MA3201 Rings and Modules, 2014

Solution Sheet 3

To be discussed on Friday 3 October and Friday 10 October.

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

Page	Problem number
248	1, 2, 3
252-3	5, 8
260	1, 4, 6, 7
268	1, 3, 6, 7

Page 248, Q1

Suppose that S is a ring and R a subring of S. Then S is an abelian group. Furthermore, the axioms:

(1) $r(s_1+s_2) = rs_1 + rs_2$ for all $r \in R$, $s_1, s_2 \in S$;
(2) $(r_1+r_2)s = r_1s + r_2s$ for all $r_1, r_2 \in R$, $s \in S$;
(3) $(r_1r_2)s = r_1(r_2s)$ for all $r_1, r_2 \in R$, $s \in S$;
(4) $1_Rs = s$ for all $s \in S$.

all hold because S is a ring and $1_R = 1_S$. So S is an R-module. It is easy to check that R is a subring of $R[x]$. So $R[x]$ becomes an R-module in the above way.

Page 248, Q2

Note that the notation (a_i) stands for the sequence $(a_1, a_2, \ldots)$. It is easy to check that the set S forms an abelian group. We check that other axioms for an R-module all hold. Let $r, r_1, r_2 \in R$ and $(a_i), (b_i) \in S$. Then

$$r((a_i)+(b_i)) = r(a_i+b_i) = (r(a_i+b_i)) = (ra_i + rb_i) = (ra_i) + (rb_i).$$
$$(r_1+r_2)(a_i) = ((r_1+r_2)a_i) = (r_1a_i + r_2a_i) = (r_1a_i) + (r_2a_i) = r_1(a_i) + r_2(a_i).$$
$$(r_1r_2)(a_i) = ((r_1r_2)a_i) = (r_1(r_2a_i)) = r_1(r_2(a_i)).$$
$$1_r(a_i) = (1_Ra_i) = (a_i).$$

Hence S is an R-module.

Page 248, Q3

Let M be an additive abelian group and suppose that M is a $\mathbb{Z}$-module. We show by induction on a that $am = m + m + \cdots + m$ (with a copies of m) for all $a > 0$ and all $m \in M$. By the axioms, we have $1m = m$ for all $m \in M$. Suppose that $(a-1)m = m + m + \cdots + m$ (with $a-1$ copies of m) for all $m \in M$. Then $am = (a-1+1)m = (a-1)m + m = m + m + \cdots + m$ (with a copies of m), and the result holds for a. Hence the result holds by induction for all $a > 0$.

We also have $0m = m$ for all $m \in M$ (as this is true in any module). If $a < 0$ and $m \in M$ then

$$0 = 0m = (-a+a)m = (-a)m + am,$$

so

$$(-a)m = -(am) = -(m + m + \cdots + m) = -m - m - \cdots - m$$

(with a copies of m). Thus we see that the am is uniquely determined for all $a \in \mathbb{Z}$.

Page 252-3, Q5

Let R be a ring, M an R-module, and

$$I = \{x \in R : xM = \{0\}\}.$$

Note that

$$xM = \{xm : m \in M\}.$$

Let $x, y \in I$. Then $(x+y)M = xM + yM = \{0\} + \{0\} = \{0\}$, so $x + y \in I$. Let $r \in R$ and $x \in I$. Then $(rx)M = r(xM) = r\{0\} = \{0\}$, so $rx \in I$. And $(xr)M = x(rM) = \{0\}$ since $rM \subseteq M$, so $xr \in I$. Hence I is an ideal of R.

Page 252-3, Q8

Let R be the ring $\mathbb{Z}$ and $M = (\mathbb{Z}, \mathbb{Z})$ the set of pairs of integers. Then M is a $\mathbb{Z}$ module, with $r(a, b) = (ra, rb)$ for all $r, a, b \in \mathbb{Z}$. In fact, M is the external direct sum $_\mathbb{Z} \oplus _\mathbb{Z}$. Let

$$K = \{(a, 0) : a \in \mathbb{Z}\}$$

and

$$K' = \{(0, b) : b \in \mathbb{Z}\}.$$

Let $L = K$ and

$$L' = \{(a, a) : a \in \mathbb{Z}\}.$$

Then it is easy to check that K, K', L, L' are $\mathbb{Z}$-submodules of M. Furthermore, as we have seen for external direct sums in lectures, M is the (internal) direct sum of the submodules K and K'.

If $(a, b) \in M$ then $(a, b) = (a - b, 0) + (b, b)$. If $(a, 0) + (b, b) = (a', 0) + (b', b')$ then $a + b = a' + b'$ and $b = b'$, so $a = b$ and $a' = b'$. It follows that M is the direct sum of L and L' also, and we can observe that $K' \neq L'$.

Page 260, Q1

(a) Firstly, $f(0_M) + f(0_M) = f(0_M + 0_M) = f(0_M)$, so $f(0_M) = 0_N$ and $\ker(f)$ is nonempty. If $m, m' \in \ker(f)$ then $f(m - m') = f(m) - f(m') = 0_N - 0_N = 0_N$. So $\ker(f)$ is a subgroup of M. If $r \in R$ and $m \in \ker(f)$ then $f(rm) = rf(m) = r0_M = 0_M$. (Note that $r0_M + r0_M = r(0_M + 0_M) = r0_M$, so $r0_M = 0_M$). So $rm \in \ker(f)$. Hence $\ker(f)$ is an R-submodule of M.

(b) Firstly note that $\mathrm{im}(f)$ is nonemmpty since $f(0_M) = 0_N$ lies in $\mathrm{im}(f)$. Let $n, n' \in \mathrm{im}(f)$. Then there are elements $m, m' \in M$ such that $f(m) = n$ and $f(n) = n'$. So $f(m - m') = n - n' \in \mathrm{im}(f)$. Let $n \in \mathrm{im}(f)$ and $r \in R$. Then there is $m \in M$ such that $f(m) = n$. We have $f(rm) = rf(m) = rn \in \mathrm{im}(f)$. Hence $\mathrm{im}(f)$ is an R-submodule of N.

Page 260, Q4

Let M be an R-module and suppose that $x \in M$ satisfies $rx = 0$ implies $r = 0$, for $r \in R$. Define $\varphi : {}_RR \to Rx$ by sending r to rx for all $r \in {}_RR$. Then, for $r, s \in {}_RR$, we have

$$\varphi(r + s) = (r + s)x = rx + sx = \varphi(r) + \varphi(s).$$

Let $a \in R$ and $r \in {}_RR$. Then $\varphi(ar) = (ar)x = a(rx) = a\varphi(r)$. So φ is an R-homomorphism.

If $\varphi(r) = 0_M$ then $rx = 0_M$ so $r = 0$ (by the assumption above). Hence $\ker\varphi = \{0\}$, so φ is one-to-one (see Prop. 3.23 in the lectures). If $y \in Rx$, $y = rx$ for some $r \in R$, so $y = \varphi(r)$. Hence the image of φ is Rx, and φ is an R-isomorphism.

Page 260, Q6

Define a map φ from K' to L' as follows. If $k' \in K'$, it can be written uniquely in the form $l + l'$. Set $\varphi(k') = l'$. Then φ is well-defined since the decomposition $l + l'$ is unique.

If $k'_0, k'_1 \in K'$ then write $k'_0 = l_0 + l'_0$ and $k'_1 = l_1 + l'_1$. So $k'_0 + k'_1 = l_0 + l'_0 + l_1 + l'_1$ and has unique decomposition $k'_0 + k'_1 = (l_0 + l_1) + (l'_0 + l'_1)$ with $l_0 + l_1 \in L$ and $l'_0 + l'_1 \in L'$. So $\varphi(k'_0 + k'_1) = l'_0 + l'_1 = \varphi(k'_0) + \varphi(k'_1)$.

If $r \in R$, $rk'_0 = r(l_0 + l'_0) = rl_0 + rl'_0$ with $rl_0 \in L$ and $rl'_0 \in L'$, so $\varphi(rk'_0) = rl'_0 = r\varphi(k'_0)$. Hence φ is an R-homomorphism.

If $k' \in \ker\varphi$, then $k' = l + 0 \in L = K$, but $k' \in K'$ also, so $k' = 0$. Hence φ is one-to-one (see Prop. 3.23 in the lectures). Let $l' \in L'$. Then $l' = k + k'$ for some $k \in K$, $k' \in K'$. So $k' = -k + l'$. Note that $k \in K = L$ so this is the decomposition of k' as a sum of an element in L and an element in L'. Hence $\varphi(k') = l'$ and we see that φ is onto. Hence φ is an R-isomorphism as required.

Page 260, Q7

Let I be a left ideal of a ring R and let φ be an isomorphism from R/I to R. Let $a = \varphi(1 + I)$ and $b + I = \varphi^{-1}(1)$. Then $1 = \varphi(b + I) = b\varphi(1 + I) = ba$. And $1 + I = \varphi^{-1}(a) = a\varphi^{-1}(1) = a(b + I) = ab + I$, so $1 - ab \in I$. Then $(ab)^2 = abab = ab$ and $(1 - ab)^2 = 1 - ab - ab + ab = 1 - ab$, so ba and $1 - ab$ are idempotents. Since $1 - ab \in I$, $R(1 - ab) \subseteq I$. If $x \in I$, then $x + I = 0 + I$ so $0 = \varphi(x + I) = \varphi(x(1 + I)) = x\varphi(1 + I) = xa$. Then $x = x1 = x(1 - ab + ab) = x(1 - ab) + xab = x(1 - ab) \in R(1 - ab)$. Hence $I = R(1 - ab)$ and we can take e to be the idempotent $1 - ab$.

Page 268, Q1

Since $e \neq 0$, $Re \neq \{0\}$ since it contains the non-zero element $1e = e$. Let $re \in Re$ be an arbitrary element. We have $(1 - e)re = r(1 - e)e = r(e - e^2) = 0$. Since $e \neq 1$, $1 - e \neq 0$, and it follows that $\{re\}$ is not linearly independent. Hence no non-empty set is a basis for Re. Since $Re \neq 0$, the empty set is not a basis either. So Re does not have a basis, and hence is not a free module.

Page 268, Q3

Let R be a ring and M a free R-module with basis $x_i, i \in \Lambda$. Then every element of M is of the form $\sum_{i\in\Lambda} r_i x_i$, with $r_i \in R$ and finitely many non-zero terms. Hence $R = \sum_{i\in\Lambda} Rx_i$. Suppose that $\sum_{i\in\Lambda} r_i x_i = 0$, with $r_i \in R$ for all i and finitely many $r_i x_i \neq 0$. Let

$$\Lambda' = \{i \in \Lambda \,:\, r_i x_i \neq 0\},$$

a finite set. Then $\sum_{i\in\Lambda'} r_i x_i = 0$, so $r_i = 0$ for all $i \in \Lambda'$. Hence $r_i x_i = 0$ for all $i \in \Lambda$. By Proposition 3.13 from lectures, $R = \bigoplus_{i\in\Lambda} Rx_i$.

We remark for later use that each submodule Rx_i is isomorphic to ${}_RR$.

Page 268, Q6

Let I be an ideal of $\mathbb{Z}$, regarded as a (left) $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a PID, $I = (a)$ for some $a \in \mathbb{Z}$. If $a = 0$, then $I = \{0\}$ and is a free module. If $a \neq 0$, then every element of I is of the form ra, $r \in \mathbb{Z}$, so $\{a\}$ generates I. If $ra = 0$ then, since $a \neq 0$, $r = 0$, so $\{a\}$ is linearly independent. Hence $\{a\}$ is a basis of I and it is a free module in this case also.

Page 268, Q7

Let R be an integral domain and I a principal left ideal in R, regarded as a left R-module. If $I = \{0\}$, it is a free module. If $I \neq \{0\}$, let $a \in R$ be such that $I = (a)$. Note that we must have $a \neq 0$. Then every element of I is of the form ra, so $\{a\}$ is a generating set for I. If $ra = 0$ then, since $a \neq 0$, we have $r = 0$ (as R is an integral domain), so $\{a\}$ is also linearly independent. Hence I has a basis, $\{a\}$, so is a free module in this case also. Note that, since $\mathbb{Z}$ is a PID, the statement in Question 6 on page 268 is implied by the statement in Q7.

R. J. Marsh, 20/09/14.