

# Dummit and Foote Exercises

April 19, 2016

# Contents

<b>10 Introduction to Module Theory</b>	<b>2</b>
10.1 Basic Definitions and Examples . . . . .	2
10.2 Quotient Modules and Module Homomorphisms . . . . .	10
10.3 Generation of Modules, Direct Sums, and Free Modules . . . . .	17
10.4 Tensor Products of Modules . . . . .	31
10.5 Exact Sequences—Projective, Injective, and Flat Modules . . . . .	35

## Chapter 10

# Introduction to Module Theory

### 10.1 Basic Definitions and Examples

In these exercises  $R$  is a ring with 1 and  $M$  is a left  $R$ -module.

**Exercise 10.1.1.** Prove that  $0m = 0$  and  $(-1)m = -m$  for all  $m \in M$ .

**Solution:** We have via straightforward application of the module axioms that

$$0m = (0 - 0)m = 0m - 0m = 0.$$

Likewise, we can compute that

$$(-1)m = -m + m + (-1)m = -m + (1)m + (-1)m = -m + (1 - 1)m = -m - 0m = -m.$$

□

**Exercise 10.1.2.** Prove that  $R^\times$  and  $M$  satisfy the two axioms in Section 1.7 for a *group action* of the multiplicative group  $R^\times$  on the set  $M$ .

**Solution:** We know that  $R^\times$  is a group, and by the module axioms we know  $1 \cdot m = m$  for all  $m \in M$  and hence the identity acts on  $M$  in accordance with a group action. We also have via the module axioms that  $uv \cdot m = u \cdot (v \cdot m)$  for all  $u, v \in R^\times$ , and so the action of  $R^\times$  satisfies both axioms of a group action.

□

**Exercise 10.1.3.** Assume that  $rm = 0$  for some  $r \in R$  and some  $m \in M$  with  $m \neq 0$ . Prove that  $r$  does not have a left inverse (i.e., there is no  $s \in R$  such that  $sr = 1$ ).

**Solution:** Suppose otherwise, so that there exists  $s \in R$  so that  $sr = 1$ . Then we have that

$$m = (sr)m = s(rm) = s0 = 0$$

a contradiction.

□

**Exercise 10.1.4.** Let  $M$  be the module  $R^n$  described in Example 3 and let  $I_1, I_2, \dots, I_n$  be left ideals of  $R$ . Prove that the following are submodules of  $M$ :

- (a)  $\{(x_1, x_2, \dots, x_n) \mid x_i \in I_i\}$

(b)  $\{(x_1, x_2, \dots, x_n) \mid x_i \in R \text{ and } x_1 + x_2 + \dots + x_n = 0\}$ .

**Solution:** (a)

The set is clearly nonempty since  $(0, 0, \dots, 0)$  is in it. The second condition of the submodule criterion is also satisfied since

$$(x_1, x_2, \dots, x_n) + r(x'_1, x'_2, \dots, x'_n) = (x_1 + rx'_1, x_2 + rx'_2, \dots, x_n + rx'_n)$$

for any  $r \in R$  and  $x_i + rx'_i \in I$  by virtue of  $I$  being an ideal. Thus the set is a submodule.

(b)

As in (a) we notice that  $(0, 0, \dots, 0)$  is in the set, and so it is nonempty. Letting  $x = (x_1, \dots, x_n)$  and  $y = (x'_1, \dots, x'_n)$  be two elements of the set we have that  $x + ry$  is in the set since

$$\begin{aligned} (x_1 + rx'_1) + (x_2 + rx'_2) + \dots + (x_n + rx'_n) &= (x_1 + x_2 + \dots + x_n) + r(x'_1 + x'_2 + \dots + x'_n) \\ &= 0 + r0 \\ &= 0. \end{aligned}$$

Thus the set satisfies the submodule criterion and is a submodule. □

**Exercise 10.1.5.** For any left ideal  $I$  of  $R$  define

$$IM = \left\{ \sum_{\text{finite}} a_i m_i \mid a_i \in I, m_i \in M \right\}$$

to be the collection of all finite sums of elements of the form  $am$  where  $a \in I$  and  $m \in M$ . Prove that  $IM$  is a submodule of  $M$ .

**Solution:** Note that  $0_M \in IM$  since  $0_R \in I$  and  $0_M \in M$  so  $0_M = 0_R \cdot 0_M \in IM$ . Now let  $x = \sum a_i m_i$  and  $y = \sum b_j m_j$  be two elements of  $IM$ . Then notice for any  $r \in R$  that

$$x + ry = \sum a_i m_i + \sum r b_j m_j$$

which is again in  $IM$  since both sums are finite and  $rb_j \in I$  by virtue of  $I$  being a left ideal. Thus  $IM$  satisfies the submodule criterion and is a submodule. □

**Exercise 10.1.6.** Show that the intersection of any nonempty collection of submodules of an  $R$ -module is a submodule.

**Solution:** Let  $M$  be an  $R$ -module and let  $\{N_\alpha\}$  be an arbitrary collection of submodules of  $M$ . Let  $N = \cap_\alpha N_\alpha$ . Notice that  $N$  is nonempty since each  $N_\alpha$  must contain zero by virtue of being a subgroup over the overall module. Then let  $x, y \in N$ . Since each  $N_\alpha$  is a submodule we have  $x + ry \in N_\alpha$  for all  $r \in R$  and all  $\alpha$ . We conclude that  $x + ry \in N$  and so  $N$  satisfies the submodule criterion. This proves the result. □

**Exercise 10.1.7.** Let  $N_1 \subseteq N_2 \subseteq \dots$  be an ascending chain of submodules of  $M$ . Prove that  $\cup_{i=1}^\infty N_i$  is a submodule of  $M$ .

**Solution:** Let  $N = \cup_{i=1}^\infty N_i$ . Note that  $0 \in N$  so  $N$  is nonempty. Then let  $x, y \in N$ . There must exist  $N_i$  so that  $x, y \in N_i$  and by virtue of  $N_i$  being a submodule we will have  $x + ry \in N_i$  for all  $r \in R$  and hence  $x + ry \in N$ . This proves that  $N$  is a submodule. □

**Exercise 10.1.8.** An element  $m$  of the  $R$ -module  $M$  is called a *torsion element* if  $rm = 0$  for some nonzero element  $r \in R$ . The set of torsion elements is denoted

$$\text{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}.$$

- (a) Prove that if  $R$  is an integral domain then  $\text{Tor}(M)$  is a submodule of  $M$  (called the *torsion submodule* of  $M$ ).
- (b) Give an example of a ring  $R$  and an  $R$ -module  $M$  such that  $\text{Tor}(M)$  is not a submodule. [Consider the torsion elements in the  $R$ -module  $R$ .]
- (c) If  $R$  has zero divisors show that every nonzero  $R$ -module has nonzero torsion elements.

**Solution:** (a)

Let  $R$  be an integral domain and observe that  $\text{Tor}(M)$  is nonempty since it contains zero. Then let  $x, y \in \text{Tor}(M)$  and let  $r_1, r_2 \in R$  be nonzero so that  $r_1x = 0$  and  $r_2y = 0$ . For an arbitrary  $r \in R$  we can notice that

$$r_1r_2(x + ry) = r_1r_2x + r_1r_2ry = r_2r_1x + r_1rr_2y = r_2 \cdot 0 + r_1r \cdot 0 = 0 + 0 = 0$$

where above we have used the commutativity of  $R$ . Furthermore observe that  $r_1r_2$  is nonzero since  $R$  is an integral domain, and so  $x + ry \in \text{Tor}(M)$ . This proves that  $\text{Tor}(M)$  is a submodule by the submodule criterion.

(b)

Consider  $\mathbb{Z}/6\mathbb{Z}$ . The torsion elements of this ring as a module over itself are  $\{0, 2, 3, 4\}$  which do not even form an additive subgroup, much less a submodule.

(c)

Suppose  $R$  has zero divisors and let  $x, y \in R$  be nonzero so that  $xy = 0$ . Then for some nonzero  $m \in M$  consider  $ym$ . If  $ym = 0$  then  $m$  is a nonzero torsion element. Otherwise  $ym$  is a nonzero torsion element since  $x(ym) = (xy)m = 0m = 0$ .

□

**Exercise 10.1.9.** If  $N$  is a submodule of  $M$ , the *annihilator of  $N$  in  $R$*  is defined to be  $\{r \in R \mid rn = 0 \text{ for all } n \in N\}$ . Prove that the annihilator of  $N$  in  $R$  is a 2-sided ideal of  $R$ .

**Solution:** Let  $N$  be a submodule and let  $I$  be its annihilator. Clearly  $I$  contains 0 and so is nonempty. Furthermore if  $a, b \in I$  then  $a - b \in I$  since for any  $n \in N$  we have

$$(a - b)n = an + (-b)n = 0 - (bn) = 0 - 0 = 0$$

where above we have used the fact that  $(-b)n = -(bn)$  which can be proved analogously to property 2 in Problem 1. Thus  $I$  is an additive subgroup of  $R$ .

Finally let  $r \in R$  be arbitrary and let  $a \in I$ . Clearly  $ra \in I$  since

$$ran = r(an) = r0 = 0$$

for any  $n \in N$ . We also have  $ar \in I$  since

$$arn = a(rn) = 0$$

for any  $n \in N$ , where above we have used that  $an \in N$ . This proves that  $I$  is a 2-sided ideal in  $R$ .

□

**Exercise 10.1.10.** If  $I$  is a right ideal of  $R$ , the *annihilator of  $I$  in  $M$*  is defined to be  $\{m \in M \mid am = 0 \text{ for all } a \in I\}$ . Prove that the annihilator of  $I$  in  $M$  is a submodule of  $M$ .

**Solution:** Let  $I$  be a right ideal of  $R$  and let  $N$  be its annihilator. Notice immediately that  $0 \in N$  since  $an = 0$  for all  $a \in I$ . Then let  $n, n' \in N$  and  $r \in R$ . We have that

$$\begin{aligned} a(n + rn') &= an + arn' \\ &= 0 + (ar)n' \\ &= 0 + 0 \\ &= 0 \end{aligned}$$

where above we have used that  $ar \in I$  by virtue of  $I$  being a right ideal. This proves that  $N$  satisfies the submodule criterion, and so it is a submodule.  $\square$

**Exercise 10.1.11.** Let  $M$  be the abelian group (i.e.,  $\mathbb{Z}$ -module)  $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$ .

- (a) Find the annihilator of  $M$  in  $\mathbb{Z}$  (i.e. a generator for this principal ideal).
- (b) Let  $I = 2\mathbb{Z}$ . Describe the annihilator of  $I$  in  $M$  as a direct product of cyclic groups.

**Solution:** (a)

Notice that if  $r \in \mathbb{Z}$  annihilates  $M$  it must annihilate each coordinate. In particular, it must be a multiple of 24, of 15, and of 50. This condition is both necessary and sufficient and so the annihilator of  $M$  is  $600\mathbb{Z}$ , the ideal generated by the least common multiple of 24, 15, and 50.

(b)

The ideal  $2\mathbb{Z}$  annihilates 0 and 12 in the first coordinate, 0 in the second coordinate, and 0 and 25 in the third coordinate. Hence the annihilator of  $2\mathbb{Z}$  is the set

$$\{(0, 0, 0), (12, 0, 0), (0, 0, 25), (12, 0, 25)\}$$

which as a direct product of cyclic groups is isomorphic to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .  $\square$

**Exercise 10.1.12.** In the notation of the preceding exercises prove the following facts about annihilators.

- (a) Let  $N$  be a submodule of  $M$  and let  $I$  be its annihilator in  $R$ . Prove that the annihilator of  $I$  in  $M$  contains  $N$ . Give an example where the annihilator of  $I$  in  $M$  does not equal  $N$ .
- (b) Let  $I$  be a right ideal of  $R$  and let  $N$  be its annihilator in  $M$ . Prove that the annihilator of  $N$  in  $R$  contains  $I$ . Give an example where the annihilator of  $N$  in  $R$  does not equal  $I$ .

**Solution:** (a)

Let  $A$  be the annihilator of  $I$  in  $M$  and let  $n \in N$ . Then  $an = 0$  for all  $a \in I$  by definition. But this means that  $n \in A$ . This proves that  $N \subseteq A$  as desired. As an example where containment is strict let  $M = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  be a  $\mathbb{Z}$ -module and let  $N$  be the subgroup  $\{(0, 0), (1, 0)\}$ . Notice that  $2\mathbb{Z}$  is the annihilator of  $N$ , but the annihilator of  $2\mathbb{Z}$  is all of  $M$ .

(b)

Let  $J$  be the annihilator of  $N$  in  $R$  and let  $a \in I$ . Then  $an = 0$  for all  $n \in N$ . But then by definition

$a \in J$ , and so  $I \subseteq J$  as desired. An example where containment is strict occurs when considering the annihilator of  $6\mathbb{Z}$  in the  $\mathbb{Z}$ -module  $M = N = \mathbb{Z}/2\mathbb{Z}$ . This ideal annihilates all of  $M$ , but the annihilator of  $M$  is  $2\mathbb{Z}$  which strictly contains  $6\mathbb{Z}$ . □

**Exercise 10.1.13.** Let  $I$  be an ideal of  $R$ . Let  $M'$  be the subset of elements  $a$  of  $M$  that are annihilated by some power,  $I^k$  of the ideal  $I$ , where the power may depend on  $a$ . Prove that  $M'$  is a submodule of  $M$ . [Use Exercise 7.]

**Solution:** Let  $N_k$  be the annihilator of  $I^k$ . Elements of  $I^k$  are of the form  $\sum a_i^k$  where the sum is finite and each  $a_i$  is an element of  $I$ . We thus notice that  $N_k \subseteq N_{k+1}$  since if  $n$  is annihilated by all finite sums  $\sum a_i^k$  with  $a_i \in I$  then

$$\left(\sum a_i^{k+1}\right)n = \sum (a_i^{k+1}n) = \sum (a_i a_i^k n) = \sum (a_i 0) = 0$$

and so it is also annihilated by elements of  $I^{k+1}$ . Thus the union of all  $N_k$  is a submodule by Exercise 7. This union is exactly  $M'$ , proving the desired result. □

**Exercise 10.1.14.** Let  $z$  be an element of the center of  $R$ , i.e.  $zr = rz$  for all  $r \in R$ . Prove that  $zM$  is a submodule of  $M$ , where  $zM = \{zm \mid m \in M\}$ . Show that if  $R$  is the ring of  $2 \times 2$  matrices over a field and  $e$  is the matrix with a 1 in position 1, 1 and zeros elsewhere then  $eR$  is *not* a left  $R$ -submodule (where  $M = R$  is considered as a left  $R$ -module as in Example 1)—in this case the matrix  $e$  is not in the center of  $R$ .

**Solution:** Note that  $0 = z0 \in zM$  and so  $zM$  is nonempty. Letting  $zx, zy \in zM$  where  $x, y \in M$  are arbitrary and letting  $r \in R$  we have that

$$zx + rzy = zx + zry = z(x + ry) \in zM$$

and so  $zM$  satisfies the submodule criterion.

Notice that

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$$

and so in the example  $eM$  is the set of matrices with zero entries in the bottom row and arbitrary entries in the top row. This collection is not a submodule since as a set it is not invariant under the left action of  $R$  on it. In particular,

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

which is not a matrix with zero entries in the bottom row. We conclude that  $e$  is indeed not in the center of  $R$ . □

**Exercise 10.1.15.** If  $M$  is a finite abelian group then  $M$  is naturally a  $\mathbb{Z}$ -module. Can this action be extended to make  $M$  into a  $\mathbb{Q}$ -module?

**Solution:** No, not always. Consider the  $\mathbb{Z}$ -module  $\mathbb{Z}/2\mathbb{Z}$ . If this were naturally a  $\mathbb{Q}$ -module then it would have some element  $\frac{1}{2} \cdot 1$ . This element would satisfy

$$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1 = \left(\frac{1}{2} + \frac{1}{2}\right) \cdot 1 = 1 \cdot 1 = 1$$

and in particular it would have order at least three as an element of the group  $\mathbb{Z}/2\mathbb{Z}$ . This is not possible. More generally, for any finite abelian group  $G$  one can consider the action of  $\frac{1}{|G|}$  to derive a contradiction. Thus finite abelian group never has a  $\mathbb{Q}$  action compatible with the natural  $\mathbb{Z}$  action.

However, if an abelian group is divisible then we can extend its natural  $\mathbb{Z}$  action to a  $\mathbb{Q}$  action. Of course nonzero divisible abelian groups are necessarily infinite, so this falls outside the scope of the problem.  $\square$

**Exercise 10.1.16.** Prove that the submodules  $U_k$  describe in the example of  $F[x]$ -modules are all of the  $F[x]$ -submodules for the shift operator.

**Solution:** Let  $V = F^n$  be a  $F[x]$  module where  $x$  acts as the shift operator and  $F$  acts as normal. Let  $U \subseteq V$  be a submodule of  $V$ . Let  $k$  be the largest index such that there exists a vector in  $U$  whose  $k$ -th coordinate is nonzero. Then we claim  $U = U_k$ . The inclusion  $U \subseteq U_k$  is trivial since  $U_k$  is all vectors in  $V$  where coordinates following the  $k$ -th are zero. Hence we only have to show  $U_k \subseteq U$ .

To show that  $U_k \subseteq U$  we will show straightforwardly that  $e_i$  is in  $U$  for  $1 \leq i \leq k$ . The set of these  $e_i$  forms a basis for  $U_k$  and so it will follow that  $U_k \subseteq U$ . Notice that we really only need to construct  $e_k$ , since all  $e_i$  for  $i < k$  can be obtained by the action of  $x$ , which will still be in  $U$  since  $U$  is a submodule. To construct  $e_k$ , let  $v = (v_1, v_2, \dots, v_k, 0, 0, \dots, 0)$  be a vector in  $U$  where  $v_k \neq 0$ . Then we can construct the basis vector  $e_k$  by repeatedly zeroing out smaller coordinates in  $v_k$ : first consider

$$v - \left( \frac{v_{k-1}}{v_k} x \right) v \in U.$$

The  $(k-1)$ -th coordinate of this vector will be  $v_k - v_k = 0$ . We can repeat this process, acting on our new vector by  $x^2$  multiplied by an appropriate scalar, subtracting the result, and so on. This eventually leads to a vector  $(0, 0, \dots, 0, v_k, 0, 0, \dots, 0)$  which can be transformed to  $e_k$  via multiplication by the scalar  $\frac{1}{v_k}$ . This proves that  $e_k \in U$ , and as previously discussed this implies that  $e_i \in U$  for all  $1 \leq i \leq k$ . Hence  $U_k \subseteq U$  and we are done.  $\square$

**Exercise 10.1.17.** Let  $T$  be the shift operator on the vector space  $V$  and let  $e_1, \dots, e_n$  be the usual basis vector described in the example of  $F[x]$ -modules. If  $m \geq n$  find  $(a_m x^m + a_{m-1} x^{m-1} + \dots + a_0) e_n$ .

**Solution:** For convenience let  $p(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_0$ . We compute directly that

$$\begin{aligned} p(x) \cdot e_n &= \left( \sum_{i=0}^m a_i x^i \right) \cdot e_n \\ &= \sum_{i=0}^m a_i (x^i \cdot e_n) && \text{Via module axioms} \\ &= \sum_{i=0}^n a_i (x^i \cdot e_n) && \text{Since } x^i \cdot e_n = 0 \text{ for } i > n \\ &= \sum_{i=0}^n a_i (e_{n-i}) && \text{Since } x \text{ acts as shift operator} \\ &= (a_n, a_{n-1}, \dots, a_1, a_0). \end{aligned}$$

Thus  $p(x) \cdot e_n$  gives us the first  $n+1$  coefficients in  $p(x)$  in a vector in reverse order.  $\square$



**Exercise 10.1.18.** Let  $F = \mathbb{R}$ . Let  $V = \mathbb{R}^2$  and let  $T$  be the linear transformation from  $V$  to  $V$  which is rotation clockwise about the origin by  $\pi/2$  radians. Show that  $V$  and  $0$  are the only  $F[x]$ -submodules for this  $T$ .

**Solution:** It suffices to show that every nontrivial submodule is equal to  $V$ . Given a nontrivial submodule  $U$ , let  $v$  be a nonzero vector in  $U$ . Then notice that  $x \cdot v \in U$  is linearly independent from  $v$ . Since  $U$  must also be a subspace of the vector space  $V$ , we see that  $U$  contains  $\text{span}\{v, x \cdot v\} = V$ . Hence  $U$  is all of  $V$ .  $\square$

**Exercise 10.1.19.** Let  $F = \mathbb{R}$ , let  $V = \mathbb{R}^2$  and let  $T$  be the linear transformation from  $V$  to  $V$  which is projection onto the  $y$ -axis. Show that  $V, 0$ , the  $x$ -axis and the  $y$ -axis are the only  $F[x]$ -submodules for this  $T$ .

**Solution:** We know that  $0$  and  $V$  are always submodules. It remains to characterize the nontrivial proper submodules. Notice that such submodules are necessarily 1-dimensional subspaces of  $V = \mathbb{R}^2$  since submodules under the action of  $F[x]$  are always subspaces and 0- and 2-dimensional subspaces are trivial and non-proper submodules respectively.

Let  $U = \text{span}\{v\}$  be some nontrivial proper submodule. Since  $U$  is 1-dimensional we must have that  $x \cdot v = av$  for some scalar  $a$ . In particular  $v$  is an eigenvector of  $T$  and so  $U$  is an eigenspace of  $T$ . The only eigenspaces are clearly the  $x$  and  $y$  axes. One can verify quickly that these are submodules: they both are subspaces (in particular subgroups) of  $V$  and are invariant under the action of  $F[x]$  since the  $y$ -axis is only scaled and the  $x$ -axis is annihilated by any nonunits in  $F[x]$ .  $\square$

**Exercise 10.1.20.** Let  $F = \mathbb{R}$ , let  $V = \mathbb{R}^2$  and let  $T$  be the linear transformation from  $V$  to  $V$  which is rotation clockwise about the origin by  $\pi$  radians. Show that *every* subspace of  $V$  is an  $F[x]$  submodule for this  $T$ .

**Solution:** Rotating by  $\pi$  radians is the same as additive negation. Hence we have  $x \cdot v = -v$  for all vectors  $v$ . Being invariant under the action of  $F$  and  $x$  is enough to be a submodule, and subspaces are invariant under both by the definition of being a subspace (and hence an additive subgroup). Thus all subspaces are submodules.  $\square$

**Exercise 10.1.21.** Let  $n \in \mathbb{Z}^+$ ,  $n > 1$  and let  $R$  be the ring of  $n \times n$  matrices with entries from a field  $F$ . Let  $M$  be the set of  $n \times n$  matrices with arbitrary elements of  $F$  in the first column and zeros elsewhere. Show that  $M$  is a submodule of  $R$  when  $R$  is considered as a left module over itself, but  $M$  is not a submodule of  $R$  when  $R$  is considered as a right  $R$ -module.

**Solution:** It is clear that  $M$  is an additive subgroup of the module  $R$ . When  $R$  acts on  $M$  from the left  $M$  is invariant since the  $i$ -th column of  $rm$  for  $r \in R$  and  $m \in M$  is just the product of  $r$  with the  $i$ -th column in  $m$ . For  $i > 1$  this column is zero and so must be  $r$ 's product with it. Hence  $rm \in M$ .

On the other hand when  $R$  acts from the right the columns in  $mr$  beyond the first may be nonzero, as illustrated by the small example below.

$$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \notin M.$$

$\square$

**Exercise 10.1.22.** Suppose that  $A$  is a ring with identity  $1_A$  that is a (unital) left  $R$ -module satisfying  $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$  for all  $r \in R$  and  $a, b \in A$ . Prove that the map  $f : R \rightarrow A$  defined by  $f(r) = r \cdot 1_A$  is a ring homomorphism mapping  $1_R$  to  $1_A$  and  $f(R)$  is contained in the center of  $A$ . Conclude that  $A$  is an  $R$ -algebra and that the  $R$ -module structure on  $A$  induced by its algebra structure is precisely the original  $R$ -module structure.

**Solution:** That  $f$  maps  $1_R$  to  $1_A$  follows from the fact that  $f(1_R) = 1_R \cdot 1_A = 1_A$ . Given  $r, s \in R$  we have that

$$f(r + s) = (r + s) \cdot 1_A = r \cdot 1_A + s \cdot 1_A = f(r) + f(s)$$

and

$$f(rs) = rs \cdot 1_A = r \cdot (s \cdot 1_A) = r \cdot (s \cdot 1_A 1_A) = r \cdot (1_A(s \cdot 1_A)) = (r \cdot 1_A)(s \cdot 1_A) = f(r)f(s)$$

so  $f$  is a ring homomorphism. Let  $r \cdot 1_A \in f(R)$  and  $a \in A$ . Then we have that

$$(r \cdot 1_A)a = r \cdot (1_A a) = r \cdot a = r \cdot (a 1_A) = a(r \cdot 1_A)$$

and so  $f(R)$  is in the center of  $A$ . This proves that  $A$  is an  $R$ -algebra. The  $R$ -module structure on  $A$  as an algebra is the same as its original structure since  $r \cdot a = r \cdot (1_A a) = (r \cdot 1_A)a$ . □

**Exercise 10.1.23.** Let  $A$  be the direct product ring  $\mathbb{C} \times \mathbb{C}$  (cf Section 7.6). Let  $\tau_1$  denote the identity map on  $\mathbb{C}$  and let  $\tau_2$  denote complex conjugation. For any pair  $p, q \in \{1, 2\}$  (not necessarily distinct) define

$$f_{p,q} : \mathbb{C} \rightarrow \mathbb{C} \times \mathbb{C} \quad \text{by} \quad f_{p,q}(z) = (\tau_p(z), \tau_q(z)).$$

So, for example  $f_{2,1} : z \mapsto (\bar{z}, z)$  where  $\bar{z}$  is the complex conjugate of  $z$ , i.e.  $\tau_2(z)$ .

- (a) Prove that each  $f_{p,q}$  is an injective ring homomorphism, and that they all agree on the subfield  $\mathbb{R}$  of  $\mathbb{C}$ . Deduce that  $A$  has four distinct  $\mathbb{C}$ -algebra structures. Explicitly give the action  $z \cdot (u, v)$  of a complex number  $z$  on an ordered pair in  $A$  in each case.
- (b) Prove that if  $f_{p,q} \neq f_{p',q'}$  then the identity map on  $A$  is *not* a  $\mathbb{C}$ -algebra homomorphism from  $A$  considered as a  $\mathbb{C}$ -algebra via  $f_{p,q}$  to  $A$  considered as a  $\mathbb{C}$  algebra via  $f_{p',q'}$  (although the identity is an  $\mathbb{R}$  algebra isomorphism).
- (c) Prove that for any pair  $p, q$  there is some ring isomorphism from  $A$  to itself such that  $A$  is isomorphic as a  $\mathbb{C}$  algebra via  $f_{p,q}$  to  $A$  considered as a  $\mathbb{C}$  algebra via  $f_{1,1}$  (the “natural”  $\mathbb{C}$ -algebra structure on  $A$ ).

*Remark:* In the preceding exercise  $A = \mathbb{C} \times \mathbb{C}$  is not a  $\mathbb{C}$ -algebra over either of the direct factor component copies of  $\mathbb{C}$  (for example the subring  $\mathbb{C} \times 0 \cong \mathbb{C}$ ) since it is not a unital module over these copies of  $\mathbb{C}$  (the 1 of these subrings is not the same as the 1 of  $A$ ).

**Solution:** (a)

That each  $f_{p,q}$  agrees on  $\mathbb{R}$  is trivial since complex conjugation fixes  $\mathbb{R}$ . Also recall that complex conjugation is an automorphism of  $\mathbb{C}$  and so each  $\tau_p$  is an automorphism. Hence  $f_{p,q}$  behaves as a ring homomorphism in each coordinate and overall will be a homomorphism. It is a proper ring homomorphism since it maps  $1_{\mathbb{C}} = 1$  to  $1_{\mathbb{C} \times \mathbb{C}} = (1, 1)$ . That each  $f_{p,q}$  is injective follows from the injectivity of  $\tau_p$  for  $p = 1, 2$ . In particular if  $z$  is nonzero then  $f_{p,q}(z)$  is nonzero for all  $p, q$  and hence the kernel of  $f_{p,q}$  is trivial.

The explicit action induced by  $f_{p,q}$  is just

$$z \cdot (u, v) = (\tau_p(z)u, \tau_q(z)v).$$

In particular,  $f_{1,1}$  acts via natural scalar multiplication.

(b)

If  $f_{p,q} \neq f_{p',q'}$  then we notice that

$$f_{p,q}(i) \neq f_{p',q'}(i)$$

since there must be a coordinate in which one map conjugates and the other does not. Hence the action of  $i \in \mathbb{C}$  induced by  $f_{p,q}$  differs from that induced by  $f_{p',q'}$  and in particular there exists  $(z_1, z_2) \in \mathbb{C} \times \mathbb{C}$  so that the action of  $i$  on  $(z_1, z_2)$  induced by each is a different element of  $\mathbb{C} \times \mathbb{C}$ . Denote by  $\cdot$  the action induced by  $f_{p,q}$  and by  $\circ$  the action induced by  $f_{p',q'}$ . If the identity map  $\text{Id}$  on  $\mathbb{C} \times \mathbb{C}$  were a  $\mathbb{C}$ -algebra homomorphism we would have that

$$i \cdot (z_1, z_2) = \text{Id}(i \cdot (z_1, z_2)) = i \circ \text{Id}((z_1, z_2)) = i \circ (z_1, z_2)$$

which is a contradiction. Hence the identity is not a  $\mathbb{C}$ -algebra homomorphism.

(c)

For  $f_{p,q}$  the isomorphism of  $\mathbb{C} \times \mathbb{C}$  which makes it isomorphic to the natural action is the isomorphism which acts as  $\tau_p$  in the first coordinate and  $\tau_q$  in the second. Let  $\phi$  denote this map. The map  $\phi$  is clearly a ring isomorphism since  $\tau_p$  and  $\tau_q$  are ring isomorphisms of each coordinate. To see that this gives  $\mathbb{C} \times \mathbb{C}$  the natural  $\mathbb{C}$ -algebra structure, let  $\cdot$  denote the natural action and  $\circ$  denote the action induced by  $f_{p,q}$ . Then we have that  $\phi$  is a  $\mathbb{C}$ -algebra isomorphism since

$$\begin{aligned} \phi(z \circ (z_1, z_2)) &= \phi((\tau_p(z)z_1, \tau_q(z)z_2)) \\ &= (\tau_p(\tau_p(z)z_1), \tau_q(\tau_q(z)z_2)) \\ &= (z\tau_p(z_1), z\tau_q(z_2)) && \text{Since } \tau_p(\tau_p(z)) = z \text{ for all } \tau_p \\ &= z \cdot (\tau_p(z_1), \tau_q(z_2)) \\ &= z \cdot \phi((z_1, z_2)). \end{aligned}$$

Hence  $\mathbb{C} \times \mathbb{C}$  with the  $f_{p,q}$  action is  $\mathbb{C}$ -algebra isomorphic to  $\mathbb{C} \times \mathbb{C}$  with the natural action, as desired. □

## 10.2 Quotient Modules and Module Homomorphisms

In these exercises  $R$  is a ring with 1 and  $M$  is a left  $R$ -module.

**Exercise 10.2.1.** Use the submodule criterion to show that kernels and images of  $R$ -module homomorphisms are submodules.

**Solution:** Kernels and images of  $R$ -module homomorphisms always contain zero by virtue of being kernels and images of the underlying group homomorphisms. Thus they are nonempty. Let  $\phi : N \rightarrow M$  be an  $R$ -module homomorphism. We will check the second condition of the submodule criterion for  $\ker \phi$  and  $\phi(N)$ . Letting  $x_1, x_2 \in \ker \phi$  and  $r \in R$  we notice that

$$\phi(x_1 + rx_2) = \phi(x_1) + r\phi(x_2) = 0 + r0 = 0$$

and so  $x_1 + rx_2 \in \ker \phi$ . This proves that  $\ker \phi$  is a submodule of  $N$ . Letting  $\phi(n_1)$  and  $\phi(n_2)$  be arbitrary elements of  $\phi(N)$  and letting  $r \in R$  we have

$$\phi(n_1) + r\phi(n_2) = \phi(n_1 + rn_2) \in \phi(N).$$

Hence  $\phi(N)$  also satisfies the second condition of the submodule criterion and is a submodule.  $\square$

**Exercise 10.2.2.** Show that the relation “is  $R$ -module isomorphic to” is an equivalence relation on any set of  $R$ -modules.

**Solution:** We verify each property of an equivalence relation directly.

- *Reflexivity:* Any  $R$ -module is isomorphic to itself via the identity map.
- *Symmetry:* Let  $\phi : N \rightarrow M$  be an isomorphism of  $R$ -modules. We claim that the map  $\phi^{-1}$  is also an  $R$ -module isomorphism. We know it is a group isomorphism since  $\phi$  is a group isomorphism, and so all we have to verify is that it preserves the action of  $R$ . Let  $m \in M$  and  $r \in R$ . We know  $m = \phi(n)$  for some  $n \in N$  and since  $\phi$  is an  $R$ -module isomorphism we also have  $\phi(rn) = r\phi(n) = rm$ . Putting this together, we have

$$\phi^{-1}(rm) = \phi^{-1}(\phi(rn)) = rn = r\phi^{-1}(m)$$

and so  $\phi^{-1}$  is a homomorphism of  $R$ -modules. This proves that  $M$  is  $R$ -module isomorphic to  $N$ .

- *Transitivity:* Let

$$N \xrightarrow{\phi} M \xrightarrow{\psi} L$$

be a sequence of  $R$ -module isomorphisms. We claim that  $\psi \circ \phi$  is an  $R$ -module isomorphism from  $N$  to  $L$ . It is a group isomorphism by virtue of  $\phi$  and  $\psi$  being group isomorphisms, so we need only verify that the action of  $R$  is preserved. Given  $r \in R$  and  $n \in N$  we have directly that

$$\psi(\phi(rn)) = \psi(r\phi(n)) = r\psi(\phi(n))$$

by virtue of  $\phi$  and  $\psi$  being  $R$ -module isomorphisms. This proves that  $N$  is  $R$ -module isomorphic to  $L$ , as desired. We conclude that “is  $R$ -module isomorphic to” is an equivalence relation.  $\square$

**Exercise 10.2.3.** Give an explicit example of a map from one  $R$ -module to another which is a group homomorphism but not an  $R$ -module homomorphism.

**Solution:** Natural examples occur whenever a module  $M$  has two distinct  $R$ -module structures on it. In this case the identity map from  $M$  to  $M$  is a group homomorphism, but not an  $R$ -module homomorphism. Some examples of modules  $M$  which can have distinct structures are described below.

- The algebra  $A = \mathbb{C} \times \mathbb{C}$  described in 10.1.23 as a module over  $\mathbb{C}$ .
- A vector space as an  $F[x]$  module, where the action of  $x$  can be various linear transformations.

- Example 2 on page 346 also works: the map  $x \mapsto x^2$  in  $M = F[x]$  is never an  $F[x]$ -module homomorphism. Indeed, one can generalize this by sending  $\phi : x \mapsto f(x)$  for any  $f(x) \neq x$ . This is a group homomorphism but not an  $F[x]$  module homomorphism since we would have  $f(x) = \phi(x) = \phi(x \cdot 1) = x\phi(1) = x$ . Perhaps most generally one can consider a ring with unity and a nontrivial endomorphism. This endomorphism serves as a group homomorphism that is not an  $R$ -module homomorphism.

□

**Exercise 10.2.4.** Let  $A$  be any  $\mathbb{Z}$ -module, let  $a$  be any element of  $A$  and let  $n$  be a positive integer. Prove that the map  $\phi_a : \mathbb{Z}/n\mathbb{Z} \rightarrow A$  given by  $\phi_a(\bar{k}) = ka$  is a well defined  $\mathbb{Z}$ -module homomorphism if and only if  $na = 0$ . Prove that  $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$  where  $A_n = \{a \in A \mid na = 0\}$  (so  $A_n$  is the annihilator in  $A$  of the ideal  $(n)$  of  $\mathbb{Z}$  — cf. Exercise 10, Section 1).

**Solution:** We begin by proving that  $\phi_a$  is a well defined  $\mathbb{Z}$ -module homomorphism if and only if  $na = 0$ .

( $\Rightarrow$ ) Suppose  $\phi_a$  is a well defined  $\mathbb{Z}$ -module homomorphism. Then we have that  $na = \phi_a(\bar{n}) = \phi_a(0)$  which must be zero since  $\phi_a$  is a homomorphism of groups.

( $\Leftarrow$ ) Suppose  $na = 0$ . To show  $\phi_a$  is well defined we need to show that  $\phi_a(\bar{k})$  does not depend on our choice of representative for  $\bar{k}$ . Letting  $k + bn$  be an arbitrary representative of  $\bar{k}$  we have that

$$\phi_a(\overline{k + bn}) = (k + bn)a = ka + bna = ka + b(0) = ka$$

and so the map is well defined. To prove it is a group homomorphism let  $\bar{k}_1, \bar{k}_2 \in \mathbb{Z}/n\mathbb{Z}$ . Then we have

$$\phi_a(\overline{k_1 + k_2}) = (\overline{k_1} + \overline{k_2})a = \overline{k_1}a + \overline{k_2}a = \phi(\overline{k_1}) + \phi(\overline{k_2}).$$

To see it is a  $\mathbb{Z}$ -module homomorphism, let  $z \in \mathbb{Z}$  and observe that

$$\phi_a(z\bar{k}) = \phi_a(\overline{zk}) = \overline{zka} = z\bar{k}a = z\phi_a(\bar{k})$$

where the second to last equality follows from the fact that  $z$  acts the same on multiples of  $a$  as any  $z'$  congruent to  $z \pmod{n}$ . This shows that  $\phi_a$  is a homomorphism of  $\mathbb{Z}$ -modules.

To prove that  $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$  we show that each homomorphism  $\phi$  from  $\mathbb{Z}/n\mathbb{Z}$  to  $A$  is uniquely determined by  $\phi(1)$  and  $\phi(1) \in A_n$ . In fact, we show that all  $\phi \in \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$  are of the form  $\phi_a$  for some  $a \in A_n$ . Given an homomorphism  $\phi : \mathbb{Z}/n\mathbb{Z} \rightarrow A$  consider  $\phi(1) = a$ . We know that  $\phi(1) \in A_n$  since

$$na = n\phi(1) = \phi(n) = \phi(0) = 0.$$

Extending  $\phi$  to the rest of  $\mathbb{Z}/n\mathbb{Z}$  we see that necessarily  $\phi = \phi_a$ . By the result proven earlier in the problem, we conclude that every homomorphism in  $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$  is of the form  $\phi_a$  for  $a \in A_n$ . To prove that  $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$  is isomorphic to  $A_n$  as a module, notice that by the properties of homomorphisms we have  $\phi_a + \phi_b = \phi_{a+b}$  and  $z\phi_a = \phi_{za}$  and also  $\phi_a = \phi_b$  if and only if  $a = b$ . Hence the map  $\phi_a \mapsto a$  is an isomorphism of  $\mathbb{Z}$ -modules and we conclude the desired result. □

**Exercise 10.2.5.** Exhibit all  $\mathbb{Z}$ -module homomorphisms from  $\mathbb{Z}/30\mathbb{Z}$  to  $\mathbb{Z}/21\mathbb{Z}$ .

**Solution:** By the previous exercise we know that  $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/30\mathbb{Z}, \mathbb{Z}/21\mathbb{Z})$  consists of maps  $\phi_a$  where  $a \in \mathbb{Z}/21\mathbb{Z}$  is annihilated by  $30\mathbb{Z}$ . The elements in  $\mathbb{Z}/21\mathbb{Z}$  annihilated by 30 are exactly those which are multiples of 7. Hence the only maps are the zero map,  $a \mapsto 7a$  and  $a \mapsto 14a$ . □

**Exercise 10.2.6.** Prove that  $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n, m)\mathbb{Z}$ .

**Solution:** By 10.2.4 we have that  $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$  is isomorphic to the annihilator of  $n\mathbb{Z}$  in  $\mathbb{Z}/m\mathbb{Z}$ . This annihilator will consist of exactly the  $a \in \mathbb{Z}/m\mathbb{Z}$  for which  $na$  is a multiple of  $m$ . Let  $d$  be the greatest common divisor of  $n$  and  $m$ . Then this annihilator can be easily described as the cyclic module generated by  $m/d$  in  $\mathbb{Z}/m\mathbb{Z}$ . Indeed,  $na$  is a multiple of  $m$  if and only if  $a$  is a multiple of  $m/d$ . The cyclic module generated by  $m/d$  has  $d$  elements, and hence is isomorphic to  $\mathbb{Z}/d\mathbb{Z}$ . This proves the result.  $\square$

**Exercise 10.2.7.** Let  $z$  be a fixed element of the center of  $R$ . Prove that the map  $m \mapsto zm$  is an  $R$ -module homomorphism from  $M$  to itself. Show that for a commutative ring  $R$  the map from  $R$  to  $\text{End}_R(M)$  given by  $r \mapsto rI$  is a ring homomorphism (where  $I$  is the identity endomorphism).

**Solution:** This is a group homomorphism since  $z(m_1 + m_2) = zm_1 + zm_2$  by the module axioms. Since  $z$  is in the center of  $r$  we also have  $r(zm) = z(rm)$  for all  $r \in R$  and so this map also respects the  $R$ -module structure.

Let  $\phi$  denote the map  $r \mapsto rI$ . Then the ring homomorphism conditions are easily verified:  $\phi(r_1 + r_2) = (r_1 + r_2)I = r_1I + r_2I = \phi(r_1) + \phi(r_2)$ , and  $\phi(r_1r_2) = r_1r_2I = r_1Ir_2I = \phi(r_1)\phi(r_2)$ . This proves the result.  $\square$

**Exercise 10.2.8.** Let  $\phi : M \rightarrow N$  be an  $R$ -module homomorphism. Prove that  $\phi(\text{Tor}(M)) \subseteq \text{Tor}(N)$  (cf. Exercise 8 in Section 1).

**Solution:** Let  $m \in \text{Tor}(M)$  and  $r \in R$  be nonzero so that  $rm = 0$ . Then  $r\phi(m) = \phi(rm) = \phi(0) = 0$  and so  $\phi(m) \in \text{Tor}(N)$ . This proves the result.  $\square$

**Exercise 10.2.9.** Let  $R$  be a commutative ring. Prove that  $\text{Hom}_R(R, M)$  and  $M$  are isomorphic as left  $R$ -modules. [Show that each element of  $\text{Hom}_R(R, M)$  is determined by its value on the identity of  $R$ .]

**Solution:** Let  $\phi \in \text{Hom}_R(R, M)$  and let  $r \in R$ . We will show that  $\phi(r)$  can be expressed in terms of  $\phi(1)$ . Notice that

$$\phi(r) = \phi(r \cdot 1) = r\phi(1)$$

by definition of being an  $R$ -module homomorphism. Hence each  $\phi$  can be expressed as  $\phi_m$  for  $m \in M$  where  $\phi_m(r) = rm$ . We claim that the map  $m \mapsto \phi_m$  is a homomorphism of the  $R$ -modules  $M$  and  $\text{Hom}_R(R, M)$ .

First, note that this map is injective since  $\phi_{m_1} = \phi_{m_2}$  means that  $m_1 = \phi_{m_1}(1) = \phi_{m_2}(1) = m_2$ . Furthermore it is surjective since every homomorphism is uniquely determined by its value on 1 and can be written as  $\phi_m$ . This map is also a group homomorphism since

$$\phi_{m_1+m_2}(s) = s(m_1 + m_2) = sm_1 + sm_2 = \phi_{m_1}(s) + \phi_{m_2}(s)$$

for all  $s \in R$  and hence  $\phi_{m_1+m_2} = \phi_{m_1} + \phi_{m_2}$ . To show this map respects the  $R$ -module structure, let  $r \in R$  and observe that

$$r\phi_m(s) = rsm = s(rm) = \phi_{rm}(s)$$

for all  $s \in R$ , and so  $r\phi_m = \phi_{rm}$ . We conclude that  $m \mapsto \phi_m$  is an  $R$ -module isomorphism as desired.  $\square$

**Exercise 10.2.10.** Let  $R$  be a commutative ring. Prove that  $\text{Hom}_R(R, R)$  and  $R$  are isomorphic as rings.

**Solution:** Consider the map  $r \mapsto rI$  where  $I$  is the identity map on  $R$ . By 10.2.7 this is a homomorphism from  $R$  to  $\text{End}_R(R) = \text{Hom}_R(R, R)$ . But this is also the exact map described in the proof of 10.2.9. In particular, this is an isomorphism of the  $R$ -module  $\text{Hom}_R(R, R)$  with the  $R$ -module  $R$ . We conclude that this map is bijective, and by virtue of being a ring homomorphism it must be a ring isomorphism. This proves the result.  $\square$

**Exercise 10.2.11.** Let  $A_1, A_2, \dots, A_n$  be  $R$ -modules and let  $B_i$  be a submodule of  $A_i$  for each  $i = 1, 2, \dots, n$ . Prove that

$$(A_1 \times \cdots \times A_n)/(B_1 \times \cdots \times B_n) \cong (A_1/B_1) \times \cdots \times (A_n/B_n).$$

[Recall Exercise 14 in Section 5.1.]

**Solution:** Consider the map  $\phi: A_1 \times \cdots \times A_n \rightarrow (A_1/B_1) \times \cdots \times (A_n/B_n)$  defined by

$$\phi(a_1, a_2, \dots, a_n) = (a_1 + B_1, a_2 + B_2, \dots, a_n + B_n).$$

Note that this is a homomorphism of  $R$ -modules since it is  $R$ -linear in each coordinate. Indeed,

$$a_i + ra'_i + B_i = (a_i + B_i) + r(a'_i + B_i)$$

by definition of the quotient module  $A_i/B_i$ . Then consider the kernel of this map. If  $(a_1, \dots, a_n) \in \ker \phi$  we must have  $a_i + B_i = 0 + B_i$  for all  $i$ . That is, we must have  $a_i \in B_i$  and in particular  $(a_1, \dots, a_n) \in B_1 \times \cdots \times B_n$ . This condition is obviously necessary and sufficient to be in the kernel, and so the kernel is  $B_1 \times \cdots \times B_n$ . Also note that the map is surjective, with a preimage of  $(a_1 + B_1, \dots, a_n + B_n)$  being simply  $(a_1, \dots, a_n)$ . By the first isomorphism theorem we conclude that

$$\begin{aligned} (A_1 \times \cdots \times A_n)/(B_1 \times \cdots \times B_n) &= (A_1 \times \cdots \times A_n)/\ker \phi \\ &\cong \phi(A_1 \times \cdots \times A_n) \\ &= (A_1/B_1) \times \cdots \times (A_n/B_n) \end{aligned}$$

which proves the result.  $\square$

**Exercise 10.2.12.** Let  $I$  be a left ideal of  $R$  and let  $n$  be a positive integer. Prove

$$R^n/IR^n \cong R/IR \times \cdots \times R/IR \quad (n \text{ times})$$

where  $IR^n$  is defined as in Exercise 5 of Section 1. [Use the preceding exercise.]

**Solution:** By definition  $R^n = R \times \cdots \times R$  where the product is taken  $n$  times. Thus we only need to show that  $IR^n = (IR)^n$ , and the result will follow immediately from the previous problem. To prove this we show containment in both directions. Elements of  $IR^n$  are of the form  $a(r_1, \dots, r_n) = (ar_1, \dots, ar_n)$  where  $a \in I$ . Such elements are clearly in  $(IR)^n$  since elements in  $(IR)^n$  have the form  $(a_1r_1, \dots, a_nr_n)$  for  $a_i \in I$ . Thus we have  $IR^n \subseteq (IR)^n$  immediately.

To show that  $(IR)^n \subseteq IR^n$  consider an arbitrary element  $(a_1r_1, \dots, a_nr_n) \in (IR)^n$ . Notice that the tuple  $v_i = (0, \dots, a_ir_i, \dots, 0)$  which is zero in all coordinates but the  $i$ -th is in  $IR^n$  since it is just  $a_i(0, \dots, a_i, \dots, 0)$ . But  $IR^n$  is closed under finite sums, and so we can write

$$(a_1r_1, \dots, a_nr_n) = \sum_{i=1}^n v_i \in IR^n.$$

This proves that  $(IR)^n \subseteq IR^n$ , and so we conclude the desired result. As an interesting aside, I believe this also holds when the product is infinite since we only allow finitely many nonzero coordinates.  $\square$

**Exercise 10.2.13.** Let  $I$  be a nilpotent ideal in a commutative ring  $R$  (cf. Exercise 37, 7.3), let  $M$  and  $N$  be  $R$ -modules and let  $\phi : M \rightarrow N$  be an  $R$ -module homomorphism. Show that if the induced map  $\bar{\phi} : M/IM \rightarrow N/IN$  is surjective, then  $\phi$  is surjective.

**Solution:** *Note: I referred to <https://crazyproject.wordpress.com/aadf/#df-10> for the solution to this problem. Wrote my own version of the solution however.*

We will first prove that  $N = \phi(M) + I^k N$  for all  $k$ , independent of the fact that  $I$  is nilpotent. Consider the following diagram:

$$\begin{array}{ccc} M & \xrightarrow{\phi} & N \\ \pi_M \downarrow & & \downarrow \pi_N \\ M/IM & \xrightarrow{\bar{\phi}} & N/IN \end{array}$$

Above we have  $\pi_M$  and  $\pi_N$  as projection mod  $IM$  and  $IN$  respectively. This diagram commutes by virtue of  $\bar{\phi}$  being the induced map. We begin by showing that  $N = \phi(M) + IN$ . Notice that  $N$  is clearly the preimage of  $N/IN$  under  $\pi_N$ . Also  $N/IN = \bar{\phi}(M/IM)$  and so any  $n + IN \in N/IN$  can be written as  $\phi(m) + IN$  for some  $m \in M$ . This implies that the preimage of  $N/IN$  under  $\pi_N$  will be  $\phi(M) + IN$ . Indeed,  $\pi_N(n) = \phi(m) + IN$  implies that  $n$  is the sum of something in  $\phi(M)$  and the kernel of  $\pi_N$  which is  $IN$ . So far we have shown that  $N = \phi(M) + IN$ .

To prove that  $N = \phi(M) + I^k N$  we use induction on  $k$ , where we have just proven the base case. For the inductive step, we have

$$N = \phi(M) + I^k N = \phi(M) + I^k(\phi(M) + IN) = \phi(M) + I^k \phi(M) + I^{k+1} N = \phi(M) + I^{k+1} N$$

where the last equality follows from the fact that  $I^k \phi(M) \subseteq \phi(M)$ . By induction we conclude that  $N = \phi(M) + I^k N$  for all  $k$ . Taking  $k$  large enough we have  $I^k = 0$  and so  $\phi(M) = N$  as desired.

It is illustrative to see the equality  $N = \phi(M) + I^k N$  for some non-nilpotent ideal. For an example, we take  $R = M = N = \mathbb{Z}$ . Let  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$  be the doubling map (i.e.  $\phi(z) = 2z$ ), which is indeed a homomorphism of  $\mathbb{Z}$  modules since it is a homomorphism of abelian groups. Notice that it is not surjective. For our ideal  $I$  we choose  $3\mathbb{Z}$ . Then our diagram of modules becomes

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\phi \text{ (doubling)}} & \mathbb{Z} \\ \pi \downarrow & & \downarrow \pi \\ \mathbb{Z}/3\mathbb{Z} & \xrightarrow{\bar{\phi} \text{ (doubling)}} & \mathbb{Z}/3\mathbb{Z} \end{array}$$

Now, the induced map is surjective since we have  $0 \mapsto 0$ ,  $1 \mapsto 2$  and  $2 \mapsto 1$ . Our result states that  $\mathbb{Z} = \phi(\mathbb{Z}) + 3^k \mathbb{Z}$  for all  $k$ . Since  $\phi(\mathbb{Z}) = 2\mathbb{Z}$  and  $2\mathbb{Z}$  and  $3^k \mathbb{Z}$  are always comaximal ideals, we see that the result holds. □

**Exercise 10.2.14.** Let  $R = \mathbb{Z}[x]$  be the ring of polynomials in  $x$  and let  $A = \mathbb{Z}[t_1, t_2, \dots]$  be the ring of polynomials in the independent indeterminates  $t_1, t_2, \dots$ . Define an action of  $R$  on  $A$  as follows: 1) let  $1 \in R$  act on  $A$  as the identity, 2) for  $n \geq 1$  let  $x^n \circ 1 = t_n$ , let  $x^n \circ t_i = t_{n+i}$  for  $i = 1, 2, \dots$ , and let  $x^n$  act as 0 on monomials in  $A$  of (total) degree at least two, and 3) extend  $\mathbb{Z}$ -linearly, i.e., so that the module axioms 2(a) and 2(c) are satisfied.

- (a) Show that  $x^{p+q} \circ t_i = x^p \circ (x^q \circ t_i) = t_{p+q+i}$  and use this show that under this action the ring  $A$  is a (unital)  $R$ -module.



- (b) Show that the map  $\phi : R \rightarrow A$  defined by  $\phi(r) = r \circ 1_A$  is an  $R$ -module homomorphism of the ring  $R$  into the ring  $A$  mapping  $1_R$  to  $1_A$ , but not a ring homomorphism from  $R$  to  $A$ .

**Solution:** (a)

We can compute directly that

$$x^{p+q} \circ t_i = t_{p+q+i} = x^p \circ t_{q+i} = x^p \circ (x^q \circ t_i)$$

as desired. We can use this to show that  $A$  is an  $R$ -module by considering arbitrary polynomials  $f = \sum_{i=0}^n a_i x^i$  and  $g = \sum_{j=0}^m b_j x^j$  in  $\mathbb{Z}[x]$ . To prove that  $fg \circ T = f \circ g \circ T$  for all  $T \in A$  it suffices to consider  $T = t_k$  since the action is by definition extended linearly and acts as zero on monomials of higher degree. We have that

$$\begin{aligned} fg \circ t_k &= \left( \sum_{i=0}^n a_i x^i \right) \left( \sum_{j=0}^m b_j x^j \right) \circ t_k \\ &= \left( \sum_{i=0}^{n+m} \left( \sum_{j=0}^i a_j b_{i-j} \right) x^i \right) \circ t_k \\ &= \sum_{i=0}^{n+m} \left( \sum_{j=0}^i a_j b_{i-j} \right) (x^i \circ t_k) && \text{By } R\text{-linearity} \\ &= \sum_{i=0}^{n+m} \left( \sum_{j=0}^i a_j b_{i-j} \right) t_{k+i} && \text{By definition of the action} \end{aligned}$$

Now, we can change the indices in this sum as follows. The various coefficients  $a_j b_{j-i}$  are all of the form  $a_{i'} b_{j'}$  where  $0 \leq i' \leq n$  and  $0 \leq j' \leq m$  (there are some additional pairs but for these we have  $a_j = 0$  or  $b_{j-i} = 0$ ). The coefficient  $a_{i'} b_{j'}$  appears as the coefficient of  $t_{k+i'+j'}$ . Hence this all simplifies as

$$\begin{aligned} fg \circ t_k &= \sum_{i=0}^n \sum_{j=0}^m a_i b_j t_{k+i+j} \\ &= \sum_{i=0}^n \sum_{j=0}^m a_i b_j x^i \circ (x^j \circ t_k) \\ &= \sum_{i=0}^n \sum_{j=0}^m a_i x_i \circ b_j (x^j \circ t_k) \\ &= \sum_{i=0}^n a_i x^i \circ \left( \sum_{j=0}^m b_j (x^j \circ t_k) \right) \\ &= \sum_{i=0}^n a_i x^i \circ (g \circ t_k) \\ &= f \circ (g \circ t_k). \end{aligned}$$

This shows that the action obeys axiom 2(b) for modules. We already know it satisfies the other axioms so  $A$  is indeed an  $R$ -module. That the action is unital follows directly from the definition

since  $1 \in R$  acts as identity. Thus  $A$  is a unital  $R$ -module as desired.

(b)

This map is naturally a homomorphism of the abelian groups since

$$\phi(r_1 + r_2) = (r_1 + r_2) \circ 1_A = r_1 \circ 1_A + r_2 \circ 1_A = \phi(r_1) + \phi(r_2).$$

Indeed this is an example of the maps  $\phi_a$  described in the solution to Problem 10.2.9. It maps  $1_R$  to  $1_A$  since the module action is unital.

To see that this is not a ring homomorphism, consider the image of  $x^2$ . We have that  $\phi(x^2) = t_2$ . But  $\phi(x)\phi(x) = t_1^2 \neq t_2$  so the map is not a ring homomorphism.  $\square$

### 10.3 Generation of Modules, Direct Sums, and Free Modules

In these exercises  $R$  is a ring with 1 and  $M$  is a left  $R$ -module.

**Exercise 10.3.1.** Prove that if  $A$  and  $B$  are sets of the same cardinality, then the free modules  $F(A)$  and  $F(B)$  are isomorphic.

**Solution:** Let  $\phi : A \rightarrow B$  be a bijection and  $\phi^{-1}$  be its inverse. Then Theorem 6 tells us that there exist unique  $R$ -module homomorphisms  $\Phi : F(A) \rightarrow F(B)$  and  $\Phi^{-1} : F(B) \rightarrow F(A)$  so that  $\Phi$  agrees with  $\phi$  on  $A$  and  $\Phi^{-1}$  agrees with  $\phi^{-1}$  on  $B$ . We claim that  $\Phi$  is an  $R$ -module isomorphism. It is clear that  $\Phi^{-1} \circ \Phi$  is identity on  $F(A)$  and so  $\Phi$  must be injective. On the other hand  $\Phi \circ \Phi^{-1}$  is identity on  $F(B)$  which means that  $\Phi$  must be surjective. Hence  $\Phi$  is an isomorphism, proving the result.  $\square$

**Exercise 10.3.2.** Assume  $R$  is commutative. Prove that  $R^n \cong R^m$  if and only if  $n = m$ , i.e., two free  $R$ -modules of finite rank are isomorphic if and only if they have the same rank. [Apply Exercise 12 of Section 2 with  $I$  a maximal ideal of  $R$ . You may assume that if  $F$  is a field, then  $F^n \cong F^m$  if and only if  $n = m$ , i.e. two finite dimensional vector spaces over  $F$  are isomorphic if and only if they have the same dimension — this will be proved later in Section 11.1]

**Solution:** ( $\Leftarrow$ ) If the modules have the same rank then they are isomorphic by the previous problem together with the result that any free module of rank  $n$  is free over its basis.

( $\Rightarrow$ ) We begin by proving the following general fact. If  $M \cong N$  as  $R$ -modules and  $I$  is an ideal of  $R$ , then  $M/IM \cong N/IN$ . To prove this let  $\phi : M \rightarrow N$  be an  $R$ -module isomorphism and consider its induced map  $\bar{\phi} : M/IM \rightarrow N/IN$  which maps  $m + IM \mapsto \phi(m) + IN$ . This map is well defined since we are taking a quotient of each module by the action of the same ideal. This map is surjective since if  $n + IN \in N/IN$  it has as a preimage  $\phi^{-1}(n) + IM \in M/IM$ . On the other hand it is well defined to talk about the induced inverse  $\bar{\phi}^{-1} : N/IN \rightarrow M/IM$ . One can observe that  $\bar{\phi}^{-1} \circ \bar{\phi}$  acts as identity on  $M/IM$  since

$$\bar{\phi}^{-1}(\bar{\phi}(m + IM)) = \bar{\phi}^{-1}(\phi(m) + IN) = \phi^{-1}(\phi(m)) + IM = m + IM.$$

Hence  $\bar{\phi}$  must be injective. We conclude that  $\bar{\phi}$  is an isomorphism.

Now suppose that  $R^n \cong R^m$ . Letting  $I$  be a maximal ideal, we have from 10.2.12 that

$$(R/IR)^n \cong R^n/IR^n \cong R^m/IR^m \cong (R/IR)^m$$

where the middle isomorphism is the one induced from  $R^n \cong R^m$  when modding out by the action of  $I$ . But this says that two vector spaces of dimension  $m$  and  $n$  respectively are isomorphic, and hence  $m = n$ . This proves the result.  $\square$

**Exercise 10.3.3.** Show that the  $F[x]$ -modules in Exercises 18 and 19 of Section 1 are both cyclic.

**Solution:** **Exercise 18:** This module is  $V = \mathbb{R}^2$  with the action of  $x$  being given by the linear transformation that rotates by  $\pi/2$ . We notice that  $V$  is generated by  $(1, 0)$  since we have  $x \cdot (1, 0) = (0, 1)$  and  $\{(1, 0), (0, 1)\}$  spans  $\mathbb{R}^2$  over  $\mathbb{R}$ , which is a subring of  $\mathbb{R}[x]$ . In fact we could choose any nonzero vector and  $V$  would be cyclicly generated by it.

**Exercise 19:** Again the module if  $V = \mathbb{R}^2$ , but now the action of  $x$  is given by projection onto the  $y$ -axis. In this case we see that  $V$  is not cyclicly generated by  $(1, 0)$  since the projection of this is just the zero vector. However,  $V$  is generated by  $(1, 1)$  since  $x \cdot (1, 1) = (0, 1)$  which is linearly independent from  $(1, 1)$ . Hence together  $(1, 1)$  and  $x \cdot (1, 1)$  span  $V$  over  $\mathbb{R}$  and since  $\mathbb{R} \subseteq \mathbb{R}[x]$  we see that  $(1, 1)$  generated  $V$ . □

**Exercise 10.3.4.** An  $R$ -module  $M$  is called a *torsion* module if for each  $m \in M$  there is a nonzero element of  $r \in R$  such that  $rm = 0$ , where  $r$  may depend on  $m$  (i.e.,  $M = \text{Tor}(M)$  in the notation of Exercise 8 of Section 1). Prove that every finite abelian group is a torsion  $\mathbb{Z}$ -module. Give an example of an infinite abelian group that is a torsion  $\mathbb{Z}$ -module.

**Solution:** Let  $G$  be an abelian group. Then the nonzero element  $|G| \in \mathbb{Z}$  annihilates  $G$  and we conclude that  $G$  is a torsion module.

For an example of an infinite abelian group one can consider  $\mathbb{Q}/\mathbb{Z}$ . Every element has finite order and hence is annihilated by some integer. A less interesting example is any infinite product of finite abelian groups. □

**Exercise 10.3.5.** Let  $R$  be an integral domain. Prove that every finitely generated torsion  $R$ -module has a nonzero annihilator i.e., there is a nonzero element  $r \in R$  such that  $rm = 0$  for all  $m \in M$  — here  $r$  does not depend on  $m$  (the annihilator of a module was defined in Exercise 9 of Section 1). Give an example of a torsion  $R$ -module whose annihilator is the zero ideal.

**Solution:** Let  $M = RA$  for a finite set  $\{a_1, \dots, a_n\}$ . For each  $a_i$  let  $r_i \neq 0$  be such that  $r_i a_i = 0$ . We claim that  $r = r_1 r_2 \cdots r_n$  is a nonzero element of the annihilator of  $M$  in  $R$ . That  $r \neq 0$  follows from the fact that  $R$  is an integral domain. To see that  $r$  is in the annihilator of  $M$  notice that  $r$  annihilates each  $a_i$  by the commutativity of  $R$ . Since  $r$  annihilates a generating set for  $M$  it must annihilate  $M$ , proving the result.

For an example where the annihilator is zero and the module is still torsion, consider the group  $G$  which is the product of  $\mathbb{Z}/n\mathbb{Z}$  for all  $n \geq 2$ , considered as a  $\mathbb{Z}$ -module. Every element is annihilated by the least common multiple of its nonzero components, but no nonzero integer can annihilate every element of  $G$  simultaneously. □

**Exercise 10.3.6.** Prove that if  $M$  is a finitely generated  $R$ -module that is generated by  $n$  elements then every quotient of  $M$  may be generated by  $n$  (or fewer) elements. Deduce that quotients of cyclic modules are cyclic.

**Solution:** Let  $\{a_1, \dots, a_n\}$  be a generating set for an  $R$ -module  $M$ . Then we claim that  $\{a_1 + N, \dots, a_n + N\}$  generates  $M/N$  as an  $R$ -module. Indeed, notice that any  $m + N \in M/N$  can be written as

$$m + N = \left( \sum r_i a_i \right) + N = \sum r_i (a_i + N)$$

proving the result. Hence the quotient of a cyclic module can be generated by 1 or 0 elements and is again cyclic. □

**Exercise 10.3.7.** Let  $N$  be a submodule of  $M$ . Prove that if both  $M/N$  and  $N$  are finitely generated then so is  $M$ .

**Solution:** Let  $\{a_1, \dots, a_n\}$  be a finite generating set for  $N$  and let  $\{b_1 + N, \dots, b_m + N\}$  be a finite generating set for  $M/N$ . We claim that the set

$$A = \{a_1, \dots, a_n, b_1, \dots, b_m\}$$

generates  $M$  as an  $R$ -module. Let  $\pi : M \rightarrow M/N$  be the natural projection map. For an arbitrary  $m \in M$ , let  $r_1, \dots, r_m$  be such that

$$m + N = \sum r_i(b_i + N) = \left(\sum r_i b_i\right) + N$$

Now notice that  $m - \sum r_i b_i$  must be in the kernel of  $\pi$ , i.e. in  $N$ . Then there must exist  $s_1, \dots, s_n$  so that

$$m - \sum r_i b_i = \sum s_j a_j$$

which implies

$$m = \sum r_i b_i + \sum s_j a_j \in RA.$$

Hence  $RA = M$  and  $A$  is a finite generating set for  $M$ . This proves the result.  $\square$

**Exercise 10.3.8.** Let  $S$  be the collection of sequences  $(a_1, a_2, a_3, \dots)$  of integers  $a_1, a_2, a_3, \dots$  where all but finitely many of the  $a_i$  are 0 (called the *direct sum* of infinitely many copies of  $\mathbb{Z}$ ). Recall that  $S$  is a ring under componentwise addition and multiplication and  $S$  does not have a multiplicative identity — cf. Exercise 20, Section 7.1. Prove that  $S$  is not finitely generated as a module over itself.

**Solution:** Given any finite set  $A = \{a_1, \dots, a_n\}$  let  $n_i$  be an integer such that  $N > n_i$  implies that the  $N$ -th component of  $a_i$  is zero. Taking the maximum  $M$  of all  $n_i$  we see that every  $a_i$  is zero past index  $M$ . Hence the set  $A$  does not generate any list which is nonzero after  $M$  and  $A$  does not generate  $S$  as a module.  $\square$

**Exercise 10.3.9.** An  $R$ -module  $M$  is called *irreducible* if  $M \neq 0$  and if 0 and  $M$  are the only submodules of  $M$ . Show that  $M$  is irreducible if and only if  $M \neq 0$  and  $M$  is a cyclic module with any nonzero element as a generator. Determine all the irreducible  $\mathbb{Z}$ -modules.

**Solution:** ( $\Rightarrow$ ) Suppose that  $M$  is irreducible. We know by definition  $M \neq 0$ . Taking some nonzero  $m \in M$ , we see that  $Rm$  is a nonzero submodule of  $M$ , and so  $Rm = M$ . This proves that  $M$  is generated by any nonzero element.

( $\Leftarrow$ ) Suppose  $M \neq 0$  and  $M$  is cyclic with any nonzero element as a generator. Then let  $N \subseteq M$  be any nonzero submodule of  $M$ . Let  $n \in N$  be nonzero and notice then that  $M = Rn \subseteq N$  and so  $N = M$ . This proves that the only nonzero submodule of  $M$  is  $M$  itself and so  $M$  is irreducible.

To classify all irreducible  $\mathbb{Z}$ -modules, we need only consider cyclic modules. If a cyclic module is not a torsion module it is isomorphic to  $\mathbb{Z}$ . But this is not irreducible since it contains a submodule isomorphic to  $2\mathbb{Z}$ . This leaves cyclic torsion modules of  $\mathbb{Z}$ . These are simply finite cyclic groups. Among these we see that the only irreducible ones are  $\mathbb{Z}/p\mathbb{Z}$  for some prime  $p$ .  $\square$

**Exercise 10.3.10.** Assume  $R$  is commutative. Show that an  $R$ -module  $M$  is irreducible if and only if  $M$  is isomorphic (as an  $R$ -module) to  $R/I$  where  $I$  is a maximal ideal of  $R$ . [By the previous exercise, if  $M$  is irreducible then there is a natural map  $R \rightarrow M$  defined by  $r \mapsto rm$  where  $m$  is any fixed nonzero element of  $M$ .]

**Solution:** ( $\Rightarrow$ ) Suppose that  $M$  is an irreducible  $R$ -module and fix some nonzero  $m \in M$ . We know that  $Rm = M$ . Let  $\phi : R \rightarrow M$  be the map  $r \mapsto rm$ . This is certainly a homomorphism of  $R$ -modules and furthermore it is surjective. Thus we have  $M \cong R/\ker \phi$ . If we can show  $\ker \phi$  (as a submodule of  $R$ ) is a maximal ideal of  $R$  then we are done. First by virtue of being a submodule of the commutative ring  $R$  we know that  $\ker \phi$  is an ideal.

Next notice that  $\ker \phi$  is exactly the annihilator of  $m$  (and hence  $M$ ) in  $R$ . Thus any ideal  $J$  strictly containing  $\ker \phi$  must contain some  $r$  so that  $rm \neq 0$ . But then we have that  $JM \neq 0$  and so  $JM = M$ . This means that  $J$  contains some element  $s$  so that  $sm = m$ , or equivalently  $(s - 1)m = 0$ . We conclude that  $s - 1 \in \ker \phi$ . But  $\ker \phi \subseteq J$  and so we have  $s, s - 1 \in J$  which means  $1 \in J$ . We conclude that  $J = R$  and so  $I$  is maximal. This proves the result.

( $\Leftarrow$ ) Suppose  $M \cong R/I$  for a maximal ideal  $I$ . We aim to show that  $Rm = M$  for all nonzero  $m \in M$ . We can write any nonzero  $m \in M$  as  $a + I$  via the isomorphism between  $M$  and  $R/I$  where  $a \notin I$ . But then  $R(a + I) = Ra + RI = Ra + I$ . Notice that  $Ra + I$  is an ideal strictly containing  $I$  since it contains  $a$ , and so  $Ra + I = R$  since  $I$  is maximal. We conclude that  $R(a + I) = R/I$  in the module  $R/I$ , proving the result.  $\square$

**Exercise 10.3.11.** Show that if  $M_1$  and  $M_2$  are irreducible  $R$ -modules, then any nonzero  $R$ -module homomorphism from  $M_1$  to  $M_2$  is an isomorphism. Deduce that if  $M$  is irreducible then  $\text{End}_R(M)$  is a division ring (this result is called *Schur's Lemma*). [Consider the kernel and the image.]

**Solution:** Let  $\phi : M_1 \rightarrow M_2$  be a nonzero  $R$ -module homomorphism. We know that  $\ker \phi$  is not all of  $M_1$ , and hence  $\ker \phi = \{0\}$ . On the other hand we know  $\phi(M_1) \neq \{0\}$  and so it is all of  $M_2$ . This tells us that  $\phi$  is injective and surjective, and so we conclude that  $\phi$  is an isomorphism.  $\square$

**Exercise 10.3.12.** Let  $R$  be a commutative ring and let  $A, B$  and  $M$  be  $R$ -modules. Prove the following isomorphisms of  $R$ -modules:

$$(a) \text{ Hom}_R(A \times B, M) \cong \text{Hom}_R(A, M) \times \text{Hom}_R(B, M)$$

$$(b) \text{ Hom}_R(M, A \times B) \cong \text{Hom}_R(M, A) \times \text{Hom}_R(M, B).$$

**Solution:** (a)

Let  $(\phi, \psi) \in \text{Hom}_R(A, M) \times \text{Hom}_R(B, M)$ . We claim that the map sending  $(\phi, \psi) \mapsto \Phi$  where  $\Phi$  acts as  $\phi$  in the first coordinate and  $\psi$  in the second is an isomorphism of  $R$ -modules. More specifically, we define  $\Phi(a, b) = \phi(a) + \psi(b)$ . First we show that it is even a well defined map between the hom-sets of concern, namely that  $\Phi \in \text{Hom}_R(A \times B, M)$ . This is straightforward since if  $(a, b), (a', b') \in A \times B$  and  $r \in R$  then we have

$$\begin{aligned} \Phi((a, b) + r(a', b')) &= \Phi(a + ra', b + rb') \\ &= \phi(a + ra') + \psi(b + rb') \\ &= \phi(a) + \psi(b) + r\phi(a') + r\psi(b') \\ &= \Phi(a, b) + r\Phi(a', b'). \end{aligned}$$

Now we need to show that  $(\phi, \psi) \mapsto \Phi$  is a homomorphism of  $R$ -modules. Suppose we have  $(\phi, \psi) \mapsto \Phi$  and  $(\phi', \psi') \mapsto \Phi'$ . It is clear that  $(\phi + r\phi', \psi + r\psi')$  maps to  $\Phi + r\Phi'$  and so we see that the map is an  $R$ -module homomorphism.

Injectivity is straightforward since the only map  $\Phi$  that can act as zero in both coordinates comes from  $\phi = \psi = 0$ . For surjectivity, notice that any  $\Phi$  acts as an  $R$ -module homomorphism in each coordinate. In particular, if we define  $\Phi_A : A \rightarrow M$  by  $\Phi_A(a) = \Phi(a, 0)$  and  $\Phi_B$  symmetrically then we see that  $(\Phi_A, \Phi_B) \mapsto \Phi$ . Hence the map is surjective and we conclude the desired

isomorphism.

(b)

The proof here is essentially the same as (a): the isomorphism is given by decomposing any homomorphism in  $\text{Hom}_R(M, A \times B)$  into its coordinate pieces on  $A$  and  $B$ . In particular, we associate  $\Phi \in \text{Hom}_R(M, A \times B)$  with the pair  $(\phi, \psi)$  where  $\phi(a)$  is the first coordinate of  $\Phi(a)$  and  $\psi(b)$  is the second coordinate of  $\Phi(b)$ .  $\square$

**Exercise 10.3.13.** Let  $R$  be a commutative ring and let  $F$  be a free  $R$ -module of finite rank. Prove the following isomorphism of  $R$ -modules:  $\text{Hom}_R(F, R) \cong F$ .

**Solution:** Write  $F \cong R^n$ . Applying the result of the previous exercise we have that

$$\begin{aligned} \text{Hom}_R(F, R) &\cong \text{Hom}_R(R^n, R) \\ &\cong \text{Hom}_R(R, R)^n \\ &\cong R^n \\ &\cong F. \end{aligned}$$

Note that above we have used the fact that  $\text{Hom}_R(R, R) \cong R$ , which was proven in another exercise.  $\square$

**Exercise 10.3.14.** Let  $R$  be a commutative ring and let  $F$  be the free  $R$ -module of rank  $n$ . Prove that  $\text{Hom}_R(F, M) \cong M \times \cdots \times M$  ( $n$  times). [Use Exercise 9 in Section 2 and Exercise 12.]

**Solution:** Recall from 10.2.9 that  $\text{Hom}_R(R, M) \cong M$  since every homomorphism is determined by its value on  $1 \in R$ . Hence we have (similar to the previous exercise) that

$$\begin{aligned} \text{Hom}_R(F, M) &\cong \text{Hom}_R(R^n, M) \\ &\cong \text{Hom}_R(R, M)^n \\ &\cong M^n. \end{aligned}$$

This is exactly what we hoped to show. Note that the previous exercise is in fact a special case of this.  $\square$

**Exercise 10.3.15.** An element  $e \in R$  is called a *central idempotent* if  $e^2 = e$  and  $er = re$  for all  $r \in R$ . If  $e$  is a central idempotent in  $R$ , prove that  $M = eM \oplus (1 - e)M$ . [Recall Exercise 14 in Section 1.]

**Solution:** We must show two things. First, that  $M$  is generated by  $eM$  together with  $(1 - e)M$ . Second, that  $eM \cap (1 - e)M = \{0\}$ .

For the first statement, notice that since  $e$  is in the center of  $R$  the subsets  $eM = \{em \mid m \in M\}$  and  $(1 - e)M = \{(1 - e)m \mid m \in M\}$  are indeed submodules of  $M$ . Then let  $m \in M$  be arbitrary and notice that

$$m = 1 \cdot m = (e + (1 - e)) \cdot m = e \cdot m + (1 - e) \cdot m$$

and so  $eM$  together with  $(1 - e)M$  generates  $M$ . Note this is independent of  $e$  being central idempotent.

To prove that the sum of  $eM$  and  $(1 - e)M$  is direct, suppose that  $m \in eM \cap (1 - e)M$ . Then there exist  $m_1, m_2 \in M$  so that

$$em_1 = m = (1 - e)m_2.$$

But acting on the left and right quantities above by  $e$  yields

$$e^2 m_1 = (e - e^2) m_2$$

which simplifies to  $em_1 = 0$  since  $e - e^2 = 0$ . But this tells us immediately that  $m = 0$ , so the sum of  $eM$  and  $(1 - e)M$  is direct.  $\square$

The next two exercises establish the Chinese Remainder Theorem for modules (cf. Section 7.6).

**Exercise 10.3.16.** For any ideal  $I$  of  $R$  let  $IM$  be the submodule defined in Exercise 5 of Section 1. Let  $A_1, \dots, A_k$  be any ideals in the ring  $R$ . Prove that the map

$$M \rightarrow M/A_1M \times \cdots \times M/A_kM \quad \text{defined by} \quad m \mapsto (m + A_1M, \dots, m + A_kM)$$

is an  $R$ -module homomorphism with kernel  $A_1M \cap A_2M \cap \cdots \cap A_kM$ .

**Solution:** Suppose that  $m$  is in the kernel of this map. Then  $m + A_iM$  is zero for all  $A_i$  in the quotient. In particular  $m \in A_iM$  for all  $i$ . Since this condition is necessary and sufficient we conclude that the kernel is indeed  $A_1M \cap A_2M \cap \cdots \cap A_kM$ .  $\square$

**Exercise 10.3.17.** In the notation of the preceding exercise, assume further that the ideals  $A_1, \dots, A_k$  are pairwise comaximal (i.e.  $A_i + A_j = R$  for all  $i \neq j$ ). Prove that

$$M/(A_1 \cdots A_k)M \cong M/A_1M \times \cdots \times M/A_kM.$$

[See the proof of the Chinese Remainder Theorem for rings in Section 7.6.]

**Solution:** We will show that  $A_1M \cap \cdots \cap A_kM = (A_1 \cdots A_k)M$ . First note that  $A_1 \cdots A_k \subseteq A_i$  for all  $i$  since each  $A_i$  is an ideal and hence absorbs multiplication by other ideals on both the left and right. This tells us that inclusion in the  $\supseteq$  direction holds.

For inclusion in the other direction, we will proceed by induction on  $k$ . For  $k = 1$  we have only one ideal and the inclusion is obvious. For the inductive step we assume that  $A_2M \cap \cdots \cap A_kM = (A_2 \cdots A_k)M$ . From this we have that  $A_1M \cap A_2M \cap \cdots \cap A_kM = A_1M \cap (A_2 \cdots A_k)M$ . Now notice that  $A_1$  and  $A_2 \cdots A_k$  are comaximal. Indeed, for each  $2 \leq i \leq k$  we are guaranteed that there is some  $a_i \in A_1$  and  $a'_i \in A_i$  so that  $1 = a_i + a'_i$ . We then have that  $1 = (a_1 + a'_1)(a_2 + a'_2) \cdots (a_k + a'_k)$  is an element of  $A_1 + (A_2 \cdots A_k)$  since every term in the expanded product is a product of something in  $A_1$  with something in  $A_2 \cdots A_k$ . This tells us that  $A_1$  and  $A_2 \cdots A_k$  are comaximal and so we can write  $1 = a + a'$  with  $a \in A_1$  and  $a' \in A_2 \cdots A_k$ . But this means that  $A_1 \cap A_2 \cap \cdots \cap A_k \subseteq A_1 A_2 \cdots A_k$  since for any  $b$  in the intersection we have  $b = 1b = (a + a')b = ab + a'b = ab + ba'$  which is in  $A_1(A_2 \cdots A_k)$  since  $a \in A_1$ ,  $a' \in A_2 \cdots A_k$  and  $b$  is in both. (Here we have assumed  $R$  is commutative to write  $a'b = ba'$ , which seems necessary.)

Putting all of this together, we may write

$$\begin{aligned} A_1M \cap A_2M \cap \cdots \cap A_kM &= A_1M \cap (A_2 \cdots A_k)M \\ &\subseteq A_1M \cap (A_2 \cap A_3 \cap \cdots \cap A_k)M && \text{We are intersecting with the} \\ & && \text{larger submodule } (A_2 \cdots A_k)M. \\ &\subseteq A_1M \cap A_2M \cap \cdots \cap A_kM && (A \cap B)M \subseteq AM \cap BM \text{ in general.} \end{aligned}$$

This concludes the proof that  $A_1M \cap \cdots \cap A_kM = (A_1 \cdots A_k)M$ .

Now we show that the map defined in the previous problem is surjective. Call this map  $\phi$  for convenience. We will proceed by induction on  $k$ . When  $k = 2$  we have by the comaximality of  $A_1$  and  $A_2$  that there are some  $a_1 \in A_1$  and  $a_2 \in A_2$  so that  $1 = a_1 + a_2$ . To show the map is surjective it suffices to demonstrate a preimage for  $(m + A_1, 0)$  and  $(0, m + A_2)$  for all  $m \in M$ . For this, notice that

$$\phi(a_1 m) = (0, a_1 m + A_2) = (0, (1 - a_2)m + A_2) = (0, m - a_2 m + A_2) = (0, m + A_2)$$

and similarly

$$\phi(a_2 m) = (a_2 m + A_1, 0) = ((1 - a_1)m + A_1, 0) = (m - a_1 m + A_1, 0) = (m + A_1, 0).$$

Hence the map is surjective in this base case. For the inductive step, the inductive hypothesis tells us that the map is surjective onto all elements of the form  $(m_1 + A_1, m_2 + A_2 M, \dots, a_k + A_k M)$  where all values of  $m_2, \dots, m_k$  are achieved but possibly not all values of  $m_1$ . To show that the map is surjective it thus suffices to find preimages for  $(m_1 + A_1, 0, \dots, 0)$  for all possible  $m_1$ . Recall we showed in earlier in our solution that  $A_1$  and  $A_2 \cdots A_k$  are comaximal. Hence we can write  $1 = a + a'$  for  $a \in A_1$  and  $a' \in A_2 \cdots A_k$ . Then notice that

$$\begin{aligned} \phi(a' m_1) &= (a' m_1 + A_1 M, a' m_1 + A_2 M, \dots, a' m_1 + A_k M) \\ &= (m_1 - a m_1 + A_1 M, 0, \dots, 0) && \text{Since } a' \in A_i \text{ for all } 2 \leq i \leq k \\ &= (m_1 + A_1 M, 0, \dots, 0). \end{aligned}$$

Hence the image of  $M$  under  $\phi$  is all of  $M/A_1 M \times \cdots \times M/A_k M$ . Now, by the first isomorphism theorem for modules we have that

$$M/\ker \phi \cong M/A_1 M \times \cdots \times M/A_k M$$

But  $\ker \phi = A_1 M \cap \cdots \cap A_k M$ , and earlier in the solution we proved that  $A_1 M \cap \cdots \cap A_k M = (A_1 \cdots A_k)M$ . We conclude that

$$M/(A_1 \cdots A_k) \cong M/A_1 M \times \cdots \times M/A_k M$$

as desired. □

**Exercise 10.3.18.** Let  $R$  be a Principal Ideal Domain and let  $M$  be an  $R$ -module that is annihilated by the nonzero, proper ideal  $(a)$ . Let  $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$  be the unique factorization of  $a$  into distinct prime powers in  $R$ . Let  $M_i$  be the annihilator of  $p_i^{\alpha_i}$  in  $M$ , i.e.  $M_i$  is the set  $\{m \in M \mid p_i^{\alpha_i} m = 0\}$ —called the  $p_i$ -primary component of  $M$ . Prove that

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_k.$$

**Solution:** We first claim that the sum of the various  $M_i$  is direct. To show this we prove that  $M_i \cap (\sum_{j \neq i} M_j) = 0$  for all  $i$ . Let  $m_i \in M_i$  and assume  $m_i \in \sum_{j \neq i} M_j$ . Then we see that  $m_i$  is annihilated by  $p_i^{\alpha_i}$  as well as  $\prod_{j \neq i} p_j^{\alpha_j}$ . Hence these are both elements of the ideal annihilating  $m_i$ . This ideal then contains their greatest common divisor, which is clearly 1 since  $p_i^{\alpha_i}$  does not share any prime factors with  $\prod_{j \neq i} p_j^{\alpha_j}$ . Thus we have  $m_i = 1m_i = 0$ , proving that the sum of the  $M_i$  is direct.

It remains to show that the sum of the various  $M_i$  is in fact all of  $M$ . We have from the previous problem that

$$M \cong M/(a)M \cong M/(p_1^{\alpha_1})M \times M/(p_2^{\alpha_2})M \times \cdots \times M/(p_k^{\alpha_k})M$$



since  $(a)M = 0$  and the various ideals  $(p_i^{\alpha_i})$  are comaximal by virtue of the various  $p_i$  being distinct prime factors. In the previous problem we saw that the isomorphism is given by the natural map

$$\phi(m) = (m + p_1^{\alpha_1}M, m + p_2^{\alpha_2}M, \dots, m + p_k^{\alpha_k}M).$$

We want to show that this map, when restricted to the direct sum  $M_1 \oplus \dots \oplus M_k \subseteq M$  is still surjective. In fact it suffices to show that the inverse of  $\phi$  maps into this direct sum. To prove this we need only show that the tuple with  $m + (p_i^{\alpha_i})M$  in the  $i$ -th component and zeroes elsewhere maps into the direct sum of the  $M_i$ , since the set of all vectors of this form generate the direct product. The image of such a tuple will be some  $m' \in M$  which is zero modulo  $p_j^{\alpha_j}M$  for all  $j \neq i$ . In particular, we have that  $m' = q_i m''$  for some  $m'' \in M$ , where  $q_i = a/p_i^{\alpha_i}$ . But then clearly  $m' \in M_i$  since

$$p_i^{\alpha_i}m = p_i^{\alpha_i}q_i m'' = am'' = 0.$$

This proves that  $\phi^{-1}$  maps to values in the direct sum of the various  $M_i$  and so the direct sum is itself  $M$ . This concludes the proof.  $\square$

**Exercise 10.3.19.** Show that if  $M$  is a finite abelian group of order  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  then, considered as a  $\mathbb{Z}$ -module,  $M$  is annihilated by  $(a)$ , the  $p_i$ -primary component of  $M$  is the unique Sylow  $p_i$ -subgroup of  $M$  and  $M$  is isomorphic to the direct product of its Sylow subgroups.

**Solution:** That  $M$  is annihilated by  $a$  follows immediately from Lagrange's theorem. We know that Sylow  $p_i$ -subgroups are unique since  $M$  is an abelian group and all Sylow subgroups are conjugates of one another. This leaves that the  $p_i$ -primary component is indeed a Sylow  $p_i$ -subgroup. Let  $H_i$  be the Sylow  $p_i$ -subgroup guaranteed by the Sylow theorems. Each element in this group has order dividing  $p_i^{\alpha_i}$ , since this is the order of  $H_i$  and so we see right away that  $H_i \subseteq M_i$  where  $M_i$  is the annihilator of  $p_i^{\alpha_i}$  as described in the previous problem statement. To prove containment in the other direction, suppose  $m \in M$  is annihilated by  $p_i^{\alpha_i}$ . Then its order is a power of  $p_i$  and so it must be in  $H_i$ . Hence the Sylow  $p_i$ -subgroups are exactly the  $p_i$ -primary components of  $M$ . By the previous problem we conclude that  $M$  is the direct sum of its Sylow  $p_i$ -subgroups.  $\square$

**Exercise 10.3.20.** Let  $I$  be a nonempty index set and for each  $i \in I$  let  $M_i$  be an  $R$ -module. The *direct product* of the modules  $M_i$  is defined to be their direct product as abelian groups (cf. Exercise 15 in Section 5.1) with the action of  $R$  componentwise multiplication. The *direct sum* of the modules  $M_i$  is defined to be the restricted direct product of the abelian groups  $M_i$  (cf. Exercise 17 in Section 5.1) with the action of  $R$  componentwise multiplication. In other words, the direct sum of the  $M_i$ 's is the subset of the direct product  $\prod_{i \in I} M_i$ , which consists of all elements  $\prod_{i \in I} m_i$  such that only finitely many of the components  $m_i$  are nonzero; the action of  $R$  on the direct product or direct sum is given by  $r \prod_{i \in I} m_i = \prod_{i \in I} r m_i$  (cf. Appendix I for the definition of the Cartesian products of infinitely many sets). The direct sum will be denoted by  $\oplus_{i \in I} M_i$ .

- (a) Prove that the direct product of the  $M_i$ 's is an  $R$ -module and the direct sum of the  $M_i$ 's is a submodule of their direct product.
- (b) Show that if  $R = \mathbb{Z}$ ,  $I = \mathbb{Z}^+$  and  $M_i$  is the cyclic group of order  $i$  for each  $i$ , then the direct sum of the  $M_i$ 's is not isomorphic to their direct product. [Look at torsion.]

**Solution:** (a)

We know already that the direct product of the  $M_i$  will be an abelian group. Thus we only have to

verify that the action of  $r$  satisfies the module axioms. If  $\prod_{i \in I} m_i$  and  $\prod_{i \in I} m'_i$  are two elements in  $\oplus_{i \in I} M_i$  then we observe that

$$\begin{aligned} r \left( \prod_{i \in I} m_i + \prod_{i \in I} m'_i \right) &= r \prod_{i \in I} (m_i + m'_i) \\ &= \prod_{i \in I} r(m_i + m'_i) \\ &= \prod_{i \in I} (rm_i + rm'_i) \\ &= \prod_{i \in I} rm_i + \prod_{i \in I} rm'_i \\ &= r \prod_{i \in I} m_i + r \prod_{i \in I} m'_i. \end{aligned}$$

If  $s \in R$  then we can also verify that

$$(sr) \prod_{i \in I} m_i = \prod_{i \in I} (sr)m_i = \prod_{i \in I} s(rm_i) = s \prod_{i \in I} rm_i = s \left( r \prod_{i \in I} m_i \right)$$

and furthermore

$$\begin{aligned} (s + r) \prod_{i \in I} m_i &= \prod_{i \in I} (s + r)m_i \\ &= \prod_{i \in I} (sm_i + rm_i) \\ &= \prod_{i \in I} sm_i + \prod_{i \in I} rm_i \\ &= s \prod_{i \in I} m_i + r \prod_{i \in I} m_i. \end{aligned}$$

Finally, if  $R$  has unity then we see the direct product is unital since  $1 \prod_{i \in I} m_i = \prod_{i \in I} 1m_i = \prod_{i \in I} m_i$ .

Next we show that the direct sum is a submodule. We know it is a subgroup, and so we only need to check it is invariant under the action of  $R$ . This is immediate because  $r \prod_{i \in I} m_i = \prod_{i \in I} rm_i$  will have no more nonzero terms than  $\prod_{i \in I} m_i$ , since  $r0 = 0$ .

(b)

We claim that the direct sum is a torsion module but the direct product is not. For any element  $\prod_{i \in I} m_i$  we see that it is annihilated by the product of the  $i$  for which  $m_i \neq 0$ . Hence the direct sum is torsion. Of course we cannot do this when there are infinitely many nonzero  $m_i$ . In particular the element  $\prod_{i \in I} 1$  in the direct product is not annihilated by any nonzero integer since no nonzero integer is congruent to zero mod every other integer.  $\square$

**Exercise 10.3.21.** let  $I$  be a nonempty index set and for each  $i \in I$  let  $N_i$  be a submodule of  $M$ . Prove that the following are equivalent:

- (i) the submodule of  $M$  generated by all the  $N_i$ 's is isomorphic to the direct sum of the  $N_i$ 's
- (ii) if  $\{i_1, i_2, \dots, i_k\}$  is any finite subset of  $I$  then  $N_{i_1} \cap (N_{i_2} + \dots + N_{i_k}) = 0$

- (iii) if  $\{i_1, i_2, \dots, i_k\}$  is any finite subset of  $I$  then  $N_{i_1} + \dots + N_{i_k} = N_{i_1} \oplus \dots \oplus N_{i_k}$
- (iv) for every element  $x$  of the submodule of  $M$  generated by the  $N_i$ 's there are unique elements  $a_i \in N_i$  for all  $i \in I$  such that all but a finite number of the  $a_i$  are zero and  $x$  is the (finite) sum of the  $a_i$ .

**Solution:** (Note: Referenced <https://crazyproject.wordpress.com/aadf/> to clarify details since it was not clear to me whether the direct sum of the  $N_i$ 's was internal or not.)

( $i \Rightarrow ii$ ) Suppose  $\sum_{i \in I} N_i \cong \oplus_{i \in I} N_i$  via the natural isomorphism (which we will denote  $\phi$ ) and let  $\{i_1, i_2, \dots, i_k\} \subseteq I$ . Then consider the intersection of the submodules  $N_{i_1}$  and  $(N_{i_2} + \dots + N_{i_k})$  of  $M$ . Let  $n$  be in this intersection. Then we know  $n = a_1$  for some  $a_1 \in N_{i_1}$  and also that  $n = \sum_{j=2}^k a_j$  for  $a_j \in N_{i_j}$ . Then  $a_1 - \sum_{j=2}^k a_j$  is in the kernel of  $\phi$  since it is zero. But its image under  $\phi$  maps  $a_1$  and each  $a_j$  to a separate coordinate, and hence each coordinate must be zero. In particular  $a_1$  and all  $a_j$  are zero. Hence  $n = 0$ .

( $ii \Rightarrow iii$ ) This is immediate since the property that  $N_{i_1} \cap (N_{i_2} + \dots + N_{i_k}) = 0$  is the definition of being an (internal) direct sum.

( $iii \Rightarrow iv$ ) Suppose  $x \in \sum_{i \in I} N_i$ . Then by definition of being generated by the  $N_i$  we know that there exists a finite collection of nonzero  $a_{i_1}, \dots, a_{i_k}$  with  $a_{i_j} \in N_{i_j}$  and

$$x = \sum_{j=1}^k a_{i_j}.$$

Since the sum of the  $N_{i_j}$  is direct we know this representation is unique within the module generated by the  $N_{i_j}$ . We must show it is unique overall. Given another representation of  $x$  as

$$x = \sum_{j=1}^{k'} a'_{i'_j}.$$

we consider it in the submodule generated by all  $N_{i_j}$  and  $N_{i'_j}$ . This is still a finite sum of submodules and so by (iii) we see that these representations must be the same. Hence the representation of  $x$  as a sum of elements in various  $N_{i_j}$  is unique.

( $iv \Rightarrow i$ ) Let  $\phi : \oplus_{i \in I} N_i \rightarrow \sum_{i \in I} N_i$  be the natural projection map. This is clearly a surjective  $R$ -module homomorphism, and we want to show it is injective. For any  $n \in \sum_{i \in I} N_i$  we have from (iv) a unique representation of it as a sum of finitely many nonzero  $a_i$  with  $a_i \in N_i$ . This is equivalent to  $n$  having a unique preimage under  $\phi$  since  $\phi$  is by definition the sum of components map. Hence  $\phi$  is injective, and an isomorphism.  $\square$

**Exercise 10.3.22.** Let  $R$  be a Principal Ideal Domain, let  $M$  be a torsion  $R$ -module (cf. Exercise 4) and let  $p$  be a prime in  $R$  (do not assume  $M$  is finitely generated, hence it need not have a nonzero annihilator — cf. Exercise 5). The  $p$ -primary component of  $M$  is the set of all elements of  $M$  that are annihilated by some positive power of  $p$ .

- (a) Prove that the  $p$ -primary component is a submodule. [See Exercise 13 in Section 1.]
- (b) Prove that this definition of  $p$ -primary component agrees with the one given in Exercise 18 when  $M$  has a nonzero annihilator.
- (c) Prove that  $M$  is the (possible infinite) direct sum of its  $p$ -primary components, as  $p$  runs over all primes of  $R$ .

**Solution:** (a)

Note that  $m$  is annihilated by some power of  $p$  if and only if it is annihilated by the principal ideal  $(p^k) = (p)^k$  for some  $k$ . Exercise 10.1.13 tells us immediately that the  $p$ -primary component is a submodule.

(b)

Suppose  $M$  has a nonzero annihilator generated by  $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ . Then we want to show that  $m$  is annihilated by some power of  $p_i$  if and only if it is annihilated by  $p_i^{\alpha_i}$ . The reverse implication is trivial, and so we show that if  $p_i^k m = 0$  then  $p_i^{\alpha_i} m = 0$ . Notice that  $(p_i^k)$  contains  $a$  and hence  $a$  is a multiple of  $p_i^k$ . In particular,  $k \leq \alpha_i$  and so  $p_i^{\alpha_i} m = p_i^{\alpha_i - k} p_i^k m = p_i^{\alpha_i - k} 0 = 0$ . This proves the desired statement.

(c)

We first show that every element of  $M$  can be written as a finite sum of  $p$ -primary elements. Given  $m \in M$  we know there is some nonzero  $r \in R$  so that  $rm = 0$  since  $M$  is a torsion module. Let  $r = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  be the unique factorization of  $r$  in the PID  $R$ . Then define  $q_i = \prod_{j \neq i} p_j^{\alpha_j}$  (that is  $q_i$  is  $r$  with  $p_i^{\alpha_i}$  removed as a factor). Notice that taken together all  $q_i$  have a gcd of one, and hence the ideal generated by them is all of  $R$ . This tells us that there exist  $r_1, \dots, r_k$  so that

$$1 = r_1 q_1 + \cdots + r_k q_k.$$

We then have for any  $m \in M$  that

$$m = 1m = r_1 q_1 m + r_2 q_2 m + \cdots + r_k q_k m.$$

Now notice that  $r_i q_i m$  is annihilated by  $p_i^{\alpha_i}$ , and in particular is in the  $p_i$ -primary component of  $M$ . This shows that the internal sum of all  $p$ -primary components is in fact  $M$ .

Next we show that the sum is direct. We will show in particular that condition (ii) given in Exercise 10.3.21 is satisfied by the various  $p$ -primary components. Suppose that  $M_1, \dots, M_k$  is a finite collection of distinct  $p$ -primary components, with associated primes  $p_1, \dots, p_k$ . We want to show that if  $m \in M_1$  and  $m \in \sum_{i=2}^k M_i$  then  $m$  is zero. Let  $p_1^{\alpha_1}$  be a power of  $p_1$  annihilating  $m$ . Then also write

$$m = m_2 + \cdots + m_k$$

with  $m_i \in M_i$  and let  $p_i^{\alpha_i}$  be a power of  $p_i$  annihilating  $m_i$ . Then notice that  $p = p_2^{\alpha_2} \cdots p_k^{\alpha_k}$  annihilates  $m$  since it annihilates each  $m_i$  in the sum. Now consider the ideal containing all elements of  $R$  that annihilate  $m$ . We see that  $p_1^{\alpha_1}$  and  $p$  are both in this ideal, and so must be their greatest common divisor, namely 1. Thus we have  $m = 1m = 0$ , as desired. This proves that the sum of all  $p$ -primary components is direct, and we conclude the desired result.  $\square$

**Exercise 10.3.23.** Show that any direct sum of free  $R$ -modules is free.

**Solution:** Let  $\{M_i\}_{i \in I}$  be a collection of free  $R$ -modules, each with basis  $A_i$ . We claim that  $\bigoplus_{i \in I} M_i$  is free over  $\bigcup_{i \in I} A_i$ . Letting  $m \in \bigoplus_{i \in I} M_i$  we know we can write  $m$  as a finite sum  $m = m_{i_1} + \cdots + m_{i_k}$  with  $m_{i_j} \in M_{i_j}$ . Furthermore this expression of  $m$  is unique since the coordinates in a direct sum are independent. But each  $m_{i_j}$  has a unique representation over the basis  $A_{i_j}$ . Hence we can express  $m$  over the basis  $\bigcup_{i \in I} A_i$ , and furthermore this representation of  $m$  is unique. This proves the result. Note that we relied on the direct *sum* structure (as opposed to direct product) so that we could write  $m$  as a finite sum of elements in the various  $M_i$ .  $\square$

**Exercise 10.3.24.** (*An arbitrary direct product of free modules need not be free*) For each positive integer  $i$  let  $M_i$  be the free  $\mathbb{Z}$ -module  $\mathbb{Z}$ , and let  $M$  be the direct product  $\prod_{i \in \mathbb{Z}^+} M_i$  (cf. Exercise 20). Each element of  $M$  can be written uniquely in the form  $(a_1, a_2, a_3, \dots)$  with  $a_i \in \mathbb{Z}$  for all  $i$ . Let  $N$  be the submodule of  $M$  consisting of all such tuples with only finitely many nonzero  $a_i$ . Assume  $M$  is a free  $\mathbb{Z}$  module with basis  $\mathcal{B}$ .

- (a) Show that  $N$  is countable.
- (b) Show that there is some countable subset  $\mathcal{B}_1$  of  $\mathcal{B}$  such that  $N$  is contained in the submodule,  $N_1$ , generated by  $\mathcal{B}_1$ . Show also that  $N_1$  is countable.
- (c) Let  $\overline{M} = M/N_1$ . Show that  $\overline{M}$  is a free  $\mathbb{Z}$ -module. Deduce that if  $\overline{x}$  is any nonzero element of  $\overline{M}$  then there are only finitely many distinct positive integers  $k$  such that  $\overline{x} = k\overline{m}$  for some  $m \in M$  (depending on  $k$ ).
- (d) Let  $\mathcal{S} = \{(b_1, b_2, b_3, \dots) \mid b_i = \pm i! \text{ for all } i\}$ . Prove that  $\mathcal{S}$  is uncountable. Deduce that there is some  $s \in \mathcal{S}$  with  $s \notin N_1$ .
- (e) Show that the assumption  $M$  is free leads to a contradiction: By (d) we may choose  $s \in \mathcal{S}$  with  $s \notin N_1$ . Show that for each positive integer  $k$  there is some  $m \in M$  with  $\overline{s} = k\overline{m}$ , contrary to (c). [Use the fact that  $N \subseteq N_1$ .]

**Solution:** (a)

We will show that  $N$  is a countable union of countable sets. For each  $i \in \mathbb{Z}_{\geq 0}$  define  $N_i$  to be the set of elements in  $N$  with nonzero entries only in indices less than or equal to  $i$ . Clearly  $N$  is the union of all  $N_i$ , of which there are countably many. To see that  $N_i$  is countable notice that it is (effectively) a finite product of countable sets, i.e.  $N_i = \mathbb{Z}^i$ , and hence is countable.

(b)

For each  $n \in N$ , we know that  $n$  can be expressed as an  $\mathbb{Z}$ -linear combination of a finite number of basis elements. For each  $n$  let  $\mathcal{B}_n$  be the set of these basis elements. Then the set  $\mathcal{B}_1 = \bigcup \mathcal{B}_n$  is a countable union of finite sets, and hence countable, and furthermore the submodule generated by it clearly contains  $N$ .

To see that  $N_1$  is countable note that  $N_1$  is exactly all finite  $\mathbb{Z}$ -linear combinations of elements in  $\mathcal{B}_1$ , and so it will suffice show that we can count all such combinations. But each combination is uniquely determined by a countable tuple containing elements of  $\mathbb{Z}$  with only finitely many nonzero entries (each coordinate corresponds to some  $b \in \mathcal{B}_1$  and the integers give weights to each). The set of such tuples is countable since it is in fact exactly  $N$ .

(c)

We know that  $M$  is free over  $\mathcal{B}$  and since  $N_1$  is generated by  $\mathcal{B}_1 \subseteq \mathcal{B}$  taking the quotient  $M/N_1$  gives us a module isomorphic to the free module over  $\mathcal{B} \setminus \mathcal{B}_1$ . Indeed, the quotient corresponds to simply zeroing out the basis elements in  $\mathcal{B}_1$ .

For some  $\overline{x} \in \overline{M}$  we know then that  $\overline{x}$  is a finite  $\mathbb{Z}$ -linear combination of basis elements for  $\overline{M}$ . Among these finitely many integers we may choose one with a maximum absolute value  $k$ , and notice that for any  $|k'| > |k|$  we cannot write  $\overline{x} = k'\overline{m}$  for any  $m \in M$ , since this would be writing  $\overline{x}$  as a strictly different  $\mathbb{Z}$ -linear combination of basis elements (after writing  $\overline{m}$  in terms of the basis for  $\overline{M}$ ) and this would contradict that  $\overline{M}$  is free.

(d)

To show that  $\mathcal{S}$  is uncountable, we notice that every element of  $\mathcal{S}$  can be uniquely associated with a countable binary vector, where 0 corresponds to  $b_i = i!$  and 1 corresponds to  $b_i = -i!$ . It suffices to prove that this set of binary vectors is uncountable. This can be done straightforwardly via diagonalization. In particular, if we are given an enumeration  $v_1, v_2, \dots$ , of these vectors then we can construct a vector which disagrees with each  $v_i$ , in particular in the  $i$ -th coordinate. Since  $N_1$  is countable we know there is some  $s \in \mathcal{S}$  with  $s \notin N_1$ .

(e)

Choose  $s \in \mathcal{S}$  so that  $s \notin N_1$ . Then  $\bar{s}$  is nonzero in  $\overline{M}$ . Furthermore, we see in  $\overline{M}$  that elements whose coordinates differ in a finite number of entries are the same, since their difference is in  $N \subseteq N_1$ . With this in mind, let  $s_k$  be the tuple whose first  $k$  entries are exactly  $k!$ , and whose following entries agree with  $s$ . We notice that  $\bar{s} = \bar{s}_k$  for all  $k$ . Furthermore,  $s_k = km_k$  for some  $m_k \in M$  since each entry is divisible by  $k$ . We conclude that  $\bar{s} = k\bar{m}_k$  for all  $k$ . But this implies that  $\bar{s} = 0$  by (c), a contradiction. This concludes the proof.  $\square$

**Exercise 10.3.25.** In the construction of direct limits, Exercise 8 of Section 7.6, show that if all  $A_i$  are  $R$ -modules and the maps  $\rho_{ij}$  are  $R$ -module homomorphisms, then the direct limit  $A = \varinjlim A_i$  may be given the structure of an  $R$ -module in a natural way such that the maps  $\rho_i : A_i \rightarrow A$  are all  $R$ -module homomorphisms. Verify the corresponding universal property (part (e)) for  $R$ -module homomorphism  $\phi_i : A_i \rightarrow C$  commuting with the  $\rho_{ij}$ .

**Solution:** We know from the construction that  $A$  is an abelian group, and so we need only show that there is an action of  $R$  on  $A$  that makes it an  $R$ -module, and that the various  $\rho_i$  are  $R$ -module homomorphisms. If  $[a] \in A$  is some equivalence class of elements in the various  $A_i$  and  $r \in R$  then we will define the action by  $r[a] = [ra]$ . First we show this is well defined. If  $[a_i] = [a_j]$  then we know there is some  $k$  so that  $\rho_{ik}(a_i) = \rho_{jk}(a_j)$ . Since  $\rho_{ik}$  and  $\rho_{jk}$  are  $R$ -module homomorphisms we have that

$$\rho_{ik}(ra_i) = r\rho_{ik}(a_i) = r\rho_{jk}(a_j) = \rho_{jk}(a_j)$$

which proves that  $[ra_i] = [ra_j]$ . Hence the action is well defined. Since we may choose arbitrary representatives for the equivalence classes it is clear that the action gives  $A$  an  $R$ -module structure, which arises from the action of  $R$  on the representatives for the equivalence classes.

Next we show that  $\rho_i : A_i \rightarrow A$  is an  $R$ -module homomorphism for all  $i$ . Recall that  $\rho_i(a_i) = [a_i]$ . Then we have directly by definition of the action of  $R$  on  $A$  that

$$\rho_i(ra_i) = [ra_i] = r[a_i] = r\rho_i(a_i)$$

and so clearly each  $\rho_i$  is an  $R$ -module homomorphism.

Finally, we must show that the universal property holds. The universal property for the direct limit of modules is as follows: If  $C$  is an  $R$ -module such that for each  $i \in I$  there is an  $R$ -module homomorphism  $\phi_i : A_i \rightarrow C$  with  $\phi_i = \phi_j \circ \rho_{ij}$  for all  $j \leq i$ , then there is a unique  $R$ -module homomorphism  $\phi : A \rightarrow C$  such that  $\phi \circ \rho_i = \phi_i$  for all  $i$  (where  $\rho_i$  is the natural map from  $A_i$  to  $A$ ). That is, there exists a unique  $\phi$  so that the diagram below commutes for all  $i$ :

$$\begin{array}{ccc} A_i & \xrightarrow{\rho_i} & A \\ \downarrow & & \downarrow \phi \\ & \xrightarrow{\phi_i} & C \end{array}$$

(The CD package doesn't allow for diagonal arrows, sorry).

Under the given hypotheses constructing a candidate for  $\phi$  is not difficult: For each equivalence class  $[a] \in A$ , fix some  $a_i \in A_i$  so that  $\rho_i(a_i) = [a]$ . Then define  $\phi([a]) = \phi_i(a_i)$ . We first argue that this is well defined. Suppose that we choose different representatives for some  $[a]$ , so that  $a_i \in A_i$  and  $a_j \in A_j$  had the property  $\rho_i(a_i) = [a]$  and  $\rho_j(a_j) = [a]$ . Since  $[a] = [a_i] = [a_j]$  we have that there is some  $k$  so that  $i \leq k$ ,  $j \leq k$  and

$$\rho_{ik}(a_i) = \rho_{jk}(a_j).$$

Now observe from the hypothesis of the problem that

$$\phi_i(a_i) = \phi_k(\rho_{ik}(a_i)) = \phi_k(\rho_{jk}(a_j)) = \phi_j(a_j)$$

and so our definition of  $\phi$  is independent of the representatives that we choose for the various equivalence classes  $[a] \in A$ .

With this it is straightforward to show that  $\phi$  is a homomorphism of  $R$ -modules. The action of  $R$  on  $A$  is given by  $r[a] = [ra]$  and we have argued previously that this action is independent of the choice of representative for  $[a]$ . Then we have that

$$\phi(r[a]) = \phi([ra]) = \phi_i(ra_i) = r\phi_i(a_i) = r\phi([a_i]) = r\phi([a])$$

where the representative  $a_i$  is in  $A_i$ . One can also verify easily that this map respects the group structure and is therefore a homomorphism.

Our final task is to argue uniqueness of  $\phi$ . To this end suppose we have some  $R$ -module homomorphism  $\psi : A \rightarrow C$  so that each  $\phi_i$  factors through  $\psi$ . Furthermore suppose that  $\psi$  disagrees with  $\phi$  on some  $[a_i]$ . This means that  $\psi([a_i]) \neq \phi_i(a_i)$ , but this is a direct contradiction to the fact that we require the diagram described previously to commute for all  $i$ . Hence the choice of  $\phi$  is unique. □

**Exercise 10.3.26.** Carry out the analysis of the preceding exercise corresponding to the inverse limits to show that the inverse limit of  $R$ -modules is an  $R$ -module satisfying the appropriate universal property (cf. Exercise 10 of Section 7.6).

**Solution:** TODO □

**Exercise 10.3.27.** (*Free modules over noncommutative rings need not have a unique rank*) Let  $M$  be the  $\mathbb{Z}$ -module  $\mathbb{Z} \times \mathbb{Z} \times \cdots$  of Exercise 24 and let  $R$  be its endomorphism ring,  $R = \text{End}_{\mathbb{Z}}(M)$  (cf. Exercises 29 and 30 in Section 7.1). Define  $\phi_1, \phi_2 \in R$  by

$$\begin{aligned}\phi_1(a_1, a_2, a_3, \dots) &= (a_1, a_3, a_5, \dots) \\ \phi_2(a_1, a_2, a_3, \dots) &= (a_2, a_4, a_6, \dots)\end{aligned}$$

- (a) Prove that  $\{\phi_1, \phi_2\}$  is a free basis of the left  $R$ -module  $R$ . [Define the maps  $\psi_1$  and  $\psi_2$  by  $\psi_1(a_1, a_2, \dots) = (a_1, 0, a_2, 0, \dots)$  and  $\psi_2(a_1, a_2, \dots) = (0, a_1, 0, a_2, \dots)$ . Verify that  $\phi_i\psi_i = 1$ ,  $\phi_1\psi_2 = 0 = \phi_2\psi_1$  and  $\psi_1\phi + \psi_2\phi = 1$ . use these relations to prove that  $\phi_1, \phi_2$  are independent and generate  $R$  as a left  $R$ -module.]

- (b) Use (a) to prove that  $R \cong R^2$  and deduce that  $R \cong R^n$  for all  $n \in \mathbb{Z}^+$ .

**Solution:** TODO □

## 10.4 Tensor Products of Modules

Let  $R$  be a ring with 1.

**Exercise 10.4.1.** Let  $f : R \rightarrow S$  be a ring homomorphism from the ring  $R$  to the ring  $S$  with  $f(1_R) = 1_S$ . Verify the details that  $sr = sf(r)$  defines a right  $R$ -action on  $S$  under which  $S$  is an  $(S, R)$ -bimodule.

**Solution:** TODO

□

**Exercise 10.4.2.** Show that the element “ $2 \otimes 1$ ” is 0 in  $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$  but is nonzero in  $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ .

**Solution:** TODO

□

**Exercise 10.4.3.** Show that  $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$  and  $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$  are both left  $\mathbb{R}$ -modules but are not isomorphic as  $\mathbb{R}$ -modules.

**Solution:** TODO

□

**Exercise 10.4.4.** Show that  $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$  and  $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$  are isomorphic left  $\mathbb{Q}$ -modules. [Show they are both 1-dimensional vector spaces over  $\mathbb{Q}$ .]

**Solution:** TODO

□

**Exercise 10.4.5.** Let  $A$  be a finite abelian group of order  $n$  and let  $p^k$  be the largest power of the prime  $p$  dividing  $n$ . Prove that  $\mathbb{Z}/p^k\mathbb{Z} \otimes_{\mathbb{Z}} A$  is isomorphic to the Sylow  $p$ -subgroup of  $A$ .

**Solution:** TODO

□

**Exercise 10.4.6.** If  $R$  is any integral domain with a quotient field  $Q$ , prove that  $(Q/R) \otimes_R (Q/R) = 0$ .

**Solution:** TODO

□

**Exercise 10.4.7.** If  $R$  is any integral domain with quotient field  $Q$  and  $N$  is a left  $R$ -module, prove that every element of the tensor product  $Q \otimes_R N$  can be written as a simple tensor of the form  $(1/d) \otimes n$  for some nonzero  $d \in R$  and some  $n \in N$ .

**Solution:** TODO

□

**Exercise 10.4.8.** Suppose  $R$  is an integral domain with quotient field  $Q$  and let  $N$  be any  $R$ -module. Let  $U = R^\times$  be the set of nonzero elements in  $R$  and define  $U^{-1}N$  to be the set of equivalence classes of ordered pairs of elements  $(u, n)$  with  $u \in U$  and  $n \in N$  under the equivalence relation  $(u, n) \sim (u', n')$  if and only if  $u'n = un'$  in  $N$ .

- (a) Prove that  $U^{-1}N$  is an abelian group under the addition defined by  $\overline{(u_1, n_1)} + \overline{(u_2, n_2)} = \overline{(u_1 u_2, u_2 n_1 + u_1 n_2)}$ . Prove that  $r(u, n) = \overline{(u, rn)}$  defines an action of  $R$  on  $U^{-1}N$  making it into an  $R$ -module. [This is an example of *localization* considered in general in Section 4 of Chapter 15, cf. also Section 6 in Chapter 7.]



- (b) Show that the map from  $Q \times N$  to  $U^{-1}N$  defined by sending  $(a/b, n)$  to  $\overline{(b, an)}$  for  $a \in R, b \in U, n \in N$ , is an  $R$ -balanced map, so induces a homomorphism  $f$  from  $Q \otimes_R N$  to  $U^{-1}N$ . Show that the map  $g$  from  $U^{-1}N$  to  $Q \otimes_R N$  defined by  $g(\overline{(u, n)}) = (1/u) \otimes n$  is well defined and is an inverse homomorphism to  $f$ . Conclude that  $Q \otimes_R N \cong U^{-1}N$  as  $R$ -modules.
- (c) Conclude from (b) that  $(1/d) \otimes n$  is 0 in  $Q \otimes_R N$  if and only if  $rn = 0$  for some nonzero  $r \in R$ .
- (d) If  $A$  is an abelian group show that  $\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$  if and only if  $A$  is a torsion abelian group (i.e., every element of  $A$  has finite order).

**Solution:** TODO

□

**Exercise 10.4.9.** Suppose  $R$  is an integral domain with the quotient field  $Q$  and let  $N$  be any  $R$ -module. Let  $Q \otimes_R N$  be the module obtained from  $N$  by extension of scalars from  $R$  to  $Q$ . Prove that the kernel of the  $R$ -module homomorphism  $\iota : N \rightarrow Q \otimes_R N$  is the torsion submodule of  $N$  (cf. Exercise 8 in Section 1). [Use the previous exercise.]

**Solution:** TODO

□

**Exercise 10.4.10.** Suppose  $R$  is commutative and  $N \cong R^n$  is a free  $R$ -module of rank  $n$  with  $R$ -module basis  $e_1, \dots, e_n$ .

- (a) For any nonzero  $R$ -module  $M$  show that every element of  $M \otimes N$  can be written uniquely in the form  $\sum_{i=1}^n m_i \otimes e_i$  where  $m_i \in M$ . Deduce that if  $\sum_{i=1}^n m_i \otimes e_i = 0$  in  $M \otimes N$  then  $m_i = 0$  for  $i = 1, \dots, n$ .
- (b) Show that if  $\sum m_i \otimes n_i = 0$  in  $M \otimes N$  where  $n_i$  are merely assumed to be  $R$ -linearly independent then it is not necessarily true that all  $m_i$  are 0. [Consider  $R = \mathbb{Z}, n = 1, M = \mathbb{Z}/2\mathbb{Z}$  and the element  $1 \otimes 2$ .]

**Solution:** TODO

□

**Exercise 10.4.11.** Let  $\{e_1, e_2\}$  be a basis of  $V = \mathbb{R}^2$ . Show that the element  $e_1 \otimes e_2 + e_2 \otimes e_1$  in  $V \otimes_{\mathbb{R}} V$  cannot be written as a simple tensor  $v \otimes w$  for any  $v, w \in \mathbb{R}^2$ .

**Solution:** TODO

□

**Exercise 10.4.12.** Let  $V$  be a vector space over the field  $F$  and let  $v, v'$  be nonzero elements of  $V$ . Prove that  $v \otimes v' = v' \otimes v$  in  $V \otimes_F V$  if and only if  $v = av'$  for some  $a \in F$ .

**Solution:** TODO

□

**Exercise 10.4.13.** Prove that the usual dot product of vectors defined by letting  $(a_1, \dots, a_n) \cdots (b_1, \dots, b_n)$  be  $a_1 b_1 + \dots + a_n b_n$  is a bilinear map from  $R^n \times R^n$  to  $\mathbb{R}$ .

**Solution:** TODO

□

**Exercise 10.4.14.** Let  $I$  be an arbitrary nonempty index set and for each  $i \in I$  let  $N_i$  be a left  $R$ -modules. Let  $M$  be a right  $R$ -module. Prove the group isomorphism:  $M \otimes (\oplus_{i \in I} N_i) \cong \oplus_{i \in I} (M \otimes N_i)$ , where the direct sum of an arbitrary collection of modules is defined in Exercise 20, Section 3. [Use the same argument as for the direct sum of two modules, taking care to note where the direct *sum* hypothesis is needed — cf. the next exercise.]

**Solution:** TODO

□

**Exercise 10.4.15.** Show that tensor products do not commute with direct products in general. [Consider the extension of scalars from  $\mathbb{Z}$  to  $\mathbb{Q}$  of the direct product of the modules  $M_i = \mathbb{Z}/2^i\mathbb{Z}$ ,  $i = 1, 2, \dots$ ].

**Solution:** TODO

□

**Exercise 10.4.16.** Suppose  $R$  is commutative and let  $I$  and  $J$  be ideals of  $R$ , so  $R/I$  and  $R/J$  are naturally  $R$ -modules.

- (a) Prove that every element of  $R/I \otimes_R R/J$  can be written as a simple tensor of the form  $(1 \bmod I) \otimes (r \bmod J)$ .
- (b) Prove that there is an  $R$ -module isomorphism  $R/I \otimes_R R/J \cong R/(I+J)$  mapping  $(r \bmod I) \otimes (r' \bmod J)$  to  $rr' \bmod (I+J)$ .

**Solution:** TODO

□

**Exercise 10.4.17.** Let  $I = (2, x)$  be the ideal generated by 2 and  $x$  in the ring  $R = \mathbb{Z}[x]$ . The ring  $\mathbb{Z}/2\mathbb{Z} = R/I$  is naturally an  $R$ -module annihilated by both 2 and  $x$ .

- (a) Show that the map  $\phi : I \times I \rightarrow \mathbb{Z}/2\mathbb{Z}$  defined by

$$\phi(a_0 + a_1x + \cdots a_nx^n, b_0 + b_1x + \cdots b_mx^m) = \frac{a_0}{2}b_1 \bmod 2$$

is  $R$ -bilinear.

- (b) Show that there is an  $R$ -module homomorphism from  $I \otimes_R I \rightarrow \mathbb{Z}/2\mathbb{Z}$  mapping  $p(x) \otimes q(x)$  to  $\frac{p(0)}{2}q'(0)$  where  $q'$  denotes the usual polynomial derivative of  $q$ .
- (c) Show that  $2 \otimes x \neq x \otimes 2$  in  $I \otimes_R I$ .

**Solution:** TODO

□

**Exercise 10.4.18.** Suppose  $I$  is a principal ideal in the integral domain  $R$ . Prove that the  $R$ -modules  $I \otimes_R I$  has no nonzero torsion elements (i.e.  $rm = 0$  with  $0 \neq r \in R$  and  $m \in I \otimes_R I$  implies  $m = 0$ ).

**Solution:** TODO

□

**Exercise 10.4.19.** Let  $I = (2, x)$  be the ideal generated by 2 and  $x$  in the ring  $R = \mathbb{Z}[x]$  as in Exercise 17. Show that the nonzero element  $2 \otimes x - x \otimes 2$  in  $I \otimes_R I$  is a torsion element. Show in fact that  $2 \otimes x - x \otimes 2$  is annihilated by both 2 and  $x$  and that the submodule of  $I \otimes_R I$  generated by  $2 \otimes x - x \otimes 2$  is isomorphic to  $R/I$ .

**Solution:** TODO

□

**Exercise 10.4.20.** Let  $I = (2, x)$  be the ideal generated by 2 and  $x$  in the ring  $R = \mathbb{Z}[x]$ . Show that the element  $2 \otimes 2 + x \otimes x$  in  $I \otimes_R I$  is not a simple tensor, i.e. cannot be written as  $a \otimes b$  for some  $a, b \in I$ .

**Solution:** TODO

□

**Exercise 10.4.21.** Suppose  $R$  is commutative and let  $I$  and  $J$  be ideals of  $R$ .

- (a) Show that there is a surjective  $R$ -module homomorphism from  $I \otimes_R J$  to the product ideal  $IJ$  mapping  $I \otimes J$  to the element  $ij$ .
- (b) Give an example to show that the map in (a) need not be injective (cf. Exercise 17).

**Solution:** TODO

□

**Exercise 10.4.22.** Suppose that  $M$  is a left and a right  $R$ -module such that  $rm = mr$  for all  $r \in R$  and  $m \in M$ . Show that the elements  $r_1 r_2$  and  $r_2 r_1$  act the same on  $M$  for every  $r_1, r_2 \in R$ . (This explains why the assumption that  $R$  is commutative in the definition of an  $R$ -algebra is a fairly natural one.)

**Solution:** TODO

□

**Exercise 10.4.23.** Verify the details that the multiplication in Proposition 19 makes  $A \otimes_R B$  into an  $R$ -algebra.

**Solution:** TODO

□

**Exercise 10.4.24.** Prove that the extension of scalars from  $\mathbb{Z}$  to the Gaussian integers  $\mathbb{Z}[i]$  of the ring  $\mathbb{R}$  is isomorphic to  $\mathbb{C}$  as a ring:  $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{C}$  as rings.

**Solution:** TODO

□

**Exercise 10.4.25.** Let  $R$  be a subring of the commutative ring  $S$  and let  $x$  be an indeterminate over  $S$ . Prove that  $S[x]$  and  $S \otimes_R R[x]$  are isomorphic as  $S$ -algebras.

**Solution:** TODO

□

**Exercise 10.4.26.** Let  $S$  be a commutative ring containing  $R$  (with  $1_S = 1_R$ ) and let  $x_1, \dots, x_n$  be independent indeterminates over the ring  $S$ . Show that for every ideal  $I$  in the polynomial ring  $R[x_1, \dots, x_n]$  that  $S \otimes_R (R[x_1, \dots, x_n]/I) \cong S[x_1, \dots, x_n]/IS[x_1, \dots, x_n]$ .

**Solution:** TODO

□

**Exercise 10.4.27.** The next exercise shows the ring  $C \otimes_R \mathbb{C}$  introduced at the end of this section is isomorphic to  $\mathbb{C} \times \mathbb{C}$ . One may also prove this via Exercise 26 and Proposition 16 in Section 9.5, since  $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$ . The ring  $C \times \mathbb{C}$  is also discussed in Exercise 23 of Section 1.

- (a) Write down a formula for the multiplication of two elements  $a \cdot 1 + b \cdot e_2 + c \cdot e_3 + d \cdot e_4$  and  $a' \cdot 1 + b' \cdot e_2 + c' \cdot e_3 + d' \cdot e_4$  in the example  $A = \mathbb{C} \otimes \mathbb{R}\mathbb{C}$  following Proposition 21 (where  $1 = 1 \otimes 1$  is the identity of  $A$ ).
- (b) Let  $\epsilon_1 = \frac{1}{2}(1 \otimes 1 + i \otimes i)$  and let  $\epsilon_2 = \frac{1}{2}(1 \otimes 1 - i \otimes i)$ . Show that  $\epsilon_1 \epsilon_2 = 0$ ,  $\epsilon_1 + \epsilon_2 = 1$  and  $\epsilon_j^2 = \epsilon_j$  for  $j = 1, 2$  ( $\epsilon_1$  and  $\epsilon_2$  are called *orthogonal idempotents* in  $A$ ). Deduce that  $A$  is isomorphic as a ring to the direct product of two principal ideals:  $A \cong A\epsilon_1 \times A\epsilon_2$  (cf. Exercise 1, Section 7.6).
- (c) Prove that the map  $\phi : \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C} \times \mathbb{C}$  by  $\phi(z_1, z_2) = (z_1 z_2, z_1 \bar{z}_2)$ , where  $\bar{z}_2$  denotes the complex conjugate of  $z_2$ , is an  $\mathbb{R}$ -bilinear map.
- (d) Let  $\Phi$  be the  $\mathbb{R}$ -module homomorphism from  $A$  to  $\mathbb{C} \times \mathbb{C}$  obtained from  $\phi$  in (c). Show that  $\Phi(\epsilon_1) = (0, 1)$  and  $\Phi(\epsilon_2) = (1, 0)$ . Show also that  $\Phi$  is  $\mathbb{C}$ -linear, where the action of  $\mathbb{C}$  is on the left tensor factor in  $A$  and on both factors in  $\mathbb{C} \times \mathbb{C}$ . Deduce that  $\Phi$  is surjective. Show that  $\Phi$  is a  $\mathbb{C}$ -algebra isomorphism.

**Solution:** TODO

□

## 10.5 Exact Sequences—Projective, Injective, and Flat Modules

**Exercise 10.5.1.** Suppose that

$$\begin{array}{ccccc} A & \xrightarrow{\psi} & B & \xrightarrow{\phi} & C \\ \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow \\ A' & \xrightarrow{\psi'} & B' & \xrightarrow{\phi'} & C' \end{array}$$

is a commutative diagram of groups and that the rows are exact. Prove that

- (a) If  $\phi$  and  $\alpha$  are surjective, and  $\beta$  is injective then  $\gamma$  is injective. [If  $c \in \ker \gamma$ , show there is a  $b \in B$  with  $\phi(b) = c$ . Show that  $\phi'(\beta(b)) = 0$  and deduce that  $\beta(b) = \phi'(a')$  for some  $a' \in A'$ . Show that there is an  $a \in A$  with  $\alpha(a) = a'$  and that  $\beta(\psi(a)) = \beta(b)$ . Conclude that  $b = \psi(a)$  and hence  $c = \phi(b) = 0$ .]
- (b) If  $\phi', \alpha$  and  $\gamma$  are injective, then  $\beta$  is injective.
- (c) If  $\phi, \alpha$  and  $\gamma$  are surjective, then  $\beta$  is surjective.
- (d) If  $\beta$  is injective,  $\alpha$  and  $\phi$  are surjective, then  $\gamma$  is injective.
- (e) If  $\beta$  is surjective,  $\gamma$  and  $\psi'$  are injective, then  $\alpha$  is surjective.

**Solution:** TODO

□

**Exercise 10.5.2.** Suppose that

$$\begin{array}{ccccccc} A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & D \\ \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & & \delta \downarrow \\ A' & \xrightarrow{\quad} & B' & \longrightarrow & C' & \longrightarrow & D' \end{array}$$

is a commutative diagram of groups and that the rows are exact. Prove that

- (a) If  $\alpha$  is surjective and  $\beta, \delta$  are injective, then  $\gamma$  is injective.
- (b) If  $\delta$  is injective, and  $\alpha, \gamma$  are surjective, then  $\beta$  is surjective.

**Solution:** TODO

□

**Exercise 10.5.3.** Let  $P_1$  and  $P_2$  be  $R$ -modules. Prove that  $P_1 \oplus P_2$  is a projective  $R$ -module if and only if both  $P_1$  and  $P_2$  are projective.

**Solution:** TODO

□

**Exercise 10.5.4.** Let  $Q_1$  and  $Q_2$  be  $R$ -modules. Prove that  $Q_1 \oplus Q_2$  is an injective  $R$ -modules if and only if both  $Q_1$  and  $Q_2$  are injective.

**Solution:** TODO

□

**Exercise 10.5.5.** Let  $A_1$  and  $A_2$  be  $R$ -modules. Prove that  $A_1 \oplus A_2$  is a flat  $R$ -modules if and only if both  $A_1$  and  $A_2$  are flat. More generally, prove that an arbitrary direct sum  $\sum A_i$  of  $R$ -modules is flat if and only if each  $A_i$  is flat. [Use the fact that tensor product commutes with arbitrary direct sums.]

**Solution:** TODO

□

**Exercise 10.5.6.** Prove that the following are equivalent for a ring  $R$ :

- (i) Every  $R$ -module is projective.
- (ii) Every  $R$ -module is injective.

**Solution:** TODO

□

**Exercise 10.5.7.** Let  $A$  be a nonzero finite abelian group.

- (a) Prove that  $A$  is not a projective  $\mathbb{Z}$ -module.
- (b) Prove that  $A$  is not an injective  $\mathbb{Z}$ -module.

**Solution:** TODO

□

**Exercise 10.5.8.** Let  $Q$  be a nonzero divisible  $\mathbb{Z}$ -module. Prove that  $Q$  is not a projective  $\mathbb{Z}$ -module. Deduce that the rational numbers  $\mathbb{Q}$  is not a projective  $\mathbb{Z}$ -module. [Show first that if  $F$  is any free module then  $\cap_{n=1}^{\infty} nF = 0$  (use a basis of  $F$  to prove this). Now suppose to the contrary that  $Q$  is projective and derive a contradiction from Proposition 30(4).]

**Solution:** TODO

□

**Exercise 10.5.9.** Assume  $R$  is commutative with 1.

- (a) Prove that the tensor product of two free  $R$ -modules is free. [Use the fact that tensor products commute with arbitrary direct sums.]
- (b) Use (a) to prove that the tensor product of two projective  $R$ -modules is projective.

**Solution:** TODO

□

**Exercise 10.5.10.** Let  $R$  and  $S$  be rings with 1 and let  $M$  and  $N$  be left  $R$ -modules. Assume also that  $M$  is an  $(R, S)$ -bimodule.

- (a) For  $s \in S$  and for  $\phi \in \text{Hom}_R(M, N)$  define  $(s\phi) : M \rightarrow N$  by  $(s\phi)(m) = \phi(ms)$ . Prove that  $s\phi$  is a homomorphism of left  $R$ -modules, and that this action of  $S$  on  $\text{Hom}_R(M, N)$  makes it into a *left*  $S$ -module.
- (b) Let  $S = R$  and let  $M = R$  (considered as an  $(R, R)$ -bimodule by left and right ring multiplication on itself). For each  $n \in N$  define  $\phi_n : R \rightarrow N$  by  $\phi_n(r) = rn$ , i.e.  $\phi_n$  is the unique  $R$ -module homomorphism mapping  $1_R$  to  $n$ . Show that  $\phi_n \in \text{Hom}_R(R, N)$ . Use part (a) to show that the map  $n \mapsto \phi_n$  is an isomorphism of left  $R$ -modules:  $N \cong \text{Hom}_R(R, N)$ .
- (c) Deduce that if  $N$  is a free (respective, projective, injective, flat) left  $R$ -module, then  $\text{Hom}_R(R, N)$  is also a free (respective, projective, injective, flat) left  $R$ -module.

**Solution:** TODO

□

**Exercise 10.5.11.** Let  $R$  and  $S$  be rings with 1 and let  $M$  and  $N$  be left  $R$ -modules. Assume also that  $M$  is an  $(R, S)$ -bimodule.

- (a) For  $s \in S$  and for  $\phi \in \text{Hom}_R(M, N)$  define  $(\phi s) : M \rightarrow N$  by  $(\phi s)(m) = \phi(m)s$ . Prove that  $\phi s$  is a homomorphism of left  $R$ -modules, and that this action of  $S$  on  $\text{Hom}_R(M, N)$  makes it into a *right*  $S$ -module. Deduce that  $\text{Hom}_R(M, R)$  is a right  $R$ -module, for any  $R$ -module  $M$  — called the *dual module* to  $M$ .
- (b) Let  $N = R$  be considered as an  $(R, R)$  bimodule as usual. Under the action defined in part (a) show that the map  $r \mapsto \phi_r$  is an isomorphism of right  $R$ -modules:  $\text{Hom}_R(R, R) \cong R$ , where  $\phi_r$  is the homomorphism that maps  $1_R$  to  $r$ . Deduce that if  $M$  is a finitely generated free left  $R$ -module, then  $\text{Hom}_R(M, R)$  is a free right  $R$ -module of the same rank. (cf. also Exercise 13).
- (c) Show that if  $M$  is a finitely generated projective  $R$ -module then its dual module  $\text{Hom}_R(M, R)$  is also projective.

**Solution:** TODO

□

**Exercise 10.5.12.** Let  $A$  be an  $R$ -module, let  $I$  be any nonempty index set and for each  $i \in I$  let  $B_i$  be an  $R$ -module. Prove the following isomorphisms of abelian groups; when  $R$  is commutative prove also that these are  $R$ -module isomorphisms. (Arbitrary direct sums and direct products of modules are introduced in Exercise 20 of Section 3.)

- (a)  $\text{Hom}_R(\bigoplus_{i \in I} B_i, A) \cong \prod_{i \in I} \text{Hom}_R(B_i, A)$
- (b)  $\text{Hom}_R(A, \prod_{i \in I} B_i) \cong \prod_{i \in I} \text{Hom}_R(A, B_i)$ .

**Solution:** TODO

□

**Exercise 10.5.13.** (a) Show that the dual of the free  $\mathbb{Z}$ -module with countable basis is not free. [Use the preceding exercise and Exercise 24, Section 3.] (See also Exercise 5 in Section 11.3.)

- (b) Show that the dual of the free  $\mathbb{Z}$ -module with countable basis is not projective. [You may use the fact that any submodule of a free  $\mathbb{Z}$ -module is free.]

**Solution:** TODO

□

**Exercise 10.5.14.** Let  $0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\phi} N \longrightarrow 0$  be a sequence of  $R$ -modules.

- (a) Prove that the associated sequence

$$0 \longrightarrow \text{Hom}_R(D, L) \xrightarrow{\psi'} \text{Hom}_R(D, M) \xrightarrow{\phi'} \text{Hom}_R(D, N) \longrightarrow 0$$

is a short exact sequence of abelian groups for all  $R$ -modules  $D$  if and only if the original sequence is a split short exact sequence. [To show the sequence splits, take  $D = N$  and show the lift of the identity map in  $\text{Hom}_R(N, N)$  to  $\text{Hom}_R(N, M)$  is a splitting homomorphism for  $\phi$ .]

- (b) Prove that the associated sequence

$$0 \longrightarrow \text{Hom}_R(N, D) \xrightarrow{\phi'} \text{Hom}_R(M, D) \xrightarrow{\psi'} \text{Hom}_R(L, D) \longrightarrow 0$$

is a short exact sequence of abelian groups for all  $R$ -modules  $D$  if and only if the original sequence is a split short exact sequence.

**Solution:** TODO

□

**Exercise 10.5.15.** Let  $M$  be a left  $\mathbb{Z}$ -module and let  $R$  be a ring with 1.

- (a) Show that  $\text{Hom}_{\mathbb{Z}}(R, M)$  is a left  $R$ -module under the action  $(r\phi)(r') = \phi(r'r)$  (see Exercise 10).
- (b) Suppose that  $0 \longrightarrow A \xrightarrow{\psi} B$  is an exact sequence of  $R$ -modules. Prove that if every  $\mathbb{Z}$ -module homomorphism  $f$  from  $A$  to  $M$  lifts to a  $\mathbb{Z}$ -module homomorphism  $F$  from  $B$  to  $M$  with  $f = F \circ \psi$ , then every  $R$ -module homomorphism  $f'$  from  $A$  to  $\text{Hom}_{\mathbb{Z}}(R, M)$  lifts to an  $R$ -module homomorphism  $F'$  from  $B$  to  $\text{Hom}_{\mathbb{Z}}(R, M)$  with  $f' = F' \circ \psi$ . [Given  $f'$ , show that  $f(a) = f'(a)(1_R)$  defines a  $\mathbb{Z}$ -module homomorphism of  $A$  to  $M$ . If  $F$  is the associated lift of  $f$  to  $B$ , show that  $F'(b)(r) = F(rb)$  defines an  $R$ -modules homomorphism from  $B$  to  $\text{Hom}_{\mathbb{Z}}(R, M)$  that lifts  $f'$ .]

(c) Prove that if  $Q$  is an injective  $\mathbb{Z}$ -module then  $\text{Hom}_{\mathbb{Z}}(R, Q)$  is an injective  $R$ -module.

**Solution:** TODO

□

**Exercise 10.5.16.** This exercise proves Theorem 38 that every left  $R$ -module  $M$  is contained in an injective left  $R$ -module.

(a) Show that  $M$  is contained in an injective  $\mathbb{Z}$ -module  $Q$ . [ $M$  is a  $\mathbb{Z}$ -module—use Corollary 37.]

(b) Show that  $\text{Hom}_R(R, M) \subseteq \text{Hom}_{\mathbb{Z}}(R, M) \subseteq \text{Hom}_{\mathbb{Z}}(R, Q)$ .

(c) Use the  $R$ -module isomorphism  $M \cong \text{Hom}_R(R, M)$  (Exercise 10) and the previous exercise to conclude that  $M$  is contained in an injective  $R$ -module.

**Solution:** TODO

□

**Exercise 10.5.17.** This exercise completes the proof of Proposition 34. Suppose that  $Q$  is an  $R$ -module with the property that every short exact sequence  $0 \longrightarrow Q \longrightarrow M_1 \longrightarrow N \longrightarrow 0$  splits and suppose that the sequence  $0 \longrightarrow L \xrightarrow{\psi} M$  is exact. Prove that every  $R$ -module homomorphism  $f$  from  $L$  to  $Q$  can be lifted to an  $R$ -module homomorphism  $F$  from  $M$  to  $Q$  with  $f = F \circ \psi$ . [By the previous exercise,  $Q$  is contained in an injective  $R$ -module. Use the splitting property together with Exercise 4 (noting that Exercise 4 can be proved using (2) in Proposition 34 as the definition of an injective module).]

**Solution:** TODO

□

**Exercise 10.5.18.** Prove that the injective hull of the  $\mathbb{Z}$ -module  $\mathbb{Z}$  is  $\mathbb{Q}$  [Let  $H$  be the injective hull of  $\mathbb{Z}$  and argue that  $\mathbb{Q}$  contains an isomorphic copy of  $H$ . Use the divisibility of  $H$  to show that  $1/n \in H$  for all nonzero integers  $n$ , and deduce that  $H = \mathbb{Q}$ .]

**Solution:** TODO

□

**Exercise 10.5.19.** If  $F$  is a field, prove that the injective hull of  $F$  is  $F$ .

**Solution:** TODO

□

**Exercise 10.5.20.** Prove that the polynomial ring  $R[x]$  with indeterminate  $x$  over the commutative ring  $R$  is a flat  $R$ -module.

**Solution:** TODO

□

**Exercise 10.5.21.** Let  $R$  and  $S$  be rings with 1 and suppose  $M$  is a right  $R$ -module, and  $N$  is an  $(R, S)$ -bimodule. If  $M$  is flat over  $R$  and  $N$  is flat as an  $S$ -module prove that  $M \otimes_R N$  is flat as a right  $S$ -module.

**Solution:** TODO

□



**Exercise 10.5.22.** Suppose that  $R$  is a commutative ring and that  $M$  and  $N$  are flat  $R$ -modules. Prove that  $M \otimes_R N$  is a flat  $R$ -module. [Use the previous exercise.]

**Solution:** TODO

□

**Exercise 10.5.23.** Prove that the (right) module  $M \otimes_R S$  obtained by changing the base from the ring  $R$  to the ring  $S$  (by some homomorphism  $f : R \rightarrow S$  with  $f(1_R) = 1_S$  cf. Example 6 following Corollary 12 in Section 4) of the flat (right)  $R$ -module  $M$  is a flat  $S$ -module.

**Solution:** TODO

□

**Exercise 10.5.24.** Prove that  $A$  is a flat  $R$ -module if and only if for any left  $R$ -modules  $L$  and  $M$  where  $L$  is *finitely egenerated*, then  $\psi : L \rightarrow M$  is injective implies that also  $1 \otimes \psi : A \otimes_R L \rightarrow A \otimes_R M$  is injective. [Use the techniques if the proof of corollary 42.]

**Solution:** TODO

□

**Exercise 10.5.25.** (A Flatness Criterion) Parts (a)-(c) of this exercise prove that  $A$  is a flat  $R$ -module if and only if for every finitely generated ideal  $I$  of  $R$ , the map from  $A \otimes_R I \rightarrow A \otimes_R R \cong A$  induced by the inclusion  $I \subseteq R$  is again injective (or equivalently,  $A \otimes_R I \cong AI \subseteq A$ ).

- (a) Prove that if  $A$  is flat then  $A \otimes_R I \rightarrow A \otimes_R R$  is injective.
- (b) If  $A \otimes_R I \rightarrow A \otimes_R R$  is injective for every finitely generated ideal  $I$ , prove that  $A \otimes_R I \rightarrow A \otimes_R R$  is injective for every ideal  $I$ . Show that if  $K$  is any submodule of a finitely generated free module  $F$  then  $A \otimes_R K \rightarrow A \otimes_R F$  is injective. Show that the same is true for any free module  $F$ . [Cf. the proof of Corollary 42.]
- (c) Under the assumption in (b), suppose  $L$  and  $M$  are  $R$ -modules and  $L \xrightarrow{\psi} M$  is injective. Prove that  $A \otimes_R L \xrightarrow{1 \otimes \psi} A \otimes_R M$  is injective and conclude that  $A$  is flat. [Write  $M$  as a quotient of the free module  $F$ , giving a short exact sequence

$$0 \longrightarrow K \longrightarrow F \xrightarrow{f} M \longrightarrow 0.$$

Show that if  $J = f^{-1}(\psi(L))$  and  $\iota : J \rightarrow F$  is the natural injection, then the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & K & \longrightarrow & J & \longrightarrow & L \longrightarrow 0 \\ & & id \downarrow & & \iota \downarrow & & \psi \downarrow \\ 0 & \longrightarrow & K & \longrightarrow & F & \longrightarrow & M \longrightarrow 0 \end{array}$$

is commutative with exact rows. Show that the induced diagram

$$\begin{array}{ccccccc} A \otimes_R K & \longrightarrow & A \otimes_R J & \longrightarrow & A \otimes_R L & \longrightarrow & 0 \\ & & id \downarrow & & 1 \otimes \iota \downarrow & & 1 \otimes \psi \downarrow \\ A \otimes_R K & \longrightarrow & A \otimes_R F & \longrightarrow & A \otimes_R M & \longrightarrow & 0 \end{array}$$

is commutative with exact rows. Use (b) to show that  $1 \otimes \iota$  is injective, then use Exercise 1 to conclude that  $1 \otimes \psi$  is injective.]

- (d) (A Flatness Criterion for quotients) Suppose  $A = F/K$  where  $F$  is flat (e.g., if  $F$  is free) and  $K$  is an  $R$ -submodule of  $F$ . Prove that  $A$  is flat if and only if  $FI \cap K = KI$  for every finitely generated ideal  $I$  of  $R$ . [Use (a) to prove  $F \otimes_R I \cong FI$  and observe the image of  $K \otimes_R I$  is  $KI$ ; tensor the exact sequence  $0 \rightarrow K \rightarrow F \rightarrow A \rightarrow 0$  with  $I$  to prove that  $A \otimes_R I \cong FI/KI$ , and apply the flatness criterion.]

**Solution:** TODO

□

**Exercise 10.5.26.** Suppose  $R$  is a PID. This exercise proves that  $A$  is a flat  $R$ -module if and only if  $A$  is a torsion free  $R$ -module (i.e., if  $a \in A$  is nonzero and  $r \in R$ , then  $ra = 0$  implies  $r = 0$ ).

- (a) Suppose that  $A$  is flat and for fixed  $r \in R$  consider the map  $\psi_r : R \rightarrow R$  defined by multiplication by  $r$ :  $\psi_r(x) = rx$ . If  $r$  is nonzero show that  $\psi_r$  is an injection. Conclude from the flatness of  $A$  that the map from  $A$  to  $A$  defined by mapping  $a$  to  $ra$  is injective and that  $A$  is torsion free.
- (b) Suppose that  $A$  is torsion free. If  $I$  is a nonzero ideal of  $R$ , then  $I = rR$  for some nonzero  $r \in R$ . Show that the map  $\psi_r$  in (a) induces an isomorphism  $R \cong I$  of  $R$ -modules and that the composite  $R \xrightarrow{\psi_r} I \xrightarrow{\iota} R$  of  $\psi_r$  with the inclusion  $\iota : I \subseteq R$  is multiplication by  $r$ . Prove that the composite  $A \otimes_R R \xrightarrow{1 \otimes \psi_r} A \otimes_R I \xrightarrow{1 \otimes \iota} A \otimes_R R$  corresponds to the map  $a \mapsto ra$  under the identification  $A \otimes_R R = A$  and that this composite is injective since  $A$  is torsion free. Show that  $1 \otimes \psi_r$  is an isomorphism and deduce that  $1 \otimes i$  is injective. Use the previous exercise to conclude that  $A$  is flat.

**Solution:** TODO

□

**Exercise 10.5.27.** Let  $M, A$  and  $B$  be  $R$ -modules.

- (a) Suppose  $f : A \rightarrow M$  and  $g : B \rightarrow M$  are  $R$ -module homomorphisms. Prove that  $X = \{(a, b) \mid a \in A, b \in B \text{ with } f(a) = g(b)\}$  is an  $R$ -submodule of the direct sum  $A \oplus B$  (called the *pullback* or *fiber product* of  $f$  and  $g$ ) and that there is a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\pi_2} & B \\ \pi_1 \downarrow & & \downarrow g \\ A & \xrightarrow{f} & M \end{array}$$

where  $\pi_1$  and  $\pi_2$  are the natural projections onto the first and second components.

- (b) Suppose  $f' : M \rightarrow A$  and  $g' : M \rightarrow B$  are  $R$ -module homomorphisms. Prove that the quotient  $Y$  of  $A \oplus B$  by  $\{(f'(m), -g'(m)) \mid m \in M\}$  is an  $R$ -module (called the *pushout* or *fiber sum* of  $f'$  and  $g'$ ) and that there is a commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{g'} & B \\ f' \downarrow & & \downarrow \pi'_2 \\ A & \xrightarrow{\pi'_1} & X \end{array}$$

where  $\phi'_1$  and  $\phi'_2$  are the natural maps to the quotient induced by the maps into the first and second components.

**Solution:** TODO

□

**Exercise 10.5.28.** (a) (*Schanuel's Lemma*) If  $0 \longrightarrow K \longrightarrow P \xrightarrow{\phi} M \longrightarrow 0$  and  $0 \longrightarrow K' \longrightarrow P' \xrightarrow{\phi'} M \longrightarrow 0$  are exact sequences of  $R$ -modules where  $P$  and  $P'$  are projective, prove that  $P \oplus K' \cong P' \oplus K$  as  $R$ -modules. [Show that there is an exact sequence  $0 \longrightarrow \ker \phi \longrightarrow X \xrightarrow{\pi} P \longrightarrow 0$  with  $\ker \pi \cong K'$ , where  $X$  is the fiber product of  $\phi$  and  $\phi'$  as in the previous exercise. Deduce that  $X \cong P \oplus K'$ . Show similarly that  $X \cong P' \oplus K$ .]

(b) If  $0 \longrightarrow M \longrightarrow Q \xrightarrow{\psi} L \longrightarrow 0$  and  $0 \longrightarrow M \longrightarrow Q' \xrightarrow{\psi'} L' \longrightarrow 0$  are exact sequences of  $R$ -modules where  $Q$  and  $Q'$  are injective, prove that  $Q \oplus L' \cong Q' \oplus L$  as  $R$ -modules.

The  $R$  modules  $M$  and  $N$  are said to be *projectively equivalent* if  $M \oplus P \cong N \oplus P'$  for some projective modules  $P, P'$ . Similarly,  $M$  and  $N$  are *injectively equivalent* if  $M \oplus Q \cong N \oplus Q'$  for some injective modules  $Q, Q'$ . The previous exercise shows  $K$  and  $K'$  are projectively equivalent and  $L$  and  $L'$  are injectively equivalent.

**Solution:** TODO

□