MATH593 Algebra I

AResseges Stery

July 19, 2024

Preface

The notes are taken for MATH593 Algebra I by Prof. Mircea Mustaţă in 2023 Fall at University of Michigan. The contents covered are mainly on module theory, with a bit of extension into Commutative Algebra, Category Theory and Homological Algebra. Here I appreciate the kind help of Prof. Mustaţă throughout the whole semester.

Some contents are marked with asterisk (*). These are contents excluded from testing, but out of personal interest I have recorded it. There are also some minor results that I added from the original course contents (which indicates that there may be typos or errors in the notes). Revisions, or pull requests to this repository, are more than welcomed.

For notes separated for each chapter one may consult this repository.

Contents

Chapter 1

Ring

1.1 Ring homomorphism, Quotient Ring

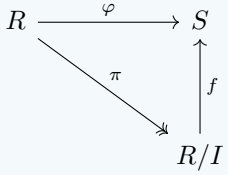
Definition 1.1.1 (Ring Homomorphism). Let X, Y be rings. A **Ring Homomorphism** is a map $f : X \to Y$ satisfying the following properties:

- $f(1) = 1$.
- $\forall x_1, x_2 \in X, f(x_1) + f(x_2) = f(x_1 + x_2)$.
- $\forall x_1, x_2 \in X, f(x_1 x_2) = f(x_1) f(x_2)$

Definition 1.1.2 (Quotient Ring). Let R be a ring and $I \subseteq R$ a two-sided ideal. The **Quotient Ring** (R/I) is defined as $(R/\sim)$ with an equivalence relation $\sim$ where $a \sim b$ if and only if $a - b = I$. Elements in (R/I) are denoted as $\bar{a}$, where $\bar{a} = \bar{b}$ if and only if $a \sim b$.

The natural homomorphism $\pi_I : R \to (R/I)$ is defined as $\pi(a) = \bar{a}$, which satisfies the *universal property of quotient rings*:

Theorem 1.1.3 (Fundamental Theorem of Ring Homomorphisms). Let $\varphi : R \to S$ be a ring homomorphism, I a two-sided ideal s.t. $I \subseteq \ker \varphi$, and π be the natural ring homomorphism from R to (R/I). Then there exists a unique ring homomorphism $f : R/I \to S$ s.t. the following diagram commutes,



i.e. $\varphi = f \circ \pi$.

Proof. It suffices to prove that f exists and is unique, and verify that f is indeed a ring homomorphism.

- **Uniqueness.** By the requirement that f should make the diagram commute, $f(\bar{a}) = \varphi(a)$, $\forall a \in R$. Uniqueness of f follows from the fact that φ maps every element in R to a unique element in S.

- **Existence.** It suffices to verify that f is well-defined, i.e. does not vary w.r.t. change of representative in (R/I). For all $a, b \in R$ s.t. $\bar{a} = \bar{b}$, $(a-b) \in I \implies \varphi(a-b) = 0 \implies \varphi(a) = \varphi(b)$ since φ is a ring homomorphism. By the uniqueness of f it is specified that $f(\bar{a}) = \varphi(a)$, which implies that for all $\bar{a} = \bar{b} \in (R/I)$, $f(\bar{a}) = \varphi(a) = \varphi(b) = f(\bar{b})$.
- f **is indeed a homomorphism.** This follows from the fact that φ is a ring homomorphism.

□

1.2 Ring of Fractions

Definition 1.2.1 (Multiplicative System). A subset $S \subseteq R$ for a ring R is a **multiplicative system** if $1 \in S$, and $\forall s_1, s_2 \in S, s_1 \cdot s_2 \in S$, where $\cdot$ is the multiplication in R.

Definition 1.2.2 (Ring of Fractions). Let R be a commutative ring, with $S \subseteq R$ a multiplicative subset, the **ring of fraction** $S^{-1}R$ is defined as $R \times S/\sim$, where $(s_1, r_1) \sim (s_2, r_2)$ if and only if there exists $t \in S$ s.t. $t(s_1 r_2 - s_2 r_1) = 0$. $(s, r) \in S^{-1}R$ is denoted as $\frac{r}{s}$. The definition of operations follows directly from analogy of that in $\mathbb{Q}$.

The natural homomorphism (inclusion map) from R to $S^{-1}R$ is defined as $r \hookrightarrow \frac{r}{1}$.

Remark 1.2.3. If R is an integral domain, then $(s_1, r_1) \sim (s_2, r_2)$ iff $s_1 r_2 = s_2 r_1$, as for $\mathbb{Q}$.

Remark 1.2.4. If R is not an integral domain, and S contains zero divisors, then the inclusion map ceases to be injective, as choosing t s.t. it satisfies $ts_1 = ts_2 = 0$ for some s_1, s_2 that are zero divisors gives $\varphi(s_1) = \varphi(s_2)$. Changing R to an integral domain guarantees that the inclusion map φ is injective.

Proposition 1.2.5. $\sim$ is an equivalence relation.

Proof. It is clear that $\sim$ is reflexive and symmetric. For transitivity, consider $(s_1, r_1) \sim (s_2, r_2) \wedge (s_2, r_2) \sim (s_3, r_3)$. That is, there exists some $t_1, t_2 \in R$ s.t.

$$\begin{cases} t_1(s_1 r_2 - s_2 r_1) = 0 \\ t_2(s_2 r_3 - s_3 r_2) = 0 \end{cases} \implies t_1 t_2 (s_1 r_2 s_3 - s_2 r_1 s_3) = t_1 t_2 (s_1 s_2 r_3 - s_2 r_1 s_3) = t_1 t_2 s_2 (s_1 r_3 - s_3 r_1) = 0$$

□

Remark 1.2.6. Notice that if $s \in S, then \frac{s}{a}$ for $a \in R$ is invertible. This tends more to a field, with more elements being "reachable" via multiplying an element from one side. A direct consequence is that less ideals exist in $S^{-1}R$, with ideals in R whose generators differ by a factor that divides s being identified in $S^{-1}R$.

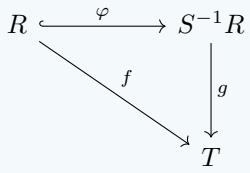
Remark 1.2.7. It is required that R is commutative is to preserve the most structures from R, i.e. ensure that $S^{-1}I$ is an ideal for all ideals in R. This is due to the addition in action:

$$\forall \frac{r_1}{s_1}, \frac{r_2}{s_2} \in S^{-1}R, \qquad \frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + s_1 r_2}{s_1 s_2}$$

which indicates that $S^{-1}I$ is a two-sided ideal if and only if $I \subseteq R$ is a two-sided ideal. For one-sided (left/right) ideal the

property is not fully inherited.

Theorem 1.2.8 (Universal Property of Ring of Fractions)**.** Suppose R and T are commutative rings, with φ the inclusion of R into $S^{-1}R$. Then for $f : R \to T$ s.t. $\forall s \in S, f(s)$ is invertible in T, there exists a unique ring homomorphism g s.t. $f = g \circ \varphi$, i.e. make the following diagram commute:



Proof. Adopt the same strategy as in the previous section:

- **Existence.** For all $\frac{a}{s} \in S^{-1}R$, $g(\frac{a}{s}) := f(a)(f(s))^{-1}$ which is well-defined since f is required to map all elements in S to invertible elements. g being a ring homomorphism follows from the fact that f is a ring homomorphism.
- **Uniqueness.** Follows from specifying $g(\frac{a}{s}) := f(a)(f(s))^{-1}$.

□

Remark 1.2.9. If $S := R \setminus \{0\}$, then $S^{-1}R$ is the whole field, with localization equivalent to completion of inverse of R.

Definition 1.2.10. A commutative ring $R \neq \{0\}$ is **local** if it admits a unique maximal ideal M. Local rings are denoted by a pair (R, M).

Example 1.2.11. Let R be a commutative ring, with $\mathfrak{p} \subseteq R$ a prime ideal. Let $S = R \setminus p$ be a multiplicative system. Then the ring $S^{-1}R$ is local, with the maximal ideal of it being $S^{-1}\mathfrak{p}$. This results from the fact that $S^{-1}I$ is an ideal if and only if I is an ideal in R. Further since $\mathbb{Z}$ is a PID (see next section), all prime ideals are maximal, $S^{-1}\mathfrak{p}$ is indeed maximal. The fact that there is only one such maximal ideal results from that all other primes are in S, i.e. $S^{-1}\mathfrak{p}' = S^{-1}R$ for all $\mathfrak{p}' \neq \mathfrak{p}$.

Proposition 1.2.12. Let $R \neq \{0\}$ be a commutative ring. Then R being local if and only if for all $a \in R$, either a is invertible or $(1 - a)$ is invertible. In this case, the maximal ideal M is the set of all non-invertible elements.

Proof. Proceed by showing implication in both directions:

$\Rightarrow$: Suppose that (R, M) is the local ring of interest. Proceed by showing a contradiction: suppose that both a and $(1 - a)$ are non-invertible. Then since R is local $(a) \subseteq M$, $(1 - a) \subseteq M$ indicating that $1 \in M$ which is a contradiction. In this case for all a non-invertible, $(a) \subseteq M$, which implies that M is the set of all non-invertible elements.

$\Leftarrow$: Define set $M := \{a \in R \mid \forall x \in R, ax \neq 1\}$. By construction if M is an ideal then it must be maximal, as including an invertible element expands the ideal to the whole ring. Verify that M is indeed an ideal:

- *Closed with addition.* Proceed via showing that the contraposition. Suppose that there exists $a, b \in R$ s.t. both a and b are non-invertible, but there exists some $c \in R$ s.t. $c(a + b) = 1$. Then $ca = 1 - (cb)$ is non-invertible, which implies that $1 - ca$ is invertible. But notice $1 - ca = cb$ is also non-invertible, which is a contradiction.
- *Absorption with multiplication.* This simply results from the fact that a non-invertible element multiplied by a unit is still non-invertible.

Further notice that this is indeed the only maximal ideal, as for all $u \in R \setminus M$, it is invertible, i.e. for all ideals $I \subseteq R$, $u \in I \implies 1 \in I \implies I = R$. Therefore (R, M) is local.

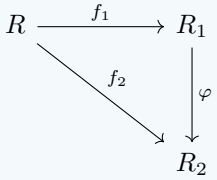
□

1.3 Polynomial Rings

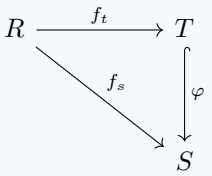
Definition 1.3.1 (R-algebra). Let R be a ring. Then a ring S is an R-**algebra** for the specific R mentioned if there exists a ring homomorphism $\varphi : R \to S$ s.t. $\forall r \in R, s \in S, \varphi(r)s = s\varphi(r)$. When the homomorphism needs to be specified, the algebra is often denoted as a pair $\langle S, \varphi \rangle$

Remark 1.3.2. An R-algebra is a two-sided R-module, which can be regarded as a generalization of the structure in R. R itself is not necessarily commutative, which implies that the associated homomorphism maps R to the center of S.

Definition 1.3.3 (Morphism of R-algebras). Let $\langle R_1, f_1 \rangle, \langle R_2, f_2 \rangle$ be R-algebras. A **Morphism of** R-**algebras** is a ring homomorphism $\varphi : R_1 \to R_2$ s.t. the following diagram commute; i.e. $f_2 = \varphi \circ f_1$:



Definition 1.3.4 (R-subalgebra). Let $\langle S, f_s \rangle$ be a R-algebra for R a ring. $\langle T, f_t \rangle$ is a R-**subalgebra** of S if T is a R-algebra, with $f_t(R) \subseteq S$; and there exists a morphism φ from T to S, i.e. φ makes the following diagram commute:



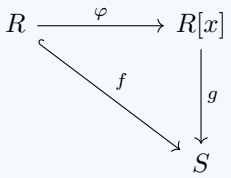
Definition 1.3.5 (Polynomial Ring). Let R be a commutative ring. The **polynomial ring of** R, denoted $R[x]$, is defined as

$$R[x] := \left\{ \sum_{i=0}^{n} c_i x^i \mid n \in \mathbb{N}, c_i \in R \right\}$$

with the addition and multiplication the same as in polynomials over $\mathbb{Z}$. The natural inclusion from R to $R[x]$ is defined as $r \mapsto r$ which is a polynomial of degree 0.

Remark 1.3.6. If R is a domain, then $R[x]$ is also a domain (consider the product of terms with highest degree); where $\deg(fg) \leq \deg(f) + \deg(g)$.

Theorem 1.3.7 (Universal Property of Polynomial Ring). Let R be a ring and $\langle S, f\rangle$ an R-algebra, and φ be the inclusion map from R to $R[x]$. For all $s \in S$, there exists a unique morphism of R-algebra $g : R[x] \to S$ s.t. $g(x) = a$, and the following diagram commutes, i.e. $f = g \circ \varphi$:



Proof. Proceed similarly by first determining the form that g takes, and then showing the uniqueness and existence.

- **Uniqueness.** Since it is required that g is a morphism of R-algebras, we have

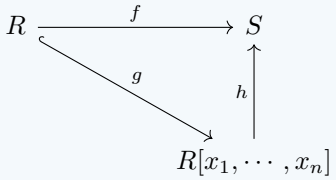
$$g\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} g(a_i)g(x^i) = \sum_{i=0}^{n} f(a_i)g(x^i) = \sum_{i=0}^{n} f(a_i)a^i$$

  by the requirement that $g(x) = a$. This is the only form that g could take, and thus proves its uniqueness.

- **Existence.** For existence it suffices to check that g is indeed a ring homomorphism. By the uniqueness g is fixed by sending $x \in R[x]$ to $a \in R$. Notice that R is commutative, which indicates that both left and right composition is satisfied; with the addition condition verified in the uniqueness part.

□

Theorem 1.3.8 (Universal Property of Polynomial Ring of Several Variables). Let A be a commutative R-algebra and g be the inclusion map from R to $R[x_1, \cdots, x_n]$ with a fixed n. For every R-algebra S and $(a_1, \cdots, a_n) \in S$, there exists a unique homomorphism of R-algebra $h : R[x_1, \cdots, x_n] \to S$ s.t. $h(x_i) = a_i$ for all $i \in [\![1, n]\!]$, and the following diagram commutes, i.e. $f = h \circ g$:



Sketch of Proof. The idea is similarly consider substitution $x_i \mapsto a_i$, and proceed to verify that this is indeed a ring homomorphism. One step that requires caution is that polynomials of several variables are defined in an inductive manner; therefore here proof should also be done inductively, on the number of variables involved. □

Using polynomial of several variables, it is clearer to formalize the "generating set" of a ring via specifying which element each variable maps to:

Definition 1.3.9 (Finitely Generated R-algebra). Let R be a commutative ring, with A a commutative R-algebra. Fix $(a_1, \cdots, a_n) \in A$. By the universal property of polynomial of several variables, there exists a unique homomorphism $\varphi : R[x_1, \cdots, x_n]$ s.t. $\varphi(x_i) = a_i$. Then the subalgebra $\operatorname{im} \varphi$ is said to be **generated** by $\{a_1, \cdots, a_n\}$.

Remark 1.3.10. Using the samre-formalization as in the definition above, $\operatorname{im}\varphi$ is smallest R-subalgebra of A that contains $\{a_1, \cdots, a_n\}$.

Proof. It is clear that $\operatorname{im}\varphi$ contains $\{a_1, \cdots, a_n\}$. To see that it is smallest, suppose there is a smaller one A', then there must be some $\sum_{i=0}^{n} a_i x^i \notin A'$, which contradicts with the fact that a ring should be closed. □

Notice that in the definition of polynomial ring it is only required that x could be multiplied with powers of itself. This enables making polynomial a representation of groups:

Definition 1.3.11 (Group Ring)**.** Let R a commutative ring, and G a group. A **group ring of R on G** is defined as

$$R[G] := \left\{ \sum_{g \in G} a_g g \mid a_g \in R \right\}$$

with the addition and multiplication the same as that in the polynomial ring.

Remark 1.3.12. The operation between the ring and the group is not required to be defined and is simply a notation. The polynomial cannot admit any structure that is more complicated (e.g. changing the group to be a ring) as otherwise the addition will not be well-defined.

1.4 Ideals

Definition 1.4.1 (Finitely-Generated Ideals)**.** Let R be a ring. Then

- Let (I_α) be a family of ideals for $\alpha \in \Lambda$ the index set, then the **ideal generated by (sum of)** (I_α) is defined as

$$\sum_{\alpha \in \Lambda' \subseteq \Lambda} I_\alpha := \left\{ \sum_{\alpha \in \Lambda'} a_\alpha \middle| a_\alpha \in I_\alpha, |\Lambda'| \text{ finite} \right\}$$

- Alternatively one could consider the **ideal generated by (product of)** two ideals (which can be easily extended to several ideal cases) I and J to be

$$I \cdot J := \left\{ \sum_{i=1}^{n} a_i b_i \middle| n \in \mathbb{Z}_{>0}, a_i \in I, b_i \in J \forall i \right\}$$

- Suppose further that R is commutative. Let $\Lambda := \{\lambda_1, \cdots, \lambda_n\}$ be a subset of R. Then the **ideal generated by** Λ is defined as

$$(\lambda_1, \cdots, \lambda_n) := \left\{ \sum_{k=1}^{n} r_k \lambda_k \middle| r_k \in R \right\}$$

Remark 1.4.2. Ideals generated by only one element is principal. For finitely generated ideals, the ideal generated by a set of elements is the same as the ideal generated by the corresponding principal ideals of the elements. This simply results from the fact that $(a) = \{ra | r \in R\}$.

Specify R to be a commutative ring, with $I \subseteq R$ an ideal of R. Consider the following special cases of ideals:

Definition 1.4.3 (Radical Ideal)**.** $I \subseteq R$ is a **radical ideal** if for all $a \in R$, $\exists n \in \mathbb{Z}_{>0}\ a^n \in I \implies a \in I$.

Definition 1.4.4 (Prime Ideal)**.** $I \subseteq R$ is a **prime ideal** if $I \neq R$, and for all $a, b \in R, ab \in I \implies (a \in I) \vee (b \in I)$.

Definition 1.4.5 (Maximal Ideal)**.** $I \subseteq R$ is a **maximal ideal** if $I \neq R$; and there is no ideal J in R s.t. $I \subsetneqq J \subsetneqq R$.

Remark 1.4.6. Recall that R is a domain if and only if for all $a, b \in R$, $ab = 0 \implies a = 0 \vee b = 0$. This implies that for any ring R with $\mathfrak{p}$ a prime ideal in it, $R/\mathfrak{p}$ is a domain.

Definition 1.4.7 (Reduced Ring)**.** A R is a **reduced ring** if and only if it does not have any nilpotent elements, i.e. for all $u \in R, u^n = 0 \implies u = 0$ for all $n \in \mathbb{Z}_{>0}$.

Remark 1.4.8. For a commutative ring R, I is a radical ideal if and only if R/I is a reduced ring.

Proposition 1.4.9. I is a maximal ideal if and only if R/I is a field.

Proof. This fact follows directly from the following simple lemma. □

Lemma 1.4.10. $R = K$ is a field if and only if it only has two ideals (0) and (1).

Proof. Consider in both directions:

$\Rightarrow$: If K is a field, then either there are no invertible elements, which in this case the ideal I can only contain 0 as this is the only non-invertible element in a field; or 1 and therefore every element is in the ideal, as $\forall g \in I, \exists g^{-1} \in K, gg^{-1} = 1 \in I$.

$\Leftarrow$: If a ring R has only two ideals (0) and (1), then for all $0 \neq u \in R$ consider (u). By hypothesis $(u) = (1)$, i.e. there exists some $u^{-1} \in R$, which implies that R is actually a field.

□

Proposition 1.4.11. An ideal being maximal implies that it is prime; and an ideal being prime implies that it is radical.

Proof. Maximal ideals are prime. Suppose that $I \subseteq R$ is maximal but is not prime, i.e. there exists some $a, b \in R$ s.t. $ab \in R, a \notin R, b \notin R$. By hypothesis $I \cup \{a\} = R.$, i.e. there exists some $r \in R, t \in I$ s.t. $a + rt = 1$. But then $b = ba + (br)t \in I$ which is a contradiction.

Prime ideals are radical. Consider inductively on a and a^{n-1}; apply the definition of prime ideals. □

Example 1.4.12. Consider counterexamples of the converse of the proposition above:

- $\mathbb{Z}_N$ for N not a power of prime is radical, but not prime.
- A trivial case for an ideal being prime but not maximal is (0), where as long as the ring is not a field, it is maximal.
- A more interesting case for an ideal being prime but not maximal is for finitely generated non-PIDs, adding a generator

to a prime ideal suffices to create a "larger" ideal. Take the example $(x) \subseteq R[x]$ where R is a domain, which is prime as $R[x]/\langle x \rangle \cong R$ is also a field. But $(x) \subseteq (2, x)$ which is not the whole ring.

1.5 Noetherian Ring

Lemma 1.5.1 (Zorn's Lemma)**.** Suppose that $(P, \leq)$ is an ordered set s.t. every totally order subset $P_0 \subseteq P$ has an upper bound, then P has a maximal element.

Theorem 1.5.2. Let $I \subseteq R$ be an ideal of a commutative ring R. Then there exists some maximal ideal M s.t. $I \subseteq M$.

Proof. The proof is simply a re-formalization of Zorn's Lemma (Lemma 1.5.1).

Consider $P := \{J \subseteq R \mid J \text{ ideals}, I \subseteq J, J \neq R\}$, with the order of inclusion. Take $P_0 := \{I_\alpha \mid \alpha \in \Lambda\} \subseteq P$ to be totally ordered. Then $J := \bigcup_\alpha I_\alpha$ is also an ideal. Further $1 \notin J$, otherwise there will exist some $\alpha \in \Lambda$ s.t. $I_\alpha = R$, which contradicts the hypothesis. Therefore J is the upper bound for the family P_0. Applying Zorn's Lemma finishes the proof. □

Definition 1.5.3 (Noetherian Ring)**.** A ring R is (left) **Noetherian** if it satisfies the Ascending Chain Condition (ACC), for (left) ideals, i.e. there is no infinite strictly increasing sequence of (left) ideals:

$$I_1 \subsetneqq I_2 \subsetneqq \cdots$$

Proposition 1.5.4. Let R be a ring, then the followings are equivalent:

1. R is (left) Noetherian.
2. Let P be a family of (left) ideals in R, then P has a maximal element.
3. Every (left) ideal in R is finitely generated.

Proof.

- (i) being equivalent to (ii) is via simply reformalizing the definition.
- (i) implies (iii). Proceed by proving the contraposition. Suppose that there exists an ideal $I_0 \subseteq R$ that is not finitely generated, then there exists an infinite sequence of generators of I_0 (a_i), $i \in \mathcal{I}$. Then there exists an infinite ACC $(a_1) \subsetneqq (a_1, a_2) \subsetneqq (a_1, \cdots, a_k), \subsetneqq \cdots$.
- (iii) implies (i). Prove by showing a contradiction. Suppose that there exists an infinite ACC $I_1 \subsetneqq I_2 \subsetneqq \cdots \subsetneqq I_k \subsetneqq \cdots$. Then consider $I := \bigcup_{n \geq 1} I_n$. By the hypothesis it is finitely generated, i.e. there exists some $(a_1, \cdots, a_m)$ s.t. $a_i \in I_{n_i}$ for all $i \in [\![1, m]\!]$. Define $n := \max\{n_i \mid i \in [\![1, m]\!]\}$. Then $I_n = I_{n+1}$ which is a contradiction.

□

Theorem 1.5.5 (Hilbert's Basis Theorem)**.** Let R be a commutative Noetherian ring. Then $R[x]$ is a Noetherian ring.

Proof. By proposition 1.5.4 it suffices to show that every ideal of $R[x]$ is finitely generated.

In the case that $I = (0)$, it is finitely generated as R is Noetherian. For the case of that $I \neq (0)$, consider a family of ideals where $f_1 \in I \setminus \{0\}$, with $f_k \in I \setminus (f_1, \cdots, f_k)$ for $k > 1$ s.t. $\deg f_k = \min\{\deg f \mid f \in I \setminus (f_1, \cdots, f_k)\}$. If there exists some k

s.t. $(f_1, \cdots, f_k) = I$ then $R[x]$ is by definition Noetherian. Suppose that it is not. Then there exists an infinite ascending chain. Denote $f_n = a_n x^{d_n} + \sum_{k=0}^{d_n - 1} a_k x^k$. From the construction it is clear that $d_1 \leq d_2 \leq \cdots \leq d_n \leq \cdots$.

Define $I := (a_1, \cdots, a_n \mid n \geq 1)$. By hypothesis $I \subseteq R$, which implies that it is finitely generated. Then there exists some k s.t. $I = (a_1, \cdots, a_k)$, with $d_i \geq 1$ (otherwise suppose there exists some $a_0 \in R \setminus (a_1, \cdots, a_k)$, simply add $a_0 x$ to the generators; and do the similar to ensure that the degree of polynomial associated with the corresponding coefficients is at least one. Since R is Noetherian, it is finitely generated, i.e. the process above will terminate, which does not interfere with the condition that the ascending chain does not terminate.)

For f_{k+1}, we know that there exists a family $(c_j)_{j=1}^k$ s.t. $a_{k+1} = \sum_{j=1}^{k} c_j a_j$ since $(a_1, \cdots, a_k)$ are generators. Then consider

$$f = f_{k+1} - \sum_{i=1}^{k} c_i x^{d_{k+1} - d_i} f_i$$

which is a polynomial that is not in $I \setminus (f_1, \cdots, f_n)$, which is a contradiction. □

Corollary 1.5.6. By induction $R[x_1, \cdots, x_n]$ is also Noetherian if R is Noetherian. Quotient and localization preserves the property that a ring is Noetherian.

1.6 Euclidean Domain, PIDs and UFDs

Definition 1.6.1 (Principal Ideal Domain (PID)). Let R be a integral domain. R is a **Principal Ideal Domain (PID)** if every ideal in R is principal.

Remark 1.6.2. If R is a PID, then R is Noetherian, as principal ideals are by definition finitely generated.

Proposition 1.6.3. If R is a PID, then every prime ideal in it is maximal.

Proof. Prove by contradiction. Suppose that $I = (p)$ is a prime ideal that is not maximal. Then by Theorem 1.5.2 there exists some maximal ideal $x \notin I$ s.t. $I \subseteq (x)$, i.e. there exists some $r \in R$ s.t. $p = xr$. Since $x \notin I, r \in I$. Write $r = pr'$ for $r' \in R$. Then $xr' = 1$, i.e. $(x) = (1)$ which is a contradiction. □

Definition 1.6.4 (Euclidean Domain). A **Euclidean Domain** is an integral domain R, for which there exists a function (norm) $N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$, s.t. $\forall a, b \in R, \neq 0$, there exists some $q, r \in R$ s.t. $a = bq + r$; and either $r = 0$, or $N(r) < N(b)$.

Proposition 1.6.5. A Euclidean Domain is a PID.

Proof. Let R be a euclidean domain. Since the domain of the norm is $\mathbb{Z}_{\geq 0}$, there exists some element b s.t. $N(b)$ is minimal. Claim that $R = (b)$.

This is indeed true, as there does not exist any r s.t. $N(r) < N(b)$. Then apply the definition of a Euclidean Domain. □

Definition 1.6.6. Let $a, b \in R \setminus \{0\}$. Then a is **associated with** b (denoted $a \sim b$) if there exists some u invertible, s.t. $a = ub$.

Remark 1.6.7. $a \sim b$ if and only if $(a) = (b)$.

Definition 1.6.8 (Greatest Common Divisor)**.** Let $a, b \in R$ that are not both zero. The **Greatest Common Divisor** of a and b is an element in $R \setminus \{0\}$ s.t. $d \mid a, d \mid b$; and for all $x \in R \setminus \{0\}$, $x \mid a \wedge x \mid b \implies x \mid d$.

Proposition 1.6.9. Let R be a domain, and d be the gcd of a and b. If $(a, b) = (d)$, then $d = \gcd(a, b)$.

Proof. d is a common divisor of a and b as $a, b \in (d)$. It is the greatest one as since $d \in (a, b)$, there exists some $\lambda, \mu \in R$ s.t. $\lambda a + \mu b = d$. Both sides should divide d, which implies that if there exists some $d' \mid a, d' \mid b$, then $d' \mid d$. □

Definition 1.6.10 (Prime; Irreducible)**.** Let R be a domain, and a a non-zero element. Then

- a is a **prime** if (a) is a prime ideal.
- a is **irreducible** if for all $b_1, b_2 \in R$ s.t. $a = b_1 b_2$, either b_1 is invertible or b_2 is invertible.

Proposition 1.6.11. Let R be a PID and $r \in R$ a non-zero element. Then r is irreducible if and only if (r) is a maximal ideal.

Proof. Proceed by showing implication in two directions:

$\Rightarrow$: Let r be an irreducible element. Suppose that there exists an ideal I s.t. $(r) \subsetneqq I \subsetneqq R$. Since R is a PID, there exists some $a \in R$ s.t. $I = (a)$, which indicates that there exists some $x \in R$ s.t. $r = ax$. But since r is irreducible, either a is a unit, i.e. $I = R$, or x is a unit, i.e. $I = (r)$. Both of which lead to a contradiction.

$\Leftarrow$: Proceed by showing the contraposition. Suppose that r is not irreducible, then there exists $p, q \in R$ which are not units s.t. $r = pq$. Then $(r) \subsetneqq (p) \subsetneqq R$ which implies that (r) is not maximal.

□

Proposition 1.6.12. If a is prime, then a is irreducible.

Proof. Let a be a prime. Suppose that there exists $b_1, b_2 \in R$ s.t. $b_1 b_2 = a$. Then $b_1 b_2 \in (a)$. Without loss of generality assume $b_1 \in (a)$, i.e. there exists some $r \in R$ s.t. $b_1 = ar$. This gives $arb_2 = a$, i.e. b_2 is invertible. □

Remark 1.6.13. The converse is generally not true. Consider in $\mathbb{Z}[\sqrt{5}i]$ which is not a UFD. Then (2) is not prime (as $2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$) but 2 is irreducible.

Definition 1.6.14 (Unique Factorization Domain (UFD))**.** A domain R is a **Unique Factorization Domain (UFD)** if for all nonzero $a \in R$ that is not invertible, there exists a decomposition $a = p_1 \cdots p_r$ where $p_1, \cdots, p_r$ are irreducible. For all other families of irreducible elements $q_1, \cdots, q_r \in R$ s.t. $a = q_1 \cdots q_r$, there exists a permutation $\varepsilon : [r + 1] \to [r + 1]$ s.t. $p_i \sim q_{\varepsilon(i)} \forall i$.

Proposition 1.6.15. Let R be a UFD. Then every irreducible element $p \in R$ is prime.

Proof. Claim that (p) is a prime ideal given that p is irreducible. Since p is irreducible and R is UFD, for all $b_1 b_2 \in (p)$, there exists some irreducible q_is for $i \in I$ s.t. $b_1 b_2 = p \cdot \prod_{i \in I} q_i$. Since factorization unique, at least one of b_1 and b_2 admits a divisor p, which indicates that (p) is a prime ideal. □

Proposition 1.6.16. Let R be a domain s.t. every irreducible element is prime. Then R is a UFD.

Proof. It suffices to prove that factorization is unique up to permutation and multiplication by units. Suppose that p_is and q_is are two irreducible decomposition of a, i.e. $a = p_1 \cdots p_r = q_1 \cdots q_s$. Then either

- $r = 0$. Then a is a unit, which indicates that $s = 0$.
- $r \neq 0$. Then $s \neq 0$. Since p_i is prime for all i, there exists some q_j s.t. $p_i \mid q_j$. this implies that $r \leq s$. Then consider q_is as prime, which implies $s \leq r$ and therefore $s = r$. Further since p_is and q_is are irreducible, for $p_i \mid q_j$ this implies $q_j = p_i u$ for u a unit.

This verifies the definition of a UFD. □

Proposition 1.6.17. Let R be a Noetherian ring. Then every element $a \in R$ attains an irreducible decomposition $a = p_1 \cdots p_r$ with p_i irreducible for all i.

Proof. This is simply a re-formalization of the fact that Noetherian rings are finitely generated. Consider the following cases:

- a is irreducible. Then the factorization process is done.
- $a = b_1 b_2$ where b_1 and b_2 are both not units. Then consider separately b_1 and b_2 with this process. This process is sure to terminate at some point as otherwise this gives an ideal of infinite generators.

□

Remark 1.6.18. Noetherian rings are generally not UFDs. A simple example is $\mathbb{Z}[\sqrt{5}i]$, the Gaussian Integers.

Theorem 1.6.19. Every PID is a UFD.

Proof. Since principal ideals are finitely generated, all PIDs are Noetherian. By proposition 1.6.17 there exists a decomposition; and by proposition 1.6.11 and 1.6.3 irreducible elements are prime. By proposition 1.6.16 it is a UFD. □

Example 1.6.20. An example where a ring is a UFD but not a PID (where prime ideals are not maximal) is $\mathbb{Z}[x]$, with the ideal $(2, x)$ which is not principal. (x) is prime, but not maximal.

The following proves the theorem:

Theorem 1.6.21. Let R be a UFD, then $R[x]$ is also a UFD.

Definition 1.6.22 (Primitive; Content). Let $f \in R[x]$ a nonzero polynomial. Then

- The **content** of f, denoted as $c(f)$ is the greatest common divisor of the coefficient of its terms.
- $f \in R[x]$ is **primitive** if its content is a unit.

Lemma 1.6.23. Let R be a UFD. Define $K := \mathrm{Frac}(R)$, i.e. $K = S^{-1}R$ for $S := R \setminus \{0\}$. A nonzero element $f \in R[x]$ is irreducible if and only if either of the following holds:

- $\deg f = 0$, and f is irreducible in R.
- $\deg f \geq 1$, f is primitive and is irreducible in $K[x]$.

Proof. Consider the following two cases:

- $\deg f = 0$. Since $R \subseteq R[x]$, f irreducible in $R[x]$ implies that it is irreducible in R. For the converse, notice that R is a domain, where the degree of product of two polynomials is at the sum of the degree of the two polynomials, indicating that $f \in \mathbb{R}[x]$ could only attain degree 0 factors. The fact that f is irreducible in R finishes the proof.
- $\deg f \geq 1$. Consider the two directions:

  $\Rightarrow$: Suppose that f is irreducible in $R[x]$. Notice that for all $g \in K[x]$, $c(g)^{-1}g \in R[x]$. Proceed by showing a contradiction. Suppose that there exists $f_1, f_2 \in K[x]$ of degree at least one s.t. $f = f_1 f_2$ (i.e. f is not irreducible in $K[x]$). Then

  $$f = (c(f_1)^{-1}f_1)(c(f_2)^{-1}f_2)c(f_1)c(f_2)$$

  where the four operands for multiplication are all in R. Since f is irreducible in R, either $(c(f_1)^{-1}f_1)$ or $(c(f_2)^{-1}f_2)$ is a unit, which contradicts the hypothesis that $\deg f_1 \geq 1 \wedge \deg f_2 \geq 1$.

  $\Leftarrow$: Proceed by showing that the contraposition is true. Suppose that $f = f_1 f_2$ where f_1, f_2 are both not units, in R. Then $f = f_1 f_2 \in K[x]$ which is also not irreducible.

□

Lemma 1.6.24. Let K be a field. Then $K[x]$ is a PID.

Proof. Let I be an ideal in $K[x]$. Define $k := \{\deg f \mid f \in I\}$. Such k indeed exists as the degree has a lower bound 0; and k could take only finitely many values with some element $f_0 \in I$ fixed; namely $[\![0, \deg f_0]\!]$. Claim that $I = (x^k)$.

Either $k = 0$, where $I = (1)$; or $k \neq 0$, where for all $f = \sum_{i \mid d_i \geq d} c_i x^{d_i} \sum_i c_i x^{d_i - d} \in K[x]$. □

Proof of Theorem 1.6.21. Define $K = S^{-1}R$ for $S = R \setminus \{0\}$. From lemma 1.6.24 we know $K[x]$ is a PID, which is therefore a UFD. The general strategy is to transform the whole problem into $K[x]$ using lemma 1.6.23, and use the fact that $K[x]$ is a UFD, with elements differ only by a factor in R (which is also a UFD) from those in $R[x]$.

It suffices to show that the decomposition exists and is unique:

- *Existence.* Decompose f in $R[x]$ $f = c(f)g$ s.t. g is primitive. Then $c(g) = u$ where u is some unit in R. Applying the inclusion map gives $g \in K[x]$, where it could be decomposed into $g = g_1 \cdots g_n$ where g_is are irreducible. Denote

$g_i = c(g_i)h_i$, which gives $g = \prod_{i=1}^{n} c(g_i)h_i = c(g)\prod_{i=1}^{n} h_1 = u\prod_{i=1}^{n} h_1$. Since $c(f) \in R$ which is a UFD, there exists a decomposition $c(f) = f_1 \cdots f_n$. This gives an irreducible decomposition $f = f_1 \cdots f_n h_1 \cdots h_n$.

- *Uniqueness.* This follows from the fact that both f and $K[x]$ are UFDs, i.e. decomposition of $f \in R$ and $g \in K[x]$ are unique.

  (Alternatively one could prove that irreducible elements in $R[x]$ are also prime, which is essentially the same approach as the content is prime follows from the fact that R is UFD; and the primitive is prime as $K[x]$ is a UFD).

□

Chapter 2

Module

2.1 Module

Definition 2.1.1 (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. $1 \times x = x$.
  - Associativity. For all $a, b \in R, x \in M$, $a(b \times x) = (ab) \times x$.
  - Distributivity in R. For all $a_1, a_2 \in R$, $(a_1 + a_2) \times x = a_1 \times x + a_2 \times x$.
  - Distributivity in M. For all $a \in R, x_1, x_2 \in M$, $a \times (x_1 + x_2) = a \times x_1 + a \times x_2$.

Right modules are defined with the same structure, but with multiplication in the form $x \times a$ for $a \in R, x \in M$.

Definition 2.1.2 (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 $n \in N, r \in R, r \times n \in N$.

Remark 2.1.3. 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 2.1.4. (Left) ideals of R are submodules of R taken as an R-submodule.

Remark 2.1.5. 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:

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

2.2 Morphism of R-Modules

Definition 2.2.1 (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 2.2.2. Let $f : M \to N$ be a morphism of R-modules. Then $\mathrm{im}\, f \subseteq N$ 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

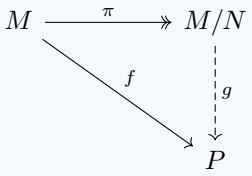
$\Rightarrow$: Consider the contraposition. Suppose that $0 \neq a \in \ker f$. Then $f(1) = f(1 + a)$ with $1 \neq 1 + a$ which is a contradiction.

$\Leftarrow$: 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 $0 \neq (a-b) \in \ker f$.

□

Definition 2.2.3 (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 2.2.4 (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 morphism of R-modules $g : M/N \to P$ s.t. $f = g \circ \pi$, i.e. the following diagram commutes:

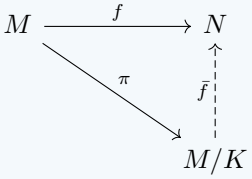


Proof. It suffices to verify that such map exists and is unique.

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



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

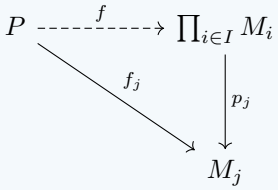
Proof. By the universal property of morphism of R-modules (Theorem 2.2.4), a morphism $\bar{f} : M/K \to N$ s.t. the diagram above commutes exists. It suffices to verify that $\bar{f}$ is bijective. It is surjective as f is surjective; and is injective as $f(x) - f(y) = 0$ if and only if $(x - y) \in K$. □

Definition 2.2.6 (Direct Product; Direct Sum). Let $(R_i)_{i \in I}$ be a family (potentially infinite) of R-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** $\bigoplus_{i \in I} R_i$ is a submodule of the direct product $\prod_{i \in I} R_i$ where only finitely many elements can be non-zero.

- M is the **(internal) direct sum** of M_1 and M_2 if there exists an isomorphism $f : M_1 \oplus M_2 \to M$.

Theorem 2.2.7 (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:

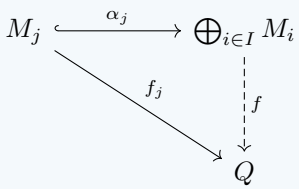


Proof. Uniqueness follows from the fact that $p_j \circ f$ should commute with f_j for all j. Existence holds as f_j is itself a morphism of R-modules. □

Theorem 2.2.8 (Universal Property of Direct Sum)**.** Let Q be an R-module, $(M_i)_{i\in I}$ be a family of modules, with $f_j : M_j \to Q$ a family of morphism of R-modules. Denote α_j to be the natrual embedding s.t.

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

Then there exists a unique R-linear map $f : \bigoplus_{i\in I} M_i \to Q$ 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. □

2.3 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, $\langle A \rangle := \bigcap \{N \mid N \text{ submodule of } M, A \subseteq N\}$. The following proposition provides an explicit expression:

> **Proposition 2.3.1.** The submodule generated by $A \subseteq M$ has the following explicit expression:
>
> $$\langle A \rangle = \left\{ \sum_{i=1}^{N} a_i x_i \;\middle|\; a_i \in R,\ x_i \in A, N \in \mathbb{N}^* \right\}$$

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.

□

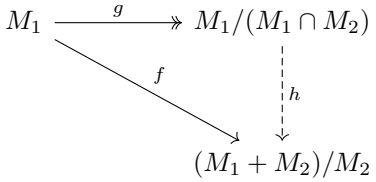
3. Let $(M_i)_{i \in I}$ be a family of submodules of M. Then

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

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

> **Theorem 2.3.2** (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 $g : M_1 \to M_1/(M_1 \cap M_2)$. 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

$$IN := \left\{ \sum_{i=1}^{N} a_i x_i \;\middle|\; a_i \in I,\ x_i \in N, N \in \mathbb{N}^* \right\}$$

2.4 Free Modules

Definition 2.4.1 (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 $\sum_{i\in I} r_i x_i$.

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

Definition 2.4.2 (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 2.4.3 (Finite Generation). M is **finitely generated** if it admits a finite system of generators.

Definition 2.4.4 (Linear Independence). $A \subseteq M$ a subset of M is **linearly independent** if any finite sum $\sum_{a_i\in A, r_i\in R} r_i a_i = 0$ implies that for all i, $r_i = 0$.

Definition 2.4.5 (Basis). A basis of M is an independent system of generators.

Definition 2.4.6 (Free Module). M is a **free R-module** if it admits a basis.

Remark 2.4.7. 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 $N = n\mathbb{Z}$. $N \oplus (M/N)$ has a finite nontrivial subgroup as $n \cdot (0, 1) = (0, 0)$; but all nontrivial subgroups of M are infinite.
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 $R^{(I)} := \bigoplus_{i\in I} M_i = \left\{(x_i)_{i\in I} \;\middle|\; x_i \in M_i, \text{ finitely nonzero } x_i\text{s}\right\}$, 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 2.4.8 (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 2.4.9. 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.

2.5 Finiteness Conditions on Modules

Definition 2.5.1 (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 2.5.2 (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 2.5.3. 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 2.5.4. 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 2.5.5. 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 2.5.6. 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 2.5.7** (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 2.5.8.** A nice application of the Correspondence Theorem (Parenthesis 2.5.7) 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 2.5.9.** 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 2.5.10.** In Remark 2.4.7 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 2.5.11. 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.

□

2.6 Modules of Finite Length

Definition 2.6.1. 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 2.6.2. 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 2.6.3. 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 2.6.4. 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 2.6.5. 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 2.6.6 (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 2.6.5, 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:

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

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

□

Corollary 2.6.7. For $N \subseteq M$ a submodule, $\ell(M) = \ell(N) + \ell(M/N)$.

Proof. By Parenthesis 2.5.7 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 2.6.8. 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 2.6.9 (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:

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

□

2.7 Digression on Commutative Algebra

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

Lemma 2.7.1 (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 2.7.2. 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 2.7.3. 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 2.7.1 gives $M/N = 0$, i.e. $M = N$. □

Theorem 2.7.4 (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 2.7.5 (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 2.7.6. 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 2.7.7 (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 2.7.8 (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 2.7.9. 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 2.7.4):

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 2.7.9, 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.

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

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 2.7.10 (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 $N \subseteq I^{a+1} M \cap N \subseteq IN$.

□

2.8 Artinian/Noetherian Commutative Ring

Definition 2.8.1 (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 2.8.2. 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 2.8.3. In this section 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 2.8.2. 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 2.8.4. If R is Noetherian, then R has finite minimal prime ideals.

Theorem 2.8.5. 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 2.8.4:

Definition 2.8.6 (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 2.8.7. 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 2.8.4. 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)). □

2.9 Finitely Generated Modules Over PIDs

Definition 2.9.1 (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

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

Remark 2.9.2. 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 $\mathrm{rank}(M) = \dim_K(S^{-1}R^n) = n$.

Remark 2.9.3. 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 $\mathrm{rank}(M) = \mathrm{rank}(N) + \mathrm{rank}(M/N)$.

Definition 2.9.4 (Hom Module). Let R be a commutative ring, with M and N R-modules. Then the **Hom Module** between M and N is

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

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.

Remark 2.9.5. It is vital that R is commutative, as otherwise the multiplication will not be necessarily R-linear.

Suppose that $r_1, r_2 \in R$, $f \in \mathrm{Hom}_R(M, N)$, and $s \in M$. Then

$$(r_1 f)(r_2 s) = (r_1 r_2) f(s) \overset{?}{=} (r_2 r_1) f(s) = r_2 (r_1 f)(s)$$

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

Theorem 2.9.6. Let F be a finitely generated free R-module, R a PID and $G \subseteq F$ a submodule. Then there exists a basis $e_1, \dots, e_n$ of F, and elements $a_1, \dots, a_m$ 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:* $\mathrm{rank}(G) = 0$. By definition this implies that $\dim_{\mathrm{Frac}(R)}(S^{-1}G) = 0$, 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 $a_1, \dots, a_k$ 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 $\varphi \in \mathrm{Hom}_R(F, R)$, $\varphi(G)$ is an ideal in R, there exists some $\varphi_0 \in \mathrm{Hom}_R(F, R)$ 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 $\varphi' \in \mathrm{Hom}_R(F, R)$, $\varphi'(G) = 0$. 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 $\mathrm{rank}(G) > 0$.

  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 2.9.7. 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 2.9.8 (Sturcture, v1). Let M be a finitely generated R-module, with R a PID. Then there exists $a_1, \ldots, a_m \in R \setminus \{0\}$ 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 2.9.6, there exists some $a_1, \ldots, a_{n-k}, a'_1, \ldots, a'_k \in R$ ($a'_i = 0, a_1 \neq 0$ for all i) s.t. $G = (a_1f_1, \cdots, a_nf_n)$. 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 2.9.6. □

Remark 2.9.9. 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 2.9.8)

Theorem 2.9.10 (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.

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

Chapter 3

Linear Algebra on a Ring

3.1 Linear Transformations on a Ring

Recall the two versions of Structural Theorem of finitely generated modules over PID:

Theorem 3.1.1 (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. $a_1 \mid a_2 \mid \cdots \mid a_m$.

Theorem 3.1.2 (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. $M \simeq R^r \oplus R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_r^{n_r})$.

Example 3.1.3. Let $R = \mathbb{Z}$, with M an R-module. Since defining scalar multiplication on modules is equivalent to defining maps from R to endomorphisms on M, it is sufficient for M to be an abelian group. By Structural Theorem, there exists p_is and m_is s.t. $M \simeq \mathbb{Z}^r \oplus \mathbb{Z}/(p_1^{m_1}) \oplus \cdots \oplus \mathbb{Z}/(p_k^{m_k})$. M is finite (as a group) if and only if $r = 0$.

The direct sum allows describing it with a basis, which gives a generalization of linear algebra defined on ring (module) structure.

Parenthesis 3.1.4. Linear maps between elements in free modules can be represented as invertible matrices.

Proof. The reasoning is similar to that under the context of vector spaces. Fix R to be a commutative ring, with M a finitely generated R-module. Let $n = \operatorname{rank}(M)$. Then $M \simeq R^n$. Choose $B = (e_1, \dots, e_n)$ to be a basis of M.

For all $u \in M$, there exists a unique decomposition of u into the basis, i.e. there exists $a_1, \dots, a_n$ s.t. $u = \sum_{k=1}^n a_k e_k$. Denote $M_B(u) = (a_1, \dots, a_k)^T$.

Now consider change of basis. Suppose that $B' = (e_1', \dots, e_n')$ is another basis of M. There exists b_{ik}s s.t. $e_i = \sum_{k=1}^n b_{ik} e_k'$; and there exists c_{ik}s s.t. $e_i' = \sum_{k=1}^n b_{ik} e_k$. Apply the substitution twice gives

$$e_i = \sum_{j=1}^n b_{ij} e_j' = \sum_{j=1}^n b_{ij} \left(\sum_{k=1}^n c_{jk} e_k \right) = \sum_{k=1}^n \sum_{j=1}^n (b_{ij} c_{jk}) e_k \implies \left(\sum_{k=1}^n \sum_{j=1}^n (b_{ij} c_{jk}) e_k \right) - e_i = 0$$

Since e_is give a basis, this implies that $\sum_{j=1}^{n}(b_{ij}c_{jk}) = \delta_{ik}$. Let $V = (b_{ij}) \in M_n(R)$ to be the transition matrix from B to B', abd $U = (c_{ij}) \in M_n(R)$ the transition matrix from B' to B. Conducting this concurrently gives $UV = \mathrm{Id}_B$. Similarly $VU = \mathrm{Id}_{B'}$. □

Proposition 3.1.5. The converse of the above also holds, i.e. If (c_{kl}) is invertible in $M_n(R)$, then for $e'_k = \sum_{l=1}^{n} c_{kl}e_l$, e'_ks also give a basis.

Proof. It suffices to verify that e'_ks are R-linearly independent, and they span the whole module:

- If there exists λ_is that are not all zero, that $\sum_{i=1}^{n} \lambda_i e'_i = 0$, then $\sum_{i=1}^{n} \lambda_i \sum_{k=1}^{n} c_{ik}e_k = 0$ which implies that e_k are not R-linearly independent, which is a contradiction.
- Since (c_{kl}) is invertible, there exists some (b_{kl}) s.t. $e_k = \sum_{l=1}^{n} b_{kl}e_l$. Then, for all $u \in M$ with decomposition into the original basis $u = \sum_{i=1}^{n} u_i e_i$, there exists a decomposition into e'_ks: $u = \sum_{i=1}^{n} u_i \sum_{j=1}^{n} b_{ij}e_j$.

□

Remark 3.1.6. The transition matrix is compatible with representation of an element in the basis. Let $M \ni u = \sum_{i=1}^{n} u_i e_i$, with $U = (b_{ij})$ the transition matrix from $B = (e_i)$ to $B' = (e'_i)$. Then

$$u = \sum_{i=1}^{n} u_i e_i = \sum_{i=1}^{n} \left(u_i \sum_{j=1}^{n} b_{ij} e'_i \right) \implies M_{B'}(u) = U \cdot M_B(u)$$

Remark 3.1.7. Using such formalization the operations are represented in the identical way as that in vector spaces:

1. *Applying a linear map.* If $T : F \to G$ is not an endomorphism and T is specified via specifying the image of the basis $T(e_j) = \sum_{i=1}^{n} a_{ij} f_j$, where F and G are finitely generated free R-modules; and $B_F = (e_i), B_G = (f_i)$ give a basis in the corresponding module. Then the matrix representation of T under such bases is $M_{B_F B_G}(T) = (a_{ij})$. It acts in the same way as matrices acting on vectors, as for $M_{B_F}(u) = (b_1, \ldots, b_u)^T$

$$\begin{aligned} T(u) = T\left(\sum_{j=1}^{n} b_j e_j \right) = \sum_{j=1}^{n} b_j T(e_j) = \sum_{j=1}^{n} b_j \left(\sum_{i=1}^{n} a_{ij} f_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{n} (a_{ij} b_j) f_j \\ \implies M_{B_G}(T(u)) = M_{B_F B_G}(T) \cdot M_{B_F}(u) \end{aligned}$$

2. *Composition of linear maps.* Consider $T : F \to G$ and $S : G \to H$ where $B_F = (e_i), B_G = (f_i)$ and $B_H = (g_i)$. To specify the linear maps, it suffices to specify where the elements of the basis is mapped to. Suppose that $T(e_i) = \sum_{j=1}^{n} a_{ji} f_j$; $S(f_i) = \sum_{j=1}^{n} b_{ji} h_j$. For $F \ni u = \sum_{i=1}^{n} u_i e_i$, considering $g \circ f$ gives

$$\begin{aligned} (S \circ T)(u) = (S \circ T)\left(\sum_{i=1}^{n} u_i e_i \right) = S\left(\sum_{i=1}^{n} u_i \sum_{j=1}^{n} a_{ji} f_j \right) = \sum_{i=1}^{n} u_i \sum_{j=1}^{n} a_{ji} S(f_j) \\ = \sum_{i=1}^{n} u_i \sum_{j=1}^{n} a_{ji} \sum_{k=1}^{n} b_{kj} h_j = \sum_{i=1}^{n} u_i \sum_{j=1}^{n} \left(\sum_{k=1}^{n} (a_{ji} b_{kj}) h_j \right) \\ \implies M_{B_F B_H}(S \circ T) = B_{B_G B_H}(S) \cdot M_{B_F B_G}(T) \end{aligned}$$

   where the elements of $M_{B_F B_H}(S \circ T)$ is specified by $\sum_{j=1}^{n} \sum_{k=1}^{n} (a_{ji} b_{kj})$.

3. *Change of basis.* Now consider change of basis under the context of a linear transformation. Let $T : F \to G$ be an R-linear map, with $M_{B_F B_G}(T)$ the matrix representation of T under B_F and B_G. Now consider change of basis maps $U : B_F \to B'_F$ and $\tilde{U} : B_G \to B'_G$. We are interested in the corresponding map $\tilde{T}$ of T after applying the change of basis:

$$\begin{array}{ccc} B'_F & \xrightarrow{\tilde{T}} & B'_G \\ {\scriptstyle U}\uparrow & & \uparrow{\scriptstyle \tilde{U}} \\ B_F & \xrightarrow{T} & B_G \end{array}$$

As proven above it is valid to express linear transformation and change of basis using matrices, and matrices corresponding to change of basis are invertible, we have for $u \in F$,

$$M_{B'_G}(T(u)) = M_{B_G B'_G}(\tilde{U}) M_{B_F B_G}(T) M_{B'_F B_F}(U) = M_{B_G B'_G}(\tilde{U}) M_{B_F B_G}(T) (M_{B_F B'_F}(U))^{-1}$$

4. *Change of basis on endomorphisms.* Then the equality above becomes

$$M_{B'_G}(T(u)) = M_{B_G B'_G}(U) M_{B_G}(T) M_{B'_G B_G}(U) = (M_{B'_G B_G}(U))^{-1} M_{B_G}(T) M_{B'_G B_G}(U)$$

which is exactly the conjugate of a matrix.

Definition 3.1.8. Two matrices A and B in $M_n(R)$ are **similar** if there exists some invertible $U \in M_n(R)$ s.t. $A = U^{-1}BU$. Two R-linear maps T and $T' : F \to F'$ are **similar** if there exists some isomorphism φ s.t. $T' = \varphi^{-1} T \varphi$.

Remark 3.1.9. Similarity is an equivalence relation, with $(A = U^{-1}BU) \wedge (B = V^{-1}CV) \implies A = (VU)^{-1}C(VU)$ for transitivity.

R-linear maps are similar to each other if and only if the corresponding matrix is similar, as on free modules linear maps can be represented by matrices.

Proposition 3.1.10. There exists a canonical bijection between:

$$\{R\text{-linear endomorphisms } F \to F\}/\text{similarity} \simeq M_n(R)/\text{similarity}$$

Proof. Choose B_F to be a basis of F. First verify that the map is bijective: as is formalized above since F is free, with a fixed basis linear transformations could be represented via matrices to indicate how the basis is transformed. Therefore, for any linear transformation there exists one matrix to represent it under B_F and vice versa. Further the choice of M_n is unique as matrices under different basis are conjugate w.r.t. the change of basis matrix. □

Remark 3.1.11. The bijection will still be valid without the quotient. However this will cease to be canonical as the map differs by the choice of basis on which the matrix conducts the representation.

3.2 Rational and Smith Normal Form

The main idea of this section is to classify (and represent) linear transformations up to similarity. The construction seeks to embed a specific map into the module structure.

Let k be a field, with V a finite-dimensional k-vector space. Let T be an endomorphism of V. Then (V, T) could be viewed as an $k[x]$-module via specifying that $xu := T(u)$ for all $u \in V$.

Remark 3.2.1. Since the only difference in module structure introduced by (V, T) from V is the application of T when multiplying by x, submodules are preserved as long as it is closed w.r.t. T. That is, for all $W \subseteq V$ k-vector subspaces, $W \subseteq V$ is a $k[x]$-submodule as long as $T(W) \subseteq W$.

Proposition 3.2.2. $(V, T) \simeq (V, T')$ if and only if T and T' are similar.

Proof. Proceed via showing implication in both directions:

$\Rightarrow$ Suppose that there exists isomorphism φ from (V, T) to (V, T'). Then for $u \in V$ consider

$$\varphi(T(u)) = \varphi(xu) = x\varphi(u) = T'(\varphi(u)) \implies T(u) = \varphi^{-1}(T(\varphi(u)))$$

which implies that T and T' are similar.

$\Leftarrow$ If T and T' are similar, there exists some isomorphism φ s.t. $T' = \varphi^{-1} \circ T \circ \varphi$. Then φ gives an isomorphism from (V, T) to (V, T') with the same process as above.

□

Since $k[x]$ is a PID, applying Structural Theorem gives $V \simeq k[x]^n \oplus k[x]/(f_1) \oplus \cdots \oplus k[x]/(f_r)$. Since $k[x]$ is of infinite dimension if viewed as a k-vector space, $n = 0$, which gives

$$V \simeq k[x]/(f_1) \oplus \cdots \oplus k[x]/(f_r), \quad f_1 \mid \cdots \mid f_r \tag{$*$}$$

To make the representation canonical, fix f_is to be monic, i.e. the leading coefficients for f_is are 1 for all i.

Now consider the matrix representation of applying T on V. It is sufficient to consider the situation under $k[x]/(f_i)$, as V is isomorphic to the direct sum of some copies of this, which only differs in f_is chosen. This gives the following definition:

Definition 3.2.3 (Companion Matrix). Let $f = a_0 + a_1 x + \ldots + a_{d-1}x^{d-1} + x^d$. Then multiplication by x (application of T) is represented as

$$\mathcal{C}_{f_i} = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & \ddots & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{d-1} \end{pmatrix}$$

which is the **companion matrix** of f.

Definition 3.2.4 (Rational Canonical Form). A matrix $A \in M_n(k)$ is in **rational canonical form** if it is in the form of

$$\begin{pmatrix} \mathcal{C}_{f_1} & & 0 \\ & \ddots & \\ 0 & & \mathcal{C}_{f_r} \end{pmatrix}, \qquad f_1 \mid \cdots \mid f_r, \quad f_i \text{ monic}, \quad \deg f_i \geq 1 \; \forall \, i$$

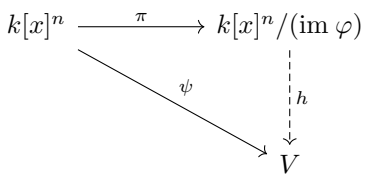
Then choosing basis to be $x^n \in k[x]/(f_i)$ s.t. $n < \deg f_i$ and appending the basis of the summands gives the matrix of T in rational canonical form. Note that this is a basis as a k-vector space, but is not one for V as a $k[x]$-module.

Remark 3.2.5. $T, T' \in \mathrm{End}_K V$ are similar if and only if they can be described in some basis in the same rational canonical form:

Proof. By Remark 3.2.2 this implies that $(V, T) \simeq (V, T')$. Using Eq. $(*)$ gives that they have the same f_is in $(*)$, i.e. they have the same rational canonical form. □

Proposition 3.2.6. Let V be a finite-dimensional k-vector space with basis $B_V = (u_1, \ldots, u_n)$. Let (V, T) be the extension into $k[x]$-module with $T \in \mathrm{End}_K(V)$, and A be the matrix representation of T using basis B_V. Consider $\varphi : k[x]^n \to k[x]^n$ s.t. it is represented by $(x\mathrm{Id}_n - A)$ in the canonical basis. Then $V \simeq k[x]^n/(\mathrm{im}\, \varphi)$; and φ is injective.

Proof. Consider the following commutative diagram:



Specify $\psi : e_i \mapsto u_i \; \forall \, i$. To prove that $V \simeq k[x]^n/(\mathrm{im}\, \varphi)$ it suffices to verify that $\ker \psi = \mathrm{im}\, \varphi$. Proceed via showing inclusion in both directions:

$\supseteq$: It suffices to verify that for all j, $\psi(\varphi(e_i)) = 0$. Applying the definition of the maps gives

$$\psi(\varphi(e_i)) = \psi(xe_i - \sum_{j=1}^{n} a_{ij} e_j) = x\psi(e_i) - \sum_{j=1}^{n} a_{ij}\psi(e_j) = T(u_i) - T(u_i) = 0$$

$\subseteq$: Specify $h : \bar{e}_i \mapsto u_i$. $\ker \psi \supseteq \mathrm{im}\, \varphi$ gives that h is surjective. Notice that h is an isomorphism between $k[x]$-modules if and only if h is an isomorphism of k-vector spaces that are closed w.r.t. multiplication by x (or application of T). Therefore, to show that h is an isomorphism it suffices to show that the k-linear span of $\bar{e}_i$s is $k[x]^n/(\mathrm{im}\, \varphi) =: U$.

It suffices to verify that $x^m \bar{e}_i \in U$. Proceed via induction:

- *Base case.* e_i by definition is in the span of e_is for all i.
- *Inductive step.* Suppose that $x^k \bar{e}_i \in U$. Since φ is a map of free $k[x]$-modules, $U \simeq \ker \varphi$, which gives

$$\varphi(e_i) = (xI_n - A)e_i = xe_i - \sum_{j=1}^{n} a_{ij} e_j = x^m e_i - \sum_{j=1}^{n} x^{m-1} a_{ij} e_j = 0$$

i.e. $x^m e_i$ is spanned by $(x^{m-1} a_{ij} e_j)$s, which by inductive hypothesis are in k-linear span of e_is.

It remains to show that φ is injective. Since $\operatorname{rank}_{k[x]}(V) = 0$, by $V \simeq k[x]^n/(\operatorname{im}\varphi)$, $\operatorname{rank}(\operatorname{im}\varphi) = \operatorname{rank}(k[x]^n) = n$. But notice $k[x]^n/\ker\varphi \simeq \operatorname{im}\varphi$, i.e. $\operatorname{rankker}\varphi = \operatorname{rank}k[x]^n - \operatorname{rankim}\varphi = 0$. But $\ker\varphi$ as a submodule of $k[x]$ is free, which implies that $\ker\varphi = \{0\}$, i.e. φ is injective. □

The map $(x\mathrm{Id}_n - A)$ is important as it annihilates the torsion module of modules on $k[x]$, it reveals the information of f_is. Specifically, for each summand in the direct sum of $\bigoplus_i k[x]/(f_i)$, f_i is the minimal annihilator of the whole module.

Definition 3.2.7 (Smith Normal Form)**.** Let (V, T) be a $k[x]$-module where V is a finite-dimensional k-vector space, and $T \in \operatorname{End}_k(V)$. Let the matrix representation of T in a certain basis to be A. The **Smith Normal Form** of $(x\mathrm{Id}_n - A) =: M$, is a matrix in the form of

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & f_1 & \\ & & & \ddots \\ & & & & f_r \end{pmatrix} \qquad f_1 \mid \cdots \mid f_r, \quad f_i \text{ monic}, \quad \deg f_i \geq 1 \; \forall\, i$$

s.t. it can be transformed from M via the following transformations:

1. Swap the rows/columns of M.
2. Multiply a row/column of M by $\lambda \in k \setminus \{0\}$.
3. Add one row/column of M multiplied by $f \in k[x]$ to another row/column.

The f_is are called elementary divisors, or invariant factors.

Remark 3.2.8. The valid operations allowed in making the transformation of M are the same as applying invertible transformation, with column/row operations corresponding to manipulation of basis in the source/image.

Multiplication of one row is only allowed up to non-zero elements in k as $k[x]$ is not a domain, where multiplication is not invertible.

Remark 3.2.9. It could be read off from the matrix that $\operatorname{Ann}_{k[x]}(V) = \{g \in k[x] : f_i \mid g \; \forall\, i\}$, as there are no 1 elements on the diagonal of the matrix.

3.3 Minimal and Characteristic Polynomials

Return to the case where V is a finite-dimensional k-vector space; and morphisms are considered in the context of $k[x]$-modules. Recall that the structure of V, given as a $k[x]$-module, is

$$V \simeq k[x]/(f_1) \oplus \cdots \oplus k[x]/(f_r), \quad f_1 \mid \cdots \mid f_r$$

Definition 3.3.1 (Minimal Polynomial)**.** The **minimal polynomial** of $T \in \operatorname{End}_k(V)$ is the monic generator of $\operatorname{Ann}_{k[x]}(V)$, denoted to be $m_T(x)$. Expressing V in the form of Eq. (∗), or using Smith Normal Form, $m_T(x) = f_r$.

Definition 3.3.2 (Characteristic Polynomial). Let $A \in M_n(k)$. The **characteristic polynomial** of A is given as $c_A(x) = \det(x\mathrm{Id}_n - A) \in k[x]$.

Remark 3.3.3. Inheriting the notations in Smith Normal Form of V, $c_T(x) = f_1 \dots f_r$.

Remark 3.3.4. If $A \sim A'$, then $m_A(x) = m_{A'}(x)$, and $c_A(x) = c_{A'}(x)$; but the converse does not necessarily hold.

Remark 3.3.5. Since the minimal/characteristic polynomial is defined on the structure or invariant factors in Smith Normal Form, they are invariant w.r.t. change of basis.

Definition 3.3.6 (Eigenvalue). Given $T \in \mathrm{End}_k(V)$, λ is an **eigenvalue** of T if the following equivalent conditions are satisfied:

- There exists some $v \in V \setminus \{0\}$ s.t. $\lambda v = Tv$, i.e. $(\lambda\mathrm{Id} - T)v = 0$.
- $\det(\lambda\mathrm{Id} - T)v = 0$, i.e. $c_T(\lambda) = 0$.

Proposition 3.3.7. If $(V, T) \simeq \bigoplus_{i=1}^r k[x]/(f_i)$ where f_is are the invariant factors of T as a morphism of $k[x]$-modules. Then $c_T(x) = \Pi_{i=1}^r f_i$.

Proof. There exists some basis in which V is in the rational canonical form. Then $c_T(x) = \Pi_{i=1}^r \det \mathcal{C}_{f_i}$. It then suffices to show that $\det \mathcal{C}_{f_i} = f_i$ for all i. Notice

$$\det \begin{pmatrix} x & & 0 & a_0 \\ -1 & \ddots & & a_1 \\ & \ddots & x & \vdots \\ 0 & & -1 & x + a_{d-1} \end{pmatrix} = x \begin{pmatrix} x & & 0 & a_1 \\ -1 & \ddots & & a_2 \\ & \ddots & x & \vdots \\ 0 & & -1 & x + a_{d-1} \end{pmatrix} + \underbrace{a_0 \cdot (-1)^{n+1} \cdot (-1)^{n-1}}_{a_0}$$

where, performing finitely many (d) steps recovers the full polynomial. □

Remark 3.3.8. This proposition is also a direct result of the existence of Smith Normal Form, as after finitely many elementary row/column operations which do not change the determinant, $(x\mathrm{Id}_n - A)$ has f_is and 1s on the diagonal; and the result is given via simply multiplying all of them.

The conclusion is that for $V \simeq k[x]/(f_1) \oplus \cdots \oplus k[x]/(f_r)$, $\quad f_1 \mid \cdots \mid f_r$ where $f_1 \mid \cdots \mid f_r$, $m_T = f_r$; and $c_T = f_1 \dots f_r$. This gives

$$m_T \mid c_T, \qquad c_T \mid m_T^r$$

Further, since f_r is the monic generator of $\mathrm{Ann}_{k[x]}(V)$, $m_T(T)(u) = f_r \cdot u = 0$ for all $u \in V$, i.e. $m_T(T) = 0$. Since $m_T \mid c_T$, $c_T(T) = 0$, which is the result from Cayley-Hamilton.

Remark 3.3.9. Notice that the structure of V is closely connected to that of T. Since application of $k[x]$ is specified by T; and V is a k-vector space, i.e. no element in k annihilates non-zero elements in V, $\mathrm{Ann}_{k[x]}(V) = \mathrm{Ann}_{k[x]}(T)$.

3.4 Jordan Normal Form

Parenthesis 3.4.1. Let f be monic in $k[x]$. Then

1. $k = \mathbb{C}$. Then irreducible polynomials f has form $f = x - a$ for some $a \in \mathbb{C}$.
2. $k = \mathbb{R}$. Then f irreducible takes either of the following forms:
   - $f = x - a$ for $a \in \mathbb{R}$.
   - $f = (x - \lambda)(x - \bar{\lambda})$ for $\lambda \in \mathbb{C}$.

Proof. 1.) follows directly from the fact that $\mathbb{C}$ is algebraically closed. 2.) follows from the fact that if f is of degree higher than 1, it must admit a root in $\mathbb{C}$, which indicates that the conjugate of that is also a root. Otherwise this is the case as in $\mathbb{C}$. □

Remark 3.4.2. This classification is harder for $\mathbb{Q}$, as it is easy to construct a polynomial with all of its roots being irrational numbers.

Now consider k to be an algebraically closed field, i.e. all irreducible factors of $f \in k[x]$ are of degree 1. Then applying Structural Theorem gives

$$M \simeq \bigoplus_{i=1}^{s} k[x]/(x - \lambda_i)^{m_i}$$

Now adopt the basis $\overline{(x - \lambda_i)^{m_i - 1}}, \ldots, \overline{x - \lambda_i}, 1$ s.t. multiplication by x on polynomials of degree $m_i - 1$ can be represented by a single entry on the matrix. Then the alternative transition companion matrix is

$$\widetilde{\mathcal{C}_f} = \begin{pmatrix} \lambda_i & 1 & & 0 \\ 0 & \ddots & \ddots & \\ \vdots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & \lambda_i \end{pmatrix} =: J_i$$

which is a **Jordan block**. Therefore, combination of such basis in each summands of V gives the matrix in **Jordan Canonical Form** or **Jordan Normal Form**:

$$T = \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_s \end{pmatrix}$$

Definition 3.4.3. A matrix M is **diagonalizable** if it is similar to a diagonal matrix (or equivalently its Jordan Normal Form is diagonal). A linear transformation is **diagonalizable** if it can be represented by a diagonal matrix in some basis.

Remark 3.4.4. A matrix has a Jordan Normal Form where all Jordan blocks are of size 1 is diagonal.

Proposition 3.4.5. $T \in \mathrm{End}_k(V)$ is diagonalizable if and only if m_T splits as a product of distinct degree-1 monic polynomials.

Proof. Proceed via showing implication in both directions:

$\Rightarrow$: Prove the contraposition. Suppose that m_T does not split into distinct monic polynomials. Then the summands of direct sum of M includes $k[x]/(x-\lambda_i)m_i$ for $m_i \geq 2$, i.e. there exists a Jordan block of size greater than 1, which indicates that T is not diagonalizable.

An alternative proof for this part would be to consider $p(x) = \prod_{i=1}^{r}(x-\lambda_i)$, which gives $p(A) = 0$. Since p splits, and m_T generates p, $m_T \mid p$, i.e. m_T splits.

$\Leftarrow$: Suppose that m_T splits. Then $V \simeq \bigoplus_{i=1}^{r} k[x]/(f_i)$ where f_r splits. Since $f_i \mid f_r$ for all i, f_i splits; and by Chinese Remainder Theorem $M = \bigoplus_{i=1}^{s} k[x]/(f_i)$ where f_is are not necessarily different. Then all Jordan blocks of T are of size 1.

□

Remark 3.4.6. Given a linear transformation T with its matrix representation A. Then

$$c_T(x) = x^n - \operatorname{tr}(A)x^{n-1} + \cdots + (-1)^n \det A$$

which is clear via considering the permutation of elements in A.

Chapter 4

Categories and Functors

4.1 Category; Functor

Definition 4.1.1 (Category). A **category** $\mathscr{C}$ consists of

- A class of objects $\mathscr{C}$ (which, for example, could contain all sets), denoted $\mathrm{Ob}(\mathscr{C})$.
- For all $A, B \in \mathrm{Ob}(\mathscr{C})$, a set $\mathrm{Hom}_{\mathscr{C}}(A, B)$ the "morphisms in $\mathscr{C}$ from A to B" with map $\mathrm{Hom}_{\mathscr{C}}(A, B) \times \mathrm{Hom}_{\mathscr{C}}(B, C) \to \times \mathrm{Hom}_{\mathscr{C}}(A, C)$ the "morphism composition" denoted $f \times g \rightsquigarrow (g \circ f)$, satisfying
  - *Existence of an identity.* for all $A \in \mathrm{Ob}(\mathscr{C})$, there exists $1_A \in \mathrm{Hom}_{\mathscr{C}}(A, A)$ s.t.

$$\begin{cases} 1_A \circ f = f & \forall f \in \mathrm{Hom}_{\mathscr{C}}(A, B) \\ g \circ 1_A = g & \forall g \in \mathrm{Hom}_{\mathscr{C}}(B, A) \end{cases}$$

  - *Associativity.* For all $f \in \mathrm{Hom}_{\mathscr{C}}(A, B), g \in \mathrm{Hom}_{\mathscr{C}}(B, C), h \in \mathrm{Hom}_{\mathscr{C}}(C, D)$,

$$(h \circ g) \circ f = h \circ (g \circ f)$$

Remark 4.1.2. The definition much resembles previous algebraic structures; but the morphisms and composition laws could be defined in a particularly strange way:

1. Similar to monoids, the definition implies that the identity is unique. Suppose that there are two identities $1_A, 1'_A \in \mathrm{Hom}_{\mathscr{C}}(A, A)$ for $A \in \mathrm{Ob}(\mathscr{C})$, then $1_A = 1_A \circ 1'_A = 1'_A$.
2. The morphism is not necessarily a function; and in such cases composition needs to be re-defined respectively.

Example 4.1.3. Consider the following categories:

- *Category of Sets* Sets, where the objects are sets, and morphisms are maps between sets.
- *Category of Rings* Rings, where the objects are rings, and morphisms are ring homomorphisms.
- *Category of (left) R-modules* ${}_R\mathrm{Mod}$, where objects are lef R-modules, and morphisms R-linear maps.

- Consider the category $\mathscr{C}$ defined on a partially-ordered set $(A, \leq)$ where
  - $\mathrm{Ob}(\mathscr{C})$ consists of elements in A.
  - Morphisms are defined as
    $$\mathrm{Hom}_{\mathscr{C}}(A, B) = \begin{cases} \{*\} & A \leq B \\ \emptyset & \text{otherwise} \end{cases}$$
    where the composition of maps is defined as intersection. This is due to the fact that there can be no maps whose image is the empty set.

Definition 4.1.4 (Functor). Let $\mathscr{C}$ and $\mathscr{D}$ be categories. The **functor** $F : \mathscr{C} \to \mathscr{D}$ consists of mappings for both objects and morphisms:

- For all $A \in \mathrm{Ob}(\mathscr{C})$, $F(A) \in \mathscr{D}$.
- For all $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$. $F(f) \in \mathrm{Hom}_{\mathscr{D}}(F(A), F(b))$ s.t.
  - $F(1_A) = 1_{F(A)}$ for all $A \in \mathrm{Ob}(\mathscr{C})$.
  - For all $f \circ g$ where $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$, $g \in \mathrm{Hom}_{\mathscr{C}}(B, C)$, $F(f \circ g) = F(f) \circ F(g)$.

The composition of functors is conducted in a natural way, i.e. applying consecutively.

Example 4.1.5. Functors represent the induced maps w.r.t. a transformation in the structure:

1. Let R be a commutative ring and $S \subseteq R$ a multiplicative system. Consider the functor $F : {}_R\underline{\mathrm{Mod}} \to {}_{S^{-1}R}\underline{\mathrm{Mod}}$ where
   - $F(M) = S^{-1}M$ for all $M \in \mathrm{Ob}({}_R\underline{\mathrm{Mod}})$.
   - For $f : M \to N$, define $F(f) := S^{-1}M \to S^{-1}N$, where $\frac{u}{s} \mapsto \frac{f(u)}{s}$.
2. Let R be a ring, with $I \subseteq R$ a two-sided ideal of R; and M a left R-module. Consider the functor $F : {}_R\underline{\mathrm{Mod}} \to {}_{R/I}\underline{\mathrm{Mod}}$ where
   - $F(M) = M/IM$ for all $M \in \mathrm{Ob}({}_R\underline{\mathrm{Mod}})$.
   - Let $f : M \to N$ be a morphism of left R-modules. Then it induces a map $\bar{f} : M/IM \to N/IN$ s.t. $\bar{f}(\bar{(u)}) = \overline{f(u)}$. Define $F(f) = \bar{f}$.
3. Functors generally can abandon structures. Let M be a left R-module. By definition it is valid to view M as an abelian group. Then functor $F : {}_R\underline{\mathrm{Mod}} \to \underline{\mathrm{Ab}}$ where objects are taken to itself; and morphisms are taken to group homomorphisms. These are called *forgetful functors*.

4.2 Morphism of Categories

The dual of a category is where the direction of morphisms is inverted. The following gives a formalization of this:

Definition 4.2.1 (Contravariant Functor). A **contravariant functor** $F : \mathscr{C} \to \mathscr{D}$ is a functor which maps composition to that in the inverse order, i.e.

- For all $A \in Ob(\mathscr{C})$, $F(A) \in \mathrm{Ob}(\mathscr{D})$.

- For all $f \in \mathrm{Hom}_{\mathscr{C}}(A, B), F(f) \in \mathrm{Hom}_{\mathscr{C}}(F(B), F(A))$ s.t.
  - $F(1_A) = 1_{F(A)}$ for all $A \in \mathrm{Ob}(\mathscr{C})$.
  - For all $f \circ g$ where $f \in \mathrm{Hom}_{\mathscr{C}}(A, B), g \in \mathrm{Hom}_{\mathscr{C}}(B, C), F(f \circ g) = F(g) \circ F(f)$.

Definition 4.2.2 (Dual Category). Let $\mathscr{C}$ be a category. Then the **dual category** $\mathscr{C}^\circ$ of $\mathscr{C}$ is a category with

- $\mathrm{Ob}(\mathscr{C}) = \mathrm{Ob}(\mathscr{C}^\circ)$.
- $\mathrm{Hom}_{\mathscr{C}}(A, B) = \mathrm{Hom}_{\mathscr{C}^\circ}(B, A)$.

The composition is compatible as the inversion is done in the functor.

Remark 4.2.3. Since the dual category is defined on the contravariant of the functor, replacing a functor with its contravariant is equivalent to replacing the category with its dual.

Similar to the case of modules we can define the *Hom Functors*; but as a concept one level up it leaves the image unspecified:

Definition 4.2.4 (Hom Functor). Let $\mathscr{C}$ be a category, and $A \in \mathrm{Ob}(\mathscr{C})$. Then the **Hom functor** $\mathrm{Hom}_{\mathscr{C}}(A, -) : \mathscr{C} \to \underline{\mathrm{Sets}}$ where

- For $B \in \mathrm{Ob}(\mathscr{C}), F(B) = \mathrm{Hom}_{\mathscr{C}}(A, B)$.
- For $f : \mathrm{Hom}_{\mathscr{C}}(B_1, B_2), F(g) : \mathrm{Hom}_{\mathscr{C}}(A, B_1) \to \mathrm{Hom}_{\mathscr{C}}(A, B_2), g \mapsto f \circ g$.

Remark 4.2.5. Similarly, we can consider the contravariant functor of the Hom functor. $\mathrm{Hom}_{\mathscr{C}^\circ}(-, A) : \mathscr{C}^\circ \to \underline{\mathrm{Sets}}$. By definition $\mathrm{Hom}_{\mathscr{C}}(A, -) = \mathrm{Hom}_{\mathscr{C}^\circ}(-, A)$.

Remark 4.2.6. Let $\mathscr{C} = {}_R\underline{\mathrm{Mod}}$. Then $\mathrm{Hom}_{\mathscr{C}}(X, -)$ could be lifted to $\mathscr{C} \to \underline{\mathrm{Ab}}$. It can be further lifted to $\mathscr{C} \to {}_R\underline{\mathrm{Mod}}$ if R is commutative, which ensures that the morphisms will be R-linear. In this case this is just the Hom Module of (left) R-modules.

Definition 4.2.7. Let $\mathscr{C}$ be a category. Then $u \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ is an **isomorphism** if there exists $v \in \mathrm{Hom}_{\mathscr{C}}(B, A)$ s.t. $u \circ v = \mathrm{Id}_B, v \circ u = \mathrm{Id}_A$.

Remark 4.2.8. For a fixed u, such v is unique. Suppose that there exists two distinct vs, we have

$$v = v \circ \mathrm{Id}_B = v \circ (u \circ v') = (v \circ u) \circ v' = v'$$

which is a contradiction.

Remark 4.2.9. Let $F : \mathscr{C} \to \mathscr{D}$ a functor. Then $u \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ being an isomorphism implies that $F(u)$ is an isomorphism.

This results from the fact that $\mathrm{Id}_{F(B)} = F(\mathrm{Id}_B) = F(u \circ v) = F(u) \circ F(v)$. Result for A is similar; and uniqueness follows from the same reasoning.

Definition 4.2.10. Let $\mathscr{C}$ be a category:

- $X \in \mathrm{Ob}(\mathscr{C})$ is an **initial object** if $\forall Y \in \mathrm{Ob}(\mathscr{C}), |\mathrm{Hom}_{\mathscr{C}}(X, Y)| = 1$.
- $X \in \mathrm{Ob}(\mathscr{C})$ is a **final object** if $\forall Y \in \mathrm{Ob}(\mathscr{C}), |\mathrm{Hom}_{\mathscr{C}}(Y, X)| = 1$.
- $X \in \mathrm{Ob}(\mathscr{C})$ is a **zero-object** if it is both an initial object and a final object.

Remark 4.2.11. Let $X \in \mathrm{Ob}(\mathscr{C})$ be an initial (final, zero) object. Then X' is initial (final, zero) if and only if there exists an isomorphism between X and X'.

Proof is similar for all three cases. Suppose that X and X' are both initial. Then there exists a unique $f \in \mathrm{Hom}_{\mathscr{C}}(X, X')$ and $f' \in \mathrm{Hom}_{\mathscr{C}}(X', X)$, i.e. $f' \circ f \in \mathrm{Hom}_{\mathscr{C}}(X, X)$. X being initial implies that this is the unique morphism from X to itself, which contains Id_X. Therefore $f' \circ f = \mathrm{Id}_X$. Similar result holds for $f \circ f' = \mathrm{Id}_{X'}$, which implies that X and X' are isomorphic.

Example 4.2.12. Although if initial/final objects are unique up to isomorphism if they exist, but they actually do not necessarily exist:

1. In ${}_R\underline{\mathrm{Mod}}$, $\{0\}$ is a zero-object.

   The only element in a left R-module that should be preserved in a morphism of R-module is the zero element. For any element $a \neq 0$, there exists two maps that either maps a to 0, or another non-zero element, which indicates that this is not initial.

   Suppose that the final object has (at least) two elements $\{0, a\}$ for $a \neq 0$, then there exists at least two maps from a non-trivial module generated by $(u_1, \cdots, u_r)$ to it: for each u_i it is either mapped to 0 or a, which gives two morphisms.

2. In $\underline{\mathrm{Sets}}$, $\emptyset$ is initial, and $\{*\}$ (a set containing an arbitrary element) is final.

   Suppose that there exists an element in the initial object, then it could be mapped to any element as morphisms of $\underline{\mathrm{Sets}}$do not have constraints.

3. In $\underline{\mathrm{Rings}}$, $\mathbb{Z}$ is initial; and $\{0\}$ is final.

   $\mathbb{Z}$ being initial results from the fact that ring homomorphisms are required to preserve the 0 and 1 elements; and the maximal ring generated by $(0, 1)$ is isomorphic to $\mathbb{Z}$.

4. In $\underline{\mathrm{Fields}}$, there are no initial or final objects.

   This results directly from the fact that $1 \neq 0$ in fields. For every two fields, there exists two maps: one that maps 1 to 1; and the other maps 1 to 0.

Definition 4.2.13. Let $\mathscr{C}$ be a category. $u \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ is a **monomorphism** if for all $C \in \mathrm{Ob}(\mathscr{C})$ and $v_1, v_2 \in \mathrm{Hom}_{\mathscr{C}}(C, A)$ s.t. $u \circ v_1 = u \circ v_2$ implies $v_1 = v_2$. $u \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ is an **epimorphism** if for all v_1, v_2 with the same comdition above satisfies $v_1 \circ u = v_2 \circ u$ implies $v_1 = v_2$, i.e. it is a monomorphism in $\mathscr{C}^{\circ}$.

Remark 4.2.14. These are analogies of injective/surjective in the context of category. Since on the category level it is only valid to consider objects or morphisms, such analogies could be only made to morphisms.

Example 4.2.15. It is not always the case that monomorphisms could correspond to injective maps, and epimorphisms could correspond to surjective maps:

1. In Sets, monomorphisms correspond to injective maps, and epimorphisms correspond to surjective maps.
2. In ${}_R\text{Mod}$, such analogy is still true via choosing the v_1, v_2:

$$\ker u \overset{\text{incl.}}{\underset{0}{\rightrightarrows}} A \xrightarrow{u} B \qquad\qquad A \xrightarrow{u} B \overset{\pi}{\underset{0}{\rightrightarrows}} B/\text{im } u$$

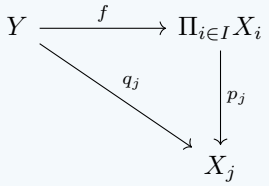
   - For u being a monomorphism, $u(\ker u) = u(0) = 0$, i.e. the inclusion map from $\ker u$ to A is the same as the zero map, i.e. $\ker u = \{0\}$.
   - For u being an epimorphism, $\pi(u(A)) = 0$ in $B/\text{im } u$, i.e. $\pi(B) = 0$ which indicates that $\text{im } u = B$.

3. In Rings, monomorphisms are still injective, via for $f : R \to S$ considering $\mathbb{Z}[x] \overset{x\mapsto u}{\underset{0}{\rightrightarrows}} R \xrightarrow{f} S$ for all $u \in \ker f$. This implies that $u = 0$, i.e. $\ker f = \{0\}$.

   But epimorphisms in rings are not necessarily surjective. Take the example $\alpha : \mathbb{Z} \hookrightarrow \mathbb{Q}$ which is the inclusion map. This is an epimorphism as $v_1 \circ \alpha = v_2 \circ \alpha$ if and only if 1 is mapped to the same element; but this always holds as ring homomorphisms preserve the multiplicative unit.

4.3 Product and Coproduct

Definition 4.3.1 (Product). Let $\mathscr{C}$ be a category, with $(X_i)_{i\in I}$ a family of objects in $\mathscr{C}$. Then the **product** of this family is given by an object $\Pi_{i\in I}X_i$ where for all $Y \in \text{Ob}(\mathscr{C})$, with morphisms $q_j : Y \to X_j$ for $j \in I$, there exists a unique morphism f s.t. $q_j = p_j \circ f$ for all j, i.e. the following diagram commute. The p_j is the projection morphism, where $p_j(\Pi_{i\in I}x_i) = x_i$.



Remark 4.3.2. Product of a family of objects is unique up to isomorphism. Suppose that there exists another product X' which satisfies the criterion for being a product. Then there exists unique φ and φ' s.t.

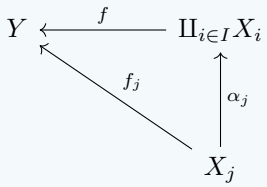
$$\varphi : X \to X' \qquad \varphi' : X' \to X$$

since both f and f' are unique. But this gives

$$\begin{cases} p_j = p'_j \circ \varphi' \\ p'_j = p_j \circ \varphi \end{cases} \implies \exists \varphi, \varphi' \text{ s.t. } \begin{cases} \varphi \circ \varphi' = \text{Id}_{X'} \\ \varphi' \circ \varphi = \text{Id}_X \end{cases}$$

By uniqueness this gives that X and X' must be isomorphic.

Definition 4.3.3 (Coproduct). Given a family $(X_i)_{i\in I} \in \mathrm{Ob}(\mathscr{C})$, the coproduct $\amalg_{i\in I} X_i$ is the product in the dual category, i.e. with all the arrow reversed. That is, for $Y \in \mathrm{Ob}(\mathscr{C})$ and $f_j : X_j \to Y$, denote α_j to be the natural embedding of X_j into the product $\amalg_{i\in I} X_i$, then there exists a unique f s.t. $f \circ \alpha_j = f_j$ for all j, i.e. the following diagram commute:



Remark 4.3.4. In Sets, the product is given by Cartesian product, and the coproduct is given by disjoint union. Notice the difference: projection has no corresponding morphism from disjoint union; and so is natural embedding into Cartesian product.

In ${}_R$Mod, the coproduct is given by the direct sum; and the product is given by the direct product.

Remark 4.3.5. Product in the context of categories provides a generalization of Cartesian product, where specifying morphisms into the product gives the morphisms into each of its components. Coproduct, being the dual notion of product, simply "reverses the arrows", i.e. specifying morphisms from the coproduct gives morphisms from each of its components.

Definition 4.3.6 (Preadditive Category). A **preadditive category** $\mathscr{C}$ is a category s.t. its morphisms form an abelian group, and is bilinear w.r.t. composition.

Remark 4.3.7. Rings is not a preadditive category, as its morphisms do not have a zero element (since ring homomorphisms are required to map 1 to 1.) ${}_R$Mod, with out such constraint, is a preadditive category.

Definition 4.3.8 (Additive Functor). Let $\mathscr{C}$ and $\mathscr{D}$ be preadditive categories. $F : \mathscr{C} \to \mathscr{D}$ is an **additive functor** if for all $A, B \in \mathrm{Ob}(\mathscr{C})$, F w.r.t. morphisms is a group homomorphism.

Remark 4.3.9. The definition of "linear", or "group homomorphism" implicitly requires that the underlying structure should have a valid operation. Those who don't, for example Sets, are naturally excluded from such discussion.

Example 4.3.10. Let R be a commutative ring and $I \subseteq R$ an ideal. Then the functor

$$F : {}_R\mathrm{Mod} \to {}_R\mathrm{Mod}, \qquad M \mapsto M/IM$$

is an additive functor. This results from the fact that morphism of R-modules $M \to N$ and the quotient morphism are both R-linear.

Remark 4.3.11. Let $\mathscr{C}$ be a preadditive category. Then

1. If $X \in \mathrm{Ob}(\mathscr{C})$ is an initial/final object, then it is a zero object.

   Consider $\mathrm{Hom}_{\mathscr{C}}(X, X)$. Since $\mathscr{C}$ is preadditive, this forms a group of one element, which is zero. Therefore for all $f \in \mathrm{Hom}_{\mathscr{C}}(X, X)$ this gives $f = 1_X \circ f = 0 \circ f = 0$. This immediately implies that X is a zero object, as for all $g \in \mathrm{Hom}_{\mathscr{C}}(Y, X)$, $h \in \mathrm{Hom}_{\mathscr{C}}(X, Y)$

   $$g = g \circ 1_X = g \circ 0 = 0, \qquad h = 1_X \circ h = 0 \circ h = 0$$

2. $\mathscr{C}$ being preadditive implies that $\mathscr{C}^\circ$ is preadditive, as reversing the arrow does not interfere with the group structure, or the additive property.

3. Let $F : \mathscr{C} \to \mathscr{D}$ an additive functor, with $\mathscr{C}$ and $\mathscr{D}$ preadditive categories. Then for $0 \in \mathrm{Ob}(\mathscr{C})$ the zero object in $\mathscr{C}$, $F(0)$ is also the zero object in $\mathscr{D}$.

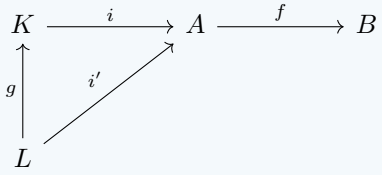
   This results directly from the fact that group homomorphisms map 0 to 0; and by the first point in the remark, an object X is zero if and only if $1_X = 0$ in $\mathrm{Hom}_{\mathscr{C}}(X, X)$.

4.4 Kernel and Cokernel

Throughout the discussion, fix $\mathscr{C}$ to be a preadditive category.

Definition 4.4.1 (Kernel). Let $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$. The **kernel** of f is a morphism $i : K \to A$ s.t.

- $f \circ i = 0$.
- f is universal with this property (factors uniquely through i), i.e. for $i' : L \to A$, there exists a unique morphism $g : L \to K$ s.t. $i' = i \circ g$:



Remark 4.4.2. Using exactly the same reasoning as in products, the kernel of a morphism is unique up to isomorphism. Adopting the same notation as above, consider i' to be the kernel. Then there exists a unique $g' : K \to L$ s.t. the diagram commute, which gives $g \circ g' = \mathrm{Id}$.

Remark 4.4.3. Let $i : K \to A$ be the kernel. Then i is a monomorphism.

This follows directly from the uniqueness in the universal property. Suppose that there exists $f_1, f_2 : V \to K$ s.t. $i \circ f_1 = i \circ f_2 = g$, then $g : V \to F$ factors uniquely through i, i.e. there exists a unique h s.t. $g = i \circ h$. This implies that $f_1 = f_2 = h$.

Example 4.4.4. The kernel often comes with an associated K, which is the kernel in the algebraic sense.

Take $M, N \in \mathrm{Ob}({}_R\underline{\mathrm{Mod}})$, and $f : M \to N$ is a morphism of R-modules. Then naturally one can construct the following s.t. $g = \ker f$.

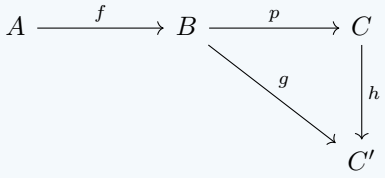
$$\ker f \xhookrightarrow{g} M \xrightarrow{f} N$$

Definition 4.4.5 (Cokernel). The **cokernel** of f is the kernel in the dual category, which effectively annihilates a morphism.

Explicitly, let $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$, $p \in \mathrm{Hom}_{\mathscr{C}}(B, C)$. p is the cokernel of f if

- $p \circ f = 0$.

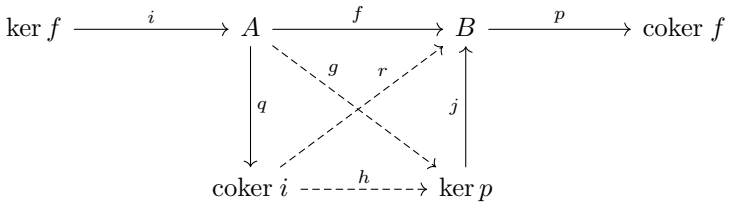
- For all $g : B \to C'$, there exists a unique morphism $h : C \to C'$ s.t. $g = h \circ p$; i.e. any cokernel of f factors uniquely through p:



Remark 4.4.6. The dual argument w.r.t. kernel holds. That is, if cokernel exists, it is unique up to isomorphism; and cokernel is always an epimorphism.

Example 4.4.7. Let $f : M \to N$ be a morphism of ${}_R\underline{\mathrm{Mod}}$. Then the cokernel of f is given via $\pi : N \to N/\mathrm{im}\ f$ which is the quotient map.

It is in particular interesting to put in juxtaposition of the two concepts. Let $\mathscr{C}$ be a preadditive category, and for all morphisms in $\mathscr{C}$ its kernel and cokernel exist. Then consider the following commutative diagram:



The universal property of kernel and cokernel gives:

- f factors uniquely through q, i.e. there exists a unique r s.t. $f = r \circ q$.
- f factors uniquely through j, i.e. there exists a unique g s.t. $f = j \circ g$.
- g factors uniquely through q, i.e. there exists a unique h s.t. $g = h \circ q$.

Combining these gives the uniqueness of h s.t. $f = j \circ h \circ q$.

Remark 4.4.8. This resembles the first isomorphism theorem.

In ${}_R\underline{\mathrm{Mod}}$, it is given that $\mathrm{coker}\ i = A/\ker f$, and $\ker p = B/(B/\mathrm{im}\ f) \simeq \mathrm{im}\ f$, which is exactly the first isomorphism theorem.

Definition 4.4.9 (Additive Category)**.** An **additive category** $\mathscr{C}$ is a preadditive category s.t.

- $\mathscr{C}$ has a zero object.
- $\forall X, Y \in \mathrm{Ob}(\mathscr{C})$, the product $X \times Y$ exists (and it's isomorphic to their coproduct).

Definition 4.4.10 (Abelian Category)**.** An **abelian category** is an additive category $\mathscr{C}$ s.t.

- Every morphism has a kernel and a cokernel.
- "The first isomorphism theorem holds", i.e. for f considered as above, the morphism $h : \mathrm{coker}\ i \to \ker p$ is an

isomorphism.

4.5 Natural Transformation of Functors

Definition 4.5.1 (Natural Transformation)**.** Let $F, G : \mathscr{C} \to \mathscr{D}$ be functors. Then the **natural transformation** from F to G $T : F \Rightarrow G$ is given by $T_U : F(U) \to G(U)$ for all $U \in \mathrm{Ob}(\mathscr{C})$ s.t. for all $f : A \to B$ in $\mathscr{C}$ the following diagram commutes:

$$\begin{array}{ccc} F(A) & \xrightarrow{T_A} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow{T_B} & G(B) \end{array}$$

Example 4.5.2. In ${}_R\underline{\mathrm{Mod}}$ where R is commutative, one can consider ideals $I \subseteq J$ the transformation

$$\begin{array}{ccc} M/IM & \xrightarrow{T_A} & M/JM \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ N/IN & \xrightarrow{T_B} & N/JN \end{array}$$

which maps $u \pmod{IM}$ to $u \pmod{JM}$. This is possible as $I \subseteq J$, where no information is missing.

Remark 4.5.3. The trivial natural transformation is simply the identity $\mathrm{Id}_F : F \Rightarrow F$. Via composing the commutative diagrams, it is easy to see that natural transformations is valid through composition.

Definition 4.5.4. A natural transformation $T : \mathscr{C} \to \mathscr{D}$ is an **isomorphism of functors** if for all $A \in \mathscr{C}$, T_A is an isomorphism (in $\mathscr{D}$).

Remark 4.5.5. A natural transformation T is an isomorphism if there exists $T' : G \Rightarrow F$ s.t. $T \circ T' = \mathrm{Id}_F$, $T' \circ T = \mathrm{Id}_G$.

This results from the fact that every isomorphism has an inverse in $\mathscr{D}$; and two natural transformations are equal iff they match on all instances of objects in $\mathscr{D}$.

Example 4.5.6. Consider two functors $F, G : {}_R\underline{\mathrm{Mod}} \to \underline{\mathrm{Ab}}$, where F is the forgetful functor, and $G = \mathrm{Hom}_{{}_R\underline{\mathrm{Mod}}}(R, -)$. Since a morphism of R-modules from R suffices to specify where 1 is mapped to, $\mathrm{Hom}_{{}_R\underline{\mathrm{Mod}}}(R, M) \simeq M$, which implies that F and G are isomorphic functors.

Definition 4.5.7. Two categories $\mathscr{C}$ and $\mathscr{D}$ are **isomorphic** if there exists a functor isomorphism $F : \mathscr{C} \to \mathscr{D}$ s.t. there exists $G : \mathscr{D} \to \mathscr{C}$ s.t. $F \circ G = \mathrm{Id}_{\mathscr{D}}$, $G \circ F = \mathrm{Id}_{\mathscr{C}}$. They are **equivalent** if instead $F \circ G \simeq \mathrm{Id}_{\mathscr{D}}$, $G \circ F \simeq \mathrm{Id}_{\mathscr{C}}$.

Chapter 5

Tensor Product

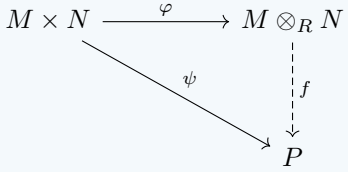
5.1 Tensor Product of Modules

Definition 5.1.1 (R-balanced Maps)**.** Let R be a ring, with M a right R-module, N a left R-module and P an abelian group. Then the map $\varphi : M \times N$ is **R-balanced** if the followings are satisfied:

- $\varphi(u, v_1 + v_2) = \varphi(u, v_1) + \varphi(u, v_2)$ for all $u \in M, v_1, v_2 \in N$.
- $\varphi(u_1 + u_2, v) = \varphi(u_1, v) + \varphi(u_2, v)$ for all $u_1, u_2 \in M$, $v \in N$.
- $\varphi(ua, v) = \varphi(u, av)$ for all $a \in R, u \in M, b \in N$.

Remark 5.1.2. The only difference between R-balanced maps and R-linear maps is the third condition: the coefficient in R could be transferred between different positions, but not out of the expression.

Definition 5.1.3 (Tensor Product)**.** A **tensor product** of M and N is an abelian group $M \otimes_R N$ with an R-balanced map $\varphi : M \times N \to M \otimes_R N$ which is universal w.r.t. the property: i.e. $\forall \psi : M \times N \to P$ which is R-balanced, there exists a unique $f : M \otimes_R N \to P$ s.t. $\psi = f \circ \varphi$ (ψ factors uniquely through φ), i.e. the following diagram commute:



Remark 5.1.4. If $\otimes_R$ exists, then it is unique up to a canonical isomorphism.

Suppose that for $M, N \in {}_R\underline{\text{Mod}}$, there exists two tensor products T and T'. Denote the canonical map from $M \times N$ to T and T' be φ and φ', respectively. Then by universal property of tensor product, there exists a unique isomorphism f and f' s.t. $f \circ \varphi = \varphi'$ and $f' \circ \varphi' = \varphi$, which gives $f \circ f' = \mathrm{Id}$.

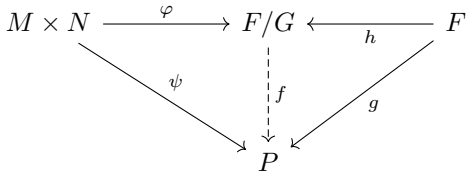
Proposition 5.1.5. The tensor product exists.

Proof. Proceed to show this via introducing relations on the free group structure. Let $F := \mathbb{Z}^{M\times N}$ be a free abelian group with basis $\{e_{(u,v)} \mid (u,v) \in M \times N\}$. Quotient out the elements that are claimed to be equivalent by the constraint that the canonical map φ should be R-balanced: consider $G \subseteq F$ to be generated by the following elements:

- $(e_{u_1+u_2,v} - e_{u_1,v} - e_{u_2,v})$, for all $u_1, u_2 \in M, v \in N$.
- $(e_{u,v_1+v_2} - e_{u,v_1} - e_{u,v_2})$, for all $u \in M, v_1, v_2 \in N$.
- $(e_{ua,v} - e_{u,av})$ for all $u \in M, v \in N, a \in R$.

By construction it is clear that the canonical map $\varphi : M \times N \to M \otimes_R N$ is R-balanced, via specifying $\varphi(u,v) = \overline{e_{u,v}}$.

It suffices to verify that the construction is compatible with the universal property. Consider the R-balanced map $\psi : M\times N \to P$, with the group homomorphism $g : F \to P$ s.t. $g(e_{u,v}) = \psi(u,v)$:



- *Existence.* Applying the universal property of quotient groups, which implies that there exists a unique f s.t. $f \circ h = g$ where h is the induced group homomorphism of the quotient. This is indeed valid, as ψ is R-balanced, which by construction has kernel G.
- *Uniqueness.* This follows from the result of universal property above; and the fact that φ is surjective.

□

Remark 5.1.6. The construction above, together with the fact that tensor products exist uniquely up to isomorphism, implies that for R-modules M and N with their system of generators, (u_i) and (v_i) respectively, for all $x \in M \otimes_R N$, there exists $(d_i) \in \mathbb{Z}$ s.t.

$$x = \sum_{i=1}^{n} d_i(u_i \otimes_R v_i)$$

where the multiplication by integers is simply adding repetitively the elements to itself.

The tensor products could also behave *functorially*, via composing with the canonical map of tensor product:

Let $f : M \to M'$ a morphism of right R-modules, and $g : N \to N'$ a morphism of left R-modules. Then one could define a map $\psi : M \times N \to M' \otimes_R N'$, where $(u,v) \mapsto f(u) \otimes_R g(v)$. The map is R-balanced since the canonical map of tensor product is R-balanced. Therefore it is valid to apply the universal property of tensor product, which gives a unique group homomorphism $f : M \otimes_R N \to M' \otimes_R N'$. This is uniquely determined by f and g; and is often denoted as $f \otimes_R g$.

Remark 5.1.7. This is also compatible with composition, via applying the universal property twice. Explicitly, for $f : M \to M', f' : M' \to M''$ a morphism of right R-modules, and $g : N \to N', g' : N' \to N''$ a morphism of left R-modules, we have

$$(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$$

Remark 5.1.8. In particular the constructions above induces a functor $M \otimes - : {}_R\underline{\mathrm{Mod}} \to \underline{\mathrm{Ab}}$ for M a right R-module, where

$$N \in \mathrm{Ob}({}_R\underline{\mathrm{Mod}}) \mapsto M \otimes N, \qquad f : N \to N' \mapsto \mathrm{Id}_M \otimes f$$

Similar to the case of Hom Functors, we seek to lift the functor to ${}_R\underline{\mathrm{Mod}} \to {}_R\underline{\mathrm{Mod}}$. This requires extra structure on the module of interest. As before, making R commutative, and restricting M and N to be both R-modules could resolve the issue, but the condition is too strong.

5.2 Bimodule

Definition 5.2.1 (Bimodule)**.** Let S and R be rings. An **R-S bimodule** M is given by an an abelian group M that is both a left S-module and a right R-module; and module operations is compatible, i.e.

$$(au)b = a(ub) \qquad \forall u \in M, a \in S, b \in R$$

Remark 5.2.2. If R is commutative, then every R-module is an R-R bimodule (which is why making R commutative suffices to ensure the Hom module has an R-module structure). In particular, R is an R-R bimodule.

Remark 5.2.3. Morphisms between S-R bimodules inherits from corresponding modules. Compatibility does not interfere with morphisms.

Proposition 5.2.4. Let R and S be rings, with M an S-R bimodule, and N a left R-module. Then there exists a unique left S-module structure on $M \otimes N$ s.t. $\lambda \cdot (u \otimes v) = (\lambda u) \otimes v$, for all $\lambda \in S, u \in M, v \in N$.

Proof. Use the universal property, with $P = M \otimes N$. Fix $\lambda \in S$; consider $\varphi : M \times N \to M \otimes N$ s.t. $\varphi(u, v) = (\lambda u) \otimes v$. This map is R-balanced, as the tensor product on R is balanced.

Then by universal property there exists a unique group homomorphism $f_\lambda : M \otimes N \to M \otimes N$, $u \otimes v \mapsto (\lambda u) \otimes v$. This gives the scalar multiplication of λ, which induces an S-module structure on $M \otimes N$. □

Proposition 5.2.5. The extra structure on the modules gives extra structure on the morphisms in the universal property:

Let M be a S-R bimodule, N a left R-module, and P a left S-module. Let $\varphi : M \times N \to M \otimes_R N$ the canonical map of tensor product. Suppose further that the map $\psi : M \times N \to P$ is S-bilinear. Then there exists a unique morphism of S-modules $f : M \otimes_R N \to P$.

Proof. By the universal property of tensor product, such morphism f exists, and is uniquely specified by $f(u \otimes v) = \psi(u, v)$. It suffices to check that this is indeed a morphism of S-modules, i.e. for all $a \in S$, $f((au) \otimes v) = af(u \otimes v)$. It then suffices to check that for certain (set of) fixed u and v, as every element in $M \otimes N$ is of such form. This is clear as

$$f((au) \otimes v) = \psi(au, v) \overset{!}{=} a\psi(u, v) = a \cdot f(u \otimes v)$$

Equality (!) requires that ψ is S-bilinear, and M being a bimodule ensures that this is well-formed under the context of S-modules. □

Remark 5.2.6. The proposition above lifts the functor $M \otimes -$ to ${}_R\underline{\mathrm{Mod}} \to {}_S\underline{\mathrm{Mod}}$ for all S-R bimodule M.

Remark 5.2.7. It may be interesting to consider the following property of bimodules:

1. If R is commutative, then left or right R-modules are the same; and in this case $M \otimes_R N$ is an R-module.
2. If M is a T-R bimodule, and N is an R-S bimodule, then $M \otimes_R N$ is a T-S bimodule.

For the second remark, it is clear that $M \otimes_R N$ is both a left T-module, and a right S-module, via applying the same proof as in Proposition 5.2.4. It suffices to prove that they are compatible. This is also clear from the construction in the proposition referred:

$$(a(u \otimes_R v))b = (au \otimes v)b = (au) \otimes (vb) = a(u \otimes (vb)) = a((u \otimes v)b)$$

Remark 5.2.8. Let R be a ring. Then R is an R-R bimodule. Let M be a left R-module, which implies that $R \otimes_R M$ is a left R-module. Then there exists a functorial isomorphism $R \otimes_R M \simeq M$ for all $M \in \mathrm{Ob}({}_R\underline{\mathrm{Mod}})$. (This is called functorial as this could be regarded as the property of functor $R \otimes_R -$.)

Proof. Proof via using the universal property. Consider the morphism of R-modules $\alpha : R \times M \to M$, where $\alpha(a, u) = au$ for all $a \in R$, $u \in M$. It is R-linear, which is by definition R-balanced. The universal property gives that there exists a unique $f : R \otimes M \to M$ s.t. $f(a \otimes u) = au$. Designate $g : M \to R \otimes M$, $g(u) = 1 \otimes u$ for all $u \in M$. This is clearly R-balanced. This gives an isomorphism as $g \circ f = \mathrm{Id}_R$, $f \circ g = \mathrm{Id}_{R \otimes M}$. □

5.3 Extension of Scalar

Let S and R be rings, together with a ring homomorphism $\varphi : R \to S$. Then

1. It is clear that there is a *restriction of scalar* functor:

$$F : {}_S\underline{\mathrm{Mod}} \to {}_R\underline{\mathrm{Mod}}, \quad {}_SM \to {}_RM \qquad \text{where } a \cdot u := \varphi(a) \cdot u \ \ (\forall a \in R, u \in {}_SM)$$

2. It is more interesting to consider the *extension of scalar* functor $G : {}_R\underline{\mathrm{Mod}} \to {}_S\underline{\mathrm{Mod}}$. Notice that φ gives S a natural R-module structure, where $rs := \varphi(r)s$ for all $r \in R$, $s \in S$. This gives a natural extension of scalar functor $(S \otimes_R -)$:
   - For $M \in \mathrm{Ob}({}_R\underline{\mathrm{Mod}})$, this gives $S \otimes_R M$.
   - For $f : M_1 \to M_2$ a morphism of R-modules, this gives $\mathrm{Id}_S \otimes f$.

Example 5.3.1. Consider the following examples:

- Let $\varphi : R \to R/I$ the canonical quotient map. Then this induces the isomorphism $G(M) \simeq M/IM$.

  Extension of scalar gives $G(M) \simeq R/I \otimes M$. To show that these two left R/I-modules are isomorphic, it suffices to specify maps between them s.t. the composition gives identity. Consider

$$f : R/I \otimes M \to M/IM, \quad \overline{r} \otimes u \mapsto \overline{ru}, \qquad g : M/IM \to R/I \otimes M, \overline{u} \mapsto 1_{R/I} \otimes u$$

It is clear that $f \circ g = \mathrm{Id}_{R/I\otimes M}$. Notice

$$g \circ f(\bar{r} \otimes u) = g(\overline{ru}) = 1 \otimes \overline{ru} = 1 \otimes \bar{r} \cdot \bar{u} = \bar{r} \otimes \bar{u}$$

since the canonical map of tensor product is R-balanced.

- Let R be a ring, and $S \subseteq R$ a multiplicative system. Let φ be the canonical map $R \to S^{-1}R$, $\varphi(a) = \frac{a}{1}$. Then this induces an isomorphism $G(M) \simeq S^{-1}M$.

  Apply the similar strategy. It suffices to show that $G(M) = S^{-1}R \otimes M \simeq S^{-1}M$. Consider

  $$f : S^{-1}R \otimes M \to S^{-1}M, \quad \frac{r}{s} \otimes u \mapsto \frac{ru}{s}, \qquad g : S^{-1}M \mapsto S^{-1}R \otimes M, \quad \frac{u}{s} \mapsto \frac{1}{s} \otimes u$$

  It is clear $f \circ g(\frac{u}{s}) = f(\frac{1}{s} \otimes u) = \frac{u}{s}$. For the other direction, check

  $$g \circ f(\frac{r}{s} \otimes u) = g(\frac{ru}{s}) = \frac{1}{s} \otimes (ru) = \left(\frac{1}{s}\right) \cdot r \otimes u = \frac{1}{s} \cdot \frac{r}{1} \otimes u = \frac{r}{s} \otimes u$$

- Tensor of module and localization of a ring is isomorphic to the localization of the module. Let R be a commutative ring, M be an R-module, and U a multiplicative system in R. Then we have the isomorphism

  $$M_U \simeq M \otimes_R R_U$$

  Proof is done via constructing concrete maps. Consider the morphisms

  $$f : M_U \to M \otimes_R R_U, \quad \frac{u}{s} \mapsto u \otimes \frac{1}{s}$$
  $$g : M \otimes_R R_U \to M_U, \quad u \otimes \frac{r}{s} \mapsto \frac{ru}{s}$$

  for all $u \in M, r \in R, s \in R \setminus U$. First verify that these maps are indeed well-defined morphisms of R-modules:

  - Consider $\frac{u_1}{s_1} \sim \frac{u_2}{s_2}$ where both of which are in M_U. By the definition of localization this indicates that there exists some $t \in R \setminus U$ s.t. $t(s_1u_2 - s_2u_1) = 0$. This gives

    $$f\left(\frac{u_1}{s_1}\right) - f\left(\frac{u_2}{s_2}\right) = (s_2u_1 - s_1u_2) \otimes \frac{1}{s_1s_2} = (t(s_2u_1 - s_1u_2)) \otimes \frac{1}{s_1s_2t} = 0$$

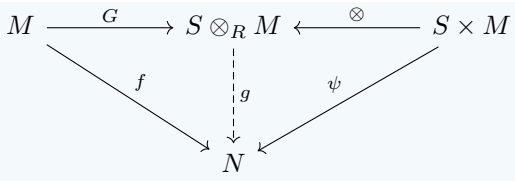
    which indicates that the image does not depend on the choice of representative.
  - Consider $g' : M \times R_U \to M_U, g'(u, \frac{r}{s}) = \frac{ru}{s}$. It is clear that g' is bilinear as R is commutative, which implies that g' is R-balanced. Then g exists by the universal property of tensor product.

  Then verify that the composition gives identity:

  $$f \circ g\left(u \otimes \frac{r}{s}\right) = ru \otimes \frac{1}{s} = u \cdot r \otimes \frac{1}{s} = u \otimes \frac{r}{s} \implies f \circ g = \mathrm{Id}_{M\otimes R_U}, \qquad g \circ f\left(\frac{u}{s}\right) = \frac{u}{s} \implies g \circ f = \mathrm{Id}_{M_U}$$

  This gives the desired isomorphism.

Theorem 5.3.2 (Universal Property of Extension of Scalars)**.** Let M be a left R-module, N be a left S-module, together with a ring homomorphism $\varphi : R \to S$. Let $f : M \to N$ a morphism of R-modules (in the sense of restriction of scalars). Then there exists a unique morphism of S-modules $g : S \otimes_R M \to N$ s.t. $g(1 \otimes u) = f(u)$ for all $u \in M$:



Proof. Construct using the universal property of tensor product. Since f is a morphism of S-modules, it is in particular S-linear, i.e.

$$f(su) = sf(u) \implies \psi(s,u) = sf(u)$$

There exists a canonical morphism into the setting of universal property, as $G(su) = \otimes(1, su) = \otimes(s,u)$ for all $s \in S, u \in M$; and ψ is R-linear:

$$\psi(sr,u) = (s\varphi(r))f(u) = s(\varphi(r)f(u)) = sf(\varphi(r)u) = \psi(s,ru)$$

$$\psi(ss',u) = ss'f(u) = sf(s'u) = \psi(s,s'u)$$

Then the strengthened version of universal property gives the desired result. □

Remark 5.3.3. Functorially, for tensor products we have the natural transformation (given the ring homomorphism $\varphi : R \to S$)

$$\mathrm{Hom}_S(S \otimes_R M, N) \to \mathrm{Hom}_R(M,N), \qquad g \mapsto (u \mapsto g(1 \otimes u))$$

The universal property gives that this is actually a bijection. Since $\mathrm{Hom}_R(M,N)$ is in essence the restriction of scalar, there is a bijection (which is exactly rephrasing the result above)

$$\mathrm{Hom}_S(G(M), N) \simeq \mathrm{Hom}_R(M, F(N))$$

Definition 5.3.4 (Adjoint Pair). Consider functors $F : \mathscr{C} \to \mathscr{D}$, $G : \mathscr{D} \to \mathscr{C}$. They form an **adjoint pair** (F,G) if for all $a \in \mathrm{Ob}(\mathscr{C})$ and $b \in \mathrm{Ob}(\mathscr{D})$, we have a bijection $\mathrm{Hom}_{\mathscr{C}}(G(b), a) \simeq \mathrm{Hom}_{\mathscr{D}}(b, F(a))$ which is functorial w.r.t. both a and b, i.e. there exists a natural transformation from $\mathrm{Hom}_{\mathscr{C}}(G(-), a)$ to $\mathrm{Hom}_{\mathscr{D}}(-, F(a))$.

Remark 5.3.5. Extension of scalar functor G and restriction of scalar functor F form an adjoint pair.

5.4 General Properties of Tensor Product

Proposition 5.4.1. Tensor product is *commutative*, i.e. there exists an isomorphism of abelian groups $M \otimes_R N \simeq N \otimes_{R^{\mathrm{op}}} M$. Similarly, if R is commutative, then this is an isomorphism of R-modules.

Proof. Proceed via using the universal property of tensor product. Consider the map $\varphi : M \times N \to N \otimes_{R^{\mathrm{op}}} M$ given by $\varphi(v,u) = u \otimes_{R^{\mathrm{op}}} v$. It is clear φ commutes with addition in either field. To show that φ is indeed R-balanced it suffices to check the third property, which gives

$$\varphi(va,u) = u \otimes_{R^{\mathrm{op}}} (va) = u \otimes_{R^{\mathrm{op}}} a^{\mathrm{op}} v = ua^{\mathrm{op}} \otimes_{R^{\mathrm{op}}} v = (au) \otimes_{R^{\mathrm{op}}} v = \varphi(v, au)$$

Similarly there exists an R-balanced map $\tilde{\psi} : N \times M \to M \otimes_R N$ (as R^{op} modules) which is given by $\psi(u,v) = v \otimes u$. This induces a map $\psi : N \otimes_{R^{\mathrm{op}}} M \to M \otimes_R N$. It is clear that $\varphi \circ \psi = \mathrm{Id}_{N \otimes_{R^{\mathrm{op}}} M}$, $\psi \circ \varphi = \mathrm{Id}_{M \otimes_R N}$. □

Remark 5.4.2. If R is commutative, then the left R-modules are the same as right R-modules, which indicates that $M \otimes_R N \simeq N \otimes_R M$ (as in the commutative setting the opposite ring is the same as the original ring).

Proposition 5.4.3. Tensor product is *associative*, i.e. for M a right R-module, N an R-S bimodule, and P a left S-module, there exists a unique isomorphism $f : (M \otimes_R N) \otimes_S P \to M \otimes_R (N \otimes_S P)$ s.t. $f((u \otimes_R v) \otimes_S w) = u \otimes_R (v \otimes_S w)$.

Proof. Apply the universal property of tensor product twice. First consider map $f_z : M \times N \to M \otimes_R (N \otimes_S P)$ given by $f_z(x, y) = x \otimes_R (y \otimes_S z)$ for some $z \in P$. f_z is R-balanced, as for all $a \in R$,

$$f_z(x, ay) = x \otimes_R (ay \otimes_S z) = x \otimes_R a(y \otimes_S z) = (xa) \otimes_R (y \otimes_S z) = f_z(xa, y)$$

By universal property of tensor product this gives a unique map $\tilde{f_z} : M \otimes_R N \to M \otimes_R (N \otimes_S P)$, $f_z(x \otimes y) = x \otimes (y \otimes z)$. Now consider the map $f : M \otimes_R N \times P \to M \otimes_R (N \otimes_S P)$ given by $f(x \otimes y, z) = f_z(x, y)$. This is S-linear, as for all $a \in S$,

$$f((x \otimes y)a, z) = f((x \otimes ya), z) = x \otimes (ya \otimes z) = x \otimes (y \otimes (az)) = f((x \otimes y), az)$$

Similarly this gives a unique map $\tilde{f} : (M \otimes_R N) \otimes_S P \to M \otimes_R (N \otimes_S P)$. Repeat the process in the converse direction gives the inverse map, and it is clear that the composition of them is identity in the corresponding structure. □

Proposition 5.4.4. Let R be a commutative ring, and $f_1 : R \to S_1$ and $f_2 : R \to S_2$ be two R-algebras. Then there is a unique R-algebra structure on $S_1 \otimes_R S_2$ s.t.

$$(u_1 \otimes v_1) \cdot (u_2 \otimes v_2) = (u_1 u_2) \otimes (v_1 v_2)$$

Proof. Since we are in the commutative setting, by using the associativity and commutativity of tensor product, there is an isomorphism $\Phi : (S_1 \otimes S_2) \otimes (S_1 \otimes S_2) \simeq (S_1 \otimes S_1) \otimes (S_2 \otimes S_2)$. By universal of property of $S_1 \otimes S_1$ and $S_2 \otimes S_2$, there exists a unique morphism of R-module $f_i(a_i \otimes b_i) = a_i b_i$ for all $a_i, b_i \in S_i$ with $i \in \{1, 2\}$. This gives $f_1 \otimes f_2 : (S_1 \otimes S_1) \otimes (S_2 \otimes S_2) \to S_1 \otimes S_2$, which indicates that there is a unique map $f_1 \otimes f_2 \circ \Phi$ that maps $(S_1 \otimes S_2) \otimes (S_1 \otimes S_2) \to S_1 \otimes S_2$. Composing this with the tensoring of $(S_1 \otimes S_2)$ with itself gives the desired result. □

Proposition 5.4.5. There exists an isomorphism of abelian groups $\Phi : \mathrm{Hom}_S(M \otimes_R N, P) \simeq \mathrm{Hom}_R(N, \mathrm{Hom}_S(M, P))$ for N a left R-module, P a left S-module, and M an S-R bimodule.

Proof. The only natural way to define this isomorphism is via $\Phi(\varphi) = (N \mapsto (M \mapsto \varphi(M \otimes N)))$, where for $f \in \mathrm{Hom}_S(M, P)$, $a \in R, u \in M$, $af(u) := f(ua)$. By construction this is a bijection, and additivity is satisfied in P. □

Remark 5.4.6. This indicates that $M \otimes_R -$ and $\mathrm{Hom}_S(M, -)$ form an adjoint pair for M being a S-R bimodule. Furthermore, if $f : R \to S$ gives an R-algebra structure, then taking $M = S$ gives the adjoint pair of extension/restriction of scalar functors.

Chapter 6

Introduction to Homological Algebra

6.1 Exactness

Definition 6.1.1 (Complex). A **Complex** of R-modules is a family of R-modules (M_i) and R-linear maps $d_i : M_i \to M_{i+1}$ s.t. for all i, $d_{i+1} \circ d_i = 0$.

Remark 6.1.2. The followings are some specifications on the notations:

- The complex is often denoted by a chain

$$\cdots \xrightarrow{d_{i-2}} M^{i-1} \xrightarrow{d_{i-1}} M^i \xrightarrow{d_i} M^{i+1} \xrightarrow{d_{i+1}} \cdots$$

  or a chain with indices on the bottom with $M^i = M_{-i}$.

- The complex extends to infinity in both ends. If the notation terminated on one side, all modules not written out are the trivial (the zero module).

Remark 6.1.3. The definition of a complex is the same as stating that $\operatorname{im} d_i \subseteq \ker d_{i+1}$ for all i.

Definition 6.1.4. For a sequence $A \xrightarrow{f} B \xrightarrow{g} C$ where f and g are R-linear maps, it is **exact at B** if the equality is reached in the remark above, i.e. $\operatorname{im} f = \ker g$.

A sequence is exact if it is exact at A_i for all i. A complex is exact if it is exact everywhere.

Example 6.1.5. The sequence $0 \longrightarrow A \xrightarrow{f} B$ is exact implies that $\ker f = \{0\}$, i.e. f is injective. Similarly, $A \xrightarrow{g} B \longrightarrow 0$ implies that g is surjective.

Definition 6.1.6. A **Short Exact Sequence (SES)** is an exact sequence

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$$

Proposition 6.1.7. Given a sequence $(*) : 0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$, the followings are equvalent:

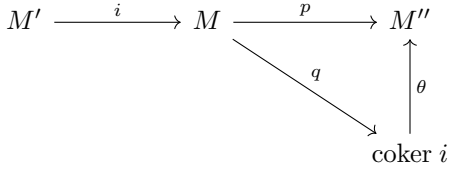
i) $(*)$ is a short exact sequence.

ii) i is injective, and for $q : M \to \operatorname{coker} i$, there exists a unique isomorphism θ s.t. $\theta \circ q = p$.

iii) p is surjective, and for $j : M \to \ker p$, there exists a unique isomorphism η s.t. $i = \eta \circ j$.

Proof. It suffices to prove the equivalence between i) and ii), as the case with iii) is similar:

- *i)⇒ ii).* Apply the universal property of cokernel. Since $(*)$ is exact, $p \circ i = 0$, there exists a map θ s.t. the following diagram commutes.



  The fact that p is surjective, and the diagram should commute gives θ should be surjective. To prove that θ is injective, it suffices to verify that $\theta(b) = 0 \implies b = 0$ for $b \in \operatorname{coker} i$. Since q by definition is surjective, there exists $a \in M$ s.t. $q(a) = b$. This gives $a \in \ker p = \operatorname{im} i$, which implies that $q(a) = 0$ as the cokernel is defined by $M/\operatorname{im} i$.

- *ii)⇒ i).* Given that μ is an isomorphism and i is injective, it suffices to verify that p is surjective, and $\operatorname{im} i = \ker p$. μ being surjective implies that p is surjective; and μ being an isomorphism implies that $\ker p = \ker q = \operatorname{im} i$.

□

Proposition 6.1.8. Given a short exact sequence $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$, the following statements are equivalent:

i) There exists $j : M \to M'$ s.t. $j \circ i = \mathrm{Id}_{M'}$

ii) There exists $q : M'' \to M$ s.t. $p \circ q = \mathrm{Id}_{M''}$

iii) There exists a submodule $N \subseteq M$ s.t. M can be expressed by the internal direct sum $M = i(M') \oplus N$; and p induces an isomorphism $N \simeq M''$.

Such a short exact sequence is a split exact sequence.

Proof. It suffices to give the equivalence between i) and iii), as for ii) it is similar.

- *i)⇒ iii).* Let $N = \ker j$. Check that this gives an internal direct sum:
  - $N \cap i(M') = \{0\}$. Let $x \in i(M') \cap N$. Then there exists $u \in M'$ s.t. $i(u) \in \ker j$, i.e. $j \circ i(u) = 0$. But this indicates that $u = 0$ as $j \circ i = \mathrm{Id}_{M'}$. Since i is a morphism of modules, $i(0) = 0$, which indicates that the only element that is in both $i(M')$ and N is 0.
  - $N + i(M') = M$. Notice $v - i \circ j(v) \in \ker q$, and by inspection $i \circ j(v) \in \operatorname{im} i$.

  By the first isomorphism theorem, $\operatorname{im} i = \ker p$ implies $M/\operatorname{im} i \simeq N \simeq M''$.

- *iii)⇒ i).* Define $j : i(M') \oplus N \to i(M') \simeq M'$ since i is injective.

□

Remark 6.1.9. Generally short exact sequences do not split. A counterexample is

$$0 \longrightarrow \mathbb{Z} \xrightarrow{i} 2\mathbb{Z} \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

where $i(\mathbb{Z}) \simeq \mathbb{Z}$, but the inverse map cannot be extended properly to the whole ring $\mathbb{Z}$. If R is a field, then all short exact sequences split as one can complete a basis in a vector space; and subspaces spanned by a subset of a basis is always a direct summand of the whole space.

The following present a common technique known as "diagram chasing":

Proposition 6.1.10 (The 5-Lemma). Consider the following diagram, with blocks commute and rows exact:

$$\begin{array}{ccccccccc} A_1 & \xrightarrow{u_1} & A_2 & \xrightarrow{u_2} & A_3 & \xrightarrow{u_3} & A_4 & \xrightarrow{u_4} & A_5 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\ B_1 & \xrightarrow{v_1} & B_2 & \xrightarrow{v_2} & B_3 & \xrightarrow{v_3} & B_4 & \xrightarrow{v_4} & B_5 \end{array}$$

1. If f_2, f_4 are injective, f_1 is surjective, then f_3 is injective.
2. If f_2, f_4 are surjective, f_5 is injective, then f_3 is surjective.
3. (Combining i) and ii)) If f_1, f_2, f_4, f_5 are all isomorphisms, then f_3 is an isomorphism.

Proof. The argument is symmetric, so it suffices to prove the first one. f_3 is injective if and only if $f_3(b) = 0 \implies b = 0$. Following the steps:

- Consider the third square. $v_3 \circ f_3(b) = v_3(0) = 0$, giving $f_4 \circ u_3(b) = 0$. f_4 being injective implies that $u_3(b) = 0$.
- Consider the second square. The top row being exact implies that $b \in \operatorname{im} u_2$, i.e. there exists some $c \in A_2$ s.t. $u_2(c) = b$. Commutativity gives that $v_2 \circ f_2(c) = 0$, i.e. $c' := f_2(c) \in \ker v_1$.
- Consider the first square. The bottom row being exact implies that there exists some $d' \in B_1$ s.t. $v_1(d') = c'$. Since f_1 is surjective, there exists $d \in A_1$ s.t. $f_1(d) = d'$. For the diagram to commute, it is required that $u_1(d) = c$. But this indicates that $c \in \operatorname{im} u_1$, i.e. $c \in \ker u_2$, which gives $b = u_2(c) = 0$.

□

Definition 6.1.11. Let R and S be rings, and $F : {}_R\underline{\mathrm{Mod}} \to {}_S\underline{\mathrm{Mod}}$ is an additive functor. Then F is **exact** if for all short exact sequences of R-modules $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$, the corresponding sequence after applying F is also exact.

Proposition 6.1.12. F is exact if and only if for all exact sequence $A \xrightarrow{f} B \xrightarrow{g} C$, $F(A) \xrightarrow{f} F(B) \xrightarrow{g} F(C)$ is also exact.

Proof. Proceed by showing implication in two directions:

$\Leftarrow$: This holds by definition, where one can consider the particular case where f is injective and g is surjective.

$\Rightarrow$: Consider the following short exact sequences:

$$\begin{aligned}(1): &\quad 0 \longrightarrow \ker f \longrightarrow A \xrightarrow{\alpha_1} \operatorname{im} f \longrightarrow 0\\ (2): &\quad 0 \longrightarrow \ker g \xrightarrow{\alpha_2} B \xrightarrow{\beta_1} \operatorname{im} g \longrightarrow 0\\ (3): &\quad 0 \longrightarrow \operatorname{im} g \xrightarrow{\beta_2} C \longrightarrow \operatorname{coker} g \longrightarrow 0\end{aligned}$$

where $\operatorname{im} f = \ker g$ as the sequence given is exact. These by construction are all short exact sequences, where applying F gives also short exact sequences. Combining gives the sequence which is still exact after applying F:

$$A \xrightarrow{\alpha_1} \operatorname{im} f \xrightarrow{\alpha_2} B \xrightarrow{\beta_1} \operatorname{im} g \xrightarrow{\beta_2} C$$

where α_1, β_1 are surjective; and α_2, β_2 are injective. What we want to show is $\operatorname{im} F(f) = \ker F(g)$. Since α_1 is surjective, $\operatorname{im} F(f) = \operatorname{im} F(\alpha_2)$; and since β_2 is injective, $\ker F(g) = \ker F(\beta_1)$. From the result of (2) after applying F, we have $\operatorname{im} F(\alpha_2) = \ker F(\beta_1)$.

□

Remark 6.1.13. "One-sided" exact sequences can be understood functorially:

- Given exact sequence $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M''$ is the same as saying that i is injective; and M' is the kernel of p.
- Similarly, given exact sequence $M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$ is the same as saying that p is surjective; and M'' is the cokernel of i.

Definition 6.1.14. Just as in the remark, one could consider exact functors only on one side. $F : {}_R\underline{\mathrm{Mod}} \to {}_S\underline{\mathrm{Mod}}$ is **left exact** if for all exact sequence $0 \longrightarrow A \longrightarrow B \longrightarrow C$, the sequence $0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C)$ is also exact; and the definition is symmetric for right exact functors. Notice that since F is an additive functor, $F(0) = 0$ (as zero morphisms are mapped to zero morphisms).

Proposition 6.1.15. Let M be an R-S bimodule. Then functor $F = \operatorname{Hom}_R(M, -) : {}_R\underline{\mathrm{Mod}} \to {}_S\underline{\mathrm{Mod}}$ is left exact; and the converse is also true, i.e. if $0 \longrightarrow \operatorname{Hom}_R(M, A) \longrightarrow \operatorname{Hom}_R(M, B) \longrightarrow \operatorname{Hom}_R(M, C)$ is exact, then $0 \longrightarrow A \longrightarrow B \longrightarrow C$ is exact.

Proof. What we first want to show is that if the sequence $0 \longrightarrow A \longrightarrow B \longrightarrow C$ is exact, then the corresponding sequence $0 \longrightarrow \operatorname{Hom}(M, A) \longrightarrow \operatorname{Hom}(M, B) \longrightarrow \operatorname{Hom}(M, C)$ is exact:

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ & & & \nwarrow^{u} & \uparrow{\scriptstyle v} & & \\ & & & & M & & \end{array}$$

The natural way to define the functor F is via specifying $\operatorname{Hom}(M, A) \ni u \mapsto f \circ u$, $\operatorname{Hom}(M, B) \ni v \mapsto g \circ v$. Exactness follows from the universal property of kernel, where for all $v \in \operatorname{Hom}(M, B)$ s.t. $\operatorname{Hom}(M, C) \ni g \circ v = 0$, it factors uniquely through f. Furthermore, since F is an additive functor, it preserves injectivity (via considering elements in $\underline{\mathrm{Sets}}$), which indicates that $F(f)$ is also injective.

For the converse, take $M = A$. This gives the exact sequence $0 \longrightarrow \operatorname{Hom}(A, A) \xrightarrow{\alpha} \operatorname{Hom}(A, B) \xrightarrow{\beta} \operatorname{Hom}(A, C)$. The natural ways to define the map is via specifying $\alpha = f \circ -$, $\beta = g \circ -$. Observe that the exactness of the sequence gives $\beta \circ \alpha = g \circ f \circ - = 0$, which indicates that $g \circ f = 0$ by associativity. α being injective follows directly from the fact that f is injective. □

Remark 6.1.16. The dual argument is also true, via applying the universal property of cokernel. That is, the functor $\mathrm{Hom}_R(-, M)$ is right exact. The direction of exactness reverses as the functor is contravariant.

Proposition 6.1.17. If M is an S-R bimodule, then $M \otimes_R -$ is right exact.

Proof. From the right exact version of Proposition 6.1.15, it suffices to prove that for left R-module N the sequence

$$\mathrm{Hom}(M \otimes A, N) \longrightarrow \mathrm{Hom}(M \otimes B, N) \longrightarrow \mathrm{Hom}(M \otimes C, N) \longrightarrow 0$$

is exact. First make a parenthesis on the generalization of the adjoint property of extension and restriction of scalars:

Parenthesis 6.1.18 (Prop 4.4 [c6])**.** Let M be an S-R bimodule, C a left R-module, and N a left S-module, then there is a functorial isomorphism

$$\mathrm{Hom}_S(M \otimes_R C, N) \simeq \mathrm{Hom}_R(C, \mathrm{Hom}_S(M, N))$$

Proof. By the universal property of tensor product, it suffices to give every R-balanced map $f : M \times C \to N$ a map in $\mathrm{Hom}_R(C, \mathrm{Hom}_S(M, N))$. Let the isomorphism be F defined via $F(\tilde{f}[u \otimes v \mapsto f(u, v)]) = v \mapsto (u \mapsto f(u, v))$. The inverse exists by inspection. It is well-defined as one can consider the map $u \times v \mapsto f(u, v)$; and use the universal property of tensor product. □

Then apply the parenthesis and Proposition 6.1.15 gives that it suffices to verify that $0 \longrightarrow \mathrm{Hom}(M, C) \longrightarrow \mathrm{Hom}(M, B) \longrightarrow \mathrm{Hom}(M, A)$ is exact, which holds as M is in particular a right R-module; and in this case the functor $\mathrm{Hom}_R(-, \mathrm{Hom}_S(M, N))$ is a contravariant functor. Recall that for a contravariant functor $\mathrm{Hom}(-, N)$, if the sequence $A \longrightarrow B \longrightarrow C \longrightarrow 0$ is exact, then $0 \longrightarrow \mathrm{Hom}(C, N) \longrightarrow \mathrm{Hom}(B, N) \longrightarrow \mathrm{Hom}(A, N)$ is exact. This finishes the proof. □

Remark 6.1.19. Recall that the above isomorphism holds for all adjoint pairs (F, G). Therefore, the proof applies as long as F is left exact (for G being right exact) or the converse holds.

In general, the above two functors and the contravariant is only left (right) exact instead of exact. Consider the short exact sequence:

$$0 \longrightarrow \mathbb{Z} \longrightarrow 2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

- Applying $- \otimes \mathbb{Z}/2\mathbb{Z}$ gives
$$0 \longrightarrow \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{i} 2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$
where $2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} = 0$ and $\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$, as the map being R-linear restricts that $f(0,1) = f(1,0) = f(0,0)$. This implies that i is not injective.
- Applying $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z}/2\mathbb{Z})$ gives
$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \xrightarrow{i} \mathrm{Hom}_{\mathbb{Z}}(2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \xrightarrow{p} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \longrightarrow 0$$
where $\mathrm{Hom}_{\mathbb{Z}}(2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \ni h = 0$ as it is required that $h(1) + h(1) = \bar{1} + \bar{1} = 0$ which indicates that p is not surjective. Similar situations appear in the contravariant case.

It is then of specific interest in which modules are the above functors exact.

6.2 Flat, Projective, and Injective Modules

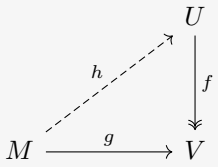
Definition 6.2.1. Let R be a ring, and M a left R-module. Then:

- M is a **flat module** if $- \otimes_R M$ is an exact functor.
- M is a **projective module** if $\mathrm{Hom}_R(M, -)$ is an exact functor.
- M is an **injective module** if $\mathrm{Hom}_R(-, M)$ is an exact functor.

Remark 6.2.2. By comparing with the results obtained in the propositions aforementioned (Proposition 6.1.15, 6.1.17), it is clear what is further required by the definitions:

- By Proposition 6.1.17, a module is flat if and only if for all injective maps $M_1 \to M_2$, the corresponding map $M_1 \otimes M \to M_2 \otimes M$ is injective.
- By Proposition 6.1.15, a module is projective if and only if for all surjective maps $M_1 \to M_2$, the corresponding map $\mathrm{Hom}_R(M, M_1) \to \mathrm{Hom}_R(M, M_2)$ is surjective; or the corresponding map is injective if the functor is contravariant.

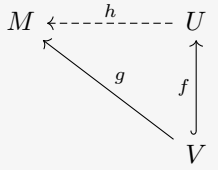
Remark 6.2.3. The fact that Hom functors in the remark above is surjective is the same as the following definition (for projective modules): M is a projective R-module if and only if for all morphism of R-modules $g : M \to V$ with module U for which there exists a surjective morphism $f : U \to V$, there exists a morphism of R-modules $h : M \to U$ s.t. $g = f \circ h$; that is, making the following diagram commute:



In plain words, there exists an embedding into some module (for example, free modules) that could "project" surjectively to V. This embedding (injection) definitely needs not be unique, as for example one could always embed the projective module to a free module with higher rank.

This definition is indeed equivalent with the previous one, as for a surjective morphism $f : U \to V$, for any $g : M \to V$ there exists some $h : M \to U$ s.t. the diagram commute. This indicates that the morphism $\mathrm{Hom}(M, U) \to \mathrm{Hom}(M, V)$ is a surjection.

The dual result holds also for injective modules: for all R-module M being injective, it is equivalent to state that for any morphism $g : M \to V$, there exists some R-module U with an injection $f : V \to U$ and some morphism $h : U \to M$ s.t. $g = h \circ f$, i.e. the following diagram commutes:



Proposition 6.2.4. Let M be a left R-module. Then the following statements are equivalent:

i) M is a projective R-module.

ii) M is a direct summand of a free R-module. That is, there exists a free R-module F and an R-module N s.t. $F \simeq M \oplus N$.

iii) Let P be an R-module, and F be a free R-module. Then every short exact sequence $0 \longrightarrow P \longrightarrow F \longrightarrow M \longrightarrow 0$ is split exact.

Proof.

- *i)* $\implies$ *iii).* Apply the definition given in Remark 6.2.3. M being an R-module implies that it admits a system of generators, namely there exists some $(g_i)_{i\in I}$ s.t. $M = (g_i)_{i\in I}$. Then there exist $F = R^{(I)}$ where there exists a surjection $f : F \to M, f(e_i) = g_i$. Let $g : M \to M$ be the identity map. By the alternative definition there exists some $h : M \to F$ s.t. $f \circ h = g = \mathrm{Id}_M$. By Proposition 6.1.8 this indicates that the sequence of interest splits.
- *iii)* $\implies$ *ii).* Consider the projection $p : F \to M$ where $M = (g_i)_{i\in I}$ and $F = R^{(I)}$. Therefore, the sequence

$$0 \longrightarrow \ker p \xrightarrow{i} F \longrightarrow M \longrightarrow 0$$

  is short exact, which gives $F \simeq i(\ker p) \oplus M = \ker p \oplus M$.
- *ii)* $\implies$ *i).* Consider F as a projective module. This is true as F can be trivially embedded to itself. It then suffices to prove that if F is projective and $F \simeq M \oplus N$, then M is projective. By Remark 6.2.2, it suffices to prove that $\mathrm{Hom}_R(M, U) \to \mathrm{Hom}_R(M, V)$ is surjective for all $U \to V$ surjective. F is projective indicates that $\mathrm{Hom}_R(F, U) \to \mathrm{Hom}_R(F, V)$ is surjective. By the fact that $\mathrm{Hom}_R(F, U) \simeq \mathrm{Hom}_R(M, U) \oplus \mathrm{Hom}_R(N, U)$, $\mathrm{Hom}_R(M, U) \to \mathrm{Hom}_R(M, V)$ is surjective.

□

Corollary 6.2.5. The category of ${}_R\underline{\mathrm{Mod}}$ has enough projective modules. In particular, for $M = (g_i)_{i\in I}$ one can take $F = R^{(I)}$.

Similarly, we would like to prove that there are "enough" injective objects in ${}_R\underline{\mathrm{Mod}}$:

Theorem 6.2.6. The category of ${}_R\underline{\mathrm{Mod}}$ has enough injective objects. That is, for all R-module M, there exists an injective embedding $M \hookrightarrow Q$ where Q is an injective module.

Proposition 6.2.7 (Baer). Let M be an R-module. Then M is injective if and only if $\mathrm{Hom}_R(R, M) \to \mathrm{Hom}_R(I, M)$ is surjective for all left ideals $I \subseteq R$. That is, for all R-linear maps $f : I \to M$, there exists some $u \in M$ s.t. $f(x) = xu$ for all $x \in I$ (and this gives an extension into R).

Proof. The implication from M being injective to the condition follows directly from the definition of injective modules, where one considers the map $I \hookrightarrow R$ to be the injection. For the other direction, consider the following construction:

Let $i : M_1 \hookrightarrow M_2$ be an injection, where M_1, M_2 are R-modules; and let $f : M_1 \to M$ be an R-linear map. It suffices to show that there exists some $g : M_2 \to M$ s.t. $g \circ i = f$. Consider the family of modules N_i and corresponding maps h_i s.t. $M_1 \subseteq N_i \subseteq M_2$ for all i; and $h_i|_{M_1} = f$. Define the partial order $(N, h) \leq (N', h')$ if and only if $N \subseteq N'$, and $h'|_N = h$. Notice that such family is non-empty, as in particular M_1 is in the family. Further it is bounded above by M_2, which allows us to apply Zorn's Lemma to retrieve a maximal element $(\bar{N}, \bar{h})$. Handle the cases respectively:

- $\bar{N} = M_2$. Then letting $g = \bar{h}$ finishes the proof.
- $\bar{N} \neq M_2$. Proceed to show that this map can be further extended, which is a contradiction.

  By the inequality there exists some $x \in M_2 - \bar{N}$. Consider $I = \{a \in R \mid ax \in N\}$ which is the submodule of M_2 generated by x. Consider the morphism of R-modules f' where $f'(a) = \bar{h}(ax)$. By hypothesis there exists $u \in M$ s.t. $f'(x) = xu$ for all $x \in I$. Notice that $\bar{h} \circ \bar{i} = f$ where $\bar{i} : M_1 \hookrightarrow \bar{N}$ is the injection. Define the map $\tilde{h} : \bar{N} + I = \bar{N} + Rx \to M$, $\tilde{h}(a + vx) = \bar{h}(a) + vu$ for $a \in \bar{N}$ and $v \in N$. This is well-defined, as for all v s.t. $vx \in \bar{N}$, $\bar{h}(vx) = h(vx) = f'(v) = vu$ by hypothesis. This indicates that $\bar{N}$ is not maximal as the map can be extended to $\bar{N} + Rx$, which is a contradiction.

□

Definition 6.2.8. Let M be an R-module. Then it is **divisble** if and only if for all $u \in M$, $n \in \mathbb{Z}_{\geq 0}$, there exists $v \in M$ s.t. $nv = u$ where multiplication by $n \in \mathbb{Z}_{\geq 0}$ is adding n copies of the elements to itself.

Corollary 6.2.9. If $R = \mathbb{Z}$, then M being an R-module is injective if and only if it is divisible.

Proof. If M is divisible, then for all $n \in \mathbb{Z}_{\geq 0}$, $u \in M$ there exists $v \in M$ s.t. $u = nv$. That is, for all $f : I \to M$ with $n \in I \subseteq \mathbb{Z}$, there exists $v \in M$ s.t. $f(n) = u = nv$. This gives the criterion in Proposition 6.2.7. The converse holds as the converse holds in the proposition. □

Proof of Theorem 6.2.6. First prove the theorem with restriction $R = \mathbb{Z}$. From the the previous remark it is clear that $\mathbb{Z}$-modules are injective if and only if it is divisible; and $\mathbb{Q}$ as a $\mathbb{Z}$ module is divisible. Consider the canonical projection $\pi : \mathbb{Z}^{(I)} \to M$ where bases are mapped to generators. Then $M \simeq \mathbb{Z}^{(I)} / \ker \pi$, which embeds into $\mathbb{Q}^{(I)} / \ker \pi$. Since $\ker \pi$ is a submodule of $\mathbb{Z}^{(I)}$, $\mathbb{Q}^{(I)} / \ker \pi$ is divisible and thus injective; which satisfies the condition of interest.

Now consider the general case by reducing to the case of $\mathbb{Z}$-modules. As $\mathbb{Z}$ modules, there exists an injection $h : M \hookrightarrow Q$, where Q is an injective module. Q being injective indicates that the functor $\mathrm{Hom}_{\mathbb{Z}}(-, Q)$ is exact (on R-modules). But notice that by applying the adjoint property this gives

$$\mathrm{Hom}_{\mathbb{Z}}(-, Q) \simeq \mathrm{Hom}_{\mathbb{Z}}(R \otimes_R -, Q) \simeq \mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbb{Z}}(R, Q))$$

which indicates that the functor $\mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbb{Z}}(R, Q))$ is exact, i.e. $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an injective module. It then suffices to give an injective map from M to $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$, which is given by $u \mapsto (x \mapsto (h(xu)))$, where $u \in M$, and $x \in R$. It is well-defined and bilinear by inspection. □

The followings turn to the discussion of flat modules:

Remark 6.2.10. Since the functor $- \otimes M$ for a given R-module M is right exact, M is flat if and only if for all injective maps $M_1 \to M_2$, $M_1 \otimes M \to M_2 \otimes M$ is also injective.

Proposition 6.2.11. Given a family of left R-modules $(M_i)_{i \in I}$, $\bigoplus_{i \in I} M_i$ is flat if and only if M_i is flat for all i.

Proof. Since direct sum commutes with tensor product, given any injective R-linear map $N_1 \hookrightarrow N_2$, we have the following commutative diagram:

$$\begin{array}{ccc} N_1 \otimes (\bigoplus_{i\in I} M_i) & \xrightarrow{f} & N_2 \otimes (\bigoplus_{i\in I} M_i) \\ \downarrow\simeq & & \downarrow\simeq \\ \bigoplus_{i\in I}(N_1 \otimes M_i) & \xrightarrow{f'} & \bigoplus_{i\in I}(N_2 \otimes M_i) \end{array}$$

Notice f' is an injection if and only if f'_i is an injection for all i by the universal property of coproduct; and f is an injection if and only if f' is an injection, as the diagram should commute. □

Corollary 6.2.12. Projective modules are flat.

Proof. By Proposition 6.2.4, an R-module M is projective if and only if there exists R-modules F and N where F is free s.t. $F \simeq M \oplus N$. By the previous proposition, it suffices to prove that F is flat. Since $F \simeq \oplus_{i\in I} R^{(I)}$, it suffices to prove that R is flat. This is indeed the case as $- \otimes_R R = \mathrm{Id}_R$, which is trivially exact. □

Definition 6.2.13. Let R be a commutative ring, and $\varphi : R \to S$ specifies an R-algebra. Then S is a **flat R-algebra** if it is flat as an R-module.

Remark 6.2.14. This implies that the extension of scalar functor is exact, as by the fact that tensor product should be R-balanced, multiplication is indeed scalar multiplication on the R-module itself, which preserves injection.

Example 6.2.15. Consider the following flat structures:

- $R \to R[x_1, \cdots, x_n]$ is a flat R-algebra, as $R[x_1, \cdots, x_n]$ has a free R-module structure, where the basis is all monomials.
- Let $S \subseteq R$ be a multiplicative system. Then $R \to S^{-1}R$ is a flat R-algebra. It suffices to verify that $S^{-1}R \otimes -$ is exact. Notice $S^{-1}R \otimes M \simeq S^{-1}M$, this is the same as stating that $S^{-1}(-)$ is exact.

  Since $N \subseteq M \implies S^{-1}N \subseteq S^{-1}M$, $S^{-1}(-)$ preserves injections; and since $S^{-1}(M/N) \simeq S^{-1}M/S^{-1}N$, $S^{-1}(-)$ preserves surjection. Thus verifies the exactness and flatness.

Proposition 6.2.16. Let $(R, \mathfrak{m})$ be a local Noetherian ring, and M a finitely generated R-module. Then M is projective if and only if M is free.

Proof. It suffices to verify that M is free if it is projective. By Nakayama's Lemma, $(u_1, \cdots, u_m)$ forms a minimal system of generators of M if and only if $(\bar{u}_1, \cdots, \bar{u}_m)$ forms a basis in $M/\mathfrak{m}$, This is indeed the case, as denoting $N = (u_1, \cdots, u_m)$, this gives $N + \mathfrak{m}M = M$, which indicates that $N = M$. Minimality is given by the minimality of cardinality of basis. Choose $F = R^m$ with $\varphi : F \to M$ s.t. $\varphi(e_i) = u_i$ for all i. Since M is projective, consider the short exact sequence that splits:

$$0 \longrightarrow K \longrightarrow F \xrightarrow{\varphi} M \longrightarrow 0$$

To prove that M is free, it suffices to show that $K = 0$. Note that if $(a_1, \cdots, a_m) \in K$, then $\sum_{i=1}^m a_i u_i = 0 \implies \sum_{i=1}^m \bar{a}_i \bar{u}_i = 0 \implies \bar{a}_i = 0 \implies a_i \in \mathfrak{m}$ for all i since $\bar{u}_i$s give a basis. That is, $K \subseteq \mathfrak{m}R^m$. Now apply the functor $- \otimes R/\mathfrak{m}$. This is an additive functor, which preserves morphisms as it acts as a group homomorphism, i.e. split exact sequences remain split exact after applying the functor. This gives the sequence

$$0 \longrightarrow K/\mathfrak{m}K \xrightarrow{\alpha} F/\mathfrak{m}F \longrightarrow M/\mathfrak{m}M \longrightarrow 0$$

which is also split. Since $K \subseteq \mathfrak{m}R^m$, $K \subseteq \mathfrak{m}F$, which indicates that $\alpha = 0$. Since α is injective as the sequence is exact, $K/\mathfrak{m}K = 0 \implies K = 0$. The sequence being split exact gives $F \simeq M \oplus K$, which implies $F \simeq M$. □

Corollary 6.2.17. Let R be a Noetherian commutative ring, and M a finitely generated R-module. Them M is projective if and only if for all maximal ideals p in R, M_p is a free R_p module.

Proof. By Proposition 6.2.16, it suffices to show that M is projective if and only if for all maximal ideals p, the module M_p is a projective R_p module:

$\Rightarrow$: We prove a generalization of the statement. Let $\varphi : R \to S$ be a ring homomorphism, and M be a projective R-module, then $M \otimes_R S$ is a projective S-module. Since M is a projective R-module, there exists an R-module N s.t. $R^{(I)} \simeq M \oplus N$. As tensor product commutes with direct sum, this gives the isomorphism $(M \otimes_R S) \oplus (N \otimes_R S) \simeq R^{(I)} \otimes_R S \simeq S^{(I)}$.

$\Leftarrow$: Since for all maximal ideals p, M_p is a projective R_p module, by the definition of projective modules we have that for all R-modules A and B where there exists a surjective map $A \twoheadrightarrow B$, the morphism of R-modules $\mathrm{Hom}_{R_p}(M_p, A_p) \to \mathrm{Hom}_{R_p}(M_p, B_p)$ is surjective. Since tensor product is right exact, to show that $\mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B)$ is surjective it suffices to show that the map $\mathrm{Hom}_R(M, A) \otimes R_p \to \mathrm{Hom}_R(M, B) \otimes R_p$ is surjective. The identification is shown via the following proposition:

Proposition 6.2.18. Let ring S be a flat R-module, and $f : R \to S$ a ring homomorphism. Let M and N be R-modules. Then there is a canonical morphism of S-modules $\mathrm{Hom}_R(M, N) \otimes_R S \to \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)$ which is functorial w.r.t. M and N. Further, if R is Noetherian, and M is finitely generated, then this is an isomorphism.

Proof. Consider the morphism of R-modules $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)$, $f \mapsto f \otimes_R \mathrm{Id}_S$. Then by universal property of extension of scalars there exists a unique morphism of S-modules

$$\theta_M : \mathrm{Hom}_R(M, N) \otimes_R S \to \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S), \qquad f \otimes a \mapsto a(f \otimes \mathrm{Id}_S) \tag{$*$}$$

This is functorial w.r.t. both M and N. Now regard this as a contravariant functor where M is the argument: denote the morphism above to be $U(M) \to V(M)$. Observe the following facts:

- If $M = R$, then this is an isomorphism, as both sides are isomorphic to $N \otimes_R S$.
- If M is free, then this is also an isomorphism. This is a direct result of the fact above, and the fact that the functors are both additive, which commutes with direct sum.

Now consider the general case where M is finitely generated over a Noetherian ring R. Then there exists a free module F s.t. $F \to M$ is surjective, where e_i is mapped to u_i which gives a system of generators in M. R is Noetherian indicates that F is a Noetherian R-module, which gives that $K := \ker \varphi$ is finitely generated.

Then similarly it is possible to take a free module G where $G \to K$ is surjective. This gives an exact sequence $G \longrightarrow F \longrightarrow M \longrightarrow 0$. (as $\mathrm{im}\ (G \to F) = \ker(F \to M)$). Applying U and V on the exact sequence gives the commutative diagram where the rows are exact, and the blocks commute:

$$\begin{array}{ccccccccc} 0 & \dashrightarrow & 0 & \longrightarrow & U(M) & \longrightarrow & U(F) & \longrightarrow & U(G) \\ \vdots & & \vdots & & \downarrow{\scriptstyle \theta_M} & & \downarrow{\scriptstyle \theta_F} & & \downarrow{\scriptstyle \theta_G} \\ 0 & \dashrightarrow & 0 & \longrightarrow & V(M) & \longrightarrow & V(F) & \longrightarrow & V(G) \end{array}$$

The lines are indeed exact, as S is flat on R, which gives that $- \otimes_S N$ is right exact, and $\mathrm{Hom}(-, N)$ is left exact. By the results on free modules, θ_F and θ_G are isomorphisms, which implies that θ_M is also an isomorphism by the 5-lemma. □

This is indeed applicable, as in general localization preserves flatness. Consider M a flat R-module, S a multiplicative system in R, with an exact sequence $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$. To verify that this is true, it suffices to verify that the sequence $0 \longrightarrow A \otimes_{S^{-1}R} S^{-1}M \longrightarrow B \otimes_{S^{-1}R} S^{-1}M \longrightarrow C \otimes_{S^{-1}R} S^{-1}M \longrightarrow 0$ is exact. This is indeed true from the isomorphism

$$A \otimes_{S^{-1}R} S^{-1}M \simeq A \otimes_{S^{-1}R} (S^{-1}R \otimes_R M) \simeq (A \otimes_{S^{-1}R} S^{-1}R) \otimes_R M \simeq A \otimes_R M$$

indicates that the sequence can be identified with $0 \longrightarrow A \otimes_R M \longrightarrow B \otimes_R M \longrightarrow C \otimes_R M \longrightarrow 0$, which is exact as M is flat. In this case R itself is flat as an R-module, which indicates that R_p is also flat.

□

6.3 Complexes*

Recall that a complex is an infinite chain where the composition of any two successive morphisms gives zero. This section is devoted to further study this object.

First present another lemma which again uses the technique of "chasing the diagram":

Proposition 6.3.1 (The Snake Lemma)**.** Consider the diagram below, where all objects are in an additive category, where the rows are exact, blocks commute, and 0 denotes the zero object:

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array}$$

Then there exists an exact sequence

$$\ker a \longrightarrow \ker b \longrightarrow \ker c \xrightarrow{\delta} \operatorname{coker} a \longrightarrow \operatorname{coker} b \longrightarrow \operatorname{coker} c$$

where δ is known as the connecting homomorphism.

Sketch of Proof. The proof is done only for the case where the category is taken as ${}_R\mathrm{Mod}$.

First define the map. Let $x \in \ker c$. g being surjective implies that there exists some $y \in B$ s.t. $g(y) = x$. Denote $y' = b(y)$. By the fact that blocks commute, $g'(b(y)) = c(g(y)) = 0$, which implies that $y' \in \ker g'$. Since the second row is exact, y' is in the image of f', which implies that there exists some $z' \in A'$ s.t. $f'(z') = y'$. Define $\delta(x) = \bar{z'} \in A'/\operatorname{im} a$. This is a homomorphism as all maps used above are homomorphisms.

Now check that this map is well-defined. Since f' is injective by the exactness, it suffices to check that the choice of z does not vary w.r.t. the choice of y. Suppose that there exists $y_1, y_2 \in B$ s.t. $(y_1 - y_2) \in \ker g$. By the exactness of the top row there exists $\tilde{z} \in A$ s.t. $f(\tilde{z}) = y_1 - y_2$ as $\ker g = \operatorname{im} f$. Let z_1, z_2 be the corresponding output where y_1 and y_2 are used, respectively. By the commutativity of the left block, together with the fact that δ is a homomorphism, $z_1' - z_2' = a(\tilde{z})$, which indicates that they have the same image in $\operatorname{coker} a$.

Now check the exactness. Consider the expanded commutative diagram:

$$\begin{array}{ccccccccc}
 & & \ker a & \xrightarrow{\alpha} & \ker b & \xrightarrow{\beta} & \ker c & \xrightarrow{\delta} & \\
 & & \downarrow{\scriptstyle a_1} & & \downarrow{\scriptstyle b_1} & & \downarrow{\scriptstyle c_1} & & \\
 & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \\
0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \\
 & & \downarrow{\scriptstyle a_2} & & \downarrow{\scriptstyle b_2} & & \downarrow{\scriptstyle c_2} & & \\
 & \xrightarrow{\delta} & \operatorname{coker} a & \xrightarrow{\alpha'} & \operatorname{coker} b & \xrightarrow{\beta'} & \operatorname{coker} c & &
\end{array}$$

where the long exact sequence becomes

$$\ker a \xrightarrow{\alpha} \ker b \xrightarrow{\beta} \ker c \xrightarrow{\delta} \operatorname{coker} a \xrightarrow{\alpha'} \operatorname{coker} b \xrightarrow{\beta'} \operatorname{coker} c$$

Check the exactness respectively:

- At $\ker b$. We only need to show $\operatorname{im}\alpha = \ker\beta$. Since a_1, b_1 and c_1 are embeddings, this is just given by $\ker\beta = \ker b \cap \ker g$.
- At $\ker c$. We need to show that $\operatorname{im}\beta = \ker\delta$. $x \in \operatorname{im}\beta$ implies that the corresponding y' is zero. Then by injectivity of f' this gives $\delta(x) = 0$, which gives $x \in \ker\delta$.

The exactness at rest two objects can be verified using a symmetric argument. □

Now we turn to the subject of complexes.

Definition 6.3.2 (Morphism of Complexes). Let K° and L° be complexes whose objects are R-modules. A morphism of complexes $f : K^\circ \to L^\circ$ is given by a family of R-linear maps $f^n : K^n \to L^n$ s.t. all the squares in the following diagram is commutative:

$$\begin{array}{ccccccc}
\cdots & \longrightarrow & K^n & \longrightarrow & K^{n+1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f^n} & & \downarrow{\scriptstyle f^{n+1}} & & \\
\cdots & \longrightarrow & L^n & \longrightarrow & L^{n+1} & \longrightarrow & \cdots
\end{array}$$

Remark 6.3.3. Clearly commutative is transited through composition of morphisms. Since ${}_R\underline{\mathrm{Mod}}$ gives an additive category structure, this is also a category $\underline{\mathrm{Kom}}({}_R\underline{\mathrm{Mod}})$ (or $\underline{\mathrm{Kom}}_R$).

Definition 6.3.4 (Cohomology). For a complex $K^\circ : \cdots \xrightarrow{d^{n-1}} K^n \xrightarrow{d^n} K^{n+1} \longrightarrow \cdots$, the n-**th cohomology** of K° is defined as $H^n(K) := \ker(d^n)/\operatorname{im}(d^{n-1})$.

Remark 6.3.5. Cohomology measures how far a point in the complex is from being exact. The complex K° is exact if and only if $H^n(K^\circ) = 0$ for all n.

Proposition 6.3.6. $H^n : \underline{\mathrm{Kom}}_R \to {}_R\underline{\mathrm{Mod}}$ is a functor.

Proof. Define $H^n(f) := f^n$ which is the mapping $H^n(K^\circ) \to H^n(L^\circ)$. Check according to the definition:

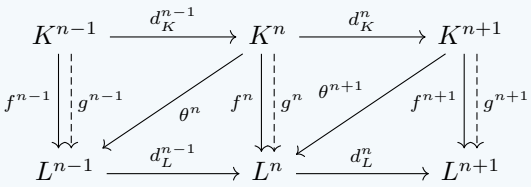
- For any complex K°, $H^n(K^\circ)$ is by definition an R-module.
- Identity is mapped to identity, as the same complex has the same cohomology.
- $H^n(f \circ g) = H^n(f) \circ H^n(g)$ by the commutativity of the diagram.

□

Definition 6.3.7. Suppose that $f, g >: K^\circ \to L^\circ$ be morphism of complexes. Then f is **homotopic** to g (denoted $f \sim g$) if there exists R-linear maps $\theta^n : K^n \to L^{n-1}$ for all $n \in \mathbb{Z}$, s.t.

$$f^n - g^n = d_L^{n-1} \circ \theta^n + \theta^{n+1} \circ d_K^n \quad \forall n \in \mathbb{Z}$$

It may be clearer to consult the following diagram:



Remark 6.3.8. Homotopy implies that they induces the same cohomology everywhere. That is, if $f \sim g$, Consider for $x \in \ker d_K^n$,

$$f^n(x) - g^n(x) = d_L^{n-1} \circ \theta^n(x) + \theta^{n+1} \circ d_K^n(x) = d_L^{n-1} \circ \theta^n(x) \in \operatorname{im} d_L^{n-1} = \ker d_L^n$$

Remark 6.3.9. If $F : {}_R\underline{\mathrm{Mod}} \to {}_S\underline{\mathrm{Mod}}$ is an additive functor, then

- If K° is a complex, then the chain given by $\cdots \xrightarrow{F(d^{n-1})} F(K^n) \xrightarrow{F(d^n)} F(K^{n+1}) \xrightarrow{F(d^{n+1})} \cdots$ is also a complex. Exactness follows directly from considering the image of the corresponding submodules after applying the functor.
- Let $f = (f^n) : K^\circ \to L^\circ$ be a morphism of complex. Then $F(f)$ is also a morphism of complex.
- If $f \sim g$, then $F(f) \sim F(g)$, as functors by definition commutes with composition; and additive functors commute with addition.

Proposition 6.3.10. Given a short exact sequence of complexes $0 \longrightarrow K^\circ \xrightarrow{f} L^\circ \xrightarrow{g} M^\circ \longrightarrow 0$ (tjhat is, for all n the sequence with corresponding maps $0 \longrightarrow K^n \longrightarrow L^n \longrightarrow M^n \longrightarrow 0$ is exact), then there exists a canonical morphism $H^{n-1}(M^\circ) \xrightarrow{\delta^{n-1}} H^n(K^\circ)$ for all n s.t. we have a "long exact sequence in cohomology":

$$\cdots \longrightarrow H^n(K^\circ) \xrightarrow{H^n(f)} H^n(L^\circ) \xrightarrow{H^n(g)} H^n(M^\circ) \xrightarrow{\delta^n} H^{n+1}(K^\circ) \longrightarrow \cdots$$

Proof. Notice that $(\ker d_M^n / \operatorname{im} d_M^{n-1})$ and $(\ker d_M^{n+1} / \operatorname{im} d_M^n)$ are the kernel and cokernel of d_M^n, respectively. Applying Snake Lemma gives the desired result. □

6.4 Projective and Injective Resolution*

Definition 6.4.1 (Projective Resolution). Given an R-module M, a **projective resolution** of M $P_\bullet$ is a complex

$$\cdots \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow 0$$

where all P_is are porjective, together with a map $P_\bullet \to M$ s.t. the following sequence is exact:

$$\cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

The projective resolution is often simply denoted by $P_\bullet \to M$.

Proposition 6.4.2. Projective resolution approximates an exact sequence to a module:

i) Every R-module M has a projective resolution.

ii) Given any morphism $f : M \to M'$ and projective resolutions $P_\bullet \to M$ and $P'_0 \to M'$, there exists $F : P_0 \to P'_0$ a morphism of complex s.t. the diagram is commutative:

$$\begin{array}{ccc} P_0 & \longrightarrow & M \\ \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle f} \\ P'_0 & \longrightarrow & M' \end{array}$$

Proof. Construct the proof correspondingly:

i) Consider $P_\bullet \to M$ be the map where P_0 is free; and elements in the basis is mapped to the system of generators. Similarly let $f_n : P_{n+1} \to \ker f_{n-1}$ be a similar map. This gives the construction of an infinite chain.

ii) Similarly, do this inductively. Since P_0 is projective, by definition there exists F_0 s.t. $f \circ \varepsilon = \varepsilon' \circ F_0$ (via considering $P'_0 \to M'$ be the projection). Commutativity gives $F_0(\ker \varepsilon) \subseteq \ker \varepsilon'$. Repeat via replacing M, M' with $\ker \varepsilon$ and $\ker \varepsilon'$ respectively.

□

Remark 6.4.3. If there exists two functors F and F' which both satisfy the condition in ii), then $F \sim F'$. The proof is similar to what presented above.

Definition 6.4.4 (Injective Resolution). Dually, an **injective resolution** of an R-module M is given by a complex

$$0 \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \cdots$$

with I^n injective for all n; and a morphism $M \to I$ s.t. the following sequence is an exact complex:

$$0 \longrightarrow M \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \cdots$$

Remark 6.4.5. The corresponding propositions as above also hold under the context of injective modules, as by Thoerem 6.2.6 every module can be embedded into some injective module.

6.5 Derived Functors*

Definition 6.5.1 (Homological δ-Functor)**.** Let $F : {}_R\underline{\text{Mod}} \to {}_S\underline{\text{Mod}}$ be a right exact functor (e.g. $F = N \otimes_R -$ for N an S-R bimodule). For all left R-module M, choose a projective resolution $P_\bullet \to M$. Define the **homological δ-functor** $L_iF(M) := H_i(F(P_\bullet)) = \ker \beta / \text{im } \alpha$ for $F(P_{i+1}) \xrightarrow{\alpha} F(P_i) \xrightarrow{\beta} F(P_{i-1})$. For morphisms, given two projective resolutions $P_\bullet \to M$, $P'_\bullet \to M'$ with $f : M \to M'$ R-linear, define $L_IF(f) := H_i(F(P_0)) \to H_i(F(P'_0))$.

Remark 6.5.2. The choice of g does not matter, as this is a map on the cohomology, which only makes classification up to homotopy class.

Remark 6.5.3. Define $g : P_\bullet \to P'_\bullet$ s.t. $L_iF(f) = H_i(F(g))$. Let $P_\bullet \to M$ and $\tilde{P}_\bullet \to M$ be two projective resolutions of M. Then $g \circ h$ (and $h \circ g$) are homotopic to identity. (Applying H_i they are inverse isomorphisms) This implies that up to a canonical isomorphism, the definition does not depend on the choice of resolution.

Definition 6.5.4. The Tor functor is defined as $\text{Tor}_i^R(N, M) := L_iF(M)$ for $F = N \otimes_R -$.

Remark 6.5.5. We have the isomorphism $L_0F \simeq F$, as $L_0F = H_0(\cdots \longrightarrow F(P_1) \longrightarrow F(P_0) \longrightarrow 0) = \text{coker } (F(P_1) \to F(P_0)) \simeq F(M)$ since F is right exact.

Remark 6.5.6. Similar to the previous chapter where we have the long exact sequence in cohomology, using the same strategy we can prove that there exists a long exact sequence for derived functors. Given the short exact sequence $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$, we have

$$L_1F(M') \longrightarrow L_1F(M) \longrightarrow L_1F(M'') \longrightarrow F(M') \longrightarrow F(M) \longrightarrow F(M'') \longrightarrow 0$$

Chapter 7

Multilinear Algebra

7.1 The Tensor Algebra

Definition 7.1.1 (Multilinear). Let R be a commutative ring, and $M_1, \cdots, M_n, N$ be R-modules. A map $\varphi : M_1 \times \cdots \times M_n \to N$ is **multilinear** if for all $i \in [\![1, n]\!]$, for all $x_j \in M_j$ for $j \neq i$, the map $\varphi(x_1, \cdots, x_{i-1}, -, x_{i+1}, \cdots, x_n) : M_i \to M$ is R-linear.

Remark 7.1.2. Via performing induction on n, it can be shown that for a multilinear map $f : M_1 \times \cdots \times M_n \to N$, with the tensor map $\varphi : M_1 \times \cdots \times M_n \to M_1 \otimes_R \cdots \otimes_R M_n$ (which is multilinear), there exists a R-linear map $g : M_1 \otimes_R \cdots \otimes_R M_n \to P$ s.t. $g \circ \varphi = f$.

Definition 7.1.3 (Tensor Algebra). Let M be a fixed R-module. Define $T^0(M) := R, T^1(M) = M$; and for $n \geq 2$, define $T^n(M) := \underbrace{M \otimes_R \cdots \otimes_R M}_{n \text{ times}}$. Then the **tensor algebra** is defined as

$$T(M) := \bigoplus_{i \geq 0} T^i(M) = R \oplus M \oplus (M \otimes_R M) \oplus \cdots$$

Remark 7.1.4. Since for all i, $T^i(M)$ has an R-module structure, $T(M)$ is also an R-module.

Proposition 7.1.5. $T(M)$ also has an R-algebra structure.

Proof. It suffices to define multiplication for each summand of $T(M)$ and check that it is well-defined. Define

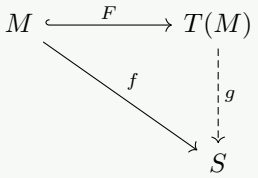
$$\alpha_{ij} : T^i(M) \times T^j(M) \to T^{i+j}(M), \quad (a_1 \otimes \cdots \otimes a_i, b_1 \otimes \cdots \otimes b_j) \mapsto (a_1 \otimes \cdots \otimes a_i \otimes b_1 \otimes \cdots \otimes b_j)$$

This is indeed well-defined, as by applying the universal property of tensor product for i times gives the desired map. Notice that for the case where $i = 0$ or $j = 0$ this is just scalar multiplication, this is just scalar multiplication. □

Remark 7.1.6. This can be extended to a map $T(M) \times T(M) \to T(M)$, which makes $T(M)$ a ring. The map is given by for $x = \oplus_{i\geq 0} x_i$, $y = \oplus_{j\geq 0} y_j$, the multiplication is defined as $x \cdot y = \oplus_{i,j\geq 0} \alpha_{i,j}(x_i, y_j)$, with $1 \in T^0(M) = R$. Moreover, the inclusion $R = T^0(M) \hookrightarrow T(M)$ is a ring homomorphism which makes $T(M)$ an R-algebra.

Remark 7.1.7. Notice that this differs from the polynomial ring in that it is not commutative (in terms of the direct summands). Therefore, the terms in $\oplus_{i,j}\alpha_{ij}$ cannot be collected into one. $T^n = M \otimes \cdots \otimes M$ has a basis given by $x_{i_1} \otimes \cdots \otimes x_{i_n}$, where $i_k \in [\![1, d]\!]$ for all $k \in [\![1, n]\!]$. Therefore, for $n \geq 2$, $T^n(M)$ is not commutative.

Proposition 7.1.8 (Universal Property of $T(M)$)**.** Consider the (forgetful) functor $F :_R \underline{\text{Alg}} \to {}_R\underline{\text{Mod}}, M \mapsto T(M)$. Let M be an R-module and S an R-algebra. If $f : M \to S$ is a morphism of R-modules, then there exists a unique morphism of R-algebras $g : T(M) \to S$ s.t. $g|_{T^1(M)} = f$, i.e. $g \circ F = f$:



Proof. Apply the universal property of tensor product and direct sum.

Define $f_n : \underbrace{M \times \cdots \times M}_{n \text{ times}} \to S$, where $f_n(x_1, \cdots, x_n) = f(x_1) \cdots f(x_n)$. This is clearly multilinear, which implies that there exists a unique R-linear map $g_n : T^n(M) \to S$ s.t. $g_n(x_1 \otimes \cdots \otimes x_n) = f(x_1) \cdots f(x_n)$. Apply the universal property of direct sum on the superscript gives that there exists a unique R-linear map $g : T(M) \to S$ s.t. $g|_{T^n(M)} = g_n$. Check the followings:

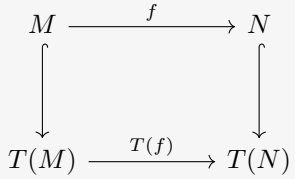
- g is a morphism of R-algebras. Since it is already a morphism of R-modules, it suffices to check that this definition is compatible with multiplication. For $x = \oplus_{i=0}^n x_i, y = \oplus_{j=0}^m y_j$, this gives

  $$g(x \cdot y) = g(x_0 \otimes \cdots \otimes x_n \otimes y_0 \otimes \cdots \otimes y_m) = \Pi_{i=0}^n f(x_i) \cdot \Pi_{j=0}^m f(y_j) = g(x_0 \otimes \cdots \otimes x_n) \cdot g(y_0 \otimes \cdots \otimes y_m) = g(x) \cdot g(y)$$

- g is the unique morphism of R-algebras $T(M) \to S$, s.t. $g|_{T^1(M)} = f$. This is clear as defining $g|_{T^1(M)}$ gives the map on $g|_{T^n(M)}$ for all n, as by the definition of the multiplication. Furthermore, the map restricted to $T^0(M)$ is given by the associated morphism with the R-algebra S. Both of which are uniquely determined.

□

Remark 7.1.9. This makes T a functor, which maps from R-modules to R-algebras. For all R-linear maps $f : M \to N$, there exists a unique morphism of R-algebras $T(f)$ s.t. the following diagram commutes:



This makes T a functor as it preserves compositions. Further this is the left adjoint of the forgetful functor G which only regards S as an R-module, i.e. we have the following isomorphism

$$\text{Hom}_{R\underline{\text{Alg}}}(T(M), S) \simeq \text{Hom}_R(M, G(S))$$

as by the universal property of tensor algebra the morphism from $T(M)$ to S is uniquely defined by the map $f : M \to S$.

Definition 7.1.10 (Graded Ring). A ring R is a **graded ring** if it comes with a decomposition $R = \oplus_{i\geq 0} R_i$ as abelian groups; and multiplication satisfies the relation $R_p \cdot R_q \subseteq R_{p+q}$ for all $p, q \geq 0$.

Remark 7.1.11. Consider the subring $R \subseteq R_0$. If R_0 lies in the center of R, i.e. $R_0 \subseteq \{a \in R \mid ab = ba \forall b \in R\}$, then R becomes an R_0-algebra; and the decomposition $R = \oplus_{i\geq 0} R_i$ is a direct sum of R_0-modules.

Example 7.1.12. Consider the following examples of graded rings:

1. The tensor algebra $T(M)$ is a graded ring, where $R_0 = T^0(M) = R$
2. The multivariate polynomials $S = R[x_1, \cdots, x_n]$ is a graded ring, where $S_d = \oplus_{\{i_1,\cdots,i_d | \sum_k i_k = d\}} R x_1^{i_1} \cdots x_d^{i_d}$.

Definition 7.1.13 (Homogeneous). If $R = \oplus_{i\geq 0} R_i$ is a graded ring, the elements of R_n are **homogeneous of degree** n.

Definition 7.1.14 (Morphism of Graded Rings). If R and S are graded rings, then a morphism of graded rings $f : R \to S$ is a ring homomorphism s.t. $f(R_i) \subseteq S_i$ for all i. Such definition gives the result that graded rings form a category.

Definition 7.1.15 (Homogeneous Ideal). If R is a graded ring, and $I \subseteq R$ an ideal. I is a **homogeneous ideal** if $I = \oplus_{i\geq 0}(I \cap R_i)$. Equivalently, for all $f \in I$, for all $f_i \in R_i$ s.t. $f = \sum_{i=0}^{d} f_i$, then $f_j \in I$ for all j.

Remark 7.1.16. If further I is two-sided, then $R/I = \oplus_{i\geq 0}(R_i/(R_i \cap I))$ as a direct sum of abelian groups. In this case, R/I is a graded ring, and the quotient $\pi : R \to R/I$ is a morphism of graded rings.

Proposition 7.1.17. Let R be a graded ring, and $I \subseteq R$ an ideal. Then I is homogeneous if and only if it can be generated by homogeneous elements.

Proof. Show implication in two directions:

$\Rightarrow$: Since I is homogeneous, there exists ideals $I_k \subseteq R_k$ s.t. $I = \oplus_{k\geq 0} I_k$. Then it is generated by the generating sets of I_k, which are all homogeneous.

$\Leftarrow$: If I can be generated by homogeneous elements, then for all $x \in R$ there exists a decomposition

$$x = \sum_{r\in R} c_r r = \sum_{i\geq 0} \sum_{r\in R_i} c_{ri} r_i$$

where only finitely many c_{ri}s can be non-zero, and $r_i \in I$. Collecting all the terms in the inner summation gives $x = \sum_{i\geq 0} c_i r_i$ for $r_i \in I_i \subseteq R_i$, which satisfies the definition of homogeneous ideals.

□

Remark 7.1.18. It is not necessary (and also not true) that all the homogeneous elements must (can) have the same degree. For example, it is completely valid to have $R \cdot (I \cap R_0) \subsetneq I \cap R_1$, which prevents any homogeneous generating set of the same degree from existing.

7.2 Exterior and Symmetric Algebra

Definition 7.2.1 (Symmetric, Alternating Maps). Let R be a commutative ring, with M and N R-modules. Let $\varphi : M^n \to N$ be a multilinear map. It is defined to be:

i) **Symmetric**, if for all $\sigma \in S_n$, and for all $x_1, \cdots, x_n \in M$, $\varphi(x_1, \cdots, x_n) = \varphi(x_{\sigma(1)}, \cdots, \varphi(x_{\sigma(n)}))$.

ii) **Alternating**, if $\varphi(x_1, \cdots, x_n) = 0$ whenever $x_i = x_j$ for $i \neq j$. This is equivalent to stating that φ is **skew-symmetric**, where $\varphi(x_1, \cdots, x_i, \cdots, x_j, \cdots, x_n) = -\varphi(x_1, \cdots, x_j, \cdots, x_i, \cdots, x_n)$ for all $i < j$.

Remark 7.2.2. Since all elements in S_n (symmetric group) are generated by transpositions, to show that a map is symmetric it suffices to show the equality for all transpositions.

Definition 7.2.3 (Exterior Algebra). Let T be the tensor algebra, with J_n an T^n-submodule generated by $\{x_1 \otimes \cdots \otimes x_n \mid x_i = x_j \ \forall i \neq j\}$. Define $\Lambda^n(M) := T^n(M)/J_n$; and the **exterior algebra** $\Lambda(M) := \oplus_{n \geq 0} \Lambda^n(M)$. The algebra structure is inherited from that of the tensor algebra.

Remark 7.2.4. Consider the ideal $J := \oplus_{i \geq 2} J_n \subseteq T(M)$. Here only summands with degree greater than or equal to 2 are taken into consideration as the definition "alternating" makes no sense for the lower degree cases. This is a two-sided ideal as tensor product is R-balanced; and each summand is an element in J_n for some n. It is further homogeneous, as by definition. In this notation the exterior algebra can also be expressed as $\Lambda(M) := T(M)/J$.

Remark 7.2.5. The equivalence class of $x_1 \otimes \cdots \otimes x_n$ in $\Lambda(M)$ is often denoted as $x_1 \wedge \cdots \wedge x_n$, i.e. the wedge product.

Proposition 7.2.6 (Universal Property of $\Lambda^n(M)$). The map $\varphi : M^n \to \lambda^n(M)$, $(x_1, \cdots, x_n) \mapsto x_1 \wedge \cdots \wedge x_n$ is an alternating multilinear map; and for all alternating multilinear map $\psi : M^n \to P$, there exists a unique R-linear map $f : \Lambda^n(M) \to P$ s.t. $f \circ \varphi = \psi$

Proof. This follows directly from the definition of the exterior algebra, and the universal property of tensor product. □

Example 7.2.7. If $g : M \to P$ is an R-linear map, then this gives an R-linear map $\Lambda^n g : \Lambda^n(M) \to \Lambda^n(P)$ for all n, s.t. $x_1 \wedge \cdots \wedge x_n \mapsto g(x_1) \wedge \cdots \wedge g(x_n)$. The construction implies that combining all $\Lambda^n g$s gives a morphism of graded R-algebra.

Proposition 7.2.8. If $(x_1, \cdots, x_d)$ is a system of generators of M, then $\Lambda^n(M)$ is generated as an R-module by $\{x_{i_1} \wedge \cdots \wedge x_{i_n} \mid 1 \leq i_1 < \cdots < i_n \leq d\}$. In particular, for all $n > d$, $\Lambda^n(M) = 0$, which implies that $\Lambda(M)$ is a finitely generated R-module.

Proof. For the cases where $n \leq d$, the result follows from the fact that the tensor of several modules is generated by the tensor of the generators of the corresponding modules; and multilinear maps into the tensor product is alternating. □

Proposition 7.2.9. M is a free, finitely generated R-module, with basis $(x_1, \cdots, x_d)$. Then for all $n \leq d$, $\Lambda^n(M)$ is free with basis given by $\{x_{i_1} \wedge \cdots \wedge x_{i_n} \mid 1 \leq i_1 < \cdots < i_n \leq d\}$. Its rank is $\binom{d}{n}$.

Proof. By the previous proposition, we only need to show that all the elements are linearly independent over R. Since the tensor product is commutative, fix the representation for e_I for $I \subseteq \{1, \cdots, d\}$ to be $e_I = x_{i_1} \wedge \cdots \wedge x_{i_n}$ for $i_1 < \cdots < i_n$.

Now consider the Is respectively. For a fixed I, define $\bar{I} := \{1, \cdots, d\} \backslash I$. By the fact that maps into the exterior algebra is alternating, we have

$$0 = e_{\bar{I}} \wedge \sum_{|J|=n} a_J e_J = \sum_{|J|=n} a_J (e_{\bar{I}} \wedge e_J) = a_I (x_1 \wedge \cdots \wedge x_n) \tag{$*$}$$

We now seek to prove that $a_I = 0$ for all I, via apply a transformation into R. Consider the map $\psi : M^d \to R$ s.t. $\psi(u_1, \cdots, u_d) = \det(a_{ij})$, where $u_i = \sum_{i=1}^n a_{ij} x_j$, which is multilinear and alternating by construction. Then, by the universal property of exterior algebra, there exists a map $f : \Lambda^d(M) \to R$ s.t. $\psi(u_1, \cdots, u_d) = f(u_1 \wedge \cdots \wedge u_d)$. In particular, $f(x_1 \wedge \cdots \wedge x_d) = 1$. Applying f to ($*$) gives $a_I = 0$, which gives as a consequence the linear independence. □

Definition 7.2.10 (Symmetric Algebra)**.** Define I as the two-sided ideal generated by elements in the form of $\{x \otimes y - y \otimes x \mid x, y \in M\}$. The **symmetric algebra** $S(M) := T(M)/I$. This is a commutative R-algebra.

Remark 7.2.11. By construction I is generated by homogeneous elements of degree 2, which is a homogeneous ideal (with $I_0 = I_1 = \{0\}$). This gives an alternative expression for the symmetric algebra

$$S(M) = \bigoplus_{n \geq 0} \frac{T^n(M)}{I \cap T^n(M)}$$

which indicates that this is a graded ring. The denominator $I \cap T^n(M)$ is often denoted $S^n(M)$ or $\mathrm{Sym}^n(M)$.

Proposition 7.2.12 (Universal Property of $S(M)$)**.** $S(M)$ is a commutative R-algebra; and we have an inclusion $M \hookrightarrow S(M)$ which gives an isomorphism $M \simeq S^1(M)$. If S is a commutative R-algebra, and $\beta : M \to S$ is a R-linear map, then there exists a unique R-algebra homomorphism $f : S(M) \to S$ s.t. $f \circ \alpha = \beta$.

Proof. By the universal property of $T(M)$, there exists a unique R-algebra homomorphism $\tilde{\beta} : T(M) \to S$ s.t. $\tilde{\beta} \mid_M = \alpha$. Since S is commutative, $I \subseteq \ker(\tilde{\beta})$. By the universal property of quotient, there exists a unique morphism $\beta : S(M) \to S$ s.t. $\beta \mid_M = \alpha$. □

Example 7.2.13. Let M be a free R-module, with basis $x_1, \cdots, x_n$. The above universal property gives the isomorphisms where S is a commutative R-algebra:

$$\{R\text{-algebra homomorphisms } S(M) \to S\} \simeq \{R\text{-linear maps } M \to S\} \simeq \{\text{maps } \{x_1, \cdots, x_n\} \to S\}$$

which implies that $S(M)$ satisfies the universal property of multivariate polynomials, i.e. we have the isomorphism $S(M) \simeq R[x_1, \cdots, x_n]$.

Example 7.2.14. Let $\varphi : M^p \to T^p(M) \to S^p(M)$ be a symmetric multilinear map. For every symmetric multilinear map $\psi : M^p \to N$, there exists a unique R-linear map $f : S^p(M) \to N$ s.t. $\psi = f \circ \varphi$. This can be proved similarly using the

universal property of quotient rings.

7.3 Symmetric, Alternating and Hermitian Forms

Definition 7.3.1 (Hermitian)**.** Let E be a finite-dimensional $\mathbb{C}$-vector space. $g : E \times E \to \mathbb{C}$ is **Hermitian** if:

i) $g(-, v)$ is linear for all $v \in E$.

ii) $\overline{g(v, -)}$ is linear for all $v \in E$.

iii) $g(v, w) = \overline{g(w, v)}$ for all $v, w \in E$.

Remark 7.3.2. By the definition, if $v = w$ this gives $g(v, v) = \overline{g(v, v)}$, which implies that $g(v, v) \in \mathbb{R}$ if g is Hermitian.

Definition 7.3.3. The **kernel** of a bilinear (Hermitian) map g is defined as

$$\ker(g) := \{v \in E \mid g(v, w) = 0 \ \forall w \in E\}$$

which is a linear subspace of E.

Definition 7.3.4 (Orthogonality)**.** Let $F \subseteq E$ be a linear subspace. Then its **orthogonal complement** $F^\perp := \{v \in E \mid g(v, w) = 0 \ \forall w \in F\}$. which is a linear subspace of E. Two vector subspaces $F_1, F_2 \subseteq E$ are **orthogonal** if $F_1 \subseteq F_2^\perp$, which is equivalently $g(v, w) = 0$ for all $v \in F_1, w \in F_2$.

Example 7.3.5. $E^\perp$ w.r.t. g is the kernel of g.

Remark 7.3.6. For orthogonal vector subspaces F_1 and F_2, it is often denoted $F_1 \perp F_2$ for $F_1 \subseteq F_2^\perp$; and $E = F_1 \perp F_2$ if $E = F_1 \oplus F_2$ for $F_1 \perp F_2$.

Definition 7.3.7. A bilinear (Hermitian) form g is **nondegenerate** if $\ker(g) = 0$.

Remark 7.3.8. If $W \subseteq E$ is a subspace s.t. $E = \ker g \perp W$, then $g|_W$ is nondegenerate.

Suppose that there exists $x \in W$ s.t. $x \in \ker g|_W$. By definition $g(x, y) = 0$ for all $y \in \ker g$. This implies that $x \in \ker g$, which contradicts with the hypothesis that E is the internal direct sum of $\ker g$ and W.

Proposition 7.3.9. Let $F \subseteq E$ be a linear subspace. Suppose that g is nondegenerate. Then

i) $\dim F^\perp + \dim F = \dim E$; and $(F^\perp)^\perp = F$.

ii) The following statements are equivalent:

(a) $g|_{F \times F}$ is nondegenerate.

(b) $E = F \perp F^\perp$.

(c) $g|_{F^\perp \times F^\perp}$ is nondegenerate.

Proof. Consider V^* to be the dual vector space of V, which is $\mathrm{Hom}_K(V, K)$ for g bilinear, and conjugate linear maps for G Hermitian. Since to specify the linear maps it suffices to specify where the basis is mapped to, $\dim_K(V) = \dim_K(V^*)$. This gives a natural map $\varphi : E \to E^*$ defined as $\varphi(v) := g(v, -)$. φ is further an isomorphism, as since g is nondegenerate $\ker g = 0$; and by construction $\ker \varphi = \ker g$.

Define $K := \ker(E^* \to F^*)$. This gives an exact sequence

$$0 \longrightarrow K \longrightarrow E^* \longrightarrow F^* \longrightarrow 0$$

where since $F^\perp = \varphi^{-1}(K)$ we have $\dim F^\perp = \dim K = \dim E - \dim F$. By definition $F \subseteq (F^\perp)^\perp$; and applying the above argument again gives $\dim F = \dim(F^\perp)^\perp$.

For the second argument, $g|_{F\times F}$ being nondegenerate implies that $F \cap F^\perp = \{0\}$, indicating that $E = F \perp F^\perp$. Applying symmetric argument gives the other equivalence. □

Definition 7.3.10. If g is symmetric of Hermitian, an **orthogonal basis** of E is a basis $(e_1, \cdots, e_n)$ s.t. for all $i \neq j$, $g(e_i, e_j) = 0$.

Remark 7.3.11. This definition is meaningless for g being alternating, as by definition $g(e_i, e_i) = 0$, which implies that the whole space is the kernel of g.

Proposition 7.3.12. If g is Hermitian; or g is symmetric with $\mathrm{char}(K) \neq 2$, then there exists an orthogonal basis.

Proof. Perform induction on the dimension of the vector space. Since the base case is vacuous, it suffices to show the inductive step.

Suppose that the above proposition is true for vector spaces whose dimension is no greater than d. Consider a vector space E over K s.t. $\dim E = d + 1$. Let $F \subseteq E$ to be a vector subspace with dimension d, and $v \in E \setminus F$ s.t. $g(v, v) \neq 0$. Assume that g is non-degenerate (or otherwise consider W where $E = \ker(g) \oplus W$; and set up the dimensions accordingly). Now consider the cases separately:

- g is symmetric. Since 2 is invertible, for all $v, w \in E$, $g(v, w) = 2^{-1}(g(v + w, v + w) - g(v, v) - g(w, w))$. which can be set to 0 for suitable choice of v.
- g is Hermitian. Consider separately the real part and the imaginary part. The above construction gives

  $$g(v, w) + g(w, v) = g(v + w, v + w) - g(v, v) - g(w, w)$$

  which indicates that $\mathrm{Re}(g(v, w)) = 0$. Further consider $g(iv, w)$, which gives $\mathrm{Im}(g(v, w)) = 0$.

Since $g_{F\times F}$ is nondegenerate (by the choice of v), $E = F \perp F^\perp$, which indicates that the basis of F and $F^\perp$ combined gives an orthogonal basis. □

Theorem 7.3.13 (Sylvester)**.** If g is a symmetric and nondegenerate bilinear form over $K = \mathbb{R}$, then there exists $r \in \mathbb{N}$ s.t. for all orthogonal basis $(e_1, \cdots, e_n)$, from the sets $g(e_k, e_k)$ for $k \in [\![1, n]\!]$ exactly r out of them are positive, and the rest

are negative since g is nondegenerate. For the r defined as above $(r, \dim E - r)$ is defined as the **signature** of g.

Proof. Let (e_i) and (e'_i) be two orthogonal bases. Define $a_i = g(e_i, e_i)$, and $b_j = g(e'_j, e'_j)$ for all i and j. Reorder the basis s.t. $a_i > 0$ if and only if $i \leq r$; and $b_j > 0$ if and only if $j \leq s$. We would like to show that $r = s$, via showing $r \leq s$ through the fact that $(e_1, \cdots, e_r, e'_{s+1}, \cdots, e'_n)$ are linearly independent; and by symmetric argument.

Suppose

$$\sum_{i=1}^{r} \alpha_i e_i - \sum_{j=1}^{n-s} \beta_j e'_{s+j} = 0$$

define u as such and notice the follows:

$$u = \sum_{i=1}^{r} \alpha_i e_i = \sum_{j=1}^{n-s} \beta_j e'_{s+j} \implies g(u,u) = \underbrace{\sum_{i=1}^{r} \alpha_i^2 a_i}_{\geq 0} = \underbrace{\sum_{j=1}^{r} \beta^2 b_{s+j}}_{\leq 0}$$

which implies that $\alpha_i = \beta_j = 0$ for all $i \leq r, j \leq s$. □

Remark 7.3.14. For the Hermitian case, since $g(r, r) \in \mathbb{R}$ for all r, the proof is exactly the same via replacing α_i^2 by $\alpha_i \cdot \overline{\alpha_i}$ and same for β_js.

Remark 7.3.15. If $e_i, \cdots, e_n$ is an orthogonal basis of g, one can find λ_i s.t. $e'_i = \lambda_i e_i$ satisfying that $g(e'_i, e'_i) = \pm 1$ for all i. Such (e'_i) gives an **orthonormal basis**.

Definition 7.3.16. A symmetric (Hermitian) bilinear form g is **positive definite** if it is nondegenerate with signature $(\dim E, 0)$. Equivalently, g is positive definite if and only if $g(v, v) > 0$ for all $v \in E$ s.t. $v \neq \{0\}$.

Example 7.3.17. If H is a positive definite Hermitian form, with $(e_1, \cdots, e_n)$ an orthonormal basis, then for $v = \sum_i \alpha_i e_i$ and $w = \sum_j \beta_j e_j$, $H(v, w) = \sum_i \alpha_i \overline{\beta_i}$.

Proposition 7.3.18. If g is a nondegenerate alternating form, then $E = E_1 \perp \cdots \perp E_m$; and each E_i has a basis (u_i, v_i) s.t. $g(u_i, v_i) = 1$ for all i.

Proof. For $v, u \in E$ which are linearly independent, g being alternating implies $g(v, u) = 0$. Further if there exists $u_1, u_2 \in E$ s.t. $g(v, u_1) \neq 0$, $g(v, u_2) \neq 0$, this gives that there exists $c \in K$ s.t. $g(v, u_1 - cu_2) = 0$ which implies that (v, u_1, u_2) is not linearly independent. □

7.4 The Spectral Theorem

Remark 7.4.1. Fix the notation. For g being symmetric bilinear or Hermitian, $g(-,-)$ is often denoted as $\langle -, - \rangle$.

In this part two kinds of maps are considered:

1. E is a finite dimensional vector space over $K = \mathbb{R}$, with a positive-definite symmetric bilinear form.
2. E is a finite dimensional vector space over $K = \mathbb{C}$, with a positive-definite Hermitian form.

Remark 7.4.2. Any symmetric or Hermitian bilinear form can be described using a matrix w.r.t. any basis $(e_1, \cdots, e_n)$ of V: $A = (g(e_i, e_j))$, $1 \leq i, j \leq n$. g being symmetric gives ${}^tA = A$; and g being Hermitian gives ${}^tA = \bar{A}$. If the basis is orthonormal, then it has ± 1 on the diagonal.

Definition 7.4.3 (Adjoint of linear operators). Fix $y \in E$. Consider $E \ni x \mapsto \langle y, u(x)\rangle \in K$. This map is in E^*, which is $\mathrm{Hom}_{\mathbb{R}}(E, \mathbb{R})$ in the first case, and conjugate linear maps to $\mathbb{C}$ in the second. Suppose further that $\langle -, -\rangle$ is nondegenerate, there exists a unique map u^* s.t. $\langle u^*(y), x\rangle = \langle y, u(x)\rangle$.

Remark 7.4.4. u^* is also linear. Consider the following identification:

$$u^*(\lambda y) = \langle \lambda y, u(x)\rangle = \lambda \langle y, u(x)\rangle = \lambda \langle u^*(y), x\rangle = \lambda u^*(y)$$

Definition 7.4.5. For u symmetric or Hermitian, it is **self-adjoint** if $u = u^*$, i.e. for all $x, y \in E$, $\langle u(x), y\rangle = \langle x, u(y)\rangle$.

Proposition 7.4.6. A linear map is self-adjoint if and only if its matrix representation is symmetric or Hermitian.

Proof. Let $(e_1, \cdots, e_n)$ be an orthonormal basis of E. By linearity it suffices to consider the evaluation of the map on the basis. Let the matrix representations of u and u^* be (a_{ij}) and (b_{ij}), respectively. Then the evaluation can be expressed via

$$u(e_k) = \sum_{i=1}^{n} a_{ik} e_i, \quad u^*(e_\ell) = \sum_{j=1}^{n} b_{j\ell} e_j$$

Now consider the criterion for judging whether an operator is self-adjoint: for $\langle e_\ell, u(e_k)\rangle = \langle u^*(e_\ell), e_k\rangle$ we have

$$\text{LHS} = \left\langle e_\ell, \sum_{i=1}^{n} a_{ik} e_k \right\rangle = \overline{a_{\ell k}}, \qquad \text{RHS} = \left\langle \sum_{j=1}^{n} b_{j\ell} e_j, e_k \right\rangle = b_{kl}$$

which implies that $B = \overline{{}^tA}$. □

Theorem 7.4.7 (Spectral Theorem). Let $u : E \to E$ be a self-adjoint linear map. Then:

i) All eigenvalues of u are in $\mathbb{R}$.

ii) If u_1, u_2 are eigenvectors corresponding to distinct eigenvalues λ_1, λ_2, then $\langle u_1, u_2\rangle = 0$.

iii) There exists an orthonormal basis of E consisting of eigenvectors of u, which implies that u is diagonalizable.

Remark 7.4.8. In particular, this implies that symmetric linear maps on $\mathbb{R}$, and Hermitian linear maps on $\mathbb{C}$, are diagonalizable.

Proof of Theorem 7.4.7. Consider the statements sequentially:

i) Let $\lambda \in \mathbb{C}$ be a root of the characteristic polynomial of u:

- First consider E as a vector space over $\mathbb{C}$. Let y be an eigenvector associated to λ. This gives

$$\lambda \langle y, y\rangle = \langle \lambda y, y\rangle = \langle u(y), y\rangle = \langle y, u(y)\rangle = \langle y, \lambda y\rangle = \overline{\lambda} \langle y, y\rangle$$

Since $y \neq 0$, $\langle y, y\rangle \neq 0$, which implies that $\lambda = \overline{\lambda}$.

- Now let E be a vector space over $\mathbb{R}$. Seek to reduce to the case above. Consider the extension of scalars $E_{\mathbb{C}} := E \otimes_{\mathbb{R}} \mathbb{C}$, with the inclusion $E \hookrightarrow E_{\mathbb{C}}$, $x \mapsto x \otimes 1$. This gives an extension of $\langle -, - \rangle$ to $E_{\mathbb{C}}$, which is also Hermitian. This implies that orthogonality in $E_{\mathbb{C}}$ is well-defined, and any orthonormal basis in E is also orthonormal in $E_{\mathbb{C}}$.

  Now consider the corresponding map after the extension of scalar $i_{\mathbb{C}} := u \otimes \mathrm{Id}_{\mathbb{C}}$, which is given by the same matrix representation as that in E. By the result in the first case, this is self-adjoint; and since the characteristic polynomial of these two maps are the same, all roots are real numbers.

ii) Let λ_1, λ_2 be the eigenvalues to which the eigenvectors v_1, v_2 are associated to. Since u is self-adjoint, this gives

$$\lambda_1 \langle v_1, v_2 \rangle = \langle u(v_1), v_2 \rangle = \langle v_1, u(v_2) \rangle = \overline{\lambda_2} \langle v_1, v_2 \rangle = \lambda_2 \langle v_1, v_2 \rangle$$

By hypothesis $\lambda_1 \neq \lambda_2$, and by definition they are non-zero. This gives $\langle v_1, v_2 \rangle = 0$.

iii) Show this via induction on the dimension of E:

- *Base case.* Then for any element in the vector space it is linear in some basis vector that is normalized.
- *Inductive step.* Let $v \in E$ be an eigenvector of u associated to the eigenvalue λ. Define $F = (K \cdot v)^{\perp}$ where K is the underlying field. Since we are working over a vector space, this gives $E = F \oplus F^{\perp}$, indicating that $\langle -, - \rangle |_{F^{\perp} \times F^{\perp}}$ is positive definite (since the basis is orthonormalized). Let $y \in F^{\perp}$. By construction $\langle u(y), v \rangle = \langle \sum_i \alpha_i \lambda_i y_i, v \rangle = 0$ where y_i is associated to the eigenvalue λ_i. Further $u|_{F^{\perp} \times F^{\perp}}$ is self-adjoint, as taking a perspective on its matrix representation a matrix with one column and one row deleted remains to be Hermitian if itself is. Then v together with an orthonormal basis of $F^{\perp}$ gives an orthonormal basis of E.

□

Definition 7.4.9 (Unitary Operator). A linear map $u : E \to E$ is **unitary** if it is a bijection; and $u^* = u^{-1}$.

Remark 7.4.10. Equivalently, this gives $\langle u^{-1}(x), y \rangle = \langle x, u(y) \rangle$, which implies that

$$\langle x, y \rangle = \langle u(x), u(y) \rangle \implies \langle x, x \rangle = \langle u(x), u(x) \rangle \implies x = 0 \text{ if and only if } u(x) = 0$$

Remark 7.4.11. Translating this into the matrix representation A of u, u is unitary if and only if $A \cdot \overline{{}^t A} = \mathrm{Id}$. This implies that a matrix is unitary if and only if its inverse is (assuming that it is invertible).

Proposition 7.4.12. If B is an orthonormal basis, and A is a change of basis matrix between B and B'. Then B' is orthonormal if and only if A is unitary.

Proof. By the Remark 7.4.11 and symmetric argument it suffices to prove that for one direction. Remark 7.4.10 $\langle u(v_i), u(v_j) \rangle = \langle v_i, v_j \rangle$ which is ± 1 for $i = j$; and 0 otherwise. This is exactly the definition of an orthonormal basis. □

Remark 7.4.13. By Spectral Theorem, there exists an orthonormal basis consists of eigenvectors. Further the matrix U with columns elements of the orthonormal basis is unitary. Then for A Hermitian, $U \cdot A \cdot U^{-1}$ is diagonal.