Topics in Mathematical Science VI, Fall 2019: Module Theory and Homological Algebra

Erik Darpö, Graduate School of Mathematics, Nagoya University
Notes by: Xuanrui Qi

October 22, 2019

Chapter 1

Rings and modules

1.1 Review of basic ring theory

To introduce the concept of modules, we must first introduce the concept of the ring, which should be covered in any undergraduate algebra course. Here, we revisit the definition:

Definition 1.1.1 (ring)**.** A **ring** is a triple $(R, +, \cdot)$ where R is a set and $+$ and $\cdot$ are operations on R, i.e. $R \times R \to R$, satisfying the following axioms:

1. $\exists 0 \in R$, $\forall a \in R$, $0 + a = a$ (existence of additive neutral element)
2. $\forall a \in R$, $\exists b \in R$, $a + b = 0$ (additive inverse)
3. $\forall a, b, c \in R$, $a + (b + c) = (a + b) + c$ (associativity of addition)
4. $\forall a, b \in R$, $a + b = b + a$ (commutativity of addition). In other words, $(R, +)$ forms a abelian group.
5. $\exists 1 \in R$, $\forall a \in R$, $1 \cdot a = a$ (existence of multiplicative neutral element)
6. $\forall a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity of multiplication). In other words, $(R, \cdot)$ forms a monoid.
7. $\forall a, b, c \in R$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ (distributivity of multiplication over addition).

Remark. In axiom 1, the additive neutral element 0 is always unique. The proof is left as an exercise for the reader.

Remark. In axiom 2, b is always uniquely determined by a. For this reason we usually denote b as $-a$.

Remark. It could be easily shown that $\forall a \in R, 0 \cdot a = 0$, and that $\forall a \in R, (-1) \cdot a = -a$.

Definition 1.1.2. A ring is **commutative** if $\forall a, b \in R, ab = ba$.

Example 1.1.1. Here are some examples of rings:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}/n\mathbb{Z}$ form rings under usual addition and multiplication. These rings are all commutative;

2. let R be a ring and $n \in \mathbb{Z}^+$. Then, the set of $n \times n$ matrices, $R^{n \times n}$, forms a (non-commutative) ring under elementwise addition and matrix multiplication;

3. let R be a ring. We define a **polynomial** over R as the symbolic expression
$$\sum_{i=0}^{n} a_i x^i$$
where $a_i \in R$ and $n \in \mathbb{Z}^+$. The set of polynomials over R, or $R[x]$, forms a ring. Addition is defined as elementwise addition, and multiplication follows the usual rules (i.e., as in the multiplication of real polynomials);

4. let X be a set and R a ring, then
$$R^X = \{f \mid f : X \to R\}$$
is also a ring, where addition and multiplication are defined pointwise. R^X and $R[x]$ are commutative if and only if R is commutative.

Definition 1.1.3. Let R be a ring and $S \subseteq R$. S is a **subring** of R if:

1. $1_R \in S$
2. $\forall a, b \in S$, $a + b \in S$
3. $\forall a \in S$, $-a \in S$
4. $\forall a, b \in S$, $ab \in S$

Definition 1.1.4. Let R be a ring. The **group of units** in R is the set $R^\times = \{a \in R \mid \exists b \in R, ab = 1\}$. It is easy to verify that it forms a group under multiplication in R.

Definition 1.1.5. A ring is a **division ring** in case that $R^\times = R \backslash \{0\}$. A **field** is a division ring that is commutative.

1.2 Modules over a ring

Now that we have reviewed the basics of ring theory, we can give the definition of a module.

Definition 1.2.1 (module)**.** Let R be a ring. A (left) R-**module** is a pair $(M, \cdot)$ where $M = (M, +)$ is an abelian group and $\cdot$ is an operation $R \times M \to M$, $(a, m) \mapsto am$, satisfying the following axioms:

1. $\forall a \in R$, $\forall m, n \in M$, $a(m +_M n) = am + an$
2. $\forall a, b \in R$, $\forall m \in M$, $(a +_R b)m = am + bm$
3. $\forall a, b \in R$, $\forall m \in M$, $(ab)m = a(bm)$
4. $\forall m \in M$, $1_R m = m$

Remark. These axioms are exactly the same axioms as that of an vector space, except that in the definition of a vector space the ring R is further limited to a field.

Alternatively, we can give a definition of modules in term of morphism groups:

Remark. Let M be an R-module. Every $a \in R$ determines a map $\rho_a : M \to M$, $x \mapsto ax$. It is easy to verify that ρ_a is a group morphism, if $(M, +)$ is viewed as an abelian group.

Then, we can define a map $\rho : R \to \mathrm{End}(M, +)$, $a \mapsto \rho_a$, where $\mathrm{End}(M, +)$ is the set of group (endo)morphisms $(M, +) \to (M, +)$.

Next, we shall verify that $\mathrm{End}(M, +)$ is a ring. First, we note that it is an abelian group under pointwise addition of morphisms.

We then define multiplication as $\phi \cdot \psi = \phi \circ \psi$ (i.e., function composition). It is easy to see that under pointwise addition as addition, and composition as multiplication, $\mathrm{End}(M, +)$ is a ring, called the **endomorphism ring** of $(M, +)$. The proof is left as an exercise for the reader.

Therefore, axiom 2 tells us that $\rho_{a+b}(m) = (a + b)m = am + bm = \rho_a(m) + \rho_b(m)$, i.e., $\rho_{a+b} = \rho_a + \rho_b$, i.e. ρ is a group morphism. Furthermore, axioms 3 and 4 tell us that ρ is a ring morphism; the proof is left as an exercise for the reader.

As such, we can equivalently define a R-module M to be an abelian group equipped with a ring morphism $\rho : R \to \mathrm{End}(M, +)$.

Example 1.2.1. Here are some examples of modules:

1. if K is a field, then a K-module is exactly a K vector space;

2. a $\mathbb{Z}$-module is exactly an abelian group. The proof is omitted here but is not difficult, and can be an easy exercise;

3. let R be a ring. A natural example of a module would be the vectors R^n, which form an R-module;

4. a $K[x]$-module is a K-vector space V equipped with a linear map $V \to V$.

Definition 1.2.2. Let M be an R-module and A a subgroup of A. We call A a **submodule** of M if $\forall r \in R$, $\forall x \in A$, $rx \in A$.

The definition we have just given is for a **left** module. Dually, we can define a **right** module, where scalar multiplication operates on the right:

Definition 1.2.3 (right module)**.** Let R be a ring. A right R-module is a pair $(M, \cdot)$ where $M = (M, +)$ is an abelian group and $\cdot$ is an operation $M \times R \to M$, $(x, r) \mapsto xr$, satisfying the following axioms:

1. $\forall m, n \in M$, $\forall a \in R$, $(m + n)a = ma + na$

2. $\forall m \in M$, $\forall a, b \in R$, $m(a + b) = ma + mb$

3. $\forall m \in M$, $\forall a, b \in R$, $m(ab) = (ma)b$

4. $\forall m \in M$, $m \cdot 1_R = m$

However, every left module is equivalent to a right module, and vice versa. To show this, we need to introduce the concept of an **opposite ring**:

Definition 1.2.4. Let R be a ring. The **opposite ring** of R, $R^{\text{op}} = (R, *)$, where R^{op} is the same abelian group as R, but with the multiplication operation $*$ defined as $a * b = b_R a_R$.

Then, any right R-module is equivalently a left R^{op}-module under the scalr multiplication $R^{\text{op}} \times M \to M$, $(r, x) \mapsto r * x = xr$.

Furthermore, if R is a commutative ring, then $R^{\text{op}} = R$, so in this case the left and right R-modules are exactly the same.

1.3 Constructions on modules

There are a number of basic constructions on R-modules that yield new R-modules.

Theorem 1.3.1. *The intersection of an arbitrary number of submodules of M is again a submodule of M.*

Proof. Left as an exercise for the reader. Use the definition of a submodule. □

The next construction on submodules is the *sum* construction. We give the definition as following:

Definition 1.3.1. (sum of submodules) Let M be an R-module and $\{A_i\}_{i\in I}$ be an I-indexed family of submodules of M. The **sum** of the modules A_1, A_2, ..., is the set

$$\{\sum_{i\in I} a_i = a_1 + a_2 + ... \mid a_i \in A_i\}$$

Theorem 1.3.2. *Let M be an R-module. The sum of a family of submodules of M is again a submodule of M.*

Proof. Left as an exercise for the reader. Use the definition of a submodule. □

Submodules can also be generated by subsets of a module, similar to how subsets of a linear space can span a linear subspace.

Definition 1.3.2. Let M be an R-module and $X \subset M$. Then the **submodule generated by** X, or $\langle X\rangle$, is the set:

$$\{\sum_{i\in I} r_i x_i \mid r_i = 0 \text{ for almost all } i \in I\}$$

where I is an indexing set, and r_i and x_i include all elements in R and X, respectively.

It is easy to show that $\langle X\rangle$ is indeed a submodule of M.

Remark. Here, "almost all" means "except for finitely many". Apparently, the sum needs to be finite for this to make sense, hence the "almost all" condition. Furthermore, when R and X are finite, this condition vanishes.

Consider an R-module M and a submodule N. Consider M and N as abelian groups; we can form the quotient (or factor) group M/N. From group theory, we know that the elements of M/N are the equivalence classes $[x]$, where $x \in M$. We claim that M/N is also an R-module.

Theorem 1.3.3. *Let M be an R-module and $N \subset M$ a submodule of M. Then the quotient group M/N is also an R module, with scalar defined as: $\forall[x] \in M/N$, $\forall r \in R$, $r[x] = [rx]$. Therefore, we call M/N the* ***quotient module*** *of M over N.*

Proof. It is easy to verify that this construction satisfies all the module axioms using the properties of quotient groups. □

Finally, we define three more constructions on modules, which are direct analogies from constructions on vector spaces in linear algebra:

Definition 1.3.3. Let $(M_i)_{i\in I}$ be an indexed family of R-modules. The **direct product** of $(M_i)_{i\in I}$ is defined as:

$$\prod_{i\in I} M_i = \{(x_i)_{i\in I} \mid x_i \in M_i\}$$

It is trivial to verify that this is an R-module, with both addition and scalar multiplication defined elementwise.

Example 1.3.1. If I is a countable set (say $I = \{1, 2, ..., n\}$), then

$$\prod_{i\in I} M_i = M_1 \times M_2 \times ...M_n$$

is simply the Cartesian product. This is apparently an R-module, with the scalar product defined as

$$r(x_1, x_2, ..., x_n) = (rx_1, rx_2, ..., rx_n)$$

Therefore, the direct product is a generalization of the usual Cartesian product.

Definition 1.3.4. Let $(M_i)_{i\in I}$ be an indexed family of R-modules. The **coproduct** of $(M_i)_{i\in I}$ is defined as:

$$\coprod_{i\in I} M_i = \{(x_i)_{i\in I} \in \prod_{i\in I} M_i \mid x_i \text{ for almost all } i \in I\}$$

That is, a coproduct is a product in which only finitely many elements are nonzero.

Remark. $\coprod_{i\in I} M_i \subseteq \prod_{i\in I}$ and is a submodule of the latter.

Remark. In the finite case, the direct product and the coproduct coincide. That is, $\coprod_{i\in I} M_i = \prod_{i\in I}$.

The last construction we introduce is the *direct sum*, which generates the relationship between a vector space and its basis in linear algebra.

Definition 1.3.5. Let M be an R-module. M is a **direct sum** of the submodules $L_1, ..., L_n \subseteq M$ if $\forall m \in M$, $\exists! x_i \in L_i$ (i.e., exists one and only one $x_i \in L_i$), where $i \in \{1, ..., n\}$, such that

$$m = x_1 + ... + x_n$$

In this case, we write that:

$$M = L_1 \oplus ... \oplus L_n$$

Remark. If M is the direct sum of a family of submodules, then it is also the sum of this family of submodules.

Remark. If $M = L_1 \oplus L_2$, then $M = L_1 + L_2$ and $L_1 \cap L_2 = \{0\}$.

Remark. Let $M_1, ..., M_n$ be R-modules, then

$$\widetilde{M_i} = 0 \times ... \times M_i \times 0 \times ... \times 0 \subseteq \prod_{i \in I} M_i$$

is an R-module. Moreover,

$$M_1 \times ... \times M_n = \widetilde{M_1} \oplus ... \oplus \widetilde{M_n}$$

1.4 Ideals

Definition 1.4.1. Let R be a ring:

1. a **left ideal** in R is a submodule of R when viewed as a left module over itself, i.e. $I \subseteq {}_R R$;
2. a **right ideal** in R is a submodule of R when viewed as a right module over itself, i.e. $I \subseteq R_R$;
3. a **(two-sided) ideal** in R is both a left ideal and a right ideal in R. In this case, we write $I \lhd R$.

Remark. If we plug in the definition of a submodule, then we obtain the more familiar definition of a submodule. If R is a ring, then $I \subseteq R$ is a left ideal in R if

1. $0 \in I$;
2. $\forall x, y \in I$, $x + y \in I$;

3. $\forall r \in R, \forall x \in I, rx \in I$.

We could do the same to obtain the more familiar definition of a right ideal.

Example 1.4.1. Let R be a ring and $R^{2\times 2}$ the ring of all 2×2 matrices in R. The set

$$\begin{pmatrix} R & 0 \\ R & 0 \end{pmatrix} = \left\{ \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \middle| r, s \in R \right\} \subset R^{2\times 2}$$

is a left ideal in R, but *not* a right ideal in R, because:

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \notin \begin{pmatrix} R & 0 \\ R & 0 \end{pmatrix}$$

Similarly,

$$\begin{pmatrix} R & R \\ 0 & 0 \end{pmatrix}$$

is a right, but not left, ideal in R.

Definition 1.4.2. Let R be a commutative ring and let $a \in R$ an element of R.

$$(a) = Ra = \{ra \mid r \in R\} \lhd R$$

the **principal ideal** determined by a.

Remark. Apparently, this is a two-sided ideal in R. The proof is trivial.

Example 1.4.2. Let K be a field and $a \in K$. Then

$$\{f(x) \in K[x] \mid f(a) = 0\}$$

is a principal ideal in $K[x]$, generated by $x - a$.

Lemma 1.4.1. *Let R be a ring and $I \lhd R$, then the quotient group R/I is a left R-module, with scalar multiplication defined as*

$$r \cdot [x] = [rx]$$

as well as a right R-module, with scalar multiplication defined as

$$[x] \cdot r = [xr]$$

as well as a ring, with multiplication defined as

$$[x][y] = [xy]$$

Remark. Therefore, we also call R/I a **quotient ring**.

Lemma 1.4.2. *A proper left or right ideal $I \subset R$ cannot contain an invertible element. In other words, if an ideal $I \subseteq R$ contains an invertible element, then $I = R$.*

Proof. Suppose $x \in I$ is invertible, and let a be any element in R, then by definition $(ax^{-1})x \in I$. However, $(ax^{-1})x = a(x^{-1}x) = a$, so $\forall a \in R$, $a \in I$, i.e., $I = R$. □

Corollary 1.4.3. *Any division ring D has only two ideals, the zero ideal $\{0\}$ and the trivial ideal which is D itself.*

Remark. The ideals in $\mathbb{Z}$ are exactly the subsets $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$.

1.5 Module morphisms

Like any other algebraic structure, modules come with morphisms between them, defined in a natural manner.

Definition 1.5.1. Let R be a ring and $M, N \in \text{Mod } R$. A map $f : M \to N$ is a **morphism of R-modules**, or an **R-linear map**, if $\forall x, y \in M$, $r \in R$,

1. $f(x + y) = f(x) + f(y)$, and
2. $f(rx) = r \cdot f(x)$.

Now, we shall introduce some terminology related to module morphisms.

Definition 1.5.2. Let $f : M \to N$ be a morphism of R-modules. We say that f is:

1. a **monomorphism**, in case that it is injective. Here, we also write that $f : M \rightarrowtail N$;
2. an **epimorphism**, in case that it is surjective. Here, we also write that $f : M \twoheadrightarrow N$;
3. an **isomorphism**, in case that it is bijective. Here, we also write that $f : M \xrightarrow{\sim} N$;
4. an **endomorphism**, in case that $M = N$;
5. an **automorphism**, in case that it is endo and iso.

Remark. Let $L \subset M$ be an inclusion of R-modules. Consider the *inclusion map* from L to M:

$$\iota : L \to M, \iota = x \mapsto x$$

Here, ι is clearly mono.

Meanwhile, the map

$$\pi : M \to M/L, \pi = x \mapsto [x]$$

is clearly an epi.

Remark. Every morphism $f : M \to N$ of R-modules determines:

1. a submodule Ker $f \subseteq M$;
2. a submodule Ker $f \subseteq N$.

The next result is similar to well-known, analogous theorems about ring, field and linear space morphisms:

Lemma 1.5.1. *Let $f : M \to N$ be a morphism of R-modules, then:*

1. *f is mono if and only if* Ker $f = 0$*;*
2. *f is an epi if and only if* Im $f = N$*;*
3. *f is iso if and only if $\exists g : M \to N$ a R-module morphism, such that $g \circ f = \mathbb{1}_M$ and $f \circ g = \mathbb{1}_N$. In other words, a morphism is iso in case that it is invertible.*