DT8248 Stage 4 Ring Theory Assignment 1

Name: Jason Borland

Student Number: D17129310

Date: 04 March 2021

Question 1: A ring R is called simple if its only two-sided ideals are the full ring and the zero ideal. Prove that the matrix ring $M_2(F)$ is simple if F is a field?

Let:

$$M_2(F) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in F \right\}$$

The Zero matrix, **0** in $M_2(F)$ is:

$$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Where $0 \in F$ is the additive identity. Also note that since F is a field, it contains the multiplicative identity 1, so $M_2(F)$ contains the identity matrix.

First note $M_2(F) \neq \{\mathbf{0}\}$. Now suppose that **J** is an ideal of $M_2(F)$ and that $J \neq \{\mathbf{0}\}$. We want to prove $J = M_2(F)$. This is equivalent to proving that **J** contains the identity matrix. Since $J \neq \{\mathbf{0}\}$, there exists a matrix $A \in J$ which is not zero in every entry, such that $\{A\} \subseteq J$. We will try to build the identity matrix starting from A using operations under which ideals are stable, that is, internal sum and multiplication with elements of $M_2(F)$.

Consider the matrix $A \in J$.

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

Where $a_{ij} \in F$ and at least one of the $a_{ij} \neq 0$. We shall arbitarily select $a_{12} \neq 0$.

Now consider the following elementary matrices in $M_2(F)$:

$$E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, E_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, E_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, E_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Now since **J** is a two-sided Ideal we can multiply, $A \in J$ on either side by elements of $M_2(F)$ and remain in **J**.

$$E_{11}AE_{21} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} a_{12} & 0 \\ 0 & 0 \end{bmatrix} = E_{11} \in J$$

Another matrix operation is multiplication by a scalar. Since F is a field and $a_{12} \in F$ we know $a_{12}^{-1} \in F$. Therefore:

$$a_{12}^{-1}E_{11}AE_{21} = a_{12}^{-1}\begin{bmatrix} a_{12} & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in J$$

Similarly:

$$E_{21}AE_{22} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & a_{12} \end{bmatrix} \in J$$

$$a_{12}^{-1}E_{21}AE_{22} = a_{12}^{-1}\begin{bmatrix} 0 & 0 \\ 0 & a_{12} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = E_{22} \in J$$

Continuing our construction. Since **J** is an Ideal the addition of two elements of **J** remains in **J**:

$$E_{11} + E_{22} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2 \in J$$

We have shown that the identity is in **J**. Since $I \in J$, then the ideal **J** contains the whole matrix ring $M_2(F)$. As such we have proven that $M_2(F)$ is simple.

Note this construction used a_{12}, any a_{ij} could of been chosen and $E_{11} = -a_{ij}E_{1i}AE_{1j}$ and $E_{22} = -a_{ij}E_{2i}AE_{2j}$ (I think).

Question 2(a):

Suppose that R is a ring with multiplicative identity, 1, and $\phi : R \to S$ is a homomorphism onto S, then prove that $\phi(1)$ is the multiplicative identity of S.

Let $1_R \in R$ be the identity in R. Let $1_S \in S$ be the identity in S. Since ϕ is a homomorphism, say $s = \phi(1_R) \in S$.

Let $r \in R$ be: $\phi(r) = 1_S$. We know that r exists as ϕ is onto.

Consider:

$$1_S = \phi(r) = \phi(r.1_R) = \phi(r)\phi(1_R) = \phi(r).s = 1_S.s = s = \phi(1_R)$$

We have proven $1_S = \phi(1_R)$.

Question 2(b):

Given $\phi : R \to S$ is a homomorphism onto S. Prove that the kernel of ϕ is an ideal of R, where the kernel of ϕ is the set $ker(\phi) = \{r \in R : \phi(r) = 0\}$.

The Ideal Test Therorem: A non-empty subset A of ring R is an ideal of R if:

1. $a - b \in A$ whenever $a, b \in A$.
2. $ra \in A, ar \in A$ whenever $a \in A$ and $r \in R$.

First we need to show $ker(\phi)$ is non-empty. As ϕ is a ring homomorphism:

$$\begin{aligned} \phi(0+0) &= \phi(0) + \phi(0) \\ \therefore \phi(0) &= \phi(0) + \phi(0) \\ \therefore \phi(0) &= 0 \end{aligned}$$

So $0 \in Ker(\phi) \neq \emptyset$.

Consider elements $a, b \in Ker(\phi)$ and $r \in R$. We will next show ker(ϕ) is an ideal of R:

Is $a - b \in \ker(\phi)$?

$$\begin{aligned} \phi(a-b) &= \phi(a) + \phi(-b) \\ &= \phi(a) - \phi(b) \\ &= 0 - 0 \\ &= 0 \\ \therefore a - b &\in Ker(\phi) \end{aligned}$$

Is $ra \in \ker(\phi)$?

$$\begin{aligned} \phi(ra) &= \phi(r)\phi(a) \\ &= \phi(r).0 \\ &= 0 \\ \therefore ra &\in Ker(\phi) \end{aligned}$$

Is $ar \in \ker(\phi)$?

$$\begin{aligned} \phi(ar) &= \phi(a)\phi(r) \\ &= 0.\phi(r) \\ &= 0 \\ \therefore ar &\in Ker(\phi) \end{aligned}$$

So $\ker(\phi)$ is an ideal of R.

Question 2(c):

Show that $A = \{(3x, 5y) : x, y \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z} \oplus \mathbb{Z}$. Prove A is not a prime ideal.

First show that A is non-empty. Since $0 \in \mathbb{Z}$, then $(3.0, 5.0) = (0, 0) \in A$. So A is non-empty.

Consider $a = (3x_1, 5y_1), b = (3x_2, 5y_2) \in A$ and $r = (x_3, y_3) \in \mathbb{Z} \oplus \mathbb{Z}$.

Is $a - b \in A$?

$$\begin{aligned} a - b &= (3x_1, 5y_1) - (3x_2, 5y_2) \\ &= (3x_1 - 3x_2, 5y_1 - 5y_2) \\ &= (3(x_1 - x_2), 5(y_1 - y_2)) \in A \\ Since\ x_1 &- x_2, y_1 - y_2 \in \mathbb{Z} \end{aligned}$$

Is $ra \in A$ (Note operations on elements of $\mathbb{Z}$ are commutative) ?

$$\begin{aligned} ra &= (x_3, y_3).(3x_1, 5y_1) \\ &= (x_3(3x_1), y_3(5y_1)) \\ &= (3x_1x_3, 5y_1y_3) \in A \\ Since\ x_1x_3&, y_1y_3 \in \mathbb{Z} \end{aligned}$$

Is $ar \in A$?

$$\begin{aligned} ar &= (3x_1, 5y_1)(x_3, y_3) \\ &= (3x_1x_3, 5y_1y_3) \in A \\ Since\ x_1x_3&, y_1y_3 \in \mathbb{Z} \end{aligned}$$

So A is an Ideal of $\mathbb{Z} \oplus \mathbb{Z}$. Is A a prime Ideal?

Prime Ideal Definition: A prime ideal P of a commutative ring R is a proper ideal of R such that: $a, b \in R$ and $ab \in P$ imply $a \in P$ or $b \in P$.

The contrapositive is $a \notin P$ and $b \notin P$ implies $ab \notin P$.

So consider $(3, 1) \notin A$ and $(1, 5) \notin A$. Note that $(3, 1).(1, 5) = (3, 5) \in A$. So $a \notin A$ and $b \notin A$ but $ab \in A$. So A is not a prime ideal.

Question 2(d):

Show that $B = \{(3x, y) : x, y \in \mathbb{Z}\}$ is a maximal ideal of $\mathbb{Z} \oplus \mathbb{Z}$.

First we need to show that B is an ideal of $\mathbb{Z} \oplus \mathbb{Z}$.

Show that B is non-empty. Since $0 \in \mathbb{Z}$, then $(3.0, 0) = (0, 0) \in B$. So B is non-empty.

Consider $a = (3x_1, y_1), b = (3x_2, y_2) \in B$ and $r = (x_3, y_3) \in \mathbb{Z} \oplus \mathbb{Z}$.

Is $a - b \in B$?

$$\begin{aligned} a - b &= (3x_1, y_1) + (3x_2, y_2) \\ &= (3x_1 - 3x_2, y_1 - y_2) \\ &= (3(x_1 - x_2), (y_1 - y_2)) \in B \\ Since\ x_1 &- x_2, y_1 - y_2 \in \mathbb{Z} \end{aligned}$$

Is $ra \in B$ (Note operations on elements of $\mathbb{Z}$ are commutative) ?

$$\begin{aligned} ra &= (x_3, y_3).(3x_1, y_1) \\ &= (x_3(3x_1), y_3y_1) \\ &= (3x_1x_3, y_1y_3) \in B \\ Since\ x_1x_3&, y_1y_3 \in \mathbb{Z} \end{aligned}$$

Is $ar \in B$?

$$\begin{aligned} ar &= (3x_1, y_1)(x_3, y_3) \\ &= (3x_1x_3, y_1y_3) \in B \\ Since\ x_1x_3&, y_1y_3 \in \mathbb{Z} \end{aligned}$$

So B is an Ideal of $\mathbb{Z} \oplus \mathbb{Z}$.

Now we need to show B is a maximal Ideal of B.

We will use the theorem: Let R be a commutative ring with identity and let A be an ideal of R. Then R/A is a field iff A is a maximal ideal.

$$\begin{aligned} \frac{\mathbb{Z} \oplus \mathbb{Z}}{B} &= \{(0, y) + (3x, y), (1, y) + (3x, y), (2, y) + (3x, y)\} \\ &= \{[0]_3, [1]_3, [2]_3\} \\ &= \mathbb{Z}_3 \end{aligned}$$

Now if we consider a homomorphism from $\mathbb{Z} \oplus \mathbb{Z}$ to $\mathbb{Z}_3$. $\phi : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}_3$. Where $\phi((x, y)) = [x]_3$.

Is ϕ a homomorphism? Consider $(x_1, y_1), (x_2, y_2) \in \mathbb{Z} \oplus \mathbb{Z}$.

$$\begin{aligned} \phi(x_1, y_1) + \phi(x_2, y_2) &= [x_1]_3 + [x_2]_3 \\ &= [x_1 + x_2]_3 \\ &= \phi((x_1 + x_2, y_1 + y_2)) \\ &= \phi((x_1, y_1) + (x_2, y_2)) \end{aligned}$$

Also

$$\begin{aligned} \phi(x_1, y_1).\phi(x_2, y_2) &= [x_1]_3.[x_2]_3 \\ &= [x_1.x_2]_3 \\ &= \phi((x_1.x_2, y_1.y_2)) \\ &= \phi((x_1, y_1).(x_2, y_2)) \end{aligned}$$

So ϕ is a homomorphism. Now we need to find the kernel of the homomorphism.

$$\begin{aligned} Ker(\phi) &= \{(x, y) : [x]_3 = [0]_3\} \\ &= \{(x, y) : 3|x, x \in \mathbb{Z}\} \\ Ker(\phi) &= \{(3x, y) : x, y \in \mathbb{Z}\} = B \end{aligned}$$

The Ring Homomorphism Theorem states :

$$\frac{\mathbb{Z} \oplus \mathbb{Z}}{Ker(\phi)} \cong \mathbb{Z}_3$$

Since $\mathbb{Z}_3$ is a finite field, so is $\frac{\mathbb{Z} \oplus \mathbb{Z}}{Ker(\phi)}$. Thus $B = Ker(\phi)$ is a maximal ideal.

Question 3(a):

For ring R, define $\langle a, b \rangle$ to be the smallest ideal containing both a and b. Prove that if R is a commutative ring with identity then $\langle a, b \rangle = \{ra + sb : r, s \in R\}$.

First lets prove <a,b> is an ideal. Is $\langle a, b \rangle = \{ra + sb : r, s \in R\} \neq \emptyset$?

Consider $a, b \in \langle a, b \rangle, and r = 1 = s :$

$\therefore a + b \in \langle a, b \rangle$. So $\langle a, b \rangle \neq \emptyset$.

Consider elements $x = (r_1a + s_1b), y = (r_2a + s_2b) \in \langle a, b \rangle and\ r \in R$.

Is $x - y \in \langle a, b \rangle$?

$$\begin{aligned} x - y &= (r_1a + s_1b) - (r_2a + s_2b) \\ &= (r_1a - r_2a) + (s_1b - s_2b) \\ &= (r_1 - r_2)a + (s_1 - s_2)b \in \langle a, b \rangle \\ Since\ (r_1 - r_2)&, (s_1 - s_2) \in R \end{aligned}$$

Is $rx \in \langle a, b \rangle$?

$$\begin{aligned} rx &= r(r_1a + s_1b) \\ &= rr_1a + rs_1b \in \langle a, b \rangle \\ Since\ rr_1&, rs_1 \in R \end{aligned}$$

Is $xr \in \langle a, b \rangle$? (Note R is communative Ring so this is strictly not necessary as in a communatative if the left ideal exists then so does the right.)

$$\begin{aligned} xr &= (r_1a + s_1b)r \\ &= r_1ar + s_1br \\ &= r_1ra + s_1rb \in \langle a, b \rangle \\ Since\ r_1r&, s_1r \in R \end{aligned}$$

So $\langle a, b \rangle$ is an ideal of R. Is $\langle a, b \rangle$ the smallest ideal of R containing a and b?

Definition of a Principal Ideal: Given any Ring R, and any element of $a \in R$, the principal ideal generated by a is the smallest ideal of R that contains a. It is denoted $\langle a \rangle$. In the case of communatative ring with identity $\langle a \rangle = Ra$.

This means the smallest ideal of R, containing a is $A = \langle a \rangle = Ra$ Also, the smallest ideal of R, containing b is $B = \langle b \rangle = Rb$

Now if we consider another ideal C of R, containing both a and b. If $a \in C$ then $ra \in C$ where $r \in R$. Similarly if $b \in C$ then $sb \in C$ where $s \in R$. Since $ra, sb \in C$ then $ra + sb \in C$. Therefore $\langle a, b \rangle \subseteq C$. So $\langle a, b \rangle$ is the smallest ideal of R containing a and b.

Question 3(b):

Illustrate that $\mathbb{Z}[x]$ is not a principal ideal domain by giving an example of an ideal which is not a principal ideal. (Hint consider the ideal $\langle 2, x \rangle$).

Definition of PID: If R is an integral domain and every ideal of R is principal, then R is called a PID.

To show $\mathbb{Z}[x]$ is not a PID, we need to find an ideal of R which is not a principal ideal.

Consider $J = \langle 2, x \rangle$ which is an ideal of $\mathbb{Z}[x]$ (note given in the question so not necessary to prove).

$$J = \langle 2, x \rangle = \{2p(x) + xq(x) | p, q \in \mathbb{Z}[x]\}$$

If J is a principal ideal then there exists an $f \in \mathbb{Z}[x]$ such that:

$$J = \langle 2, x \rangle = \langle f \rangle$$

Then $f|2$ and $f|x$ so $f = \pm 1$.

But this is a contradiction because $\pm 1 \notin J$. This is because J must have an even constant term.

So we cannot write the ideal $J = \langle f \rangle$, so J is not a principal ideal and therefore $\mathbb{Z}[x]$ is not a PID.

Question 3(c):

Show that $\langle 2, x \rangle$ is a prime ideal of $\mathbb{Z}[x]$.

Definition: P is a prime ideal of ring R, if $ab \in P$ then $a \in P$ or $b \in P$. The contrapositive of this is : if $a \notin P$ and $b \notin P$ then $ab \notin P$.

$$J = \langle 2, x \rangle = \{2p(x) + xq(x) | p, q \in \mathbb{Z}[x]\}$$

Thus the ideal J consists of all polynomials of the form

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

where a_0 is even.

Consider: $a(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ where $a_0 = 2p + 1$ i.e. odd, and $a(x) \notin J$.

$b(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$ where $b_0 = 2q + 1$ i.e. odd, and $b(x) \notin J$.

$\therefore\ a(x)b(x) = \cdots + a_0b_0 \notin J$ as $a_0.b_0 = 2(2pq + p + q) + 1$ which is odd.

This means J is a prime ideal.

```
In [ ]:
```