13

Modules and vector spaces

In this chapter, we introduce the basic definitions and results concerning modules over a ring R and vector spaces over a field F. The reader may have seen some of these notions before, but perhaps only in the context of vector spaces over a specific field, such as the real or complex numbers, and not in the context of, say, finite fields like $\mathbb{Z}_p$.

13.1 Definitions, basic properties, and examples

Throughout this section, R denotes a ring (i.e., a commutative ring with unity).

Definition 13.1. *An R-**module** is a set M together with an addition operation on M and a function $\mu : R \times M \to M$, such that the set M under addition forms an abelian group, and moreover, for all $c, d \in R$ and $\alpha, \beta \in M$, we have:*

(i) $\mu(c, \mu(d, \alpha)) = \mu(cd, \alpha)$;

(ii) $\mu(c + d, \alpha) = \mu(c, \alpha) + \mu(d, \alpha)$;

(iii) $\mu(c, \alpha + \beta) = \mu(c, \alpha) + \mu(c, \beta)$;

(iv) $\mu(1_R, \alpha) = \alpha$.

One may also call an R-module M a **module over** R, and elements of R are sometimes called **scalars**. The function μ in the definition is called a **scalar multiplication map**, and the value $\mu(c, \alpha)$ is called the **scalar product** of c and α. Usually, we shall simply write $c\alpha$ (or $c \cdot \alpha$) instead of $\mu(c, \alpha)$. When we do this, properties (i)–(iv) of the definition may be written as follows:

$$c(d\alpha) = (cd)\alpha, \quad (c + d)\alpha = c\alpha + d\alpha, \quad c(\alpha + \beta) = c\alpha + c\beta, \quad 1_R\alpha = \alpha.$$

Note that there are two addition operations at play here: addition in R (such as $c + d$) and addition in M (such as $\alpha + \beta$). Likewise, there are two multiplication operations at play: multiplication in R (such as cd) and scalar multiplication (such

as $c\alpha$). Note that by property (i), we may write $cd\alpha$ without any ambiguity, as both possible interpretations, $c(d\alpha)$ and $(cd)\alpha$, yield the same value.

For fixed $c \in R$, the map that sends $\alpha \in M$ to $c\alpha \in M$ is a group homomorphism with respect to the additive group operation of M (by property (iii) of the definition); likewise, for fixed $\alpha \in M$, the map that sends $c \in R$ to $c\alpha \in M$ is a group homomorphism from the additive group of R into the additive group of M (by property (ii)). Combining these observations with basic facts about group homomorphisms (see Theorem 6.19), we may easily derive the following basic facts about R-modules:

Theorem 13.2. *If M is a module over R, then for all $c \in R$, $\alpha \in M$, and $k \in \mathbb{Z}$, we have:*

(i) $0_R \cdot \alpha = 0_M$;

(ii) $c \cdot 0_M = 0_M$;

(iii) $(-c)\alpha = -(c\alpha) = c(-\alpha)$;

(iv) $(kc)\alpha = k(c\alpha) = c(k\alpha)$.

Proof. Exercise. □

An R-module M may be **trivial**, consisting of just the zero element 0_M. If R is the trivial ring, then any R-module M is trivial, since for every $\alpha \in M$, we have $\alpha = 1_R\alpha = 0_R\alpha = 0_M$.

Example 13.1. The ring R itself can be viewed as an R-module in the obvious way, with addition and scalar multiplication defined in terms of the addition and multiplication operations of R. □

Example 13.2. The set $R^{\times n}$, which consists of all of n-tuples of elements of R, forms an R-module, with addition and scalar multiplication defined componentwise: for $\alpha = (a_1, \ldots, a_n) \in R^{\times n}$, $\beta = (b_1, \ldots, b_n) \in R^{\times n}$, and $c \in R$, we define

$$\alpha + \beta := (a_1 + b_1, \ldots, a_n + b_n) \text{ and } c\alpha := (ca_1, \ldots, ca_n). \quad \square$$

Example 13.3. The ring of polynomials $R[X]$ over R forms an R-module in the natural way, with addition and scalar multiplication defined in terms of the addition and multiplication operations of the polynomial ring. □

Example 13.4. As in Example 7.39, let f be a non-zero polynomial over R with $\mathrm{lc}(f) \in R^*$, and consider the quotient ring $E := R[X]/(f)$. Then E is a module over R, with addition defined in terms of the addition operation of E, and scalar multiplication defined by $c[g]_f := [c]_f \cdot [g]_f = [cg]_f$, for $c \in R$ and $g \in R[X]$. □

Example 13.5. Generalizing Example 13.3, if E is any ring containing R as a

subring (i.e., E is an extension ring of R), then E is a module over R, with addition and scalar multiplication defined in terms of the addition and multiplication operations of E. □

Example 13.6. Any abelian group G, written additively, can be viewed as a $\mathbb{Z}$-module, with scalar multiplication defined in terms of the usual integer multiplication map (see Theorem 6.4). □

Example 13.7. Let G be any group, written additively, whose exponent divides n. Then we may define a scalar multiplication that maps $[k]_n \in \mathbb{Z}_n$ and $\alpha \in G$ to $k\alpha$. That this map is unambiguously defined follows from the fact that G has exponent dividing n, so that if $k \equiv k' \pmod{n}$, we have $k\alpha - k'\alpha = (k - k')\alpha = 0_G$, since $n \mid (k - k')$. It is easy to check that this scalar multiplication map indeed makes G into a $\mathbb{Z}_n$-module. □

Example 13.8. Of course, viewing a group as a module does not depend on whether or not we happen to use additive notation for the group operation. If we specialize the previous example to the group $G = \mathbb{Z}_p^*$, where p is prime, then we may view G as a $\mathbb{Z}_{p-1}$-module. However, since the group operation itself is written multiplicatively, the "scalar product" of $[k]_{p-1} \in \mathbb{Z}_{p-1}$ and $\alpha \in \mathbb{Z}_p^*$ is the power α^k. □

Example 13.9. If $M_1, \ldots, M_k$ are R-modules, then so is their direct product $M_1 \times \cdots \times M_k$, where addition and scalar product are defined component-wise. If $M = M_1 = \cdots = M_k$, we write this as $M^{\times k}$. □

Example 13.10. If I is an arbitrary set, and M is an R-module, then $\mathrm{Map}(I, M)$, which is the set of all functions $f : I \to M$, may be naturally viewed as an R-module, with point-wise addition and scalar multiplication: for $f, g \in \mathrm{Map}(I, M)$ and $c \in R$, we define

$$(f + g)(i) := f(i) + g(i) \text{ and } (cf)(i) := cf(i) \text{ for all } i \in I. \quad \square$$

13.2 Submodules and quotient modules

Again, throughout this section, R denotes a ring. The notions of subgroups and quotient groups extend in the obvious way to R-modules.

Definition 13.3. *Let M be an R-module. A subset N of M is a* ***submodule (over R) of M*** *if*

(i) N is a subgroup of the additive group M, and

(ii) $c\alpha \in N$ for all $c \in R$ and $\alpha \in N$ (i.e., N is closed under scalar multiplication).

It is easy to see that a submodule N of an R-module M is also an R-module in its own right, with addition and scalar multiplication operations inherited from M.

Expanding the above definition, we see that a non-empty subset N of M is a submodule if and only if for all $c \in R$ and all $\alpha, \beta \in N$, we have

$$\alpha + \beta \in N, \quad -\alpha \in N, \quad \text{and} \quad c\alpha \in N.$$

Observe that the condition $-\alpha \in N$ is redundant, as it is implied by the condition $c\alpha \in N$ with $c = -1_R$.

Clearly, $\{0_M\}$ and M are submodules of M. For $k \in \mathbb{Z}$, it is easy to see that not only are kM and $M\{k\}$ subgroups of M (see Theorems 6.7 and 6.8), they are also submodules of M. Moreover, for $c \in R$,

$$cM := \{c\alpha : \alpha \in M\} \quad \text{and} \quad M\{c\} := \{\alpha \in M : c\alpha = 0_M\}$$

are also submodules of M. Further, for $\alpha \in M$,

$$R\alpha := \{c\alpha : c \in R\}$$

is a submodule of M. Finally, if N_1 and N_2 are submodules of M, then $N_1 + N_2$ and $N_1 \cap N_2$ are not only subgroups of M, they are also submodules of M. We leave it to the reader to verify all these facts: they are quite straightforward.

Let $\alpha_1, \ldots, \alpha_k \in M$. The submodule

$$R\alpha_1 + \cdots + R\alpha_k$$

is called the **submodule (over R) generated by** $\alpha_1, \ldots, \alpha_k$. It consists of all **$R$-linear combinations**

$$c_1\alpha_1 + \cdots + c_k\alpha_k,$$

where the c_i's are elements of R, and is the smallest submodule of M that contains the elements $\alpha_1, \ldots, \alpha_k$. We shall also write this submodule as $\langle \alpha_1, \ldots, \alpha_k \rangle_R$. As a matter of definition, we allow $k = 0$, in which case this submodule is $\{0_M\}$. We say that M is **finitely generated (over R)** if $M = \langle \alpha_1, \ldots, \alpha_k \rangle_R$ for some $\alpha_1, \ldots, \alpha_k \in M$.

Example 13.11. For a given integer $\ell \geq 0$, define $R[X]_{<\ell}$ to be the set of polynomials of degree less than ℓ. The reader may verify that $R[X]_{<\ell}$ is a submodule of the R-module $R[X]$, and indeed, is the submodule generated by $1, X, \ldots, X^{\ell-1}$. If $\ell = 0$, then this submodule is the trivial submodule $\{0_R\}$. □

Example 13.12. Let G be an abelian group. As in Example 13.6, we can view G as a $\mathbb{Z}$-module in a natural way. Subgroups of G are just the same thing as submodules of G, and for $a_1, \ldots, a_k \in G$, the subgroup $\langle a_1, \ldots, a_k \rangle$ is the same as the submodule $\langle a_1, \ldots, a_k \rangle_{\mathbb{Z}}$. □

Example 13.13. As in Example 13.1, we may view the ring R itself as an R-module. With respect to this module structure, ideals of R are just the same thing as submodules of R, and for $a_1, \ldots, a_k \in R$, the ideal $(a_1, \ldots, a_k)$ is the same as the submodule $\langle a_1, \ldots, a_k \rangle_R$. Note that for $a \in R$, the ideal generated by a may be written either as aR, using the notation introduced in §7.3, or as Ra, using the notation introduced in this section. □

Example 13.14. If E is an extension ring of R, then we may view E as an R-module, as in Example 13.5. It is easy to see that every ideal of E is a submodule; however, the converse is not true in general. Indeed, the submodule $R[X]_{<\ell}$ of $R[X]$ discussed in Example 13.11 is not an ideal of the ring $R[X]$. □

If N is a submodule of M, then in particular, it is also a subgroup of M, and we can form the quotient group M/N in the usual way (see §6.3), which consists of all cosets $[\alpha]_N$, where $\alpha \in M$. Moreover, because N is closed under scalar multiplication, we can also define a scalar multiplication on M/N in a natural way. Namely, for $c \in R$ and $\alpha \in M$, we define

$$c \cdot [\alpha]_N := [c\alpha]_N.$$

As usual, one must check that this definition is unambiguous, which means that $c\alpha \equiv c\alpha' \pmod{N}$ whenever $\alpha \equiv \alpha' \pmod{N}$. But this follows (as the reader may verify) from the fact that N is closed under scalar multiplication. One can also easily check that with scalar multiplication defined in this way, M/N is an R-module; it is called the **quotient module (over R) of M modulo N**.

Example 13.15. Suppose E is an extension ring of R, and I is an ideal of E. Viewing E as an R-module, I is a submodule of E, and hence the quotient ring E/I may naturally be viewed as an R-module, with scalar multiplication defined by $c \cdot [\alpha]_I := [c\alpha]_I$ for $c \in R$ and $\alpha \in E$. Example 13.4 is a special case of this, applied to the extension ring $R[X]$ and the ideal (f). □

EXERCISE 13.1. Show that if N is a submodule of an R-module M, then a set $P \subseteq N$ is a submodule of M if and only if P is a submodule of N.

EXERCISE 13.2. Let M_1 and M_2 be R-modules, and let N_1 be a submodule of M_1 and N_2 a submodule of M_2. Show that $N_1 \times N_2$ is a submodule of $M_1 \times M_2$.

EXERCISE 13.3. Show that if R is non-trivial, then the R-module $R[X]$ is not finitely generated.

13.3 Module homomorphisms and isomorphisms

Again, throughout this section, R is a ring. The notion of a group homomorphism extends in the obvious way to R-modules.

Definition 13.4. *Let M and M' be modules over R. An **R-module homomorphism** from M to M' is a function $\rho : M \to M'$, such that*

(i) ρ is a group homomorphism from M to M', and

(ii) $\rho(c\alpha) = c\rho(\alpha)$ for all $c \in R$ and $\alpha \in M$.

An R-module homomorphism is also called an **R-linear map**. We shall use this terminology from now on. Expanding the definition, we see that a map $\rho : M \to M'$ is an R-linear map if and only if $\rho(\alpha + \beta) = \rho(\alpha) + \rho(\beta)$ and $\rho(c\alpha) = c\rho(\alpha)$ for all $\alpha, \beta \in M$ and all $c \in R$.

Example 13.16. If N is a submodule of an R-module M, then the inclusion map $i : N \to M$ is obviously an R-linear map. □

Example 13.17. Suppose N is a submodule of an R-module M. Then the *natural map* (see Example 6.36)

$$\begin{aligned} \rho : \quad & M \to M/N \\ & \alpha \mapsto [\alpha]_N \end{aligned}$$

is not just a group homomorphism, it is also easily seen to be an R-linear map. □

Example 13.18. Let M be an R-module, and let k be an integer. Then the k-multiplication map on M (see Example 6.38) is not only a group homomorphism, but it is also easily seen to be an R-linear map. Its image is the submodule kM, and its kernel the submodule $M\{k\}$. □

Example 13.19. Let M be an R-module, and let c be an element of R. The map

$$\begin{aligned} \rho : \quad & M \to M \\ & \alpha \mapsto c\alpha \end{aligned}$$

is called **c-multiplication map on M**, and is easily seen to be an R-linear map whose image is the submodule cM, and whose kernel is the submodule $M\{c\}$. The set of all $c \in R$ for which $cM = \{0_M\}$ is called the **R-exponent of M**, and is easily seen to be an ideal of R. □

Example 13.20. Let M be an R-module, and let α be an element of M. The map

$$\begin{aligned} \rho : \quad & R \to M \\ & c \mapsto c\alpha \end{aligned}$$

is easily seen to be an R-linear map whose image is the submodule $R\alpha$ (i.e., the submodule generated by α). The kernel of this map is called the **R-order of α**, and is easily seen to be an ideal of R. □

Example 13.21. Generalizing the previous example, let M be an R-module, and let $\alpha_1, \ldots, \alpha_k$ be elements of M. The map

$$\begin{aligned} \rho : \quad & R^{\times k} \to M \\ & (c_1, \ldots, c_k) \mapsto c_1\alpha_1 + \cdots + c_k\alpha_k \end{aligned}$$

is easily seen to be an R-linear map whose image is the submodule $R\alpha_1 + \cdots + R\alpha_k$ (i.e., the submodule generated by $\alpha_1, \ldots, \alpha_k$). □

Example 13.22. Suppose that $M_1, \ldots, M_k$ are submodules of an R-module M. Then the map

$$\begin{aligned} \rho : \quad & M_1 \times \cdots \times M_k \to M \\ & (\alpha_1, \ldots, \alpha_k) \mapsto \alpha_1 + \cdots + \alpha_k \end{aligned}$$

is easily seen to be an R-linear map whose image is the submodule $M_1 + \cdots + M_k$. □

Example 13.23. Let E be an extension ring of R. As we saw in Example 13.5, E may be viewed as an R-module in a natural way. Let $\alpha \in E$, and consider the α-multiplication map on E, which sends $\beta \in E$ to $\alpha\beta \in E$. Then it is easy to see that this is an R-linear map. □

Example 13.24. Let E and E' be extension rings of R, which may be viewed as R-modules as in Example 13.5. Suppose that $\rho : E \to E'$ is a ring homomorphism whose restriction to R is the identity map (i.e., $\rho(c) = c$ for all $c \in R$). Then ρ is an R-linear map. Indeed, for every $c \in R$ and $\alpha, \beta \in E$, we have $\rho(\alpha+\beta) = \rho(\alpha)+\rho(\beta)$ and $\rho(c\alpha) = \rho(c)\rho(\alpha) = c\rho(\alpha)$. □

Example 13.25. Let G and G' be abelian groups. As we saw in Example 13.6, G and G' may be viewed as $\mathbb{Z}$-modules. In addition, every group homomorphism $\rho : G \to G'$ is also a $\mathbb{Z}$-linear map. □

Since an R-module homomorphism is also a group homomorphism on the underlying additive groups, all of the statements in Theorem 6.19 apply. In particular, an R-linear map is injective if and only if the kernel is trivial (i.e., contains only the zero element). However, in the case of R-module homomorphisms, we can extend Theorem 6.19, as follows:

Theorem 13.5. *Let $\rho : M \to M'$ be an R-linear map. Then:*

(i) for every submodule N of M, $\rho(N)$ is a submodule of M'; in particular (setting $N := M$), $\operatorname{Im}\rho$ is a submodule of M';

(ii) *for every submodule N' of M', $\rho^{-1}(N')$ is a submodule of M'; in particular (setting $N' := \{0_{M'}\}$),* $\operatorname{Ker}\rho$ *is a submodule of M.*

Proof. Exercise. □

Theorems 6.20 and 6.21 have natural R-module analogs, which the reader may easily verify:

Theorem 13.6. *If $\rho : M \to M'$ and $\rho' : M' \to M''$ are R-linear maps, then so is their composition $\rho' \circ \rho : M \to M''$.*

Theorem 13.7. *Let $\rho_i : M \to M_i'$, for $i = 1, \ldots, k$, be R-linear maps. Then the map*

$$\begin{aligned} \rho : \quad & M \to M_1' \times \cdots \times M_k' \\ & \alpha \mapsto (\rho_1(\alpha), \ldots, \rho_k(\alpha)) \end{aligned}$$

is an R-linear map.

If an R-linear map $\rho : M \to M'$ is bijective, then it is called an **R-module isomorphism** of M with M'. If such an R-module isomorphism ρ exists, we say that M **is isomorphic to** M', and write $M \cong M'$. Moreover, if $M = M'$, then ρ is called an **R-module automorphism** on M.

Theorems 6.22–6.26 also have natural R-module analogs, which the reader may easily verify:

Theorem 13.8. *If ρ is an R-module isomorphism of M with M', then the inverse function ρ^{-1} is an R-module isomorphism of M' with M.*

Theorem 13.9 (First isomorphism theorem). *Let $\rho : M \to M'$ be an R-linear map with kernel K and image N'. Then we have an R-module isomorphism*

$$M/K \cong N'.$$

Specifically, the map

$$\begin{aligned} \bar{\rho} : \quad & M/K \to M' \\ & [\alpha]_K \mapsto \rho(\alpha) \end{aligned}$$

is an injective R-linear map whose image is N'.

Theorem 13.10. *Let $\rho : M \to M'$ be an R-linear map. Then for every submodule N of M with $N \subseteq \operatorname{Ker}\rho$, we may define an R-linear map*

$$\begin{aligned} \bar{\rho} : \quad & M/N \to M' \\ & [\alpha]_N \mapsto \rho(\alpha). \end{aligned}$$

Moreover, $\operatorname{Im}\bar{\rho} = \operatorname{Im}\rho$, *and $\bar{\rho}$ is injective if and only if* $N = \operatorname{Ker}\rho$.

Theorem 13.11 (Internal direct product). *Let M be an R-module with submodules N_1, N_2, where $N_1 \cap N_2 = \{0_M\}$. Then we have an R-module isomorphism*

$$N_1 \times N_2 \cong N_1 + N_2$$

given by the map

$$\begin{aligned} \rho : \quad & N_1 \times N_2 \to N_1 + N_2 \\ & (\alpha_1, \alpha_2) \mapsto \alpha_1 + \alpha_2. \end{aligned}$$

Theorem 13.12. *Let M and M' be R-modules, and consider the R-module of functions* $\mathrm{Map}(M, M')$ *(see Example 13.10). Then*

$$\mathrm{Hom}_R(M, M') := \{\sigma \in \mathrm{Map}(M, M') : \sigma \text{ is an } R\text{-linear map}\}$$

is a submodule of $\mathrm{Map}(M, M')$.

Example 13.26. Consider again the R-module $R[X]/(f)$ discussed in Example 13.4, where $f \in R[X]$ is of degree $\ell \geq 0$ and $\mathrm{lc}(f) \in R^*$. As an R-module, $R[X]/(f)$ is isomorphic to $R[X]_{<\ell}$ (see Example 13.11). Indeed, based on the observations in Example 7.39, the map $\rho : R[X]_{<\ell} \to R[X]/(f)$ that sends a polynomial $g \in R[X]$ of degree less than ℓ to $[g]_f \in R[X]/(f)$ is an isomorphism of $R[X]_{<\ell}$ with $R[X]/(f)$. Furthermore, $R[X]_{<\ell}$ is isomorphic as an R-module to $R^{\times \ell}$. Indeed, the map $\rho' : R[X]_{<\ell} \to R^{\times \ell}$ that sends $g = \sum_{i=0}^{\ell-1} a_i X^i \in R[X]_{<\ell}$ to $(a_0, \ldots, a_{\ell-1}) \in R^{\times \ell}$ is an isomorphism of $R[X]_{<\ell}$ with $R^{\times \ell}$. □

EXERCISE 13.4. Verify that the "is isomorphic to" relation on R-modules is an equivalence relation; that is, for all R-modules M_1, M_2, M_3, we have:

(a) $M_1 \cong M_1$;

(b) $M_1 \cong M_2$ implies $M_2 \cong M_1$;

(c) $M_1 \cong M_2$ and $M_2 \cong M_3$ implies $M_1 \cong M_3$.

EXERCISE 13.5. Let $\rho_i : M_i \to M_i'$, for $i = 1, \ldots, k$, be R-linear maps. Show that the map

$$\begin{aligned} \rho : \quad & M_1 \times \cdots \times M_k \to M_1' \times \cdots \times M_k' \\ & (\alpha_1, \ldots, \alpha_k) \mapsto (\rho_1(\alpha_1), \ldots, \rho_k(\alpha_k)) \end{aligned}$$

is an R-linear map.

EXERCISE 13.6. Let $\rho : M \to M'$ be an R-linear map, and let $c \in R$. Show that $\rho(cM) = c\rho(M)$.

EXERCISE 13.7. Let $\rho : M \to M'$ be an R-linear map. Let N be a submodule of

M, and let $\tau : N \to M'$ be the restriction of ρ to N. Show that τ is an R-linear map and that $\operatorname{Ker} \tau = \operatorname{Ker} \rho \cap N$.

EXERCISE 13.8. Suppose $M_1, \ldots, M_k$ are R-modules. Show that for each $i = 1, \ldots, k$, the projection map $\pi_i : M_1 \times \cdots \times M_k \to M_i$ that sends $(\alpha_1, \ldots, \alpha_k)$ to α_i is a surjective R-linear map.

EXERCISE 13.9. Show that if $M = M_1 \times M_2$ for R-modules M_1 and M_2, and N_1 is a subgroup of M_1 and N_2 is a subgroup of M_2, then we have an R-module isomorphism $M/(N_1 \times N_2) \cong M_1/N_1 \times M_2/N_2$.

EXERCISE 13.10. Let M be an R-module with submodules N_1 and N_2. Show that we have an R-module isomorphism $(N_1 + N_2)/N_2 \cong N_1/(N_1 \cap N_2)$.

EXERCISE 13.11. Let M be an R-module with submodules N_1, N_2, and A, where $N_2 \subseteq N_1$. Show that $(N_1 \cap A)/(N_2 \cap A)$ is isomorphic to a submodule of N_1/N_2.

EXERCISE 13.12. Let $\rho : M \to M'$ be an R-linear map with kernel K. Let N be a submodule of M. Show that we have an R-module isomorphism $M/(N + K) \cong \rho(M)/\rho(N)$.

EXERCISE 13.13. Let $\rho : M \to M'$ be a surjective R-linear map. Let S be the set of all submodules of M that contain $\operatorname{Ker} \rho$, and let S' be the set of all submodules of M'. Show that the sets S and S' are in one-to-one correspondence, via the map that sends $N \in S$ to $\rho(N) \in S'$.

13.4 Linear independence and bases

Throughout this section, R denotes a ring.

Definition 13.13. *Let M be an R-module, and let $\{\alpha_i\}_{i=1}^n$ be a family of elements of M. We say that $\{\alpha_i\}_{i=1}^n$*

*(i) is **linearly dependent (over R)** if there exist $c_1, \ldots, c_n \in R$, not all zero, such that $c_1\alpha_1 + \cdots + c_n\alpha_n = 0_M$;*

*(ii) is **linearly independent (over R)** if it is not linearly dependent;*

*(iii) **spans M (over R)** if for every $\alpha \in M$, there exist $c_1, \ldots, c_n \in R$ such that $c_1\alpha_1 + \cdots + c_n\alpha_n = \alpha$;*

*(iv) is a **basis for M (over R)** if it is linearly independent and spans M.*

The family $\{\alpha_i\}_{i=1}^n$ always spans some submodule of M, namely, the submodule N generated by $\alpha_1, \ldots, \alpha_n$. In this case, we may also call N the **submodule (over R) spanned by** $\{\alpha_i\}_{i=1}^n$.

The family $\{\alpha_i\}_{i=1}^n$ may contain duplicates, in which case it is linearly dependent

(unless R is trivial). Indeed, if, say, $\alpha_1 = \alpha_2$, then setting $c_1 := 1$, $c_2 := -1$, and $c_3 := \cdots := c_n := 0$, we have the linear relation $\sum_{i=1}^n c_i\alpha_i = 0_M$.

If the family $\{\alpha_i\}_{i=1}^n$ contains 0_M, then it is also linear dependent (unless R is trivial). Indeed, if, say, $\alpha_1 = 0_M$, then setting $c_1 := 1$ and $c_2 := \cdots := c_n := 0$, we have the linear relation $\sum_{i=1}^n c_i\alpha_i = 0_M$.

The family $\{\alpha_i\}_{i=1}^n$ may also be empty (i.e., $n = 0$), in which case it is linearly independent, and spans the submodule $\{0_M\}$.

In the above definition, the ordering of the elements $\alpha_1, \ldots, \alpha_n$ makes no difference. As such, when convenient, we may apply the terminology in the definition to any family $\{\alpha_i\}_{i \in I}$, where I is an arbitrary, finite index set.

Example 13.27. Consider the R-module $R^{\times n}$. Define $\alpha_1, \ldots, \alpha_n \in R^{\times n}$ as follows:

$$\alpha_1 := (1, 0, \ldots, 0),\ \alpha_2 := (0, 1, 0, \ldots, 0), \ldots,\ \alpha_n := (0, \ldots, 0, 1);$$

that is, α_i has a 1 in position i and is zero everywhere else. It is easy to see that $\{\alpha_i\}_{i=1}^n$ is a basis for $R^{\times n}$. Indeed, for all $c_1, \ldots, c_n \in R$, we have

$$c_1\alpha_1 + \cdots + c_n\alpha_n = (c_1, \ldots, c_n),$$

from which it is clear that $\{\alpha_i\}_{i=1}^n$ spans $R^{\times n}$ and is linearly independent. The family $\{\alpha_i\}_{i=1}^n$ is called the **standard basis** for $R^{\times n}$. □

Example 13.28. Consider the $\mathbb{Z}$-module $\mathbb{Z}^{\times 3}$. In addition to the standard basis, which consists of the tuples

$$(1, 0, 0), (0, 1, 0), (0, 0, 1),$$

the tuples

$$\alpha_1 := (1, 1, 1),\ \alpha_2 := (0, 1, 0),\ \alpha_3 := (2, 0, 1)$$

also form a basis. To see this, first observe that for all $c_1, c_2, c_3, d_1, d_2, d_3 \in \mathbb{Z}$, we have

$$(d_1, d_2, d_3) = c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3$$

if and only if

$$d_1 = c_1 + 2c_3,\ d_2 = c_1 + c_2,\ \text{and } d_3 = c_1 + c_3. \tag{13.1}$$

If (13.1) holds with $d_1 = d_2 = d_3 = 0$, then subtracting the equation $c_1 + c_3 = 0$ from $c_1 + 2c_3 = 0$, we see that $c_3 = 0$, from which it easily follows that $c_1 = c_2 = 0$. This shows that the family $\{\alpha_i\}_{i=1}^3$ is linearly independent. To show that it spans $\mathbb{Z}^{\times 3}$, the reader may verify that for any given $d_1, d_2, d_3 \in \mathbb{Z}$, the values

$$c_1 := -d_1 + 2d_3,\ c_2 := d_1 + d_2 - 2d_3,\ c_3 := d_1 - d_3$$

satisfy (13.1).

The family of tuples $(1,1,1),(0,1,0),(1,0,1)$ is not a basis, as it is linearly dependent: the third tuple is equal to the first minus the second.

The family of tuples $(1,0,12),(0,1,30),(0,0,18)$ is linearly independent, but does not span $\mathbb{Z}^{\times 3}$: the last component of any $\mathbb{Z}$-linear combination of these tuples must be divisible by $\gcd(12,30,18) = 6$. However, this family of tuples is a basis for the $\mathbb{Q}$-module $\mathbb{Q}^{\times 3}$. □

Example 13.29. Consider again the submodule $R[X]_{<\ell}$ of $R[X]$, where $\ell \geq 0$, consisting of all polynomials of degree less than ℓ (see Example 13.11). Then $\{X^{i-1}\}_{i=1}^{\ell}$ is a basis for $R[X]_{<\ell}$ over R. □

Example 13.30. Consider again the ring $E = R[X]/(f)$, where $f \in R[X]$ with $\deg(f) = \ell \geq 0$ and $\mathrm{lc}(f) \in R^*$. As in Example 13.4, we may naturally view E as a module over R. From the observations in Example 7.39, it is clear that $\{\xi^{i-1}\}_{i=1}^{\ell}$ is a basis for E over R, where $\xi := [X]_f \in E$. □

The next theorem highlights a critical property of bases:

Theorem 13.14. *If $\{\alpha_i\}_{i=1}^n$ is a basis for an R-module M, then the map*

$$\begin{aligned} \varepsilon : \quad & R^{\times n} \to M \\ & (c_1,\ldots,c_n) \mapsto c_1\alpha_1 + \cdots + c_n\alpha_n \end{aligned}$$

is an R-module isomorphism. In particular, every element of M can be expressed in a unique way as $c_1\alpha_1 + \cdots + c_n\alpha_n$, for $c_1,\ldots,c_n \in R$.

Proof. We already saw that ε is an R-linear map in Example 13.21. Since $\{\alpha_i\}_{i=1}^n$ is linearly independent, it follows that the kernel of ε is trivial, so that ε is injective. That ε is surjective follows immediately from the fact that $\{\alpha_i\}_{i=1}^n$ spans M. □

The following is an immediate corollary of this theorem:

Theorem 13.15. *Any two R-modules with bases of the same size are isomorphic.*

The following theorem develops an important connection between bases and linear maps.

Theorem 13.16. *Let $\{\alpha_i\}_{i=1}^n$ be a basis for an R-module M, and let $\rho : M \to M'$ be an R-linear map. Then:*

(i) ρ is surjective if and only if $\{\rho(\alpha_i)\}_{i=1}^n$ spans M';

(ii) ρ is injective if and only if $\{\rho(\alpha_i)\}_{i=1}^n$ is linearly independent;

(iii) ρ is an isomorphism if and only if $\{\rho(\alpha_i)\}_{i=1}^n$ is a basis for M'.

Proof. By the previous theorem, we know that every element of M can be written uniquely as $\sum_i c_i\alpha_i$, where the c_i's are in R. Therefore, every element in $\operatorname{Im}\rho$ can be expressed as $\rho(\sum_i c_i\alpha_i) = \sum_i c_i\rho(\alpha_i)$. It follows that $\operatorname{Im}\rho$ is equal to the subspace of M' spanned by $\{\rho(\alpha_i)\}_{i=1}^n$. From this, (i) is clear.

For (ii), consider a non-zero element $\sum_i c_i\alpha_i$ of M, so that not all c_i's are zero. Now, $\sum_i c_i\alpha_i \in \operatorname{Ker}\rho$ if and only if $\sum_i c_i\rho(\alpha_i) = 0_{M'}$, and thus, $\operatorname{Ker}\rho$ is non-trivial if and only if $\{\rho(\alpha_i)\}_{i=1}^n$ is linearly dependent. That proves (ii).

(iii) follows from (i) and (ii). □

EXERCISE 13.14. Let M be an R-module. Suppose $\{\alpha_i\}_{i=1}^n$ is a linearly independent family of elements of M. Show that for every $J \subseteq \{1,\ldots,n\}$, the subfamily $\{\alpha_j\}_{j\in J}$ is also linearly independent.

EXERCISE 13.15. Suppose $\rho : M \to M'$ is an R-linear map. Show that if $\{\alpha_i\}_{i=1}^n$ is a linearly dependent family of elements of M, then $\{\rho(\alpha_i)\}_{i=1}^n$ is also linearly dependent.

EXERCISE 13.16. Suppose $\rho : M \to M'$ is an injective R-linear map and that $\{\alpha_i\}_{i=1}^n$ is a linearly independent family of elements of M. Show that $\{\rho(\alpha_i)\}_{i=1}^n$ is linearly independent.

EXERCISE 13.17. Suppose that $\{\alpha_i\}_{i=1}^n$ spans an R-module M and that $\rho : M \to M'$ is an R-linear map. Show that:

(a) ρ is surjective if and only if $\{\rho(\alpha_i)\}_{i=1}^n$ spans M';

(b) if $\{\rho(\alpha_i)\}_{i=1}^n$ is linearly independent, then ρ is injective.

13.5 Vector spaces and dimension

Throughout this section, F denotes a field.

A module over a field is also called a **vector space**. In particular, an F-module is called an **F-vector space**, or a **vector space over F**.

For vector spaces over F, one typically uses the terms **subspace** and **quotient space**, instead of (respectively) submodule and quotient module; likewise, one usually uses the terms **F-vector space homomorphism**, **isomorphism** and **automorphism**, as appropriate.

We now develop the basic theory of dimension for *finitely generated* vector spaces. Recall that a vector space V over F is finitely generated if we have $V = \langle\alpha_1,\ldots,\alpha_n\rangle_F$ for some $\alpha_1,\ldots,\alpha_n$ of V. The main results here are that

- every finitely generated vector space has a basis, and
- all such bases have the same number of elements.

Throughout the rest of this section, V denotes a vector space over F. We begin with a technical fact that will be used several times throughout this section:

Theorem 13.17. *Suppose that $\{\alpha_i\}_{i=1}^n$ is a linearly independent family of elements that spans a subspace $W \subsetneq V$, and that $\alpha_{n+1} \in V \setminus W$. Then $\{\alpha_i\}_{i=1}^{n+1}$ is also linearly independent.*

Proof. Suppose we have a linear relation

$$0_V = c_1\alpha_1 + \cdots + c_n\alpha_n + c_{n+1}\alpha_{n+1},$$

where the c_i's are in F. We want to show that all the c_i's are zero. If $c_{n+1} \neq 0$, then we have

$$\alpha_{n+1} = -c_{n+1}^{-1}(c_1\alpha_1 + \cdots + c_n\alpha_n) \in W,$$

contradicting the assumption that $\alpha_{n+1} \notin W$. Therefore, we must have $c_{n+1} = 0$, and the linear independence of $\{\alpha_i\}_{i=1}^n$ implies that $c_1 = \cdots = c_n = 0$. □

The next theorem says that every finitely generated vector space has a basis, and in fact, any family that spans a vector space contains a subfamily that is a basis for the vector space.

Theorem 13.18. *Suppose $\{\alpha_i\}_{i=1}^n$ is a family of elements that spans V. Then for some subset $J \subseteq \{1, \ldots, n\}$, the subfamily $\{\alpha_j\}_{j\in J}$ is a basis for V.*

Proof. We prove this by induction on n. If $n = 0$, the theorem is clear, so assume $n > 0$. Consider the subspace W of V spanned by $\{\alpha_i\}_{i=1}^{n-1}$. By the induction hypothesis, for some $K \subseteq \{1, \ldots, n-1\}$, the subfamily $\{\alpha_k\}_{k\in K}$ is a basis for W. There are two cases to consider.

Case 1: $\alpha_n \in W$. In this case, $W = V$, and the theorem clearly holds with $J := K$.

Case 2: $\alpha_n \notin W$. We claim that setting $J := K \cup \{n\}$, the subfamily $\{\alpha_j\}_{j\in J}$ is a basis for V. Indeed, since $\{\alpha_k\}_{k\in K}$ is linearly independent, and $\alpha_n \notin W$, Theorem 13.17 immediately implies that $\{\alpha_j\}_{j\in J}$ is linearly independent. Also, since $\{\alpha_k\}_{k\in K}$ spans W, it is clear that $\{\alpha_j\}_{j\in J}$ spans $W + \langle\alpha_n\rangle_F = V$. □

Theorem 13.19. *If V is spanned by some family of n elements of V, then every family of $n+1$ elements of V is linearly dependent.*

Proof. We prove this by induction on n. If $n = 0$, the theorem is clear, so assume that $n > 0$. Let $\{\alpha_i\}_{i=1}^n$ be a family that spans V, and let $\{\beta_i\}_{i=1}^{n+1}$ be an arbitrary family of elements of V. We wish to show that $\{\beta_i\}_{i=1}^{n+1}$ is linearly dependent.

We know that β_{n+1} is a linear combination of the α_i's, say,

$$\beta_{n+1} = c_1\alpha_1 + \cdots + c_n\alpha_n. \tag{13.2}$$

If all the c_i's were zero, then we would have $\beta_{n+1} = 0_V$, and so trivially, $\{\beta_i\}_{i=1}^{n+1}$ is linearly dependent. So assume that some c_i is non-zero, and for concreteness, say $c_n \neq 0$. Dividing equation (13.2) through by c_n, it follows that α_n is an F-linear combination of $\alpha_1, \ldots, \alpha_{n-1}, \beta_{n+1}$. Therefore,

$$\langle \alpha_1, \ldots, \alpha_{n-1}, \beta_{n+1} \rangle_F \supseteq \langle \alpha_1, \ldots, \alpha_{n-1} \rangle_F + \langle \alpha_n \rangle_F = V.$$

Now consider the subspace $W := \langle \beta_{n+1} \rangle_F$ and the quotient space V/W. Since the family of elements $\alpha_1, \ldots, \alpha_{n-1}, \beta_{n+1}$ spans V, it is easy to see that $\{[\alpha_i]_W\}_{i=1}^{n-1}$ spans V/W; therefore, by induction, $\{[\beta_i]_W\}_{i=1}^{n}$ is linearly dependent. This means that there exist $d_1, \ldots, d_n \in F$, not all zero, such that $d_1\beta_1 + \cdots + d_n\beta_n \equiv 0 \pmod{W}$, which means that for some $d_{n+1} \in F$, we have $d_1\beta_1 + \cdots + d_n\beta_n = d_{n+1}\beta_{n+1}$. That proves that $\{\beta_i\}_{i=1}^{n+1}$ is linearly dependent. □

An important corollary of Theorem 13.19 is the following:

Theorem 13.20. *If V is finitely generated, then any two bases for V have the same size.*

Proof. If one basis had more elements than another, then Theorem 13.19 would imply that the first basis was linearly dependent, which contradicts the definition of a basis. □

Theorem 13.20 allows us to make the following definition:

Definition 13.21. *If V is finitely generated, the common size of any basis is called the **dimension** of V, and is denoted* $\dim_F(V)$.

Note that from the definitions, we have $\dim_F(V) = 0$ if and only if V is the trivial vector space (i.e., $V = \{0_V\}$). We also note that one often refers to a finitely generated vector space as a **finite dimensional** vector space. We shall give preference to this terminology from now on.

To summarize the main results in this section up to this point: if V is finite dimensional, it has a basis, and any two bases have the same size, which is called the dimension of V.

Theorem 13.22. *Suppose that* $\dim_F(V) = n$, *and that* $\{\alpha_i\}_{i=1}^{n}$ *is a family of n elements of V. The following are equivalent:*

(i) $\{\alpha_i\}_{i=1}^{n}$ *is linearly independent;*

(ii) $\{\alpha_i\}_{i=1}^{n}$ *spans V;*

(iii) $\{\alpha_i\}_{i=1}^{n}$ *is a basis for V.*

Proof. Let W be the subspace of V spanned by $\{\alpha_i\}_{i=1}^{n}$.

First, let us show that (i) implies (ii). Suppose $\{\alpha_i\}_{i=1}^{n}$ is linearly independent.

Also, by way of contradiction, suppose that $W \subsetneq V$, and choose $\alpha_{n+1} \in V \setminus W$. Then Theorem 13.17 implies that $\{\alpha_i\}_{i=1}^{n+1}$ is linearly independent. But then we have a linearly independent family of $n+1$ elements of V, which is impossible by Theorem 13.19.

Second, let us prove that (ii) implies (i). Let us assume that $\{\alpha_i\}_{i=1}^{n}$ is linearly dependent, and prove that $W \subsetneq V$. By Theorem 13.18, we can find a basis for W among the α_i's, and since $\{\alpha_i\}_{i=1}^{n}$ is linearly dependent, this basis must contain strictly fewer than n elements. Hence, $\dim_F(W) < \dim_F(V)$, and therefore, $W \subsetneq V$.

The theorem now follows from the above arguments, and the fact that, by definition, (iii) holds if and only if both (i) and (ii) hold. □

We next examine the dimension of subspaces of finite dimensional vector spaces.

Theorem 13.23. *Suppose that V is finite dimensional and W is a subspace of V. Then W is also finite dimensional, with $\dim_F(W) \leq \dim_F(V)$. Moreover, $\dim_F(W) = \dim_F(V)$ if and only if $W = V$.*

Proof. Suppose $\dim_F(V) = n$. Consider the set S of all linearly independent families of the form $\{\alpha_i\}_{i=1}^{m}$, where $m \geq 0$ and each α_i is in W. The set S is certainly non-empty, as it contains the empty family. Moreover, by Theorem 13.19, every member of S must have at most n elements. Therefore, we may choose some particular element $\{\alpha_i\}_{i=1}^{m}$ of S, where m is as large as possible. We claim that this family $\{\alpha_i\}_{i=1}^{m}$ is a basis for W. By definition, $\{\alpha_i\}_{i=1}^{m}$ is linearly independent and spans some subspace W' of W. If $W' \subsetneq W$, we can choose an element $\alpha_{m+1} \in W \setminus W'$, and by Theorem 13.17, the family $\{\alpha_i\}_{i=1}^{m+1}$ is linearly independent, and therefore, this family also belongs to S, contradicting the assumption that m is as large as possible.

That proves that W is finite dimensional with $\dim_F(W) \leq \dim_F(V)$. It remains to show that these dimensions are equal if and only if $W = V$. Now, if $W = V$, then clearly $\dim_F(W) = \dim_F(V)$. Conversely, if $\dim_F(W) = \dim_F(V)$, then by Theorem 13.22, any basis for W must already span V. □

Theorem 13.24. *If V is finite dimensional, and W is a subspace of V, then the quotient space V/W is also finite dimensional, and*

$$\dim_F(V/W) = \dim_F(V) - \dim_F(W).$$

Proof. Suppose that $\{\alpha_i\}_{i=1}^{n}$ spans V. Then it is clear that $\{[\alpha_i]_W\}_{i=1}^{n}$ spans V/W. By Theorem 13.18, we know that V/W has a basis of the form $\{[\alpha_i]_W\}_{i=1}^{\ell}$, where $\ell \leq n$ (renumbering the α_i's as necessary). By Theorem 13.23, we know that W has a basis, say $\{\beta_j\}_{j=1}^{m}$. The theorem will follow immediately from the following:

Claim. The elements

$$\alpha_1, \ldots, \alpha_\ell, \ \beta_1, \ldots, \beta_m \tag{13.3}$$

form a basis for V.

To see that this family spans V, consider any element γ of V. Then since $\{[\alpha_i]_W\}_{i=1}^{\ell}$ spans V/W, we have $\gamma \equiv \sum_i c_i\alpha_i \pmod{W}$ for some $c_1, \ldots, c_\ell \in F$. If we set $\beta := \gamma - \sum_i c_i\alpha_i \in W$, then since $\{\beta_j\}_{j=1}^{m}$ spans W, we have $\beta = \sum_j d_j\beta_j$ for some $d_1, \ldots, d_m \in F$, and hence $\gamma = \sum_i c_i\alpha_i + \sum_j d_j\beta_j$. That proves that the family of elements (13.3) spans V. To prove this family is linearly independent, suppose we have a relation of the form $\sum_i c_i\alpha_i + \sum_j d_j\beta_j = 0_V$, where $c_1, \ldots, c_\ell \in F$ and $d_1, \ldots, d_m \in F$. If any of the c_i's were non-zero, this would contradict the assumption that $\{[\alpha_i]_W\}_{i=1}^{\ell}$ is linearly independent. So assume that all the c_i's are zero. If any of the d_j's were non-zero, this would contradict the assumption that $\{\beta_j\}_{j=1}^{m}$ is linearly independent. Thus, all the c_i's and d_j's must be zero, which proves that the family of elements (13.3) is linearly independent. That proves the claim. □

Theorem 13.25. *If V is finite dimensional, then every linearly independent family of elements of V can be extended to form a basis for V.*

Proof. One can prove this by generalizing the proof of Theorem 13.18. Alternatively, we can adapt the proof of the previous theorem. Let $\{\beta_j\}_{j=1}^{m}$ be a linearly independent family of elements that spans a subspace W of V. As in the proof of the previous theorem, if $\{[\alpha_i]_W\}_{i=1}^{\ell}$ is a basis for the quotient space V/W, then the elements

$$\alpha_1, \ldots, \alpha_\ell, \ \beta_1, \ldots, \beta_m$$

form a basis for V. □

Example 13.31. Suppose that F is finite, say $|F| = q$, and that V is finite dimensional, say $\dim_F(V) = n$. Then clearly $|V| = q^n$. If W is a subspace with $\dim_F(W) = m$, then $|W| = q^m$, and by Theorem 13.24, $\dim_F(V/W) = n - m$, and hence $|V/W| = q^{n-m}$. Just viewing V and W as additive groups, we know that the index of W in V is $[V : W] = |V/W| = |V|/|W| = q^{n-m}$, which agrees with the above calculations. □

We next consider the relation between the notion of dimension and linear maps. First, observe that by Theorem 13.15, if two finite dimensional vector spaces have the same dimension, then they are isomorphic. The following theorem is the converse:

Theorem 13.26. *If V is of finite dimension n, and V is isomorphic to V', then V' is also of finite dimension n.*

Proof. If $\{\alpha_i\}_{i=1}^n$ is a basis for V, then by Theorem 13.16, $\{\rho(\alpha_i)\}_{i=1}^n$ is a basis for V'. □

Thus, two finite dimensional vector spaces are isomorphic if and only if they have the same dimension.

We next illustrate one way in which the notion of dimension is particularly useful. In general, if we have a function $f : A \to B$, injectivity does not imply surjectivity, nor does surjectivity imply injectivity. If A and B are finite sets of equal size, then these implications do indeed hold. The following theorem gives us another important setting where these implications hold, with finite dimensionality playing the role corresponding to finite cardinality:

Theorem 13.27. *If $\rho : V \to V'$ is an F-linear map, and if V and V' are finite dimensional with $\dim_F(V) = \dim_F(V')$, then we have:*

ρ is injective if and only if ρ is surjective.

Proof. Let $\{\alpha_i\}_{i=1}^n$ be a basis for V. Then

$$\begin{aligned}\rho \text{ is injective} &\iff \{\rho(\alpha_i)\}_{i=1}^n \text{ is linearly independent (by Theorem 13.16)}\\ &\iff \{\rho(\alpha_i)\}_{i=1}^n \text{ spans } V' \text{ (by Theorem 13.22)}\\ &\iff \rho \text{ is surjective (again by Theorem 13.16).}\ \square\end{aligned}$$

This theorem may be generalized as follows:

Theorem 13.28. *If V is finite dimensional, and $\rho : V \to V'$ is an F-linear map, then $\operatorname{Im}\rho$ is a finite dimensional vector space, and*

$$\dim_F(V) = \dim_F(\operatorname{Im}\rho) + \dim_F(\operatorname{Ker}\rho).$$

Proof. As the reader may verify, this follows immediately from Theorem 13.24, together with Theorems 13.26 and 13.9. □

Intuitively, one way to think of Theorem 13.28 is as a "law of conservation" for dimension: any "dimensionality" going into ρ that is not "lost" to the kernel of ρ must show up in the image of ρ.

EXERCISE 13.18. Show that if $V_1, \ldots, V_n$ are finite dimensional vector spaces over F, then $V_1 \times \cdots \times V_n$ has dimension $\sum_{i=1}^n \dim_F(V_i)$.

EXERCISE 13.19. Show that if V is a finite dimensional vector space over F with subspaces W_1 and W_2, then

$$\dim_F(W_1 + W_2) = \dim_F(W_1) + \dim_F(W_2) - \dim_F(W_1 \cap W_2).$$

EXERCISE 13.20. From the previous exercise, one might be tempted to think that a more general "inclusion/exclusion principle" for dimension holds. Determine if the following statement is true or false: if V is a finite dimensional vector space over F with subspaces W_1, W_2, and W_3, then

$$\begin{aligned}\dim_F(W_1 + W_2 + W_3) &= \dim_F(W_1) + \dim_F(W_2) + \dim_F(W_3) \\ &\quad - \dim_F(W_1 \cap W_2) - \dim_F(W_1 \cap W_3) - \dim_F(W_2 \cap W_3) \\ &\quad + \dim_F(W_1 \cap W_2 \cap W_3).\end{aligned}$$

EXERCISE 13.21. Suppose that V and W are vector spaces over F, V is finite dimensional, and $\{\alpha_i\}_{i=1}^k$ is a linearly independent family of elements of V. In addition, let $\beta_1, \ldots, \beta_k$ be arbitrary elements of W. Show that there exists an F-linear map $\rho : V \to W$ such that $\rho(\alpha_i) = \beta_i$ for $i = 1, \ldots, k$.

EXERCISE 13.22. Let V be a vector space over F with basis $\{\alpha_i\}_{i=1}^n$. Let S be a finite, non-empty subset of F, and define

$$B := \left\{ \sum_{i=1}^n c_i \alpha_i : c_1, \ldots, c_n \in S \right\}.$$

Show that if W is a subspace of V, with $W \subsetneq V$, then $|B \cap W| \leq |S|^{n-1}$.

EXERCISE 13.23. The theory of dimension for finitely generated vector spaces is quite elegant and powerful. There is a theory of dimension (of sorts) for modules over an arbitrary, non-trivial ring R, but it is much more awkward and limited. This exercise develops a proof of one aspect of this theory: if an R-module M has a basis at all, then any two bases have the same size. To prove this, we need the fact that any non-trivial ring has a maximal ideal (this was proved in Exercise 7.40 for countable rings). Let n, m be positive integers, let $\alpha_1, \ldots, \alpha_m$ be elements of $R^{\times n}$, and let I be an ideal of R.

(a) Show that if $\{\alpha_i\}_{i=1}^m$ spans $R^{\times n}$, then every element of $I^{\times n}$ can be expressed as $c_1\alpha_1 + \cdots + c_m\alpha_m$, where $c_1, \ldots, c_m$ belong to I.

(b) Show that if $m > n$ and I is a maximal ideal, then there exist $c_1, \ldots, c_m \in R$, not all in I, such that $c_1\alpha_1 + \cdots + c_m\alpha_m \in I^{\times n}$.

(c) From (a) and (b), deduce that if $m > n$, then $\{\alpha_i\}_{i=1}^m$ cannot be a basis for $R^{\times n}$.

(d) From (c), conclude that any two bases for a given R-module M must have the same size.