Homework 10

Anthony Jones

1a) Let $x, y \in R$ be nilpotent elements.

Then $x^n = y^m = 0$ for $n, m \in \mathbb{N}$.

Consider $x+y \in R$:

$$(x+y)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^{m+n-k} y^k,$$

According to the binomial theorem, as R is communiative, when $k < m$ then $m+n-k \geq n$ and thus the x element drifts to 0 as $x^n = 0$; similarly, when $k \geq m$ then the y element drifts to 0 as $y^m = 0$. Thus

$$(x+y)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} 0 = 0$$

as $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$.

Consider $xy \in R$:

Because R is commmunative, $xy = yx$, and therefore

$$(xy)^{mn} = x^{mn} y^{mn} = (x^n)^m (y^m)^n = 0.$$

Thus both $x+y$ and xy are nilpotent.

1b) Let $u \in U(R)$ be a unit and $x \in R$ be a nilpotent element.

Then $\exists v \in R$ such that $u \cdot v = v \cdot u = 1_R$ and $\exists n \in \mathbb{N}$ such that $x^n = 0$.

Consider $1 + v \cdot x \in R$:

$$(1 + vx)\left(1 + \sum_{k=1}^{k=n-1} (-vx)^k\right)$$

$$= (1+vx)\left(1 - (vx) + (vx)^2 - (vx)^3 + \cdots + (vx)^{n-1}\right)$$

$$= \left(1 + (vx - vx) + ((vx)^2 - (vx)^2) + \cdots + (vx)^n\right)$$

$$= 1 + (vx)^n = 1 + v^n x^n = 1,$$

Because R is commutative and therefore $(vx)^n$ is nilpotent as $(vx)^n = v^n x^n$.

Thus by definition u is invertible and $1 + v \cdot x$ is invertible as well, so

$$u(1 + v \cdot x) = u + u \cdot v \cdot x = u + x$$

is also invertible; meaning for some $w \in R$, $(u+x) \cdot w = w \cdot (u+x) = 1$ and hence $u+x$ is a unit, ~~as R is commutative and therefore w commutes~~ where $w = v(1 + vx)^{-1}$.

1c) When R is noncommunicative, $x+y$ is not necessarily nilpotent because $(x+y)(x+y) = x^2 + yx + xy + y^2$ cannot be reduced into a sum of $x^i y^j$ terms, as $xy \neq yx$; thus alternating expansions of x and y such as $x \cdot y \cdot x \cdot y \cdot x \cdot y \ldots$ may cycle without necessarily collapsing to 0.

Similarly, $x \cdot y$ is not necessarily nilpotent for the same reason, as $xy \neq yx$ and therefore expansions of x and y may cycle without collapsing to 0.

$$(x \cdot y)^n = \overbrace{x \cdot y \cdot x \cdot y \cdot x \cdot y \ldots x \cdot y}^{n \text{ times}}$$

Finally, $u + x$ is not necessarily a unit because the inverse of u, which is v, may not necessarily commute with the inverse of $1 + v \cdot x$, which is necessary for $(u+x) \cdot w = w \cdot (u+x)$:

$$(u+x)\left(v(1+vx)^{-1}\right) \neq v(1+vx)^{-1}(u+x).$$

2a) Let R have the identity 1_R.

Suppose $\text{char}(R) = n \in \mathbb{N}$ for which $nr = 0$ for all $r \in R$. Let $s, t \in R$ be nonzero elements. Then

$$n \cdot s = n \cdot t = 0,$$

And by the definition of identity,

$$n \cdot (1_R \cdot s) = n \cdot (1_R \cdot t) = 0.$$

Since rings are associative by multiplication,

$$(n \cdot 1_R) \cdot s = (n \cdot 1_R) \cdot t = 0,$$

which as s and t are not 0, means $n \cdot 1_R = 0$, and likewise is minimal as $x \cdot 1_R \cdot r \neq 0$ for $x < n \in \mathbb{N}$.

Suppose $\text{char}(R) = n \in \mathbb{N}$ for which $n 1_R = 0$. Let $r \in R$ be a nonzero element:

$$nr = n(1_R \cdot r) = (n 1_R) r = 0 \cdot r = 0,$$

and this is similarly minimal as if $xr = 0$ for some $x < n \in \mathbb{N}$, then like above, $(x \cdot 1_R) r = 0$ and since r is not zero, $x \cdot 1_R$ would have to be so.

2b) Let $char(R) = p$ for some $p \in \mathbb{N}$.

If there is no n for which $nr = 0$ for all $r \in R$, then $p = 0$.

Else $pr = 0$ for all $r \in R$ and $p > 0$.

Let $r, s \in R$.

Assume p is not prime. Then $p = a \cdot b$ for $a \neq 1$ and $b \neq 1$ and $a, b \in \mathbb{N}$ (positive divisors), $p > a$ and $p > b$.

Then for $rs \in R$, $prs = abrs = arbs = 0$, and as R is an integral domain then $(ar)(bs) = 0 \implies ar = 0$ or $bs = 0$.

But recall that by definition p is the minimal value for which $nr = 0$, and when p is not prime then either $a < p$ or $b < p$ satisfies the same characteristic property. Thus this is a contradiction and p must be prime.

Therefore $char(R)$ is either 0 or a positive prime.

3) Let T be the subset of $M_2(\mathbb{R})$ consisting of all matrices

$$\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} \text{ for } a,b \in \mathbb{R}.$$

Observe that for $u, v \in T$,

$$u \cdot v = \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} \begin{bmatrix} 0 & c \\ 0 & d \end{bmatrix} = \begin{bmatrix} 0 & ad \\ 0 & bd \end{bmatrix} \in T$$

and

$$u + v = \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} + \begin{bmatrix} 0 & c \\ 0 & d \end{bmatrix} = \begin{bmatrix} 0 & a+c \\ 0 & b+d \end{bmatrix} \in T,$$

So T is closed under the operations of $M_2(\mathbb{R})$ and is therefore a subring.

Finally consider $1_R = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$:

$$\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$$

and therefore there exists a right identity. Note, however, that a left identity cannot exist as the product of $u \cdot v$ gives an element comprised in terms a, b, d, and ~~therefore~~ therefore the top term on any right multiplicant cannot be fixed as $c = ad$ is always dependent on d.

4) Suppose $n=1$. This creates our base case, as R is communicative and therefore

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k,$$

which besides the first and last terms will have coeffecients divisible by p as

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$$

However, since $\text{char}(R) = p$, each coeffecient term with p or divisible by p must be 0, so

$$\begin{aligned}(a+b)^p &= a^p + pa^{p-1}b + \dots + pab^{p-1} + b^p \\ &= a^p + 0 + 0 + \dots + 0 + 0 + b^p \\ &= a^p + b^p.\end{aligned}$$

Now consider $n+1$:

$$(a+b)^{p^{n+1}} = (a+b)^{p^n p} = \left((a+b)^{p^n}\right)^p = \left(a^{p^n} + b^{p^n}\right)^p$$

Similarly does this give $\sum_{k=0}^{p} \binom{p}{k} (a^{p^n})^{p-k} (b^{p^n})^k$

and hence $(a+b)^{p^{n+1}} = (a^{p^n})^p + (b^{p^n})^p$

$$= a^{p^{n+1}} + b^{p^{n+1}}.$$

5) Let $r \in R$.

We can show that any element of R has the characteristic property 2:

$$2r = 4r - 2r$$
$$= 4r^2 - 2r$$
$$= (2r)^2 - 2r$$
$$= 2r - 2r = 0$$

Furthermore this is minimal because a ring characteristic 1 is by definition just the trivial ring $\{0\}$.

Now let $x, y \in R$:

$$x+y = (x+y)^2 = x^2 + y^2 + xy + yx$$
$$\longrightarrow \quad x+y = x+y+xy+yx.$$

Hence $xy = -yx = (-yx)^2 = (yx)^2 = yx$, and R is therefore commutative.