MA3201 Rings and Modules, 2014

Solution Sheet 2

To be discussed on Friday 19 September and Friday 26 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
187	4 (second part)
194	2,4
202	4, 6
209	3
210	1, 2

Page 187, Q4 second part.

By Corollary 2.29 from lectures, the ideals of $\mathbb{Z}/(10)$ are of the form $I/(10)$ for an ideal I of $\mathbb{Z}$ containing (10). The ideals of $\mathbb{Z}$ are of the form (a), for $a \in \mathbb{Z}$. Since $(a) = (-a)$ and $(10) \not\subseteq (0)$ we can assume that $a > 0$. We have $(10) \subseteq (a)$ if and only if $a|10$, so the ideals of $\mathbb{Z}$ containing (10) are $(1) = \mathbb{Z}$, (2), (5) and (10). Hence the ideals of $\mathbb{Z}/(10)$ are

$$\mathbb{Z}/(10),\ (2)/(10),\ (5)/(10),\ (10)/(10).$$

Page 194, Q2.

We answer the corresponding question with $\mathbb{Z}$ replaced by $\mathbb{Q}$. Define a map $\varphi : \mathbb{Q}[x] \to \mathbb{Q}[i]$ by setting

$$\varphi(a_0 + a_1x + \cdots + a_rx^r) = a_0 + a_1i + \cdots + a_ri^r$$

for any polynomial $a_0 + a_1x + \cdots + a_rx^r \in \mathbb{Q}[x]$. Then it can be shown that φ is a ring homomorphism.

If $f \in \mathbb{Q}[x]$ lies in the kernel of φ, then $f(i) = 0$. Since f has real coefficients, $f(-i) = 0$ also. Write $f = q \cdot (x^2 + 1) + r$ where $q, r \in \mathbb{Q}[x]$ and $r = 0$ or the degree of r is less than 2. Since $f(i) = f(-i) = 0$, $r(i) = r(-i) = 0$, which gives a contradiction unless $r = 0$. So $f \in (x^2 + 1)$.

If $f \in (x^2+1)$ then $f = q \cdot (x^2+1)$ for some $q \in \mathbb{Q}[x]$, so $\varphi(f) = q(i)(i^2+1) = 0$ and $f \in \ker \varphi$. Hence $\ker \varphi = (x^2 + 1)$.

The image of φ contains 1 and $\varphi(x) = i$, so must be the whole of $\mathbb{Q}[i]$, as it is a subring of $\mathbb{Q}[i]$. Hence, applying the Fundamental Theorem of Homomorphisms, we obtain an isomorphism:

$$\overline{\varphi} : \frac{\mathbb{Q}[x]}{(x^2 + 1)} \cong \mathbb{Q}[i]$$

as required.

For the original question (i.e. working over $\mathbb{Z}$ instead of $\mathbb{Q}$), we can use a version of the division algorithm over a commutative integral domain (since $\mathbb{Z}$ is a commutative integral domain): see the book, Section 11.4, Theorem 4.1 on page 220 (but this is beyond the scope of the course).

Page 194, Q4.

Let R be a commutative ring. Recall that an element r in R is said to be *nilpotent* if $r^n = 0$ for some integer $n \geq 1$. Let N be the set of all nilpotent elements in R. Let $x, y \in N$. Then there are integers $n, m \geq 1$ such that $x^n = 0$ and $y^m = 0$. We have, using the binomial expansion,

$$(x+y)^{n+m} = \sum_{r=0}^{n+m} \binom{n+m}{r} x^r y^{n+m-r}. \tag{1}$$

Fix $0 \leq r \leq n+m$. If $r < n$ then $n+m-r > n+m-n = m$. It follows that each of the terms on the right hand side of (1) is zero and thus that $x+y \in N$.

Let $r \in R$ and $x \in N$. Then there is an integer $n \geq 1$ such that $x^n = 0$. So $(rx)^n = r^n x^n = 0$, and thus $rx \in N$. We have shown that N is an ideal in R.

If $r+N$ is a nilpotent element in R/N, then $(r+N)^n = 0$ for some integer $n \geq 1$, so $r^n + N = 0 + N$ and therefore $r^n \in N$ and is itself nilpotent. Therefore there is an integer $m \geq 1$ such that $(r^n)^m = 0$, so $r^{nm} = 0$ and $r \in N$. Hence $r + N = 0$ and we see that the only nilpotent element of R/N is $0 + N$.

Let $R = M_2(\mathbb{Z})$. Then R is a noncommutative ring. Let

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in R.$$

Then $X^2 = Y^2 = 0$. But

$$X + Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad (X+Y)^2 = 1_R. \tag{2}$$

If $X+Y$ is nilpotent then let n be minimal such that $(X+Y)^n = 0_R$. Then $n > 1$. But then $(X+Y)^{n-2} = 0_R$ by (2), a contradiction.

Page 202, Q4.

Let $e \in R$ be idempotent. Then eR and $(1-e)R$ are right ideals of R. We argue as in Lemma 2.36 from lectures. Note that $(1-e)e = e - e^2 = 0$, $e(1-e) = e - e^2 = 0$ and $(1-e)^2 = 1 - e - e + e^2 = 1 - e$. Suppose that $er + (1-e)s = er' + (1-e)s'$ for $r, s \in R$. Then

$$e^2 r + e(1-e)s = e^2 r' + e(1-e)s',$$

so $er = er'$. Similarly, $(1-e)s = (1-e)s'$, so the sum $eR + (1-e)R$ is direct. Furthermore $1 = e1 + (1-e)1 \in eR + (1-e)R$, so $eR \oplus (1-e)R = R$.

Page 202, Q6.

(a) We have seen in lectures that for any ring R and $a \in R$, Ra is a left ideal of R and aR is a right ideal of R.

(b) Let A be a non-zero left ideal of R contained in Re_{ii}. Let X be a non-zero matrix in A. Since $e_{jk}e_{ii} = 0$ for $i \neq k$ and $e_{ji}e_{ii} = e_{ji}$, we have

$$X = X_{1i}e_{1i} + \cdots + X_{ni}e_{ni}.$$

Since X is non-zero, we have $X_{ji} \neq 0$ for some j. Then $X_{ji}^{-1} e_{1j} X = e_{1i} \in A$. Hence $e_{j1}e_{1i} = e_{ji} \in A$ for all j, and it follows that $A = Re_{ii}$. The statement for right ideals is similar.

(c) We have $1 = e_{11} + \cdots e_{nn}$ lies in the sum of the Re_{ii}, so the sum is equal to R. Furthermore, $e_{ii}e_{jj} = 0$ for all $i \neq j$. By Lemma 2.36 in the lectures

$$R = \bigoplus_{i=1}^{n} Re_{ii}.$$

The other statement is similar.

(d) By (b), each of the ideals Re_{ii} is a miminal left ideal. So, by (c) and Example 3.4(e) in the book, every left ideal in R is of the form Re, where e is an idempotent. The statement for right ideals is similar.

Page 209, Q3.

Let $a = x^2 + 2x + 2$ and $b = x^2 - 2x + 2$, elements of $\mathbb{Q}[x]$. Then $ab = (x^4 + 4)$. But any non-zero element of $(x^4 + 4)$ will have degree at least 4, so $a, b \notin (x^4 + 4)$. It follows (from Theorem 2.48 in lectures) that $(x^4 + 4)$ is not a prime ideal in $\mathbb{Q}[x]$.

Page 210, Q1.

Let A, B be nilpotent ideals in a ring R. Then there are integers n, m such that $A^n = \{0\}$ and $B^m = \{0\}$. Recall that

$$A + B = \{a + b \,:\, a \in A, b \in B\}.$$

Then any element of $(A + B)^{n+m}$ is a finite sum of elements of R of the form $(a_1 + b_1)(a_2 + b_2) \cdots (a_{n+m} + b_{n+m})$ for $a_i \in A$, $b_i \in B$. Expanding this out, we obtain a sum of products, each of which contains r elements from A and $n + m - r$ elements from B, for some r with $0 \leq r \leq n + m$. If $r < n$ then $n + m - r > m$, so there are always either at least n elements from A or at least m elements from B in each product. So each product lies in A^n or B^m (since A, B are ideals), and hence is zero. It follows that $(A + B)^{n+m} = \{0\}$ and $A + B$ is nilpotent as required.

Page 210, Q2.

Let $A_1, \ldots, A_n$ be nil ideals in a commutative ring R. Let $x \in A_1 + \cdots + A_n$. Then there are $a_1 \in A_1, \ldots,\ a_n \in A_n$ such that $x = a_1 + \cdots + a_n$. For each i, $a_i \in A_i$, so there is an integer m_i such that $a_i^{m_i} = 0$. Then $x^{m_1+\cdots+m_n}$ is a sum of products, each containing $m_1 + \cdots + m_n$ elements from $\{a_1, \ldots, a_n\}$. Such a product cannot contain fewer than m_i instances of a_i for each i, so there must be some i for which it contains at least m_i instances of a_i. Since R is commutative, such a product is zero. It follows that $x^{m_1+\cdots+m_n} = 0$ and therefore $A_1 + \cdots + A_n$ is nil.

Problem 1. Let R be a commutative ring and P a prime ideal of R. Show that R/P is an integral domain.

Since $P \neq R$, R/P is a non-zero ring. Let $a, b \in R$ and suppose that $(a + P)(b + P) = 0 + P$. Then $ab \in P$. Since P is a prime ideal, either $a \in P$ or $b \in P$. Hence either $a + P = 0 + P$ or $b + P = 0 + P$. Hence R/P is an integral domain.

Problem 2. Let $\mathbb{F}$ be a field and let

$$R = U_3(\mathbb{F}) = \begin{pmatrix} \mathbb{F} & \mathbb{F} & \mathbb{F} \\ 0 & \mathbb{F} & \mathbb{F} \\ 0 & 0 & \mathbb{F} \end{pmatrix}.$$

Show that

$$I = \begin{pmatrix} 0 & \mathbb{F} & \mathbb{F} \\ 0 & 0 & \mathbb{F} \\ 0 & 0 & 0 \end{pmatrix}$$

is an ideal of R and find the ideals of R containing I. Which of these are maximal ideals of R?

Define a map $\varphi : R \to \mathbb{F} \times \mathbb{F} \times \mathbb{F}$ by setting

$$\varphi\left(\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}\right) = (a, d, f).$$

It is easy to check that φ is a ring homomorphism. The kernel is I, so I is an ideal of R. The image is $\mathbb{F} \times \mathbb{F} \times \mathbb{F}$. Note that the only ideals in $\mathbb{F}$ are $\{0\}$ and $\mathbb{F}$. Applying an analogous argument to Problem 4 on Problem Sheet 1, we see that the left ideals (and hence the ideals) of $\mathbb{F} \times \mathbb{F} \times \mathbb{F}$ are of the form $I_1 \times I_2 \times I_3$ where each I_i is either $\{0\}$ or $\mathbb{F}$. By the Correspondence Theorem (Theorem 2.28) we see that the ideals of R containing I are of the form $\varphi^{-1}(I_1 \times I_2 \times I_3)$ with I_1, I_2, I_3 as above, i.e.

$$\begin{pmatrix} 0 & \mathbb{F} & \mathbb{F} \\ 0 & 0 & \mathbb{F} \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} \mathbb{F} & \mathbb{F} & \mathbb{F} \\ 0 & 0 & \mathbb{F} \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \mathbb{F} & \mathbb{F} \\ 0 & \mathbb{F} & \mathbb{F} \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \mathbb{F} & \mathbb{F} \\ 0 & 0 & \mathbb{F} \\ 0 & 0 & \mathbb{F} \end{pmatrix},$$

$$\begin{pmatrix} \mathbb{F} & \mathbb{F} & \mathbb{F} \\ 0 & \mathbb{F} & \mathbb{F} \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} \mathbb{F} & \mathbb{F} & \mathbb{F} \\ 0 & 0 & \mathbb{F} \\ 0 & 0 & \mathbb{F} \end{pmatrix}, \begin{pmatrix} 0 & \mathbb{F} & \mathbb{F} \\ 0 & \mathbb{F} & \mathbb{F} \\ 0 & 0 & \mathbb{F} \end{pmatrix}, \begin{pmatrix} \mathbb{F} & \mathbb{F} & \mathbb{F} \\ 0 & \mathbb{F} & \mathbb{F} \\ 0 & 0 & \mathbb{F} \end{pmatrix}.$$

Let J be one of these ideals, $J \neq R$. Then J is maximal if $J \subseteq K$ for some ideal K implies $K = J$ or $K = R$. If $J \subseteq K$ then $I \subseteq K$ (as $I \subseteq J$) so J is maximal if no other ideal in the list contains J, apart from J itself or the whole of R.

We see that the maximal ideals of R containing I are

$$\begin{pmatrix} \mathbb{F} & \mathbb{F} & \mathbb{F} \\ 0 & \mathbb{F} & \mathbb{F} \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} \mathbb{F} & \mathbb{F} & \mathbb{F} \\ 0 & 0 & \mathbb{F} \\ 0 & 0 & \mathbb{F} \end{pmatrix}, \begin{pmatrix} 0 & \mathbb{F} & \mathbb{F} \\ 0 & \mathbb{F} & \mathbb{F} \\ 0 & 0 & \mathbb{F} \end{pmatrix}.$$

Problem 3.

Let n be an integer, $n \geq 2$. Show that the ring $\mathbb{Z}$ cannot be written as a direct sum of n non-zero left ideals.

Firstly, since $\mathbb{Z}$ is commutative, left ideals and ideals in $\mathbb{Z}$ are the same thing. Suppose that $\mathbb{Z} = I_1 + \cdots + I_n$, where each I_i is a non-zero ideal of $\mathbb{Z}$ and $n \geq 2$. Then, for each i, $I_i = (a_i)$ for some non-zero integer a_i. Then we have $1 = x_1 + \cdots + x_n$, with $x_i \in I_i$ for all i. But we also have

$$1 = (x_1 - a_1a_2) + (x_2 + a_1a_2) + x_3 + \cdots + x_n,$$

noting that $x_1 - a_1a_2 \in I_1$ and $x_2 + a_1a_2 \in I_2$. Hence the sum $I_1 + \cdots + I_n$ is not direct.