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

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

November 1, 2019

Contents

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. This is the definition of a ring with unity. Some authors do not require that the multiplicative identity exists, but hereafter whenever we refer to a "ring", we always mean a ring with unity.

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 1.1.3. 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 1.1.4. 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 1.1.5. 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 1.1.6. 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 $R \times M \to M$, $(a, m) \mapsto am$, often called *scalar multiplication*, 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 1.2.2. 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 1.2.3. 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 1.2.4 (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 1.2.5. 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 1.3.4. 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 1.3.5. 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 1.3.6. 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 1.4.2. 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 1.4.3. Let R be a commutative ring and let $a \in R$ an element of R. Then

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

is called the **principal ideal** determined by a.

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

Example 1.4.4. 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 $\operatorname{Ker} f \subseteq M$;
2. a submodule $\operatorname{Ker} f \subseteq N$.

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 $\operatorname{Ker} f = \{0\}$;*
2. *f is an epi if and only if $\operatorname{Im} f = N$;*
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.*

1.6 The isomorphism theorems

There are three isomorphism theorems on modules, analogous to the isomorphism theorems for groups and/or rings. Let M and N be R-modules; in this section, we will denote the inclusion map $M \hookrightarrow N$ as ι, and the coset map $M \to M/N$, $x \mapsto [x]$, as π, without further explanation.

Theorem 1.6.1 (the first isomorphism theorem)**.** *Every morphism $f : M \to N$ of R-modules determines an isomorphism $\overline{f} : M/\operatorname{Ker} f \to \operatorname{Im} f$, such that $f = \iota \circ \overline{f} \circ \pi$.*

Proof. We note that $\overline{f} = [x] \mapsto f(x)$, where $x \in M$. Thus, we need to show that:

1. $\overline{f}$ is well-defined (i.e., indeed a map);

2. $\overline{f}$ is a morphism;

3. $\overline{f}$ is bijective (i.e., iso);

4. that $f = \iota \circ \overline{f} \circ \pi$.

We prove these goals one by one.

1. For $\overline{f}$ to be well defined, we need to show that, if $[x] = [y]$ in $M/\operatorname{Ker} f$, then $f(x) = f(y)$.

   If $[x] = [y]$, then $x + \operatorname{Ker} f = y + \operatorname{Ker} f$, which means that $x - y \in \operatorname{Ker} f$, by the definition of a coset. Moreover, as $f(x - y) = f(x) - f(y) = 0$, we know that $f(x) = f(y)$.

2. It is trivial to show that $\overline{f}$ is a morphism of R-modules. The interested reader may verify it using definitions.

3. We would like to show that $\overline{f}$ is both injective and surjective. First we shall prove the injectivity of $\overline{f}$ using lemma 1.5.1.

   Suppose $\overline{f}([x]) = 0$, then we have $f(x) = 0$, that is $x \in \operatorname{Ker} f$. In other words, $[x] = [0]$. Therefore, $\operatorname{Ker} \overline{f} = \{[0]\}$, so by lemma 1.5.1 $\overline{f}$ is injective.

   The surjectivity of $\overline{f}$ is easy to prove. By definition, for every $y \in \operatorname{Im} f$, $\exists x \in M$ such that $f(x) = y$. That is, there is a coset $[x]$ such that $\overline{f}([x]) = y$.

4. Having proven the first three items, this is easy to verify. For each $x \in M$,

   $$\iota \circ \overline{f} \circ \pi(x) = \iota(\overline{f}(\pi(x))) = \iota(\overline{f}([x])) = \iota(f(x)) = f(x)$$

   thus $\iota \circ \overline{f} \circ \pi = f$.

□

The next two isomorphism theorems will be given without proof.

Theorem 1.6.2 (the second isomorphism theorem)**.** *Let N be an R-module and $L, M \subseteq N$ submodules of N. Then the map*

$$\begin{aligned} L/(L \cap M) &\to (L + M)/M \\ [x] &\mapsto [x] \end{aligned}$$

is an isomorphism.

Theorem 1.6.3 (the third isomorphism theorem)**.** *Let $L \subseteq M \subseteq N$ be an inclusion of R-modules. Then M/L is a submodule of N/L, and furthermore the map*

$$(N/L)/(M/L) \to N/M$$
$$(x + L) + (M/L) \mapsto x + M$$

is an isomorphism.

Now, we shall revisit the familiar concept of a ring homomorphism.

Definition 1.6.1 (homomorphism of rings)**.** Let R, S be rings. A ring homomorphism is a map $f : R \to S$, such that $\forall a, b \in R$:

1. $f(a + b) = f(a) + f(b)$;
2. $f(ab) = f(a)f(b)$;
3. $f(1_R) = 1_S$.

Remark. For every ring morphism $f : R \to S$, $\operatorname{Ker} f \lhd R$ is a (two-sided) ideal, and $\operatorname{Im} f \subseteq S$ is a subring.

Since every ring is a module over itself, all three isomorphism theorems apply to rings too, with "submodule" replaced by "ideal". The proof is of course trivial, so we will not repeat them here.

Example 1.6.2. For any ring R, there exists a unique isomorphism

$$\chi : \mathbb{Z} \to R, \chi = n \mapsto n1_R = \overbrace{1_R + ... + 1_R}^{n \text{ times}}.$$

Since $\operatorname{Ker} \chi \lhd \mathbb{Z}$, so $\operatorname{Ker} \chi = m\mathbb{Z}$ for some $m \in \mathbb{N}$. Moreover, by the the first isomorphism theorem we know that χ determines an isomorphism $\overline{\chi} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}1_R$. This (uniquely determined) $m \in \mathbb{N}$ is called the **characteristic** of R, or $\operatorname{char} R$.

Corollary 1.6.4. *The characteristic of a field is either 0 or a prime number.*

Proof. Left as an exercise for the reader. □

1.7 Finitely generated modules and finite dimensional algebras

Definition 1.7.1. Let M be an R-module. We say that M is **finitely generated** if $\exists x_1, ..., x_n \in M$, such that $M = \langle \{x_1, ..., x_n\} \rangle$. Often, we will omit the curly braces and just write that $M = \langle x_1, ..., x_n \rangle$.

We denote the collection (or category) of finitely generated R-modules as mod R.

Example 1.7.2. Let $R = K$ be a field, then a R-module is a vector space V over K. V is finitely generated if and only if $\exists x_1, ..., x_n \in V$ such that $V = \text{span}_K\{x_1, ..., x_n\}$. From linear algebra, we know that we can always reduce a spanning set to a basis, so V must have a finite basis $u = (u_1, ..., u_l)$ where $l \leq n$.

Therefore, a K-vector space is a finite generated K-module if and only if it is a finite dimensional vector space.

Example 1.7.3. Let R be a commutative ring, and let $\Lambda = R[x]$. Then

1. $\langle 1_\Lambda \rangle = \Lambda$ is a finitely generated Λ-module;
2. let $a \in R$, $M = R$, and define scalar multiplication as

$$\begin{aligned} \Lambda \times M &\to M \\ (f(x), M) &\mapsto f(x) \cdot m := f(a) \cdot m. \end{aligned}$$

Then, $M = R$ is a Λ-module.

Proposition 1.7.1. *Let M be an R-module. M is finitely generated if and only if there exists an $n \in \mathbb{Z}_+$, such that there exists an epimorphism ${}_RR \times ... \times {}_RR \twoheadrightarrow M$.*

Definition 1.7.4. If $M = \langle x_1, ..., x_n \rangle$, we define the map $e_i : {}_RR \times ... \times {}_RR \to M$ to be

$$e_i = (0, ..., 1, ..., 0) \mapsto x_i$$

where on the left-hand side the i-th element is 1.

Definition 1.7.5. Let K be a field. A K-algebra is a ring Λ with a map $K \times \Lambda \to \Lambda$, $(c, \lambda) \mapsto c\lambda$ making Λ a K-vector space, such that $\forall x, y \in \Lambda$, $\forall c \in K$, $c(xy) = (cx)y = x(cy)$.

In particular, $\cdot$ in Λ is bilinear. That is, $\forall a \in \Lambda$,

$$L_a : \Lambda \to \Lambda, L_a = x \mapsto ax$$

and

$$R_a : \Lambda \to \Lambda, R_a = x \mapsto xa$$

are both K-linear maps.

We define the dimension of the K-algebra Λ, or $\dim_K \Lambda$, as the dimension of Λ as a vector space. We say that Λ is a finite-dimensional K-algebra if it is a finite-dimensional vector space.

Remark. Any K-algebra is a ring, and the map $K \to \Lambda$, $a \mapsto a \cdot 1_\Lambda$ is a ring homomorphism.

Remark. Let R be a ring, K a field, and $\varepsilon : K \to R$ a ring homomorphism. Then R becomes a K-algebra, with $\cdot$ defined as

$$\begin{aligned} K \times R &\to R \\ (c, r) &\mapsto \varepsilon(c) \cdot r = cr. \end{aligned}$$

Remark. Let Λ be a K-algebra and M a Λ-module, then M is also a K-module, via

$$\begin{aligned} K \times M &\to M \\ (c, m) &\mapsto (c \cdot 1_R) \cdot m = cm. \end{aligned}$$

Remark. If Λ is a finite dimensional K-algebra, then

$$\operatorname{mod} \Lambda = \{M \in \operatorname{Mod} \Lambda \mid \dim_K M < \infty\}$$

i.e., the finitely generated Λ-modules are exactly the modules that are also finite dimensional K-algebras.

1.8 Chain conditions

In this section we define the *chain conditions* on modules, concerning chains of module inclusions.

Definition 1.8.1. An R-module M is **Noetherian** if the **ascending chain condition**, explained below, holds.

Let $M_0 \subseteq M_1 \subseteq M_2 \subseteq ...$ be a chain of inclusion of submodules of M, i.e., M_0 is a submodule of M_1, M_1 a submodule of M_2, and so on. We say that R satisfies the ascending chain condition if for any such chain, $\exists N \in \mathbb{N}$, $\forall n \geq N$, we have $M_n = M_N$. That is, all ascending chains in M are well-founded.

Noetherian modules are named after Emmy Noether, who first studied the ascending chain condition in detail.

Dually, there are also descending chains and a similar condition.

Definition 1.8.2. An R-module M is **Artinian**, named after Emil Artin, if the **descending chain condition** holds.

Let $M_0 \supseteq M_1 \supseteq M_2 \supseteq ...$ be a chain of reverse inclusion of submodules of M, i.e., M_1 is a submodule of M_0, M_2 a submodule of M_1, and so on. We say that R satisfies the descending chain condition if for any such chain, $\exists N \in \mathbb{N}$, $\forall n \geq N$, we have $M_n = M_N$. That is, all descending chains in M are well-founded.

Since rings are modules over themselves, we can also define the chain condition for rings.

Definition 1.8.3. A ring is left (or right) Noetherian/Artinian if ${}_RR$ (or R_R) is Noetherian/Artinian.

Definition 1.8.4. A ring is Noetherian/Artinian if it is both left and right Noetherian/Artinian.

Remark. A finite module is apparently both Noetherian and Artinian.

Proposition 1.8.1. *If Λ is a finite dimensional K-algbera, then every finitely-generated Λ-module is both Noetherian and Artinian.*

Proposition 1.8.2. *$\mathbb{Z}$ is a Noetherian ring.*

Proof. Let us write $(n) = n\mathbb{Z}$, and let $(n_0) \subseteq (n_1) \subseteq (n_2) \subseteq ...$ be an ascending chain in $\mathbb{Z}$.

Let $i < j \in \mathbb{N}$, and we have $(n_i) \subseteq (n_j) = \{mn_j \mid m \in \mathbb{Z}\}$. Therefore, $n_i = mn_j$ for some $m \in \mathbb{Z}$, i.e. $n_j \mid n_i$.

Since $n_j < n_i$, we know that $\exists N \in \mathbb{N}$, such that $\forall j \geq N$, $n_j = n_N$ (because every integer has a unique and finite prime factorization). □

Remark. However, $\mathbb{Z}$ is not Artinian. For example, the chain

$$\mathbb{Z}/2\mathbb{Z} \supseteq \mathbb{Z}/4\mathbb{Z} \supseteq \mathbb{Z}/8\mathbb{Z} \supseteq ...$$

is not well-founded.

Example 1.8.5. Let $M = \mathbb{Q}/\mathbb{Z}$ be a $\mathbb{Z}$-module, and p a prime number. Then

$$M_p = \left\{ \left[\frac{m}{p^a}\right] \in M \mid m \in \mathbb{Z}, a \in \mathbb{N} \right\}$$

is Artinian but not Noetherian.

Proof. Left as an exercise for the reader. □

The following lemma states some basic properties of Noetherian modules.

Lemma 1.8.3. *Let R be a ring and M an R-module, then the following are equivalent:*

(1) M is Noetherian;

(2) every submodule of M is finitely generated;

(3) for every submodule $L \subseteq M$, L and M/L are both Noetherian.

Proof. This is a chain of implications, so we prove that (1) implies (2), (2) implies (3), and (3) implies (1). This will show that (1), (2) and (3) imply each other.

- (1) $\implies$ (2):

  We use proof by contradiction here. Assume that there is a submodule $\exists L \subseteq M$ which is not finitely generated. Then, for any finite family of elements in L, say they are $x_1, ..., x_n$, we know that $\langle x_1, ..., x_n \rangle \subset L$.

  By assumption, there is an $x_{n+1} \in L$, such that $x_{n+1} \notin \langle x_1, ..., x_n \rangle$. Thus, $\{0\} \subset \langle x_1 \rangle \subset \langle x_1, x_2 \rangle \langle . \rangle ..$ is a non-well-founded ascending chain, therefore LM is not Noetherian. We have a contradiction. As such, it must be the case that all submodules of M are finitely generated.

- (2) $\implies$ (3):

  Let $L \subseteq M$ be any submodule of M. We want to show that both L and M/L are Noetherian.

  (a) Show that L is Noetherian.
  Let $L_0 \subseteq L_1 \subseteq L2 \subseteq ...$ be any ascending chain in L. We observe that
  $$\widetilde{L} = \bigcup_{i \in \mathbb{N}} L_i \subseteq L$$
  is a submodule of L and thus M. Therefore, $\widetilde{L}$ is finitely generated, and as such there are $x_1, ..., x_n \in \widetilde{L}$ such that $\widetilde{L} = \langle x_1, ..., x_n \rangle$.
  Let $i_1, ..., i_n \in \{1, ..., n\}$ (which are not necessarily distinct). Suppose that $x_1 \in L_{i_1}, x_2 \in L_{i_2}, ..., x_n \in L_{i_n}$, and take $m = \max\{i_1, ..., i_n\}$. Then, $x_1, ..., x_n \in L_m$ (since $\forall i \in \{i_1, ..., i_n\}$, $L_i \subseteq L_m$).
  Therefore, $\widetilde{L} = \langle x_1, ..., x_n \rangle \subseteq L_m \subseteq \widetilde{L}$, and as such $L_m = \widetilde{L}$. That is to say, for each and every $r > m$, $L_r = L_m$. Thus L is Noetherian.

(b) Show that M/L is Noetherian.

Let $N_0 \subseteq N_1 \subseteq N_2 \subseteq ...$ be an ascending chain in M/L. Observe that M is Noetherian (as M is a submodule of itself). Let us consider the canonical quotient projection $\pi : M \to M/L$.

For each chain $N_0 \subseteq N_1 \subseteq N_2 \subseteq ...$ in M/L, there is a corresponding chain $\pi^{-1}(N_0) \subseteq \pi^{-1}(N_1) \subseteq \pi^{-1}(N_2) \subseteq ...$ in M. Since the later is well-founded, the earlier must also be well-founded. Therefore, M/L is Noetherian.

- (3) $\implies$ (1):

  This is trivial: simply take $L = M$.

□

A similar lemma holds for Artinian modules, however (2) no longer holds in the Artinian case. The proof is also rather similar to the proof we have just presented.

Lemma 1.8.4. *Let M be an R-module. M is Artinian if and only if for every submodule $L \subseteq M$, both L and M/L are Artinian.*

Proof. Left as an exercise for the reader. □

Chain conditions on modules imply important facts about endomorphisms on them.

Lemma 1.8.5. *Let M be an R-module.*

(1) If M is Noetherian, then any epimorphism $f : M \to M$ is an iso.

(2) If M is Artinian, then any monomorphism $f : M \to M$ is an iso.

Proof. There are two separate cases we will need to consider here.

(1) The Notherian case.

If M is Noetherian and $f : M \to M$ is epic (i.e., surjective), in order to show that f is iso, we simply need to show that f is injective. By lemma 1.5.1, we can prove this by showing that $\operatorname{Ker} f = \{0\}$.

Observe that $\operatorname{Ker} f \subseteq \operatorname{Ker} f^2 \subseteq \operatorname{Ker} f^3 \subseteq ...$ forms an ascending chain in M. Since M is Noetherian, we know that there is an $m \in \mathbb{N}$ such that $\operatorname{Ker} f^m = \operatorname{Ker} f^{m+1}$.

If f is epic, then f^m is also epic (since the composition of surjections is itself a surjection). Therefore, for every $x \in \operatorname{Ker} f$, by the definition of surjectivity there is an element $y \in M$ such that $x = f^m(y)$. Then,

$$0 = f(x) = f(f^m(y)) = f^{m+1}(y)$$

which is to say that $y \in \operatorname{Ker} f^{m+1} = \operatorname{Ker} f^m$. Since $f^m(y) = 0$, we know that $x = 0$, that is $\operatorname{Ker} f = \{0\}$.

(2) The Artinian case. The proof for this case is left as an exercise for the reader.

□

1.9 Composition series and finite length modules

First, we begin with some definitions necessary to build up the theory in this section.

Definition 1.9.1. An R-module S is **simple** if $S \neq \{0\}$ and $\forall x \in S \backslash \{0\}, \langle x \rangle = S$.

Remark. If S is simple, then it has only two submodules (the trivial submodule $\{0\}$ and S itself).

Definition 1.9.2. Let M be an R-module and L a submodule of M such that $L \neq M$. We say that L is **maximal** in M if for all submodules X of M, if $L \subset X$, then $X = M$.

Remark. If $L \subset M$ is maximal, then there are only two submodules that contain L (M and L).

Lemma 1.9.1. *Let M be an R-module and $L \subset M$ a submodule. L is maximal if and only if M/L is simple.*

Now we can define composition series of modules.

Definition 1.9.3. Let M be an R-module. A **composition series** of M is a finite chain $(F) : \{0\} = M_0 \subseteq M_1 \subseteq ... \subseteq M_n = M$, such that $\forall i \in \{1, ..., n\}$, M_i/M_{i-1} is simple. We say that M is of **finite length** if it has a composition series.

The most important theorem in the theory of composition modules is the Jordan-Hölder theorem. However, it takes some machinery to develop the statement and the proof of the theorem. In order to prove the Jordan-Hölder theorem, we need to introduce some additional concepts.

Definition 1.9.4. A **generalized composition series** of M is a finite chain $(F) : \{0\} = M_0 \subseteq M_1 \subseteq ... \subseteq M_n = M$ such that $\forall i \in \{1, ..., n\}$, M_i/M_{i-1} is either simple or $\{0\}$.

Let S be a simple group and F a generalized composition series. We define the **multiplicity** of M with respect to the generalized composition series F and the group S as

$$m_S^F(M) = \big|\big\{i \leq n \mid M_i/M_{i-1} \cong S\big\}\big|$$

and the **length** of M with respect to F as

$$l^F(M) = \big|\big\{i \leq n \mid M_i/M_{i-1} \neq \{0\}\big\}\big|.$$

Remark.

$$\sum_S m_S^F(M) = l^F(M)$$

The multiplicity and length of a module is actually independent of the generalized composition series chosen. This is essentially the Jordan-Hölder theorem, but we need a few more lemmas to prove it.

Lemma 1.9.2. *Let M be an R-module and $X, Y \subseteq M$ be its submodules. If Y is maximal in M, then either:*

(1) $X/(X \cap Y) \cong M/Y$, and $\pi(Y) = M/X$, or:

(2) $X \cap Y = X$, that is $X \subseteq Y$, and $(M/X)\big/\pi(Y) \cong M/Y$

where $\pi : M \to M/X$ is the canonical quotient map.

Proof. Observe that $Y \subseteq X + Y \subseteq M$ is an inclusion of submodules. Since Y is maximal, we know that either (i) $X + Y = M$, or (ii) $X + Y = Y$.

(i) $M = X + Y$.

In this case, by the second isomorphism theorem, we know that

$$X\big/(X \cap Y) \cong M/Y$$

$$M/X \cong Y\big/(X \cap Y) \cong \pi(Y).$$

since $X \cap Y = \operatorname{Ker} \pi|_Y$.

(ii) $Y = X + Y$, i.e., $X \subseteq Y$ and $X \cap Y = X$.

In this case, by the third isomorphism theorem, we know that

$$\frac{M/X}{\pi(Y)} = \frac{M/X}{Y/X} \cong M/Y.$$

□

This lemma implies some important results about composition series, although the following lemma might not strike one as related to the lemma we have just proven.

Lemma 1.9.3. *Let M be an R-module and $L \subseteq M$ a submodule.*

(1) Let $(F_L) : 0 = L_0 \subseteq L_1 \subseteq ... \subseteq L_l = L$ and $(F_N) : 0 = N_0 \subseteq N_1 \subseteq ... \subseteq N_n = M/L$ be composition series for L and M/L, respectively. Then

$$(F) : 0 = L_0 \subseteq L_1 \subseteq ... \subseteq L_l = \pi^{-1}(N_0) \subseteq \pi^{-1}(N_1) \subseteq ... \subseteq \pi^{-1}(N_n) = M$$

is a composition series for M.

(2) Let $(F) : 0 = M_0 \subseteq M_1 \subseteq ... \subseteq M_m = M$ be a composition series. Then

$$(F_L) : 0 = L \cap M_0 \subseteq L \cap M_1 \subseteq ... \subseteq L \cap M_m = L$$

and

$$(F_N) : 0 = \pi(M_0) \subseteq \pi(M_1) \subseteq ... \subseteq \pi(M_m) = M/L$$

are generalized composition series, and $\forall i \in \{1, ..., m\}$, either:

$$\frac{L \cap M_i}{L \cap M_{i-1}} \cong \frac{M_i}{M_{i-1}},$$

where

$$\pi(M_i)/\pi(M_{i-1}) = \{0\},$$

or:

$$\frac{L \cap M_i}{L \cap M_{i-1}} = 0,$$

where

$$\frac{\pi(M_i)}{\pi(M_{i-1})} \cong \frac{M_i}{M_{i-1}}.$$

Here, π is the canonical quotient map $\pi : M \to M/L$.

In particular, in both cases, for any simple group S, we have:

$$m_S^F(M) = m_S^{F_L}(L) + m_S^{F_N}(M/L)$$

and

$$l^F(M) = l^{F_L}(L) + l^{F_N}(M/L)$$

Proof. We prove the two parts of this lemma separately.

(1) For every $i \in \{1, ..., m\}$, we have $L \subseteq \pi^{-1}(N_{i-1}) \subseteq \pi^{-1}(N_i)$. By the the third isomorphism theorem,

$$\frac{\pi^{-1}(N_i)}{\pi^{-1}(N_{i-1})} \cong \frac{\pi^{-1}(N_i)/L}{\pi^{-1}(N_{i-1})/L} = \frac{N_i}{N_{i-1}}$$

which is a simple group by assumption. Therefore, F is a composition series.

(2) Observe that for every $i \in \{1, ..., m\}$, we have $L \cap M_i = \operatorname{Ker} \pi|_{M_i}$. Note also that M_{i-1} is maximal in M_i. By lemma 1.9.2, we know that either:

$$\frac{L \cap M_i}{(L \cap M_i) \cap M_{i-1}} = \frac{L \cap M_i}{L \cap M_{i-1}} \cong \frac{M_i}{M_{i-1}}$$

where $\pi(M_{i-1}) = M_i/(L \cap M_i) = \pi(M_i)$, or: $L \cap M_i = L \cap M_{i-1}$, i.e.

$$\frac{L \cap M_i}{L \cap M_{i-1}} = \{0\}$$

and

$$\frac{\pi(M_i)}{\pi(M_{i-1})} \cong \frac{M_i}{M_{i-1}}.$$

The results about multiplicity and length follow naturally. □