Algebra III: Rings and Modules
Solutions for Problem Sheet 4, Autumn Term 2022-23

John Nicholson

1. Let R be a commutative ring and let $I \subseteq R$ be an ideal.

   (i) Prove that I is a free R-module if and only if I is principal and is generated by an element which is not a zero divisor. [Optional: Find a non-commutative ring where this is false.]

   (ii) Deduce that a commutative ring R is a principal ideal domain if and only if every ideal $I \subseteq R$ is free as an R-module.

   Solution: (i) Suppose $I = (x)$ and x is not a zero divisor. Let $f : R \to I$ be the map $r \mapsto r \cdot x$. This is a surjective R-module homomorphism. If $r \in \ker(f)$, then $r \cdot x = 0$ which implies that $r = 0$ since x is not a zero divisor. Hence $\ker(f) = \{0\}$ and so $R \cong I$ by the first isomorphism theorem.

   Now suppose I is a free R-module. Let $S \subseteq I$ be a basis. If $|S| \geq 2$, then let $m_1, m_2 \in S$. Since R is commutative, we have $m_1 m_2 - m_2 m_1 = 0$ which is a contradiction since S is linearly independent. Hence $|S| = 1$. Let $S = \{m\}$. Then $I = (m)$ is principal. Furthermore, m is not a zero divisor since, otherwise, S would not be linearly independent.

   (ii) If R is a principal ideal domain, then every ideal is of the form $I = (x)$. If $x = 0$, then $(x) = \{0\}$ is free of rank 0. If $x \neq 0$ then, since R is an integral domain, x is not a zero divisor. Hence (x) is free by part (i).

   Conversely, suppose R is a commutative ring such that every ideal $I \subseteq R$ is free as an R-module. By (i), all ideals are therefore principal.

2. Let R be a ring and let M be a free R-module. Give a proof or counterexample to each of the following statements:

   (i) Every spanning set for M over R contains a basis for M.

   (ii) Every linearly independent subset of M over R can be extended to a basis for M.

   Solution: (i) False. Let $R = M = \mathbb{Z}$. Then the only bases for M are ± 1, as every two-element subset of M is linearly dependent. So $\{2, 3\}$ is a spanning set that does not contain a basis.

   (ii) False. With R and M as above, $\{2\}$ is a linearly independent set that can not be extended to a basis.

3. Let R be a non-trivial commutative ring. Prove that R is a field if and only if every finitely generated R-module is free. [Optional: Prove this is also equivalent to every R-module being free. You will need to use the axiom of choice.]

Solution: ($\Rightarrow$) Proof 1: Let R be a field and let M be a finitely generated R-module. We claim that M has a basis. (Note that this is the same as proving that every finite-dimensional vector space has a basis. So we can use the same argument from linear algebra.)

Let n be the minimum size of a generating set for M. We first claim that, if $S \subseteq M$ is linearly independent, then $|S| \leq n$. If $|S| > n$, then let $\{v_1, \cdots, v_{n+1}\}$ be linearly independent. Suppose M is generated by $\{m_1, \cdots, m_n\}$. For each $1 \leq i \leq n+1$, we can write $v_i = \sum_{j=1}^{n} a_{ij} m_j$. Let $A = (a_{ij})$, which is an $n+1 \times n$ matrix over a field R. Consider the system of equations $A^T x = 0$ for $x \in R^n$. This is a system of $n+1$ equations in n variables and so there exists a non-zero solution $b \in R^n \setminus \{0\}$. Hence $\sum_{i=1}^{n+1} b_i v_i = \sum_{j=1}^{n} (A^T b)_j m_j = 0$, which is a contradiction.

Next we claim that, if $S \subseteq M$ is a linearly independent set which does not span M, then $S \subseteq \{v\}$ is linearly independent for any $v \in M$ not contained in the span on S. If not, let $S = \{v_1, \cdots, v_n\}$. Then there exists $a, a_i \in R$ such that $av + \sum_{i=1}^{n} a_i v_i$. Since S is linearly independent, we must have $a \neq 0$. Since R is a field, we then have $a \in R^\times$ and so $v = -a^{-1} \cdot \sum_{i=1}^{n} a_i v_i$ which contradicts the fact that v is not in the span of S.

If $M = \{0\}$, then it is free so assume $M \neq \{0\}$. Let $S_1 = \{v_1\}$ for any $v_1 \neq 0$. Then §$_1$ is linearly independent since $v_1 \neq 0$ and, since R is a field, R has no zero divisors. If S_1 spans M, then S_1 is a basis and so we are done. If not, we can apply the second claim to extend S_1 to a linearly independent set S_2 with $|S_2| = 2$. This process will eventually terminate in a basis after n steps since every linearly independent set has size at most n.

Proof 2: Use the fact that fields are PIDs and then apply the classification of finitely generated modules over a PID. We need only note that $R/(d) \cong \{0\}$ for all $d \neq 0$ since $d \in R^\times$.

($\Leftarrow$) Suppose R is not a field. Then there exists a non-unit $a \in R \setminus \{0\}$. Consider the quotient R-module $M := R/(a)$. We claim that M is not free. Note that, for all $m \in M$, we have $a \cdot m = 0$. If $f : M \to R^{(S)}$ is an isomorphism, then $a \cdot m = 0$ for all $m \in R^{(S)}$.

We claim that $r \cdot m = 0$ for all $m \in R^{(S)}$ implies $r = 0$. This gives a contradiction and so would complete the proof. This is true when $S = \emptyset$ so assume $S \neq \emptyset$. Let $s \in S$ and let $m = (x_i)_{i \in S}$ be any element with $x_s = 1$. If $r \cdot m = 0$, then restricting to the sth coordinate gives that $r = r \cdot 1 = 0 \in R$ as required.

We can phrase this proof another way. Define the annihilator of an R-module M to be $\mathrm{Ann}_R(M) = \{r \in R : r \cdot m = 0 \text{ for all } m \in M\}$. If M is free, then $\mathrm{Ann}_R(M) = \{0\}$. However, we have $\mathrm{Ann}_R(R/(a)) = (a) \neq \{0\}$. Hence $R/(a)$ is not free.

4. Let R be a ring, let $S \subseteq R$ be a multiplicative submonoid and let $N \leq M$ be R-modules. Show that there is an isomorphism of $S^{-1}R$-modules $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.

Solution: Let $f : S^{-1}M \to S^{-1}(M/N)$ be the map sending $(m, s) \in S^{-1}M$ to $(m + N, s) \in S^{-1}(M/N)$. We can check that this is an $S^{-1}R$-module homomorphism. It is clearly surjective.

Since $N \leq M$, we have that $S^{-1}N \leq S^{-1}M$. By the first isomorphism theorem for modules, it now suffices to prove that $\ker(f) = S^{-1}N$. It is clear that $S^{-1}N \subseteq \ker(f)$. Now suppose $(m, s) \in \ker(f)$. Then $(m + N, s) \sim (0 + N, 1)$ in $S^{-1}(M/N)$, i.e. there exists $t \in S$ such that $t \cdot (m + N) = 0$ and so $t \cdot m \in N$. This implies that $(m, s) = (t \cdot m, t \cdot s) \in S^{-1}N$.

5. Let R be a ring, M a right R-module and N a left R-module. The tensor product $M \otimes_R N$ is defined to be the abelian group

$$M \otimes_R N = \mathbb{Z}[M \times N] \,/\, ((va, w) - (v, aw),\ (v, w) + (v', w) - (v + v', w),\\ (v, w) + (v, w') - (v, w + w') \mid a \in R, v, v' \in M, w, w' \in N).$$

For left R-modules M and N, let $\mathrm{Hom}_R(M, N)$ denote the set of left R-module homomorphisms $f : M \to N$, which is an abelian group under pointwise addition.

From now on, let R be a commutative ring.

(i) Let M, N be left R-modules (which we can also view as right modules since R is commutative). Show that $M \otimes_R N$ is an R-module with action $a(v \otimes_R w) = av \otimes_R w$ for $a \in R$, $v \in M$ and $w \in N$.

(ii) Let M, N be left R-modules. Show that $\mathrm{Hom}_R(M, N)$ is an R-module, with action: for $a \in R$ and $\varphi : M \to N$, define $a \cdot \varphi : M \to N$ by $(a \cdot \varphi)(b) = a\varphi(b)$ for $b \in M$.

(iii) Show that, if M, N, and T are all R-modules, then $\mathrm{Hom}_R(M \otimes_R N, T)$ is identified with the set of *R-bilinear maps* $\varphi : M \times N \to T$, which means functions satisfying $\varphi(au, v) = a\varphi(u, v) = \varphi(u, av)$ and $\varphi(u + u', v) = \varphi(u, v) + \varphi(u', v)$ as well as $\varphi(u, v + v') + \varphi(u, v) + \varphi(u, v')$. Use this to give an alternative definition of tensor product.

Solution: (Sketch) (i) $M \otimes_R N$ is already an abelian group so we need only show that the map $\varphi : R \to \mathrm{Aut}(M \otimes_R N)$ defined by this action is a ring homomorphism. This follows directly by analysing the relations we quotiented by, e.g. $\varphi(a+b)(v \otimes_R w) = (a+b)v \otimes_R w = av \otimes_R w + bv \otimes_R w = \varphi(a)(v \otimes_R w) + \varphi(b)(v \otimes_R w)$ and so $\varphi(a + b) = \varphi(a) + \varphi(b)$.

(ii) $(a_1a_2 \cdot \varphi)(b) = a_1a_2 \cdot \varphi(b)$, so $a_1a_2 \cdot \varphi = a_1 \cdot (a_2 \cdot \varphi)$; similarly $1 \cdot \varphi = \varphi$. We need to verify that the action is well-defined, i.e., that $a \cdot \varphi$ is still a homomorphism: this is where we use R is commutative: $a_1 \cdot \varphi(a_2 \cdot b) = a_1a_2 \cdot \varphi(b) = a_2 \cdot \varphi(a_1 \cdot b)$.

(iii) This is based on the relations in the definition of tensor product. Namely $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[M \times N], T)$ equals the set of all maps (not necessarily linear), $\varphi : M \times N \to T$. Now to send the relations of $M \otimes_R N$ to zero means that $\varphi(u, av) = \varphi(au, v)$. Finally to be an R-linear map means that $\varphi(au, v) = a\varphi(u, v)$. Put together yields the statement.

We can define $M \otimes_R N$ to be the R-module for which $\mathrm{Hom}_R(M \otimes_R N, T)$ coincides with the set of R-bilinear maps. Existence is verified by the above argument. We can also check uniqueness.

6. Let R be a ring and let M be a left R-module. We say that R is a *ring with involution* (or a $*$-*ring*) if R is equipped with a map $* : R \to R$ such that $(x+y)^* = x^* + y^*$, $(xy)^* = y^*x^*$, $1^* = 1$ and $(x^*)^* = x$ for all $x, y \in R$, i.e. $*$ is an anti-homomorphism and an involution.

   (i) Show that $M^* = \mathrm{Hom}_R(M, R)$ is a right R-module with action: for $a \in R$ and $\varphi \in \mathrm{Hom}_R(M, R)$, define $\varphi \cdot a : M \to R$ by $(\varphi \cdot a)(b) = \varphi(b) \cdot_R a$ for $b \in M$. This is known as the *dual module*.

   (ii) Let R be a commutative ring. Show that R is a ring with involution. For a group G, show that $R[G]$ is a ring with involution.

   (iii) Let R be a ring with involution. Show that any right R-module M can be viewed as a left R-module with action: for $a \in R$ and $m \in M$, define $x \cdot m = m \cdot_M x^*$. Use this to define a left R-module structure on $\mathrm{Hom}_R(M, R)$. For left R-modules M and N, define a (sensible) left R-module structure on the tensor product of abelian groups $M \otimes_{\mathbb{Z}} N$. [Optional: How do these R-module structures compare to those defined in (5) in the commutative case?]

   Solution: (Sketch) (i) By (5) we know that $\mathrm{Hom}_R(M, R)$, i.e. the set of left R-module homomorphisms $f : M \to R$, is an abelian group. We can check that $\varphi \cdot a$ denotes a right R-module action directly.

   (ii) If R is commutative, we can just take $* = \mathrm{id}_R$. For the group ring $R[G]$, we can take $* : \sum_{i=1}^n a_i g_i \mapsto \sum_{i=1}^n a_i g_i^{-1}$.

   (iii) We define a left R-module structure on $\mathrm{Hom}_R(M, R)$ by using the right modules structure defined in part (i) and then using the involution to convert this to a left module structure.

   For $r \in R$ and $m \otimes n \in M \otimes_{\mathbb{Z}} N$, we can define $r \cdot (m \otimes n) := (rm \otimes rn)$.

7. Let R be a ring and let M be an R-module and let $N \leq M$ be a submodule. Show that M is Noetherian if and only if N and M/N are Noetherian.

   Solution: Let J be a submodule of M. Then $J \cap N$ is a submodule of N, hence finitely generated. Let $j_1, \ldots, j_n$ generate $J \cap N$. Let $\overline{J}$ denote the image of J in M/N; this is a submodule of M/N and thus finitely generated. Let $\overline{j}_{n+1}, \ldots, \overline{j}_m$ generate $\overline{J}$, and choose elements $j_{n+1}, \ldots, j_m$ of J mapping to $\overline{j}_{n+1}, \ldots, \overline{j}_m$, respectively.

   We now show that $j_1, \ldots, j_m$ is a generating set for J, proving the claim. Given any $j \in J$, let $\overline{j}$ be its image in M/N. Then we can write $\overline{j}$ as a sum $r_{n+1}\overline{j}_{n+1} + \cdots + r_m\overline{j}_m$. Let $j' = j - r_{n+1}j_{n+1} - r_{n+2}j_{n+2} + \cdots + r_m j_m$. Then the image of j' in M/N is zero, so j' lies in $J \cap N$. We can thus write $j'asr_1j_1 + \cdots + r_nj_n$. We then have

$$j = r_1j_1 + \cdots + r_nJ_n + r_{n+1}j_{n+1} + \cdots + r_mj_m,$$

   proving the claim.

8. Let a, b be nonzero positive integers. Find the Smith normal form of the following matrices in their respective rings:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbb{Q}), \quad \begin{pmatrix} X^2 - 5X + 6 & X - 3 \\ (X-2)^3 & X^2 - 5X + 6 \end{pmatrix} \in M_2(\mathbb{Q}[X]).$$

Solution: We perform the Euclidean algorithm on the first column, using row operations to subtract multiples of row 2 from row 1 until the norm of the entry in row 2 is strictly less than that in row 1, then interchanging rows 1 and 2. At the end of this process the greatest common divisor of a and b is in the upper left, and the lower left entry is zero. The right-hand column contains linear combinations of a and b, so its entries are both divisible by (a, b). We can thus subtract a multiple of the first column from the second to zero out the upper right entry. The matrix is now in Smith normal form, and none of the operations we have done have affected the determinant, so the lower left entry must be $\frac{a^2+b^2}{(a,b)}$. The Smith normal form is thus:

$$\begin{pmatrix} (a,b) & 0 \\ 0 & \frac{a^2+b^2}{(a,b)} \end{pmatrix}$$

A similar strategy works for the second matrix since $\mathbb{Q}[X]$ is a Euclidean domain. The Smith normal form is:

$$\begin{pmatrix} 1 & 0 \\ 0 & -(t-2)^2(t-3) \end{pmatrix}$$

9. Let G be the abelian group given by generators a, b, c and the relations $6a + 10b = 0$, $6a + 15c = 0$, $10b + 15c = 0$ (i.e. G is the free abelian group generated by a, b, c quotiented by the subgroup $(6a + 10b, 6a + 15c, 10b + 15c)$). Determine the structure of G as a direct sum of cyclic groups.

Solution: We have that $G \cong \mathbb{Z}^3/N$ where $N = \mathbb{Z}\cdot(16, 10, 0)+\mathbb{Z}\cdot(6, 0, 15)+\mathbb{Z}\cdot(0, 10, 15) \subseteq \mathbb{Z}^3$. So $G \cong \operatorname{coker}(\varphi_A)$ where

$$A = \begin{pmatrix} 6 & 6 & 0 \\ 10 & 0 & 10 \\ 0 & 15 & 15 \end{pmatrix}.$$

We can use elementary row and column operations to put A is Smith normal form, and we obtain:

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 30 & 0 \\ 0 & 0 & 60 \end{pmatrix}.$$

Since A and B differ by row and column operations, they are equivalent and so $G \cong \operatorname{coker}(\varphi_A) \cong \operatorname{coker}(\varphi_B)$. Furthermore, we have

$$\operatorname{coker}(\varphi_B) \cong \mathbb{Z}/1 \oplus \mathbb{Z}/30 \oplus \mathbb{Z}/60 \cong \mathbb{Z}/30 \oplus \mathbb{Z}/60.$$

Hence $G \cong \mathbb{Z}/30 \oplus \mathbb{Z}/60$.

10. A ring R has the *invariant basis number* property (IBN) if, for all positive integers m, n, $R^n \cong R^m$ as R-modules implies $m = n$.

    (i) For an ideal $I \subseteq R$ and an R-module M, we define an R-submodule $IM = \{am \in M : a \in I, m \in M\} \leq M$. Prove that M/IM is an R/I-module in a natural way.

    (ii) Prove that non-zero commutative rings have IBN. You may assume that every non-zero commutative ring has a maximal ideal. [This is equivalent to the axiom of choice.]

    (iii) Let S be a ring and M a free S-module with basis $\{x_i \mid i \geq 1\}$. Let $R = \mathrm{End}_S(M)$. Prove that R does not have IBN. [Hint: Note that $M \cong M_{\text{even}} \oplus M_{\text{odd}}$ where M_{even} and M_{odd} are the submodules generated by x_i for i even and odd respectively. Use this to show that $R \cong R^2$ as R-modules.]

    Solution: (i) Since $IM \leq M$ is an R-submodule, the quotient M/IM is an R-module. Suppose this is defined by a map $\varphi : R \to \mathrm{Aut}(M/IM)$.

    If $b \in I$, then its action on M/IM is

    $$b(m + IM) = bm + IM = IM.$$

    That is, $I \subseteq \ker(\varphi)$. Hence φ naturally descends to a map $\varphi' : R/I \to \mathrm{Aut}(M/IM)$ which gives M/IM the structure of an R/I-module. The action is given by

    $$(r + I) \cdot (m + IM) = r \cdot m + IM.$$

    (ii) Let I be a maximal ideal of R. Suppose we have $R^n \cong R^m$. Then we must have $R^n/IR^n \cong R^m/IR^m$ as R/I modules. By constructing an explicit isomorphism, we can then show that $R^n/IR^n \cong (R/I)^n$ and similarly for m. Since R/I is a field, the result follows by linear algebra (and, in particular, the proof of (3)).

    (iii) We have $M = S^{(\mathbb{N})} \cong M_{\text{even}} \oplus M_{\text{odd}}$ where $M_{\text{even}} = S^{(2\mathbb{N})}$ and $M_{\text{odd}} = S^{(2\mathbb{N}-1)}$. Since there are bijections $\mathbb{N} \cong 2\mathbb{N} \cong 2\mathbb{N} - 1$, we have that $M \cong M_{\text{even}} \cong M_{\text{odd}}$ as S-modules. Let $R = \mathrm{End}_S(M)$. We will define a map $\Psi : R^2 \to R$. Let $f_1, f_2 \in R$. Then $f_1, f_2 : M \to M$ are S-module homomorphisms. Given this, and the identifications $\varphi_1 : M \to M_{\text{even}}$ and $\varphi_2 : M \to M_{\text{odd}}$, we obtain an S-module homomorphism:

    $$\Psi(f_1, f_2) = (\varphi_1 \circ f_1, \varphi_2 \circ f_2) : M \to M_{\text{even}} \oplus M_{\text{odd}}.$$

    We can then check that Ψ is a bijective R-module homomorphism.

+11. Let G be a finite group, let $N = \sum_{g \in G} g \in \mathbb{Z}[G]$ and let $r \in \mathbb{Z}$ be an integer with $(r, |G|) = 1$

    (i) Show that the ideal $(N, r) \subseteq \mathbb{Z}[G]$ is projective as a $\mathbb{Z}[G]$-module.

    (ii) Let $G = C_n$ be a finite cyclic group. Show that (N, r) is free as a $\mathbb{Z}[G]$-module.

    (iii) Let $G = Q_8$ be the quaternion group of order 8. Show that $(N, 3)$ is not free as a $\mathbb{Z}[G]$-module. Is it stably free as a $\mathbb{Z}[G]$-module?

    Solution not provided. You may continue to work on this throughout the term and contact me to discuss ideas and/or hand in a solution. Remember that this problem is optional and may be significantly more challenging than the other problems.