1. (Exercise 5 in DF §10.2.) Exhibit all $\mathbf{Z}$-module homomorphisms from $\mathbf{Z}/30\mathbf{Z}$ to $\mathbf{Z}/21\mathbf{Z}$. (Prove that you have found all of them.)

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/30\mathbb{Z}, \mathbb{Z}/21\mathbb{Z}) = \{x \mapsto (7k)x : k = 0, 1, 2\}$$
(expressions are taken mod 30 on the left and mod 21 on the right)

Proof. Suppose $\varphi : \mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/21\mathbb{Z}$ is a $\mathbb{Z}$-module homomorphism, and let z be the image of 1. Then $\varphi(0) = \varphi(30) = 30\varphi(1) = 30z = 9z = 0$, so $21 \mid 9z$. This means that $7 \mid 3z$, thus $7 \mid z$. Therefore, the above set contains $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/30\mathbb{Z}, \mathbb{Z}/21\mathbb{Z})$.

Now, suppose $a = md + s$ for some $a, m \in \mathbb{Z}$ where $0 \leq s < m$. Then for any $n, j \in \mathbb{Z}$ such that $n \mid jm$,

$$\begin{aligned}(j(a \mod m)) \mod n &= (js) \mod n \\ &= (0 + js) \mod n \\ &= (jmd + js) \mod n \\ &= ja \mod n.\end{aligned}$$

Suppose φ is one of these three maps, so that $\varphi(z) = (7k)z$ for some $k = 0, 1, 2$. Letting $a = rx + y$, $j = 7k$, $m = 30$, and $n = 21$ gives us that

$$\begin{aligned}\varphi((rx + y) \mod 30) &= (7k((rx + y) \mod 30)) \mod 21 \\ &= (7k(rx + y)) \mod 21 \\ &= (7krx + 7ky) \mod 21 \\ &= [(r7kx) \mod 21 + (7ky) \mod 21] \mod 21 \\ &= [((r \mod 21)(7kx \mod 21)) \mod 21 + (7ky) \mod 21] \mod 21 \\ &= [((r \mod 21)\varphi(x)) \mod 21 + \varphi(y)] \mod 21 \\ &= r \cdot \varphi(x) + \varphi(y)\end{aligned}$$

The second equality comes from the use of the fact derived above. I carry the mod 21 on the right in order to be explicit, but in the last line it is assumed that addition is mod 21, since the the operation is taking place in $\mathbb{Z}/21\mathbb{Z}$. □

2. (Exercise 9 in DF §10.2.) Let R be a commutative ring (with 1) and M a left R-module. Prove that $\mathrm{Hom}_R(R, M)$ and M are isomorphic as left R-modules. (Hint: Show that each element of $\mathrm{Hom}_R(R, M)$ is determined by its value at 1_R.)

Proof. For any $\varphi \in \mathrm{Hom}_R(R, M)$, we must have $\varphi(r) = r \cdot \varphi(1_R)$ for any $r \in R$, so φ is completely determined by the image of 1_R. Also, for any $m \in M$ there exists a homomorphism φ_m defined by $\varphi_m(r) = r \cdot m$, since $\varphi_m(zx + y) = (zx + y) \cdot m = z \cdot (x \cdot m) + y \cdot m = z \cdot \varphi_m(x) + \varphi_m(y)$. Therefore, $\mathrm{Hom}_R(R, M)$ is the set of all maps φ_m, for all $m \in M$.

Define $f : M \to \mathrm{Hom}_R(R, M)$ by $m \mapsto \varphi_m$. Letting $r \in R$ and $m, n \in m$, we have $f(rm+n)(x) = \varphi_{rm+n}(x) = x \cdot (rm + n) = (xr) \cdot m + x \cdot n = (rx) \cdot m + x \cdot n = r \cdot (x \cdot m) + x \cdot n = r \cdot \varphi_m(x) + \varphi_n(x) = r \cdot f(m)(x) + f(n)(x)$ for all $x \in R$, thus $f(rm + n)$ is a homomorphism. f is injective because, for $m, n \in M$, if $f(m) = f(n)$ then $m = \varphi_m(1_R) = \varphi_n(1_R) = n$. f is surjective because we have shown that every element of $\mathrm{Hom}_R(R, M)$ is φ_m for some $m \in M$. Thus f is an isomorphism. □

3. (Exercise 14 in DF §10.2.) Let $R = \mathbf{Z}[x]$ be the ring of polynomials in x, and let $A = \mathbf{Z}[t_1, t_2, \ldots]$ be the ring of polynomials in the (infinitely many) independent indeterminates $t_1, t_2, \ldots$. (That is, $A = \cup_{i \in \mathbf{N}} \mathbf{Z}[t_1, \ldots, t_i]$.)

Define an action of R on A as follows:

(1) let 1_R act on A as the identity (i.e., $1_R \cdot a = a$ for every $a \in A$);

(2) for each $n \geq 1$ let $x^n \cdot 1_A = t_n$, let $x^n \cdot t_i = t_{n+i}$ for each $i \in \mathbf{N}$, and let x^n act as 0 on monomials in A of total degree at least 2 (e.g., $x^n \cdot t_1^2 = x^n \cdot t_1 t_2 = x^n \cdot t_1^3 = 0_A$);

(3) extend the above properties $\mathbf{Z}$-linearly, so that module axioms 2(a) and 2(c) (from the definition on page 337) are satisfied.

(a) Show that $x^{p+q} \cdot t_i = x^p \cdot (x^q \cdot t_i) = t_{p+q+i}$ for each $i \in \mathbf{N}$ and $p, q \in \mathbf{Z}_{\geq 0}$. Use this to show that under this action the ring A is an R-module.

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

Proof. Let $p, q \in \mathbb{Z}_{\geq 0}$. Note that $x^n \cdot t_i = x_{n+i}$ still holds even if $n = 0$, since $x^0 \cdot t_i = 1_R \cdot t_i = t_i = t_{0+i}$, so it is okay if $p = q = 0$. Then $x^{p+q} \cdot t_i = t_{p+q+i}$ by (2). Also, $t_{p+q+i} = x^p \cdot t_{q+i} = x^p \cdot (x^q \cdot t_i)$. So the first statement of (a) holds.

We have defined this action so that parts (a), (c), and (d) of the left R-module axioms hold. We will now show that (b) holds. Let $a = a_0 + a_1 x + \cdots + a_n x^n$ and $b = b_0 + b_1 x + \cdots + b_m x^m$ be polynomials in R, and let $c \in A$. We will show by induction on the number of terms in c that $a \cdot (b \cdot c) = (ab) \cdot c$.

Suppose c contains only one term $c_0 t$, where t is some product of indeterminates. First, assume t is a product of at most one indeterminate t_k, where if $t = 1_A$ then $k = 0$ (for convenience).

$$\begin{aligned}
a \cdot (b \cdot c) &= \left(\sum_{i=0}^{n} a_i x^i \right) \cdot \left(\sum_{j=0}^{m} b_j x^j \cdot c_0 t_k \right) \\
&= \left(\sum_{i=0}^{n} a_i x^i \right) \cdot \left(\sum_{j=0}^{m} b_j c_0 t_{j+k} \right) \\
&= \sum_{i=0}^{n} \sum_{j=0}^{m} a_i x^i \cdot b_j c_0 t_{j+k} \\
&= \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j c_0 t_{i+j+k} \\
&= \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j} \cdot c_0 t_k = (ab) \cdot c.
\end{aligned}$$

Now, assume that t is a product of more than one indeterminate. Then

$$\begin{aligned}
a \cdot (b \cdot c) &= \left(\sum_{i=0}^{n} a_i x^i \right) \cdot \left(\sum_{j=0}^{m} b_j x^j \cdot c_0 t \right) \\
&= \left(\sum_{i=0}^{n} a_i x^i \right) \cdot \left(b_0 c_0 t + \sum_{j=1}^{m} 0_A \right) \\
&= \left(\sum_{i=0}^{n} a_i x^i \right) \cdot (b_0 c_0 t) \\
&= \sum_{i=0}^{n} a_i x^i \cdot b_0 c_0 t \\
&= a_0 b_0 c_0 t + \sum_{i=1}^{n} 0_A = a_0 b_0 c_0 t.
\end{aligned}$$

Also,

$$(a \cdot b) \cdot c = \left(\sum_{i=0}^{n} a_i x^i \sum_{j=0}^{m} b_j x^j \right) \cdot c_0 t = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j} \cdot c_0 t = a_0 b_0 c_0 t + \sum_{i \neq 0 \text{ or } j \neq 0} 0_A = a_0 b_0 c_0 t.$$

Next, assume (b) holds whenever c has at most $k \geq 1$ terms (this is a new definition of k) terms, and assume c has $k + 1$ terms. Then $c = c_1 + c_2$ for some $c_1, c_2 \in A$ each with at most k terms. So

$$a \cdot (b \cdot c) = a \cdot (b \cdot (c_1 + c_2)) = a \cdot (b \cdot c_1 + b \cdot c_2) = a \cdot (b \cdot c_1) + a \cdot (b \cdot c_2) = (a \cdot b) \cdot c_2 + (a \cdot b) \cdot c_2 = (a \cdot b) \cdot (c_1 + c_2) = (a \cdot b) \cdot c$$

thus (b) holds in general, so A is a left R-module.

Let $\varphi : R \to A$ be defined by $\varphi(r) = r \cdot 1_A$. We have just shown in the previous exercise that this is an R-module homomorphism (this is φ_m where $m = 1_A$). However, φ is not a ring homomorphism because

$$\varphi(x^2) = x^2 \cdot 1_A = t_2 \neq t_1^2 = (x \cdot 1_A)^2 = \varphi(x)^2.$$

□

4. (Exercise 2 in DF §10.3.) Let R be a commutative ring with 1, and suppose $n, m \in \mathbf{N}$. Prove that $R^n \cong R^m$ if and only if $n = m$. (That is, two free R-modules of finite rank are isomorphic if and only if they have the same rank.)

   (Hint: Apply Exercise 12 of §10.2, which you may assume without proof, with I chosen to be a maximal ideal of R (which exists by Proposition 11 in §7.4, assuming Zorn's lemma). You may assume without proof the corresponding result for vector spaces, i.e. if F is a field, then $F^n \cong F^m$ if and only if $n = m$. (This is proved in §11.1.))

   Proof. We may assume R is not a field, since we are taking the result for granted in that case. Therefore, R contains a nonzero, proper ideal; by Proposition 11 in §7.4, this ideal must be contained in some maximal ideal I. R is commutative, so $IR = I$ and $R/IR = R/I$ is a field. Therefore, by the result we are taking for granted, $(R/IR)^n \cong (R/IR)^m$ if and only if $n = m$. By Exercise 12 of §10.2, $R^k/IR^k \cong (R/IR)^k$, so $R^n/IR^n \cong (R/IR)^n \cong (R/IR)^m \cong R^m/IR^m$ if and only if $n = m$.

   Clearly, $R^n \cong R^m$ if $n = m$, so assume that $n \neq m$ but $R^n \cong R^m$. Let $\varphi : R^n \to R^m$ be an isomorphism, and let $\overline{\varphi} : R^n \to R^m/IR^m$ be the composition of φ with the natural projection $R^m \to R^m/IR^m$.

   First, let $x \in IR^n$. Then $x = r_1x_1 + \cdots + r_kx_k$ for some $r_i \in I$, $x_i \in R^n$. Thus $\varphi(x) = r_1\varphi(x_1) + \cdots r_k\varphi(x_k) \in IR^m$ since $r_i \in I$ and $\varphi(x_i) \in R^m$. So $\varphi(x) \in 0 + IR^m$, thus $x \in \ker(\overline{\varphi})$.

   Conversely, assume $x \in \ker(\overline{\varphi})$. Then $x \mapsto 0 + IR^m$, so $\varphi(x) \in IR^m$. So $\varphi(x) = r_1x_1 + \cdots + r_kx_k$ for some $r_i \in I$, $x_i \in R^m$. So $x = r_1\varphi^{-1}(x_1) + \cdots + r_k\varphi^{-1}(x_k) \in IR^n$. So $\ker(\overline{\varphi}) = IR^n$, thus by the first isomorphism theorem $R^n/IR^n \cong R^m/IR^m$. This contradicts the result of the previous paragraph. □

5. (Exercise 6 in DF §10.3.) Let R be a ring with 1 and M a left R-module. Prove that if M is a finitely generated R-module having a generating set A with n elements, then every quotient of M is also generated by n or fewer elements.

   Proof. Suppose M is finitely generated by a set $A = \{a_1, \ldots, a_n\}$, and let N be a submodule of M. We will show that M/N is finitely generated by the set $A_N = \{a_1 + N, \ldots, a_n + N\}$, which has at most n elements.

   Any element of M/N is of the form $x + N$ for some $x \in M$, which we can represent as $x = r_1a_1 + \cdots r_na_n$ for some $r_1, \ldots, r_n \in R$. So $x + N = (r_1a_1 + \cdots + r_na_n) + N = (r_1a_1 + N) + \cdots + (r_na_n + N) = r_1(a_1 + N) + \cdots + r_n(a_n + N) \in RA_N$, thus M/N is generated by A_N. □

6. (Exercise 7 in DF §10.3.) Let R be a ring with 1 and M a left R-module. Let N be a submodule of M. Prove that if both M/N and N are finitely generated, then so is M.

   Proof. Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1 + N, \ldots, b_m + N\}$ be generating sets for M/N and N, respectively, where $a_i, b_i \in M$. Let $x \in M$. x must fall into some coset $y + N$ (since the cosets partition M), which has a representation $y + N = r_1(b_1 + N) + \cdots + r_m(b_m + N) = (r_1b_1 + \cdots + r_mb_m) + N$ for some $r_1, \ldots, r_m \in R$. This means that $x = (r_1b_1 + \cdots + r_mb_m) + n$ for some $n \in N$. But n has a representation $n = s_1a_1 + \cdots + s_na_n$. Therefore, $x = r_1b_1 + \cdots + r_mb_m + s_1a_1 + \cdots + s_na_n$. So the finite set $\{a_1, \ldots, a_n, b_1 \ldots, b_m\}$ generates M. □

7. (Exercise 13 in DF §10.3.) Let R be a commutative ring with 1 and let F be a free R-module of finite rank (that is, a free R-module that is finitely generated). Prove that $\mathrm{Hom}_R(F, R)$ and F are isomorphic as R-modules.

   Proof. Let $A = \{a_1, \ldots, a_n\}$ be a basis for F over R. Any $\varphi \in \mathrm{Hom}_R(F, R)$ satisfies $\varphi(r_1a_1 + \cdots r_na_n) = r_1\varphi(a_1) + \cdots + r_n\varphi(a_n)$, therefore φ is completely determined by its action on this basis. So denote by $\varphi_{(b_1,\ldots,b_n)}$ the homomorphism which takes a_i to $b_i \in R$ for each i, and let $f : F \to \mathrm{Hom}(F, R)$ be given by $r_1a_1 + \cdots + r_na_n \mapsto \varphi_{(r_1,\ldots,r_n)}$. Since F is generated by A, this defines f completely. Since F is free on A, f is injective. Since every homomorphism is of this form, f is surjective. So f is an isomorphism. □