3.6 Submodules of Free Modules

Copyright © 2020, Gregory G. Smith
Last updated: 2020–11–17

Over a field, submodules of a free module are automatically free because every module over a field is free. What condition on the ring guarantee that a submodule of a free module is free?

3.6.1 Theorem. *Let R be a principal ideal domain. Every submodule of a finitely generated free R-module of rank n is free of rank at most n.*

We actually prove a more precise result.

3.6.2 Lemma. *Let R be a principal ideal domain and let V be a finitely generated free R-module. For any nonzero submodule $U \subseteq V$, there exists elements $r \in R$, $v \in V$, $u \in U$ and submodules $V' \subseteq V$, $U' \subseteq U$ such that $u = r\,v$, $U' = V' \cap U$, $V = \langle v \rangle \oplus V'$, and $U = \langle u \rangle \oplus U'$.*

Proof. For any R-module homomorphism $\varphi : V \to R$, the image $\varphi(U)$ is an ideal in R. The family of these ideals in nonempty. Since principal ideal domains are noetherian, this family has a maximal element $\psi(U)$ for some R-module homomorphism $\psi : U \to R$. By hypothesis, we have $U \neq 0$, so $\psi(U) \neq 0$. Since R is a principal ideal, there exists a nonzero element $r \in R$ such that $\psi(U) = \langle r \rangle$. As $r \in \psi(U)$, there also exists an element $u \in U$ such that $\psi(u) = r$.

We claim that, for all R-module homomorphisms $\varphi : V \to R$, the element r divides $\varphi(u)$. Suppose that d generates the ideal $\langle r, \varphi(u) \rangle$ and let $a, b \in R$ satisfy $d = a\,r + b\,\varphi(u)$. Consider the R-module homomorphism $\theta := a\,\psi + b\,\varphi$. Since $r \in \langle d \rangle$, we have $\psi(U) \subseteq \langle d \rangle$. We also have $d = a\,r + b\,\varphi(u) = (a\,\psi + b\,\varphi)(u) = \theta(u) \in \theta(U)$, whence $\langle d \rangle \subseteq \theta(U)$. It follows that $\psi(U) \subseteq \theta(U)$. The maximality of $\psi(U)$ implies that $\psi(U) = \theta(U)$ and $\langle r \rangle = \langle d \rangle$, so the element r divides $\varphi(u)$.

By hypothesis, there is a positive integer n such that $V \cong \bigoplus_{i=1}^{n} R$. Identify the element $u \in U \subseteq V$ with $(s_1, s_2, \dots, s_n) \in \bigoplus_{i=1}^{n} R$. Each component $s_j := \varpi_j(u)$ is the image of u under the canonical map $\varpi_j : V \to R$, so the previous paragraph establishes that r divides all of them. Hence, there exists elements $c_1, c_2, \dots, c_n \in R$ such that $s_i = r\,c_i$ for all $1 \leqslant i \leqslant n$. Let $v \in V$ be the element identified with $(c_1, c_2, \dots, c_n) \in \bigoplus_{i=1}^{n} R$. By construction, we have $u = r\,v$ and we see that $r = \psi(u) = \psi(r\,v) = r\,\psi(v)$. Since $r \neq 0$ and R is a domain, we deduce that $\psi(v) = 1_R$.

Let $V' := \operatorname{Ker}(\psi)$ and set $U' := V' \cap U$. Every element $w \in V$ may be written as $w = \psi(w)\,v + \big(w - \psi(w)\,v\big)$. By linearity, we obtain $\psi\big(w - \psi(w)\,v\big) = \psi(w) - \psi(w)\,\psi(v) = 0$, so $w - \psi(w)\,v \in \operatorname{Ker}(\psi)$ and $V = \langle v \rangle + V'$. On the other hand, the relation $r\,v \in F'$ implies that $0 = \psi(r\,v) = r\,\psi(v)$, so $r = 0$ and $\langle v \rangle \cap V' = 0$. Thus, we deduce that $V = \langle v \rangle \oplus V'$.

When $w \in U$, we see that the element r divides $\psi(w)$ because $\psi(w) \in \psi(U) = \langle r \rangle$. Writing $\psi(w) = t\,w$ for some $t \in R$, we have $\psi(w)\,v = t\,r\,v = t\,u$. Since $w - \psi(w)\,v = w - t\,u \in U \cap V' = U'$, the argument in the previous paragraph shows that $U = \langle u \rangle \oplus U'$. □

Proof of Theorem 3.6.1. Let U be a submodule of a finitely generated free R-module V. The case $U = 0$ is vacuous, so we may assume that $U \neq 0$. Applying Lemma 3.6.2 to the submodule $U \subset V$ gives an element $u_1 \in U$ and a submodule $U_1 \subseteq U$ such that $U = \langle u_1 \rangle \oplus U_1$. If $U_1 = 0$, then we are done. Otherwise applying Lemma 3.6.2 to the submodule $U_1 \subseteq V$, we obtain an element $u_2 \in U_1$ and a submodule $U_2 \subset U_1$ such that $U = \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus U_2$. Continuing this process produces $u_1, u_2, \dots, u_m \in U$ such that $U = \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus \cdots \oplus \langle u_m \rangle \oplus U_m$ as long as the R-module U_m is nonzero. However, $m \leqslant \operatorname{rank}_R V$ because $u_1, u_2, \dots, u_m$ are linearly independent in V. It follows that the process must terminate; $U_m = 0$ for some $m \leqslant \operatorname{rank}_R V$. We conclude that $U = \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus \cdots \oplus \langle u_m \rangle$. □

3.6.3 Remark. The hypothesis in Theorem 3.6.1 that R is a principal ideal domain is necessary. The ring R fails to be a principal ideal domain if it has a zerodivisor or a non-principal ideal.

- When R is not a domain, there exists nonzero elements $a, b \in R$ such that $ab = 0$. In this case, the principal ideal $\langle a \rangle$ is not a free R-module.
- When the domain R has a non-principal ideal I, any two generators f, g are not linear independent because $(f)\,g + (-g)\,f = 0$.

3.6.4 Corollary. *A domain R is a principal ideal domain if and only if, for any finitely generated R-module V and any surjective R-module homomorphism $\varphi_0 : R^{m_0} \to V$, there exists a nonnegative integer m_1 and an R-module homomorphism $\varphi_1 : R^{m_1} \to R^{m_0}$ such that the sequence*

$$0 \longrightarrow R^{m_1} \xrightarrow{\varphi_1} R^{m_0} \xrightarrow{\varphi_0} V \longrightarrow 0$$

is exact.

Proof.

(⇒) Corollary 3.4.9 shows that there is a nonnegative integer m_0 and a surjective R-module homomorphism $\varphi_0 : R^{m_0} \to V$. Since Theorem 3.6.1 establishes that the submodule $\operatorname{Ker}(\varphi_0)$ is free, the choice of an isomorphism $\varphi_1 : R^{m_1} \to \operatorname{Ker}(\varphi_0)$ gives the desired exact sequence.

(⇐) Let I be an ideal in R and consider the exact sequence

$$0 \longrightarrow I \longrightarrow R \longrightarrow \frac{R}{I} \longrightarrow 0\,.$$

Theorem 3.6.1 implies that the ideal I is a free submodule of R^1 of rank at most 1. Thus, any nonzero ideal is principal. □

3.7 Matrices

Copyright © 2020, Gregory G. Smith
Last updated: 2020–11–17

Choosing bases for the source and the target, we obtain a concrete representation for any homomorphism between free modules.

3.7.1 Definition. Let R be a commutative ring. An $(m \times n)$-matrix over R is a rectangular array

$$\mathbf{A} := \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix} = [a_{i,j}]$$

where $a_{i,j} \in R$. The set $\operatorname{Mat}(m, n, R)$ of matrices over the ring R has a R-module structure. Addition and scalar multiplication are defined entrywise: for all $r \in R$ and all $\mathbf{A}, \mathbf{B} \in R^{m \times n}$, we have

$$r\,\mathbf{A} + \mathbf{B} = r\,[a_{i,j}] + [b_{i,j}] = [r\,a_{i,j} + b_{i,j}]\,.$$

3.7.2 Definition. Let V be a finitely generated free R-module with basis $(v_1, v_2, \dots, v_n)$. For any $v \in V$, there exists unique elements $b_1, b_2, \dots, b_n \in R$ such that as $v = b_1\,v_1 + \cdots + b_n\,v_n$. The ***matrix of*** v with respect to this basis is defined to be

$$\mathbf{M}(v) := \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \in \operatorname{Mat}(n, 1, R)\,.$$

Let W be a free R-module with basis $(w_1, w_2, \dots, w_m)$ and consider an R-module homomorphism $\varphi \colon V \to W$. For all $1 \leqslant k \leqslant n$, there exists unique elements $a_{1,k}, a_{2,k}, \dots, a_{m,k} \in R$ such that

$$\varphi(v_k) = a_{1,k}\,w_1 + a_{2,k}\,w_2 + \cdots + a_{m,k}\,w_m\,.$$

The ***matrix of*** φ with respect to these bases is

$$\mathbf{M}(\varphi) := \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix} = [a_{i,j}]\,.$$

This definition implies that, for all $r \in R$ and all $\varphi, \psi \in \operatorname{Hom}_R(V, W)$, we have $\mathbf{M}(r\,\varphi) = r\,\mathbf{M}(\varphi)$ and $\mathbf{M}(\varphi + \psi) = \mathbf{M}(\varphi) + \mathbf{M}(\psi)$. In other words, once the bases of the source and target are fixed, the map $\mathbf{M} \colon \operatorname{Hom}_R(V, W) \to \operatorname{Mat}(m, n, R)$ is an R-module isomorphism.

3.7.3 Definition. For all $\mathbf{A} \in \operatorname{Mat}(\ell, m, R)$ and all $\mathbf{B} \in \operatorname{Mat}(m, n, R)$, the ***product*** $\mathbf{A}\,\mathbf{B} \in \operatorname{Mat}(\ell, n, R)$ is defined by $\mathbf{A}\,\mathbf{B} := \big[\sum_k a_{i,k}\,b_{k,j}\big]$. This map $\operatorname{Mat}(\ell, m, R) \times \operatorname{Mat}(m, n, R) \to \operatorname{Mat}(\ell, n, R)$ inherits the following properties from the underlying ring R. For all $r \in R$ and all compatible matrices $\mathrm{A}, \mathrm{B}, \mathrm{C}$, we have

$$\mathrm{A}\,(\mathrm{B}+\mathrm{C}) = \mathrm{A}\,\mathrm{B} + \mathrm{A}\,\mathrm{C} \qquad (\mathrm{A}\,\mathrm{B})\,\mathrm{C} = \mathrm{A}\,(\mathrm{B}\,\mathrm{C})$$
$$(\mathrm{A}+\mathrm{B})\,\mathrm{C} = \mathrm{A}\,\mathrm{C} + \mathrm{B}\,\mathrm{C} \qquad r\,(\mathrm{A}\,\mathrm{B}) = (r\,\mathrm{A})\,\mathrm{B} = \mathrm{A}\,(r\,\mathrm{B})\,.$$

However, we typically have $\mathrm{A}\,\mathrm{B} \neq \mathrm{B}\,\mathrm{A}$.

3.7.4 Lemma. *Let V and W be finitely generated free R-modules with chosen bases. For all $v \in V$ and $\varphi \in \mathrm{Hom}_R(V, W)$, we have*

$$\mathrm{M}\big(\varphi(v)\big) = \mathrm{M}(\varphi)\ \mathrm{M}(v)$$

Proof. Let $(v_1, v_2, \dots, v_n)$ is the chosen basis for the free R-module V. If $\mathrm{M}(\varphi) = [a_{i,j}] \in \mathrm{Mat}(m, n, R)$ and $v = b_1\,v_1 + b_2\,v_2 + \cdots + b_n\,v_n$, then we have

$$\varphi(v) = \sum_{j=1}^{n} b_j\,\varphi(v_j) = \sum_{j=1}^{n} b_j \left(\sum_{i=1}^{m} a_{i,j}\,w_i\right) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{i,j}\,b_j\right) w_i\,,$$

so $\mathrm{M}\big(\varphi(v)\big) = [\sum_j a_{i,j}\,b_j]$ as required. □

3.7.5 Theorem. *Let U, V, W be finitely generated free R-modules with chosen bases. For any $\psi \in \mathrm{Hom}_R(U, V)$ and any $\varphi \in \mathrm{Hom}_R(V, W)$, we have $\mathrm{M}(\varphi \circ \psi) = \mathrm{M}(\varphi)\ \mathrm{M}(\psi)$.*

Theorem 3.7.5 justifies the definition of matrix multiplication.

Proof. For all $u \in U$, Lemma 3.7.4 gives

$$\begin{aligned}\mathrm{M}(\varphi \circ \psi)\ \mathrm{M}(u) &= \mathrm{M}\big((\varphi \circ \psi)(u)\big) = \mathrm{M}\big(\varphi(\psi(u))\big) \\ &= \mathrm{M}(\varphi)\ \mathrm{M}\big(\psi(u)\big) = \mathrm{M}(\varphi)\ \mathrm{M}(\psi)\ \mathrm{M}(u)\,.\end{aligned}$$

Since $\mathrm{M}(u)$ is arbitrary, the claim follows. □

3.7.6 Definition. A matrix whose rows and columns have the same index set is ***square***. Addition and multiplication of square matrices over a commutative R induce a noncommutative ring structure on $\mathrm{Mat}(n, n, R)$. The multiplicative unit is identity matrix $\mathbf{I} := [\delta_{i,j}]$. The group of invertible elements is $\mathrm{GL}(n, R)$.

3.7.7 Proposition. *Let R be a commutative ring and let V be a finitely generated free R-module with a chosen basis. The map $\varphi \mapsto \mathrm{M}(\varphi)$ defines both a ring isomorphism between $\mathrm{End}_R(V)$ and $\mathrm{Mat}(n, n, R)$ and group isomorphism between $\mathrm{Aut}_R(V)$ and $\mathrm{GL}(n, R)$.*

Proof. Follows immediately from the definitions. □