MA3201 Rings and Modules, 2014

Solution Sheet 1

To be discussed on Friday 5 September and Friday 12 September.

Problems from: Bhattacharya, P. B.; Jain, S. K.; Nagpaul, S. R. Basic abstract algebra. Second edition. Cambridge University Press, Cambridge, 1994.

Page	Problem number
174	3,4,5ab,6
187	1,2

Page 174, Question 3(a)(i)

Let $r = a + b\sqrt{-1}$, $s = c + d\sqrt{-1}$ be elements of A. Then $r - s = (a - c) + (b - d)\sqrt{-1} \in A$, since $a - c, b - d \in \mathbb{Z}$. And

$$rs = (a + b\sqrt{-1})(c + d\sqrt{-1}) = (ac - bd) + (ad + bc)\sqrt{-1} \in A$$

since $ac - bd, ad + bc \in \mathbb{Z}$.

Finally, $1 = 1 + 0\sqrt{-1} \in A$, so A is a subring of $\mathbb{C}$.

Page 174, Question 3(a)(ii)

Let $r = a + b\sqrt{-3}$, $s = c + d\sqrt{-3}$ be elements of A. Write $a = a' + e$, $b = b' + e$, $c = c' + f$ and $d = d' + f$, where $e = 0$ or $e = \frac{1}{2}$ and $f = 0$ or $f = \frac{1}{2}$. Then

$$\begin{aligned} r - s &= (a - c) + (b - d)\sqrt{-3} \\ &= (a' + e) - (c' + f) + ((b' + e) - (d' + f))\sqrt{-3} \\ &= a' - c' + e - f + (b' - d' + e - f)\sqrt{-3} \end{aligned}$$

Since $e - f =\in \{0, \frac{1}{2}, -\frac{1}{2}\}$, we see that $a - c$ and $b - d$ are either both integers or both half odd integers and $r - s \in A$.

We also have

$$\begin{aligned} rs &= ac - 3bd + (ad + bc)\sqrt{-3} \\ &= (a' + e)(c' + f) - 3(b' + e)(d' + f) + ((a' + e)(d' + f) + (b' + e)(c' + f))\sqrt{-3} \\ &= a'c' + a'f + ec' + ef - 3b' - 3b'f - 3ed' - 3ef + \\ &\qquad + (a'd' + a'f + ed' + ef + b'c' + b'f + ec' + ef)\sqrt{-3} \\ &= a'c' - 3b'd' + e(c' - 3d') + f(a' - 3b') - 2ef + \\ &\qquad + (a'd' + b'c' + e(c' + d') + f(a' + b') + 2ef)\sqrt{-3} \\ &= x + y\sqrt{-3}, \end{aligned}$$

where $x = a'c' - 3b'd' + e(c' - 3d') + f(a' - 3b') - 2ef$ and $y = (a'd' + b'c' + e(c' + d') + f(a' + b') + 2ef)\sqrt{-3}$.

Since $e, f \in \{0, \frac{1}{2}\}$, x and y are either integers or half of odd integers. We also have:

$$y - x = a'd' + b'c' - a'c' + 3b'd' + 4d'e + 4b'f + 4ef \in \mathbb{Z},$$

and it follows that either x, y are both integers or both half odd integers. Hence $rs \in A$. Since also $1 = 1 + 0\sqrt{-3} \in A$, A is a subring of $\mathbb{C}$.

Page 174, Question 3(b)

Let $r, s \in eAe$. Then there are elements $a, b \in A$ such that $r = eae$, $s = ebe$. So $r - s = eae - ebe = e(ae - eb)e \in eAe$ and $rs = eaeebe = e(aeb)e \in eAe$. In fact, in general $1 \notin eAe$, so it is not a subring of A in our sense. But it is a ring, with identity element e.

Page 174, Question 4

Let R be an integrable domain, and suppose that $e \in R$ is an idempotent. Then $e^2 = e = e \cdot 1$. Hence $e(e - 1) = 0$. So, since R is an integrable domain, $e = 0$ or $e - 1 = 0$ and therefore $e = 0$ or $e = 1$. These elements are idempotents, so we see that the only idempotents of R are 0 and 1 as required.

Page 174, Question 5(a)(i)
We have

$$\mathbb{Z}/(4) = \{0, 1, 2, 3\}$$

(using i to represent the coset $i + (4)$). We have $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 0$ and $3^2 \equiv 1$ mod 4. So the idempotents are 0 and 1.

The powers of 1 are all equal to 1, so it is not niplotent. The powers of 3 alternate between 1 and 3, so it is not nilpotent. Since $0^2 \equiv 0$ and $2^2 \equiv 0$, the nilpotent elements are 0 and 2.

We have $3 \cdot 3 \equiv 1 \mod 4$, but no multiple of 2 is equal to 1 mod 4. So the invertible elements are 1 and 3.

Page 174, Question 5(a)(ii)
A check shows that the idempotents are $\{0, 1, 5, 16\}$.

The powers of 2 are $2, 4, 8, 16, 12, 4, 8, \ldots$, then repeating, so 2 is not nilpotent. If one of these powers was nilpotent, then 2 would be, so none of these elements is nilpotent. The powers of 3 are $3, 9, 7, 1, 3, 9, 7, \ldots$ then repeating. So $3, 7, 9$ are not nilpotent. The powers of 6 are $6, 16, 16, \ldots$, then repeating, so $6, 16$ are not nilpotent. Since 5 is a non-zero idempotent, it cannot be nilpotent. Since 1 is the identity, it cannot be nilpotent.

If x is nilpotent then $x^n \equiv 0$ for some positive integer n, so $(-x)^n \equiv (-1)^n x^n \equiv 0$. Therefore x is nilpotent if and only if $-x$ is nilpotent. Hence $1, 2, 3, 4, 5, 6, 7, 8, 9$ and their negatives, $11, 12, 13, 14, 15, 16, 17, 18, 19$ are not nilpotent. But $10^2 \equiv 0$, so 10 is nilpotent. So there are two nilpotent elements: 0 and 10.

The elements are $1, 3, 7, 9, 11, 13, 17$ and 19 are invertible, since 1 is the identity, $3 \cdot 7 \equiv 1$, $13 \cdot 17 \equiv 1$, $9 \cdot 9 \equiv 1$ and $11 \cdot 11 \equiv 1$ (noting that multiplication is commutative in $\mathbb{Z}/(20)$ so we only have to compute these products one way round. Furthermore, an even number cannot be invertible in $\mathbb{Z}/(20)$ since the product of an even number with any number is even, so cannot be congruent to 1 mod 20. Similarly, the product of 5 with any number will be divisible by 5, and hence congruent to $0, 5, 10$ or 20 mod 20.

Therefore the invertible elements are $1, 3, 7, 9, 11, 13, 17, 19$. (Or, see part (c) of this question).

Page 174, Question 5(b)
Suppose that $r, s \in U(R)$. Then $s^{-1}r^{-1}(rs) = 1_R = (rs)(s^{-1}r^{-1})$, so $rs \in U(R)$. Clearly $1_R \in U(R)$, and $1_R r = r 1_R = r$ for all $r \in U(R)$. Since multiplication in R is associative, so is multiplication in $U(R)$. And, if $r \in U(R)$, then $r^{-1}r = rr^{-1} = 1_R$, so $r\ r^{-1} \in U(R)$ and is an inverse for r in $U(R)$. Hence $U(R)$ is a multplicative group.

Page 174, Question 6(a)
Let $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and $B = \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}$, with $a, b, c, d, e, f \in \mathbb{Z}$, be arbitrary elements of S. Then

$$A - B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} \begin{pmatrix} a-d & b-e \\ 0 & c-f \end{pmatrix}$$

lies in S (since $a - d, b - e$ and $c - f \in \mathbb{Z}$). And

$$AB = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix}$$

lies in S (noting that $ad, ae + bf, cf$ all lie in $\mathbb{Z}$). And finally $1_{M_2(Z)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$.

Hence S is a subring of $M_2(\mathbb{Z})$, and hence a ring.

Page 174, Question 6(b)
We prove this by induction on k. For $k = 1$, we have

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^1 = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

is of the required form. Suppose that the result holds for k, i.e. that

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^k = \begin{pmatrix} a & x \\ 0 & c \end{pmatrix}$$

for some integer x. Then

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{k+1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a^k & x \\ 0 & c^k \end{pmatrix}^k = \begin{pmatrix} a^{k+1} & a^k x + bc^k \\ 0 & c^k \end{pmatrix}$$

which is of the required form. The result follows by induction.

Page 174, Question 6(b)

The matrix

$$X = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

is idempotent if and only if $X^2 = X$, i.e. if and only if

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a^2 & ab + bc \\ 0 & c^2 \end{pmatrix}$$

which holds if and only if $a^2 = a$, $c^2 = c$ and $ab + bc = b$. If this holds, a, c must be 0 or 1 and $b(a + c) = b$, so $b = 0$ or $a + c = 1$. Hence X must be a matrix of the form

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

with $b \in \mathbb{Z}$. It is easy to check that these are idempotent matrices, so this is the list of idempotents in $M_2(\mathbb{Z})$.

By part (a), if the matrix X is nilpotent then there is some positive integer k such that $a^k = c^k = 0$, so $a = c = 0$, and X must be of the form

$$X = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix},$$

for $b \in \mathbb{Z}$. It is easy to check that then $X^2 = 0$, so these are exactly the nilpotent matrices in $M_2(\mathbb{Z})$.

Let

$$X = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$$

be nilpotent matrices. Then

$$X - Y = \begin{pmatrix} 0 & a - b \\ 0 & 0 \end{pmatrix}$$

is of the same form, so is nilpotent, and so is

$$XY = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

However, the identity matrix is not nilpotent, so the nilpotent matrices do not form a subring of $M_2(\mathbb{Z})$.

Page 187, Question 1

Let R be a commutative ring, and suppose that R has no non-trivial ideals, i.e. the only ideals of R are $\{0\}$ and R itself. We must assume also that $R \neq \{0\}$. Let x be a non-zero element of R. Then (x) is a non-zero ideal of R, hence equal to R. So there is $y \in R$ such that $xy = 1$ (and $yx = 1$ as R is commutative). Hence R is a field.

Page 187, Question 2

Suppose that R is a field and let I be a non-zero ideal of R. Then there is a non-zero element $x \in I$. Since R is a field, there is $y \in R$ such that $yx = 1$. So $1 \in I$, and hence $I = R$.

Problem 1. Let R be a ring. Find the centre of the ring $M_2(R)$.

Suppose that $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ lies in the centre of R. Then $E_{11}X = XE_{11}$, so

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix},$$

so $b = c = 0$. Furthermore, Then $E_{12}X = XE_{12}$, so

$$\begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix},$$

so $a = d$. If $r \in R$, then

$$\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} X = X \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix},$$

so

$$\begin{pmatrix} ra & 0 \\ 0 & ra \end{pmatrix} = \begin{pmatrix} ar & 0 \\ 0 & ar \end{pmatrix}$$

and therefore $ra = ar$, so $a \in Z(R)$. Thus we have that

$$X = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},$$

with $a \in Z(R)$. It is easy to check that all such elements lie in the centre of $M_2(R)$, so

$$Z(M_2(R)) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \, : \, a \in Z(R) \right\}.$$

Problem 2. Let $\mathbb{F}$ be a field. Let I be the subset:

$$I = \left\{ \begin{pmatrix} x & x \\ y & y \end{pmatrix} \, : \, x, y \in \mathbb{F} \right\}$$

of $M_2(\mathbb{F})$. Show that I is a left ideal of $M_2(\mathbb{F})$. Is I a subring of $M_2(\mathbb{F})$?

Let

$$X = \begin{pmatrix} x & x \\ y & y \end{pmatrix}, X' = \begin{pmatrix} x' & x' \\ y' & y' \end{pmatrix} \in I.$$

Then

$$X - X' = \begin{pmatrix} x - x' & x - x' \\ y - y' & y - y' \end{pmatrix} \in I.$$

Let $X = \begin{pmatrix} x & x \\ y & y \end{pmatrix} \in I$ and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{F})$. Then $AX = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & x \\ y & y \end{pmatrix} = \begin{pmatrix} ax+by & ax+by \\ cx+dy & cx+dy \end{pmatrix} \in I$.

Hence I is a left ideal of $M_2(\mathbb{F})$. Since $1_{M_2(\mathbb{F})} \notin I$, I is not a subring of $M_2(\mathbb{F})$.

Problem 3. Let $\mathbb{F}$ be a field. Let Q be the quiver:

$$1 \xrightarrow{\alpha} 2 \xrightarrow{\beta} 3$$

and $R = \mathbb{F}Q$ the corresponding path algebra. Show that the subspace I of R spanned by $\alpha, \beta, \beta\alpha$ is an ideal of R.

Since I is a subspace of I, it follows that for all $x, y \in I$, $x - y \in I$.

Note that the set $\{\alpha, \beta, \beta\alpha\}$ consists of all the paths in Q of length at least 1. Multiplying such a path (on either side) by any other path will give a path at least as long or zero (if the composition cannot be done). In either case the answer will lie in I. It follows that multiplying any linear combination of these elements (on either side) by any other linear combination of paths must lie in I. Hence I is an ideal of $\mathbb{F}Q$.

Problem 4. Let R and S be rings. Show that the left ideals of the direct product $R \times S$ are all of the form

$$I \times J = \{(x, y) \, : \, x \in I, y \in J\},$$

where I is a left ideal of R and J is a left ideal of S.

Suppose that I is a left ideal of R and J is a left ideal of S. Let $(x, y), (x', y') \in I \times J$. Then $x - x' \in I$ since I is a left ideal of R, and $y - y' \in J$ since J is a left ideal of S. Hence $(x, y) - (x', y') = (x - x', y - y') \in I \times J$. Let $(r, s) \in R$ and $(x, y) \in I \times J$. Then $(r, s)(x, y) = (rx, sy)$. Since I is a left ideal of R, $rx \in I$. Since J is a left ideal of S, $sy \in J$. Hence $(rx, sy) \in I \times J$. So $I \times J$ is a left ideal of S.

Suppose that K is a left ideal of $R \times S$. Let I be the set of elements $r \in R$ such that there is an element $s \in S$ such that $(r, s) \in K$. Let J be the set of elements $s \in S$ such that there is an element $r \in R$ such that $(r, s) \in K$. We claim that $K = I \times J$.

Suppose that $(r, s) \in K$. Then $r \in I$ and $s \in J$ by definition. So $(r, s) \in I \times J$. Conversely, suppose that $(r, s) \in I \times J$. Then there is an element $s' \in S$ such that $(r, s') \in K$ and an element $r' \in R$ such that $(r', s) \in K$. Then $(r, s) = (1, 0)(r, s') + (0, 1)(r', s) \in K$. We have shown that $K = I \times J$ as required. The result follows.

R. J. Marsh, 2014-09-09.