1. Rings and modules

The notion of a module is a generalization of the familiar notion of a vector space. The generalization consists in that the scalars used for scalar multiplication are taken to be elements of a general ring. We first define rings.

DEFINITION 1.1. A *ring* is a triple $(R, +, \cdot)$ consisting of a set R and two maps $+\colon R \times R \to R$ and $\cdot : R \times R \to R$ that satisfy the following axioms.

(A1) For all $a, b, c \in R$, $a + (b + c) = (a + b) + c$.
(A2) There exists an element $0 \in R$ such that for all $a \in R$, $a + 0 = a = 0 + a$.
(A3) For every $a \in R$, there exists $b \in R$ such that $a + b = 0 = b + a$.
(A4) For all $a, b \in R$, $a + b = b + a$.
(P1) For all $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
(P2) There exists an element $1 \in R$ such that for all $a \in R$, $a \cdot 1 = a = 1 \cdot a$.
(D) For all $a, b, c \in R$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

The ring $(R, +, \cdot)$ is called *commutative* if the following further axiom holds.

(P3) For all $a, b \in R$, $ab = ba$.

The axioms (A1)–(A4) and (P1)–(P2) express that $(R, +)$ is an abelian group and that $(R, \cdot)$ is a monoid, respectively. The axiom (D) expresses that $\cdot$ distributes over $+$. We often suppress $\cdot$ and write ab instead of $a \cdot b$. The zero element 0 which exist by axiom (A2) is unique. Indeed, if both 0 and $0'$ satisfy (A2), then

$$0' = 0 + 0' = 0.$$

Moreover, for a given $a \in R$, the element $b \in R$ such that $a + b = 0 = b + a$ which exists by (A3) is unique. Indeed, if both b and b' satisfy (A3), then

$$b = b + 0 = b + (a + b') = (b + a) + b' = 0 + b' = b'.$$

We write $-a$ instead of b for this element. Similarly, the element $1 \in R$ which exists by axiom (P2) is unique. We usuall abuse language and write R instead of $(R, +, \cdot)$.

EXAMPLE 1.2. (1) The ring $\mathbb{Z}$ of integers. It is a commutative ring.

(2) The rings $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ of rational numbers, real numbers, and complex numbers respectively. These rings are all *fields* which mean that they are commutative, that $1 \neq 0$, and that for all $a \in R \smallsetminus \{0\}$, there exists $b \in R$ such that $ab = 1 = ba$. This element b is uniquely determined by a and is written a^{-1}.

(3) The ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n. It is a field if and only if n is a prime number.

(4) The ring $\mathbb{H}$ of quarternions given by the set

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

with addition $+$ and multiplication $\cdot$ defined by

$$\begin{aligned}
&(a + bi + cj + dk) + (a' + b'i + c'j + d'k) \\
&\quad = (a + a') + (b + b')i + (c + c')j + (d + d')k \\
&(a + bi + cj + dk) \cdot (a' + b'i + c'j + d'k) \\
&\quad = (aa' - bb' - cc' - dd') + (ab' + a'b + cd' - dc')i \\
&\qquad + (ac' + a'c + db' - bd')j + (ad' + a'd + bc' - b'c)k
\end{aligned}$$

It is a *division ring* which means that $1 \neq 0$ and that for all $a \in R \smallsetminus \{0\}$, there exists $b \in R$ such that $ab = 1 = ba$. A field is a commutative division ring. The quartenions $\mathbb{H}$ is not a commutative ring. For instance, $ij = k$ but $ji = -k$.

(5) Let R be a ring and. For every positive integer n, the set of $n \times n$-matrices with entries in R equipped with matrix addition and matrix multiplication forms a ring $M_n(R)$. The multiplicative unit element $1 \in M_n(R)$ is the identity matrix and is usually written I. The ring $M_n(R)$ is not commutative except if $n = 1$ and R is commutative.

(6) The set $C^0(X, \mathbb{C})$ of continuous complex valued functions on a topological space X is a commutative ring under pointwise addition and multiplication. The multiplicative unit element $1 \in C^0(X, \mathbb{C})$ is the constant function with value $1 \in \mathbb{C}$.

DEFINITION 1.3. Let R and S be rings. A *ring homomorphism* from R to S is a map for which the following (i)—(iii) hold.

(i) $f(1) = 1$
(ii) For all $a, b \in R$, $f(a + b) = f(a) + f(b)$.
(iii) For all $a, b \in R$, $f(a \cdot b) = f(a) \cdot f(b)$.

EXERCISE 1.4. Let $f\colon R \to S$ be a ring homomorphism. Show that $f(0) = 0$ and that for all $a \in R$, $f(-a) = -f(a)$.

EXAMPLE 1.5. (1) For every ring R, the identity map $\mathrm{id}\colon R \to R$ is a ring homomorphism. Moreover, if $f\colon R \to S$ and $g\colon S \to T$ are ring homomorphisms, then so is the composite map $g \circ f\colon R \to T$.

(2) For every ring R, there is a unique ring homomorphism $f\colon \mathbb{Z} \to R$. We sometimes abuse notation and write $n \in R$ for the image of $n \in \mathbb{Z}$.

(3) There is a ring homomorphism $f\colon \mathbb{H} \to M_4(\mathbb{R})$ determined by

$$f(a + bi + cj + dk) = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

(4) The canonical inclusions of $\mathbb{Z}$ in $\mathbb{Q}$, of $\mathbb{Q}$ in $\mathbb{R}$, of $\mathbb{R}$ in $\mathbb{C}$, and of $\mathbb{C}$ in $\mathbb{H}$ are all ring homomorphims.

DEFINITION 1.6. Let R be a ring. A *left R-module* is a triple $(M, +, \cdot)$ consisting of a set M and two maps $+\colon M \times M \to M$ and $\cdot\colon R \times M \to M$ such that $(M, +)$ satisfy the axioms (A1)–(A4) and such that the following additional axioms hold.

(M1) For all $a, b \in R$ and $x \in M$, $a \cdot (b \cdot x) = (a \cdot b) \cdot x$.
(M2) For all $a \in R$ and $x, y \in M$, $a \cdot (x + y) = (a \cdot x) + (b \cdot y)$.
(M3) For all $a, b \in R$ and $x \in M$, $(a + b) \cdot x = (a \cdot x) + (b \cdot x)$.
(M4) For all $x \in M$, $1 \cdot x = x$.

The notion of a right R-module is defined analogously.

EXAMPLE 1.7. (1) The ring R is both a left R-module and a right R-module.

(2) The set R^n considered as the set of "n-dimensional column vectors" is a left $M_n(R)$-module and considered as the set of "n-dimensional row vectors" is a right $M_n(R)$-module.

(3) Let n be a positive integer, let d be a divisor in n, and define

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$$

by $(a + n\mathbb{Z}) \cdot (x + d\mathbb{Z}) = ax + d\mathbb{Z}$. This makes $\mathbb{Z}/d\mathbb{Z}$ a left $\mathbb{Z}/n\mathbb{Z}$-module.

DEFINITION 1.8. Let R be a ring and let M a left R-module.

(1) A *linear combination* of $X \subset M$ is a sum of the form
$$a_1x_1 + a_2x_2 + \cdots + a_nx_n$$
with $a_1, \ldots, a_n \in R$ and $x_1, \ldots, x_n \in X$.
(2) The subset $X \subset M$ *generates* M if every $y \in M$ can be written as a linear combination $y = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ of X.
(3) The subset $X \subset M$ is *linearly independent* if for the linear combination $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ to equal 0 implies that $a_1, \ldots, a_n$ are all zero.
(4) The subset $X \subset M$ is a *basis* if it generates M and is linearly independent.
(5) The module M is *free* if it admits a basis.

EXAMPLE 1.9. (1) The left $\mathbb{Z}/6\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ in Example 1.7 (3) is not a free module. The subset $X = \{1 + 2\mathbb{Z}\} \subset \mathbb{Z}/2\mathbb{Z}$ generates $\mathbb{Z}/2\mathbb{Z}$ but it is not linearly independent. Indeed, $(2 + 6\mathbb{Z}) \cdot (1 + 2\mathbb{Z}) = 2 + 2\mathbb{Z}$ is zero in $\mathbb{Z}/2\mathbb{Z}$, but $2 + 6\mathbb{Z}$ is not zero in $\mathbb{Z}/6\mathbb{Z}$.

(2) Let M be a left R-module. The empty subset $\emptyset \subset M$ is linearly independent and the whole subset $M \subset M$ generates M.

THEOREM 1.10. *Every left module over a division ring is free. More precisely, given two subsets $X \subset Y \subset M$ such that X is linearly independent and such that Y generates M, there exists a basis $B \subset M$ with $X \subset B \subset Y$.*

PROOF. Let S be the set that consists of all subsets $Z \subset M$ that are linearly independent and satisfy $X \subset Z \subset Y$. We will use Zorn's lemma to prove that S has a maximal element. To this end, we must verify the following (i)–(ii).

(i) The set S is non-empty.
(ii) Every to subset $T \subset S$ which is totally ordered with respect to inclusion has an upper bound in S.

Now, since $X \in S$, we conclude that (i) holds. To verify (ii), let $T \subset S$ be a totally ordered subset of S. Then $Z_T = \bigcup_{Z \in T} Z$ is a linearly independent subset of M and $X \subset Z_T \subset Y$. So $Z_T \in S$ and for all $Z \in T$, $Z \subset Z_T$ which proves (ii). By Zorn's lemma, S has a maximal element B. Since $B \in S$, $B \subset M$ is linearly independent and $X \subset B \subset Y$. We show that B generates M. If not, there exists $y \in Y$ which is not a linear combination of elements in B. We claim that $B \cup \{y\} \subset M$ is linearly independent. Indeed, suppose
$$a_1x_1 + \cdots + a_nx_n + ay = 0$$
with $a_1, \ldots, a_n, a \in R$ and $x_1, \ldots, x_n \in B$. Then $a = 0$ or else
$$y = -a^{-1}(a_1x_1 + \cdots + a_nx_n)$$
which contradicts that y is not a linear combination of elements of B. (Here we have used the assumption that R is a division ring.) Since B is linearly independent, we further have $a_1 = \cdots = a_n = 0$. This proves the claim that $B \cup \{y\}$ is linearly indenpent. Thus $B \cup \{y\} \in S$ which contradicts that $B \in S$ is the maximal element. This shows that B generates M, and hence, is a basis as desired. □

DEFINITION 1.11. A left module over a division ring is called a *left vector space*.

REMARK 1.12. Let M be a left vector space over the division ring R. One may show that the cardinality of a basis $B \subset M$ depends only on M and not on B. This

cardinality is called the *dimension* of M. For a general ring R, two different bases of the same free left R-module M do not necessarily have the same cardinality.

EXERCISE 1.13. The formula

$$(a+bi+cj+dk)\cdot\begin{pmatrix}x_1\\x_2\\x_3\\x_3\end{pmatrix}=\begin{pmatrix}a&-b&-c&-d\\b&a&-d&c\\c&d&a&-b\\d&-c&b&a\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_3\end{pmatrix}$$

defines a left $\mathbb{H}$-vector space structure on $\mathbb{R}^4$. Show that a subset $B\subset\mathbb{R}^4$ is a basis of this left $\mathbb{H}$-vector space if and only if B consists of a single non-zero vector.