2. Simple modules

We first introduce the natural notion of maps between modules.

Definition 2.1. Let R be a ring and let M and N be left R-modules. The map $f\colon M \to N$ is called R-linear if for all $x, y \in M$ and $a \in R$,

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ f(a \cdot x) &= a \cdot f(x). \end{aligned}$$

The set of R-linear maps $f\colon M \to N$ is denoted by $\mathrm{Hom}_R(M, N)$.

Remark 2.2. The set $\mathrm{Hom}_R(M, N)$ of R-linear maps from M to N is an abelian group with addition defined by $(f+g)(x) = f(x) + g(x)$. If M and N are equal, we also write $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$. It is a ring with the product given by composition $(f \circ g)(x) = f(g(x))$.

Example 2.3. Let R be a ring and let M and N be free right R-modules with finite bases $X = \{x_1, \dots, x_m\}$ and $Y = \{y_1, \dots, y_n\}$. If $f\colon N \to M$ is an R-linear map, we let A be the $m \times n$-matrix whose entries $a_{ij} \in R$ are defined by

$$f(y_i) = x_1 a_{1i} + x_2 a_{2i} + \dots + x_m a_{mi}.$$

Then for a general element $y = y_1 s_1 + \dots + y_n s_n$ of N, we find

$$\begin{aligned} f(y) &= f(y_1)s_1 + \dots + f(y_n)s_n \\ &= (x_1 a_{11} + \dots + x_m a_{m1})s_1 + \dots + (x_1 a_{1n} + \dots + x_m a_{mn})s_n \\ &= x_1(a_{11}s_1 + \dots + a_{1n}s_n) + \dots + x_m(a_{m1}s_1 + \dots + a_{mn}s_n). \end{aligned}$$

Hence, if $y = y_1 s_1 + \dots + y_n s_n$, then $f(y) = x_1 r_1 + \dots x_m r_m$, where

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix}$$

We say that the matrix A represents the R-linear maps $f\colon N \to M$ with respect to the given bases $Y \subset N$ and $X \subset M$. We note that It is important here to consider right R-modules and not left R-modules. With left R-modules, we would obtain "row vectors" instead of "column vectors."

Proposition 2.4. *Suppose that M, N, and P are free right R-modules with finite bases $X = \{x_1, \dots, x_m\}$, $Y = \{y_1, \dots, y_n\}$, and $Z = \{z_1, \dots, z_p\}$, respectively. Let A be the $m \times n$-matrix that represents the R-linear map $f\colon N \to M$ with respect to the bases $Y \subset N$ and $X \subset M$, and let B be the $n \times p$-matrix that represents the R-linear map $g\colon P \to N$ with respect to the bases $Z \subset P$ and $Y \subset N$. Then the $m \times p$-matrix that represents the R-linear map $f \circ g\colon P \to M$ with respect to the bases $Z \subset P$ and $X \subset M$ is the product matrix AB.*

Proof. Let $z = z_1 t_1 + \cdots + z_p t_p$ be an element of P, let $g(z) = y_1 s_1 + \cdots + y_n s_n$, and let $f(g(z)) = x_1 r_1 + \cdots + x_m r_m$. By the definition of A and B,

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix}$$

$$\begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1p} \\ b_{21} & b_{22} & \cdots & b_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{np} \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_p \end{pmatrix}$$

and hence

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1p} \\ b_{21} & b_{22} & \cdots & b_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{np} \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_p \end{pmatrix}$$

The proposition follows. □

Corollary 2.5. *Let R be a ring and let M be a free* right *R-module with a finite basis $X = \{x_1, \dots, x_m\}$. Then the map*

$$\alpha \colon M_m(R) \to \operatorname{End}_R(M)$$

that takes the $m \times m$-matrix A to the R-linear map $f \colon M \to M$ represented by A with respect to the basis $X \subset M$ is a ring isomorphism.

Proof. Every R-linear map $f \colon M \to M$ is represented with respect to the basis $X \subset M$ by the unique $m \times m$-matrix defined in Example 2.3. Therefore, the map α is a bijection. Moreover, the R-linear map represented by the identity matrix I_m is the identity map id_M; the R-linear map represented by a sum $A + B$ of two matrices A and B is the sum $f + g$ of the R-linear maps f and g represented by the matrices A and B, respectively; and the R-linear map represented by the matrix product AB is the composition $f \circ g$ of the R-linear maps f and g. This shows that α is a ring homomorphism, and hence, a ring isomorphism. □

Remark 2.6. Let $R = (R, +, \cdot)$ be a ring. The opposite ring $R^{\mathrm{op}} = (R, +, *)$ has the same set R and addition $+$ but the "opposite" product $a * b = b \cdot a$. The left R-module $M = (M, +, \cdot)$ determines the right R^{op}-module $M^{\mathrm{op}} = (M, +, *)$ with $x * a = a \cdot x$. Now, the map $f \colon M \to M$ is R-linear if and only if $f \colon M^{\mathrm{op}} \to M^{\mathrm{op}}$ is R^{op}-linear, and therefore, the rings $\operatorname{End}_R(M)$ and $\operatorname{End}_{R^{\mathrm{op}}}(M^{\mathrm{op}})$ are equal. Hence, if M is a free *left* R-module with a finite basis $X = \{x_1, \dots, x_m\}$, then the map

$$\alpha \colon M_m(R^{\mathrm{op}}) \to \operatorname{End}_R(M)$$

from Corollary 2.5 is a ring isomorphism.

Exercise 2.7. Let A and B be two $n \times n$-matrices with entries in the ring R. Describe the product $A * B$ of A and B in the opposite ring $M_n(R)^{\mathrm{op}}$.

A division ring R is the simplest kind of ring in the sense that every left R-module is a free module. We will next consider a slightly more complicated class of rings that are called simple rings.

DEFINITION 2.8. Let R be a ring and let M and M' be left R-modules.

(i) The *direct sum* of M and M' is the left R-module

$$M \oplus M' = \{(x, x') \mid x \in M, x' \in M'\}$$

with sum and scalar multiplication defined by

$$(x, x') + (y, y') = (x + y, x' + y')$$
$$a \cdot (x, x') = (ax, ax').$$

(ii) The subset $N \subset M$ is a *submodule* if for all $x, y \in N$ and $a \in R$, $x+y \in N$ and $ax \in N$.

(iii) The *sum* of two submodules $N, N' \subset M$ is the submodule

$$N + N' = \{x + x' \mid x \in N, x' \in N'\} \subset M.$$

(iv) The sum of the submodules $N, N' \subset M$ is *direct* if the map

$$N \oplus N' \to N + N'$$

that to (x, x') associates $x + x'$ is an isomorphism, or equivalently, if the intersection $N \cap N'$ is the zero module $\{0\}$.

EXAMPLE 2.9. (1) A submodule $I \subset R$ of the ring R considered as a left R-module over itself is called a *left ideal* of R.

(2) Let $m, n \in \mathbb{Z}$ be integers. Then $m\mathbb{Z}, n\mathbb{Z} \subset \mathbb{Z}$ are ideals and

$$m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z} \subset m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z}$$

where (m, n) and $[m, n]$ are the greatest common divisor and least common multiple of m and n, respectively. The sum $m\mathbb{Z} + n\mathbb{Z}$ is direct if and only if one or both of m and n are zero.

(3) Let R be a ring and let $M_2(R)$ be the ring of 2×2-matrices. The subsets

$$P_{2,1}(R) = \left\{ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} \mid a, c \in R \right\} \subset M_2(R)$$
$$P_{2,2}(R) = \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \mid b, d \in R \right\} \subset M_2(R)$$

are left ideals, and the sum $P_{2,1}(R) + P_{2,2}(R)$ is direct and equals $M_2(R)$. Similarly, the subsets

$$Q_{2,1}(R) = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in R \right\} \subset M_2(R)$$
$$Q_{2,2}(R) = \left\{ \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \mid c, d \in R \right\} \subset M_2(R)$$

are right ideals, and the sum $Q_{2,1}(R) + Q_{2,2}(R)$ is direct and equal to $M_2(R)$.

DEFINITION 2.10. Let R be a ring.

(1) The left R-module S is *simple* if it is non-zero and if the only submodules of S are $\{0\}$ and S.

(2) The left R-module M is *semi-simple* if it is a direct sum

$$M = S_1 + \cdots + S_n$$

of finitely many simple submodules.

Example 2.11. Let D be a division ring. We claim that as a left module over itself, D is simple. Indeed, let $N \subset D$ be a non-zero submodule and let $a \in N$ be a non-zero element. If $b \in D$, then $b = ba^{-1} \cdot a \in N$, and hence, $N = D$ which proves the claim. Let S be any simple left D-module and let $x \in S$ be a non-zero element. We claim that the D-linear map $f \colon D \to S$ defined by $f(a) = a \cdot x$ is an isomorphism. Indeed, the image $f(D) \subset S$ is a submodule and it is not zero since $x \in f(D)$. Since S is simple, we necessarily have $f(D) = S$, so f is surjective. Similearly, the kernel $\ker(f) = \{a \in D \mid f(a) = 0\} \subset D$ is a submodule and it is not all of D since $f(1) = x \neq 0$. Since D is simple, we have $\ker(f) = \{0\}$, so f is injective. This proves the claim. We conclude that a division ring D has a unique isomorphism class of simple left D-modules.

Lemma 2.12. *Let D be a division ring and let $R = M_n(D)$. The left R-module of column n-vectors $S = M_{n,1}(D)$ is a simple left R-module.*

Proof. Let $N \subset S$ be a non-zero submodule. We must show that $N = S$. We first choose a non-zero vector $x_1 \in N$. By Theorem 1.10, we can choose additional vectors $x_2, \dots, x_n \in S$ such that $X = \{x_1, x_2, \dots, x_n\}$ is a basis of S as a right D-vector space. Here and below, we use that, by Remark 1.12, every basis of S as a right D-vector space has n elements. Now let $A \in R$ be the $n \times n$-matrix whose jth column is x_j. We claim that A is invertible. Indeed, since $X \subset S$ is a right D-vector space basis, there exists $B \in R$ such that $AB = I$ which, in turn, implies that A and B are invertible and $BA = I$. Hence

$$Bx_1 = BAe_1 = e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

which shows that $e_1 \in N$. Now, given $x \in S$, we choose $C \in R$ with x as its first column. Then $x = Ce_1 \in N$ which shows that $x \in N$ as desired. $\square$

Proposition 2.13 (Schur's lemma). *Let R be a ring and let S be a simple right R-module. Then the ring $\mathrm{End}_R(S)$ is a division ring.*

Proof. Let $f \colon S \to S$ be a non-zero R-linear map. We must show that there exists an R-linear map $g \colon S \to S$ such that both $f \circ g$ and $g \circ f$ are the identity map of S. It suffices to show that f is a bijection. For then $f^{-1} \colon S \to S$ is the desired R-linear map. Now, the image $f(S) \subset S$ is a submodule which is non-zero since f is non-zero. As S is simple, we conclude that $f(S) = S$, so f is surjective. Similarly, $\ker(f) \subset S$ is a submodule which is not all of S since f is not the zero map. Since S is simple, we conclude that $\ker(f)$ is zero, so f is injective. $\square$