

# MATH 593 - Module

ARessegetes Stery

October 19, 2023

## Contents

<b>1</b>	<b>Module</b>	<b>2</b>
<b>2</b>	<b>Morphism of <math>R</math>-Modules</b>	<b>3</b>
<b>3</b>	<b>Construction of Submodules</b>	<b>5</b>
<b>4</b>	<b>Free Modules</b>	<b>6</b>
<b>5</b>	<b>Finiteness Conditions on Modules</b>	<b>7</b>
<b>6</b>	<b>Modules of Finite Length</b>	<b>9</b>
<b>7</b>	<b>Digression on Commutative Algebra</b>	<b>12</b>
<b>8</b>	<b>Artinian/Noetherian Commutative Ring</b>	<b>13</b>
8.1	Artinian implies Noetherian: Module and Ring . . . . .	13
<b>9</b>	<b>Finitely Generated Modules Over PIDs</b>	<b>13</b>
9.1	Torsion and Module Structure . . . . .	13
<b>10</b>	<b>Linear Algebra on Modules</b>	<b>13</b>

# 1 Module

**Definition 1.1** ( $R$ -Module). An (left)  **$R$ -Module**  $M$  is a set with two operations, often denoted as  $(M, +, \times)$ :

- **Addition**  $(+): M \times M \rightarrow M$ , s.t.  $(M, +)$  is an abelian group.
- **Multiplication**  $(\times): R \times M \rightarrow M$ , s.t. it has the following properties:
  - Identity. For all  $x \in M$ , there exists  $1 \in R$  s.t.  $1 \cdot x = x$ .
  - Associativity. For all  $a, b \in R, x \in M$ ,  $a(bx) = (ab)x$ .
  - Distributivity in  $R$ . For all  $a_1, a_2 \in R, (a_1 + a_2)x = a_1x + a_2x$ .
  - Distributivity in  $M$ . For all  $a \in R, x_1, x_2 \in M$ ,  $a(x_1 + x_2) = ax_1 + ax_2$ .

Right modules are defined with the same structure, but with  $a \times b = b \cdot a$  for  $a \in R, b \in M$ , where  $\times$  is the multiplication in  $M$ , and  $\cdot$  the multiplication in  $R$ .

**Definition 1.2** (Submodule). Let  $(M, +, \times)$  be an  $R$ -module.  $N \subseteq M$  is a  **$R$ -submodule** of  $M$  if  $(N, +)$  is a subgroup of  $M$ ; and for all  $n \in N, r \in R, n \times r \in N$ .

**Remark 1.1.** Notice that  $R$  itself gives an  $R$ -module, just as  $\mathbb{K}$  gives a  $\mathbb{K}$ -vector space. Therefore  $\langle S, \varphi \rangle$  an  $R$ -algebra induces a two-sided  $R$ -module structure. Check that this is indeed the case:

- **Addition**. Adopt the addition in  $S$  as a ring.
- **Identity**: Since ring homomorphisms map identity to identity,  $\varphi(1_R) = 1_S$ , implying that  $1_R$  is the identity for scalar multiplication.
- **Associativity**. Results from the fact that multiplication in  $S$  is associative.
- **Distributivity in  $R$  and  $M$** . Follows from the fact that  $\varphi$  is a ring homomorphism.

In this sense, module generalizes the algebra structure. Generally one cannot “revert” the structure of a module back to an algebra. Specifically, suppose that  $R$  is not commutative, then  $R$  is not an  $R$ -algebra.

**Remark 1.2.** (Left) ideals of  $R$  are submodules of  $R$  taken as an  $R$ -submodule.

**Remark 1.3.** Let  $M$  be an abelian group. Making  $M$  into a (left)  $R$ -module is equivalent to specifying a ring homomorphism  $\varphi: R \rightarrow \text{End}(M)$ , where  $\text{End}(\cdot)$  denotes the ring of endomorphisms on the specific structure.

It is worth noticing how the ring of endomorphism structure is defined. Specifically, the multiplication is the composition of endomorphisms on  $M$ . This can be viewed in two aspects:

- The associativity for  $R$ -modules is essentially stating that multiplication, i.e. elements of  $R$  “acting” on those in  $M$  is associative. Applying one action after another is the same as applying the composition of action.
- Consider the definition of function as a set of pairs. Then

$$R \times M \rightarrow M \cong (R \rightarrow M) \rightarrow M \cong R \rightarrow (M \rightarrow M)$$

as the application of functions is associative.

In particular, in the consideration of  $\mathbb{Z}$ -modules, the map  $\varphi_{\mathbb{Z}} : \mathbb{Z} \rightarrow \text{End}(M)$  is determined uniquely by the requirement that  $1 \mapsto 1_M = \text{Id}_M$ . Since addition and multiplication should be preserved,  $n \mapsto n \cdot \text{Id}_M$  for all  $n \in \mathbb{Z}$ . With the specification above one could observe the correspondence:

- $\{\mathbb{Z} \text{ modules}\} \iff \{\text{Abelian groups}\}$
- $\{\mathbb{Z}/n\mathbb{Z} \text{ modules}\} \iff \{\text{Abelian groups } M \text{ s.t. } nx = 0 \forall x \in M\}$

## 2 Morphism of $R$ -Modules

**Definition 2.1** (Morphism of  $R$ -Modules). A **morphism of (left)  $R$ -modules**  $f : M \rightarrow N$  is an  $R$ -linear map, which satisfies:

- $f(u_1 + u_2) = f(u_1) + f(u_2)$  for all  $u_1, u_2 \in M$ .
- $f(au) = af(u)$ , for all  $u \in M, a \in R$ .

An isomorphism of  $R$ -modules  $f : M \rightarrow N$  is equivalently stating that

- There exists  $g : N \rightarrow M$  s.t.  $f \circ g = \text{Id}_M, g \circ f = \text{Id}_N$ .
- $f$  is a bijection.

**Proposition 2.1.** Let  $f : M \rightarrow N$  be a morphism of  $R$ -modules. Then  $\text{im } f \subseteq N$  and  $\ker f \subseteq M$  are submodules; and  $f$  is injective if and only if  $\ker f = \{0\}$ .

*Proof.* By the fact that  $f$  is  $R$ -linear, both the image and kernel should be closed w.r.t. addition and scalar multiplication, i.e. are submodules. For the condition of injectivity, check

$\Rightarrow$ : Consider the contraposition. Suppose that  $0 \neq a \in \ker f$ . Then  $f(1) = f(1 + a)$  with  $1 \neq 1 + a$  which is a contradiction.

$\Leftarrow$ : Consider the contraposition. Suppose that there exists  $a \neq b \in R$  s.t.  $f(a) = f(b)$ , i.e.  $f$  is not injective; then  $f(a - b) = 0$  which indicates that  $0 \neq (a - b) \in \ker$ .

□

**Definition 2.2** (Quotient Module). Let  $N \subseteq M$  be a  $R$ -submodule. Define the equivalence relation  $\sim$ :  $a \sim b$  if and only if  $a - b \in N$ . Then  $M/N := M/\sim$  is a **quotient module**, with  $\pi : m \rightarrow M/N$  the induced morphism of  $R$ -modules.

**Theorem 2.1** (Universal Property of Quotient Modules). Let  $f : M \rightarrow P$  be a morphism of  $R$ -modules. Let  $N$  be a submodule of  $M$ , with  $\pi$  the induced morphism of  $R$ -modules. Further suppose that  $N \subseteq \ker f$ . Then there exists a unique  $g : M/N \rightarrow P$  s.t.  $f = g \circ \pi$ , i.e. the following diagram commutes:

$$\begin{array}{ccc} M & \xrightarrow{\pi} & M/N \\ & \searrow f & \downarrow g \\ & & P \end{array}$$

*Proof.* It suffices to verify that such map exists and is unique.

- *Uniqueness.* Since the diagram is required to commute, if such function exists, it is fixed by  $f(x) = g(\pi(x)) = g(\bar{x})$ .
- *Existence.* Then it suffices to check that  $g$  such defined is indeed a morphism of  $R$ -modules. This is indeed the case as  $f$  is a morphism of  $R$ -modules.

□

**Theorem 2.2** (First Isomorphism Theorem). *Let  $f : M \rightarrow N$  be a surjective morphism of  $R$ -modules. Define  $K := \ker f$ . If there exists a morphism of  $R$ -modules  $\bar{f} : M/K \rightarrow N$  s.t. it is  $R$ -linear and  $\bar{f} \circ \pi = f$ , i.e. the following diagram commutes:*

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ & \searrow \pi & \uparrow \bar{f} \\ & & M/K \end{array}$$

*Then  $\bar{f}$  is an isomorphism.*

*Proof.* By the universal property of morphism of  $R$ -modules (Theorem 2.1), a morphism  $f : M/K \rightarrow N$  s.t. the diagram above commutes exists. It suffices to verify that  $\bar{f}$  is bijective. It is surjective as  $f$  is surjective; and is injective as  $f(x) - f(y) = 0$  if and only if  $(x - y) \in K$ . □

**Definition 2.3** (Direct Product; Direct Sum). *Let  $(R_i)_{i \in I}$  be a family (potentially infinite) of modules. Then*

- The **direct product** of them is the cartesian product  $\prod_{i \in I} R_i$ , where addition and multiplication is defined element-wise.
- The **direct sum** is a sub-ring of the direct sum  $\bigoplus_{i \in I} R_i$  where only finitely many elements can be non-zero.
- $M$  is the **(internal) direct sum** if  $M_1$  and  $M_2$  if there exists an isomorphism  $f : M_1 \oplus M_2 \rightarrow M$ .

**Theorem 2.3** (Universal Property of Direct Product). *Let  $P$  be an  $R$ -module,  $(M_i)_{i \in I}$  be a family of  $R$ -modules, with  $f_j : P \rightarrow M_j$  a morphism of  $R$ -modules. Further let  $p_j : \prod_{i \in I} M_i \rightarrow M_j$  the projection map s.t.  $p_j(x) = x_j$  which is the  $j$ -th entry of the input. Then there exists a unique morphism of  $R$ -modules  $f : P \rightarrow \prod_{i \in I} M_i$  s.t.  $f(x) = (f_1(x), \dots, f_n(x), \dots)$ ; i.e. the following diagram commutes:*

$$\begin{array}{ccc} P & \xrightarrow{\quad f \quad} & \prod_{i \in I} M_i \\ & \searrow f_j & \downarrow p_j \\ & & M_j \end{array}$$

*Proof.* Uniqueness follows from the fact that  $p_j \circ f$  should commute with  $f_j$  for all  $j$ . Existence holds as  $f_j$  is itself a morphism of  $R$ -modules. □

**Theorem 2.4** (Universal Property of Direct Sum). *Let  $(M_i)_{i \in I}$  be a family of modules, with  $f_j : M_j \rightarrow Q$  a family of morphism of  $R$ -algebras. Denote  $\alpha_j$  to be the natural embedding s.t.*

$$\alpha_j : M_j \rightarrow \bigoplus_{i \in I} M_i, \quad \alpha_j(x) = (x_i)_i, \quad \text{where } x_i = \begin{cases} x, & i = j \\ 0, & \text{otherwise} \end{cases}$$

*Then there exists a unique  $R$ -linear map  $f : \bigoplus_{i \in I} M_i \rightarrow Q$  s.t.  $f \circ \alpha_j = f_j$  for all  $j$ , i.e. the following diagram commutes:*

$$\begin{array}{ccc} M_j & \xrightarrow{\alpha_j} & \bigoplus_{i \in I} M_i \\ & \searrow f_j & \downarrow f \\ & & Q \end{array}$$

*Proof.* Since  $f$  is required to be a morphism of  $R$ -modules, for all  $x = (x_i)_{i \in I} \in \bigoplus_{i \in I} M_i$  it should satisfy the following conditions:

$$f(x) = f\left(\sum_{k \in I} \alpha_k(p_k(x))\right) = \sum_{k \in I} f(\alpha_k(p_k(x))) = \sum_{k \in I} f_k(p_k(x))$$

which is unique as  $f_k$ s and  $p_k$ s are uniquely defined. Since both  $f_k$  and  $p_k$  are homomorphisms, the composition is also a homomorphism.  $\square$

### 3 Construction of Submodules

This interlude provides some general constructions on how to obtain submodules of a given module. For the setup, let  $R$  be a ring, with  $M$  a left  $R$ -module.

1. Let  $(M_i)_{i \in I}$  be a family of submodules of  $M$ . Then  $\bigcap_{i \in I} M_i$  is a submodule of  $M$ .
2. Consider the submodule generated by a subset  $A \subseteq M$ . By definition,  $\langle A \rangle := \bigcup \{N \mid N \subseteq M, A \subseteq N, N \text{ submodules}\}$ . The following proposition provides an explicit expression:

**Proposition 3.1.** *The submodule generated by  $A \subseteq M$  has the following explicit expression:*

$$\langle A \rangle = \left\{ \sum_{i \in I} a_i x_i \mid a_i \in R, x_i \in A, \text{ finitely many nonzero } a_i \right\}$$

*Proof.* This is simply a re-formalization of the definition. Proceed by showing the double inclusion:

- $\subseteq$ : Notice that RHS is indeed a module; and all elements in  $A$  are contained in it by setting  $a_i = 1$  and  $x_i$  to be the desired element.
- $\supseteq$ : By the fact that module should be closed w.r.t scalar multiplication and addition.

$\square$

3. Let  $(M_i)_{i \in I}$  a family of modules. Then

$$\sum_{i \in I} M_i := \left\langle \bigcup_{i \in I} M_i \right\rangle := \left\{ \sum_{i \in I} x_i \mid x_i \in M_i \forall i, \text{ finitely many nonzero } x_i \right\}$$

4. It would be interesting to consider the following isomorphism of quotient of  $R$ -modules:

**Theorem 3.1** (Third Isomorphism Theorem). *Let  $M_1$  and  $M_2$  be  $R$ -submodules of  $M$ . Then*

$$(M_1 + M_2)/M_2 \cong M_1/(M_1 \cap M_2)$$

*Proof.* Consider two functions  $f : M_1 \rightarrow (M_1 + M_2)/M_2$  and  $g : M_1 \rightarrow M_1/(M_1 \cap M_2)$ . Attempt to show this via applying the first isomorphism theorem. Consider the following diagram:

$$\begin{array}{ccc} M_1 & \xrightarrow{g} & M_1/(M_1 \cap M_2) \\ & \searrow f & \downarrow h \\ & & (M_1 + M_2)/M_2 \end{array}$$

In order to apply the first isomorphism theorem, it suffices to show that  $M_1 \cap M_2 = \ker f$ : as then the universal property grants the existence of such  $h$ , which allows the application of the First Isomorphism Theorem. This is indeed the case, as

- $M_1 \cap M_2 \subseteq \ker f$ , as  $M_1 \cap M_2 \subseteq M_2$  which is mapped to 0 by  $f$ .
- $M_1 \cap M_2 \supseteq \ker f$ . For all  $x \in \ker f$ , by hypothesis  $x \in M_1$ ; and the only elements that are annihilated by the quotient are those in  $M_2$ .

□

5. Let  $N \subseteq M$  a left submodule. Let  $I \subseteq R$  an ideal. Then consider the submodule

$$IN := \left\{ \sum_{i \in I} a_i x_i \mid a_i \in I, x_i \in N, \text{ finitely many nonzero } a_i \right\}$$

## 4 Free Modules

**Definition 4.1** (Linear Combination (Module)). *Let  $M$  be an  $R$ -module, with  $(x_i)_{i \in I}$  a finite family of elements in  $M$ . Then a **linear combination** of  $x_i$ s for some fixed family of elements  $(r_i)_{i \in I}$  in  $R$  is the sum  $\sum_{i \in I} x_i r_i$ .*

For the following definitions, fix  $M$  to be an  $R$ -module.

**Definition 4.2** (System of Generators).  $(x_i)_{i \in I} \subseteq M$  is a **system of generators** if  $\langle \{x_i \mid i \in I\} \rangle = M$ ; i.e. every element in  $M$  is a finite linear combination of generators.

**Definition 4.3** (Finite Generation).  $M$  is **finitely generated** if it admits a finite system of generators.

**Definition 4.4** (Linear Independence).  $A \subseteq M$  a subset of  $M$  is **linearly independent** if the finite sum  $\sum_{a_i \in A, u_i \in U} a_i u_i = 0$  implies that for all  $i$ ,  $u_i = 0$ .

**Definition 4.5** (Basis). *A basis of  $M$  is an independent system of generators.*

**Definition 4.6** (Free Module).  *$M$  is a **Free  $R$ -module** if it admits a basis.*

**Remark 4.1.**  $R$  not admitting a multiplicative inverse makes modules slightly different from vector spaces. Consider the following examples:

1. A nonzero module may not admit an independent subset. For example  $R = \mathbb{Z}$  with  $M = \mathbb{Z}/n\mathbb{Z}$ . Then  $n$  annihilates the whole ring.
2. For  $N \subseteq M$  a submodule, generally  $M \cong N \oplus M/N$  does not hold. Take the example where  $M = \mathbb{Z}$  and  $N = n\mathbb{Z}$ .  $N \oplus (M/N)$  is not an integral domain as  $n \cdot (0, 1) = (0, 0)$ ; but  $M$  is effectively an integral domain.
3. Similar to the case of vector spaces, it is useful to think in terms of modules in the canonical form. A useful result in vector space is that all  $K$ -vector spaces with dimension  $n$  is isomorphic to  $K^n$ . We make the analogy in terms of modules.  
Let  $I$  be a set. Denote  $R^{(I)} := \bigoplus_{i \in I} M_i = \left\{ (x_i)_{i \in I} \mid \text{finitely nonzero } x_i \right\}$ , where  $M_i = R$ . This has a basis  $(e_j)_{j \in I}$  which has 1 in the  $j$ -th entry. Every free (left)  $R$ -module is isomorphism to some  $R^{(I)}$  which sends the bases to bases.
4. If  $R$  is commutative, then any two bases of a free  $R$ -module has the same cardinality (which is given by considering the quotient of maximal ideals and observe that every basis is a basis in the field; which has the same cardinality as this is in a vector space). But this can fail if  $R$  is not commutative.

**Theorem 4.1** (Universal Property of Free Modules). *Let  $F$  be a free  $R$ -module with basis  $(e_i)_{i \in I}$ , and  $N$  an arbitrary  $R$ -module. For all  $(u_i)_{i \in I} \subseteq N$ , there exists a unique morphism of  $R$ -modules  $f : F \rightarrow N$  s.t.  $f(e_i) = u_i$  for all  $i$ .*

*Proof.*  $f$  gives the definition and therefore restricts the map to be unique. The fact that  $e_i$ s construct a basis in  $F$  ensures that this is a morphism of  $R$ -modules. □

**Remark 4.2.** The general thought is the same as that of the universal property of ring homomorphisms of polynomial rings, where it is possible to decompose the whole structure into several discrete structures; and designate maps on them correspondingly.

## 5 Finiteness Conditions on Modules

**Definition 5.1** (Noetherian Module). *Let  $R$  be a ring and  $M$  a left  $R$ -module. Then  $M$  is **Noetherian** if it satisfies the ACC (Ascending Chain) condition on submodules, i.e. there does not exist a family of submodules of  $M$   $(M_i)_{i \in I}$  s.t.*

$$(0) \subseteq M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n \subsetneq \cdots$$

**Definition 5.2** (Artinian Module). *Let  $R$  be a ring and  $M$  a left  $R$ -module. Then  $M$  is **Artinian** if it satisfies the DCC (Descending Chain) condition on submodules, i.e. there does not exist a family of submodules of  $M$   $(M_i)_{i \in I}$  s.t.*

$$\cdots \subsetneq M_n \subsetneq \cdots \subsetneq M_1 \subsetneq M_0 \subseteq M$$

**Remark 5.1.**  $R$  is Noetherian (or Artinian) if it is a Noetherian (or Artinian)  $R$ -module.

*Proof.* This simply results from the fact that when  $R$  is taken as an  $R$ -module, then its submodules are the ideals of  $R$ . □

**Remark 5.2.**  $M$  is a Noetherian  $R$ -module if and only if all of its submodules are finitely generated. The proof is generally the same as that for rings.

**Remark 5.3.** Modules generally are not Artinian. The ring of integers  $\mathbb{Z}$  is a clear counterexample, with the infinite descending chain  $(2^n)$ . The following are some examples:

- All  $K$  fields. This is trivial as the only ideals in  $K$  are  $(1)$  and  $(0)$ ; and submodules of a ring corresponds to its ideals.
- $\mathbb{Z}/n\mathbb{Z}$  for all  $n \in \mathbb{Z}_{\geq 0}$ . Rings of such form are finite, which can only admit finitely many ideals as they are by definition subsets of  $R$ .
- $K[x]/(x^n)$  for all  $n \in \mathbb{Z}_{\geq 0}$  and  $K$  fields. Since  $K[x]/(x^n)$  contains only elements of degree less than or equal to  $(n - 1)$  and  $K$  is a field, any element with degree  $n_0 < n$  linearly spans all elements of the same degree.

Claim that if  $I_1 \subsetneq I_2$  in  $k[x]/x^n$ , then there exists some  $k$  s.t.  $n^k \notin I_1$  and  $n^k \in I_2$ . Suppose not, i.e. for all  $k$  there exists some  $a_1^{(k)}, a_2^{(k)} \in K$  s.t.  $a_1^{(k)}n^k \in I_1$  and  $a_2^{(k)}n^k \in I_2$ . Since  $(a_1^{(k)})^{-1}a_2^{(k)} \in K$ , this implies that  $I_2 \subseteq I_1$ , which is a contradiction.

Therefore, for each proper submodule the number of monomials with different degrees in the submodule must decrease; and since there are only finitely many  $(n)$  of them, the descending chain must terminate at some point.

**Proposition 5.1.** Let  $N$  be a submodule of  $M$ . Then  $M$  is Noetherian (or Artinian) if and only if both  $N$  and  $M/N$  are Noetherian (or Artinian)

*Proof.* Consider implication in both directions:

$\Rightarrow$ : Since  $M$  is Noetherian, all of its submodules are finitely generated. Since  $N$  is a submodule of  $M$ , all of its submodules are also submodules of  $M$ , which are finitely generated, i.e.  $N$  is Noetherian.

To verify that the quotient module  $M/N$  is Noetherian, consider the following parenthesis:

**Parenthesis 5.1** (Correspondence). There is a bijection between submodules of  $M/N$  and submodules of  $M$  containing  $N$ .

*Proof.* It suffices to specify the map and check that it is indeed bijective. Define  $\pi : M \rightarrow M/N$  which is the induced morphism of  $R$ -modules. Check that it is bijective:

- For any submodule  $U \subseteq M/N$ ,  $\pi^{-1}(U) = \{u + n \mid u \in U, n \in N_s\}$  where  $N_s \subseteq N$  is an arbitrary submodule of  $N$ . Codomain being submodules in  $M$  containing  $N$  restricts  $N_s = N$ . This gives  $\pi(\pi^{-1}(U)) = U$  by definition of the quotient.
- For any submodule  $S \subseteq M$ ,  $\pi(S) = \{\pi(s) \mid s \in S\}$ ; with  $\pi^{-1}(\pi(S)) = \{s + n \mid s \in S, n \in N_s\}$  where  $N_s$  is some submodule of  $N$ . Similarly since it is required that the module in  $M$  should contain  $N$ , it fixes  $N_s = N$ .

□

$\Leftarrow$ : The general idea is to split  $M$  into those contained in  $N$  and those which maps non-trivially to  $M/N$ , and use the fact that both  $N$  and  $M/N$  are Noetherian to conclude that any ascending chain in  $M$  must also stabilize.

Consider  $\{M_1, \dots, M_n, \dots\}$  to be an infinite ascending chain s.t.  $M_1 \subseteq M_2 \subseteq \dots \subseteq M_n \subseteq \dots$ . We seek to verify that this ascending chain stabilizes at some time, i.e. there exists some  $n_0$  s.t. for all  $n \geq n_0$ ,  $M_n = M_{n+1}$ . Consider the following two ascending chains:



$$(1) M_1 \cap N \subseteq \cdots \subseteq M_k \cap N \subseteq \cdots$$

$$(2) \pi(M_1) \subseteq \cdots \subseteq \pi(M_k) \subseteq \cdots$$

Since both  $N$  and  $M/N$  are Noetherian, the two chains must stabilize, i.e. there exists some  $i_0$  s.t. beyond which both chains stabilize. Claim that  $n_0 = i_0$ . It suffices to verify that  $\forall i \geq i_0, M_{i+1} = M_i$ . By definition  $M_i \subseteq M_{i+1}$ . For inclusion in the other direction consider  $x \in M_i$  and  $y \in M_{i+1}$ . Notice  $\pi(x) = \pi(y)$  since  $M_i/N = M_{i+1}/N$  by hypothesis, i.e.  $x - y \in \ker \pi = N$ . Further notice that  $x - y \in M_{i+1}$  by inclusion  $M_i \subseteq M_{i+1}$ . Therefore  $x - y \in M_{i+1} \cap N$ . Since the first chain stabilizes,  $x - y \in M_i \cap N$ , i.e.  $x \in M_i \cap N$ , which implies  $x \in M_i$ . This gives  $M_{i+1} \subseteq M_i$ , i.e.  $M_i = M_{i+1}$ .

□

**Remark 5.4.** A nice application of the Correspondence Theorem (Parenthesis 5.1) is an alternative proof of the statement that all maximal ideals are prime.

Let  $I$  be maximal in  $R$ . Consider  $R/I$  which is a field (which is a domain), and elements in  $I$  are mapped to 0. The fact that  $R/I$  admits no zero-divisors gives the result that  $I$  is prime.

**Corollary 5.1.** Let  $M_1, M_2$  be left  $R$ -modules. Then  $M_1 \oplus M_2$  is Noetherian (Artinian) if and only if both  $M_1$  and  $M_2$  are Noetherian (Artinian). If  $R$  is Noetherian, then  $R^n$  is Noetherian for all  $n \in \mathbb{Z}_{\geq 0}$ .

**Remark 5.5.** In Remark 4.1 it is mentioned that generally  $M \not\simeq M/N \times N$ . However this is true if the product is an internal direct sum. Generally, if there exists some submodule  $K \subseteq M_1 \oplus M_2$  s.t.  $K \simeq M_1$ , then  $(M_1 \oplus M_2)/K \simeq M_2$ .

**Proposition 5.2.** Let  $R$  be a left Noetherian ring. Then a left  $R$ -module  $M$  is Noetherian if and only if  $M$  is finitely generated.

*Proof.* Proceed via showing implication in two directions:

$\Rightarrow$ :  $M$  being Noetherian implies that every submodule of it is finitely generated. Specifically,  $M$  is finitely generated.

$\Leftarrow$ : Proceed via finding a surjective map from a Noetherian  $R$ -module to  $M$ . Since  $M$  is finitely generated, it attains a system of generators in the form of  $\{u_1, \dots, u_n\}$ . Consider the morphism of  $R$ -modules  $\varphi : R^n \rightarrow M$  s.t.  $\varphi(e_i) = u_i$ , where  $e_i$  is the  $i$ -th element of the canonical basis of  $R^n$ . Since  $u_i$ s give a system of generators,  $\varphi$  is surjective.  $M$  having an infinite ascending chain implies there exists an infinite ascending chain in  $R^n$ , which contradicts the hypothesis that  $R$  is Noetherian. Therefore  $M$  is Noetherian.

□

## 6 Modules of Finite Length

**Definition 6.1.** Let  $R$  be a ring, and  $M$  a left  $R$ -module.  $M$  is **simple** if  $M$  is not the zero module, and it does not admit non-trivial submodules (i.e. for  $a; N \subseteq M, N = \{0\}$  or  $N = M$ )

**Proposition 6.1.** Let  $M_1$  and  $M_2$  be both  $R$ -modules, and  $f : M_1 \rightarrow M_2$  a morphism of  $R$ -modules which does not map every element to 0 in  $M_2$ . Then

- If  $M_2$  is simple, then  $f$  is surjective.
- If  $M_1$  is simple, then  $f$  is injective.

- If both  $M_1$  and  $M_2$  are simple, then  $f$  is an isomorphism.

*Proof.* Since  $f$  is a morphism of  $R$ -modules, it is  $R$ -linear, i.e. preserves  $R$ -module structures. Therefore  $f(M_1) \subseteq M_2$  is an  $R$ -module.  $M_2$  is simple implies that its only submodules are  $\{0\}$  and  $M_2$ . Since  $f$  does not map all elements to zero,  $f(M_1) = M_2$ , i.e.  $f$  is surjective.

Similarly,  $f(M_1)$  is a module. Suppose that  $f$  is not injective, i.e. there exists  $a \neq b \in M_1$  s.t.  $f(a) = f(b)$ . Then  $f(a - b) = 0$ , i.e.  $(a - b) \in \ker f$ . Consider the submodule of  $M_1$  generated by  $(a - b)$ . Since  $M_1$  does not admit non-trivial submodules,  $(a - b) = M_1 \subseteq \ker f$ , i.e.  $f$  maps all elements to zero, which is a contradiction. The third statement results directly from the previous two statements.  $\square$

**Remark 6.1.** Let  $M \simeq R/I$  which is a simple  $R$ -module. If  $R$  is commutative then  $I$  is maximal.  $M$  is also an  $R/I$ -vector space, but not a free  $R$ -module as all elements in  $I$  are annihilators. Simple free modules over a field are equivalent to a 1-dimensional vector space.

**Definition 6.2.** An  $R$ -module  $M$  has **finite length** if there exists a sequence of submodules

$$(0) \subsetneq M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M$$

s.t. for all  $i \in \llbracket 0, r-1 \rrbracket$   $M_{i+1}/M_i$  is simple. The sequence is a **composition series**, with each  $M_{i+1}/M_i$  a **factor** of the composition series. The **length** of the module is  $r$ , denoted as  $\ell(m)$ .

**Proposition 6.2.**  $M$  has finite length if and only if  $M$  is both Artinian and Noetherian.

*Proof.* Proceed via showing implication in both directions:

$\Rightarrow$ : Proceed via showing a contradiction. Suppose that  $M$  is not Noetherian. Then there exists an infinite ascending chain with each factor admitting at least one simple factor, i.e.  $M$  is not of finite length. Symmetric argument applies on the case of Artinian modules.

$\Leftarrow$ : For a given chain of modules, require that each factor is simple. By the fact that  $M$  is both Noetherian and Artinian it must admit a maximal and a minimal element. Such gives a composition series, and the length of it can be read off.  $\square$

**Theorem 6.1** (Jordan-Hölder). If  $M$  is of finite length, then any two composition series have the same length; and their simple factors are isomorphic after reordering.

*Proof.* Denote  $\mathcal{P}$  the family of submodules of  $M$  that this does not hold. Proceed via showing a contradiction on  $\mathcal{P} \neq \emptyset$ . By Prop 6.2,  $M$  is Artinian, i.e.  $\mathcal{P}$  has a minimal element (otherwise this gives an infinite descending chain). Denote that to be  $M'$ . By hypothesis it admits two non-equivalent (of different length) composition series:

$$\begin{aligned} \mathcal{M} : \quad (0) \subsetneq M_s \subsetneq \cdots \subsetneq M_1 \subsetneq M' \\ \mathcal{N} : \quad (0) \subsetneq N_r \subsetneq \cdots \subsetneq N_1 \subsetneq M' \end{aligned}$$

Then it falls into either of the following cases:

- $M$  is simple. Then  $M_1 = N_1 = (0)$  which is a contradiction.
- $M_1 = N_1$ . Since  $M$  is minimal in  $\mathcal{P}$ , both  $M_1$  and  $N_1$  admit a unique composition series, i.e.  $\ell(M_1) = \ell(N_1)$ . Then by definition  $\ell(M) = \ell(M_1) + 1$  which is a contradiction.
- $M_1 \neq N_1$ . Observe that  $M_1/M_1 \cap N_1$  is simple, as from the Third Isomorphism Theorem  $M_1/M_1 \cap N_1 \simeq (M_1 + N_1)/M_1$ ; and since  $M'/M_1$  is a simple factor with  $M_1 \neq N_1$ ,  $M_1 \subsetneq (M_1 + N_1) \subseteq M'$ , this gives  $M' = M_1 + N_1$ . Similarly  $N_1/M_1 \cap N_1$  is simple. By hypothesis  $M_1$  and  $N_1$  have isomorphic simple factors after reordering, there exists a composition series in both  $M_1$  and  $N_1$  admitting the first simple factor  $M_1/M_1 \cap N_1$  and  $N_1/M_1 \cap N_1$ ; and since  $M'$  is minimal in  $\mathcal{P}$  the theorem holds for  $M_1 \cap N_1$  which admits a unique (up to equivalence) composition series  $\mathcal{F}$ . Then the composition series of  $M'$  must take the following form:

$$\begin{array}{ccccc} \cdots & \subseteq & M_1 \cap N_1 & \subseteq & M_1 & \subseteq & M & (\mathcal{M}) \\ & & & \subseteq & & \subsetneq & & \\ (\mathcal{F}) & & & & N_1 & & & (\mathcal{N}) \end{array}$$

By Third Isomorphism Theorem it is shown that these two composition series are equivalent, which implies that  $M' \notin \mathcal{P}$ . □

**Corollary 6.1.** For  $N \subseteq M$  a submodule,  $\ell(M) = \ell(N) + \ell(M/N)$ .

*Proof.* By Parenthesis 5.1 modules in  $M/N$  are in bijection with modules in  $M$  that contains  $N$ . Since both  $N$  and  $M/N$  are of finite length, they admit a unique (up to equivalence) composition series:

$$\begin{array}{ll} (N) : & (0) \subsetneq N_s \subsetneq \cdots \subsetneq N_1 = N \\ (M/N) : & (0) \subsetneq P_r \subsetneq \cdots \subsetneq P_1 = M/N \end{array}$$

Then this gives a composition series for  $M$  via concatenating the two composition series with necessary alterations:

$$(M) : (0) \subsetneq N_s \subsetneq \cdots \subsetneq N_1 \subsetneq (P_r + N) \subsetneq \cdots \subsetneq (P_1 + N)$$

□

**Remark 6.2.** Consider  $R = \mathbb{Z}/n\mathbb{Z}$  (or equivalently  $\mathbb{Z}$ ), with  $M = \mathbb{Z}/n\mathbb{Z}$  an  $R$ -module. Then  $M$  is of finite length as it only admits finitely many elements. It is possible to write that in an explicit form, as for decomposition of  $n$ :  $n = p_1 \cdots p_r$ , this gives a composition series

$$(0) = (p_1 \cdots p_r)\mathbb{Z}/n\mathbb{Z} \subsetneq \cdots \subsetneq p_1 p_2 \mathbb{Z}/n\mathbb{Z} \subsetneq p_1 \mathbb{Z}/n\mathbb{Z} \subsetneq \mathbb{Z}/n\mathbb{Z} = M$$

**Parenthesis 6.1** (Second Isomorphism Theorem). Let  $R$  be a domain and  $a, b \in R$  nonzero elements. Then  $R/(b) \simeq (a)/(ab)$ .

*Proof.* The isomorphism is specified by  $\varphi : x \mapsto (ax)$ . It may be helpful to consider the following diagram: □

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & (a) \\ \cup & & \cup \\ (b) & \xrightarrow{\varphi} & (ab) \end{array}$$

## 7 Digression on Commutative Algebra

For discussions in this section, fix  $R$  to be a commutative ring.

**Lemma 7.1** (Nakayama's Lemma). *Let  $M$  be a finitely generated  $R$ -module, and  $I \subsetneq R$  an ideal contained in every maximal ideal of  $R$ . Then  $IM = M \implies M = 0$ .*

**Remark 7.1.** Consider  $(R, I)$  a local ring. Then  $R/I =: K$  is a field, i.e.  $M/IM$  can be viewed as either a  $R/I$  module or equivalently a  $K$ -vector space. Therefore if  $M/IM = 0$ , then  $M = 0$ .

*Proof.* Since  $M$  is finitely generated, there exists a system of generators  $(u_1, \dots, u_r)$ . Then for all  $j$  s.t.  $u_j \in IM$ , there exists  $a_{ij} \in I$  s.t.  $u_j = \sum_{i=1}^r a_{ij}u_i$ . Denote  $(a_{ij}) \in M_{n,n}(R)$ . Written in matrix form this gives

$$(I - (a_{ij})) \begin{pmatrix} u_1 \\ \vdots \\ u_r \end{pmatrix} = 0 \implies \begin{pmatrix} \det(\text{Id} - (a_{ij})) & & 0 \\ & \ddots & \\ 0 & & \det(\text{Id} - (a_{ij})) \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_r \end{pmatrix} = 0$$

where the implication results from left-multiplying the adjoint matrix of  $(I - (a_{ij}))$ , which implies that for all  $i$ ,  $\det(\text{Id} - (a_{ij}))u_i = 0$ . But notice that the determinant is the sum of all permutation of product of elements in distinct rows; and since all  $a_{ij}$  elements are in  $I$ ,  $\det(\text{Id} - (a_{ij}))$  must take the form of  $(1 + u)$  where  $u \in I$  as it is a product of  $a_{ij}$ s. Since  $I$  is in every maximal ideal,  $u$  cannot be invertible, which indicates that  $u_i = 0$  for all  $i$ . Since  $M$  is generated by zero, it must be the zero module itself.  $\square$

**Corollary 7.1.** Let  $I \subseteq R$  be an ideal contained in all maximal ideals. Let  $M$  be a finitely generated module and  $N \subseteq M$  a submodule of it. If  $M = N + IM$ , then  $N = M$ .

*Proof.* Apply quotient w.r.t  $N$  on both sides, which gives  $M/N = I(M/N)$ . Nakayama's Lemma 7.1 gives  $M/N = 0$ , i.e.  $M = N$ .  $\square$

**Theorem 7.1** (Artin-Rees). *Let  $R$  be a Noetherian commutative ring,  $M$  a finitely generated  $R$ -module, and  $N$  a submodule of  $M$ . Then there exists  $a \in \mathbb{Z}_{\geq 0}$  s.t. for all  $n > a$ ,*

$$I^n M \cap N \subseteq I^{n-a} N$$

*Proof.* To prove this theorem some scaffolding is necessary:

**Definition 7.1** (Rees Algebra). *The **Rees Algebra** is defined as a subring of polynomial ring  $R[t]$ :*

$$\text{Rees}(I) := \left\{ f = \sum_{k=0}^n c_k t^k \mid c_j \in I^j \forall j \geq 0 \right\} =: \bigoplus_{j=0}^n I^j t^j = R[It] \subseteq R[t]$$

**Proposition 7.1.** *If  $R$  is Noetherian, then  $\text{Rees}(I)$  is Noetherian for all  $I \subseteq R$  ideals.*

*Proof.* Notice that  $\text{Rees}(I) = R[It]$  is a finitely generated  $R$ -algebra as  $R[It] = R[f_1 t, f_2 t, \dots, f_d t]$  if  $I = (f_1, \dots, f_d)$ . Apply Hilbert's Basis Theorem for multivariate polynomials gives that  $\text{Rees}(I)$  is Noetherian.  $\square$

**Definition 7.2** (*R*-module of Polynomials). *The module of polynomials on R-modules is defined as*

$$M[t] = \left\{ \sum_{i=0}^k m_i t^i \mid k \geq 0, m_0, \dots, m_k \in M \right\}$$

with addition the sum of addition on monomials where the coefficients follow the addition in  $M$ , and scalar multiplication apply term-wise with scalar multiplication on the coefficient the same as in  $M$ .

Then similarly it is possible to define Rees Algebra on Modules:

**Definition 7.3** (Rees Algebra (on Modules)). *Rees Algebra on modules is the module over  $\text{Rees}(I)$ :*

$$\text{Rees}(I, M) := \left\{ \sum_{i=0}^k m_i t^i \mid m_j \in I^j M \forall j \right\}$$

**Remark 7.2.** It is clear that  $\text{Rees}(I)$  for  $I \subseteq R$  an ideal is a subring of polynomial ring  $R[t]$ . Suppose that  $M = (u_0, \dots, u_n)$  is finitely generated over  $R$ . Then  $\text{Rees}(I, M) = (u_0, \dots, u_n)$  over  $\text{Rees}(I)$ , i.e. is generated by the same set of elements. This simply results from the fact that coefficients are in  $M$ ; and  $I^k \subseteq I^m$  for  $m \leq k$ .

Therefore, if  $M$  is Noetherian, then  $\text{Rees}(I, M)$  is also Noetherian (given that as specified by the hypothesis  $R$  is commutative and Noetherian).

The following gives the proof of the theorem (Theorem 7.1):

Consider the submodule of  $\text{Rees}(I, M)$  as a  $\text{Rees}(I)$ -module:

$$T := \left\{ \sum_{i=0}^n m_i t^i \mid m_i \in I^i M \cap N \forall i \right\} \hookrightarrow \text{Rees}(I, M)$$

By Remark 7.2,  $T$  is Noetherian, i.e. finitely generated. Then it is valid to choose a system of generators  $\{u_0 t^{a_0}, \dots, u_n t^{a_n}\}$  s.t.  $u_j \in I^{a_j} M \cap N$  for all  $j$ . Denote  $a = \max\{a_i \mid \forall i\}$ . Then there exists  $f_i$ s in  $\text{Rees}(I)$ , i.e.  $g_i$ s in  $R$  s.t.

$$u t^n = \sum_{i=0}^n (f_i) t^{a_i} = \sum_{i=0}^n (g_i t^{n-a_i}) t^{a_i}$$

By construction  $u \in I^n M \cap N$ . Further, for all  $i$ ,  $t^{n-a} \mid t^{n-a_i}$ , giving  $u \in I^{n-a} N$ . □

## 8 Artinian/Noetherian Commutative Ring

### 8.1 Artinian implies Noetherian: Module and Ring

## 9 Finitely Generated Modules Over PIDs

### 9.1 Torsion and Module Structure

## 10 Linear Algebra on Modules