3
Module Theory

A module is an algebraic structure on a pair of underlying sets with four binary operations. Although modules can be defined over an arbitrary ring, we will focus on modules over a commutative ring.

3.0 Modules

3.0.1 Definition. Let R be a commutative ring. An ***R-module*** is an additive abelian group V with a ***scalar multiplication*** $R \times V \to V$ such that, for all $r, s \in R$ and all $u, v \in V$, we have

$$r\,(u+v) = r\,u + r\,v \qquad (r\,s)\,v = r\,(s\,v)$$
$$(r+s)\,v = r\,v + s\,v \qquad 1_R\,v = v\,.$$

3.0.2 Example. For any field K, K-vector spaces and K-modules are equivalent notions. ◇

3.0.3 Example. Every abelian group is a $\mathbb{Z}$-module in a unique way. For any positive integer n and any element g in an abelian group G, we have $0_{\mathbb{Z}}\,g = 0_G$, $(-n)\,g = -(n\,g)$, and

$$n\,g = \underbrace{g + g + \cdots + g}_{n \text{ summands}}\,. \qquad ◇$$

3.0.4 Example. Every ring R is a module over itself. ◇

3.0.5 Example. The set R^n of n-tuples of elements from R form an R-module under componentwise operations. ◇

3.0.6 Example. Every ideal in R is an R-module. ◇

3.0.7 Example. A ring homomorphism $\varphi : R \to R'$ makes R' into an R-module. For any $r \in R$ and any $v \in R'$, we have $r\,v := \varphi(r)\,v$. ◇

3.0.8 Definition. Let V and W be R-modules. A map $\varphi : V \to W$ is an ***R-module homomorphism*** or ***R-linear*** such that, for all $r \in R$ and all $u, v \in V$, we have $\varphi(r\,u + v) = r\,\varphi(u) + \varphi(v)$.

The composition of two R-module homomorphisms is an R-module homomorphism. The identity map on any R-module is an R-module homomorphism.

3.0.9 Example. For any field K, a K-module homomorphism is a linear transformation of vector spaces. ◇

3.0.10 Example. Every group homomorphism of abelian groups is a $\mathbb{Z}$-module homomorphism. ◇

3.0.11 Example. Let V and W be R-modules. The set of R-module homomorphisms from V to W forms an R-module $\mathrm{Hom}_R(V, W)$. For all $\varphi, \psi \in \mathrm{Hom}_R(V, W)$, all $r \in R$, and all $v \in V$, we have

$$(\varphi + \psi)(v) = \varphi(v) + \psi(v)\,, \qquad (r\,\varphi)(v) = r\,\varphi(v)\,.$$

An R-module homomorphism $\varphi : R \to V$ is uniquely determined by the image $\varphi(1_R)$ which can be any element of V. Hence, for any R-module V, there is a canonical isomorphism $\mathrm{Hom}_R(R, V) \cong V$ defined by $\varphi \mapsto \varphi(1_R)$. ◇

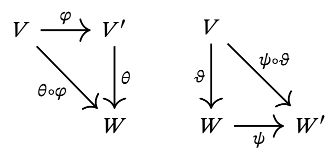

Figure 3.1: Commutative diagrams arising from Example 3.0.12

3.0.12 Example. Given R-module homomorphisms $\varphi : V \to V'$ and $\psi : W \to W'$, there are two induced R-module homomorphisms

$$\mathrm{Hom}(\varphi, W) :\ \mathrm{Hom}_R(V', W) \to \mathrm{Hom}_R(V, W)$$
$$\mathrm{Hom}(V, \psi) :\ \mathrm{Hom}_R(V, W) \to \mathrm{Hom}_R(V, W')\,,$$

defined, for all $\theta \in \mathrm{Hom}_R(V', W)$ and all $\vartheta \in \mathrm{Hom}_R(V, W)$, by $\big(\mathrm{Hom}(\varphi, W)\big)(\theta) := \theta \circ \varphi$ and $\big(\mathrm{Hom}(V, \psi)\big)(\vartheta) := \psi \circ \theta$. ◇

Multiplication by a fixed ring element $f \in R$, also called ***homothety by*** f, gives an R-module endomorphism defined, for all $v \in V$, by $v \mapsto f\,v$.

3.0.13 Example. For any R-module V, the composition of R-module homomorphisms defines a noncommutative ring structure on the R-module $\mathrm{Hom}_R(V, V)$. The multiplicative unit is the identity map $\mathrm{id}_V : V \to V$. An R-module homomorphism from V to itself is also called an ***endomorphism*** of V and $\mathrm{End}_R(V) := \mathrm{Hom}_R(V, V)$. ◇

3.0.14 Proposition. *An R-module homomorphism is an isomorphism if and only if the underlying map of sets is bijective.*

Proof.

(⇒) Suppose that the R-module homomorphism $\varphi : V \to W$ is an isomorphism. Since the underlying map of sets has an inverse, it is a bijection.

(⇐) Suppose that underlying map φ is bijective. There exists a map $\psi : W \to V$ such that $\varphi \circ \psi = \mathrm{id}_W$ and $\psi \circ \varphi = \mathrm{id}_V$. It remains to show that this set map is an R-module homomorphism. Since φ is an R-module homomorphism, it follows that, for all $r \in R$ and all $v, w \in W$, we have

$$\varphi\big(r\,\psi(v) + \psi(w)\big) = r\,\varphi\big(\psi(v)\big) + \varphi\big(\psi(w)\big) = r\,v + w$$

so $r\,\psi(v) + \psi(w) \in V$ is the unique element that φ sends to $r\,v + w$. By definition, this implies $\psi(r\,v + w) = r\,\psi(v) + \psi(w)$. □

3.1 Isomorphism Theorems

For a third time, we have theorems describing the relations between quotients, homomorphisms, and subobjects.

3.1.1 Definition. A ***submodule*** of an R-module V is a nonempty subset U that is closed under addition and scalar multiplication. In other words, a nonempty set U is a submodule of V if and only if, for all $r \in R$ and all $u, v \in U$, we have $r\,u + v \in U$.

3.1.2 Example. In any R-module V, the set $\{0\}$ is a submodule. By an abuse of notation, the zero submodule is denoted 0. ◇

3.1.3 Example. Submodules of the R-module R^1 are ideals. ◇

3.1.4 Example. For any R-module homomorphism $\varphi : V \to W$, the ***kernel*** is defined to be $\operatorname{Ker}(\varphi) := \{v \in V \mid \varphi(v) = 0\}$. For all $r \in R$ and all $u, v \in \operatorname{Ker}(\varphi)$, we have $\varphi(r\,u + v) = r\,\varphi(u) + \varphi(v) = r\,0 + 0 = 0$, so the ***kernel*** of φ is a submodule. ◇

3.1.5 Example. For any R-module homomorphism $\varphi : V \to W$, the ***image*** is defined to be

$$\operatorname{Im}(\varphi) := \{w \in W \mid \text{there exists } v \in V \text{ such that } \varphi(v) = w\}\,.$$

For all $v, w \in \operatorname{Im}(\varphi)$, there exists $v', w' \in V$ such that $\varphi(v') = v$ and $\varphi(w') = w$. Since $\varphi(r\,v' + w') = r\,\varphi(v') + \varphi(w') = r\,v + w$ for all $r \in R$, the image of φ is a submodule. ◇

3.1.6 Definition. Let V be an R-module and let U be a submodule of V. The quotient group V/U inherits an R-module structure from V defined, for all $r \in R$ and all $v \in V$, by $r(v + U) := r\,v + U$. This operation is well-defined because $v + U = u + U$ implies that $v - u \in U$ and $r\,v - r\,u = r(v-u) \in U$ establishing $r\,v + U = r\,u + U$. The module V/U is the ***quotient module***. This operation also makes the canonical map $\pi : V \to V/U$ into an R-module homomorphism.

3.1.7 Example. For any ideal I, the quotient R/I is an R-module. ◇

3.1.8 Example. For any R-module homomorphism, the ***cokernel*** is defined to be $\operatorname{Coker}(\varphi) := W / \operatorname{Im}(\varphi)$. ◇

3.1.9 Proposition. *Let $\varphi : V \to W$ be an R-module homomorphism. For any submodules $V' \subseteq V$ and $W' \subseteq W$ satisfying $\varphi(V') \subseteq W'$, the induced map $\overline{\varphi} : V/V' \to W/W'$ defined by $\overline{\varphi}(v + V') := \varphi(v) + W'$ is an R-module homomorphism.*

Proof. By Corollary 1.7.14, it suffices to verify that $\overline{\varphi}$ is compatible with scalar multiplication. For all $r \in R$ and all $v \in V$, we have

$$\begin{aligned}\overline{\varphi}\big(r(v + V')\big) &= \overline{\varphi}(r\,v + V') = \varphi(r\,v) + W' \\ &= r\,\varphi(v) + W' = r\big(\varphi(v) + W'\big) = r\,\overline{\varphi}(v + W')\,. \quad \square\end{aligned}$$

3.1.10 Theorem (First Isomorphism). *Let $\varphi : V \to W$ be an R-module homomorphism with $K := \mathrm{Ker}(\varphi)$. The induced map $\widetilde{\varphi} : V/K \to \mathrm{Im}(\varphi)$ defined, for all $v \in V$, by $\widetilde{\varphi}(v + K) = \varphi(v)$ is an isomorphism.*

Proof. By Theorem 1.8.1, it suffices to verify that $\widetilde{\varphi}$ is compatible with scalar multiplication. For all $r \in R$ and all $v \in V$, we have

$$\begin{aligned}\widetilde{\varphi}\big(r\,(v + K)\big) &= \varphi(r\,v) + K = r\,\varphi(v) + K \\ &= r\big(\varphi(v) + K\big) = r\,\widetilde{\varphi}(v + K)\,. \end{aligned}$$ □

3.1.11 Theorem (Second Isomorphism). *For two submodules U and W, there exists an R-module isomorphism $(U + W)/W \cong U/(U \cap W)$.*

Sketch of Proof. It suffices to verify that the group isomorphism in Theorem 1.8.5 is compatible with scalar multiplication. □

3.1.12 Theorem (Third Isomorphism). *Let V be an R-module. For any two submodules U and W of V satisfying $U \subseteq W$, there is an R-module isomorphism $V/W \cong (V/U)/(W/U)$.*

Sketch of Proof. It suffices to verify that the group isomorphism in Theorem 1.8.6 is compatible with scalar multiplication. □

Compare with Theorem 1.8.7 and Theorem 3.1.13.

3.1.13 Theorem (Correspondence). *Let U be a submodule of the an R-module V. The canonical R-module homomorphism $\pi : V \to V/U$ induces a bijection between the set of all submodules of V containing U and the set of all submodules of V/U.* □

Compare with Lemma 1.2.7 and Lemma 3.1.14.

3.1.14 Lemma. *For any family $\{U_j \mid j \in J\}$ of submodules in an R-module V, the intersection $U := \bigcap_{j \in J} U_j$ is also a submodule of V.* □

3.1.15 Definition. For any subset U of an R-module V, the ***submodule of V generated by U***, denoted by $\langle U \rangle$, is the intersection of all submodules of V that contain U. A module V is ***finitely generated*** if $V = \langle U \rangle$ for some finite subset $U \subseteq V$. Moreover, the module V is ***cyclic*** if $V = \langle U \rangle$ for some subset U having cardinality 1.

3.1.16 Example. For any ring R and any ideal I in R, the R-modules R^1 and R/I are cyclic, generated by their respective multiplicative identity elements. ◇

3.1.17 Definition. The ***annihilator*** of an R-module V is

$$\mathrm{Ann}(V) := \{f \in R \mid f\,v = 0 \text{ for all } v \in V\}.$$

Since $(r\,f + g)\,v = r\,(f\,v) + (g\,v) = r\,0 + 0 = 0$ for all $r \in R$ and all $f, g \in \mathrm{Ann}(V)$, the annihilator of V is an ideal in R.

3.1.18 Proposition. *For any cyclic R-module V, we have $V \cong R/\mathrm{Ann}(V)$.*

Sketch of Proof. There exists $v \in V$ such that $V = \langle v \rangle$. The map $\varphi : R \to V$, defined by $\varphi(r) := r\,v$, is a surjective R-module homomorphism with $\mathrm{Ker}(\varphi) = \mathrm{Ann}(V)$. □