n+m-1} = \sum_{\ell=0}^{n+m-1} C_{n+m-1,\ell}(-1)^\ell a^{n+m-1-\ell} b^\ell,$$

where $C_{n+m-1,\ell}$ is some integer (binomial coefficient).

If $0 \leq \ell < m$ then $n+m-1-\ell > n-1$ which implies $n+m-1-\ell \geq n$. Thus in any event $a^{n+m-1-\ell} = 0$ (when $0 \leq \ell < m$) or $b^\ell = 0$ (when $m \leq \ell \leq n+m-1$.) Therefore $(a-b)^{n+m-1} = 0$. We have shown $a - b \in N$; thus N is an additive subgroup of R.

(b) (**7**) Let $U = \{1 + n \,|\, n \in N\}$. Show that $U \trianglelefteq R^\times$. [Hint: Show that $U = \{1 - n \,|\, n \in N\}$ also. If $n^\ell = 0$ then $1 - n^\ell = 1$.]

Solution: To show $U \trianglelefteq R^\times$ we need only show $U \leq R^\times$ since R is commutative. $1 \in U$ since $1 = 1 + 0$. Suppose that $u, u' \in U$. Then $u = 1{+}n$ and $u' = 1{+}n'$ for some $n, n' \in N$. Thus $uu' = (1{+}n)(1{+}n') = 1 + (n' + n + nn')$. Since N is an ideal (subring) $n' + n + nn' \in N$. Therefore $uu' \in U$.

Now $n^\ell = 0$ for some $\ell > 0$. Since $n^{\ell+1} = 0$ we may assume $\ell \geq 2$. Thus $(-n)^\ell = (-1)^\ell n^\ell = (-1)^\ell 0 = 0$. Since $n = -(-n)$, and R is commutative, the calculation

$$(1 - (-n))(1 + (-n) + (-n)^2 + \cdots + (-n)^{\ell-1}) = 1 - (-n)^\ell = 1$$

shows that $1{+}n$ has an inverse in R which is $1{-}n{+}n^2{-}\cdots{+}(-1)^{\ell-1}n^{\ell-1}$. Now $-n + n^2 - \cdots + (-1)^{\ell-1}n^{\ell-1} \in N$ since N is a subring of R. Therefore $u^{-1} \in U$.

(c) (**5**) Find a ring with unity whose set of nilpotent elements is *not* an ideal. Justify your answer. [Hint: Consider $\mathrm{M}_2(k)$ where k is a field.]

Solution: (**5**) Let $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Then $A, B \in N$ since $A^2 = 0 = B^2$, and $A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Since $(A + B)^2 = I$ the sum $A{+}B$ can not be nilpotent as $(A{+}B)^n = 0$ implies $0 = (A{+}B)^{2n} = ((A + B)^2)^n = I^n = I$, a contradiction. Thus N is not closed under addition, so N is not an ideal.

Another example. same A. Let $C = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$. Then $AC = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ and $(AC)^2 = AC$. Thus $0 \neq AC = (AC)^n$ for all $n > 0$. Therefore $AC \notin N$ which means that N is not an ideal.

Comment: For our examples k could be *any* commutative ring with unity. Why k a field? Two by two matrices over the real numbers is a very familiar object to explore.

3. (**20 total**) Let R be a commutative ring with unity and set $\mathcal{R} = R[[X]]$.

(a) (**5**) Show that $f : \mathcal{R} \longrightarrow R$ defined by $f(\sum_{n=0}^{\infty} a_n X^n) = a_0$ is a ring homomorphism.

Solution: Follows directly from definitions

$$\begin{aligned} f(\sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} b_n X^n) &= f(\sum_{n=0}^{\infty} (a_n + b_n) X^n) \\ &= a_0 + b_0 \\ &= f(\sum_{n=0}^{\infty} a_n X^n) + f(\sum_{n=0}^{\infty} b_n X^n) \end{aligned}$$

and

$$\begin{aligned} f((\sum_{n=0}^{\infty} a_n X^n)(\sum_{n=0}^{\infty} b_n X^n)) &= f(\sum_{n=0}^{\infty} (\sum_{\ell=0}^{n} a_{n-\ell} b_\ell) X^n) \\ &= \sum_{\ell=0}^{0} a_{n-\ell} b_\ell \\ &= a_0 b_0 \\ &= f(\sum_{n=0}^{\infty} a_n X^n) f(\sum_{n=0}^{\infty} b_n X^n). \end{aligned}$$

Observe that $f(1) = 1$.

(b) (**10**) Show that $\sum_{n=0}^{\infty} a_n X^n \in \mathcal{R}^\times$ if and only if $a_0 \in R^\times$.

Solution: Suppose $A = \sum_{n=0}^{\infty} a_n X^n \in \mathcal{R}$ has inverse $B \in \mathcal{R}$. Then by part (a) we have $1 = f(1) = f(AB) = f(A)f(B) = a_0 f(B)$. Since R is commutative a_0 has inverse $f(B) \in R$.

Conversely, suppose that a_0 has an inverse in R. We wish to construct a power series inverse $B = \sum_{n=0}^{\infty} b_n X^n$ for $A = \sum_{n=0}^{\infty} a_n X^n$. Since $\mathcal{R}$ is commutative, B is an inverse for A if and only if

$$\sum_{\ell=0}^{n} a_{n-\ell} b_\ell = \begin{cases} 1 & n = 0 \\ 0 & n > 0 \end{cases} \tag{1}$$

since the identity element of $\mathcal{R}$ is $1 + 0X + 0X^2 + \cdots$. We can find b_0, b_1, ... by induction. Our induction hypothesis is for $m \geq 0$ that (1) is satisfied for $0 \leq n \leq m$.

When $m = 0$ then $n = 0$ and the equation to solve is $a_0 b_0 = 1$. This has a solution $b_0 = a_0^{-1}$ since a_0 has an inverse by assumption.

Suppose that $m \geq 0$ and $b_0, \ldots, b_m$ satisfy (1) for $0 \leq n \leq m$. Then $b_0, \ldots, b_{m+1}$ satisfy (1) for all $0 \leq n \leq m+1$ provided b_{m+1} satisfies

$$\sum_{\ell=0}^{m} a_{m+1-\ell} b_\ell + a_0 b_{m+1} = 0.$$

Setting $b_{m+1} = -a_0^{-1}(\sum_{\ell=0}^{m} a_{m+1-\ell} b_\ell)$ does this.

(c) (**5**) Show that $\mathcal{R}$ is an integral domain if and only if R is an integral domain.

Solution: We may think of R as a subring of $\mathcal{R}$ via the identification $r \mapsto r + 0X + 0X^2 + \cdots$. This map is an injection or rings with unity. Thus if $\mathcal{R}$ is an integral domain the subring R must be also.

Conversely, suppose that R is an integral domain. Since $\mathcal{R}$ is a commutative ring with unity, we need only show that when $f(X) = \sum_{n=0}^{\infty} a_n X^n$ and $g(X) = \sum_{n=0}^{\infty} b_n X^n$ are not zero power series in $\mathcal{R}$ then $f(X)g(X)$ is not 0. Since $f(X), g(X) \neq 0$, each has a first non-zero coefficient a_r, b_s respectively. The coefficient of X^{r+s} in the product $f(X)g(X)$ is

$$\sum_{\ell=0}^{r+s} a_{r+s-\ell} b_\ell = \sum_{\ell=s}^{r+s} a_{r+s-\ell} b_\ell = a_r b_s \neq 0$$

since $s < \ell$ implies $r + s - \ell < r$. Thus $f(X)g(X) \neq 0$.

4. (**20 total**) Let R be ring with unity.

(a) (**10**) Suppose that $\mathcal{I}$ is a non-empty family of ideals of R. Show that $J = \bigcap_{I \in \mathcal{I}} I$ is an ideal of R. (Since R is an ideal of R, it follows that any S subset of R is contained in a smallest ideal of R, namely the intersection of all ideals containing S. This ideal is denoted by (S) and is called the ideal of R generated by S.)

Solution: From group theory we know that J is an additive subgroup of R. Let $a \in J$ and $r \in R$. Since $a \in I$ for all $I \in \mathcal{I}$, and each I is an ideal, $ra, ar \in I$ for all $I \in \mathcal{I}$ and hence $ra, ar \in J$. Therefore J is an ideal of R.

Comment: No unity is required for part (a).

(b) (**10**) Suppose that R is commutative and $S = \{a_1, \ldots, a_r\}$ is a finite subset of R. Show that

$$(S) = Ra_1 + \cdots + Ra_r.$$

Solution: Suppose I is an ideal of R with $S \subseteq I$. Then $ra_i \in I$ for all $r \in R$, and I is closed under sums. Therefore $Ra_1 + \cdots + Ra_r \subseteq I$. This means $Ra_1 + \cdots + Ra_r \subseteq (S)$.

Conversely, $a = 1a$ for all $a \in R$ shows that $S \subseteq Ra_1 + \cdots + Ra_r$. To complete the proof we need only show that $(S) \subseteq Ra_1 + \cdots + Ra_r$; that is $I = Ra_1 + \cdots + Ra_r$ is an ideal of R.

As $0 = 0a_1 + \cdots + 0a_r$ it follows that $I \neq \emptyset$.

Let $s_1a_1 + \cdots + s_ra_r, s'_1a_1 + \cdots + s'_ra_r \in I$. Since R is commutative

$$(s_1a_1 + \cdots s_ra_r) - (s'_1a_1 + \cdots s'_ra_r) = (s_1 - s'_1)a_1 + \cdots + (s_r - s'_r)a_r \in I.$$

Therefore I is an additive subgroup of R. For $s \in R$ the calculation

$$s(s_1a_1 + \cdots s_ra_r) = (ss_1)a_1 + \cdots + (ss_r)a_r \in I$$

shows that I is a left ideal of R. Since R is commutative, I is an ideal of R.

Comment: There is a better way of showing that I is an ideal from general principles. Show that Ra is a left ideal of any ring R for all $a \in R$. Show that the finite sum of left ideals of R is a left ideal of R by induction on the number; thus I is an ideal in our case since R is commutative.

5. (**20 total**) Let R by any ring with unity 1 and $\mathcal{R} = \mathrm{M}_n(R)$. Let J be an ideal of R.

(a) (**15**) Show that $\mathrm{M}_n(J)$ is an ideal of $\mathcal{R}$ and all ideals of $\mathcal{R}$ have this form.

Solution: First note that $E_{i\,j}E_{k\,\ell} = \delta_{j\,k}E_{i\,\ell}$ for all $1 \leq \imath, j, k, \ell \leq n$.

Suppose that J is an ideal of R and set $\mathcal{J} = \mathrm{M}_n(J)$. Then $\mathcal{J} \neq \emptyset$ since $J \neq \emptyset$. For $A = (A_{i\,j}), B = (B_{i\,j}) \in \mathcal{J}$ and $C = (C_{i\,j}) \in \mathcal{R}$ we have

$$(A-B)_{i\,j} = A_{i\,j} - B_{i\,j}, (CA)_{i\,j} = \sum_{\ell=1}^{n} C_{i\,\ell}A_{\ell\,j}, (AC)_{i\,j} = \sum_{\ell=1}^{n} A_{i\,\ell}C_{\ell\,j} \in J$$

for all $1 \leq i, j \leq n$ since J is an ideal of R. Thus $\mathcal{J}$ is an ideal of $\mathcal{R}$.

Conversely, suppose that $\mathcal{J}$ is an ideal of $\mathcal{R}$. Let $A = \sum_{u,v=1}^{n} A_{u\,v}E_{u\,v} \in \mathcal{J}$, where $A_{u\,v} \in R$. Since the elements of each $E_{i\,j}$ are in the center of R, for all $1 \leq j, k \leq n$ and $1 \leq i, \ell \leq n$, the calculation

$$E_{i\,j}AE_{k\,\ell} = \sum_{u,v=1}^{n} A_{u\,v}E_{i\,j}E_{u\,v}E_{k\,\ell} = \sum_{u=1}^{n} A_{u\,k}E_{i\,j}E_{u\,\ell}$$

shows that $A_{j\,k}E_{i\,\ell} \in \mathcal{J}$. Let J be the set of all elements of R which appear as an entry in some element of $\mathcal{R}$. We have shown that $E_{i\,j}\mathcal{J}E_{k\,\ell} = JE_{i\,\ell}$. Therefore, by adding, $\mathcal{J} = \mathrm{M}_n(J)$. It remains to show that J is an ideal of R.

Since $\mathcal{J} \neq \emptyset$ necessarily $J \neq \emptyset$. Suppose that $a, b \in J$ and $c \in R$. Then $aE_{1\,1}, bE_{1\,1} \in \mathcal{J}$ and the calculations

$$(a-b)E_{1\,1} = aE_{1\,1} - bE_{1\,1}, caE_{1\,1} = (cE_{1\,1})(aE_{1\,1}), acE_{1\,1} = (aE_{1\,1})(cE_{1\,1}) \in \mathcal{J}$$

show that $a - b, ca, ac \in J$. Therefore J is an ideal of R.

(b) (**5**) Show that $\mathcal{R}$ is simple if and only if R is simple.

Solution: By part (a) there is a bijective correspondence between the ideals of R and $\mathcal{R} = \mathrm{M}_n(R)$. Thus R has 2 ideals if and only if $\mathcal{R}$ has 2 ideals.

[Hint: For part (a) let $E_{i\,j} \in \mathrm{M}_n(R)$ be defined by $(E_{i\,j})_{k\,\ell} = \delta_{i,k}\delta_{j,\ell}$, where $\delta_{u,v} = \begin{cases} 1 & : \quad u = v \\ 0 & : \quad u \neq v \end{cases}$. Work out the formula for $E_{i\,j}E_{k\,\ell}$. Show that any $A = (A_{u\,v}) \in \mathrm{M}_n(R)$ can be written $A = \sum_{u,v=1}^{n} A_{u\,v}E_{u\,v}$ and consider $E_{i\,j}AE_{k\,\ell}$.]

Comment: Note that "ideal" in the preceding exercise can not be replaced by "left ideal". Take $R = k$ to be a field and $n \geq 2$. Then R has 2 left ideals. For fixed $1 \leq j \leq n$ all matrices with entries zero outside the j^{th} column form a left ideal of $\mathcal{R}$.