

PMTH332 Assignment 5

Jayden Turner (SN 220188234)

22 September 2018

Question 1

Consider the two non-zero matrices $A, B \in M(2; R)$ defined by

$$A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}$$

then $AB = 0$, so $M(2; R)$ has zero divisors. Consider matrix C given by

$$C = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$$

then $AC = \begin{pmatrix} 0 & a^2 \\ 0 & 0 \end{pmatrix}$ and $CA = 0$, so $M(2; R)$ is not commutative.

Question 2

Let F be a finite integral domain and take non-zero $a \in F$. Define F^* to be the set of non-zero elements of F , and define the map $\phi : F^* \rightarrow F^*$ by $\phi(x) = ax$.

Suppose that for $x, y \in F^*$, $\phi(x) = \phi(y)$. Then

$$ax = ay \iff ax - ay = 0 \iff a(x - y) = 0$$

As F is an integral domain, it has no zero-divisors. Therefore the above implies that either $a = 0$ or $x - y = 0$. As a is non-zero by choice, it must hold that $x = y$. Therefore ϕ is injective. Further, as F^* is finite, ϕ must be surjective. Therefore, as $1 \in F^*$, there exists $x \in F^*$ so that $\phi(x) = ax = 1$. Hence, every non-zero element of F has multiplicative inverse, so F is a field.

Question 3

Let R be a non-trivial integral domain with 1. The characteristic of R is the integer n such that $n\mathbb{Z} = \ker \epsilon$, where $\epsilon : \mathbb{Z} \rightarrow R$ is the unique homomorphism of unital rings, given by $\epsilon(n) = n \cdot 1_R$.

Given that $n\mathbb{Z} = \{x \in \mathbb{Z} | x = nm, m \in \mathbb{Z}\}$ and $\ker \epsilon = \{x \in \mathbb{Z} | x \cdot 1_R = 0_R\}$, we can deduce that if n is the characteristic of R , then $nm \cdot 1_R = (n \cdot 1_R)(m \cdot 1_R) = 0_R$ for all $m \in \mathbb{Z}$. $n = 0$ satisfies this, in which case \mathbb{Z} is a subring of R .

Suppose $n \neq 0$ and n is not prime. Then $n = kp$ for some prime $p < n$ and natural number k . n being the characteristic of R , we must have that for non-zero $a \in R$, $na \cdot 1_R = (k \cdot 1_R)(p \cdot 1_R)a = 0_R$. As R is an integral domain, R has no zero-divisors. Hence it must hold that either $k = 0$ or $p = 0$. This is a contradiction of the assumption that n is not prime, hence n must be so.

Therefore, the characteristic of an integral domain with 1 must be either 0 or prime.

Question 4

Given an integral domain D , consider $\tilde{D} = \{(b, a) | a, b \in D, a \neq 0\}$, and the equivalence relation $(b, a) \sim (d, c) \iff bc = ad$. Let F be the set of equivalence classes of this equivalence relation. Define addition and multiplication on F as

$$\begin{aligned} + : F \times F &\rightarrow F, & ([(b, a)], [(d, c)]) &\mapsto [(bc + ad, ac)] \\ \times : F \times F &\rightarrow F, & ([(b, a)], [(d, c)]) &\mapsto [(bd, ac)] \end{aligned}$$

Firstly, we show that the given operations are well defined. Given $(b, a), (b', a'), (d, c), (d', c') \in \tilde{D}$, where $(b, a) \sim (b', a')$ and $(d, c) \sim (d', c')$ we have that

$$\begin{aligned} (b, a) + (d, c) &= (ad + bc, ac) \\ \text{and} \\ (b', a') + (d', c') &= (a'd' + b'c', a'c') \end{aligned}$$

Given that $a'b = b'a$ and $c'd = d'c$, multiply the first by cc' , the second by aa' , and add to get

$$\begin{aligned} cc'a'b + aa'c'd &= cc'b'a + aa'd'c \\ bca'c' + ada'c' &= acb'c' + aca'd' \\ a'c'(ad + bc) &= ac(a'd' + b'c') \end{aligned}$$

which shows that $(b, a) + (d, c) \sim (b', a') + (d', c')$. Concerning multiplication, we have that

$$\begin{aligned} (b, a) \times (d, c) &= (bd, ac) \\ \text{and} \\ (b', a') \times (d', c') &= (b'd', a'c') \end{aligned}$$

Given that $a'b = b'a$ and $c'd = d'c$, multiply the first by the second to get

$$\begin{aligned} a'bc'd &= b'ad'c \\ a'c'bd &= acb'd' \end{aligned}$$

Which shows that $(b, a) \times (d, c) \sim (b', a') \times (d', c')$. Hence both binary operations are well-defined.

We now proceed to prove that F is a field. Firstly, as D is an integral domain, addition and multiplication under F inherit commutativity. The additive identity is $[(0, 1)]$, as

$$[(0, 1)] + [(b, a)] = [(a \cdot b + 0 \cdot a, 1 \cdot a)] = [(b, a)] = [(b, a)] + [(0, 1)]$$

for $[(b, a)] \in F$. Also, each element of F has additive inverse $[(-\frac{b}{a^2}, \frac{1}{a})]$, where $[(b, a)] + [(-\frac{b}{a^2}, \frac{1}{a})] = [(0, 1)]$. Hence $(F, +)$ is an abelian group. Further, given $[(b, a)], [(d, c)], [(f, e)]$ in F ,

$$[(b, a)] \times ([(d, c)] \times [(f, e)]) = [(b, a)] \times [(df, ce)] = [(bdf, ace)] = [(bd, ac)] \times [(f, e)] = ([(b, a)] \times [(d, c)]) \times [(f, e)]$$

so multiplication is associative. For $(F, +, \times)$ to form a commutative ring, it remains to show that the distributive laws hold. Firstly,

$$\begin{aligned} [(b, a)] \times ([(d, c)] + [(f, e)]) &= [(b, a)] \times [(cf + de, ce)] \\ &= [(bcf + bde, ace)] \\ &= [(abcf + abde, a^2ce)] \\ &= [(bd, ac)] + [(bf, ae)] \\ &= [(b, a)] \times [(d, c)] + [(b, a)] \times [(f, e)] \end{aligned}$$

Secondly,

$$\begin{aligned}
([(b, a)] + [(d, c)]) \times [(f, e)] &= [(ad + bc, ac)] \times [(f, e)] \\
&= [(adf + bcf, ace)] \\
&= [(adef + bcef, ace^2)] \\
&= [(bf, ae)] + [(df, ce)] \\
&= [(b, a)] \times [(f, e)] + [(d, c)] \times [(f, e)]
\end{aligned}$$

so $(F, +, \times)$ forms a commutative ring. Now, to show that F is a field, it remains to show that F is a commutative division ring. That is, given $[(b, a)] \neq [(0, 1)]$ in F , there exists a multiplicative inverse for that element. The multiplicative identity is $[(1, 1)]$ as $[(b, a)] \times [(1, 1)] = [(b, a)]$. $[(b^{-1}, a^{-1})]$ is the multiplicative inverse element. This always exists for non-zero elements of F , as $a \neq 0$ ever, and if $b = 0$ then $(b, a) \sim (0, 1)$, which contradicts $[(b, a)]$ being non-zero. Therefore, F is a commutative division ring, and is thus a field.