3.4 Free Modules

In analogy with free groups, we identify those modules having only the relations required by the module axioms.

3.4.1 Definition. Let R be a commutative ring. For any index set J, consider the R-module $R^{(J)} := \bigoplus_{j \in J} R^1$. For each $j \in J$ and each canonical map $\gamma_j : R^1 \to R^{(J)}$, set $e_j := \gamma_j(1_R)$. With this notation, every $r := (r_j) \in R^{(J)}$ may be written uniquely as $r = \sum_{j \in J} r_j \, e_j$. Let $\varepsilon : J \to R^{(J)}$ be set map defined by $j \mapsto e_j$.

3.4.2 Lemma. *For any R-module V and any map $\xi : J \to V$, there is a unique R-module homomorphism $\varphi : R^{(J)} \to V$ such that $\xi = \varphi \circ \varepsilon$.*

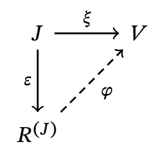

Figure 3.4: Commutative diagrams arising from Lemma 3.4.2

Proof. The condition $\xi = \varphi \circ \varepsilon$ means that $\varphi(e_j) = \xi(j)$ for all $j \in J$ which is equivalent to $\varphi(r \, e_j) = r \, \xi(j)$ for all $r \in R$ and $j \in J$. It also means that the composition $\varphi \circ \gamma_j : R \to V$ is the R-module homomorphism given by $r \mapsto r \, \xi(\alpha)$. The proposition is therefore a special case of the mapping property for direct sums. □

3.4.3 Remark. The linear map $\varphi : R^{(J)} \to V$ is said to be ***determined*** by the family $\{\xi(j)\}_{j \in J}$ of elements in V. By definition, we have

$$\varphi\Big(\sum_{j \in J} r_j \, e_j\Big) = \sum_{j \in J} r_j \, \xi(j) \, .$$

3.4.4 Definition. A family $\{v_j\}_{j \in J}$ of elements in an R-module V is ***linearly independent*** (resp. a ***basis***) if the R-module homomorphism $R^{(J)} \to V$ determined by this family is injective (resp. bijective). A module is ***free*** if it has a basis.

If R is a domain and $f, g \in R$ are distinct nonzero elements, then set $\{f, g\}$ is linearly dependent because $(-g)f + f(g) = 0$.

3.4.5 Example. Let m be an integer greater than 1. In the $\mathbb{Z}$-module $\mathbb{Z}/\langle m \rangle$ no element is linearly independent, so the quotient $\mathbb{Z}/\langle m \rangle$ is not a free module. ◇

3.4.6 Example. A free module can have nonzero elements which are not part of a basis. The R-module R^1 is free, but zerodivisors in R are not part of a basis (they are not linearly independent). ◇

3.4.7 Example. Every nonzero element of an R-module can from a linearly independent set without the module being free. The field $\mathbb{Q}$ is a $\mathbb{Z}$-module with this property: two nonzero rational numbers are always linearly dependent; for all $a, b, c, d \in \mathbb{Z}$ with $b \neq 0$ and $d \neq 0$, we have

$$(b \, c)\frac{a}{b} - (a \, d)\frac{c}{d} = 0 \, .$$

Hence, a basis could only have at most one element. However, for any $q \in \mathbb{Q}$, the set $\{n \, q \mid n \in \mathbb{Z}\}$ is a proper subset of $\mathbb{Q}$. ◇

3.4.8 Proposition. *Let V be a free R-module with basis $\{v_j\}_{j \in J}$. For any family $\{w_j\}_{j \in J}$ of elements in an R-module W, there is a unique R-module homomorphism $\psi \colon V \to W$ such that $\psi(v_j) = w_j$ for all $j \in J$. The map ψ is injective (resp. surjective) if and only if the family $\{w_j\}_{j \in J}$ of elements in W be a linearly independent (resp. generating set of W).*

Proof. This following from the definitions and Lemma 3.4.2. □

3.4.9 Corollary. *Every R-module V is the quotient of a free R-module.*

Proof. When J indexes a generating set of V, there is a surjective R-module homomorphism $R^{(J)} \to V$. In particular, one may take $J = V$. If submodule U is the kernel of this map, then Theorem 3.1.10 establishes that the R-module V is isomorphic to $R^{(J)}/U$. □

3.4.10 Corollary. *Every exact sequence of R-modules*

$$0 \longrightarrow U \xrightarrow{\varphi} V \xrightarrow{\psi} W \longrightarrow 0\,,$$

in which W is a free R-module, splits. To be precise, if $\{w_j\}_{j \in J}$ is a basis for W, and v_j is an element of V such that $\psi(v_j) = w_j$ for all $j \in J$, then the family $\{v_j\}_{j \in j}$ is linearly independent and generates a complementary submodule of $\varphi(U)$.

Proof. Since W is a free R-module, Proposition 3.4.8 demonstrates that there exists a unique R-module homomorphism $\sigma : W \to V$ such that $\sigma(w_j) = v_j$ for all $j \in J$ and Proposition 3.3.7 shows that the exact sequence splits. □

With the aim of understanding all free modules, we record the following minor observation.

3.4.11 Lemma. *Let K be a field and let $\{u_j\}_{j \in J}$ be linearly independent elements in K-vector space V. Given an element $w \in V$ that does not belong to the submodule U generated by $\{u_j\}_{j \in J}$, the family $\{w\} \cup \{u_j\}_{j \in J}$ is linearly independent.*

Proof. Suppose that we have a relation $s\,w + \sum_{j \in J} r_j\,u_j = 0$ where $s \in K$, $r_j \in K$ for all $j \in J$, and only finitely many of the r_j are nonzero. If $s \neq 0$, then it would follow that $w = -\sum_{j \in J}(s^{-1}\,r_j)\,u_j$ and hence $w \in U$ contrary to hypothesis. Thus, we must have $s = 0$ and the relation becomes $\sum_{j \in J} r_j\,u_j = 0$ which implies that $r_j = 0$ for all $j \in J$. Since the only relation among the elements is trivial, the family $\{w\} \cup \{u_j\}_{j \in J}$ is linearly independent. □

3.5 Vector Spaces

Characterizing modules over a field, also known as vector spaces, leads to deeper insights into all free modules.

3.5.1 Theorem. *Every module over a field K is a free.*

We must show that every vector space admits a basis. The subsequent more precise theorem accomplishes this task.

3.5.2 Theorem. *For any generating set $\mathcal{S}$ of a K-vector space V and any linearly independent set $\mathcal{L}$ of V contained in $\mathcal{S}$, there exists a basis $\mathcal{B}$ of V such that $\mathcal{L} \subseteq \mathcal{B} \subseteq \mathcal{S}$.*

Proof of Theorem 3.5.1. The existence of a basis for any vector space V follows from Theorem 3.5.2 by taking $\mathcal{L} = \varnothing$ and $\mathcal{S} = V$. □

Proof of Theorem 3.5.2. Let $\mathcal{E}$ be the set of all linearly independent subsets of V that contain $\mathcal{L}$ and are contained in $\mathcal{S}$. This family is nonempty, because $\mathcal{L} \in \mathcal{E}$. Partially order $\mathcal{E}$ by inclusion. Given a chain $\mathcal{C}$ in $\mathcal{E}$, we claim that $\mathcal{C}^* := \bigcup_{L \in \mathcal{C}} L$ is an upper bound for $\mathcal{C}$. Consider a finite subset $\{u_1, u_2, \dots, u_m\} \subseteq \mathcal{C}^*$. Since $\mathcal{C}$ is a chain, there exists $L \in \mathcal{C}$ such that $\{u_1, u_2, \dots, u_m\} \subseteq L$. Hence, the set $\{u_1, u_2, \dots, u_m\}$ is linearly independent. It follows that every chain in $\mathcal{E}$ has an upper bound. Hence, Zorn's Lemma implies that there exists a maximal element $\mathcal{B}$ and Lemma 3.4.11 implies that the submodule $\langle \mathcal{B} \rangle$ is equal to V. □

3.5.3 Corollary. *For any subset $\mathcal{B}$ of a K-vector space V, the following properties are equivalent:*
(a) *$\mathcal{B}$ is a basis of V.*
(b) *$\mathcal{B}$ is a maximal linearly independent subset of V.*
(c) *$\mathcal{B}$ is a minimal generating set of V.* □

3.5.4 Example. Any ring R containing a field K may be regarded as a K-vector space, so it admits a basis. In particular, every extension field of K has a basis. ◇

The field $\mathbb{R}$ admits an infinite basis as a $\mathbb{Q}$-vector space.

3.5.5 Theorem. *Two bases of a vector space have the same cardinality.*

Proof. Suppose that V is a vector space with a basis $\mathcal{B}$ of cardinality n. We show, by induction on n, that every other basis $\mathcal{B}'$ has at most n elements. The claim is trivial for $n = 0$. When $n \geqslant 1$, the set $\mathcal{B}'$ is nonempty so choose $w \in \mathcal{B}'$. By Theorem 3.5.2, there exists a subset $\mathcal{C} \subseteq \mathcal{B}$ such that $\{w\} \cup \mathcal{C}$ is a basis of V and $w \notin \mathcal{C}$ because $\{w\} \cup \mathcal{B}$ is obviously a generating set for V. As $\mathcal{B}$ is a basis for V, $\mathcal{C} = \mathcal{B}$ is impossible and hence $\mathcal{C}$ has at most $n - 1$ elements. Let U be the subspaced generated by $\mathcal{C}$ and W be the subspace generated by $\mathcal{B}' \setminus \{w\}$. Both U and W are complementary to $\langle w \rangle$ and hence isomorphic. As U admits a basis with at most $n-1$ elements, $\mathcal{B}' \setminus \{w\}$ has at most $n-1$ elements by the induction hypothesis. Therefore, $\mathcal{B}'$ has at most n elements.

Next suppose that V has an infinite basis so $V = \prod_{j \in J} V_j$ where J has infinite cardinality. We claim that every generating set has cardinality at least that of J. Let $\mathcal{S}$ be a generating set for V. For each $s \in \mathcal{S}$, let C_s be the finite set of indices $j \in J$ such that the component of s in V_j is nonzero and let $C := \bigcup_{s \in \mathcal{S}} C_s$. Every $s \in \mathcal{S}$ belongs to the submodule $\bigoplus_{j \in C} V_j$; since $\mathcal{S}$ generates V it follows that $C = J$. Since $|J| = |C| \leqslant |\mathcal{S}|$, the claim follows. □

When $\dim_K V < \infty$, the K-vector space V is finite-dimensional and otherwise it infinite-dimensional.

3.5.6 Definition. The ***dimension*** of a K-vector space V is the cardinality of any of the bases of V and denoted by $\dim_K V$.

3.5.7 Lemma. *For any family $\{V_j\}_{j \in J}$ of K-vector spaces, we have*

$$\dim_K\Big(\bigoplus_{j \in J} V_j\Big) = \sum_{j \in J} \dim_K V_j \,.$$

Sketch of Proof. If $\mathcal{B}_j$ denotes a basis for the K-vector space V_j for all $j \in J$, then the union $\mathcal{B} := \bigcup_{j \in J} \mathcal{B}_j$ is a basis for $\bigoplus_{j \in J} V_j$. The formula follows because the $\mathcal{B}_j$ are pairwise disjoint. □

3.5.8 Proposition. *For any exact sequence of K-vector spaces*

$$0 \longrightarrow V_\ell \xrightarrow{\varphi_\ell} V_{\ell-1} \xrightarrow{\varphi_{\ell-1}} \cdots \longrightarrow V_1 \xrightarrow{\varphi_1} V_0 \longrightarrow 0\,,$$

we have $\sum_{j=0}^{\ell} (-1)^j \dim_R V_j = 0$.

Proof. Setting $U_{-1} := 0$, $U_\ell := 0$, and $U_{j-1} := \operatorname{Im}(\varphi_j) = \operatorname{Ker}(\varphi_{j-1})$ for all $1 \leqslant j \leqslant \ell$, we obtain the short exact sequences

$$0 \longrightarrow U_j \longrightarrow V_j \longrightarrow U_{j-1} \longrightarrow 0\,,$$

Corollary 3.4.10 demonstrates that $V_j = U_j \oplus U_{j-1}$ and Lemma 3.5.6 establishes that $\dim_K V_j = \dim_K U_j + \dim U_{j-1}$. The alternating sum telescopes, so we have

$$0 = \sum_{j=0}^{\ell} (-1)^j \big(\dim_K U_j + \dim_K U_{j-1}\big) = \sum_{j=0}^{\ell} (-1)^j \dim_K V_j \,. \qquad \square$$

3.5.9 Corollary. *For any nonzero ring R and any free R-module V, any two basis of V have the same cardinality.*

Idea of Proof. Let I be a maximal ideal in R, let $K := R/I$ be the associated field, and let $\pi : R \to K$ be the canonical map. Consider the K-vector space $\pi^*(V) = K \otimes_R V$ obtained by extending scalars to K and let $\phi : V \to \pi^*(V)$ be the map defined by $v \mapsto 1 \otimes v$. Given $\{v_j\}_{j \in J}$ a basis of V, the family $\{\phi(v_j)\}_{j \in J}$ is a basis of $\pi^*(V)$. □

3.5.10 Definition. The cardinality of any basis for a free R-module V is called the ***rank*** of V and denoted by $\operatorname{rank}_R V$.