Finally, to see that (3) implies (1) observe first that the map $\pi$ is clearly a surjective $R$-module homomorphism. Then (3) simply implies $\pi$ is injective, hence is an isomorphism, completing the proof.

If an $R$-module $M = N_1 + N_2 + \cdots + N_k$ is the sum of submodules $N_1, N_2, \ldots, N_k$ of $M$ satisfying the equivalent conditions of the proposition above, then $M$ is said to be the *(internal) direct sum* of $N_1, N_2, \ldots, N_k$, written

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_k.$$

By the proposition, this is equivalent to the assertion that every element $m$ of $M$ can be written *uniquely* as a sum of elements $m = n_1 + n_2 + \cdots + n_k$ with $n_i \in N_i$. (Note that part (1) of the proposition is the statement that the internal direct sum of $N_1, N_2, \ldots, N_k$ is isomorphic to their external direct sum, which is the reason we identify them and use the same notation for both.)

**Definition.** An $R$-module $F$ is said to be *free* on the subset $A$ of $F$ if for every nonzero element $x$ of $F$, there exist unique nonzero elements $r_1, r_2, \ldots, r_n$ of $R$ and unique $a_1, a_2, \ldots, a_n$ in $A$ such that $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$, for some $n \in \mathbb{Z}^+$. In this situation we say $A$ is a *basis* or *set of free generators* for $F$. If $R$ is a commutative ring the cardinality of $A$ is called the *rank* of $F$ (cf. Exercise 27).

One should be careful to note the difference between the uniqueness property of direct sums (Proposition 5(3)) and the uniqueness property of free modules. Namely, in the direct sum of two modules, say $N_1 \oplus N_2$, each element can be written uniquely as $n_1 + n_2$; here the uniqueness refers to the *module elements* $n_1$ and $n_2$. In the case of free modules, the uniqueness is on the *ring elements as well as the module elements*. For example, if $R = \mathbb{Z}$ and $N_1 = N_2 = \mathbb{Z}/2\mathbb{Z}$, then each element of $N_1 \oplus N_2$ has a unique representation in the form $n_1 + n_2$ where each $n_i \in N_i$, however $n_1$ (for instance) can be expressed as $n_1$ or $3n_1$ or $5n_1 \ldots$ etc., so each element does not have a unique representation in the form $r_1a_1 + r_2a_2$, where $r_1, r_2 \in R$, $a_1 \in N_1$ and $a_2 \in N_2$. Thus $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}$-module on the set $\{(1,0), (0,1)\}$. Similarly, it is not free on any set.

**Theorem 6.** For any set $A$ there is a free $R$-module $F(A)$ on the set $A$ and $F(A)$ satisfies the following *universal property:* if $M$ is any $R$-module and $\varphi : A \to M$ is any map of sets, then there is a unique $R$-module homomorphism $\Phi : F(A) \to M$ such that $\Phi(a) = \varphi(a)$, for all $a \in A$, that is, the following diagram commutes.

$$\begin{tikzcd}
A \arrow[r, "\text{inclusion}"] \arrow[dr, "\varphi"'] & F(A) \arrow[d, "\Phi"] \\
& M
\end{tikzcd}$$

When $A$ is the finite set $\{a_1, a_2, \ldots, a_n\}$, $F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n \cong R^n$. (Compare: Section 6.3, free groups.)

*Proof:* Let $F(A) = \{0\}$ if $A = \emptyset$. If $A$ is nonempty let $F(A)$ be the collection of all set functions $f : A \to R$ such that $f(a) = 0$ for all but finitely many $a \in A$. Make

$F(A)$ into an $R$-module by pointwise addition of functions and pointwise multiplication of a ring element times a function, i.e.,

$$\begin{aligned}(f+g)(a) &= f(a)+g(a) \quad \text{and}\\ (rf)(a) &= r(f(a)), \qquad \text{for all } a \in A,\ r \in R \text{ and } f, g \in F(A).\end{aligned}$$

It is an easy matter to check that all the $R$-module axioms hold (the details are omitted). Identify $A$ as a subset of $F(A)$ by $a \mapsto f_a$, where $f_a$ is the function which is 1 at $a$ and zero elsewhere. We can, in this way, think of $F(A)$ as all finite $R$-linear combinations of elements of $A$ by identifying each function $f$ with the sum $r_1a_1 + r_2a_2 + \cdots + r_na_n$, where $f$ takes on the value $r_i$ at $a_i$ and is zero at all other elements of $A$. Moreover, each element of $F(A)$ has a unique expression as such a formal sum. To establish the universal property of $F(A)$ suppose $\varphi : A \to M$ is a map of the set $A$ into the $R$-module $M$. Define $\Phi : F(A) \to M$ by

$$\Phi : \sum_{i=1}^{n} r_ia_i \mapsto \sum_{i=1}^{n} r_i\varphi(a_i).$$

By the uniqueness of the expression for the elements of $F(A)$ as linear combinations of the $a_i$ we see easily that $\Phi$ is a well defined $R$-module homomorphism (the details are left as an exercise). By definition, the restriction of $\Phi$ to $A$ equals $\varphi$. Finally, since $F(A)$ is generated by $A$, once we know the values of an $R$-module homomorphism on $A$ its values on every element of $F(A)$ are uniquely determined, so $\Phi$ is the unique extension of $\varphi$ to all of $F(A)$.

When $A$ is the finite set $\{a_1, a_2, \ldots, a_n\}$ Proposition 5(3) shows that $F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n$. Since $R \cong Ra_i$ for all $i$ (under the map $r \mapsto ra_i$) Proposition 5(1) shows that the direct sum is isomorphic to $R^n$.

**Corollary 7.**

(1) If $F_1$ and $F_2$ are free modules on the same set $A$, there is a unique isomorphism between $F_1$ and $F_2$ which is the identity map on $A$.

(2) If $F$ is any free $R$-module with basis $A$, then $F \cong F(A)$. In particular, $F$ enjoys the same universal property with respect to $A$ as $F(A)$ does in Theorem 6.

*Proof:* Exercise.

If $F$ is a free $R$-module with basis $A$, we shall often (particularly in the case of vector spaces) define $R$-module homomorphisms from $F$ into other $R$-modules simply by specifying their values on the elements of $A$ and then saying "*extend by linearity.*" Corollary 7(2) ensures that this is permissible.

When $R = \mathbb{Z}$, the free module on a set $A$ is called the *free abelian group on A.* If $|A| = n$, $F(A)$ is called the free abelian group of *rank n* and is isomorphic to $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ ($n$ times). These definitions agree with the ones given in Chapter 5.

## EXERCISES

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

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

**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.]

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

**4.** An $R$-module $M$ is called a *torsion* module if for each $m \in M$ there is a nonzero element $r \in R$ 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.

**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.

**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.

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

**8.** Let $S$ be the collection of sequences $(a_1, a_2, a_3, \ldots)$ of integers $a_1, a_2, a_3, \ldots$ 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.

**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 generator. Determine all the irreducible $\mathbb{Z}$-modules.

**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 there is a natural map $R \to M$ defined by $r \mapsto rm$, where $m$ is any fixed nonzero element of $M$.]

**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.]

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

**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: $\text{Hom}_R(F, R) \cong F$.