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 right R-modules. The map $f\colon N \to M$ is called R-linear if for all $\boldsymbol{x}, \boldsymbol{y} \in N$ and $a \in R$,

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

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

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

Example 2.3. Let R be a ring and let M and N be free right R-modules with finite bases $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_m)$ and $(\boldsymbol{y}_1, \dots, \boldsymbol{y}_n)$. If $f\colon N \to M$ is an R-linear map, then we let $A = (a_{ij})$ be the $m \times n$-matrix, whose entries $a_{ij} \in R$ are defined by

$$f(\boldsymbol{y}_j) = \boldsymbol{x}_1 a_{1j} + \boldsymbol{x}_2 a_{2j} + \dots + \boldsymbol{x}_m a_{mj}.$$

In this situation, we find, for a general element $\boldsymbol{y} = \boldsymbol{y}_1 s_1 + \dots + \boldsymbol{y}_n s_n$ of N, that

$$\begin{aligned} f(\boldsymbol{y}) &= f(\boldsymbol{y}_1)s_1 + \dots + f(\boldsymbol{y}_n)s_n \\ &= (\boldsymbol{x}_1 a_{11} + \dots + \boldsymbol{x}_m a_{m1})s_1 + \dots + (\boldsymbol{x}_1 a_{1n} + \dots + \boldsymbol{x}_m a_{mn})s_n \\ &= \boldsymbol{x}_1(a_{11}s_1 + \dots + a_{1n}s_n) + \dots + \boldsymbol{x}_m(a_{m1}s_1 + \dots + a_{mn}s_n). \end{aligned}$$

Hence, if $\boldsymbol{y} = \boldsymbol{y}_1 s_1 + \dots + \boldsymbol{y}_n s_n$, then $f(\boldsymbol{y}) = \boldsymbol{x}_1 r_1 + \dots \boldsymbol{x}_m r_m$, 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 bases $(\boldsymbol{y}_1, \dots, \boldsymbol{y}_n)$ of N and $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_m)$ of 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 $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_m)$, $(\boldsymbol{y}_1, \dots, \boldsymbol{y}_n)$, and $(\boldsymbol{z}_1, \dots, \boldsymbol{z}_p)$, 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 $(\boldsymbol{y}_1, \dots, \boldsymbol{y}_n)$ of N and $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_m)$ of 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 $(\boldsymbol{z}_1, \dots, \boldsymbol{z}_p)$ of P and $(\boldsymbol{y}_1, \dots, \boldsymbol{y}_n)$ of N. Then the $m \times p$-matrix C that represents the R-linear map $f \circ g\colon P \to M$ with respect to the bases $(\boldsymbol{z}_1, \dots, \boldsymbol{z}_p)$ of P and $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_m)$ of M is*

$$C = AB.$$

Proof. We let $\boldsymbol{z} = \boldsymbol{z}_1 t_1 + \dots + \boldsymbol{z}_p t_p$ be a general element of P, and write $g(\boldsymbol{z}) = \boldsymbol{y}_1 s_1 + \dots + \boldsymbol{y}_n s_n$, and $f(g(\boldsymbol{z})) = \boldsymbol{x}_1 r_1 + \dots + \boldsymbol{x}_m r_m$. By the definition of the matrices A and B, we have

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

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

and hence

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

By the definition of the matrix C and by the associativity of matrix product, we conclude that $C = AB$ as stated. □

COROLLARY 2.5. *Let R be a ring and let M be a free right R-module with a finite basis $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_m)$, and let*

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

be the map that to an $m \times m$-matrix A assigns the R-linear map $f \colon M \to M$ that is represented by A with respect to the basis $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_m)$ for both domain and codomain. The map α is a ring isomorphism.

PROOF. Every R-linear map $f \colon M \to M$ is represented with respect to the basis $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_m)$ of M by the unique $m \times m$-matrix defined in Example 2.3. Hence, 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, by Proposition 2.4, the R-linear map represented by the matrix product $A \cdot B$ 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 $a * b = b \cdot a$. A left R-module $M = (M, +, \cdot)$ determines the right R^{op}-module $M^{\mathrm{op}} = (M, +, *)$ with $x * a = a \cdot x$. Now, a 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 $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_m)$, then the map

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

from Corollary 2.5 is a ring isomorphism.

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

DEFINITION 2.7. 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

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

with sum and scalar multiplication defined by

$$(\boldsymbol{x}, \boldsymbol{x}') + (\boldsymbol{y}, \boldsymbol{y}') = (\boldsymbol{x} + \boldsymbol{y}, \boldsymbol{x}' + \boldsymbol{y}')$$
$$a \cdot (\boldsymbol{x}, \boldsymbol{x}') = (a\boldsymbol{x}, a\boldsymbol{x}').$$

(ii) A subset $N \subset M$ is a *submodule* if for all $\boldsymbol{x}, \boldsymbol{y} \in N$ and $a \in R$, $\boldsymbol{x} + \boldsymbol{y} \in N$ and $a\boldsymbol{x} \in N$.

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

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

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

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

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

EXAMPLE 2.8. (1) Let R be a ring. A submodule $I \subset R$ of R considered as a left R-module 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 2.9. Let R be a ring.

(1) A left R-module S is *simple* if it is non-zero and if the only submodules of S are $\{\mathbf{0}\}$ and S.
(2) A 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 2.10. 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 $\boldsymbol{x} \in S$ be a non-zero element. We claim that the D-linear map $f \colon D \to S$ defined by $f(a) = a \cdot \boldsymbol{x}$ is an isomorphism. Indeed, the image $f(D) \subset S$ is a submodule and it is not zero since $\boldsymbol{x} \in f(D)$. Since S is simple, we necessarily have $f(D) = S$, so f is surjective. Similarly, the kernel $\ker(f) = \{a \in D \mid f(a) = \mathbf{0}\} \subset D$ is a submodule, and it is not all of D since $f(1) = \boldsymbol{x} \neq \mathbf{0}$. 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 2.11. *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 $\boldsymbol{x}_1 \in N$. By Theorem 1.12, we can choose additional vectors $\boldsymbol{x}_2, \dots, \boldsymbol{x}_n \in S$ such that the family $(\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_n)$ is a basis of S as a right D-vector space. Here and below, we use that, by Remark 1.14, 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 $\boldsymbol{x}_j$. We claim that A is invertible. Indeed, since $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ is a right D-vector space basis, there exists $B \in R$ such that $AB = I$ which, by Gauss elimination, implies that A and B are invertible and that $BA = I$. Hence
$$B\boldsymbol{x}_1 = BA\boldsymbol{e}_1 = \boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$
which shows that $\boldsymbol{e}_1 \in N$. Now, given $\boldsymbol{x} \in S$, we choose $C \in R$ with $\boldsymbol{x}$ as its first column. Then $\boldsymbol{x} = C\boldsymbol{e}_1 \in N$ which shows that $\boldsymbol{x} \in N$ as desired. □

PROPOSITION 2.12 (Schur's lemma). *Let R be a ring and let S be a simple left R-module. Then the ring* $\operatorname{End}_R(S)$ *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 the inverse of an R-linear bijection is automatically R-linear. 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. □