

Solutions to Chapter 1

Solution to Exercise 1.27. Let V be an $F[x, y]$ -module. As in the proof of Proposition 1.24, this implies in particular that V is a vector space over F . Moreover, we have a linear transformation $T : V \rightarrow V$ defined by $T(v) = xv$ and another linear transformation $U : V \rightarrow V$ defined by $U(v) = yv$. The crucial thing is that these two linear transformations commute, because $xy = yx$ in $F[x, y]$, so

$$T(U(v)) = x(yv) = (xy)v = (yx)v = y(xv) = U(T(v))$$

for all $v \in V$. Having specified how x and y act, the action of any other polynomial in x and y is determined by the module axioms. It is also easy to see that for any F -vector space V with commuting linear transformations T and U , we can define an $F[x, y]$ -module structure on V by letting $p(x, y)$ act as the linear transformation $p(T, U)$. So the answer is that an $F[x, y]$ -module is a vector space over F with two specified linear transformations T and U such that $TU = UT$.

Solution to Exercise 1.28. Whether there exists another R -module structure on R depends on what R is. If $R = \mathbb{Z}$, Proposition 1.21 shows that there is only one R -module structure on R (or on any abelian group). On the other hand, if $R = F[x]$, then Proposition 1.24 shows that there are as many different R -module structures on R as there are linear transformations of the (infinite-dimensional) vector space $F[x]$. Another noteworthy example is $R = \mathbb{C}$, where we have a second \mathbb{C} -module structure on \mathbb{C} given by $f(x, y) = \bar{x}y$, where the bar denotes complex conjugate.

Various other constructions that may have occurred to you don't work: setting $f(x, y) = 0$ is no good because of the axiom that $f(1, y) = y$ for

all y ; setting $f(x, y) = x^2y$ is no good because it fails the axiom that $f(x_1 + x_2, y) = f(x_1, y) + f(x_2, y)$. If R is non-commutative, it is tempting to think that right multiplication would work just as well as left, so that we should try $f(x, y) = yx$; but this fails the axiom that $f(xy, z) = f(x, f(y, z))$, because the left-hand side is zxy whereas the right-hand side is zyx .

Solution to Exercise 1.55.

- (i) Since \mathbb{R} is a field, the question is just asking whether \mathbb{C} is a finite-dimensional vector space over \mathbb{R} . Of course, it is – in fact two-dimensional, with $\{1, i\}$ being the best-known basis.
- (ii) Since \mathbb{Q} is a field, the question is whether \mathbb{R} is a finite-dimensional vector space over \mathbb{Q} . As you learnt in MATH3962, it is infinite-dimensional. One way to prove this is to show that there exists some transcendental element in \mathbb{R} , because any finite-dimensional field extension is algebraic. An alternative argument is to note that \mathbb{R} is uncountable, whereas any finite-dimensional vector space over \mathbb{Q} is countable.
- (iii) We prove that \mathbb{Q} is not a finitely-generated \mathbb{Z} -module by contradiction. Suppose that the \mathbb{Z} -module \mathbb{Q} had a finite generating set, say $\{\frac{r_1}{s_1}, \dots, \frac{r_k}{s_k}\}$ where $r_i, s_i \in \mathbb{Z}$, $s_i > 0$. This would say that any rational number could be written as an integer linear combination of these ones, i.e. as

$$a_1 \frac{r_1}{s_1} + \dots + a_k \frac{r_k}{s_k} = \frac{a_1 r_1 s_2 \dots s_k + \dots + a_k s_1 \dots s_{k-1} r_k}{s_1 \dots s_k}$$

for some integers a_1, \dots, a_k . But this would mean that every rational number can be given the denominator $s_1 \dots s_k$, which is clearly false. If you think about it, this argument shows that there is no subring of \mathbb{Q} which is finitely-generated as a \mathbb{Z} -module except \mathbb{Z} itself.

Solution to Exercise 1.56.

- (i) The inclusion which is true is that $N + (K \cap L) \subseteq (N + K) \cap (N + L)$, which we can prove as follows. Since $K \cap L \subseteq K$, we have $N + (K \cap L) \subseteq$

$N + K$. Similarly, $N + (K \cap L) \subseteq N + L$. Hence $N + (K \cap L) \subseteq (N + K) \cap (N + L)$.

For a counter-example for the reverse inclusion, take N, K, L to be three different one-dimensional subspaces in \mathbb{R}^2 . Then $K \cap L = \{0\}$, so the left-hand side is N , whereas $N + K$ and $N + L$ are both all of \mathbb{R}^2 , so the right-hand side is \mathbb{R}^2 .

By contrast, notice that if M is the \mathbb{Z} -module \mathbb{Z} , then both inclusions hold. If N, K, L are the ideals generated by the positive integers a, b, c , then $N + (K \cap L)$ and $(N + K) \cap (N + L)$ are the ideals generated by

$$\gcd(a, \text{lcm}(b, c)) \text{ and } \text{lcm}(\gcd(a, b), \gcd(a, c)),$$

which are indeed equal.

- (ii) The inclusion which is true is that $N \cap (K + L) \supseteq (N \cap K) + (N \cap L)$, which we can prove as follows. Since $N \cap K \subseteq N$ and $N \cap K \subseteq K \subseteq K + L$, we have $N \cap K \subseteq N \cap (K + L)$. Similarly $N \cap L \subseteq N \cap (K + L)$. Since $N \cap (K + L)$ is closed under addition, it follows that $(N \cap K) + (N \cap L) \subseteq N \cap (K + L)$.

We can use the same counter-example for the reverse inclusion as in the previous part, where N, K, L are three different one-dimensional subspaces in \mathbb{R}^2 . We have $K + L = \mathbb{R}^2$, so the left-hand side is N , whereas $N \cap K = N \cap L = \{0\}$, so the right-hand side is $\{0\}$. (As in the previous part, both inclusions hold for ideals of \mathbb{Z} .)

Solution to Exercise 1.57.

- (i) Since \mathbb{Z}^2 is not the zero \mathbb{Z} -module, there cannot be a generating set with 0 elements! So all we need to show is that no single element $(a, b) \in \mathbb{Z}^2$ generates \mathbb{Z}^2 as a \mathbb{Z} -module. Suppose it did; then we would have $(1, 0) = m(a, b)$ for some $m \in \mathbb{Z}$, which would force $a = \pm 1$ and $b = 0$, but also $(0, 1) = m'(a, b)$ for some $m' \in \mathbb{Z}$, which would force $a = 0$ and $b = \pm 1$, a contradiction.
- (ii) If (a, b) and (c, d) generate \mathbb{Z}^2 as a \mathbb{Z} -module, then $(1, 0) = p(a, b) + q(c, d)$ and $(0, 1) = r(a, b) + s(c, d)$ for some $p, q, r, s \in \mathbb{Z}$. Conversely, if such p, q, r, s exist, then $(1, 0)$ and $(0, 1)$ both belong to the submodule generated by (a, b) and (c, d) , and hence so does $m(1, 0) + n(0, 1) =$

(m, n) for all $m, n \in \mathbb{Z}$. So the condition is exactly that there exist such integers p, q, r, s . In matrix form, the two equations can be rewritten

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix},$$

so the condition is equivalent to saying that $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ is invertible **and** its inverse has integer entries. If this is the case, then by taking determinants we see that $1 = (ad - bc)(ps - qr)$, which forces $ad - bc = \pm 1$. Conversely, if $ad - bc = \pm 1$ then $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$ has integer entries. So the upshot is that (a, b) and (c, d) generate \mathbb{Z}^2 as a \mathbb{Z} -module if and only if $ad - bc = \pm 1$.

- (iii) The argument of the previous part generalizes directly: n elements of \mathbb{Z}^n form a generating set if and only if the $n \times n$ matrix of which they are the columns has determinant ± 1 . We then see that part (i) also generalizes, i.e. \mathbb{Z}^n has no generating set with fewer than n elements: if it did, then we could enlarge to a generating set with n elements by including $(0, \dots, 0)$ a certain number of times, but this would result in a matrix with determinant 0. We will go through this proof in more detail in the context of a general PID in Theorem 2.43.

Solution to Exercise 1.58. When we regard \mathbb{C}^n as a $\mathbb{C}[x]$ -module via an $n \times n$ matrix A , a submodule is exactly a vector subspace $V \subseteq \mathbb{C}^n$ which is preserved by the action of A , i.e. has the property that $Av \in V$ for all $v \in V$. Obviously the zero subspace and the whole space \mathbb{C}^n are preserved, so the question is really about one-dimensional, two-dimensional, \dots , and $(n - 1)$ -dimensional subspaces (and for the parts where $n = 2$, this means one-dimensional subspaces only). Any one-dimensional subspace is of the form $\mathbb{C}v$ for some $v \in \mathbb{C}^n$, and such a subspace is preserved by the action of A if and only if $Av = \lambda v$ for some $\lambda \in \mathbb{C}$, i.e. v is an eigenvector of A .

A generating set for \mathbb{C}^n as a $\mathbb{C}[x]$ -module is a subset $\{v_i\}$ such that the collection $\{v_i, Av_i, A^2v_i, \dots\}$ spans \mathbb{C}^n over \mathbb{C} . Obviously the standard basis $\{e_1, e_2, \dots, e_n\}$ of \mathbb{C}^n forms a generating set, but there may well be other generating sets with fewer elements.

- (i) Here A is a scalar matrix, so $Av = 2v$ for all $v \in \mathbb{C}^2$. Any one-dimensional subspace of \mathbb{C}^2 is preserved under the operation of scalar

multiplication by 2 (which is the same thing as saying that every nonzero vector in \mathbb{C}^2 is an eigenvector for this matrix). So all the subspaces of \mathbb{C}^2 are submodules in this case. The submodule generated by a single element v is obviously just $\mathbb{C}v$, so there is no generating set with a single element (i.e. the module is not cyclic), and the generating set $\{e_1, e_2\}$ is as small as possible.

- (ii) Here the only eigenvectors of A (up to scalar) are e_1 and e_2 , so the only one-dimensional subspaces which are submodules are $\mathbb{C}e_1$ (the 1-eigenspace) and $\mathbb{C}e_2$ (the 2-eigenspace). If you take any element not in either of these one-dimensional submodules, the submodule it generates must be the whole of \mathbb{C}^2 . So in this case \mathbb{C}^2 is a cyclic $\mathbb{C}[x]$ -module, and an example of a generating set is $\{e_1 + e_2\}$. (Explicitly, $A(e_1 + e_2) = e_1 + 2e_2$, and $\{e_1 + e_2, e_1 + 2e_2\}$ spans \mathbb{C}^2 over \mathbb{C} .)
- (iii) Here the only eigenvector of A (up to scalar) is e_2 , so the only one-dimensional submodule is $\mathbb{C}e_2$. As in the previous part, any element not in this submodule must generate the whole module: for example, $\{e_1\}$ is a generating set.
- (iv) As in the previous parts, the one-dimensional submodules are the eigenspaces of A , viz. $\mathbb{C}e_1$ (the 1-eigenspace), $\mathbb{C}e_2$ (the 2-eigenspace) and $\mathbb{C}e_3$ (the 3-eigenspace). The sums of two of these eigenspaces, viz. $\mathbb{C}\{e_1, e_2\}$, $\mathbb{C}\{e_1, e_3\}$ and $\mathbb{C}\{e_2, e_3\}$, are clearly two-dimensional submodules, and it turns out that these are the only ones. One way to prove this, which also addresses the generating set question, is to start with a general element $v = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \in \mathbb{C}^3$ and ask when it generates an $\mathbb{C}[x]$ -submodule which is less than three-dimensional. We have $Av = \begin{pmatrix} a_1 \\ 2a_2 \\ 3a_3 \end{pmatrix}$ and $A^2v = \begin{pmatrix} a_1 \\ 4a_2 \\ 9a_3 \end{pmatrix}$, and the only way these three vectors can fail to span all of \mathbb{C}^3 is if they are linearly dependent, which happens exactly when

$$0 = \det \begin{pmatrix} a_1 & a_1 & a_1 \\ a_2 & 2a_2 & 4a_2 \\ a_3 & 3a_3 & 9a_3 \end{pmatrix} = a_1 a_2 a_3 \det \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} = 2a_1 a_2 a_3.$$

The three possibilities $a_1 = 0$, $a_2 = 0$, or $a_3 = 0$ are all covered by the three two-dimensional submodules mentioned above. This also shows that if we start with $a_1, a_2, a_3 \neq 0$, we will generate the whole of \mathbb{C}^3 . So \mathbb{C}^3 is a cyclic $\mathbb{C}[x]$ -module in this case, with $\left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$ being one example of a generating set.

(v) Again considering eigenvectors, we see that the one-dimensional submodules are $\mathbb{C}e_3$ (the (-1) -eigenspace) and $\mathbb{C}(a_1e_1 + a_2e_2)$ for a_1, a_2 not both zero (a line in the two-dimensional 1-eigenspace). Then any sum of two of these is a two-dimensional submodule: such a sum would be either the 1-eigenspace $\mathbb{C}\{e_1, e_2\}$ or a subspace of the form $\mathbb{C}\{a_1e_1 + a_2e_2, e_3\}$ for a_1, a_2 not both zero. We claim that these are the only two-dimensional subspaces which are submodules. Suppose we take a nonzero vector $v = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$ which is not an eigenvector for A , i.e. $a_3 \neq 0$ and also a_1 and a_2 are not both zero. Then $Av = \begin{pmatrix} a_1 \\ a_2 \\ -a_3 \end{pmatrix}$ is linearly independent from v , and their span is clearly the two-dimensional submodule $\mathbb{C}\{a_1e_1 + a_2e_2, e_3\}$. This shows two things. Firstly, it shows that any submodule which is not an eigenspace must contain a subspace of the form $\mathbb{C}\{a_1e_1 + a_2e_2, e_3\}$ for a_1, a_2 not both zero, and this verifies our claim. Secondly, it shows that \mathbb{C}^3 is not a cyclic $\mathbb{C}[x]$ -module in this case, since any element v generates either a one-dimensional submodule (if v is an eigenvector for A) or a two-dimensional submodule (if v is not an eigenvector for A). An example of a two-element generating set is $\left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\}$.

(vi) Here the only one-dimensional submodule is the 1-eigenspace $\mathbb{C}e_3$. One obvious two-dimensional submodule is $\mathbb{C}\{e_2, e_3\}$. To show there are no others, consider any $v = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$ which is not contained in $\mathbb{C}\{e_2, e_3\}$; in other words, $a_1 \neq 0$. Then $Av - v = \begin{pmatrix} 0 \\ a_1 \\ a_2 \end{pmatrix}$ and $A(Av - v) - (Av - v) = \begin{pmatrix} 0 \\ 0 \\ a_1 \end{pmatrix}$ also lie in the submodule generated by v . Since

$$\det \begin{pmatrix} a_1 & 0 & 0 \\ a_2 & a_1 & 0 \\ a_3 & a_2 & a_1 \end{pmatrix} = a_1^3 \neq 0,$$

these three vectors span \mathbb{C}^3 . So v cannot be contained in a two-dimensional submodule, which demonstrates that $\mathbb{C}\{e_2, e_3\}$ is the only one. Moreover, \mathbb{C}^3 is again a cyclic $\mathbb{C}[x]$ -module, and $\{e_1\}$ is one example of a generating set.

Solution to Exercise 1.59. Neither the statement nor its converse is true in general. (What makes them tempting is that they are true for finite-dimensional vector spaces, just because any two vector spaces of the same

dimension are isomorphic.) For counter-examples, take $R = \mathbb{Z}$. Then \mathbb{Z} and $2\mathbb{Z}$ are submodules of the \mathbb{Z} -module \mathbb{Z} (i.e. ideals of \mathbb{Z}), and they are isomorphic as \mathbb{Z} -modules via the map $\theta : \mathbb{Z} \rightarrow 2\mathbb{Z} : m \mapsto 2m$; however, $\mathbb{Z}/\mathbb{Z} \cong \{0\}$ is obviously not isomorphic to $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$.

One counter-example to the converse is provided by the infinitely-generated \mathbb{Z} -module $M = \{(a_1, a_2, a_3, \dots)\}$ of ∞ -tuples of integers. Clearly $\theta : M \rightarrow M : (a_1, a_2, a_3, \dots) \mapsto (a_2, a_3, a_4, \dots)$ is a surjective \mathbb{Z} -module homomorphism, so by the First Isomorphism Theorem we have $M/\ker(\theta) \cong M \cong M/\{0\}$, although $\ker(\theta) = \{(a_1, 0, 0, \dots)\}$ is obviously not isomorphic to $\{0\}$. There are also counter-examples in finitely-generated \mathbb{Z} -modules: for instance, take $M = \mathbb{Z}_4 \oplus \mathbb{Z}_2$, $N_1 = \{(0, 0), (0, 1), (2, 0), (2, 1)\}$ and $N_2 = \{(0, 0), (1, 0), (2, 0), (3, 0)\}$. Then $M/N_1 \cong \mathbb{Z}_2 \cong M/N_2$, although N_1 and N_2 are not isomorphic as \mathbb{Z} -modules (in N_1 every element is its own negative, which is not the case in N_2).

Solution to Exercise 1.60.

- (i) It is true that if M is finitely-generated, then M/N is: if $\{x_1, \dots, x_k\}$ generates M , then any element of M/N can be written in the form $(r_1x_1 + \dots + r_kx_k) + N$ for some $r_1, \dots, r_k \in R$, which is to say that $\{x_1 + N, \dots, x_k + N\}$ generates M/N .

However, it is not true that a submodule of a finitely-generated module must be finitely-generated. To find a counter-example, it is enough to find a ring R which possesses a non-finitely-generated ideal. One such is $F[x_1, x_2, \dots]$, the ring of polynomials in countably many variables over a field F : let N be the ideal generated by x_1, x_2, \dots . Suppose for a contradiction that N were generated by finitely many polynomials, p_1, p_2, \dots, p_k say. Since each polynomial involves only finitely many of the variables, the whole collection of p_i 's involves only x_1, x_2, \dots, x_s where s is some sufficiently large number. So if we evaluate at the point $x_1 = x_2 = \dots = x_s = 0$, $x_{s+1} = x_{s+2} = \dots = 1$, all the p_i 's become zero. This contradicts the assumption that $x_{s+1} \in N$ is an $F[x_1, x_2, \dots]$ -linear combination of the p_i 's.

Note that any subspace of a finite-dimensional vector space is finite-dimensional, so we could not have constructed such a counter-example over a field; we will see in Exercise 2.27 that there are no counter-examples over any PID. (It is also easy to see that over a finite ring such

as \mathbb{Z}_n , a module is finitely-generated if and only if it has finitely many elements; so there are no counter-examples over finite rings either.)

- (ii) Suppose that $\{x_1, \dots, x_k\}$ generates N and $\{y_1 + N, \dots, y_\ell + N\}$ generates M/N . For any $m \in M$, we can write $m + N$ as an R -linear combination $r_1(y_1 + N) + \dots + r_\ell(y_\ell + N)$ for some $r_1, \dots, r_\ell \in R$. This means that

$$m - r_1y_1 - \dots - r_\ell y_\ell \in N,$$

which implies that we can write $m - r_1y_1 - \dots - r_\ell y_\ell$ as an R -linear combination $s_1x_1 + \dots + s_kx_k$ for some $s_1, \dots, s_k \in R$. So

$$m = r_1y_1 + \dots + r_\ell y_\ell + s_1x_1 + \dots + s_kx_k,$$

and we have shown that $\{x_1, \dots, x_k, y_1, \dots, y_\ell\}$ generates M .

Solution to Exercise 1.61. Part of Assignment 1.

Solution to Exercise 1.79. If $\{r\}$ is a generating set, then $1 = sr$ for some $s \in R$; the converse is also true, because if $1 = sr$ then $t = (ts)r$ for all $t \in R$. So the condition for $\{r\}$ to be a generating set is that r has a left inverse. The condition for $\{r\}$ to be linearly independent is that $sr = 0$ implies $s = 0$; that is, r is neither zero nor a right zero divisor. Since R is not the zero ring, 0 is not invertible; thus the conjunction of the two conditions is that “ r is left-invertible and not a right zero divisor”. If R is commutative, then invertibility implies that r is not a zero divisor, since $sr = 0 \Rightarrow s = srr^{-1} = 0$. So in this case the condition is just that “ r is invertible”. But in non-commutative rings there can be elements satisfying the condition which are not right-invertible.

Solution to Exercise 1.80. \mathbb{Q} is a torsion-free \mathbb{Z} -module because if $n\frac{r}{s} = 0$, then either $n = 0$ or $\frac{r}{s} = 0$ (because \mathbb{Q} is an integral domain!). However, \mathbb{Q} cannot have a basis over \mathbb{Z} , because the basis would obviously have to have at least two elements (in fact it would have to be infinite, by Exercise 1.55(iii)), and any two nonzero elements $\frac{r_1}{s_1}, \frac{r_2}{s_2}$ of \mathbb{Q} are linearly dependent over \mathbb{Z} :

$$(r_2s_1)\frac{r_1}{s_1} - (r_1s_2)\frac{r_2}{s_2} = 0.$$

So \mathbb{Q} is not a free \mathbb{Z} -module. This illustrates that “torsion-free” does not imply “free” in general; in Example 1.70 we saw that “free” does not imply “torsion-free” in general either. However, in Chapter 2 we will prove that for finitely-generated modules over a PID, “free” is equivalent to “torsion-free”.

Solution to Exercise 1.81.

- (i) We are given that both N and M/N are torsion-free. Suppose that $rm = 0$ for some nonzero $r \in R$ and nonzero $m \in M$. Then certainly $r(m+N) = 0+N$, so since M/N is torsion-free we have $m+N = 0+N$, i.e. $m \in N$. But then $rm = 0$ contradicts the torsion-freeness of N . So our assumption leads to a contradiction, and M is torsion-free.

Incidentally, the converse is not true. Any submodule of a torsion-free module is clearly torsion-free, but a quotient of a torsion-free module need not be: think of the \mathbb{Z} -module \mathbb{Z} and its quotients \mathbb{Z}_n .

- (ii) The proof of this is quite similar to that in Exercise 1.60(ii) (but note that here we do not assume that our bases are finite). Suppose that $\{x_i \mid i \in I\}$ is a basis of N and $\{y_j + N \mid j \in J\}$ is a basis of M/N . For any element m of M , we can write $m + N$ uniquely in the form $\sum_{j \in J} r_j y_j + N$ for $r_j \in R$ (all but finitely many r_j 's being zero). This amounts to saying that m can be written uniquely in the form $n + \sum_{j \in J} r_j y_j$ where $n \in N$ and $r_j \in R$. The element n can in turn be written uniquely in the form $\sum_{i \in I} s_i x_i$ for $s_i \in R$ (all but finitely many s_i 's being zero), so m can be written uniquely in the form $\sum_{i \in I} s_i x_i + \sum_{j \in J} r_j y_j$ for $s_i, r_j \in R$. That is, $\{x_i \mid i \in I\} \cup \{y_j \mid j \in J\}$ is a basis of M , which is therefore free.

The example of \mathbb{Z} and \mathbb{Z}_n shows that a quotient of a free module is not necessarily free. A submodule of a free module is not necessarily free either: for example, any non-principal ideal of a commutative ring R cannot have a basis over R , because any two nonzero elements r_1, r_2 satisfy the linear dependence $r_2 r_1 + (-r_1) r_2 = 0$.

Solution to Exercise 1.82. In defining the $F[x]$ -module structure on F^n , we use the map $\varphi : F[x] \rightarrow \text{Mat}_n(F) : p(x) \mapsto p(A)$ which substitutes the matrix A for the variable x . This map is clearly F -linear, and it cannot be

injective because $F[x]$ is an infinite-dimensional vector space over F whereas $\text{Mat}_n(F)$ is n^2 -dimensional. So $\ker(\varphi) \neq \{0\}$, which means that there is some nonzero $p(x) \in F[x]$ such that $p(A) = 0$ (the zero matrix). Then $p(x)v = p(A)v = 0$ for all $v \in F^n$, so every element of F^n is a torsion element.

Solution to Exercise 1.83. We will actually apply the assumed extension property twice, once to prove that X generates M and a second time to prove that is linearly independent.

The first application is to the case when $N = M/RX$ and f sends every element of X to the zero element $0 + RX$: the property says that there is a unique R -module homomorphism $\varphi : M \rightarrow M/RX$ such that $\varphi(x) = 0 + RX$ for all $x \in X$. But we can easily find two such homomorphisms: the projection $m \mapsto m + RX$ and the zero homomorphism $m \mapsto 0 + RX$. Therefore these must be equal, which means that $m + RX = 0 + RX$ for all $m \in M$, which means that $RX = M$.

Now assume that we have an equation $\sum_{i=1}^k r_i x_i = 0$ involving some elements x_1, \dots, x_k of X . Then consider the map $f : X \rightarrow R^k$ which sends x_i to e_i for $1 \leq i \leq k$ and all other elements of X to 0. By the extension property again, there is an R -module homomorphism $\varphi : M \rightarrow R^k$ which extends f , and then we deduce

$$0 = \varphi\left(\sum_{i=1}^k r_i x_i\right) = \sum_{i=1}^k r_i \varphi(x_i) = (r_1, r_2, \dots, r_k),$$

which means that $r_1 = r_2 = \dots = r_k = 0$. So X is linearly independent.

Solution to Exercise 1.84.

(i) For any $r = (r_{ij}) \in R$ we have

$$(rx)_{ij} = \sum_{k \geq 1} r_{ik} x_{kj} = \begin{cases} r_{i,j/2} & \text{if } j \text{ is even,} \\ 0, & \text{if } j \text{ is odd.} \end{cases}$$

So the odd-numbered columns of the matrix rx are all zero, and the even-numbered columns are the same as the columns of the matrix r .

In particular, $rx = 0$ would clearly imply $r = 0$, so x is not a torsion element of the R -module R .

- (ii) Define $y \in R$ by $y_{ij} = 1$ if $j = 2i - 1$, $y_{ij} = 0$ if $j \neq 2i - 1$. Then for any $s \in R$, the even-numbered columns of sy are all zero, and the odd-numbered columns are the same as the columns of s . It is clear that as r and s each take every possible value in R , $rx + sy$ takes every possible value in R exactly once. So $\{x, y\}$ is a basis of R over R .

Incidentally, the fact that $R \cong R \oplus R$ implies that $R \cong R \oplus (R \oplus R) \cong R \oplus R \oplus R$, etc.; so $R^n \cong R^m$ for any $n, m \in \mathbb{N}$.

Solution to Exercise 1.108. The smallest example is $R = \mathbb{Z}$, $M = \mathbb{Z}_6$: we have the internal direct sum $\mathbb{Z}_6 = \{0, 3\} \oplus \{0, 2, 4\}$, and all three are cyclic \mathbb{Z} -modules (generated by 1, 3, and 2 respectively).

Solution to Exercise 1.109. Suppose $M = \bigoplus_{i \in I} N_i$. Then we certainly have $M = \sum_{i \in I} N_i$. If $n \in N_j \cap \sum_{i \neq j} N_i$, then n is both an element of N_j and a sum of elements of the other N_i 's; by the unique expression part of the definition of direct sum, this implies that $n = 0$. Conversely, suppose that $M = \sum_{i \in I} N_i$ and that $N_j \cap \sum_{i \neq j} N_i = \{0\}$ for all $j \in I$. We want to prove that if $\sum_{i \in I} n_i = \sum_{i \in I} n'_i$ for some $n_i, n'_i \in N_i$, then $n_i = n'_i$ for all $i \in I$. But for any $j \in I$, we can rearrange the equation as $n_j - n'_j = \sum_{i \neq j} (n'_i - n_i)$, and this element is both in N_j and in $\sum_{i \neq j} N_i$, so $n_j - n'_j = 0$ as required.

Solution to Exercise 1.110. The proof that the map $N_1 \oplus N_2 \rightarrow M : (n_1, n_2) \mapsto \varphi_1(n_1) + \varphi_2(n_2)$ respects addition and the R -action is routine. If we call this map $\varphi_1 + \varphi_2$, then we have a map $\Psi : \text{Hom}_R(N_1, M) \oplus \text{Hom}_R(N_2, M) \rightarrow \text{Hom}_R(N_1 \oplus N_2, M) : (\varphi_1, \varphi_2) \mapsto \varphi_1 + \varphi_2$, and this is also easily seen to respect addition. Therefore Ψ is a homomorphism of abelian groups (which is the only structure that we have on the Hom-sets, for general R). The main thing to prove is that Ψ is bijective, i.e. every R -module homomorphism $\varphi : N_1 \oplus N_2 \rightarrow M$ is of the form $\varphi_1 + \varphi_2$ for unique $\varphi_i \in \text{Hom}_R(N_i, M)$. This is true (despite its passing resemblance to the Diagonal Fallacy), because the restriction of φ to the submodule $\{(n_1, 0) \mid n_1 \in N_1\} \cong N_1$ must also be an R -module homomorphism, and therefore we have $\varphi(n_1, 0) = \varphi_1(n_1)$ for a uniquely determined

$\varphi_1 \in \text{Hom}_R(N_1, M)$; similarly $\varphi(0, n_2) = \varphi_2(n_2)$ for a uniquely determined $\varphi_2 \in \text{Hom}_R(N_2, M)$, so

$$\varphi(n_1, n_2) = \varphi((n_1, 0) + (0, n_2)) = \varphi(n_1, 0) + \varphi(0, n_2) = \varphi_1(n_1) + \varphi_2(n_2),$$

as required.

As the question noted, the same would work for any finite number of terms, so we have an abelian group isomorphism

$$\text{Hom}_R(N_1, M) \oplus \cdots \oplus \text{Hom}_R(N_k, M) \cong \text{Hom}_R(N_1 \oplus \cdots \oplus N_k, M).$$

Now suppose we have an infinite collection of R -modules $(N_i)_{i \in I}$, and R -module homomorphisms $\varphi_i : N_i \rightarrow M$. We do get a well-defined R -module homomorphism $\bigoplus_{i \in I} N_i \rightarrow M : (n_i) \mapsto \sum_{i \in I} \varphi_i(n_i)$, because of the restriction in the definition of $\bigoplus_{i \in I} N_i$ that all but finitely many components are zero. The same argument as in the case of two terms shows that this gives an abelian group isomorphism

$$\prod_{i \in I} \text{Hom}_R(N_i, M) \cong \text{Hom}_R\left(\bigoplus_{i \in I} N_i, M\right).$$

Here we have product rather than direct sum on the left, since there is no restriction to say that all but finitely many φ_i 's are zero.

If instead we do impose such a restriction on the φ_i 's, then we get a well-defined R -module homomorphism $\prod_{i \in I} N_i \rightarrow M : (n_i) \mapsto \sum_{i \in I} \varphi_i(n_i)$. But only those homomorphisms $\prod_{i \in I} N_i \rightarrow M$ which vanish when restricted to N_i for all but finitely many i arise in this way, so the resulting abelian group homomorphism $\bigoplus_{i \in I} \text{Hom}_R(N_i, M) \rightarrow \text{Hom}_R(\prod_{i \in I} N_i, M)$ is injective but not surjective.

Solution to Exercise 1.111. As in Exercise 1.110, the only part requiring any thought is that every R -module homomorphism $M \rightarrow N_1 \oplus N_2$ is of the form $m \mapsto (\varphi_1(m), \varphi_2(m))$ for unique $\varphi_i \in \text{Hom}_R(M, N_i)$. This is because we can compose any homomorphism $M \rightarrow N_1 \oplus N_2$ with the first projection map $N_1 \oplus N_2 \rightarrow N_1$ to get a homomorphism $M \rightarrow N_1$, and similarly for the second component. The general statement for a finite number of terms is that we have an abelian group isomorphism

$$\text{Hom}_R(M, N_1) \oplus \cdots \oplus \text{Hom}_R(M, N_k) \cong \text{Hom}_R(M, N_1 \oplus \cdots \oplus N_k).$$

With an infinite collection of N_i 's, the correct statement is that

$$\prod_{i \in I} \text{Hom}_R(M, N_i) \cong \text{Hom}_R(M, \prod_{i \in I} N_i).$$

This fails if we replace products by direct sums: the natural homomorphism $\bigoplus_{i \in I} \text{Hom}_R(M, N_i) \rightarrow \text{Hom}_R(M, \bigoplus_{i \in I} N_i)$ is injective but not surjective.

Solution to Exercise 1.112. This is not true for general rings. For example, the \mathbb{Z} -module \mathbb{Z} is not semisimple, because there is no submodule (i.e. ideal) which is complementary to $2\mathbb{Z}$ in \mathbb{Z} : for any nonzero ideal $n\mathbb{Z}$, $2\mathbb{Z} \cap n\mathbb{Z}$ contains $2n$ and is hence nonzero. (The rings R for which R is a semisimple R -module are said to be semisimple rings; this includes all fields, as well as various group algebras we will encounter later.)

Solution to Exercise 1.113. Suppose that M is a semisimple R -module and N a submodule of M . To prove that N is semisimple, let L be a submodule of N . Then L is also a submodule of M , so there is some submodule L' of M such that $M = L \oplus L'$. Let $L'' = L' \cap N$, a submodule of N ; the claim is that $N = L \oplus L''$, so L'' is a complementary submodule to L in N as required. For any $n \in N$, we can write $n = \ell + \ell'$ where $\ell \in L$ and $\ell' \in L'$, since $M = L + L'$. But then $n, \ell \in N$, so $\ell' = n - \ell \in N$ also, which implies that $\ell' \in L''$. So $N = L + L''$. Also $L \cap L'' \subseteq L \cap L' = \{0\}$, so $N = L \oplus L''$ and the proof is finished.

Now if M is semisimple, every quotient module M/N is isomorphic to a submodule N' (taking N' to be complementary to N in M). Since N' is semisimple by the above proof, M/N must be semisimple also. Thus quotients of a semisimple module are semisimple.

Solution to Exercise 1.114. The first step of this 'proof' is the Diagonal Fallacy: it is not true that any submodule N of $M_1 \oplus \cdots \oplus M_k$ is of the form $N_1 \oplus \cdots \oplus N_k$ where N_i is a submodule of M_i . To correct matters, it suffices to prove the $k = 2$ case, since once we know that, we can just add on extra modules one at a time. So assume that M_1 and M_2 are semisimple and that N is a submodule of $M_1 \oplus M_2$. Let $N_1 = N \cap M_1$ and let N'_1 be a complementary submodule to N_1 in M_1 . We have $N \cap N'_1 = \{0\}$, so $N + N'_1 = N \oplus N'_1$. Moreover, $M_1 = N_1 \oplus N'_1 \subseteq N \oplus N'_1$. Now let

$N_2 = (N \oplus N'_1) \cap M_2$ and let N'_2 be a complementary submodule to N_2 in M_2 . We have $(N \oplus N'_1) \cap N'_2 = \{0\}$, so $(N \oplus N'_1) + N'_2 = (N \oplus N'_1) \oplus N'_2$. Moreover, any element $m \in M$ can be written as $m_1 + m_2$ for $m_i \in M_i$, and m_2 in turn can be written as $n_2 + n'_2$ for $n_2 \in N_2$ and $n'_2 \in N'_2$, so $m = (m_1 + n_2) + n'_2 \in (N \oplus N'_1) \oplus N'_2$. Thus $M = N \oplus N'_1 \oplus N'_2$, and $N'_1 \oplus N'_2$ is the desired complementary submodule to N in M . (It is also true that an infinite direct sum of semisimple modules is semisimple, but that is trickier.)

Solution to Exercise 1.115. Part of Assignment 1.

Solution to Exercise 1.116.

- (i) The claim is that we can let $x = (x_p) \in M$ be the element such that $x_p = 1$ for all primes p . It is clear that $x + N \neq 0 + N$, because $x \notin N$ as it is not true that $x_p = 0$ for all but finitely many p . For any prime q , we define an element $y = (y_p) \in M$ as follows: we define $y_p = q^{-1}$ (the inverse of q in the field \mathbb{Z}_p) for all $p \neq q$, and define y_q to be 0 . We then have $qy_p = x_p$ for all $p \neq q$, so the difference $qy - x$ has all components zero except for the q component, and hence $qy - x \in N$, which means that $q(y + N) = x + N$.
- (ii) If there were a complementary submodule N' to N in M , then the quotient module M/N would be isomorphic to N' . So there would have to be a nonzero element $\tilde{x} = (\tilde{x}_p) \in N'$ which had the “divisibility” property of $x + N$, viz. that for every prime q there was some $\tilde{y} \in N'$ such that $q\tilde{y} = \tilde{x}$. But the q component of this equation says that $\tilde{x}_q = 0$, so this results in a contradiction.

Incidentally, the submodule N consists exactly of the torsion elements in M , so this shows that M cannot be written as the direct sum of a torsion module and a free module. The point is that in Chapter 2 we will prove that every finitely-generated module over a PID can be written in such a way.