MATH 570: Higher Algebra I, Winter 2005

Solutions to Assignment 1

Section 1, #3: Take any $a, b \in R$. Since $c^2 = c$ for any $c \in R$, it follows that

$$(a+b)^2 = a+b, \ (a-b)^2 = a-b.$$

Hence,

$$(a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b = a + b,$$
$$\Downarrow$$
$$ab + ba = 0$$

and

$$(a-b)^2 = a^2 - ab - ba + b^2 = a - ab - ba + b = a - b,$$
$$\Downarrow$$
$$-ab - ba + b + b = 0.$$

Combining the above equalities we get $b + b = 0$ for any $b \in R$. Finally, since $b = -b$ then $ba = -ba$ and

$$ab + ba = 0 \Rightarrow ab - ba = 0 \Rightarrow ab = ba$$

for any $a, b \in R$.

Section 1, #7: a) Suppose there exist $a, c \in R$ such that $a, c \neq 0$ but either $ac = 0$ or $ca = 0$. Suppose, b is a unique element of R such that $aba = a$. Consider $a(b+c)a$. We have

$$a(b+c)a = aba + aca = a + 0 = a$$

and since b is unique for a with this property, it follows that $b + c = b$ and $c = 0$ - contradiction with our assumption.

b) If b is a unique element of R such that $aba = a$ then

$$aba = a \Rightarrow (ab)(aba) = (ab)a = a \Rightarrow a(bab)a = a \Rightarrow bab = b.$$

c,d) Take $a, b \in R$ such that $aba = a$ and consider ab. Observe that $b, ab, ba \neq 0$ since $a \neq 0$. For any $c \in R$ we check if $(ab)c = c = c(ab)$. Consider $b((ab)c - c)$. Hence,

$$b((ab)c - c) = (bab)c - bc = bc - bc = 0$$

and by **a)** we have $(ab)c - c = 0$, so $(ab)c = c$. The equality $c = c(ab)$ can be checked in the same way considering $(c(ab) - c)a$.

Also, if $0 \neq c, d \in R$ is another pair of elements such that $cdc = c$ then it is easy to see that $ab = cd$. Indeed,

$$(cd - ab)a = (cd)a - (ab)a = a - a = 0,$$

so by **a)** $cd - ab = 0$. In particular, $ab = ba$ for any $0 \neq a \in R$ and corresponding b.

Thus, for any $0 \neq a, b \in R$ such that $aba = a$ we denote $ab = 1_R$. Observe that $1_R \neq 0$ and 1_R has all the properties of the identity of R. Finally, since R has no zero divisors and for every $a \in R$ there exists a unique b such that $ab = ba = 1_R$ then R is a division ring.

Section 1, #10e): Just computations.

Section 1, #11: Let $a, b \in R$ and $n \geq 0$. By Theorem 1.6 (p.118)

$$(a \pm b)^{p^n} = \sum_{k=0}^{p^n} \frac{(p^n)!}{(p^n - k)!\ k!}\ (\pm b)^k\ a^{p^n - k}.$$

On the other hand, from **Exercise #10e**, it follows that p divides $\frac{(p^n)!}{(p^n-k)!\ k!}$ for any $1 \leq k \leq p^n - 1$ and since R is of characteristic p then

$$\frac{(p^n)!}{(p^n - k)!\ k!}\ (\pm b)^k\ a^{p^n - k} = 0$$

for any $1 \leq k \leq p^n - 1$. Thus,

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$$

Section 1, #18): At first we show that $f(\frac{1}{n}) = g(\frac{1}{n})$ for any $n \in \mathbb{Z}$. Indeed,

$$g(1) = f(1) = f(n) f\left(\frac{1}{n}\right) = g(n) f\left(\frac{1}{n}\right).$$

and we multiply both sides by $g(\frac{1}{n})$. Hence, we have

$$g\left(\frac{1}{n}\right)\left(g(n) f\left(\frac{1}{n}\right)\right) = g\left(\frac{1}{n}\right) g(1)$$

and

$$g(1) f\left(\frac{1}{n}\right)) = g\left(\frac{1}{n}\right)$$

so,

$$f\left(\frac{1}{n}\right) = f(1) f\left(\frac{1}{n}\right) = g(1) f\left(\frac{1}{n}\right) = g\left(\frac{1}{n}\right).$$

Now,

$$f\left(\frac{m}{n}\right) = m f\left(\frac{1}{n}\right) = m g\left(\frac{1}{n}\right) = g\left(\frac{m}{n}\right)$$

for any $\frac{m}{n} \in \mathbb{Q}$.

Section 2, #5: Let $r_1, r_2 \in [R : I]$ and $x \in R$. Hence,

$$x(r_1 + r_2) = xr_1 + xr_2 \in I,\ x(r_1 r_2) = (xr_1)r_2 \in I$$

since $xr_1, xr_2 \in I$ and I is an ideal. Thus, $[R : I]$ is closed under addition and multiplication, and obviously $I \subseteq [R : I]$ because I is an ideal. Finally, if $y \in R,\ r \in [R : I]$ then $yr \in I \subseteq [R : I]$ and $ry \in [R : I]$ because for any $x \in R$ we have $x(ry) = (xr)y = r'y$, where $r' \in I$, so, $r'y \in I$. Hence, $[R : I]$ is an ideal.

Section 2, #8): "⇒" Let J be an ideal in $M_n(R)$. Let I be the set composed by $(1,1)$-entries of all matrices from J. If $A = (a_{i,j}) \in J$ and $s_{i,j}(1_R)$ is the matrix all entries of which are zeros except (i,j)-entry containing 1_R then

$$s_{i,j}(1_R)\ A = i \begin{pmatrix} 0 & & \overset{j}{\cdots} & & 0 \\ \cdots & & \cdots & & \cdots \\ 0 & \cdots & 1_R & \cdots & 0 \\ \cdots & & \cdots & & \cdots \\ 0 & & \cdots & & 0 \end{pmatrix} A = i \begin{pmatrix} 0 & \cdots & 0 \\ & \cdots & \\ a_{j,1} & \cdots & a_{j,n} \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix}$$

and

$$(s_{i,j}(1_R)\ A)\ s_{k,m}(1_R) = i \begin{pmatrix} 0 & \cdots & 0 \\ & \cdots & \\ a_{j,1} & \cdots & a_{j,n} \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 0 & & \overset{m}{\cdots} & & 0 \\ \cdots & & \cdots & & \cdots \\ 0 & \cdots & 1_R & \cdots & 0 \\ \cdots & & \cdots & & \cdots \\ 0 & & \cdots & & 0 \end{pmatrix} k =$$

$$= i \begin{pmatrix} 0 & & \overset{m}{\cdots} & & 0 \\ \cdots & & \cdots & & \cdots \\ 0 & \cdots & a_{j,k} & \cdots & 0 \\ \cdots & & \cdots & & \cdots \\ 0 & & \cdots & & 0 \end{pmatrix} \in J,$$

where the only non-zero entry of $(s_{i,j}(1_R)\ A)\ s_{k,m}(1_R)$ is the (i,m)-entry containing $a_{j,k}$. That is, $(s_{i,j}(1_R)\ A)\ s_{k,m}(1_R) = s_{i,m}(a_{j,k})$ Eventually, since interchanging of rows and columns corresponds to multiplication from left and right by elementary matrices it follows that if a is any entry of a matrix from J then $s_{1,1}(a) \in J$ and hence $a \in I$. The converse is obviously true since any $B = (b_{i,j}) \in M_n(I)$ can decomposed as a sum of $s_{i,j}(b_{i,j}) \in J$, so, $B \in J$.

Finally, let $a, b \in I,\ r \in R$. Then

$$\begin{pmatrix} a & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix}, \begin{pmatrix} b & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} \in J,\ \begin{pmatrix} r & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} \in M_n(R),$$

hence,

$$\begin{pmatrix} a & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} + \begin{pmatrix} b & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} a+b & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} \in J \Rightarrow a+b \in I,$$

$$\begin{pmatrix} a & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} \cdot \begin{pmatrix} b & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} ab & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} \in J \Rightarrow ab \in I,$$

$$\begin{pmatrix} r & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} \cdot \begin{pmatrix} a & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} ra & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} \in J \Rightarrow ra \in I,$$

$$\begin{pmatrix} a & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} \cdot \begin{pmatrix} r & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} ar & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & 0 \end{pmatrix} \in J \Rightarrow ar \in I.$$

Thus, I is an ideal of R.

"$\Leftarrow$" If $J = M_n(I)$, where I is an ideal of R then it is easy to see that J is closed under addition and multiplication by elements from $M_n(R)$.

Section 2, #16: Observe that if

$$A \cap P_j \subseteq \bigcup_{i \neq j} P_i$$

for some $j \in [1, n]$, then

$$A \subseteq \bigcup_{i \neq j} P_i.$$

That is, without loss of generality one can assume that there are no "redundant" ideals in the list $P_1, \ldots, P_n$, in other words, $A \cap P_j \not\subseteq \bigcup_{i \neq j} P_i$ for every $j \in [1, n]$ which is possible only when $n > 1$. After this assumption is made, follow the hint given in the textbook and get a contradiction with $n > 1$.

Section 2, #23: Observe that

$$(1_R - e)^2 = 1_R - e - e + e^2 = 1_R - e - e + e = 1_R - e$$

and

$$r(1_R - e) = r1_R - re = 1_R r - er = (1_R - e)r$$

for any $r \in R$, so **(a)** follows.

(b) If e is a central idempotent then

$$er_1 + er_2 = e(r_1 + r_2) \in eR,$$

$$(er_1)(er_2) = e^2(r_1 r_2) = e(r_1 r_2) \in eR,$$

$$r(er_1) = e(rr_1) \in eR,\ (er_1)r = e(r_1r) \in eR$$

for any $r, r_1, r_2 \in R$, and it follows that eR is an ideal of R. From **(a)** it follows that $1_R - e$ is also a central idempotent, hence, $(1_R - e)R$ is an ideal of R. Now, observe that for any $r \in R$ we have a decomposition

$$r = er + (1_R - e)r \in eR + (1_R - e)R.$$

On the other hand, if $a \in eR \cap (1_R - e)R$ then there exist $r_1, r_2 \in R$ such that $er_1 = (1_R - e)r_2$. Thus, $er_1 = r_2 - er_2$ and $r_2 = e(r_1 + r_2) = er \in eR$. Finally, $a = (1_R - e)r_2 = (1_R - e)(er) = er - e^2r = er - er = 0$ and it follows that $eR \cap (1_R - e)R = 0$. So, $R = eR \times (1_R - e)R$.

Section 2, #24): We take advantage of the hint given in the textbook.

"**(a) $\Rightarrow$ (b)**" If $e_i = (0, \ldots, 0, 1_{R_i}, 0, \ldots, 0) \in R$ for $i \in [1, n]$ then obviously $e_i^2 = e_i$ and $e_ir = re_i$ for any $r \in R$, so every e_i is a central idempotent of R. Also, it is easy to see that $e_ie_j = 0$ when $i \neq j$ and $e_1 + \cdots + e_n = (1_{R_1}, 1_{R_2}, \ldots, 1_{R_n}) = 1_R$.

"**(b) $\Rightarrow$ (c)**" Define $A_i = e_iR$ for every $i \in [1, n]$. Since e_i is a central idempotent then like in **#23** it can be shown that A_i is an ideal of R.

Since $e_1 + \cdots + e_n = 1_R$, then for every $r \in R$ we have $r = e_1r + \cdots + e_nr \in A_1 + \cdots A_n$ and if $a \in A_i \cap A_j,\ i \neq j$ then $e_ir_1 = e_jr_2$ and $e_i(e_ir_1) = e_i(e_jr_2)$, from which it follows that $e_ir_1 = 0$. Thus, $A_i \cap A_j = 0,\ i \neq j$ and $R = A_1 \times \cdots \times A_n$.

"**(c) $\Rightarrow$ (a)**" Since $A_i \simeq R_i$ then obviously $R = A_1 \times \cdots \times A_n$ implies $R \simeq R_1 \times \cdots \times R_n$.