MATH 593 - Module

AResseges Stery

November 2, 2023

Contents

1 Module

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

- *Addition* $(+) : M \times M \to M$ *, s.t.* $(M, +)$ *is an abelian group.*
- *Multiplication* $(\times) : R \times M \to M$*, 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 φ 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 $\varphi : R \to \mathrm{End}(M)$, where $\mathrm{End}(\cdot)$ 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

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

  as the application of functions is associative.

In particular, in the consideration of $\mathbb{Z}$-modules, the map $\varphi_{\mathbb{Z}} : \mathbb{Z} \to \mathrm{End}(M)$ is determined uniquely by the requirement that $1 \mapsto 1_M = \mathrm{Id}_M$. Since addition and multiplication should be preserved, $n \mapsto n \cdot \mathrm{Id}_M$ 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** $f : M \to N$ 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 $f : M \to N$ is equivalently stating that

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

Proposition 2.1. *Let $f : M \to N$ be a morphism of R-modules. Then* $\mathrm{im}\, f \subseteq M$ *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

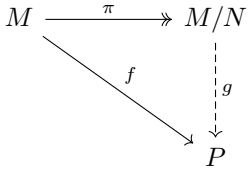
$\Rightarrow$: Consider the contraposition. Suppose that $0 \neq a \in \ker f$. Then $f(1) = f(1 + a)$ with $1 \neq 1 + a$ which is a contradiction.

$\Leftarrow$: 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 $\pi : m \to M/N$ the induced morphism of R-modules.*

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

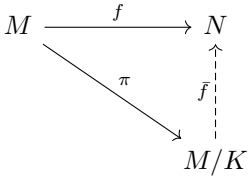


Proof. It suffices to verify that such map exists and is unique.

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



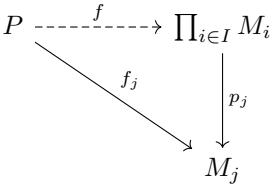
Then $\bar{f}$ is an isomorphism.

Proof. By the universal property of morphism of R-modules (Theorem 2.1), a morphism $f : M/K \to N$ 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 $f : M_1 \oplus M_2 \to M$.*

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 $f_j : P \to M_j$ a morphism of R-modules. Further let $p_j : \prod_{i \in I} M_i \to M_j$ 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 $f : P \to \prod_{i \in I} M_i$ s.t. $f(x) = (f_1(x), \cdots, f_n(x), \cdots)$; i.e. the following diagram commutes:*

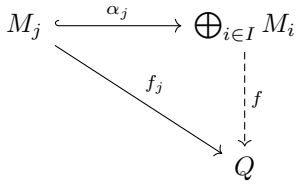


Proof. Uniqueness follows from the fact that $p_j \circ f$ should commute with f_j for all j. Existence holds as f_j is itself a morphism of R-modules. □

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

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

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



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_ks and p_ks are uniquely defined. Since both f_k and p_k are homomorphisms, the composition is also a homomorphism. □

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:*

   $$\langle A\rangle = \left\{ \sum_{i\in I} a_i x_i \;\middle|\; a_i \in R,\ x_i \in A,\ \textit{finitely many nonzero } a_i \right\}$$

   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.

   □

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

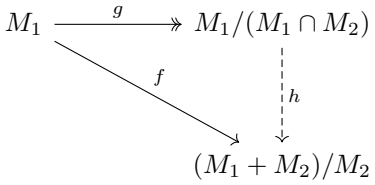
$$\sum_{i\in I} M_i := \left\langle \bigcup_{i\in I} M_i \right\rangle := \left\{ \sum_{i\in I} x_i \mid x_i \in M_i \ \forall i, \text{ finitely many nonzero } x_i \right\}$$

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



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

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

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_is 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 $R^{(I)} := \bigoplus_{i\in I} M_i = \left\{(x_i)_{i\in I} \;\middle|\; \text{finitely nonzero } x_i\text{s}\right\}$, 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 $f : F \to N$ 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_is 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 decomposition 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 $\pi : M \to M/N$ 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 $\{M_1, \cdots, M_n, \cdots\}$ to be an infinite ascending chain s.t. $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$. 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.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 $M \ncong M/N \times N$. 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 $\{u_1, \cdots, u_n\}$. Consider the morphism of R-modules $\varphi : R^n \to M$ s.t. $\varphi(e_i) = u_i$, where e_i is the i-th element of the canonical basis of R^n. Since u_is give a system of generators, φ 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 $f : M_1 \to M_2$ 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. □

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 $i \in [\![0, r-1]\!]$ 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.

□

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 $\mathcal{P} \neq 0$. 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:

$$\begin{array}{ccccccc} \cdots & \subseteq & M_1 \cap N_1 & \subseteq & M_1 & \subseteq & M \quad (\mathcal{M}) \\ & & & \nwarrow & & \swarrow & \\ (\mathcal{F}) & & & & N_1 & & (\mathcal{N}) \end{array}$$

  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:

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

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

$$(0) = (p_1 \cdots p_r)\mathbb{Z}/n\mathbb{Z} \subsetneq \cdots \subsetneq p_1p_2\mathbb{Z}/n\mathbb{Z} \subsetneq p_1\mathbb{Z}/n\mathbb{Z} \subsetneq \mathbb{Z}/n\mathbb{Z} = M$$

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: □

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

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 $(u_1, \cdots, u_r)$. 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

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

where the implication results from left-multiplying the adjoint matrix fo $(I-(a_{ij}))$, which implies that for all i, $\det(\mathrm{Id}-(a_{ij}))u_i = 0$. 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, $\det(\mathrm{Id} - (a_{ij}))$ 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. □

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. $M = N$. □

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 $R[t]$:*

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

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

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

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

$$M[t] = \left\{ \sum_{i=0}^{k} m_i t^i \;\middle|\; k \geq 0,\ m_0, \cdots, m_k \in M \right\}$$

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* $\mathrm{Rees}(I)$*:*

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

Remark 7.2. It is clear that $\mathrm{Rees}(I)$ for $I \subseteq R$ an ideal is a subring of polynomial ring $R[t]$. Suppose that $M = (u_0, \cdots, u_n)$ is finitely generated over R. Then $\mathrm{Rees}(I, M) = (u_0, \cdots, u_n)$ over $\mathrm{Rees}(I)$, 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 $\mathrm{Rees}(I, M)$ 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 $\mathrm{Rees}(I, M)$ as a $\mathrm{Rees}(I)$-module:

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

By Remark 7.2, T is Noetherian, i.e. finitely generated. Then it is valid to choose a system of generators $\{u_0 t^{a_0}, \cdots, u_n t^{a_n}\}$ 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_is in $\mathrm{Rees}(I)$, i.e. g_is 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 $u \in I^{n-a} N$. This finishes the proof. □

Theorem 7.2 (Krull's Intersection Theorem)**.** *Let R be a Noetherian commutative ring, and M a finitely generated R-module. Let $I \subseteq R$ be an ideal. If $N = \bigcap_{n \geq 1} I^n M$, then $IN = N$.*

Proof. Proceed by showing inclusion in both directions:

- $\subseteq$ By definition.
- $\supseteq$ Apply Artin-Rees with $n = a + 1$ which gives $N \subseteq I^{a+1} M \cap N \subseteq IN$.

□

8 Artinian/Noetherian Commutative Ring

Definition 8.1 (Minimal Prime Ideal)**.** *A prime ideal $\mathfrak{p}$ is a **minimal prime ideal over** I if it is minimal among all ideals containing I. Prime ideal $\mathfrak{p}$ is a **minimal prime ideal** if it is a minimal prime ideal over the zero ideal.*

Theorem 8.1. *Let R be a commutative ring. Then R is Artinian if and only if R is Noetherian, and the following two conditions are satisfied:*

- *R has only finitely many maximal ideals.*
- *Every maximal ideal in R is a minimum prime ideal.*

Remark 8.1. In Section 8.1 it will be shown that a ring being Artinian implies that is Noetherian. However, this generally does not hold in modules, as modules attain a "weaker" structure than rings as multiplication is not defined there.

Consider the following construction that specifically takes advantage of the absence of multiplication:

Let k be a field, with $S = k[x]$ the polynomial ring. Consider $R = k[x]_{(x)} := T^{-1}k[x]$ where $T := S \setminus (x)$, i.e. the localization of S at (x). Further consider $K := \mathrm{Frac}(R) := V^{-1}k[x]$ where $V := S \setminus \{0\}$, with the inclusion map $R \hookrightarrow K$. Since R is a submodule of K, it is valid to consider the pre-image of elements in the quotient module $M := K/R$ of the induced homomorphism, which gives the infinite ascending chain in K:

$$R = M_0 \subsetneq M_1 \subsetneq \cdots, \qquad M_k = R \cdot \left(\frac{1}{x^k}\right)$$

indicating that K is not Noetherian. Further notice that modules in the form of M_k as specified above are the only submodules of K, as for all $f \in K$ s.t. f = $\frac{f_n}{f_d}$ with $f_d \neq 0$, either

- $f_d \in T$. Then $f \in R$, i.e. $f \in M_0$.
- $f_d \notin T$. Then there exists some $k \in \mathbb{Z}_{>0}$ s.t. $f_d = x^k f'_d$ s.t. $f'_d \in T$. Then $f \in M_k$.

Since for all $f_i, f_j \in M_i$ and $f_i, f_j \notin M_{i+1}$, s.t. $f_i \neq f_j$, there exists $r = \frac{f_{jn}}{f_{in}} \in R$ s.t. $r \cdot f_i = f_j$ as R is a field (otherwise either f_i or f_j is in M_{i+1}). Therefore any chain of modules must be a subchain of the one listed above, which indicates that K is Artinian.

Notice that the absence of multiplication is really important here, as otherwise $(\frac{1}{x^m}) \subseteq (\frac{1}{x^k})$ for all $m \geq k$, where the chain collapses s.t. the module is Noetherian.

The following gives the proof of the theorem:

Proof of Theorem 8.1. First prove the implication where R is Artinian:

i) *R has finite many maximal ideals.* Proceed by showing the contraposition. Suppose that there exists infinitely many distinct maximal ideals $(m_1, \cdots, m_k, \cdots)$. Consider the descending chain:

$$m_1 \supsetneq m_1 m_2 \supsetneq \cdots \supsetneq m_1 \cdots m_k \supsetneq \cdots$$

Claim that $m_1 \cdots m_k m_{k+1}$ is indeed a proper sub-ideal of $m_1 \cdots m_k$. Suppose that this is not the case. Then, for all $x \in m_1 \cdots m_k$ there exists some $p \in m_{k+1}$ s.t. $yp = x$ for some $y \in m_1 \cdots m_k$. But this gives $x \in m_{k+1}$, i.e. $m_{k+1} \supseteq m_1 \cdots m_k$;

in particular $m_{k+1} \supsetneq m_1$ as the ideals are assumed to be distinct, which contradicts the fact that m_1 is maximal. Then by the claim the ring is not Artinian.

ii) *Every maximal ideal in R is a minimal prime ideal.* Notice that this is equivalent to stating that *every prime ideal is maximal.* Therefore, it suffices to prove that for any prime ideal $\mathfrak{p}$, $R/\mathfrak{p}$ is a field. Let $x \notin \mathfrak{p}$. Consider the following descending chain:

$$(x) \supseteq (x^2) \supseteq \cdots \supseteq (x^n) \supseteq \cdots$$

Since R is Artinian, there can only exist finitely many proper sub-ideals, i.e. there exists some k s.t. $(x^k) = (x^{k+1})$. That is, there exists some $r \in R$ s.t. $r \cdot x^k = x^{k+1}$. This gives $x^k(1 - xr) = 0$. Since $\mathfrak{p}$ is prime, and $0 \in \mathfrak{p}$, $(1 - xr) \in \mathfrak{p}$, i.e. $1 - xr = 0$ in $R/\mathfrak{p}$. Therefore, every element $x \notin \mathfrak{p}$ is invertible in $R/\mathfrak{p}$, which gives that $\mathfrak{p}$ is maximal.

iii) *R is Noetherian.* It suffices to prove that R is of finite length. First verify that there exists a sequence of ideals that are product of maximal ideals that gives a composition series. Then since R is Artinian each factor must be simple, which gives the desired result.

By i) there can only exist finitely many maximal ideals. Let them be $(p_1, \cdots, p_r)$. Claim that for $I = p_1 \cdots p_r$, there exists some k s.t. $I^k = (0)$. It suffices to verify that $\mathrm{Ann}_R(I^k) = R$.

Denote $J = \mathrm{Ann}_R(I^k)$. Proceed via showing a contradiction. Suppose that $J \neq R$. Then since J is an ideal in R and R is Artinian, there exists a minimal ideal J' that properly contains J. Then there exists some $x \in J' \setminus J$. Consider the ideal $J + Ix$. This is indeed an ideal as both I and J are ideals. Further $J \subseteq J + Ix \subseteq J'$ as $J + Ix \subseteq J + Rx \subseteq J'$. Since J' is minimal, and it properly contains J, it must fall into one of the following two cases:

- $J = J + Ix$. Then $Ix \in J$, which gives $Ix(I^k) = xI(I^k) = xI^{k+1} = xI^k = 0$, i.e. $x \in J$, which is a contradiction.
- $J + Ix = J'$. Since J' is minimal, J'/J is simple, i.e. x generates J'/J. As I is contained in every maximal ideal in R, it is also the case in J'/J by correspondence. Then in J'/J, $x = Ix \implies J'/J = 0$, i.e. $J' = J$ which is a contradiction.

Then a composition series is given via the construction above:

$$R \supseteq p_1 \supseteq p_1p_2 \supseteq \cdots \supseteq p_1 \cdots p_r \supseteq p_1^2 \cdots p_r \supseteq \cdots \supseteq (p_1 \cdots p_r)^k = (0)$$

Notice that for S a submodule of R, S/Sp_i is a R/p_i vector space as p_i is maximal; and it is isomorphic to some ideal of R. Therefore, it is Artinian, i.e. it is of finite dimension (otherwise it admits an infinite basis, which gives an infinite descending chain). Therefore, each factor has finite length, which indicates that R has finite length.

Now show the converse where R is Noetherian, there exists finitely many prime ideals, and they are maximal.

By hypothesis, the maximal ideals can be written out as $(p_1, \cdots, p_r)$ for finite r. Then every element in $I = p_1 \cdots p_r \subseteq p_1 \cap p_2 \cap \cdots \cap p_r$ is nilpotent. Proceed to prove the contradiction: suppose that a is not nilpotent, then the fraction ring $A^{-1}R$ is not the zero ring, where $A = \{1, a, \cdots, a^n, \cdots\}$. Consider the natural embedding of R into $A^{-1}R$. Claim that this injective, as if there exists some prime ideal $\mathfrak{p} \subseteq R$ that contains a, then it embeds to the whole ring in $A^{-1}R$, which contradicts the correspondence.

I is then finitely generated, as R is Noetherian. In particular, all elements in the system of generators of I are nilpotent, which implies that there exists some k s.t. $I^k = (0)$. Adopting the same strategy as above reaches the conclusion. □

Proposition 8.1. *If R is Noetherian, then R has finite minimal prime ideals.*

Theorem 8.2. *Let R be a Noetherian commutative ring, and M be a finitely generated R-module. Then there exists a finite sequence of R-submodules:*

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

s.t. $M_i/M_{i-1} \simeq R/p_i$ for all i. Such p_is are the associated primes of the module.

Proof. First we prove that if $M \neq 0$, there exist some $x \in M$ s.t. if $p = \mathrm{Ann}_R(x)$, then p is a prime ideal. Consider $\mathcal{P} = \{\mathrm{Ann}_R(x) \mid x \in M \setminus \{0\}\}$ which are the set of annihilators of all elements in R. Since R is Noetherian, there exists a maximal element $p \in \mathcal{P}$. Claim that the associated x is the element where the statement above holds. Suppose that $ab \in p$, and $a \notin p$. By definition $ax \neq 0$, i.e. $b \in \mathrm{Ann}_R(ax)$ since R is commutative. But since p is maximal, $\mathrm{Ann}_R(ax) \subseteq \mathrm{Ann}_R(x)$, i.e. $b \in \mathrm{Ann}_R(x) = p$ which is a prime ideal.

Then for the specific x and p, consider the R-linear map $f_{x,p} : R \to M, a \mapsto ax$. Since it has kernel p, $\mathrm{im}\, f_{x,p} \simeq R/p$ by the first isomorphism theorem. Since $f_{x,p}$ is an R-linear map, its image is a submodule. Designate $\mathrm{im}\, f_{x,p} =: M_1$. Apply recursively to R and M/M_1 to get subsequent quotients. Since R is Noetherian and M is finitely generated, M is a Noetherian R-module, which implies that the process will terminate. □

This gives a proof for proposition 8.1:

Definition 8.2 (Support)**.** *The **support** of an R-module M is the set of prime ideals s.t. $M_p := S^{-1}M$ is not the zero ring, where $S = R \setminus p$.*

Remark 8.2. If M is finitely generated, then an equivalent definition for support is

$$\mathrm{Supp}(M) = \{p \text{ prime ideal } \mid\ p \supseteq \mathrm{Ann}_R(M)\}$$

Proof of Proposition 8.1. If M is a finitely generated R-module and $N \subseteq M$ a submodule, notice $\mathrm{Supp}(M) = \mathrm{Supp}(N) \cup \mathrm{Supp}(M/N)$. as $\mathrm{Ann}_R(N) \subseteq \mathrm{Ann}_R(M)$ and so is the case for the quotient. Then

$$\mathrm{Supp}(M) = \bigcup_{i=1}^{n} \mathrm{Supp}(M_i/M_{i-1}) = \bigcup_{i=1}^{n} \mathrm{Supp}(R/p_i) = \{\text{prime ideals of } R \text{ containing } p_i\}$$

In particular, the minimal prime ideals containing $\mathrm{Ann}_R(M)$ are the p_is, which since M is Noetherian are only finitely many. If $M = R$, then $\mathrm{Ann}_R(R) = 0$, in which case the p_is are minimal prime ideals (over (0)). □

8.1 Artinian-Noetherian Implication in Ring

9 Finitely Generated Modules Over PIDs

Definition 9.1 (Rank)**.** *Let R be an integral domain, with M a finitely generated R-module; and $K = \mathrm{Frac}(R)$. The **rank** of M is defined as*

$$\mathrm{rank}(M) := \dim_K(S^{-1}M), \quad \textit{where } S = R \setminus \{0\}$$

Remark 9.1. Since K is the fraction field of R, to check that rank is well-defined it suffices to show that the addition and scalar multiplication are well-defined. Such is the case for multiplication and addition carried out respectively in the numerator. Notice that the compatibility of addition requires that R is commutative.

Suppose that M is free, naturally its rank should be the cardinality of its basis. This is indeed the case, as suppose that $M = (u_1, \cdots, u_n)$ which is free, $M \simeq R^n$, from which is clear that $\operatorname{rank}(M) = \dim_K(S^{-1}R^n) = n$.

Remark 9.2. Since M is finitely generated, it admits a system of generators $M = (u_1, \ldots, u_r)$. Notice that the module $S^{-1}M$ is generated by the natural embedding of the same elements $S^{-1}M = (\frac{u_1}{1}, \ldots, \frac{u_r}{1})$. But since $S^{-1}M$ is a $S^{-1}R$-vector space, this is actually a basis. Therefore $S^{-1}(M_1 \oplus M_2) \simeq S^{-1}M_1 \oplus S^{-1}M_2$.

In particular, choose $M_1 = M/N$ and $M_2 = N$ for $N \subseteq M$ a submodule of M. By considering the first isomorphism theorem on the quotient map $\varphi : S^{-1}M \to S^{-1}(M/N)$ we have $\ker\varphi = S^{-1}N$, i.e. $S^{-1}M \simeq S^{-1}N \oplus S^{-1}(M/N)$ as this is a vector space. This gives $\operatorname{rank}(M) = \operatorname{rank}(N) + \operatorname{rank}(M/N)$.

Definition 9.2 (Hom Module)**.** *Let R be a commutative ring, with M and N R-modules. Then the **Hom Module** between M and N is*

$$\operatorname{Hom}_R(M, N) = \{f : M \to N \mid f \text{ } R\text{-linear}\}$$

where

- Addition: $M \times M \to M : (f + g)(x) = f(x) + g(x)$ *for all* $x \in M$.
- Multiplication: $R \times M \to M : (rf)(x) = r \cdot f(x)$ *for all* $x \in M$.

where all the conditions are satisfied by the fact that they are satisfied in both M, N and R; and R is commutative.

The following work seeks to reveal the structure of R-modules over PIDs:

Theorem 9.1. *Let F be a finitely generated free R-module, R a PID and $G \subseteq F$ a submodule. Then there exists a basis $e_1, \ldots, e_n$ of F, and elements $a_1, \ldots, a_m$ such that $a_1 \mid a_2 \mid \cdots \mid a_m$; and $(a_i e_i)$s gives a basis of G.*

Proof. Proceed with induction on the rank of G. To prove that such basis exists, it suffices to show that for all G there exists some element that is mapped to $1 \in R$. The divisibility results from choosing the corresponding image to be maximal in R, and by the fact that R is a PID.

- *Base case:* $\operatorname{rank}(G) = 0$. By definition this implies that $\dim_{\operatorname{Frac}(R)}(S^{-1}G) = 0$, i.e. $S^{-1}G = 0$. This gives that for all $g \in G$, there exists some $s \in S$ s.t. $sg = 0$. By construction $s \neq 0$. Since $g \in G \subseteq F$, $g = \sum_{i=1}^n \lambda_i e_i$ for e_is a basis of F. $g \neq 0$ contradicts the fact that e_is give a basis, as in this case they are not linearly independent anymore. Therefore $g = 0$, i.e. $G = 0$.
- *Inductive step. Suppose that for all $G' \subseteq F$ R-submodules of F with rank k there exists some $a_1, \ldots, a_k$ s.t. $a_1 e_1, \cdots, a_k e_k$ give a basis of G.* Conduct the proof in the following steps:
  1) Notice that since F is finitely generated and R is Noetherian, F is Noetherian, i.e. G as an R-submodule of F is Noetherian. As for all $\varphi \in \operatorname{Hom}_R(F, R)$, $\varphi(G)$ is an ideal in R, there exists some $\varphi_0 \in \operatorname{Hom}_R(F, R)$ s.t. $\varphi_0(G)$ is maximal over R. Let $\varphi = \varphi_0$. Since R is a PID, there exists some a_1 s.t. $\varphi(G) = (a_1) \subseteq R$. Designate $x \in G$ s.t. $\varphi(x) = a_1$.
  2) $a_1 \neq 0$. Suppose that $a_1 = 0$. By the maximality of choice of φ, this implies that for all $\varphi' \in \operatorname{Hom}_R(F, R)$, $\varphi'(G) = 0$. But then specifically consider the maps π_j s.t. for all $u = \sum_{i=1}^n \alpha_i e_i$, $\pi_j(u) = \alpha_j$. This implies that $\alpha_i(u) = 0$ for all $i \in [\![1, n]\!]$, $u \in G$, which contradicts the hypothesis that $\operatorname{rank}(G) > 0$.

3) For all $\psi \in \mathrm{Hom}_R(F, R)$, $a_1 \mid \psi(x)$. Consider $d = \gcd(a_1, \psi(x))$. Since R is PID, there exists some $\alpha, \beta \in R$ s.t. $\alpha a_1 + \beta\psi(x) = d$, i.e. $d = \alpha\varphi(x) + \beta\psi(x) \supseteq (a_1) = \varphi(x)$. But by the hypothesis that (a_1) is maximal, $(a_1) \supseteq (d)$. This gives $(a_1) = (d)$, which implies the divisibility condition.

4) Specifically, it is valid to apply this on π_js, the maps of extracting j-th coefficient. Then, for $x = \sum_{i=1}^n c_i e_i$, $a_i \mid \pi_i(x) = c_i$, i.e. there exists some c_i' s.t. $c_i = a_1 c_i'$. This gives

$$\varphi(x) = \varphi\left(\sum_{i=1}^n c_i e_i\right) = \varphi\left(\sum_{i=1}^n a_1 c_i' e_i\right) = a_1\varphi\left(\sum_{i=1}^n c_i' e_i\right) = a_1 \implies \varphi\left(\sum_{i=1}^n c_i' e_i\right) = 1$$

(which essentially verifies that $a_1 = 1$, and G is free.) Therefore φ is surjective; and the submodule of G generated by (x) is of rank 1. Let $K = \ker\varphi$. Consider using the first isomorphism theorem on φ:

- $F \simeq K \oplus Re_1$:
  - $K \cap Re_1 = \{0\}$. For $r \in R$, $\varphi(re_1) = \varphi(r)\varphi(e_1) = \varphi(r) \implies r = 0$, i.e. $Re_1 \ni y = 0$ if and only if $y = 0$.
  - $K + Re_1 = F$. Let $u \in F$. Notice $\varphi(u - \varphi(u)e_1) = \varphi(u) - \varphi(u)\varphi(e_1) = 0$, i.e. $u - \varphi(u)e_1 \in K$. Such gives a decomposition of any element in F into such two components.
- $G \simeq (K \cap G) \oplus (Re_1 \cap G) = (K \cap G) \oplus (Ra_1e_1)$. As G is a submodule of F, given the result above it suffices to verify that $Re_1 \cap G = Ra_1e_1$. It results from (a_1) being the maximal ideal in G that can be reached by elements in $\mathrm{Hom}_R(F, R)$.

Since $\varphi(e_1) = 1$, $\mathrm{rank}(Ra_1e_1) = rank(R) = 1$. Therefore $\mathrm{rank}(G \cap K) = \mathrm{rank}(G) - 1$.

5) Apply induction on the rank of $G \cap K$. Let $(a_2e_2, \cdots, a_me_m)$ be a basis of K. It is clear that (a_1e_1) generates $G \setminus (G \cap K)$ as it is of rank 1, and the submodule generated by (a_1e_1) is isomorphic to R. Therefore $(a_1e_1, \cdots, a_me_m)$ is a basis of $S^{-1}G$, i.e. it is a basis of G.

6) It remains to show the divisibility condition. It suffices to show that $a_1 \mid a_2$. Reuse the maximality of (a_1): Consider $\varphi(a_1e_1 + a_2e_2) = (d)$, which since R is a PID is the gcd of a_1 and a_2. But maximality of (a_1) implies that $(d) = (a_1)$, i.e. $a_1 \mid a_2$.

□

Remark 9.3. There are some points that are worth mentioning in the proof above:

- Generally it is not true that one could reverse the process, i.e. given a basis of G complete that to become a basis of F. This simply results from the fact that scalar multiplication on modules is not reversible, which results in that submodules may have the same rank as the original module. This is completely different from being a vector space.

  Consider $R = F = \mathbb{Z}$, $G = 2\mathbb{Z}$. It is clear that one could get a basis of G via multiplying 2; but the reverse operation is impossible.

- R being a PID is used in obtaining both the maximality condition, and concluding the divisibility. If R is not a PID, it may be the case that φ above is not injective.

  Consider $R = k$, $F = k[x, y]$, with $G = (x) \subseteq k[x, y]$ where k is a field. Take the basis $F = (1, x + y, x - y)$. There are no such basis of G that could be obtained from that specific one of F.

- The a_1 in the proof is not necessarily 1, although G is free, which implies that there exists a surjective map from G to R. The homomorphisms φs are considered as elements in $\mathrm{Hom}_R(F, R)$, which does not necessarily maps G surjectively to R

as one can not complete a basis of a free submodule of F to the basis of F. a_1 is 1 if and only if F and G shares at least one same component in the basis.

Using this it is possible to generalize the structure of finitely generated modules over PIDs:

Theorem 9.2 (Sturcture, v1)**.** *Let M be a finitely generated R-module, with R a PID. Then there exists $a_1, \dots, a_m \in R \setminus \{0\}$ s.t. $a_1 \mid a_2 \mid \cdots \mid a_m$, and*

$$M \simeq R^k \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$$

Proof. Suppose that $M = (u_1, \cdots, u_n)$. Let $F = R^n$, with the canonical basis f_is. Consider morphism $\varphi : F \to M$ s.t. $f_i \mapsto u_i$. Define $G := \ker \varphi$. By Theorem 9.1, there exists some $a_1, \dots, a_{n-k}, a'_1, \dots, a'_k \in R$ ($a'_i = 0, a_1 \neq 0$ for all i) s.t. $G = (a_1 f_1, \cdots, a_n f_n)$. By first isomorphism theorem

$$M \simeq F/G \simeq \left(\bigoplus_i R/(a'_i) \oplus \bigoplus_i R/(a_i) \right) = R^k \oplus R/(a_1) \oplus \cdots \oplus R/(a^{n-k})$$

The divisibility condition follows also from Theorem 9.1. □

Remark 9.4. Notice that R being a PID implies that it is a UFD, i.e. for all a_i above there exists a unique irreducible (also prime) decomposition $a_i = u_i p_{i1}^{r_{i_1}} \dots p_{ir}$. Since R is a PID, $(a_i) = \bigcap_k p_{ik}^{r_{i_1}}$, which by Chinese Remainder Theorem gives $R/(a_i) \simeq \bigoplus_k R/(p_{ik}^{r_{i_1}})$. This gives another version of Structural Theorem (Theorem 9.2)

Theorem 9.3 (Structure, v2)**.** *Let M be a finitely generated R-module, with R a PID. Then there exists primes p_is and $n_i \in \mathbb{N}$ s.t.*

$$M \simeq R^r \oplus R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_r^{n_r})$$

9.1 Torsion and Module Structure