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 abuse language and write R instead of $(R, +, \cdot)$.

EXERCISE 1.2. Let R be a ring. Show that for all $a \in R$, $a \cdot 0 = 0 = 0 \cdot a$.

EXAMPLE 1.3. (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 quaternions given by the set of formal sums

$$\mathbb{H} = \{a + ib + jc + kd \mid a, b, c, d \in \mathbb{R}\}$$

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

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

Course homepage: `www.math.nagoya-u.ac.jp/~larsh/teaching/S2018_PM`

It is a *division ring* which means that $1 \neq 0$ and that for all $a \in R \setminus \{0\}$, 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 1.4. 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 1.5. 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 1.6. (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 $f\colon \mathbb{H} \to M_4(\mathbb{R})$ defined by

$$f(a + ib + jc + kd) = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

(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 $\mathbb{H}$ all are ring homomorphims.

Definition 1.7. 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 1.8. (1) Let R be a ring. We may view R both as a left R-module and as a right R-module via the multiplication in R.

(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.

We next recall three very important notions from linear algebra. These notions all concern *families* of elements. By definition, a *family of elements* in a set X is a map $x\colon I \to X$ from some set I to X. We also write $(x_i)_{i\in I}$ to indicate the family $x\colon I \to X$ with $x(i) = x_i$, and we say that I is the indexing set of the family. We remark that the families (1) and $(1, 1)$ of elements in $\mathbb{Z}$ are distinct, since they have distinct indexing sets, whereas the subsets $\{1\}$ and $\{1, 1\}$ of $\mathbb{Z}$ are equal.

Example 1.9. For every set X, there are two extreme examples of families of elements in X, namely, the empty family $(\ )$ with indexing set $\emptyset$, and the identity family $(x)_{x\in X}$ with indexing set X.

Let R be a ring, and let $(a_i)_{i\in I}$ be a family of elements in R. We call

$$\operatorname{supp}(a) = \{i \in I \mid a_i \neq 0\} \subset I$$

for the *support* of the family $(a_i)_{i\in I}$, and we say that the family $(a_i)_{i\in I}$ has *finite support* if its support $\operatorname{supp}(a)$ is a finite set. Let M be a left R-module, and let $(x_i)_{i\in I}$ be a family of elements in M. If $(a_i)_{i\in I}$ is a family of elements in R with the same indexing set I and with finite support, then we define

$$\sum_{i\in I} a_i x_i = \sum_{i\in\operatorname{supp}(a)} a_i x_i.$$

We say that a sum of this form is a *linear combination* of the family $(x_i)_{i\in I}$. If the support $\operatorname{supp}(a)$ is empty, then we define this sum to be equal to $0 \in M$. We say that the family $(a_i)_{i\in I}$ is the zero family, if its support is empty.

Definition 1.10. Let R be a ring, let M a left R-module, and let $(x_i)_{i\in}$ be a family of elements in M.

(1) The family $(x_i)_{i\in I}$ *generates* M if every element $y \in M$ can be written as a linear combination of $(x_i)_{i\in I}$.
(2) The family $(x_i)_{i\in I}$ is *linearly independent* if the only family $(a_i)_{i\in I}$ of elements in R such that $\sum_{i\in I} x_i a_i = 0$ is the zero family.
(3) The family $(x_i)_{i\in I}$ is a *basis* of M if it both generates M and is linearly independent.

We say that an R-module M is *free* if it admits a basis.

Example 1.11. (1) The left $\mathbb{Z}/6\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ in Example 1.8 (3) is not a free module. The family $(1+2\mathbb{Z}\ )$ 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 $\mathbb{Z}/6\mathbb{Z}$, so the family $(2 + 6\mathbb{Z})$ is not the zero family.

(2) Let M be a left R-module. The empty family $(\ )$ is linearly independent, and the identity family $(x)_{x\in M}$ generates M. The empty family is a basis if and only $M = \{0\}$, whereas the identity family never is a basis.

Let X be a set. If $(x_i)_{i\in I}$ is a family of elements in X, and if $J \subset I$ is a subset of the indexing set of the family, then we say that the family $(x_i)_{i\in J}$ is a subfamily of the family $(x_i)_{i\in I}$. In particular, the empty family is a subfamily of every family of elements in X.

THEOREM 1.12. *Every left module over a division ring R is free. More precisely, if $(x_i)_{i\in I}$ is a family of elements in M that generates M, and if $(x_i)_{i\in K}$ is a linearly independent subfamily thereof, then there exists $K \subset J \subset I$ such that $(x_i)_{i\in J}$ is a basis of M.*

PROOF. Let S be the set that consists of all subsets $K \subset Z \subset I$ such that the subfamily $(x_i)_{i\in Z}$ is linearly independent. The set S is partially ordered under inclusion and 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 subset $T \subset S$ which is totally ordered with respect to inclusion has an upper bound in S.

We know that (i) holds, since $K \in S$. To verify (ii), we let $T \subset S$ be a totally ordered subset of S and consider $Z_T = \bigcup_{Z\in T} Z$. The family $(x_i)_{i\in Z_T}$ is linearly independent. Indeed, if

$$\sum_{i\in Z_T} a_i x_i = 0,$$

then $\operatorname{supp}(a) \subset Z$ for some $Z \in T$, since $\operatorname{supp}(a)$ is finite. But then

$$\sum_{i\in Z} a_i x_i = 0,$$

which, by the linear independence of $(x_i)_{i\in Z}$, implies that $(a_i)_{i\in Z_T}$ is the zero family. So $Z_T \in S$ and $Z \subset Z_T$ for all $Z \in T$, which proves (ii). By Zorn's lemma, S has a maximal element J, and since $J \in S$, the subfamily $(x_i)_{i\in J}$ is linearly independent and $K \subset J \subset I$.

It remains to show that $(x_i)_{i\in J}$ generates M. If this is not the case, then there exists $h \in I$ such that x_h is not a linear combination of $(x_i)_{i\in J}$, and we claim that, in this case, the subfamily $(x_i)_{i\in J'}$ with $J' = J \cup \{h\} \subset I$ is linearly independent. Indeed, suppose that

$$\sum_{i\in J'} a_i x_i = 0.$$

If $a_h \neq 0$, then

$$x_h = -a_h^{-1}\big(\sum_{i\in J} a_i x_i\big),$$

which contradicts that x_h is not a linear combination of $(x_i)_{i\in J}$. (This is where we use the assumption that R is a division ring.) So $a_h = 0$, and hence

$$\sum_{i\in J} a_i x_i = 0.$$

Since $(x_i)_{i\in J}$ is linearly independent, we conclude that $(a_i)_{i\in J}$ is the zero family. Therefore, also $(a_i)_{i\in J'}$ is the zero family, which shows the claim that $(x_i)_{i\in J'}$ is linearly independent. But then $J' \in S$ and $J \subset J'$, which contractiсts the maximality of $J \in S$. This shows that $(x_i)_{i\in J}$ generates M, and hence, is a basis of M, as desired. □

DEFINITION 1.13. A left module over a division ring is called a *left vector space*. A right module over a division ring is called a *right vector space*.

REMARK 1.14. Let M be a left vector space over the division ring R. One may show that if $(x_i)_{i\in I}$ is a basis of M, then the cardinality of the indexing set I depends only on M and not on the particular choice of basis. This cardinality is called the *dimension* of M. For a general ring R, two different bases of the same free left R-module M may not have indexing sets of the same cardinality.

EXERCISE 1.15. The formula

$$(a+ib+jc+kd)\cdot\begin{pmatrix}x_1\\x_2\\x_3\\x_3\end{pmatrix}=\begin{pmatrix}a & -b & -c & -d\\ b & a & -d & c\\ c & d & a & -b\\ d & -c & b & a\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_3\end{pmatrix}$$

defines a left $\mathbb{H}$-vector space structure on $\mathbb{R}^4$. Show that any family $(\boldsymbol{x})$ consisting of a single non-zero vector $\boldsymbol{x}\in\mathbb{R}^4$ is a basis of this left $\mathbb{H}$-vector space.