Category Theory and Algebraic Geometry

Jubayer Ibn Hamid

Contents

Preface

These reading notes are a combination of material from the courses Math 145 by Prof. Zhiyu Zhang, Math 216a by Prof. Ravi Vakil at Stanford University and the texts mentioned in the references.

There are three textbooks that these notes follow closely. The first is Prof. Vakil's *"The Rising Sea: Foundations of Algebraic Geometry"* [1] and his lectures in Math 216a. In particular, almost all of the category theory notes are derived from his text/lectures. The second is David Steven Dummit and Richard M. Foote's *"Abstract Algebra"* [2] and the algebra review comes from my notes from this textbook. It is hard to overestimate the impact these two textbooks have had on me and I think they are two of the greatest textbooks ever written in mathematics; I strongly recommend reading them. The algebraic geometry notes follow Hartshorne's *"Algebraic Geometry"* [3] and [1].

I also recommend taking a look at Leinster's introduction to category theory [4]. There are some other sources, like the Stacks Project (`https://stacks.math.columbia.edu`) and the Napkin project (`https://web.evanchen.cc/napkin.html`) that I recommend checking out.

There may be major and minor errors throughout these notes. If you find any, please let me know by sending me an email at `jubayer@stanford.edu`. Oftentimes, I wrote these notes *after* I had already handwritten them elsewhere and I was careless / inefficient in rewriting the proof. I also glossed over various parts of the original texts that the reading notes were trying to follow despite them being pretty important.

1 Introduction

> *"Algebra is the offer made by the devil to the mathematician. The devil says: 'I will give you this powerful machine, it will answer any question you like. All you need to do is give me your soul: give up geometry and you will have this marvelous machine.' "*
>
> — Michael Atiyah

Algebraic geometry is about solutions of polynomial equations and the geometric structures on the space of those solutions. We use the language and techniques from abstract algebra on these geometric objects.

Geometry becomes interesting when local properties reveal to us global properties. Algebra provides us a very powerful tool to do that.

1.1 Terminology

A field k is algebraically closed if any non-constant polynomial $f \in k[x]$ has at least one root/zero in k i.e if $f \in k[x]$, then $f(x) = \mu \prod (x - \lambda_i)^{e_i}$ where $\lambda_i \in k$ are the roots. The field $\mathbb{R}$ is not algebraically closed as $f(x) = x^2 + 1$ has no root in $\mathbb{R}$, whereas $\mathbb{C}$ is algebraically closed.

The affine space of field k is denoted by $\mathbb{A}_k^n$ which is the Cartesian n-product of k.

The true coordinate ring $O(\mathbb{A}^n)$ of functions on $\mathbb{A}^n$ is the commutative ring $k[x_1, ..., x_n]$ of polynomials with n variables.

Let $f \in k[x_1, ..., x_n]$ be a polynomial. Then, $V(f)$ is the set of zeros of f and is called the hypersurface defined by f. If S is a set of polynomials from $k[x_1, .., x_n]$, then $V(S) := \{p \in \mathbb{A}_k^n | f(p) = 0, \forall f \in S\}$. One can check that $V(S) = \cap_{f \in S} V(f)$. When $S = \{f_1, ..., f_r\}$, we write $V(S)$ as $V(f_1, ..., f_r)$.

Example: Consider $k[x]$ which is a principal ideal domain. Therefore, every algebraic set can be written as the set of zeros of a single polynomial.

A subset $X \subseteq \mathbb{A}_k^n$ is called an affine algebraic set if $X = V(S)$ for some set S of polynomials in $k[x_1, ..., x_n]$. Throughout these notes, we will use the term affine variety to mean the same thing as affine algebraic sets (although some texts refer to only *irreducible* algebraic sets as affine varieties). One can easily show that if I is the ideal in $k[x_1, ..., x_n]$ generated by polynomials in S, then $V(S) = V(I)$. Suppose, $I = (f_1, ..., f_n)$, then, $V(I) = \cap_{i=1}^n V(f_i)$. Some more properties:

(1) If $\{I_\alpha\}$ is a collection of ideals, then $V(\cup_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$. (2) $I \subset J \implies V(J) \subset V(I)$ (3) $V(fg) = V(f) \cup V(g)$ (4) Any finite subset of $\mathbb{A}_k^n$ is an algebraic set (5) $V(A) = V((A))$ where (A) is the ideal generated by A.

The ideal generated by a set of functions $f_1, ..., f_m \in k[x_1, ..., x_n]$ is the set $(f_1, ..., f_m) := \{\sum_{i=1}^m g_i f_i : g_i \in k[x_1, ..., x_n]\}$. For a subset $X \subseteq \mathbb{A}_k^n$, consider the ideal in $k[x_1, ..., x_n]$ generated by polynomials that vanish on X. This ideal is called the vanishing ideal of X, denoted by $I(X)$. So,
$I(X) = \{f \in k[x_1, ..., x_n] : f(a) = 0, \forall a \in X\}$. So, if $f, g \in I$, then $f + g \in I$ and for any $h \in k[x_1, ..., x_n]$, $hf \in I$. Some more properties:

(1) $X \subset Y \implies I(Y) \subset I(X)$ (2) $I(\emptyset) = k[x_1, ..., x_n], I(\mathbb{A}^n) = \emptyset, I(\{a\}) = (x_1 - a_1, ..., x_n - a_n)$.

We say $f_1, ..., f_m$ scheme-theoretically define the affine variety $X \subset \mathbb{A}^n$ if $I(X) = (f_1, ..., f_m)$ i.e the ideal generated by $f_1, ..., f_m$. Furthermore, the ideal I is said to set-theoretically define variety X if $X = V(I)$ if It can be easily shown that $V(I(X)) = X$. $V(-)$ and $I(-)$ allow us to switch betwen the geometric world and the algebraic world which is a key tool used in algebraic geometry. In particular, later on, we will see that using Hilbert's Nullstellensatz, there is no information lost after we make this switch.

We also define fractional fields. Let R be an integral domain. Its fractional field $K = \text{Frac}(R)$ is defined as the ring

$$K := \left\{ \frac{f}{g} : f, g \in R, g \neq 0 \right\}$$

.

A polynomial mapping/morphism $p : V \to W$, where $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ are varieties, is a mapping such that

$$(x_1, ..., x_n) \to f(x_1, ..., x_n) := (f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n))$$

, where $f_i \in k[x_1, ..., x_n]$ and the image of the algebraic set V lies inside the algebraic set W. The mapping set $\text{Map}(V, W)$ is the set of all polynomial maps from V to W and in our case this is the set of all polynomial maps from V to W. We need polynomial mappings in order to investigate the relationships between varieties. Given X is an affine variety, an **automorphism** of X is a polynomial map $f : X \to X$ which is an isomorphism. $Aux(X)$ denotes the group of all automorphisms of X.

2 Category Theory

"Category theory takes a bird's eye view of mathematics. From high in the sky, details become invisible, but we can spot patterns that were impossible to detect from ground level. How is the lowest common multiple of two numbers like the direct sum of two vector spaces? What do discrete topological spaces, free groups, and fields of fractions have in common?"

— Tom Leinster [4]

2.1 Categories and subcategories

Definition 1. (Categories). A category $\mathscr{C}$ consists of a collection of objects, denoted by $\mathrm{obj}(\mathscr{C})$ or simply $\mathscr{C}$, and, for each pair of objects $A, B \in \mathscr{C}$, a set of morphisms/maps between them, denoted by $\mathrm{Mor}(A, B)$. Here, A is called the source and B is called the target of the morphism. Morphisms can also be composed i.e. if $f \in \mathrm{Mor}(A, B)$ and $g \in \mathrm{Mor}(B, C)$, then $g \circ f \in \mathrm{Mor}(A, C)$. For each object $A \in \mathscr{C}$, we also have the identity morphism $\mathrm{id}_A : A \to A$ such that left or right composing the identity with a morphism gives the same morphism.

This allows us to define isomorphism as well i.e. if $f : A \to B$ is a morphism, there exists a unique morphism $g : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.

Example 1: (Category of sets). This category's objects are sets and the morphisms are maps of sets.

Example 2:(Vec_k). This category's objects are vector spaces over the field k and the morphisms are linear transformations.

Example 3:(Automorphism group). If A is an object in category $\mathscr{C}$, then the *invertible elements* of $\mathrm{Mor}(A, A)$ form a group called the automorphism group of A, denoted by $\mathrm{Aut}(A)$. For example, $\mathrm{Aut}(\mathrm{Sets})$ are the bijective maps whereas $\mathrm{Aut}(\mathrm{Vec}_k)$ is the set of invertible matrices. In particular, two isomorphic objects have isomorphic automorphic groups i.e.,

Proposition 1. $A \cong B \implies \mathrm{Aut}(A) \cong \mathrm{Aut}(B)$.

Proof. If A and B are isomorphic objects, then we have $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$ where f is a morphism from A to B and g is a morphism from B to A. Now, let $\phi : \mathrm{Aut}(A) \to \mathrm{Aut}(B)$ by $\phi(\varphi) = f \circ \varphi \circ g$ for any $\varphi \in \mathrm{Aut}(A)$. Note that the image of ϕ is in $\mathrm{Aut}(B)$ since the inverse of $f \circ \varphi \circ g$ is $f \circ \varphi^{-1} \circ g$. This is also surjective because for any $\psi \in \mathrm{Aut}(B)$, we can find its pre-image $g \circ \psi \circ f \in \mathrm{Aut}(A)$. Similarly, it is easy to check this is injective and a homomorphism. $\square$

Example 4:(Abelian Group). This category's objects are abelian groups and the morphisms are group homomorphisms. The category is denoted by *Ab*.

Example 5:(Modules over a ring). Let A be a ring. Then the objects of the category Mod_A are the A-modules. Here, the morphisms are A-linear maps (or A-module homomorphisms) i.e., given X and Y are A-modules and $f : X \to Y$ is a morphism, then $f(x + x') = f(x) + f(x')$ for $x, x' \in X$ and $f(a \cdot x) = a \cdot f(x)$ for any $a \in A$ and $x \in X$.

Example 6: The category of rings has rings as objects and the morphisms are ring homomorphisms.

Example 7: The category of topological spaces, denoted by *Top*, has topological spaces as objects and continuous maps as morphisms.

Definition 2. (Subcategory). A subcategory $\mathscr{A}$ of a category $\mathscr{B}$ is such that $\mathrm{obj}(\mathscr{A}) \subseteq \mathrm{obj}(\mathscr{B})$ and the morphisms in $\mathscr{A}$ are a subset of the morphisms in $\mathscr{B}$ such that:
(1) $\mathrm{obj}(\mathscr{A})$ includes all the sources and targets of the morphisms in $\mathscr{A}$.
(2) morphisms in $\mathscr{A}$ include the identity morphisms on every object in $\mathscr{A}$.
(3) the morphisms are preserved under composition.

2.2 Functors

Informally, a covariant functor is a mapping from a category $\mathscr{A}$ to another category $\mathscr{B}$ such that it takes objects in the first category to objects in the second category and also defines a corresponding mapping of morphisms in the first category to morphisms in the second.

Definition 3. A covariant functor, $F : \mathscr{A} \to \mathscr{B}$, from a category $\mathscr{A}$ to a category $\mathscr{B}$ is a mapping such that:
(1)

$$F : \mathrm{obj}(\mathscr{A}) \to \mathrm{obj}(\mathscr{B})$$

(2) for each $A_1, A_2 \in \mathscr{A}$ and each morphism $m : A_1 \to A_2$, there is the corresponding morphism in $\mathscr{B}$ defined using F:

$$F(m) : F(A_1) \to F(A_2)$$

(3) for each object $A \in \mathscr{A}$,

$$F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$$

(4) and F preserves composition i.e., $F(m_2 \circ m_1) = F(m_2) \circ F(m_1)$.

The following is easy to verify:

Proposition 2. Covariant functors send isomorphisms to isomorphisms.

Proof. If A_1 and A_2 are isomorphic in category $\mathscr{A}$ via $f \circ g = \mathrm{id}_{A_2}$ and $g \circ f = \mathrm{id}_{A_1}$, then consider the functor F. Then, $F(f \circ g) = F(f) \circ F(g) = \mathrm{id}_{A_2}$ and $F(g \circ f) = F(g) \circ F(f) = \mathrm{id}_{A_1}$. So, $F(A_1) \cong F(A_2)$. □

Examples:

1. The identity functor $\mathrm{id} : \mathscr{A} \to \mathscr{A}$.
2. The function $F : \mathrm{Vec}_k \to \mathrm{Sets}$ that maps each vector space to its underlying set and linear transformations of vector spaces to the underlying mapping between the sets.
3. **(Important example)** Suppose A is an object in category $\mathscr{C}$. Then, there exists a functor
$$h^A : \mathscr{C} \to \mathrm{Sets}$$
(where, on the right hand side, each set is a set of morphisms) such that
$$h^A(B) = \mathrm{Mor}(A, B)$$
and, for $f : B_1 \to B_2$ a morphism in $\mathscr{C}$, $h^A(f) : h^A(B_1) \to h^A(B_2)$ is the map described by
$$[g : A \to B_1] \to [f \circ g : A \to B_1 \to B_2].$$

Definition 4. (Faithful covariant functors, full covariant functors).

1. $F : \mathscr{A} \to \mathscr{B}$ is a **faithful covariant functor** if for all $A, A' \in \mathscr{A}$, the map $\mathrm{Mor}_{\mathscr{A}}(A, A') \to \mathrm{Mor}_{\mathscr{B}}(F(A), F(A'))$ is *injective.*
2. $F : \mathscr{A} \to \mathscr{B}$ is a **full covariant functor** if for all $A, A' \in \mathscr{A}$, the map $\mathrm{Mor}_{\mathscr{A}}(A, A') \to \mathrm{Mor}_{\mathscr{B}}(F(A), F(A'))$ is *surjective.*

Definition 5. (Full Subcategory). The subcategory $\mathscr{A}$ of $\mathscr{B}$ is a **full subcategory** if the inclusion map $i : \mathscr{A} \to \mathscr{B}$ is full (note: inclusions are always faithful anyway).

Definition 6. (Contravariant functors). Contravariant functors are defined similarly to covariant functors except the map from morphisms to morphisms is in the opposite direction i.e. if $F : \mathscr{A} \to \mathscr{B}$ such that $F : \mathrm{obj}(\mathscr{A}) \to \mathrm{obj}(\mathscr{B})$, then for $m : A_1 \to A_2$ is a morphism in $\mathscr{A}$, $F(m) : F(A_2) \to F(A_1)$. Note that in this case, $F(m_2 \circ m_1) = F(m_1) \circ F(m_2)$.

Definition 7. (Opposite category). Let $F : \mathscr{C} \to \mathscr{D}$ be a contravariant functor. Then, $F' : \mathscr{C}^{\mathrm{opp}} \to \mathscr{D}$ is the covariant version of the same functor, where $\mathscr{C}^{\mathrm{opp}}$ is the same as $\mathscr{C}$ except the arrows go in the opposite directions.

Examples:

- Let vec_k be our category. Then, taking the dual gives contravariant functor $F : vec_k \to vec_k$. Let $f : V \to W$ be a morphism, then, $F(f) = f^\vee : W^\vee \to V^\vee$.
- Consider the functor $F : \mathrm{Top} \to \mathrm{Rings}$, where F takes topological space X to the space of real-valued continuous functions on X. Then, a morphism $m : X \to Y$ induces a pullback from functions on Y to functions on X.
- (Functor of points). Suppose $A \in \mathrm{obj}(\mathscr{C})$, there exists a contravariant functor $h_A : \mathscr{C} \to \mathrm{Sets}$ such that $h_A(B) = \mathrm{Mor}(B, A)$. Now, if $f : B_1 \to B_2$ is a morphism in $\mathscr{C}$, then $h_A(f) : \mathrm{Mor}(B_2, A) \to \mathrm{Mor}(B_1, A)$ via $h_A(f)(g : B_2 \to A) = (g \circ f : B_1 \to B_2 \to A)$.

2.3 Natural Transformations

> *"I didn't invent category theory to study functors; I invented them to study natural transformations."*
>
> — Saunders Mac Lane

Definition 8. (Natural Transformation). Let $\mathscr{A}$ and $\mathscr{B}$ be categories and let $F, G : \mathscr{A} \to \mathscr{B}$ be two covariant functors. Then, a natural transformation of covariant functors F to G is a way of going from the covariant functor F to the covariant functor G. This transformation is done by defining morphism $m_A : F(A) \to G(A)$ for each $A \in \mathscr{A}$. Then, the following diagram commutes:

$$\begin{tikzcd}
F(A) \arrow[r, "F(f)"] \arrow[d, "m_A"'] & F(A') \arrow[d, "m_{A'}"] \\
G(A) \arrow[r, "G(f)"'] & G(A')
\end{tikzcd}$$

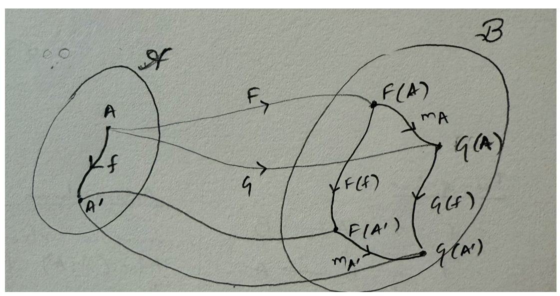


Figure 1: Illustration of natural transformations

Definition 9. (Natural isomorphism). A natural isomorphism of functors is a natural transformation of functors such that each m_A is an isomorphism. This means, for every $m_A : F(A) \to G(A)$, there exists $\tilde{m}_A : G(A) \to F(A)$ such that $\tilde{m}_A \circ m_A = \mathrm{id}_{F(A)}$ and $m_A \circ \tilde{m}_A = \mathrm{id}_{G(A)}$.

Definition 10. (Equivalence of categories). Functors $F : \mathscr{A} \to \mathscr{B}$ and $F' : \mathscr{B} \to \mathscr{A}$ such that $F \circ F'$ is naturally isomorphic to $\mathrm{id}_{\mathscr{B}}$ and $F' \circ F$ is naturally isomorphic to $\mathrm{id}_{\mathscr{A}}$.

2.4 Universal properties and isomorphisms

Definition 11. (Initial, final, and zero objects). Initial object in a category has only one map to every object. Final object has only one map from every object. Zero object is an object that is both initial and final.

Proposition 3. Any two initial objects are uniquely isomorphic. Any two final objects are uniquely isomorphic.

Note: two objects are uniquely isomorphic if there exists only one isomorphism between them

Proof. Let X and Y be initial. Then, $f : X \to Y$ is a morphism and $f' : Y \to X$ is a morphism and they are the only arrows in these directions. Now, $f' \circ f : X \to X$ but id_X is the only morphism from X to X so $f' \circ f = \mathrm{id}_X$. Similar reasoning proves the case for final objects. The unique isomorphism comes from the fact that since these are initial/final objects, there can be no other isomorphism. □

Therefore, **inital objects are unique up to unique isomorphism** and **final objects are unique up to unique isomorphism.**

Examples:

- Consider the category of rings, *Rings*, where the morphisms are the ring homomorphisms. Then, $\mathbb{Z}$ is the initial object and $\{0\}$ is the final object.
- Consider the category of topological spaces, *Top*. Then, $\{0\}$ is a final object (or any topological space with only one point) and $\{\}$ is the initial object.
- Consider the category of sets, *Sets*. Then, any singleton is a final object and $\{\}$ is the initial object.

Next, we look at localization, similar to how we defined it in ring theory (where we call it a ring of fractions).

Definition 12. (Multiplicative subset). S is a multiplicative subset of a ring A if it is closed under multiplication and $1 \in S$.

Definition 13. (Ring $S^{-1}A$). This is a ring where each $x \in S^{-1}A$ is of the form $x = \frac{a}{s}$ with $a \in A, s \in S$ with the equivalence $\frac{a_1}{s_1} = \frac{a_2}{s_2}$ if and only if $s(s_2 a_1 - s_1 a_2) = 0$ for some $s \in S$.

- There is the canonical map from A to $S^{-1}A$ given by $a \to \frac{a}{1}$.
- If $0 \in S$, then $S^{-1}A$ is the 0 ring. This is because for any $\frac{a_1}{s_1} \in S^{-1}A$, $\frac{a_1}{s_1} = \frac{0}{s_2}$ as $0(s_2 a_1 - s_2 0) = 0$.

There are a few important examples:

- $A_f = S^{-1}A$ where $S = \{1, f, f^2, \cdots\}$ for some $f \in A$. Then, $A_f \leftrightarrow A[x]/(xf - 1)$.
- $A_p = S^{-1}A$ where $S = A \backslash p$ for some prime ideal p.

- $K(A) = S^{-1}A$ where $S = A\backslash\{0\}$ and A is an integral domain. This is called a fraction field.

Recall: If A is a ring, then $x \in A$ is a zero divisor if there exists a non-zero $y \in A$ such that $xy = 0$.

If M is an A-module, then $a \in A$ is called a zero divisor if there exists $m \in M$ such that $am = 0$.

Proposition 4. The element $a \in A$ is non-zerodivisor for M if and only if $\times a : M \to M$ is an injection.

Proposition 5. $A \to S^{-1}A$ by the canonical map is injective if and only if it contains no zero divisor.

Proposition 6. $S^{-1}A$ is initial among A-algebras B where every element of S is sent to an invertible element of B. In other words, if B is an A-algebra such that $\varphi_B : A \to B$ sends every $s \in S$ to an invetible element and with $\iota : A \to S^{-1}A$ being the canonical map, then there exists a unique $\varphi : S^{-1}A \to B$ such that $\varphi_B = \varphi \circ \iota$.

Proof. (Sketch) Use $\varphi : S^{-1}A \to B$ by sending each $\frac{a}{s}$ to $\varphi_B(a)\varphi(s)^{-1}$. It is easy to then check well-definedness, homomorphism properties and uniqueness. □

2.4.1 Various products and universal properties

Recall: (Tensor Products)
Let R be a subring of S.
Let N be a left R-module.
Let M be a left R-module and a right S-module.
Then, the tensor product of M and N is $M \otimes_R N = F(M \times N)/H$ where $F(M \times N)$ is the free $\mathbb{Z}$-module (or Free Abelian group) on $M \times N$ and H is the subgroup generated by all elements of the form $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$, $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$ and $(mr, n) - (m, rn)$.
The elements of this tensor product are written as $m \otimes n$.
This is a group with the operation $m_1 \otimes n + m_2 \otimes n = (m_1 + m_2) \otimes n$ and $m \otimes n_1 + m \otimes n_2 = m \otimes (n_1 + n_2)$.
This is a module with $s\left(\sum_{\text{finite}} m_i \otimes n_i\right) = \sum_{\text{finite}} sm_i \otimes n_i$.

R-balanced or R-bilinear maps: M is a right R-module, N is a left R-module and L is an additive abelian group. Then, $\varphi : M \times N \to L$ such that $\varphi(m_1+m_2, n) = \varphi(m_1, n)+\varphi(m_2, n)$, $\varphi(m, n_1) = \varphi(m, n_1) + \varphi(m, n_2)$ and $\varphi(mr, n) = \varphi(m, rn)$.

We have the canonical R-balanced or map $\iota : M \times N \to M \otimes_R N$ by $\iota(m, n) = m \otimes n$.

(S, R)-bimodules: M such that M is a left S-module and right R-module and $s(mr) = (sm)r$. This, as in the (R, R)-bimodule structure, allows us to give M the standard R-module structure where we define $mr = rm$.
By giving M the standard R-module structure, crucially, $M \otimes_R N$ is a left R-module too with $r(m \otimes n) = rm \otimes n = m \otimes rn$.

In this section, we focus on $M \otimes_R N$ being a left R-module by giving M the standard R-module structure (i.e. $rm = mr$).

Proposition 7.
- $(\cdot) \otimes_A N$ is a covariant functor $\mathrm{Mod}_A \to \mathrm{Mod}_A$. This is the map $\varphi(M) = M \otimes_A N$ for any $M \in \mathrm{Mod}_A$.
- φ is a right-exact functor. In other words, if $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \xrightarrow{\lambda} 0$ is an exact sequence (i.e. $\mathrm{Im}\alpha = \ker\beta$ and β is surjective), then the following induced sequence is also exact:
$$M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N \to 0.$$

Proof idea: The proof is straightforward by designing $\varphi(M) = M \otimes_A N$ and $\varphi(f)(m \otimes n) = f(m) \otimes n$ for any $f : M \to M'$ an A-module homomorphism.

Definition 14. (A-bilinear map). Let M, N, P be A-modules. Then, a map $f : M \times N \to P$ is called A-bilinear if $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$ and $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$ and $f(am, n) = f(m, an) = af(m, n)$.

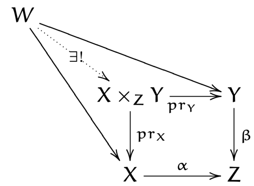
Defining Tensor Products using Universal Property:

Observation: Any A-bilinear map $f : M \times N \to P$ factors through $M \otimes_A N$:
$$M \times N \to M \otimes_A N \to P.$$

Definition: (Tensor Products). The tensor product of left A-modules M and N is an A-module T with an A-bilinear map $t : M \times N \to T$ such that given any A-bilinear map $t' : M \times N \to T'$, there exists a unique A-module homomorphism $f : T \to T'$ such that $t' = f \circ t$:

$$\begin{tikzcd}
M \times N \arrow[r, "t"] \arrow[dr, "t'"'] & T \arrow[d, "f"] \\
 & T'
\end{tikzcd}$$

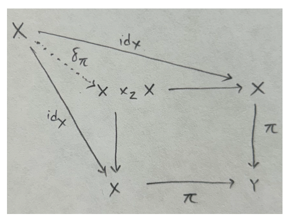
Definition 15. (Fibered Products). Let our category be $\mathscr{C}$. Let $\alpha : X \to Z$ and $\beta : Y \to Z$ be two morphisms in $\mathscr{C}$. Then the fibered product is an object $X \times_Z Y$ along with morphisms $pr_X : X \times_Z Y \to X$ and $pr_Y : X \times_Z Y \to Y$ such that $\alpha \circ pr_X$ and $\beta \circ pr_Y$ agree. Furthermore, if W is an object with maps to X and Y, then these factor through $X \times_Z Y$:



Note that even though in our notation, we write it as $X \times_Z Y$, the fibered product depends on α and β too despite them not appearing in the notation.

Also, note that there is no requirement that W itself is a fibered product or that there is a map from $X \times_Z Y$ to W.

Definition 16. (Diagonal Morphism) Let $\pi : X \to Y$ be a morphism. If the fibered product $X \times_Y X$ exists, then this determines a diagonal morphism $\delta_\pi : X \to X \times_Y X$.



Examples:

- Example of Fibered Product in *Sets*. Define $X \times_Z Y = \{(x, y) \in X \times Y \mid \alpha(x) = \beta(y)\}$. Then, $X \times_Z Y$ is a fibered product.
  - Firstly, note that with $pr_X : X \times_Z Y \to X$ by $pr_X((x, y)) = x$ and pr_Y being defined in a similar way, we have that $\alpha \circ pr_X = \beta \circ pr_Y$.
  - Let W be an object with maps f_X to X and f_Y to Y such that $\alpha \circ f_X = \beta \circ f_Y$. Then, we can define a map $\psi : W \to X \times_Z Y$ by $\psi(w) = (f_X(w), f_Y(w))$. It is easy to check that this makes the diagram commute.
- Example of Fibered Product in topological space: Let X be a topological space and consider the category of open sets in X. In other words, the objects are open sets. If $U \subseteq V$, then we can define a morphism $\iota : U \to V$. In this set, the fibered product of $U \times_W V$ is just $U \cap V$.

Proposition 8. (Important) If Z is the final object in a category $\mathscr{C}$ and if $X, Y \in \mathscr{C}$, then $X \times_Z Y$ is uniquely isomorphic to $X \times Y$.

Sketch: you can give the fibered product structure to $X \times_Z Y$ by letting pr_X be $i(x, y) = x$ and similarly for pr_Y. Use the definition of fibered products to find the isomorphism between the two products.

Proposition 9. Suppose we are given morphisms $X_1, X_2 \to Y$ and $Y \to Z$. Assume all the required fibred products exists. Then, the following commutes:

$$\begin{array}{ccc} X_1 \times_Y X_2 & \longrightarrow & X_1 \times_Z X_2 \\ \downarrow & & \downarrow \\ Y & \longrightarrow & Y \times_Z Y \end{array}$$

Proof. Take a deep breath and construct each map.

First, we note that

$$\begin{array}{ccc} X_1 \times_Y X_2 & \longrightarrow & X_2 \\ \downarrow & & \downarrow \\ X_1 & \longrightarrow & Y \end{array}$$

and

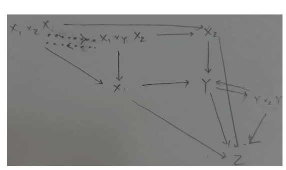
$$\begin{array}{ccc} X_1 \times_Z X_2 & \longrightarrow & X_2 \\ \downarrow & & \downarrow \\ X_1 & \longrightarrow & Z \end{array}$$

Crucially, since $X_1 \times_Z X_2$ has morphisms to X_1 and X_2, there exists a unique morphism from $X_1 \times_Z X_2$ to $X_1 \times_Y X_2$. Similarly, there exists a morphism from $X_1 \times_Y X_2$ to $X_1 \times_Z X_2$.

Next, we have the following:

$$\begin{array}{ccc} Y \times_Z Y & \longrightarrow & Y \\ \downarrow & & \downarrow \\ Y & \longrightarrow & Z \end{array}$$

But we also have the trivial identity morphism from Y to Y allowing us to find an isomorphism between Y and $Y \times_Z Y$. Now to construct the Cartesian square in the theorem, we use the following diagram that we have already constructed:



$\square$

Definition 17. (Coproduct). Consider two objects X and Y in category $\mathscr{C}$. Then the corproduct of X and Y is an object $X \amalg Y$ with injective morphisms $i_X : X \to X \amalg Y$ and $i_Y : Y \to X \amalg Y$ with the following universal property:

for any object Z with morphisms $f_X : X \to Z$ and $f_Y : Y \to Z$, there is a unique morphisms $f : X \amalg Y \to Z$ making the diagram commute i.e. $f \circ i_X = f_X$ and $f \circ i_Y = f_Y$.

$$\begin{tikzcd}
Z & & \\
& X \amalg Y \arrow[ul, dashed, "f"'] & X \arrow[l, "i_X"'] \arrow[ull, dashed, "f_x"'] \\
& Y \arrow[u, "i_Y"'] \arrow[uul, dashed, "f_Y"] &
\end{tikzcd}$$

Note: the definition of a product is similar except with all the arrows reversed.

Definition 18. (Fibred Coproduct). The fibered coproduct is defined as an object $X \amalg_Z Y$ by reversing the arrows in the definitoin of a fibred product. In other words, suppose we have morphisms $\alpha : Z \to X$ and $\beta : Z \to Y$. Then, we have a morphism $pr_X : X \to X \amalg_Z Y$ and a morphism $pr_Y : Y \to X \amalg_Z Y$ such that $pr_X \circ \alpha = pr_Y \circ \beta$. Furthermore, this satisfies the universal property that if we have object W with morphisms $X, Y \to W$, then there is a morphism $X \amalg_Z Y \to W$.

$$
\begin{tikzcd}
W & & \\
& X \amalg_Z Y \arrow[ul, dashed] & Y \arrow[l, "pr_Y"'] \arrow[ull] \\
& X \arrow[u, "pr_X"] \arrow[uul] & Z \arrow[l, "\alpha"] \arrow[u, "\beta"']
\end{tikzcd}
$$

2.4.2 Monomorphisms and Epimorphisms

Definition 19. (Monomorphisms). A morphism $\pi : X \to Y$ is called a monomorphism if any two morphisms $\mu_1 : Z \to X$ and $\mu_2 : Z \to X$ such that $\pi \circ \mu_1 = \pi \circ \mu_2$ must satisfy $\mu_1 = \mu_2$.

In other words, $\mathrm{Mor}\big(Z, X\big) \to \mathrm{Mor}\big(Z, Y\big)$ via the natural map, π, is an injection.

Note that this means monomorphisms satisfy the left cancellation property: $\pi \circ \mu_1 = \pi \circ \mu_2 \implies \mu_1 = \mu_2$.

Proposition 10. Composition of two monomorphisms is a monomorphism.

Proof. Let π_1 and π_2 be monomorphisms from X to Y and Y to W respectively. Let $\varphi_1, \varphi_2 : Z \to X$ such that $\pi_2 \circ \pi_1 \circ \varphi_1 = \pi_2 \circ \pi_1 \circ \varphi_2$. Then, since π_2 is a monomoprhism, $\pi_1 \circ \varphi_1 = \pi_1 \circ \varphi_2$. Since π_1 is a monomorphism $\varphi_1 = \varphi_2$. ☐

Theorem 11. $\pi : X \to Y$ is a monomorphism if and only if the fibered product $X \times_Y X$ exists and the induced diagonal morphism $\delta_\pi : X \to X \times_Y X$ is an isomorphism.

Proof. Suppose $\pi : X \to Y$ is a monomorphism. Now, define $X \times_Y X$ to be X. Then, in the following diagram, f must be unique (since $\pi \circ (id_X \circ f) = \pi \circ (id_X \circ f')$ implies $f = f'$ as π is a monomorphism).

$$
\begin{tikzcd}
W \arrow[dr, dashed, "f"] \arrow[drr, "p"] \arrow[ddr, "p"'] & & \\
& X \arrow[r, "id_X"] \arrow[d, "id_X"'] & X \arrow[d, "\pi"] \\
& X \arrow[r, "\pi"'] & Y
\end{tikzcd}
$$

Conversely, suppose the fibered product exists and the diagonal morphism is an isomorphism. Note that this implies that X itself is a fibered product (this is easy to check). Then, consider the following diagram with $\varphi_1, \varphi_2 : Z \to X$:

$$
\begin{tikzcd}
W \arrow[dr, dashed, "\exists!"] \arrow[drr, "\varphi_1"] \arrow[ddr, "\varphi_2"'] & & \\
& X \arrow[r, "id_X"] \arrow[d, "id_X"'] & X \arrow[d, "\pi"] \\
& X \arrow[r, "\pi"'] & Y
\end{tikzcd}
$$

Since the map from W to X is unique (because X is a fibered product), therefore, $\varphi_1 = \varphi_2$. $\square$

Definition 20. (Epimorphisms). A morphism $\pi : X \to Y$ is called an epimorphism if for any object Z and any morphisms $\mu_1, \mu_2 : Y \to Z$ such that $\mu_1 \circ \pi = \mu_2 \circ \pi$, we have that $\mu_1 = \mu_2$.

2.4.3 Yoneda's Lemma

Recall the contravariant function we saw before: for any object $A \in \mathscr{C}$, $h_A : \mathscr{C} \to \text{Sets}$ by letting $h_A(C) = \text{Mor}\big(C, A\big)$. Furthermore, for any $f : B \to C$, we have that $h_A(f) : \text{Mor}\big(C, A\big) \to \text{Mor}\big(B, A\big)$ by $h_A(f)(g) = g \circ f$. On the other hand, the covariant version has $h^A(C) = \text{Mor}\big(A, C\big)$ and $h^A(f) : \text{Mor}\big(A, B\big) \to \text{Mor}\big(A, C\big)$ by $h^A(f)(g) = f \circ g$..

Proposition 12. Let A and A' be objects in a category $\mathscr{C}$ with maps $i_C : \text{Mor}\big(C, A\big) \to \text{Mor}\big(C, A'\big)$ that commute with the maps $h_A(\cdot)$ i.e., for $f : B \to C$,

$$\begin{array}{ccc} \mathrm{Mor}\big(C,A\big) & \xrightarrow{h_A(f)} & \mathrm{Mor}\big(B,A\big) \\ \Big\downarrow{\scriptstyle i_C} & & \Big\downarrow{\scriptstyle i_B} \\ \mathrm{Mor}\big(C,A'\big) & \xrightarrow{h_{A'}(f)} & \mathrm{Mor}\big(B,A'\big) \end{array}$$

Then, the maps i_C for all $C \in \mathrm{obj}(\mathscr{C})$ are induced from a unique morphism $g : A \to A'$ i.e., there exists a unique $g : A \to A'$ such that for all $C \in \mathscr{C}$, i_C is given by $i_C(u) = g \circ u$ (here $u \in \mathrm{Mor}\big(C,A\big)$). Furthermore, if i_C are all bijections, then, g is an isomorphism.

Proof. First, we use the commutativity to realize the following:

$$\begin{aligned} (h_{A'}(f) \circ i_C)u &= (i_B \circ h_A(f))u \\ i_C(u) \circ f &= i_B \circ u \circ f \\ i_C(u) \circ f &= i_B(u \circ f) \end{aligned}$$

Replace B with C to realize that

$$i_C(u) \circ f = i_C(u \circ f). \tag{1}$$

Now, consider $i_A : \mathrm{Mor}\big(A,A\big) \to \mathrm{Mor}\big(A,A'\big)$. Then, consider $i_A(id_A) \in \mathrm{Mor}\big(A,A'\big)$ and let $g = i_A(id_A) \in \mathrm{Mor}\big(A,A'\big)$.

Now, replace B with C and C with A in the diagram above to get the following:

$$\begin{array}{ccc} \mathrm{Mor}\big(A,A\big) & \xrightarrow{h_A(v)} & \mathrm{Mor}\big(C,A\big) \\ \Big\downarrow{\scriptstyle i_A} & & \Big\downarrow{\scriptstyle i_C} \\ \mathrm{Mor}\big(A,A'\big) & \xrightarrow{h_{A'}(v)} & \mathrm{Mor}\big(C,A'\big) \end{array}$$

Then, using 1, with $v : C \to A$, we have that $i_C(id_A \circ v) = i_A(id_A) \circ v$. But $i_C(id_A \circ v) = i_C(v)$. So,

$$i_C = i_A(\mathrm{id}_A). \tag{2}$$

To see the uniqueness, suppose there exists a different $g' : A \to A'$. Consider A and i_A. Then, $i_A(id_A) = g' \circ id_A = g'$. but $i_A(id_A) = g$, so $g = g'$. $\square$

The following proposition helps us better understand h_A and h^A via isomorphisms to much simpler maps:

Proposition 13. (1) Suppose A and B are objects in category $\mathscr{C}$. There exists a bijection between the natural transformations $h^A \to h^B$ of covariant functors $\mathscr{C} \to$ Sets and the morphisms $B \to A$.
(2) Similarly, there exists a bijection between the natural transformations $h_A \to h_B$ of covariant functors $\mathscr{C} \to$ Sets and the morphisms $A \to B$.

Proof. (1) Consider $h^A(A) = \mathrm{Mor}\big(A, A\big)$ and $h^B(A) = \mathrm{Mor}\big(B, A\big)$. Let $m_1 : h^A(A) \to h^B(A)$. Then, $m_1(id_A) \in \mathrm{Mor}\big(B, A\big)$. On the other hand, suppose $f : B \to A$. Now consider the natural transformation $m_2 : h^A(A) \to h^B(A)$ by $m_2(\psi) = \psi \circ f$. These are equal to each other. To see this, note that we have the following commutative diagram:

$$\begin{array}{ccc} h^A(A) = \mathrm{Mor}\big(A, A\big) & \xrightarrow{m_1} & h^B(A) = \mathrm{Mor}\big(B, X\big) \\ \big\downarrow{\scriptstyle h^A(\psi)} & & \big\downarrow{\scriptstyle h^B(\psi)} \\ h^A(X) = \mathrm{Mor}\big(A, X\big) & \xrightarrow{m_1} & h^B(X) = \mathrm{Mor}\big(B, X\big) \end{array}$$

Then, using this,

$$\begin{aligned} (m_1 \circ h^A(\psi))(id_A) &= (h^B(\psi) \circ m_1)(id_A) \\ m_1(h^A(\psi)(id_A)) &= (\psi \circ m_1)(id_A) \\ m_1(\psi \circ id_A) &= (\psi \circ m_1)(id_A) \\ m_1(\psi) &= \psi \circ m_1. \end{aligned}$$

Then, with $f = m_1(id_A)$, we have $m_2(\psi) = \psi \circ m_1(id_A) = m_1(\psi)$. ☐

Definition 21. (Representable contravariant functors). A contravariant functor F from category $\mathscr{C}$ to category Sets is said to be representable if there is a natural isomorphism $\psi : F \to h_A$. Therefore, the representing object A is determined up to unique isomorphism by the pair $(F(A), \psi_A : F(A) \to h_A(A) = \mathrm{Mor}\big(A, A\big))$. The element $\psi^{-1}(id_A) \in F(A)$ is called the universal object.

Theorem 14. (Yoneda's Lemma). Suppose F is a covariant functor $\mathscr{C} \to$ Sets. Suppose $A \in \mathrm{obj}(\mathscr{C})$. Then, there is a bijection between the natural transformations $h^A \to F$ and $F(A)$.

Proof. Consider the natural transformation $\alpha : h^A \to F$ i.e., for each object A, $\alpha_A : h^A(A) \to F(A)$. Then, we define the map Φ from the space of natural transformations (from h^A to F) to $F(A)$ i.e.

$$\Phi : \text{ (Natural Transforms from } h^A \text{ to } F(A)) \to F(A)$$

by

$$\Phi(\alpha) = \alpha_A(id_A).$$

On the other hand, we define

$$\Psi : F(A) \to \text{ (Natural Transforms from } h^A \text{ to } F(A))$$

such that, for each $x \in F(A)$ and for any object B in category $\mathscr{C}$,

$$\Psi(x) : h^A \to F$$

and

$$\Psi(x)_B : h^A(B) \to F(B)$$

by

$$\Psi(x)(f) = F(f)(x).$$

These maps are inverses of each other. To see this, note that for any $x \in F(A)$

$$\begin{aligned}\Phi(\Psi(x)) &= \Psi(x)_A(id_A)\\ &= F(id_A)(x)\\ &= x.\end{aligned}$$

On the other hand, for any $\alpha : h^A \to F$ and any object $B \in \mathscr{C}$ and $f \in \mathrm{Mor}\big(A, B\big) = h^A(B)$, we have:

$$\begin{aligned}\Psi(\Phi(\alpha))_B(f) &= \Psi(\alpha_A(id_A))_B(f)\\ &= F(f)(\alpha_A(id_A))\\ &= (\alpha_B \circ h^A(f))(id_A)\\ &= \alpha_B(h^A(f)(id_A))\\ &= \alpha_B(f \circ id_A)\\ &= \alpha_B(f).\end{aligned}$$

In other words, $\Psi(\phi(\alpha)) = \alpha$. Here, the third line comes from the fact that α is a natural transformation:

$$\begin{array}{ccc} h^A(A) & \xrightarrow{h^A(f)} & h^A(B) \\ \Big\downarrow{\scriptstyle \alpha_A} & & \Big\downarrow{\scriptstyle \alpha_B} \\ F(A) & \xrightarrow{F(f)} & F(B) \end{array}$$

$\square$

Definition 22. (Functor Category). Given a category $\mathscr{C}$, we can create a new category, called the functor category, where the objects are contravariant functors $\mathbf{C} \to$ Sets and the morphisms are natural transformations between these contravariant functors.

We, then, have a functor, h from $\mathscr{C}$ to the functor category by $h(A) = h_A$.

2.5 Limits and Colimits

2.5.1 Limits

We start with a few definitions that only make sense if one is familiar with set theory.

Definition 23. (Small Category). A category is called a small category if the the objects form a set and the morphisms form a set.

Definition 24. (Diagram indexed by a small category). Let $\mathscr{I}$ be a small category and let $\mathscr{A}$ be any category. Then, a functor $F : \mathscr{I} \to \mathscr{A}$ such that for any object $i \in \mathscr{I}$, $F(i) = A_i \in \mathscr{A}$ (and we have the appropriate commuting morphisms) is called a diagram indexed by $\mathscr{I}$. We call $\mathscr{I}$ an *index category.*

Example of index category: A partially ordered set (or poset) is a set S with the binary relation $\geq$ such that (1) $x \geq x$ (2)$x \geq y$ and $y \geq z$ implies $x \geq z$ and (3) $x \geq y$ and $y \geq x$ implies $x = y$. Then, a poset $(S, \geq)$ can be called a category with the objects being the elements of S and a single morphism from x to y if and only if $x \geq y$ and no morphism otherwise. Note that in this category, there is at most one morphism between any two objects.

Definition 25. (Limit of diagram). Let $\mathscr{I}$ be an index category with functor $F : \mathscr{I} \to \mathscr{A}$. Then, the limit of the diagram is an object of $\mathscr{A}$, denoted by $\lim_{\mathscr{I}} A_i$, with morphisms $f_j : \lim_{\mathscr{I}} A_i \to A_j$ for each $j \in \mathscr{I}$ such that if $m : j \to k$ is a morphism in $\mathscr{I}$, then the following diagram commutes

$$\begin{tikzcd} \lim_{\mathscr{I}} A_i \arrow[d, "f_j"'] \arrow[dr, "f_k"] & \\ A_j \arrow[r, "F(m)"] & A_k \end{tikzcd}$$

In particular, the limit of the diagram and the maps to each A_j are universal with respect to this property. In other words, if W is an object with maps $g_i : W \to A_i$ such that g_i commutes with $F(m) : A_j \to A_k$ i.e.

$$\begin{tikzcd} W \arrow[d, "g_j"'] \arrow[dr, "g_k"] & \\ A_j \arrow[r, "F(m)"] & A_k \end{tikzcd}$$

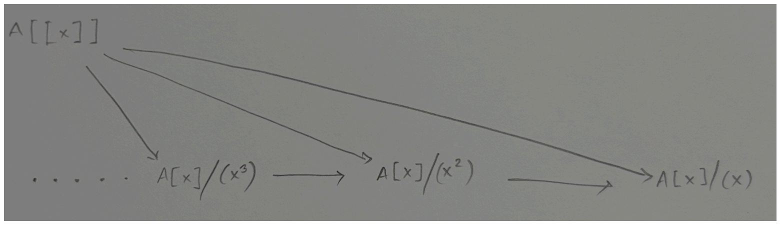
then, there exists a unique morphism $G : W \to \lim_{\mathscr{A}} A_i$ such that $g_i = f_i \circ g$ for all i. Therefore, if the limit exists, it is unique up to unique isomorphism.

Examples:

1. Formal power series: Define the formal power series, for a ring A, to be

$$A[[x]] := \{\sum_{i=0}^{\infty} a_i x^i \mid a_i \in A\}.$$

Then, $A[[x]]$ is the limit in the category of rings $A[x]/(x^n)$ for all natural numbers n:



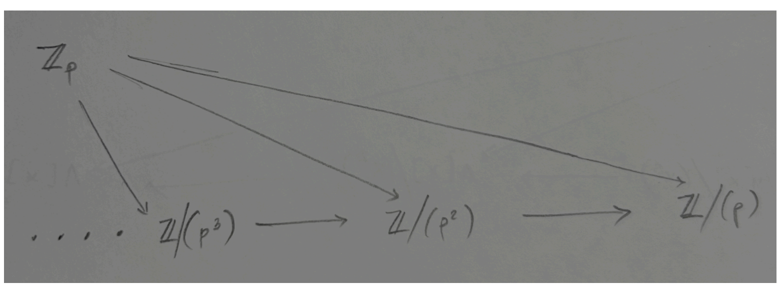
Here, the morphism from $A[[x]]$ to $A[x]/(x^n)$ takes $\sum_{i=0}^{\infty} a_i x^i$ to $\sum_{i=0}^{n-1} a_i x^i$. This example is a good illustration of why we call it the *limit* of the diagram.

2. p-adic integers: First, we define the p-adics:

Definition 26. (p-adic integers/p-adics): Given p is a prime number, the p-adic integers/p-adics are integers of the form $\sum_{i=0}^{\infty} a_i p^i$ where a_i are integers such that $0 \leq a_i < p$. Then, the set of p-adics integers is

$$\mathbb{Z}_p := \{\sum_{i=0}^{\infty} a_i p^i \mid 0 \leq a_i < p, a_i \in \mathbb{Z}\}.$$

Then, $\mathbb{Z}_p$ is a limit in the category of rings with objects $\mathbb{Z}/(p^n)$:



The morphisms here are defined in a similar way to the previous example.

Theorem 15. In the category *Sets*, the set $\prod_i A_i$ defined as:

$$\{(a_i)_{i \in \mathscr{I}} \in \prod_i A_i \mid F(m)(a_j) = a_k, \forall m \in \mathrm{Mor}\big(j,k\big) \subset \mathrm{Mor}\big(\mathscr{I}\big)\}$$

along with the natural projection maps to each A_i is the limit $\lim_{\mathscr{I}} A_i$

Proof. To write things out more clearly, we have that $j, k \in \mathscr{I}$ and a morphism in the category $\mathscr{I}$ $m : j \to k$. Then, we have the functor $F : \mathscr{I} \to \mathscr{A}$ that sends $F : i \to A_i$. The elements of A_i look like a_i. Then, $F(m)(a_j) = a_k$ (since $F(m) : A_j \to A_k$ as a covariant functor). Now, consider the set $\prod_i A_i$ where the elements look like $(a_i)_{i \in \mathscr{I}}$. Define the natural projection map here

$$\psi_j : \prod_i A_i \to A_j$$

by $\psi_j(a_1, a_2, \ldots) = a_j$. Then,

$$\begin{aligned}(F(m) \circ \psi_j)(a_i)_i &= F(m)(a_j) \\ &= a_k \\ &= \psi_k((a_i)_i).\end{aligned}$$

This shows that the diagram commutes as in the definition of limit. Lastly, if we have a set W with maps $g_i : W \to A_i$, then we can define a map $\Phi : W \to \prod_i A_i$ by letting $\Phi(w) = (g_i(w))_i$. $\square$

2.5.2 Colimits, Filtered Categories

Definition 27. (Colimits). Let $\mathscr{I}$ be a small category and let $\mathscr{C}$ be any category. Let $F : \mathscr{I} \to \mathscr{C}$ be a contravariant functor and let $m : j \to k$ be a morphism in $\mathscr{I}$. Then, the colimit of the diagram is an object, denoted by $\operatorname*{colim}_{\mathscr{I}} A_i \in \mathrm{obj}(\mathscr{C})$, with morphisms $f_j : A_j \to \operatorname*{colim}_{\mathscr{I}} A_i$ for each $j \in \mathscr{I}$ such that the following diagram commutes:

$$\begin{tikzcd} \operatorname*{colim}_{\mathscr{I}} A_i & A_j \arrow[l, "f_j"'] \\ A_k \arrow[u, "f_k"] \arrow[ur, "F(m)"'] & \end{tikzcd}$$

and given there is any other object W with morphisms $g_i : A_i \to W$ that commute with $F(m)$ (i.e. $g_k = g_j \circ F(m)$), there exists a morphism $g : \operatorname*{colim}_{\mathscr{I}} A_i \to W$ such that $g_j = g \circ f_i$.

Definition 28. (Coproducts - *again*). Let I be an index set. Then, the colimit of a diagram indexed by I is called the coproduct, denoted $\amalg_i A_i$, and it is the dual (arrow-reversed) notion to the product.

Definition 29. (Filtered Set). A non-empty partially ordered set $(S, \geq)$ is called *filtered* if for all $x, y \in S$, there exists z such that $x \geq z$ and $y \geq z$.

Definition 30. (Filtered Category). Let $\mathscr{I}$ be a non-empty category. Then $\mathscr{I}$ is called a filtered category if (1) for all $x, y \in \mathscr{I}$, there exists $z \in \mathscr{I}$ with morphisms $x \to z$ and $y \to z$ and (2) for any morphisms $u : x \to y$ and $v : x \to y$, there exists a morphism $w : y \to z$ such that $w \circ u = w \circ v$.

Proposition 16. Suppose $\mathscr{I}$ is filtered. Let $A \sqcup B$ represent the disjoint union of two sets. Now consider any diagram in the category *Sets* indexed by $\mathscr{I}$. Then this diagram has the following colimit with the natural morphisms from each object to the colimit:

$$\{(a_i, i) \in \sqcup_{i \in \mathscr{I}} A_i \mid (a_i, i) \sim (a_j, j) \text{ iff } \exists f : A_i \to A_k \text{ and } g : A_j \to A_k \text{ s.t. } f(a_i) = g(a_j)\}$$

Example of colimit in category of A-modules:
Consider the category of A-modules indexed by a filtered category $\mathscr{I}$. We define the colimit, $\underset{\mathscr{I}}{\operatorname{colim}} M_i$ as:

$$\{(x_i, i) \in \amalg_{i \in \mathscr{I}} M_i \mid (x_i, i) \sim (x_j, j) \text{ iff } \exists f : M_i \to M_k, g : M_j \to M_k, f(x_i) = g(x_j)\}.$$

Now, we need to give this object a module structure. To make it an additive group, we define $(x_i, i) + (x_j, j)$ as follows: choose $l \in \mathscr{I}$ such that there exists $u : i \to l$ and $v : j \to l$ (these exists because $\mathscr{I}$ is filtered). Then,

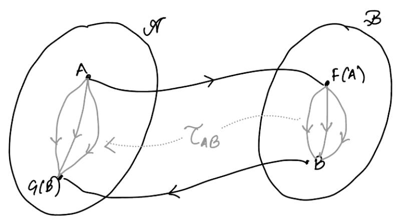
$$(x_i, i) + (x_j, j) = (F(u)(x_i) + F(v)(x_j), l) \in M_l.$$

Furthermore, $(x_i, i) \in M_i$ is 0 if and only if there exists $u : i \to l$ such that $F(u)(x_i) = 0 \in M_l$. To define multiplication by elements in A, we let $a(x_i, i) = (ax_i, i)$. One can easily check that this is a colimit using the obvious morphisms from each M_i which sends $x_i \to (x_i, i)$. To prove well-definedness and uniqueness, one needs to use the fact that $\mathscr{I}$ is a filtered category.

2.6 Adjoints

Definition 31. (Adjoint functors). Two *covariant* functors $F : \mathscr{A} \to \mathscr{B}$ and $G : \mathscr{B} \to A$ are called *adjoint* if there exists a *natural bijection* such that for all $A \in \mathscr{A}, B \in \mathscr{B}$, we have

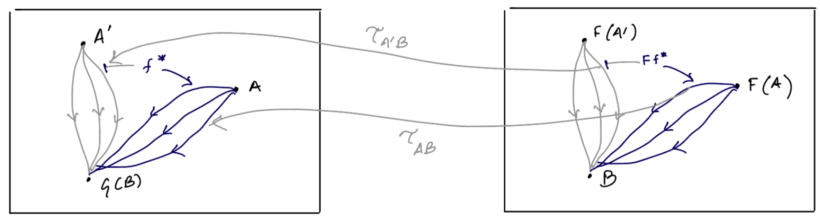
$$\tau_{AB} : \mathrm{Mor}_{\mathscr{B}}(F(A), B) \to \mathrm{Mor}_{\mathscr{A}}(A, G(B)).$$



Here, by naturality, we mean that the following diagram, for any $f : A \to A'$, commutes:

$$\begin{tikzcd}
\mathrm{Mor}_{\mathscr{B}}(F(A'), B) \arrow[r, "Ff^*"] \arrow[d, "\tau_{A'B}"] & \mathrm{Mor}_{\mathscr{B}}(F(A), B) \arrow[d, "\tau_{AB}"] \\
\mathrm{Mor}_{\mathscr{A}}(A', G(B)) \arrow[r, "f^*"] & \mathrm{Mor}_{\mathscr{A}}(A, G(B))
\end{tikzcd}$$

Here, $f^*(\varphi) = \varphi \circ f$ and $Ff^*(\varphi) = \varphi \circ F(f)$.



Similarly, for any $g : B \to B'$ in $\mathscr{B}$, the following commutes:

$$\begin{tikzcd}
\mathrm{Mor}_{\mathscr{B}}(F(A), B) \arrow[r, "g^*"] \arrow[d, "\tau_{AB}"] & \mathrm{Mor}_{\mathscr{B}}(F(A), B') \arrow[d, "\tau_{AB'}"] \\
\mathrm{Mor}_{\mathscr{A}}(A, G(B)) \arrow[r, "Gg^*"] & \mathrm{Mor}_{\mathscr{A}}(A, G(B'))
\end{tikzcd}$$

where $g^*(\varphi) = g \circ \varphi$ and $Gg^*(\varphi) = G(g) \circ \varphi$.

We say (F, G) is an adjoint pair, F is left adjoint to G and G is right adjoint to F.

Next, we look at some immediate properties of τ_{AB} and its inverse.

Claim 1: for each $A \in \mathscr{A}$, there exists a natural transformation $n_A : A \to GF(A)$ such that for any $g : F(A) \to B$, we have that $\tau_{AB}(g) : A \to G(B)$ is given by

$$A \xrightarrow{n_A} GF(A) \xrightarrow{Gg} G(B).$$

This is given by defining $n_A := \tau_{AF(A)}(\mathrm{id}_{F(A)})$.

- This can be seen by noticing that $\tau_{AF(A)} : \mathrm{Mor}_{\mathscr{B}}(F(A), F(A)) \to \mathrm{Mor}_{\mathscr{A}}(A, GF(A))$.
- Now, we need to check that this is a natural transformation. To see this, note the following diagram by letting $B = F(A')$ in the diagram for naturality of τ_{AB}:

$$\begin{tikzcd}
\mathrm{Mor}_{\mathscr{B}}(F(A'), F(A')) \arrow[r, "Ff^*"] \arrow[d, "\tau_{A'F(A')}"] & \mathrm{Mor}_{\mathscr{B}}(F(A), F(A')) \arrow[d, "\tau_{AF(A')}"] \\
\mathrm{Mor}_{\mathscr{A}}(A', G(F(A'))) \arrow[r, "f^*"] & \mathrm{Mor}_{\mathscr{A}}(A, G(F(A')))
\end{tikzcd}$$

  Now, consider $\mathrm{id}_{F(A')}$. Then,

$$\begin{aligned}
(\tau_{AF(A')} \circ Ff^*)(\mathrm{id}_{F(A')}) &= (f^* \circ \tau_{A'F(A')})(\mathrm{id}_{F(A')}) \\
(\tau_{AF(A')})(\mathrm{id}_{F(A')} \circ F(f)) &= \tau_{A'F(A')}(\mathrm{id}_{F(A')}) \circ f \\
\tau_{AF(A')}(F(f)) &= n_{A'} \circ f \\
GF(f) \circ n_A &= n_{A'} \circ f
\end{aligned}$$

  This means, the following diagram commutes:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "n_A"] & A' \arrow[d, "n_{A'}"] \\
G(F(A)) \arrow[r, "GF(f)"] & G(F(A'))
\end{tikzcd}$$

Claim 2: $\tau_{AB}(g) = Gg \circ n_A$ is natural transformation:

- First, note that n_A is a natural transformation. Then, for any $f : A \to A'$, we have that $n_{A'} \circ f = GF(f) \circ n_A$.
- Using this, we note, for any $\varphi \in \mathrm{Mor}_{\mathscr{B}}(F(A'), B)$:

$$\begin{aligned}(\tau_{AB} \circ Ff^*)(\varphi) &= \tau_{AB}(\varphi \circ F(f)) \\ &= G(\varphi \circ F(f)) \circ n_A\end{aligned}$$

  where as

$$\begin{aligned}(f^* \circ \tau_{A'B})(\varphi) &= f^*(G(\varphi) \circ n_{A'}) \\ &= (G(\varphi) \circ n_{A'}) \circ f\end{aligned}$$

  These are equal since

$$(G(\varphi) \circ n_{A'}) \circ f = G(\varphi) \circ n_{A'} \circ f = G(\varphi) \circ (G(F(f)) \circ n_A) = G(\varphi \circ F(f)) \circ n_A.$$

Claim 3: We can define the inverse as follows: for each $B \in \mathscr{B}$, there exists $\epsilon_B : FG(B) \to B$ such that for any $f : A \to G(B)$, there exists $\tau_{AB}^{-1}(f) : F(A') \to B$ defined as

$$F(A) \xrightarrow{Ff} FG(B) \xrightarrow{\epsilon_B} B.$$

Here, we define $\epsilon_B := \tau^{-1}_{G(B),B}(\mathrm{id}_{G(B)})$. One can then check that this ϵ_B is, indeed, a natural transformation, τ_{AB}^{-1} defined in this way is a natural transformation and that it is the inverse of τ_{AB}.

Thought process for constructing ϵ_B: Given $f : A \to B$, we know that $\tau_{AB}^{-1} \in \mathrm{Mor}\big(F(A), B\big)$ by $\tau_{AB}^{-1}(f) = \epsilon_B(Ff)$. Now, we need a morphism from $F(G(B))$ to B so we let $A = G(B)$ and consider $\tau_{AB}^{-1}(f) \in \mathrm{Mor}\big(F(G(B)), B\big)$. We can let $f \in \mathrm{Mor}\big(G(B), G(B)\big)$ be $\mathrm{id}_{G(B)}$. Then, note that $\epsilon_B(F\mathrm{id}_{G(B)}) = \epsilon_B(\mathrm{id}_{FG(B)}) = \epsilon_B$ and so we get $\epsilon_B := \tau^{-1}_{G(B),B}(\mathrm{id}_{G(B)})$.

The instructive idea here is that there are some simple morphisms that are guaranteed to exists, like the identity, and we define new constructions/maps like τ_{AB} by seeing whether we can compose these simple, guaranteed morphisms.

2.6.1 Examples of Adjoints in category of modules

Now, we look at a series of examples of adjoints.

Proposition 17. Suppose M, N and P are A-modules, where A is a ring. Then, there exists a bijection $\mathrm{Hom}_A(M \otimes_A N, P) \leftrightarrow \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$.

Proof. Consider $f \in \mathrm{Hom}_A(M \otimes_A N, P)$. Now we shall construct a homomorphism from M to $\mathrm{Hom}_A(N, P)$. Notice that since we have $f \in \mathrm{Hom}_A(M \otimes_A N, P)$. Note that given f, then we can construct a map $M \times N \to P$ by $f \circ \iota$ (where $\iota(m, n) = m \otimes n)$). For any $m \in M$, we can now construct $\varphi(m) = f(\iota(m, \cdot)) : N \to P$. This is an A-module homomorphism because $f \circ \iota$ is A-bilinear. Conversely, let $g \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$. Then, in particular, for any $m \in M$, we have $g(m) \in \mathrm{Hom}_A(N, P)$. Now, we construct a homomorphism $\tilde{g}$ from $M \otimes_A N$ to P by letting $\tilde{g}(m \otimes n) = g(m)(n)$. One can check that these maps are A-bilinear and that they are indeed the inverses of each other. $\square$

Corollary 18. The functor $F : \mathrm{Mod}_A \to \mathrm{Mod}_A$ by $F(M) = M \otimes_A N$ is left adjoint to the functor $G : \mathrm{Mod}_A \to \mathrm{Mod}_A$ by $G(P) = \mathrm{Hom}_A(N, P)$.

Proof. This is straightforward by using the definition of adjoint functors. The statement is proven if there exists a natural bijection enabling us to write

$$\mathrm{Mor}_{\mathrm{Mod}_A}(F(M), P) \cong \mathrm{Mor}_{\mathrm{Mod}_A}(M, \mathrm{Hom}_A(N, P)).$$

This is equivalent to saying

$$\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$$

which follows from the previous proposition. $\square$

Proposition 19. Let $\phi : B \to A$ be a morphismm of rings. If M is an A-module, then we can create a B-module M_B as follows: for any $m \in M, b \in B$, $bm = \phi(b)m \in M$. This gives us a functor $\cdot_B : \mathrm{Mod}_A \to \mathrm{Mod}_B$ from the category of A-modules to the category of B-modules. This functor is right adjoint to the functor from B-modules to the category A-modules via $\cdot_A : N \to N \otimes_B A$. In other words, we have the following:

$$\mathrm{Hom}_A\left(N \otimes_B A, M\right) \cong \mathrm{Hom}_B\left(N, M_B\right).$$

Proof. Given $f \in \mathrm{Hom}_A(N \otimes_B A, M)$, we can construct $g \in \mathrm{Hom}_B(N, M_B)$ by $g(n) = f(n \otimes 1_A)$. On the other hand, given $p \in \mathrm{Hom}_B(N, M_B)$, we can construct $q : N \otimes_B A \to M$ by $q(n \otimes a) = f(n) \cdot a$. We leave it as an exercise to show that these are module homomorphisms and that they are inverses of each other. $\square$

2.6.2 Examples of Adjoints in Category of Abelian Groups

First, we recall:

Definition 32. (Abelian semigroup). An abelian semigroup is a set with a binary operation such that we have associativity i.e. $(xy)z = x(yz)$ (we are suppressing the notation a bit by not showing the binary operation being performed).

Examples of Abelian semigroups: the set of non-negative integers and the set of positive integers under addition. The set of positive integers under multiplication.

Definition 33. (Groupification). For an abelian semigroup S, the groupification of S is a map of abelian semigroups $\pi : S \to G$ such that G is an abelian group and any map of abelian semigroups from S to an abelian group G' factors ***uniquely*** through G:

$$\begin{tikzcd} S \arrow[r, "\pi"] \arrow[dr] & G \arrow[d, "\exists!"] \\ & G' \end{tikzcd}$$

One Process of groupification: Let S be our abelian semigroup. Let $H(S)$ be the groupification of S. The elements of $H(S)$ will be ordered pairs $(a, b) \in S \times S$ which we think of as $a - b$ under the equivalence relation $(a, b) \sim (c, d)$ if $a + d + e = b + c + e$ for some $e \in S$ (*intuitively think about it as follows - let the operation in S be addition and consider when $a - b = c - d$; we see that e in this case would be* 0). Now, $H(S)$ becomes a group under the operation $(a, b) + (c, d) = (a + b, c + d)$. The identity is (x, x) for any $x \in S$ and the inverse of (a, b) becomes (b, a). Associativity can be easily checked.

We can then define one possible $\pi : S \to G$ by $\pi(x) = (x, 0)$.

Proposition 20. Suppose S is an abelian group. Then, the identity morphism $\mathrm{id}_S : S \to S$ is a groupification.

Proof. This follows straightforwardly from the definition since any morphism $\pi' : S \to S$ can be written as $\pi' \circ \mathrm{id}_S$. □

Definition 34. (Groupification Functor). This is the functor from the category of non-empty abelian semigroups to the category of abelian groups (denoted by *Ab*). We saw one example of this already in the process of groupification above, given by $\pi : S \to G$ where $\pi(x) = (x, 0)$.

Proposition 21. The groupification functor, H, is left-adjoint to the forgetful functor F (this functor maps the group G to G, which is of course automatically an abelian semi-group).

Sketch of proof: leaving all the verifications as an exercise, we can map a semigroup homomorphism $\varphi : S \to F(G)$ to a morphism $\psi : H(S) \to G$ as follows: $\psi((a, b)) = \varphi(a) - \varphi(b)$

2.7 Additive Categories

Definition 35. (Additive Categories). Let $\mathscr{C}$ be a category. Then, $\mathscr{C}$ is called an additive category if it satisfies the following:

- for each $A, B \in \mathrm{obj}(\mathscr{C})$, we have that $\mathrm{Mor}\big(A, B\big)$ is an *abelian group*. In other words, for *every pair of objects*, we have a 0_{AB}-morphism such that $f + 0_{AB} = 0_{AB} + f = f$, $f + g = g + f$ and $(f + g) + h = f + (g + h)$ for any $f, g, h \in \mathrm{Mor}\big(A, B\big)$. For any $f \in \mathrm{Mor}\big(A, B\big)$, there exists a $(-f) \in \mathrm{Mor}\big(A, B\big)$ such that $f + (-f) = 0_{AB}$.

- We have the distributive property: let $h \in \mathrm{Mor}\big(B, C\big)$ and let $k \in \mathrm{Mor}\big(P, A\big)$. Then, for any $f, g \in \mathrm{Mor}\big(A, B\big)$, we have $(f+g) \circ k = f \circ k + g \circ k$ and $h \circ (f+g) = h \circ f + h \circ g$.
- $\mathscr{C}$ has a zero object, denoted by 0. In other words, there exists $0 \in \mathrm{obj}(\mathscr{C})$ such that 0 has only one map (i.e. the zero morphism) to every object and only one map (the zero morphism) from every object.
- There exists a product for any two objects i.e., for any $A, B \in \mathscr{C}$, there exists $A \times B$. By induction, there exists a product for any finite number of objects. The product is denoted by $A \oplus B$ for reasons that will be clear soon.

Note: for *any pair of objects*, we will have at least one morphism between them i.e., the 0-morphism.

Vocabulary: In an additive category, the morphisms are called **homomorphisms** and we write $\mathrm{Mor}\big(A, B\big)$ as $\mathrm{Hom}\big(A, B\big)$.

Definition 36. (Additive functor). Let $F : \mathscr{A} \to \mathscr{B}$ be a covariant functor between the additive categories $\mathscr{A}$ and $\mathscr{B}$. Then F is an additive functor if $F(f+g) = F(f)+F(g)$ for all morphisms f and g.

Some preliminary properties...

Proposition 22. Let $\mathscr{C}$ be an additive category. Then

- $f \circ 0_{XA} = 0_{XB}$ for all $f \in \mathrm{Hom}\big(A, B\big)$. Similarlyly, $0_{BX} \circ f = 0_{AX}$.
- Consider the product $X \oplus Y$. Then, $\mathrm{id}_{X \oplus Y} = i_X \circ pr_X + i_Y \circ pr_Y$. Here $pr_X : X \oplus Y \to X$ and $pr_Y : X \oplus Y \to Y$ are the usual projection morphisms while $i_X : X \to X \oplus Y$ and $i_Y : Y \to X \oplus Y$ are morphisms such that $pr_X \circ i_X = \mathrm{id}_X$ and $pr_Y \circ i_Y = \mathrm{id}_Y$.

(We will prove the existence of these morphisms soon).

Proof. Proving the first part is straightforward: $f \circ 0 = f \circ (0+0) = f \circ 0 + f \circ 0$ implies the desired property. Proving the second part: the morphism from $X \oplus Y$ to $X \oplus Y$ is unique by the universal property of products. This means this morphism must be the identity. However, $i_X \circ pr_X + i_Y \circ pr_Y$ is also a morphism from $X \oplus Y$ to $X \oplus Y$. $\square$

Now, we finally prove the result that justifies the notation $A \oplus B$ for the product $A \times B$.

Proposition 23. In an additive category, finite products are also finite coproducts.

Proof. Let $X \times Y$ be our product of X and Y. Then, we have morphisms pr_X and pr_Y from $X \times Y$ to X and Y respectively. Furthermore, if Z is another object with morphisms to X and Y, then these morphisms factor *uniquely* through $X \times Y$. Now, notice X has morphisms id_X to

X and 0_{XY} to Y, so there exists $i_X : X \to X \times Y$ such that $\mathrm{id}_X = pr_X \circ i_X$ and $0_{XY} = pr_Y \circ i_X$. Similarly, we have $i_Y : Y \to X \times Y$ with similar properties.

Now, we have the following:

$$\begin{tikzcd}
Z & & \\
& X \times Y & X \arrow[ull, "p_{XZ}"'] \arrow[l, "i_X"'] \\
& Y \arrow[uul, "p_{YZ}"] \arrow[u, "i_Y"] &
\end{tikzcd}$$

Let $\psi : X \times Y \to Z$ such that $\psi = p_{XZ} \circ pr_X + p_{YZ} \circ pr_Y$. One can easily check that $\psi \circ i_X = p_{XZ}$ and $\psi \circ i_Y = p_{YZ}$. To show uniqueness, let $h : X \times Y \to Z$. Notice that we can write $h = h \circ id_{X \times Y} = h \circ (i_X \circ pr_X + i_Y \circ pr_Y) = p_{XZ} \circ pr_X + p_{YZ} \circ pr_Y$. $\square$

Note: the fact that products are coproducts in additive categories allows us to denote them both as $X \oplus Y$.

Proposition 24. The object Z is a zero object if and only if $\mathrm{id}_Z = 0_Z$.

Proof. Suppose Z is a zero object. Then, for any A and B we have only one morphism to and from Z respectively and they are 0_{AZ} and 0_{ZB} respectively. Let $B = A$ and we know id_Z exists so $\mathrm{id}_Z = 0_Z$. Conversely, if $\mathrm{id}_Z = 0_Z$, then we have for any A, we have $A \to Z$ by 0_{AZ}. We only need to show that this is the only morphism from A to Z. Let $f : A \to Z$ be another such morphism. Then, $f = \mathrm{id}_Z \circ f = 0_Z \circ f = 0_{AZ}$ $\square$

Proposition 25. Let $\mathscr{A}$ and $\mathscr{B}$ be additive categories. Then, any additive functor $F : \mathscr{A} \to \mathscr{B}$ sends the zero object $0_{\mathscr{A}}$ to the zero object $0_{\mathscr{B}}$.

Proof. Suppose $Z \in \mathscr{A}$ is $0_{\mathscr{A}}$. Then, $id_Z = 0_Z$. Then, $F(\mathrm{id}_Z) = F(0_Z) = 0_{F(Z)}$. But we also know that $F(\mathrm{id}_Z) = \mathrm{id}_{F(Z)}$ by definitino of covariant functors. So $\mathrm{id}_{F(Z)} = 0_{F(Z)}$. Therefore, $F(Z)$ is $0_{\mathscr{B}}$. $\square$

Proposition 26. The zero morphism $0_{AB} \in \mathrm{Hom}\big(A, B\big)$ is the composition $A \to 0 \to B$.

Proof. $A \to 0 \to B$ is a zero morphism since it is the composition of two zero morphisms. Since the zero morphism is unique (as this is the identity in an additive abelian group), we have that $0_{AB} = (A \to 0 \to B)$ $\square$

2.8 Kernel and Cokernel of Morphisms

We begin by defining the kernel and cokernel of a morphism.

Definition 37. (Kernel of a morphism). Let $\mathscr{C}$ be a category with a zero object, 0, and 0-morphisms (defined as $X \to 0 \to Y$). A kernel of a morphism $f : B \to C$ is a morphism $i : A \to B$ such that $f \circ i = 0$ and the kernel is universal with respect to this property i.e. if there exists another object Z with morphism $\psi : Z \to B$ such that $f \circ \psi = 0$, then there exists a unique morphism from Z to A. We denote the kernel of the morphism f by $\ker f$.

In other words, the kernel of the morphism $f : B \to C$ is an object A and morphism i such that i sends f to the zero morphism - hence, the name kernel.

Note: by kernel we refer to both the object A and the morphism from A to B in this definition.

Definition 38. (Cokernel of a morphism). Let $\mathscr{C}$ be a category with a zero object, 0, and 0-morphisms. The cokernel of a morphism $f : B \to C$ is a morphism $i : C \to A$ such that $i \circ f = 0$ and it is universal with respect to this property i.e., if there exists another object Z with morphism $\psi : C \to Z$ such that $\psi \circ f = 0$, then there exists a unique morphism from A to Z.

Proposition 27. The kernel of a morphism f is the limit of the diagram:

$$\begin{tikzcd} B \arrow[r, "f"] & C \\ & 0 \arrow[u] \end{tikzcd}$$

The cokernel is the colimit of the diagram:

$$\begin{tikzcd} B \arrow[r, "f"] & C \arrow[d] \\ & 0 \end{tikzcd}$$

Proposition 28. Let $\mathscr{C}$ be an additive category with kernels defined. Then, for any morphism g, g is a monomorphism if and only if $\ker g = 0$. Similarly, g is an epimorphism if and only if $\operatorname{coker} g = 0$.

Proof. These can be proven using the fact that g is a monomorphism if and only if it has the left cancellation property i.e., g is a monomorphism if and only if $g \circ \mu_1 = g \circ \mu_2 \implies \mu_1 = \mu_2$, which implies 0 is the only kernel. The statement for epimorphism can be proven similarly. $\square$

Note: it is easy to forget that the kernel of a morphism can be the non-trivial one in which case the cancellation property would not always hold. In other words, if $\ker g = \varphi \neq 0$, then $f \circ g = f' \circ g$ need not entail that $f = f'$.

Note: when chasing diagrams it is also easy to forget that $\ker g$ and coker g need not be 0.

2.9 Abelian Categories

Recall: A morphism $\pi : X \to Y$ is called a monomorphism if any two morphisms $\mu_1 : Z \to X$ and $\mu_2 : Z \to X$ such that $\pi \circ \mu_1 = \pi \circ \mu_2$ must satisfy $\mu_1 = \mu_2$.

Definition 39. (Subobject). Given $\pi : X \to Y$ is a monomorphism, we say X is a subobject of Y.

Recall: A morphism $\pi : X \to Y$ is called an epimorphism if for any object Z and any morphisms $\mu_1, \mu_2 : Y \to Z$ such that $\mu_1 \circ \pi = \mu_2 \circ \pi$, we have that $\mu_1 = \mu_2$.

Definition 40. (Abelian Categories). An Abelian category is an additive category with the following properties:

- Every morphism has a kernel and a cokernel. *In other words, for every $f : B \to C$, there exists $i : A \to B$ such that $f \circ i = 0$ and there exists $g : C \to Z$ such that $g \circ f = 0$.*
- Every monomorphism is the kernel of its cokernel. *In other words, let $f : B \to C$ be a monomorphism i.e, there exists at most one morphism $\mu : A \to B$ such that $f \circ \mu = \nu : A \to C$. Let $g : C \to Z$ such that $g \circ f = 0$. Then, f is universal with respect to this property of $g : C \to Z$.*
- Every epimorphism is the cokernel of its kernel. *In other words, let $f : B \to C$ be an epimorphism i.e., there exists at most one morphism $\mu : C \to Z$ such that $\mu \circ f = \nu : B \to Z$. Now, let $g : C \to D$ such that $g \circ f = 0$. Then, f is universal with respect to this property of $g : C \to D$.*

Note: every kernel of a cokernel is a monomorphism and similarly every cokernel of a kernel is a monomorphism in an abelian category.

Definition 41. (Quotient). The cokernel of a monomorphism is called the quotient. Given $A \to B$ is a monomorphism, the quotient is often denoted by B/A.

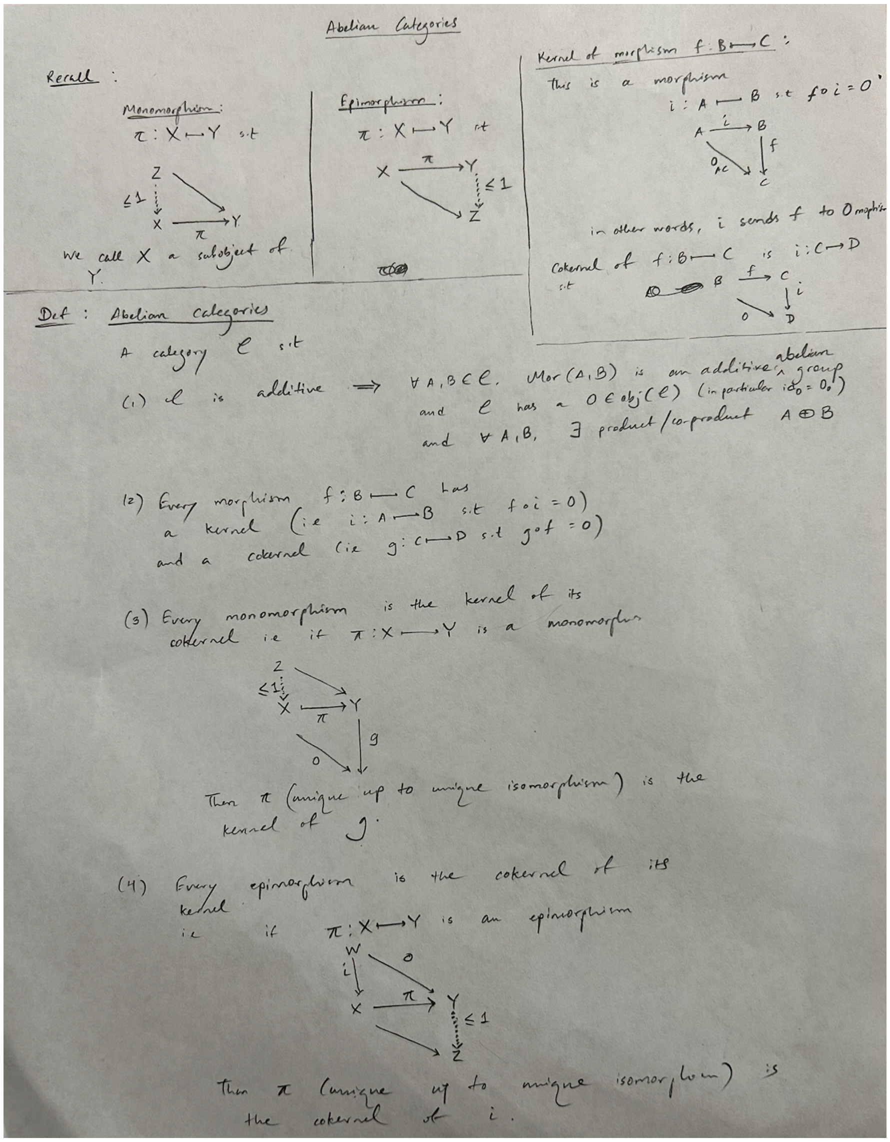


Figure 2: Definition of Abelian Categories

Definition 42. (Image of a morphism). The image of a morphism $f : A \to B$, denoted by im f, is defined to be

$$\text{im } f := \ker(\text{coker} f).$$

Definition 43. (Coimage of a morphism). The coimage of a morphism $f : A \to B$ is coim $f :=$ coker (ker f).

Proposition 29. For any morphism $f : A \to B$, we have a morphism $f_c : A \to \text{coim} f$ that is an epimorphism and we have a morphism $f_i : \text{im} f \to B$ that is a monomorphism.

Proof. Suppose $f : A \to B$ and $p : \ker f \to A$ and $q : A \to \operatorname{coker} \ker f = \operatorname{coim} f$. Now, if there exists another morphism from A to X such that we have two morphism $\mu_1, \mu_2 : \operatorname{coker} \ker f \to X$, then, we have $\mu_1 \circ q \circ p = 0$, which says there must be a *unique* morphism from $\operatorname{coker} \ker f = \operatorname{coim} f$ to X, which means $\mu_2 = \mu_1$. Similar reasoning shows the second part. □

Proposition 30. In an abelian category, for any morphism $f : X \to Y$, we can write it as $X \to \text{coim } f \to \text{im } f \to Y$.

Proof. By definition of coim f and im f, we know that there exists morphism $X \to \text{coim } f$ and $\text{im } f \to Y$. We need to show that there exists a morphism $\text{coim } f \to \text{im } f$ such that the diagram commutes. First, note that there exists a morphism $g : \text{coim } f \to Y$ - this is because the cokernel is unique but $f \circ \ker f = 0$, so there must be $g : \text{coim } f \to Y$. Now if we denote the morphism from X to coim$f$ as q, then $f = g \circ q$. Then, $\text{coker } f \circ g \circ q = 0$. Now, $\text{coker } f \circ g = 0$ because q is an epimorphism which means its cokernel is 0. But im f is unique so there must be a unique morphism from coim f to im f. □

Proposition 31. In an abelian category, $\operatorname{coker}(\ker(\operatorname{coker} f)) \cong \operatorname{coker} f$ and $\ker(\operatorname{coker}(\ker f)) = \ker f$.

Proof. Let $f : A \to B$. To prove the first part, we note that the cokernel of the image is unique but given $\varphi : B \to \operatorname{coker} f$ then $\varphi \circ$ (the map from image of f to $B = 0$. So there must be a unique morphism $\operatorname{coker} \ker \operatorname{coker} f \to \operatorname{coker} f$. On the other hand, the cokernel of f is unique but one can show that if $\psi : B \to \operatorname{coker} \ker \operatorname{coker} f$, then $\psi \circ f = 0$ so there must be a unique morphism from $\operatorname{coker} f$ to $\operatorname{coker} \ker \operatorname{coker} f$. One can check that these morphisms commute delivering us the isomorphism. The second part is proven similarly. □

Proposition 32. In an abelian category, a morphism is an isomorphism if and only if it is a monomorphism and an epimorphism.

Proof. Suppose f is an isomorphism. Then, we can exercise the left and right cancellations. In other words, suppose $g \circ f = h \circ f$. Then, $g \circ f \circ f^{-1} = h \circ f \circ f^{-1}$ gets us $g = h$ i.e., f is an epimorphism. Similarly one can prove that f is a monomorphism. Conversely, suppose f is both an epimorphism and a monomorphism. Then, the object image of f is X and the object coimage of f is Y. And by our previous proposition we know there exists a unique morphism from the coimage to image i.e. there exists $\tilde{f} : Y \to X$. This also satisfies $f = f \circ \tilde{f} \circ f$. Since this is an additive category, we have $f \circ (\tilde{f} \circ f - \mathrm{id}) = 0$, so $\tilde{f} \circ f = \mathrm{id}$ and similarly one can show that $f \circ \tilde{f} = \mathrm{id}$, giving us that f is an isomorphism. □

Proposition 33. In an abelian category, the coimage of a morphism is uniquely isomorphic to the image.

Proof. We already have the morphism from coim f to im f. A similar strategy shows that there exists a morphism from im f to coim f. Once you have these morphisms, it is easy to check that the diagram commmutes. □

Now, we look at some elementary properties of the image of a morphism:

Proposition 34. Suppose the image of the morphism $f : A \to B$ exists.

1. Then, $f : A \to B$ uniquely factors through im $f \to B$.
2. $\varphi : A \to \text{im } f$ is an epimorphism in every abelian category.
3. $\varphi : A \to \text{im } f$ is a cokernel of ker $f \to A$ in every abelian category.

Proof. Since im f is unique up to unique isomorphism (since it is the kernel of a morphism) and since coker $f \circ f = 0$, by letting im $f : X \to B$, we see that there must be a unique morphism $A \to X$. To prove the second part, we just use the fact that coim $f \cong$ im f. Given the map from A to the coim f is an epimorphism (by definition in an abelian category, since coimage is the cokernel of a kernel), we have that the map from A to im f is also an epimorphism. $\square$

Proposition 35. Suppose we are working in an abelian category. Consider the sequence $A \xrightarrow{f} B \xrightarrow{g} C$ and suppose f is an epimorphism. Then, $\operatorname{im} g \circ f = \operatorname{im} g$. On the other hand consider $X \xrightarrow{p} Y \xrightarrow{q} Z$ and suppose q is an monomorphism. Then, $\ker q \circ p = \ker p$.

Proof. Write $g : B \to C$ as $B \xrightarrow{e} \operatorname{im} g \xrightarrow{m} C$ and then, we realize $g \circ f = m \circ e \circ f$. First, one can easily show that $\operatorname{coker} g \circ f = \operatorname{coker} g$. Now, m is a monomorphism so it is the kernel of its cokernel. With this, one can see that the image of $g \circ f$ will have to be $\operatorname{im} g$ since $e \circ f$ is an epimorphism. $\square$

Proposition 36. Let $f : A \to B$ and $s : \ker f \to A$ and $t : B \to \operatorname{coker} f$. Then, s is a monomorphism and t is an epimorphism.

Proof. We show the proof for the epimorphism here. Suppose there exists $\mu, \nu : \operatorname{coker} d^i \to X$ such that $\mu \circ s = \nu \circ s$, which means $\mu \circ s \circ f = \nu \circ s \circ f = 0$, so there must be a unique morphism from $\operatorname{coker} f$ to X. This makes $\mu = \nu$. $\square$

2.9.1 Complexes and Exactness

Definition 44. (Complex at an object). The sequence

$$\cdots \to A \xrightarrow{f} B \xrightarrow{g} C \to \cdots$$

is said to be a complex at B if $g \circ f = 0$

Definition 45. (Exact at an object). The sequence

$$\cdots \to A \xrightarrow{f} B \xrightarrow{g} C \to \cdots$$

is said to be exact at B if $\ker g = \text{im } f$.

We immediately have the following result:

Proposition 37. If a sequence is exact at an object, then it is a complex at that object.

Proof. We may write f as $A \xrightarrow{\psi_1} \text{coim } f \xrightarrow{\psi_2} \text{im } f \xrightarrow{\psi_3} B \xrightarrow{g} 0$.Now since im f = $\ker g$, we have that $\psi_3 \circ g = 0$. Then, $g \circ f = g \circ \psi_3 \circ \psi_2 \circ \psi_1 = 0$. $\square$

Definition 46. (Complex and Exact Sequences). A sequence is complex/exact if it is complex/exact at each intermediate term respectively.

Definition 47. (Short exact sequence). A short exact sequence is an exact sequence with five terms such that the first and last ones are 0:

$$0 \to A \to B \to C \to 0.$$

Proposition 38. The sequence

$$\cdots \to A \xrightarrow{f} B \xrightarrow{g} C \to \cdots$$

is exact at B if and only if coker f = coker $(\ker g)$.

Proof. Suppose the sequence is exact at B. Then, $\ker g = \text{im } f = \operatorname{coker} \ker g$. Then, $\operatorname{coker} \ker g = \operatorname{coker} \text{im } f = \operatorname{coker} f$ using the definition of im f. Conversely, if $\operatorname{coker} f = \operatorname{coker} \ker g$, then $\text{im } f = \ker \operatorname{coker} f = \ker \operatorname{coker} \ker g = \ker g$. $\square$

Proposition 39. Suppose $\mathscr{C}$ is an abelian category. Then, the following holds:

1. $0 \to A \to 0$ is exact if and only if $A = 0$.
2. $0 \to A \xrightarrow{f} B$ is exact if and only if f is a monomorphism.
3. $A \xrightarrow{f} B \to 0$ is exact if and only if f is an epimorphism.
4. $0 \to A \xrightarrow{f} B \to 0$ is exact if and only if f is an isomoprhism.
5. $0 \to A \xrightarrow{f} B \xrightarrow{g} C$ is exact if and only if f is a kernel of g.

Proof. (1) If the sequence in question is exact, then, $\ker g = \operatorname{im} f$ and $g \circ f = 0$. Now, $\operatorname{im} f = 0$; this is because the object $\operatorname{coker} f$ will be A (verify this). Then, $\ker(\operatorname{coker} f)$ is the object 0 (verify this too), which gives us that $\operatorname{im} f = 0$. On the other hand, $\ker g = A$. This means $A = 0$. The reverse direction is straightforwad.
(2) Suppose the provided sequence is exact. We claim that $\ker f = 0$. This is because of the following - suppose there exists $X \xrightarrow{\psi} A \xrightarrow{f} B$ such that $f \circ \psi = 0_{XB}$. On the other hand, $f \circ 0_{0A} = 0_{0B}$. Now, consider $0_{0A} \circ 0_{X0} = 0_{XA}$. Now, $f \circ 0_{XA} = 0_{XB}$ and $f \circ \psi = 0_{XB}$, which shows $\psi = 0_{XA}$. This shows that 0 is the kernel of f. Because $\ker f = 0$, we have that f is a monomorphism (a correspondence we have proven before). Conversely, if f is a monomorphism,

its kernel is 0 and from there it is easy to see that $\ker f = \operatorname{im} 0_{0A}$. (4) Note that we can prove this using the previous parts and the fact that f is an isomorphism if and only if f is a monomorphism and an epimorphism. $\square$

Check: at this point, it is worthwhile to see why $\operatorname{im} f$ and $\ker f$ are called image and kernel by working in the category of modules, Mod_A.

2.9.2 Homology and Cohomology

Definition 48. (Homology). Consider the sequence $\cdots \to A \xrightarrow{f} B \xrightarrow{g} C \to \cdots$. If the sequence is a complex at B (i.e., $g \circ f = 0$), then its homology at B, denoted by H, is defined $H := \ker g / \operatorname{im} f$. In other words, let $i : \operatorname{im} f \to \ker g$ be a monomorphism and let H be cokernel of i with $\psi \circ i = 0$.

$$\begin{tikzcd} \operatorname{im} f \arrow[r, "i"] & \ker g \arrow[d, "\psi"] \\ & H \end{tikzcd}$$

If we write a complex by indexing in *decreasing* order

$$\cdots \to A_{i+1} \to A_i \to A_{i-1} \to \cdots$$

then, H_i is the homology at A_i.

Definition 49. (Cohomology). If we write the complex by indexing in *increasing* order

$$\cdots \to A^{i-1} \to A^i \to A^{i+1} \to \cdots$$

then, the homology at A^i is called the cohomology and denoted by H^i.

Proposition 40. Consider the sequence

$$\cdots \to A \xrightarrow{f} B \xrightarrow{g} C \to \cdots .$$

The sequence is exact at B if and only if its homology at B is 0.

Proof. Suppose the sequence is exact at B. Then, $\ker g = \operatorname{im} f$. But then $\mathrm{id} : \ker g \to \operatorname{im} f$ has the cokernel 0 because if there exists any other morphism φ such that $\varphi \circ \mathrm{id} = 0$, then $\varphi \circ \mathrm{id} = \varphi = 0$. This shows that the homology at B is 0. Conversely, suppose H is 0. Consider the sequence $\ker g \xrightarrow{\varphi} \operatorname{im} f \xrightarrow{c} 0$ such that $c \circ \varphi = 0$ and c is the cokernel morphism of the monomorphism φ. Since φ is a monomorphism, it is the kernel of its cokernel. But the kernel of $c : \operatorname{im} f \to 0$ is $\operatorname{im} f$ so $\ker g = \operatorname{im} f$. $\square$

Definition 50. (Cycles, Boundaries) Element of $\ker g$ are called cycles (assuming that the objects of the category are sets with some additional structure - like vector spaces). The elements of $\operatorname{im} f$ are called the boundaries.

Proposition 41. Given the short exact sequence $\cdots \to A^{i-1} \xrightarrow{f^{i-1}} A^i \xrightarrow{f^i} A^{i+1} \xrightarrow{f^{i+1}} \cdots$, we have the following short exact sequences:

$$0 \to \ker f^i \to A^i \to \ker f^{i+1} \to 0.$$

Proof. From the short exact sequence provided, we know $\ker f^i = \operatorname{im} f^{i-1}$. Let $\varphi : \ker f^i \to A^i$ and let $\psi : A^i \to \ker f^{i+1}$. Now let $\ker \psi$ have the morphism $\tilde{\psi} : \ker \psi \to A^i$. Now consider $\operatorname{im} \phi$. It is straightforward to check that $\operatorname{im} \varphi = \ker f^i$. Next, we claim $\ker \psi = \ker f^i$. This is because if $\ker \psi$ has the object P with morphism $\alpha : P \to A^i$, then, one can see that $f^i \circ \alpha = 0$, so there must be a unique morphism from P to $\ker f^i$ which allows $\ker f^i$ to satisfy the properties of the kernel of ψ. $\square$

Proposition 42. Given the complex:

$$\cdots \to A^{i-1} \xrightarrow{f^{i-1}} A^i \xrightarrow{f^i} A^{i+1} \xrightarrow{f^{i+1}} \cdots$$

we can factor two short exact sequences:

$$0 \to \ker f^i \to A^i \to \operatorname{im} f^i \to 0$$

and

$$0 \to \operatorname{im} f^{i-1} \to \ker f^i \to H^i \to 0.$$

Proof. We start with the first one. Suppose $\iota : \ker f^i \to A^i$ is a monomorphism. Now, let $\psi_i : A^i \to \operatorname{coim} f^i$. Now, $\operatorname{coim} f^i = A^i / \ker f^i$ and $\operatorname{coim} f^i \cong \operatorname{im} f^i$ so $\psi_i : A^i \to \operatorname{im} f^i$. Now, $\ker \psi_i = \ker \operatorname{coker} \ker f^i = \ker f^i$. On the other hand, $\operatorname{im} \ker f^i = \ker \operatorname{coker} \ker f^i = \ker f^i$. Now on to the second part. Let $\varphi : \operatorname{im} f^{i-1} \to \ker f^i$ and let $\psi : \ker f^i \to H^i = \operatorname{coker} \varphi$. Then, $\ker \psi = \ker \operatorname{coker} \varphi = \varphi$ since φ is a monomorphism. On the other hand, $\operatorname{im} \varphi = \ker \operatorname{coker} \varphi = \varphi$. Note: φ is a monomorphism because the morphism from $\operatorname{im} f^{i-1}$ to A^i is a monomorphism and the morphism from $\ker A^i$ to A^i is monic and we can easily show that there exista a unique morphism from $\operatorname{im} f^{i-1}$ to $\ker f^i$, which therefore must be a monomorphism. $\square$

Proposition 43. The following are exact sequences:

1. $0 \to \operatorname{im} f^i \to A^{i+1} \to \operatorname{coker} f^i \to 0$.
2. $0 \to H^i(A^\bullet) \to \operatorname{coker} f^{i-1} \to \operatorname{im} f^i \to 0$.

Proposition 44. Suppose the following

$$0 \xrightarrow{d^0} A^1 \xrightarrow{d^1} A^2 \xrightarrow{d^2} \cdots \xrightarrow{d^{n-1}} A^n \xrightarrow{d^n} 0$$

is a complex of dinite-dimensional k-vector spaces denoted by $A^\bullet$. Define $h^i(A^\bullet) = \dim H^i(A^\bullet)$. Then,

1. $\sum_i (-1)^i \mathrm{dim} A^i = \sum_i (-1)^i h^i(A^\bullet)$.
2. If $A^\bullet$ is exact, then $\sum_i (-1)^i \dim A^i = 0$.

Proof. Using linear algebra, $h^i(A^\bullet) = \dim H^i(A^\bullet) = \dim \ker d^i / \operatorname{im} d^{i-1} = \dim \ker d^i - \dim \operatorname{im} d^{i-1}$. On the other hand, note that $0 \to \ker A^i \to A^i \to \operatorname{im} d^{i-1} \to 0$. Then, by the rank-nullity theorem, $\dim A^i = \dim \ker d^i + \dim \operatorname{im} d^i$. Now, we proceed as follows:

$$\begin{aligned}
&\sum_i (-1)^i \dim A^i \\
&= \sum_i (-1)^i \dim \ker d^i + \sum_i (-1)^i \dim \operatorname{im} d^i \\
&= \sum_i (-1)^i \dim \ker d^i - \sum_{i=1}^{n} (-1)^i \dim \operatorname{im} d^{i-1}
\end{aligned}$$

But $\operatorname{im} d^{-1} = \operatorname{im} d^n = 0$, so

$$\begin{aligned}
&\sum_i (-1)^i \dim A^i \\
&= \sum_i (-1)^i \dim \ker d^i - \sum_{i=1}^{n} (-1)^i \dim \operatorname{im} d^{i-1} \\
&= \sum_i (-1)^i (\dim \ker d^i - \dim \operatorname{im} d^{i-1}) \\
&= \sum_i (-1)^i h^i(A^\bullet).
\end{aligned}$$

To prove the second part, we just note that if $A^\bullet$ is exact, then, $H^i(A^\bullet) = 0$ for all i. $\square$

Definition 51. (Category of complexes). Let $\mathscr{C}$ be an abelian category. The category of complexes, denoted by $\mathrm{Com}_{\mathscr{C}}$, is an abelian category that consists of the objects

$$\cdots \to A^{i-1} \xrightarrow{f^{i-1}} A^i \xrightarrow{f^i} A^{i+1} \xrightarrow{f^{i+1}} \cdots$$

and the morphisms are

$$\begin{tikzcd}
\cdots \arrow[r] & A^{i-1} \arrow[r, "f^{i-1}"] \arrow[d] & A^i \arrow[r, "f^i"] \arrow[d] & A^{i+1} \arrow[r, "f^{i+1}"] \arrow[d] & \cdots \\
\cdots \arrow[r] & B^{i-1} \arrow[r, "g^{i-1}"] & B^i \arrow[r, "g^i"] & B^{i+1} \arrow[r, "g^{i+1}"] & \cdots
\end{tikzcd}$$

Proposition 45. The morphism in $\mathrm{Com}_{\mathscr{C}}$ represented as

$$\begin{tikzcd}
\cdots \arrow[r] & A^{i-1} \arrow[r, "f^{i-1}"] \arrow[d] & A^i \arrow[r, "f^i"] \arrow[d] & A^{i+1} \arrow[r, "f^{i+1}"] \arrow[d] & \cdots \\
\cdots \arrow[r] & B^{i-1} \arrow[r, "g^{i-1}"] & B^i \arrow[r, "g^i"] & B^{i+1} \arrow[r, "g^{i+1}"] & \cdots
\end{tikzcd}$$

induces a map of cohomology $H^i(A^\bullet) \to H^i(B^\bullet)$.

Proof. The high-level idea is that we find morphisms from $\ker f^i$ to $\ker g^i$ and from $\operatorname{im} f^{i-1}$ to $\operatorname{im} g^{i-1}$, which will induce our required morphism. First, we show that there exists a morphism from $\ker f^i$ to $\ker g^i$. To see this, we label all the necessary morphisms as follows:

$$\begin{tikzcd}
\operatorname{im} f^{i-1} \arrow[r] & \ker f^i \arrow[r] \arrow[d, "k_i"] & H^i(A^\bullet) \\
A^{i-1} \arrow[u, "j_{i-1}"] \arrow[r, "f^{i-1}"] \arrow[d, "x_{i-1}"] & A^i \arrow[r, "f^i"] \arrow[d, "x_i"] & A^{i+1} \arrow[d, "x_{i+1}"] \\
B^{i-1} \arrow[r, "g^{i-1}"] \arrow[d, "\tilde{j}_{i-1}"] & B^i \arrow[r, "g^i"] & B^{i+1} \\
\operatorname{im} g^{i-1} \arrow[r] & \ker g^i \arrow[u, "\tilde{k}_i"] &
\end{tikzcd}$$

We first show that $g_i \circ x_i \circ k_i = 0$. This is straightforward since $g_i \circ x_i \circ k_i = x_{i+1} \circ f^i \circ k_i = x_{i+1} \circ 0 = 0$. Since the kernel of g_i is unique, there must be a unique morphism from $\ker f^i$ to $\ker g^i$. One can prove that there exists a morphism from $\operatorname{im} f^{i-1}$ to $\operatorname{im} g^{i-1}$ in a similar way - we consider the cokernel of g^{i-1}. Then, the kernel of this is $\operatorname{im} g^{i-1}$. Now if f^{i-1} is 0, then, the morphism from $\operatorname{im} f^{i-1}$ to $\operatorname{coker} g^{i-1}$ via x_i will be 0 since $\operatorname{im} f^{i-1}$ is 0. If not, then, A^{i-1} to $\operatorname{im} f^{i-1}$ is not 0. But then, $g^{i-1} \circ x_{i-1} = x_i \circ f^{i-1}$ and then, we again see that the morphism from $\operatorname{im} f^{i-1}$ to $\operatorname{coker} g^{i-1}$ via x_i will be 0. But the kernel of $\operatorname{coker} g^{i-1}$ is unique, so there is a morphism from $\operatorname{im} f^{i-1}$ to $\operatorname{im} g^{i-1}$. But now, we have the following:

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{im} f^{i-1} \arrow[r, "p"] \arrow[d, "\varphi"] & \ker f^i \arrow[r, "q"] \arrow[d, "\psi"] & H^i(A^\bullet) \arrow[r] & 0 \\
0 \arrow[r] & \operatorname{im} g^{i-1} \arrow[r, "p'"] & \ker g^i \arrow[r, "q'"] & H^i(B^\bullet) \arrow[r] & 0
\end{tikzcd}$$

Note that q is the unique cokernel morphism of p. But $q' \circ \psi \circ p = q' \circ p' \circ \varphi = 0 \circ \varphi = 0$. So there must be a unique morphism from $H^i(A^\bullet)$ to $H^i(B^\bullet)$. $\square$

Proposition 46. H^i is a covariant functor $\mathrm{Com}_{\mathscr{C}} \to \mathscr{C}$.

Proof. The functor is defined as follows: for any complex $A^\bullet \in \mathrm{Com}_{\mathscr{C}}$, $H^i(A^\bullet) = \ker f^i / \mathrm{im}\, f^{i-1}$. For any morphism $\psi : A^\bullet \to B^\bullet$, we define $H^i(\psi) : H^i(A^\bullet) \to H^i(B^\bullet)$ by the map that is induced from $\psi \in \mathrm{Com}_{\mathscr{C}}$. One can easily check that $H^i(\mathrm{id}_{A^\bullet}) = \mathrm{id}_{H^i(A^\bullet)}$ and that composition is obeyed: for any $A^\bullet \xrightarrow{\psi} B^\bullet \xrightarrow{\psi'} C^\bullet$, we have that $H^i(\psi' \circ \psi) = H^i(\psi') \circ H^i(\psi)$. $\square$

2.9.3 Exactness of Functors

Definition 52. (Right-exact, Left-exact, Exact covariant functor) Suppose $\mathscr{A}$ and $\mathscr{B}$ are two abelian categories. Let $F : \mathscr{A} \to \mathscr{B}$ be an additive covariant functor. Then, F is right-exact if the exactness of

$$A' \to A \to A'' \to 0$$

implies that

$$F(A') \to F(A) \to F(A'') \to 0$$

is exact. On the other hand, F is called left-exact if the exactness of

$$0 \to A' \to A \to A''$$

implies that

$$0 \to F(A') \to F(A) \to F(A'')$$

is also exact. If F is both left-exact and right-exact, then F is called an exact functor.

Recall: additive functors are functors between additive categories that preserve the additive structure of homomorphisms.

Definition 53. (Right-exact, Left-exact, Exact contravariant functor). Suppose $\mathscr{A}$ and $\mathscr{B}$ are two abelian categories. Let $F : \mathscr{A} \to \mathscr{B}$ be an additive contravariant functor. Then, F is right-exact if the exactness of

$$A' \to A \to A'' \to 0$$

implies that

$$0 \to F(A'') \to F(A) \to F(A')$$

is exact. Similarly, F is called left-exact if the exactness of

$$0 \to A' \to A \to A''$$

implies that

$$F(A'') \to F(A) \to F(A') \to 0$$

is also exact. If F is both left-exact and right-exact, then F is exact.

Proposition 47. Left-exact functors preserve monomorphisms. Right-exact functors preserve epimorphisms.

Proof. Suppose $f : A \to B$ is a monorphism. Then, $0 \to A \to B$ is exact (since kernel of a monomorphism is 0). Now, pad this sequence with whatever we require on the right to get exact sequence $0 \to A \to B \to C$, which gets mapped to an exact sequence by the left-exact functor and then the kernel of $F(f)$ will still be 0 meaning $F(f)$ is a monomorphism. $\square$

Proposition 48. Exact functors preserve exact sequences. In other words, if F is an exact covariant functor and $A' \to A \to A''$ is exact, then $F(A') \to F(A) \to F(A'')$ is also exact. Similarly, if F is an exact contravariant functor, then $F(A'') \to F(A) \to F(A')$ is exact.

Proof. The concise version of this proof, thankfully, exists on the internet [5]. The idea is to first recognize that $0 \to \ker f \to A' \to \operatorname{im} f \to 0$ is an exact sequence. This you can see by noting that $\varphi : A' \to \operatorname{im} f$ is the cokernel of $\ker f \to A'$. Similarly, you can show that $0 \to \operatorname{im} f \to A \to \operatorname{im} g \to 0$ is exact. Since F is an exact additive functor, these exact sequences remain exact after mapping with F to the category $\mathscr{B}$.

Now,

$$\begin{aligned}\operatorname{im} F(f) &= \operatorname{im} F(A') \xrightarrow{e} F(\operatorname{im} f) \xrightarrow{m} F(A)\\ &= \operatorname{im} F(\operatorname{im} f) \to F(A)\end{aligned}$$

This is because F is e is an epimorphism (since F preserves epimorphisms and monomorphisms). But then, we can proceed

$$\begin{aligned}\operatorname{im} F(f) &= \operatorname{im} F(A') \xrightarrow{e} F(\operatorname{im} f) \xrightarrow{m} F(A)\\ &= \operatorname{im} F(\operatorname{im} f) \to F(A)\\ &= \ker F(A') \to F(img)\\ &= \ker F(A') \to F(img) \to F(A'')\\ &= \ker F(g).\end{aligned}$$

$\square$

Careful: an additive covariant/contravariant functor alone does not necessarily preserve structures like kernels and cokernels - hence, they need not preserve exactness.

Proposition 49. (Ferbahnhof (FHHF) Theorem). Suppose $F : \mathscr{A} \to \mathscr{B}$ is a covariant functor of abelian categories and $C^\bullet$ is a complex in $\mathscr{A}$. Then,
(a) if F is right-exact, there exists a natural morphism $F(H^i(C^\bullet)) \to H^i(F(C^\bullet))$.
(b) if F is left-exact, there exists a natural morphism $H^i(F(C^\bullet)) \to F(H^i(C^\bullet))$.
(c) if F is exact, these two morphisms above are inverses and, therefore, form an isomorphism.

Proof. We first show that $C^i \xrightarrow{d^i} C^{i+1} \xrightarrow{s} \operatorname{coker} d^i \xrightarrow{t} 0$ is an exact sequence. This is because $\ker s = \operatorname{im} d^i$ by definition. On the other hand, $\ker t = \operatorname{coker} d^i$ and $\operatorname{im} s = \ker \operatorname{coker} s = \operatorname{coker} d^i$

(since s is epic). Given this sequence is exact,

$$F(C^i) \xrightarrow{F(d^i)} F(C^{i+1}) \xrightarrow{F(s)} F(\operatorname{coker} d^i) \xrightarrow{F(t)} 0$$

is also exact (as F is right exact and covariant). Since $F(s) \circ F(d^i) = F(s \circ d^i) = F(0) = 0$, there exists a unique morphism from $\operatorname{coker} F(d^i)$ to $F(\operatorname{coker} d^i)$ (by uniqueness of cokernel). By exactness $\ker F(s) = \operatorname{im} F(d^i)$. Letting $\varphi : \ker F(s) \to F(C^{i+1})$, one can show that $\operatorname{coker} \varphi = \operatorname{coker} F(d^i)$. But the coimage of $F(s)$ is isomorphic to image of $F(s)$ and the image of $F(s)$ is the kernel of $F(t)$ which gets us a morphism from $F(\operatorname{coker} d^i)$ to $\operatorname{coker} F(d^i)$. So we have shown that $F(\operatorname{coker} d^i) \cong \operatorname{coker} F(d^i)$.

Next, we recall that the following two are exact sequences:

1. $0 \to \operatorname{im} d^i \to C^{i+1} \to \operatorname{coker} d^i \to 0$.
2. $0 \to H^i(C^\bullet) \to \operatorname{coker} d^{i-1} \to \operatorname{im} d^i \to 0$.

Using the first, we can show that there exists an epimorphism from $F(\operatorname{im} d^i)$ to $\operatorname{im} F(d^i)$. To see this - we first use the above to say $\ker F(s) = \operatorname{im} \varphi$ and then consider $v : F(\operatorname{im} d^i) \to F(C^{i+1})$ with its cokernel $\operatorname{coker} v$. Since kernel of $\operatorname{coker} v$ is unique and it is $\operatorname{im} v$, we get the desired epimorphism.

Lastly, using the second, we can find the morphism $F(H^i(C^\bullet)) \to H^i(F(C^\bullet))$. We do this by the following: we have two exact sequences:

$$F(H^i(C^\bullet)) \to F(\operatorname{coker} d^{i-1}) \to F(\operatorname{im} d^i) \to 0$$

and

$$0 \to H^i(F(C^\bullet)) \xrightarrow{\alpha} \operatorname{coker} F(d^{i-1}) \xrightarrow{\beta} \operatorname{im} F(d^i) \to 0.$$

Using proposition 39, $H^i(F(C^\bullet)) = \ker \beta$. But since we also have the morphism from $F(\operatorname{im} d^i)$ to $\operatorname{im} F(d^i)$ and since the kernel is unique, we see that we must have the desired morphism. This concludes the proof of (a). The proof of (b) is done in a similarly tedious manner. □

3 Affine Varieties

3.1 Algebraic Sets, Affine Varieties and Zariski Topology

We start by defining the following space:

Definition 54. (Affine n-space over field k). Let k be an algebraically closed field. Then, the affine n-space over k, denoted by $\mathbb{A}_k^n$, is the set of all n-tuples, $(k_1, \cdots, k_n)$, of elements of k.

Now, we look at polynomials over the field k and their zeros.

Definition 55. (Zero set of polynomials). Consider the polynomial ring $k[x_1, \cdots, x_n]$ where k is an algebraically closed field. Then, for $T \subseteq k[x_1, \cdots, x_n]$, define the zero set of T to be

$$Z(T) := \{p \in \mathbb{A}_k^n | f(p) = 0, \forall f \in T\}.$$

If a is the ideal generated by $T \subseteq k[x_1, \cdots, x_n]$, then $Z(T) = Z(a)$.

Definition 56. A subset $Y \subseteq \mathbb{A}_k^n$ is an algebraic set if there exists a subset $T \subseteq k[x_1, \cdots, x_n]$ such that $Y = Z(T)$.

Proposition 50. The union of any two algebraic sets is an algebraic set. The intersection of a family of algebraic sets is an algebraic set. The empty set and the whole space, $\mathbb{A}_k^n$, are algebraic sets.

Proof. One can easily verify that if $Y_1 = Z(T_1)$ and $Y_2 = Z(T_2)$, then $Y_1 \cup Y_2 = Z(T_1 T_2)$ ($T_1 T_2$ is the set of product of elements in T_1 and in T_2). Similarly, if $Y_\alpha = Z(T_\alpha)$ for all α, then $\cap Y_\alpha = Z(\cup_\alpha T_\alpha)$. Lastly, $\emptyset = Z(k[x_1, ..., x_n]) = Z(1)$ and $\mathbb{A}_k^n = Z(0)$. $\square$

This last definition indicates that we can easily define a topology on the space $\mathbb{A}_k^n$, or in short, $\mathbb{A}^n$. This topology is called the Zariski topology.

Definition 57. (Zariski Topology). The Zariski topology on $\mathbb{A}^n$ is defined by letting closed sets be algebraic sets.

Example: Zariski topology on $\mathbb{A}^1$. Consider any ideal I in $k[x]$ - since $k[x]$ is a principal ideal domain, the ideal $I = (f)$ for some f. Since $f \in k[x]$ and since k is algebraically closed, we can write $f = c(x_1 - a_1) \cdots (x_n - a_n)$ where a_i are the roots of f. Thus, $Z(f) = \{a_1, \cdots, a_n\}$. Therefore, the closed sets in $\mathbb{A}^1$ are the empty set, finite subsets and $\mathbb{A}^1$. Furthermore, note that this space is not Hausdorff since the open sets are $\emptyset$, $\mathbb{A}^1$ and complements of finite subsets.

Definition 58. (Irreducible sets). A non-empty subset Y of the topological spacee X is called irreducible if one cannot write Y as $Y = X_1 \cup X_2$ where X_1 and X_2 are closed and proper (i.e. non-empty and not equal to X). The empty set is not considered irreducible.

Definition 59. (Affine variety). An affine variety is an irreducible closed subset of $\mathbb{A}^n$ in the Zariski topoology. An open subset of an affine variety is called a quasi-affine variety.

Examples:
(1) $\mathbb{A}^1$ is an affine variety - the closed, proper subsets of $\mathbb{A}^1$ are finite so $\mathbb{A}^1$ cannot be written as the union of two such sets.
(2) Any non-empty open subset of an irreducible space is irreducible and dense.
(3) If Y is an irreducible set in X then $\bar{Y}$ in X is also irreducible.

We travel between the world of $\mathbb{A}^n$ and the polynomials in $k[x_1, \cdots, x_n]$ by first defining the following:

Definition 60. (Ideals in $k[x_1, \cdots, x_n]$). For any subset $Y \subseteq \mathbb{A}^n$, define the ideal of Y in $k[x_1, \cdots, x_n]$ to be

$$I(Y) := \{f \in k[x_1, \cdots, x_n] | f(p) = 0, \forall p \in Y\}.$$

We discuss some immediate properties of the objects introduced so far:

Proposition 51. (1) If $T_1 \subseteq T_2$ in $k[x_1, .., x_n]$, then $Z(T_2) \subseteq Z(T_1)$.
(2) If $Y_1 \subseteq Y_2$ in $\mathbb{A}^n$, then $I(Y_2) \subseteq I(Y_1)$.
(3) For any two subsets Y_1 and Y_2 in $\mathbb{A}^n$, $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.

3.2 Hilbert Basis Theorem

We start with the following observation:

Proposition 52. For any $a := (a_1, ..., a_n) \in \mathbb{A}_k^n$, $I(\{a\}) = (x_1 - a_1, ..., x_n - a_n) \subset k[x_1, ..., x_n]$.

Proof. Note that $(x_1 - a_1, ..., x_n - a_n) \subset I(\{a\})$ which is straightforward. To see the other direction, suppose $f \in I(\{a\})$. Since $f \in k[x_1, .., x_n]$, we can write it as $f = \sum_{i_1,...i_n \geq 0} a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$. Since $f(a) = 0$, we can write this as $f(x) = \sum_{i_1,...i_n \geq 0} b_{i_1 \cdots i_n} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n}$ and so $f(x) \in (x_1 - a_1, ..., x_n - a_n)$. $\square$

Definition 61. A ring R is called Noetherian if every ideal in R is finitely generated.

Example: **Fields and Principal Ideal Domains (PIDs) are Noetherian rings.**

One can easily verify the following equivalent definition of a Noetherian ring:

Proposition 53. R is Noetherian if and only if every sequence of ideals $I_1 \subset I_2 \subset \cdots$ stabilizes i.e there exists N such that $I_N = I_{N+1} = \cdots$.

Proof. Forward direction: If every ideal is finitely generated then the ideal $\cup_i I_i$ is finitely generated and so the generating set of $\cup_i I_i$ must lie in some I_N. Conversely, suppose the sequence stabilizes but there exists an I that is not finitely generated. Then take a sequence of $f_i \in I$ such that $f_i \notin (f_1, ..., f_{i-1})$ yields an increasing sequence of ideals i.e $(f_1) \subset (f_1, f_2) \subset (f_1, f_2, f_3) \subset \cdots$ that does not stabilize - contradiction. $\square$

Theorem 54. (Hilbert Basis Theorem) If R is a Noetherian ring, then $R[x_1, ..., x_n]$ is a Noetherian Ring.

Proof. We know $R[x_1, ..., x_n] \cong R[x_1, ..., x_{n-1}][x_n]$. So, if we can prove that R Noetherian implies $R[x]$ is Noetherian, by induction we will have proven that $R[x_1, ..., x_n]$ is also Noetherian.

Suppose R is Noetherian. Let I be an ideal in $R[x]$. Let J denote the set of leading coefficients of polynomials in I. Then, given I is an ideal, J is an ideal in R. Since R is Noetherian, we can write that J is generated by the leading coefficients of $f_1, ..., f_r \in I$. Suppose $N \in \mathbb{Z}$ such that N is greater than the degrees of all polynomials $f_1, ..., f_r$. Then, for any $m \leq N$, we define J_m to be the ideal in R generated by the leading coefficients of all polynomials f in I such that $deg(f) \leq m$. Once again, since J_m is an ideal in R, we can say that J_m is generated by the finite set of polynomials, $\{f_{mj}\}$, such that each polynomial's degree is less than or equal to m. Finally, define I' be the ideal generated by polynomials $\{f_{mj}\}$ and f_i.

We claim $I' = I$. Suppose not i.e suppose there exists elements in I that are not in I'. Let g be the minimal element such that $g \in I$, $g \notin I'$.

Case 1: $deg(g) > N$. Then, there exists polynomials Q_i such that $\sum_i Q_i f_i$ has the same leading term as g. Therefore, $deg(g - \sum_i Q_i f_i) < deg(g)$. Since g is the minimal element and $deg(g - \sum_i Q_i f_i) < deg(g)$, therefore $g - \sum_i Q_i f_i \in I'$, which implies $g \in I'$.

Case 2: $m := deg(g) \leq N$. Then, there exists polynomials Q_j such that $\sum_j Q_j f_{mj}$ and g have the same leading term. Using a similar argument, we get that $g \in I'$. $\square$

This has the following interesting implication:

Theorem 55. An algebraic set is the intersection of a finite number of hypersurfaces.

Proof. Let $V(I)$ be an algebraic set. We prove that I is finitely generated since that implies $V(I) = V(f_1, ..., f_r) = \cap_{i=1}^{r} V(f_i)$. Given k is a field, k is a Noetherian ring and by the Hilbert Basis Theorem, $k[x]$ is also Noetherian. Therefore, the ideal I in $k[x]$ is finitely generated. $\square$

Corollary 56. $k[x_1, ..., x_n]$ is a Noetherian ring for any field k.

Proof. Follows from the Hilbert Basis Theorem. $\square$

We have some other useful corollaries:

Corollary 57. Any descending chain of subvarieties of $\mathbb{A}^n$ must stabilize i.e if $V_1 \supset V_2 \supset V_3 \cdots$, then there exists N such that $V_N = V_{N+1} = \cdots$.

Corollary 58. There exists a finite subset $B \subset A$ such that $V(A) = V(B)$.

Exercise:

Define

$$R[[x]] = \{f(x) = \sum_{n=0}^{\infty} a_n x^n : a_n \in R\}.$$

Prove (1) Given $f \in R[[x]], f(x) = \sum_{n=0}^{\infty} a_n x^n$ and suppose there exists b_0 s.t $a_0 b_0 = 1$. Then, there exists $g \in R[[x]]$ s.t $fg = 1$. (2) Given R is Noetherian, $R[[x]]$ is also Noetherian. *Hint: Similar proof to Theorem 1, but use trailing coefficient (coefficient of the smallest power) instead of leading coefficient.*

3.2.1 Module-finite, Ring-finite, Field extensions

Definition 62. (R-Module). Let R be a ring. Let M be an abelian group $(M,+)$. Then, an R-module is M with multiplication $R \times M \to M$ such that for any $a, b \in R$, $m \in M$, $(a+b)m = am + bm, a(m+n) = am + an, (ab)m = a(bm), 1_R m = m$.

Examples of modules:
(1) $\mathbb{Z}^n$ where addition is defined as $(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1 + y_1, \cdots, x_n + y_n)$ and scalar multiplication is defined as $k \cdot (x_1, \cdots, x_n) = (kx_1, \cdots, kx_n)$. Similarly, $\mathbb{R}^n$ and other vector spaces are also modules.
(2) $R[x]$ is an R-module.

Definition 63. (Submodule). A submodule N is a subgroup of R-module, M, such that $an \in N$ for any $a \in R, n \in N$.

One can check that for any $m \in M$, $0_R m = 0_M$ by noting that $0_R m = (x-x)m = xm - xm = 0_M$ for any $x \in R, m \in M$. Also, the submodule N of an R-module is an R-module itself.

Definition 64. (Submodule generated by S). Let $S := \{s_1, s_2, ...\}$ be a set of elements of the R-module M. Then the submodule generated by S is $\{\sum_i r_i s_i | r_i \in R, s_i \in S\}$.

When S is finite, we denote the submodule generated by S as $\sum_i Rs_i$.

3.2.2 Finiteness Conditions of Subrings of a Ring

Definition 65. (Finiteness conditions of subrings of a ring). Let S be a ring and let R be a subring of S.
(1) S is module-finite over R if S is finitely-generated as an R-module i.e $S = \sum_{i=1}^n Rv_i$ where $v_1, ..., v_n \in S$. More explicitly, $S = \{\sum_{i=1}^n r_i v_i : r_i \in R\}$, for $v_1, ..., v_n \in S$ fixed.
(2) S is ring-finite over R if $S = R[v_1, ..., v_n] = \{\sum_i a_i v_1^{i_1} \cdots v_n^{i_n} | a_i \in R\}$ where $v_1, ..., v_n \in S$.
(3) S is a finitely-generated field extension of R if S and R are fields and $S = R(v_1, ..., v_n)$ (the quotient field of $R[v_1, ..., v_n]$) where $v_1, ..., v_n \in S$.

(Recall: the definition of field extension. Firstly, given A is a field, then a subset $B \subseteq A$ is a subfield if it contains 1 and it is closed under addition and multiplication and taking the inverse of non-zero elements of B. Given B is a subfield of A, we call A a field extension of B.)

Proposition 59. (Properties of finiteness conditions)
1. If S is module-finite over R, then S is ring-finite over R.
2. If $L = K(x)$, then L is a finitely-generated field extension of K but L is not ring-finite over K.

Proof. (1) follows from definitions. We prove (2). Using the definition, L is a finitely generated field extension of K and so $K(x)$ is a finitely-generated field extension of K. Now, suppose L is ring-finite over K. Then, $L = K[v_1, ..., v_n]$ and so $K(x) = K[v_1, ..., v_n]$, where $v_1, ..., v_n \in k(x)$. Then, there exists $v_i := \frac{s_i}{t_i} \in K(x)$ that generate L where $i = 1, ..., n$. Define $p := 1/q$ where q is an irreducible polynomial that has a higher degree than all t_i's. Then, as $p \in K(x) = L$, $p = \frac{h}{t_1^{e_1} \cdots t_n^{e_n}}$. Since q has a higher degree than all the t_i's and q is irreducible (which means only one t_i survives whose $e_i = 1$), we see that p cannot be equal to $\frac{1}{q}$. □

3.2.3 Integral over a Ring, Algebraic over a Ring

Definition 66. (Integral over R, Algebraic over R). Let R be a subring of the ring S. Then, $v \in S$ is integral over R if there exists a monic polynomial $f = x^n + a_1 x^{n-1} + \cdots + a_n \in R[x]$ such that $f(v) = 0$ and $a_i \in R$. If R and S are fields, we say v is algebraic over R.

When all elements of S is integral over R, we say S is integral over R. When S and R are fields and S is integral over R, we call S an algebraic extension of R.

Theorem 60. Let R be a subring of an integral domain S and let $v \in S$. Then, the following are equivalent:

(1) v is integral over R.

(2) $R[v]$ is module-finite over R.

(3) There exists a subring R' of S such that R' contains $R[v]$ and it is module-finite over R.

Proof. We see (2) implies (3) readily. Now, (1) implies (2): Suppose v is integral over R with the monic polynomial $f(x) = x^n + a_1 x^{n-1} + ... + a_n$. Then, $f(v) = 0 \implies v^n \in \sum_{i=0}^{n-1} Rv^i$. Therefore, for any integer m, $v^m \in \sum_{i=0}^{n-1} Rv^i$. This implies $R[v]$ is module-finite over R.

Lastly, (3) implies (1) as follows: Suppose R' is module-finite over R. Then, $R' = \sum_{i=1}^{n} Rw_i$, where $w_i \in R'$. Then, $vw_i \in R'$, so $vw_i = \sum_j a_{ij} w_j$ where $a_{ij} \in R$. Now, $vw_i - vw_i = 0$ implies $\sum_{j=1}^{n} \delta_{ij} vw_j - vw_i = 0$ which then implies $\sum_{j=1}^{n} (\delta_{ij} v - a_{ij}) w_j = 0$ (here $\delta_{ij} = 1\{i = j\}$. Write this in matrix notation and consider these equations in the quotient field of S and note than $(w_1, ..., w_n)$ is a non-trivial solution to these equations (as we see, they give 0). Therefore, $det(\delta_{ij} v - a_{ij}) = 0$ from which we get $v^n + a_1 v^{n-1} + ... + a_n = 0$. Therefore, v is integral over R. □

Corollary 61. The set of elements of S that are integral over R is a subring of R that contains R.

Proof. Suppose a, b are elements in S that are integral over R. Now. b is integral over R implies b is integral over $R[a]$ as $R \subset R[a]$. Therefore, by Theorem 60, $R[a, b]$ is module-finite over R. Then, $a + b, a - b, ab \in R[a, b]$ and so they are all integral over R. □

We will need one simple fact from linear algebra:

Lemma 62. If $A = (r_{ij})$ is an $n \times n$ matrix over R and V is a column vector s.t $AV = 0$, then $det(A)V = 0$.

Proof. This is because $det(A)V = det(A)I_nV = adj(A)AV = 0$. $\square$

We will require the following results:

Theorem 63. Suppose an integral domain S is ring-finite over R. Then, S is module-finite over R if and only if S is integral over R.

Proof. For the forward direction: suppose the generators of S are $s_1, ..., s_n$ (where we take $s_1 = 1$ because we enlarge the set of generators as we please as long as it's finite) so $S = \sum_{i=1}^{n} Rs_i$. Then, for any $s \in S$, we can write s as $s = r_1s_1 + \cdots + r_ns_n$.

Now, $ss_i = \sum_{j=1}^{n} r_{ij}s_j$ because $ss_i \in S$ so can be written as a linear combination of s_i. Then, let I_n be the $n \times n$ identity matrix, V is the n dimensional column vectors where $V_i = s_i$ and $B = (r_{ij})$. Then, we can write these equations as $sIV = BV \implies (sI - B)V = 0$. Then, $det(sI - B)V = 0$. However, $v_1 = s_1 = 1$, so $det(sI - B) = 0$ which implies s is the root of a characteristic polynomial of B over R so s is integral over R.

Conversely, suppose S is integral over R and we are told that S is ring-finite over R i.e $S = R[s_1, ..., s_n]$. Then, for each $s_i \in S$, we have a monic polynomial from which we can write, after rearranging $s_i^{k_i} = a_{1,i}s_i^{k_i-1} + \cdots + a_{k_i-1,i}s_i + a_{k_i,i}$. Therefore, $s_i^{k_i}$ is in the submodule of S generated by $\{s_i, \cdots, s_i^{k_i-1}\}$ i.e s_i^m is in this submodule for any m. We know S is ring-finite over R with $s_1, ..., s_n$ as the generators. Now, the direct sum of the submodules (as we saw for each s_i) is also a finitely generated as an R-module and so S is itself module-finite over R. $\square$

Theorem 64. Let L be a field and let k be an algebraically closed subfield of L. Then an element of L that is algebraic over k is in k. Furthermore, an algebraically closed field has no module-finite field extension except itself.

Proof. Proof of the first part - suppose $p \in L$ that is algebraic over k. Therefore, $p^n + a_1p^{n-1} + \cdots + a_n = 0$ with $a_i \in k$. This is a polynomial in $k[x]$ with a root, so by definition of algebraic closure, $p \in k$.

Now, we prove the second part. Suppose L is module-finite over k. Then, by theorem 63, L is integral over k. Then, by the first part $L = k$. $\square$

Lastly,

Theorem 65. Let k be a field. Let $L = k(x)$ be the field of rational functions over k. Then, (a) any element of L that is integral over $k[x]$ is also in $k[x]$. (b) There is no non-zero element $f \in k[x]$ such that $\forall z \in L$, f^nz is integral over $k[x]$ for some $n > 0$.

Proof. (a) p is integral over $k[x]$ implies there exists the following polynomial $p^n + a_1 p^{n-1} + ... = 0$. Now, since $p \in k(x)$, we may write it as $p = \frac{s}{t}$ where $s, t \in k[x], t \neq 0$. Then, we get $s^n + a_1 s^{n-1} t + \cdots + a_n t^n = 0$. Rearranging, we get $s^n = -a_1 s^{n-1} t - \cdots - a_n t^n$. Since t divides the right hand side, t divides s. This means, s/t is a polynomial in $k[x]$. Therefore, $p \in k[x]$.

(b) Suppose, not. Let f be such a function. Let $p(x) \in k[x]$ such that $p(x)$ does not divide f^m for any m. Set $z = \frac{1}{p}$, so $z \in L = k(x)$. Then, $f^n z = \frac{f^n}{p}$ is integral over $k[x]$. This means, there exists $a_i \in k[x]$ such that $(\frac{f^n}{p})^d + \sum_{i=1}^{d-1} a_i (\frac{f^n}{p})^i = 0$. From this, we get $f^{nd} = \sum_{i=1}^{d-1} a_i p^{d-i} f^{in}$. Since p divides the right hand side, we get that p divides f^{nd} which contradicts our definition of p. $\square$

3.3 Hilbert's Nullstellensatz

First, we prove the following:

Theorem 66. (Zariski) If a field L is ring-finite over a subfield k, then L is module finite (and, hence, algebraic) over k.

Note that L is module finite over k if and only if L is integral over k which means L is algebraic over k.

Proof. Suppose L is ring-finite over k. Then, $L = k[v_1, ..., v_n]$ where $v_i \in L$. We proceed by induction.

Suppose $n = 1$. We have that k is a subfield of L and $L = k[v]$. Let $\psi : k[x] \to L$ be a homomorphism that takes x to v. Now $ker(\psi) = (f)$ for some f since $k[x]$ is a principal ideal domain. Then, $k[x]/(f) \cong k[v]$ by the first isomorphism theorem. This implies (f) is prime (since $k[v]$ is an integral domain).

Now, if $f = 0$. Then $k[x] \cong k[v]$, so $L \cong k[x]$. However, by the second property in proposition 59, this cannot be true. Therefore, $f \neq 0$.

Given $f \neq 0$, we can assume f is monic. Then, (f) prime implies f is irreducible and (f) is a maximal ideal (since every non-zero prime ideal in a PID is a maximal ideal). This means, $k[v] \cong k[x]/(f)$ is a field. Therefore, $k[v] = k(v)$ (since the quotient field is the "smallest" field containing $k[v]$). Since $f(v) = 0$, so v is algebraic over k and so, by theorem 60, $L = k[v]$ is module-finite over k. This concludes the proof for $n = 1$.

Now, for the inductive step, assume true for $n - 1$ i.e $k[v_1, ..., v_{n-1}]$ is module-finite over k. Let $L = k_1[v_2, ..., v_n]$ where $k_1 = k(v_1)$. Then, by the inductive hypothesis, $k_1[v_2, \cdots, v_n]$ is module-finite over k_1.

We show that v_1 is algebraic over k which would say $k[v_1]$ is module-finite over k concluding the proof. Suppose, v_1 is not algebraic over k. Then, using the inductive hypothesis, for each $i = 2, ..., n$, we have an equation $v_i^{n_i} + a_{i1}v_i^{n_i-1} + \cdots = 0$ where $a_{ij} \in k_1$.

Let $a \in k[v_1]$ such that a is a multiple of all the denominators of $a_{ij} \in k(v_1)$. We get $av_i^{n_i} + aa_{i1}(av_1)^{n_i-1} + \cdots = 0$. Then, by corollary 61, for any $z \in L = k[v_1, \cdots, v_n]$, there exists N such that $a^N z$ is integral over $k[v_1]$ (since the set of integral elements forms a subring). Since this holds for any $z \in L$, this also holds for any $z \in k(v_1)$. But by theorem 65, this is impossible. This gives us the contradiction. $\square$

Theorem 67. (Nullstellensatz Version I) Assume k is algebraically closed. If I is a proper ideal in $k[x_1, ..., x_n]$, then $Z(I) \neq \emptyset$.

Proof. For any proper ideal I, there exists a maximal ideal J containing I. So, for simplicity, we assume I is the maximal ideal itself since $Z(J) \subset Z(I)$. Then, $L = k[x_1, \cdots, x_n]/I$ is a field (since I is maximal) and k is an algebraically closed subfield of L. Note that there is a ring-homomorphism from $k[x_1, ..., x_n]$ onto L by the natural projection. This means, L is ring-finite over k. Then, by theorem 66, L is module-finite over k. Then, by theorem 64, $L = k$ i.e $k = k[x_1, ..., x_n]/I$.

Now, since $k = L$, in particular this means $k \cong k[x_1, ..., x_n]/I$. Suppose $x_i \in k[x_1, ..., x_n]$ is mapped to a_i by the homormorphism ψ whose kernel is I. Then, $x_i - a_i$ is mapped to 0, so $x_i - a_i \in I$. Now, note that $(x_1 - a_1, ..., x_n - a_n)$ is a maximal ideal as one can easily verify and it contains I, so $I = (x_1 - a_1, ..., x_n - a_n)$. So, $(a_1, ..., a_n) \in Z(I)$. Therefore, $Z(I) \neq \emptyset$. □

The fact that every maximal ideal in the polynomial ring over n variables is of the form $(x_1 - a_1, ..., x_n - a_n)$ is a very important thing to remember. In fact, we will often use the fact that points in affine varieties correspond to maximal ideals made rigorous in the following:

Lemma 68. There is a natural bijection between a point $a \in \mathbb{A}^n$ and k-algebra homomorphisms $k[x_1, \cdots, x_n] \to k$. We say the point a corresponds to the maximal ideal defined by the kernel of this homomorphism.

Proof. Let $\phi : k[x_1, ..., x_n] \to k$ be a k-algebra homomorphism defined by $\phi(x_i) = a_i$, so $x_i - a_i \in ker(\phi)$. Now, $k[x_1, ..., x_n]/ker(\phi) \cong k$ so $ker(\phi)$ is a maximal ideal. □

We recall some definitions before moving to Hilbert's Nullstellensatz.

Definition 67. The <u>radical</u> of an ideal I in R is $\sqrt{I} := \{a \in R : a^n \in I, \text{for some } n \in \mathbb{Z}, n > 0\}$. It can be easily shown that $\sqrt{I}$ is an ideal itself and $I \subseteq \sqrt{I}$.

Definition 68. (Radical Ideal). The ideal I is called a radical ideal if $I = \sqrt{I}$.

Proposition 69. Let I be an ideal of a commutative ring R. Then,

$$\sqrt{I} = \bigcap_{\substack{p \text{ prime} \\ I \subseteq p \subsetneq R}} p.$$

We have two simple observations:

Lemma 70. For any ideal I in $k[x_1 ... x_n]$, $Z(I) = Z(\sqrt{I})$.

Proof. Note that $I \subseteq \sqrt{I}$ implies $Z(\sqrt{I}) \subseteq Z(I)$. Conversely, let $v \in Z(I)$ and let $f \in \sqrt{I}$. Then, $f^n \in I$ for some $n > 0$. This implies $f^n(v) = 0$ which implies $f(v) = 0$ as k has no zero divisor. Therefore, $v \in Z(\sqrt{I})$. □

Lemma 71. $\sqrt{I} \subset I(Z(I))$.

Proof. Suppose $s \in \sqrt{I}$. Then, $s^n \in I$ for some n. Now, let $v \in Z(I)$. Then, $s^n(v) = 0$ implies $s(v) = 0$, so $s \in I(Z(I))$. □

Now, we prove Hilbert's Nullstellensatz:

Theorem 72. (Hilbert's Nullstellensatz) Let I be an ideal in $k[x_1, ..., x_n]$ where k is algebraically closed. Then, $I(Z(I)) = \sqrt{I}$.

Proof. We already know $\sqrt{I} \subset I(Z(I))$. So, we only need to prove the other direction. Let $I = (f_1, ..., f_r)$ where $f_i \in k[x_1, ..., x_n]$. Suppose, $G \in I(Z(f_1, ..., f_r))$. Define $J := (f_1, ..., f_r, x_{n+1}G - 1) \subset k[x_1, ..., x_n, x_{n+1}]$. Then, $V(J) \subset \mathbb{A}^n_k$ is $\emptyset$ since G is 0 whenever all f_i are 0 and therefore, $x_{n+1}G - 1 \neq 0$ at those points.

Since $Z(J) = \emptyset$, J is not a proper ideal by Nullstellensatz version I. Therefore, $J = k[x_1, \cdots, x_{n+1}]$. So, $1 \in J$ (since J is not a proper ideal). So $1 = \sum_i a_i(x_1, ..., x_{n+1})f_i + b(x_1, .., x_{n+1})(x_{n+1}G - 1)$.

In particular, if $x_{n+1} = \frac{1}{G}$, then, $1 = \sum_i a_i f_i + b(1-1) = \sum_i a_i f_i$. Therefore, $G^N = G^N \sum_i a_i f_i$, so $G^N \in (I)$. Therefore, $G \in \sqrt{I}$. Therefore, $I(Z(I)) \subseteq \sqrt{I}$. □

This has a series of interesting applications.

Corollary 73. If I is a radical ideal in $k[x_1, ..., x_n]$, then $I(Z(I)) = I$. Therefore, there is a one-to-one correspondence between radical ideals and algebraic sets.

Corollary 74. For any subset $Y \subseteq \mathbb{A}^n$, $Z(I(Y)) = \bar{Y}$, the closure of Y.

Proof. We note that $Y \subseteq Z(I(Y))$ and since the latter is closed, $\bar{Y} \subseteq Z(I(Y))$. Conversely, let W be a closed set containing Y, so $W = Z(a)$ for some ideal $a \in k[x_1, \cdots, x_n]$. Then, $Y \subseteq Z(a) \implies I(Z(a)) \subseteq I(Y)$. Also $a \subseteq I(Z(a))$ so $Z(I(Y)) \subseteq Z(a) = W$, so $Z(I(Y)) \subseteq \bar{Y}$. So, $Z(I(Y)) = \bar{Y}$. □

Corollary 75. An algebraic set $Z(T)$ is irreducible if and only if $I(Z(T))$ is a prime ideal. There is a one-to-one correspondence between prime ideals and irreducible algebraic sets. The maximal ideals correspond to points.

Corollary 76. Let F be a non-constant polynomial in $k[x_1, \cdots, x_n]$ with the irreducible decomposition of F being $F = F_1^{n_1} F_2^{n_2} \cdots F_r^{n_r}$. Then, $V(F) = V(F_1) \cup \cdots \cup V(F_r)$ is the decomposition of $V(F)$ into irreducible components and $I(V(F)) = (F_1 \cdots F_r)$. Therefore, there is a one-to-one correspondence between irreducible polynomials $F \in k[x_1, \cdots, x_n]$ (up to multiplication by a non-zero element of k) and irreducible hypersurfaces in $\mathbb{A}^n_k$.

Corollary 77. Let I be an ideal in $k[x_1, \cdots, x_n]$. Then, $V(I)$ is a finite set if and only if $k[x_1, \cdots, x_n]/I$ is a finite dimensional vector space over k. If this occurs, then, the number of points in $V(I)$ is at most $dim_k(k[x_1, \cdots, x_n]/I)$.

Proof. Let $p_1, \cdots, p_r \in V(I)$. Choose $f_1, \cdots, f_r \in k[x_1, \cdots, x_n]$ such that $f_i(p_j) = 0$ if $i \neq j$ and $f_i(p_i) = 1$ and let $\bar{f_i}$ be the residue class of f_i. Now, if $\sum_i \lambda_i \bar{f_i} = 0$ with $\lambda_i \in k$, then, $\sum_i \lambda_i f_i \in I$. Therefore, $\lambda_j = (\sum_i \lambda_i f_i)(p_j) = 0$. Therefore, $\bar{f_i}$ are linearly independent over k. So $r \leq dim_k(k[x_1, \cdots, x_n]/I)$.

Conversely, suppose $V(I) = (p_1, \cdots, p_r)$ and so is finite. Let $p_i = (a_{1i}, \cdots, a_{1n})$ and define $f_j := \prod_{i=1}^{r}(x_j - a_{ij}), j = 1, \cdots, n$. Then, $f_j \in I(V(I))$, so for all j, $f_j^N \in I$ for some large enough $N > 0$. Now, taking I-residues, $\bar{f_j}^N = 0$. By expanding f_j^N, we get that $\bar{x_j}^{rN}$ is a k-linear combination of $\bar{1}, \bar{x_j}, \cdots, \bar{x_j}^{rN-1}$. So, for all s, $\bar{x_j}^s$ is a k-linear combination of $\bar{1}, \bar{x_j}, \cdots, \bar{x_j}^{rN-1}$. Therefore, the set $\{\bar{x_1}^{m_1}, \cdots, \bar{x_n}^{m_n} : m_i < rN\}$ generates $k[x_1, \cdots, x_n]/I$ as a vector space over k. $\square$

Definition 69. Reduced Rings. A ring R is called reduced if $f^N = 0 \in R$ implies $f = 0$.

Examples:
(1) $\mathbb{A}^n$ is irreducible since it corresponds to the zero ideal in $k[x_1, \cdots, x_n]$, which is prime.

Definition 70. (Affine Curve). Let f be an irreducible polynomial in $k[x, y]$. Since $k[x, y]$ is a UFD, f generates a prime ideal in $k[x, y]$. Then, the set $Z(f)$ is irreducible. $Z(f)$ is called the *affine curve* defined by the equation $f(x, y) = 0$. If f is of degree d, we say that $Z(f)$ is an affine curve of degree d.

Definition 71. (Surface and hypersurface). If f is an irreducible polynomial in $k[x_1, \cdots, x_n]$, then we call the affine variety $V(f)$ a surface when $n = 3$ and a hypersurface when $n > 3$.

Next, we find irreducible decompositions of algebraic sets of an affine space.

3.4 Irreducible Components of Algebraic Sets

So far, we have seen polynomials and the varieties defined over them. Now, we bring in topological invariants.

Definition 72. Irreducible decomposition of a set. Let $V \in \mathbb{A}_k^n$ be an algebraic set. Then, V is reducible if $V = V_1 \cup V_2$ where V_1, V_2 are non-empty, algebraic sets in $\mathbb{A}_k^n$ i.e $V_i \neq V$ for $i = 1, 2$. If V is not irreducible, we call it reducible.

Theorem 78. The algebraic set V is irreducible if and only if $I(V)$ is prime.

Proof. Suppose, V is irreducible. Now, suppose for contradiction, $I(V)$ is not prime. Therefore, by definition of prime, there exists $f_1 f_2 \in I(V)$ such that $f_1 \notin I(V)$ and $f_2 \notin I(V)$. Now, $V = (V \cap Z(f_1)) \cup (V \cap Z(f_2))$ and $V \cap Z(f_i) \subset V, V \cap Z(f_i) \neq V$; to see this, note that for any $p \in V$ such that p is a zero of $f_1 f_2$, p has to be a root of either f_1 or f_2 since f_i belong to an integral domain, therefore, $p \in (V \cap V(f_1)) \cup (V \cap V(f_2))$ (the other direction is obvious). Then, $V = (V \cap V(f_1)) \cup (V \cap V(f_2))$ is decomposition of V which means V is not irreducible - contradiction.

Conversely, suppose $I(V)$ is prime. For contradiction, suppose V is reducible with $V = V_1 \cup V_2$, V_i non-empty. Then, consider $f_i \in I(V_i)$ such that $f_i \notin I(V)$. Clearly, $f_1 f_2 \in I(V)$, so $I(V)$ is not prime - contradiction. $\square$

Corollary 79. The affine space $\mathbb{A}_k^n$ is irreducible if k is infinite.

Theorem 80. Let A be a non-empty collection of ideals in a Noetherian ring R. Then, A has a maximal ideal i.e an ideal I such that $I \in A$ and no other ideal in A contains I.

Proof. Given our collection of ideals, A, choose an ideal $I_0 \in A$. Then, define $A_1 = \{I \in A : I_0 \subsetneq I\}$ and $I_1 \in A_1$, $A_2 = \{I \in A : I_1 \subsetneq I\}$ and $I_2 \in A_2$ and so on. Then, the statement in the theorem is equivalent to saying that there exists positive integer n such that A_n is empty since that would mean there exists no ideal containing I_{n-1}. Suppose this is not true. Then, with $I := \cup_{n=0}^{\infty} I_n$, since R is Noetherian, therefore there exists $f_1, ..., f_m$ that generates the ideal I where each $f_i \in I_n$ for n sufficiently large. But since the generates are all in I_n, $I = I_n$ and so $I_{n'} = I_n$ for any $n' > n$ (since $I = \cup_{n=0}^{\infty} I_n$ by definition) - contradiction. $\square$

We finally prove the main result. Note that this is pretty closely tied to the Hilbert Basis Theorem which says that every algebraic set is the intersection of a finite number of algebraic sets/hypersurfaces:

Theorem 81. Let V be an algebraic set in $\mathbb{A}_k^n$. Then, there exists unique, irreducible algebraic sets $V_1, ..., V_r$ such that $V = V_1 \cup V_2 \cdots \cup V_r$ and $V_i \subsetneq V_j$ for any $i \neq j$.

Proof. Proving this statement is equivalent to disproving that $\mathcal{F}$ is non-empty where $\mathcal{F} := \{\text{algebraic set } V \in \mathbb{A}_k^n : V \text{is not the union of finitely many irreducible algebraic sets}\}$.

Suppose, $\mathcal{F}$ is not empty. Let $V \in \mathcal{F}$ such that V is the minimal member of $\mathcal{F}$ i.e V cannot be written as the union of sets in $\mathcal{F}$.

Now, since $V \in \mathcal{F}$, V is reducible (if V is irreducible, then it is trivially the union of 1 irreducible subsets). Since V is reducible, $V = V_1 \cup V_2$ where $V_i \neq \emptyset$. Since V is the minimal member of $\mathcal{F}$, $V_i \notin \mathcal{F}$. Since $V_i \notin \mathcal{F}$, it is the union of finitely many irreducible algebraic sets, so let $V_i = V_{i1} \cup V_{i2} \cdots \cup V_{im_i}$. Then, $V = \cup_{i,j} V_{ij}$, so $V \notin \mathcal{F}$. So, we have shown that V can be written as $V = V_1 \cup \cdots \cup V_m$ where each V_i is irreducible. First, remove any V_i such that $V_i \subset V_j$. Now we prove uniqueness. Suppose $V = W_1 \cup \cdots W_m$ be another such decomposition. Then, $V_i = \cup_j (W_j \cap V_i)$. Now, $W_j \cap V_i = V_i$ since otherwise we will have found a decomposition of the irreducible set V_i. Therefore, $V_i \subset W_{j(i)}$ for some $j(i)$. Similarly, by symmetry, $W_{j(i)} \subset V_k$ for some k. But then, $V_i \subset V_k$ implies $i = k$ and so $V_i = W_{j(i)}$. Continuing this for each $i \in \{1, ..., m\}$, we get that the two decompositions are equal. □

Furthermore, we use the following terms:

Definition 73. An ideal $I \subset k[x_1, ..., x_n]$ set-theoretically defines a variety V if $V = Z(I)$. An ideal $J \subset \mathbb{A}^n$ scheme-theoretically defines a variety V if $J = I(V)$.

Here's a pretty straightforward result:

Theorem 82. For an affine variety X, if $f_1, ..., f_m$ scheme-theoretically define X, then $Z(I(X)) = X$

Two affine-varities can be isomorphic in the usual sense using the language of polynomial maps:

Definition 74. Isomorphic affine varieties. Two affine varieties $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ are isomorphic if there exists polynomial maps $f : V \to W$ and $g : W \to V$ such that $f \circ g = g \circ f = i_d$.

Theorem 83. Let f and g be two polynomials in $k[x, y]$ with no common factors. Then, $Z(f, g)$ is a finite set of points.

Proof. Check [1]. □

3.5 Coordinate Rings

Definition 75. (Coordinate Ring). If $Y \subseteq \mathbb{A}^n$ is an affine algebraic set, then we define the affine coordinate ring, $A(Y)$, of Y to be $k[x_1, \cdots, x_n]/I(Y)$.

Note that if Y is an affine variety, then $I(Y)$ is prime and so $A(Y)$ is an integral domain.

Definition 76. k-algebra. Let k be a field (i.e a commutative division ring). A ring R is a k-algebra if $k \subseteq Z(R) := \{x \in R : xy = yx, \forall y \in R\}$ and the identity of k is the same as the identity of R.

Note, $Z(R)$ is the center of the ring R.

Definition 77. Finitely generated k-algebra. A finitely generated k-algebra is a ring that is isomorphic to a quotient of a polynomial ring $k[x_1, ..., x_n]/I$.

Equivalently, a ring R is a finitely-generated k-algebra if R is generated as a ring by k with some finite set $r_1, ..., r_n$ of elements of R i.e $k[r_1, ..., r_n]$.

These definitions are equivalent. Suppose, R is a finitely generated k-algebra i.e $R = k[r_1, ..., r_n]$. Then, define a ring homomorphism that sends x_i to r_i. Since R is generated by r_i, this map is surjective and by quotienting over the kernel, we get the isomorphism $R \cong k[x_1, \cdots, x_n]$. Conversely, suppose $R \cong k[r_1, .., r_n]/I$. Then, let $\varphi : k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]/I = R$. Then, R is generated by the images of $x_1, \dots, x_n$ under φ. Let the images be $r_1, \dots, r_n$ and as such $R = k[r_1, \dots, r_n]$.

Example: Any finitely generated k-algebra which is an integral domain is the affine coordinate ring of some affine variety. This is because if B is such a finitely generated k-algebra, then $B \cong k[x_1, \dots, x_n]/I$ and then the corresponding affine variety is $Z(I)$.

3.6 Dimension of Affine Varieties

First, we define a notion of dimension on a topological space:

Definition 78. (Dimension of a topological space). Let X be a topological space. Then, the dimension of X is defined to be the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ of distinct irreducible closed subsets of X.

Definition 79. (Dimension of an affine and quasi-affine variety). Let X be an affine variety or quasi-affine variety. Then, the dimension of X is defined to be the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ of distinct irreducible closed subsets of X. So,

$$dim(X) := \sup\{n \in \mathbb{Z} \mid \exists X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n \subsetneq X, X_i \text{ irreducible closed subsets of } X\}.$$

Example: $dim(\mathbb{A}^1) = 1$ as the only irreducible closed subsets of X are single points and the whole space $\mathbb{A}^1$.

Definition 80. (Height of a prime ideal). In a ring A, the height of a prime ideal I is the supremum of integers n such that there exists a chain $I_0 \subset I_1 \subset \cdots \subset I_n = I$ of distinct prime ideals.

Definition 81. (Krull Dimension of a ring A). The Krull dimension of a ring A is the supremum of the heights of all prime ideals.

Proposition 84. Let Y be an affine algebraic set. Then, the dimension of Y is equal to the dimension of its affine coordinate ring $A(Y)$.

Proof. The closed irreducible subsets of Y correspond to prime ideals of $k[x_1, .., x_n]$ containing $I(Y)$. These correspond to prime ideals of $A(Y)$. Thus, dim Y is the length of the longest chain of prime ideals of $A(Y)$, which is its Krull dimension. $\square$

We need the following definitions to bring in some results from noetherian rings.

Definition 82. (Algebraic vs transcendental elements). Suppose L is a field extension of K (i.e. K is a subfield of L that is not equal to L). Denote this by writing L/K. An element $a \in L$ is algebraic over K if there exists a polynomial $p(x)$ in $K[x]$ s.t. $p(a) = 0$. Otherwise, we say a is transcendental over K.

Definition 83. (Algebraically independent over K). Let L/K be a field extension. Then, the set of elements of $a_1, \cdots, a_n \in L$ are algebraically independent over K if there exists no polynomial $p(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$ s.t. $p(a_1, \cdots, a_n) = 0$.

Definition 84. (Transcendence degree of a field extension L/K). The transcendence degree of a field extension L/K, denoted $tr.deg(L/K)$ is the maximum number of elements in L that are algebraically independent over K.

Proposition 85. Let k be a field. Let B be an integral domain which is a finitely generated k-algebra. Then,
(1) The dimension of B is equal to the transcendence degree of the quotient field $K(B)$ (i.e. the field of fractions) of B over k.
(2) For any prime ideal I in B, we have

$$\text{height } I + \dim B/I = \dim B.$$

We apply this as follows:

Theorem 86. The dimension of $\mathbb{A}^n$ is n.

Proof. Dimension of $\mathbb{A}^n$ is equal to the dimension of $A(\mathbb{A}^n) = k[x_1, \cdots, x_n]$. By the previous proposition's part (a), this is equal to $tr.deg(k(x_1, ..., x_n)/k)$. This is equal to n because for the variables $x_1, ..., x_n$, if there is any polynomial $p(x_1, \cdots, x_n) = 0$, then $p = 0$. There is no larger set of elements for which this is true - if we choose $T_1, \cdots, T_n, T_{n+1}$, then we can define the polynomial $p(T_1, \cdots, T_n, T_{n+1}) = f(T_1, \cdots, T_n) - T_{n+1}$ where $f(T_1, \cdots, T_n) = T_{n+1}$ and then p is 0 at $(T_1, \cdots, T_n, T_{n+1})$. $\square$

Proposition 87. If Y is a quasi-affine variety, then $\dim Y = \dim \bar{Y}$.

Theorem 88. Let A be a noetherian ring and let $f \in A$ be an element which is not a zero divisor nor a unit. Then, every minimal prime ideal p containing f has height 1.

Proposition 89. A noetherian integral domain A is a unique factorization domain if and only if every prime ideal of height 1 is principal.

Lastly, we have

Proposition 90. A variety Y in $\mathbb{A}^n$ has dimension $n-1$ if and only if it is the zero set $Z(f)$ of a single nonconstant irreducible polynomial in $k[x_1, \cdots, x_n]$.

4 Projective Varieties

4.1 Graded rings, homogenous ideals and projective varieties.

Definition 85. (Projective n-space). Let k be an algebraically closed field. The projective n-space over k, denoted $\mathbb{P}^n_k$ or $\mathbb{P}^n$, is the set of equivalence classes of $n+1$-tuples $a_0, \cdots, a_n$ of elements of k, not all zero, under the equivalence relation given by $(a_0, \cdots, a_n) \sim (\lambda a_0, \cdots, \lambda a_n)$ for all non-zero $\lambda \in k$.

An element of $\mathbb{P}^n$ is called a point. If P is a point, then any $(n+1)$-tuple $(a_0, \cdots, a_n)$ in the equivalence class of P is called a set of homogenous coordinates for P.

We will require a few constructions from algebra now.

Definition 86. (Graded Ring). A graded ring is a ring S with the decomposition $S = \oplus_{d \geq 0} S_d$ of S into a direct sum of *abelian groups* S_d such that for any $d, e \geq 0$, $S_d \cdot S_e \subseteq S_{d+e}$.

Definition 87. (Homogenous element of degree d or forms of degree d). An element of S_d in a graded ring $S = \oplus_{d \geq 0} S_d$ is called a homogenous element of degree d.

Any element of S can be written, uniquely, as a finite sum of homogenous elements.

Definition 88. (Homogenous ideals). An ideal $I \subseteq S$ is called a homogenous ideal if $I = \oplus_{d \geq 0}(I \cap S_d)$.

Proposition 91. An ideal I is homogenous if and only if it can be generated by homogenous elements

Proof. Let I be a homogenous ideal i.e. $I = \oplus_{d \geq 0}(I \cap S_d)$. Then, consider $f \in I$, which we can write as $f = f_0 + f_1 + f_2 + \cdots$ where each f_i is a homogenous element. Then, the ideal I is generated by these homogenous elements that constitute each element of I. Conversely, suppose I is generated by homogenous elements $f_1, f_2, \cdots$. Then, clearly any arbitrary element of I can be written as $a_1 f_1 + a_2 f_2 + \cdots$ where $a_i \in S$. Write each a_i as a sum of homogenous elements and we see that $I = \oplus_{d \geq 0}(I \cap S_d)$. ☐

Proposition 92. The sum, product, intersection and radical of homogenous ideals are homogenous.

Proposition 93. A homogenous ideal I is prime if, for any two *homogenous elements* f, g s.t. $fg \in I$, we have that $f \in I$ or $g \in I$.

Now, we come back to the polynomial ring. For a polynomial ring $S := k[x_1, \cdots, x_n]$, we can construct it as a graded ring by letting S_d be the set of all linear combinations of monomials (or forms) of degree d in $x_0, \cdots, x_n$.

Why do we care about homogenous polynomials? If f is a homogenous polynomial of degree d, then $f(\lambda a_0, \cdots, \lambda a_n) = \lambda^d f(a_0, \cdots, a_n)$. This means whether the polynomial is 0 or not depends only on the *equivalence class of* $(a_0, \cdots, a_n)$. Therefore, f defines a function from $\mathbb{P}^n$ to $\{0, 1\}$ by $f(P) = 0$ if $f(a_0, \cdots, a_n) = 0$ and $f(P) = 1$ if $f(a_0, \cdots, a_n) \neq 0$.

Lemma 94. (1) For any polynomial $f \in k[x_0, \cdots, x_n]$, f can be written as $f_0 + f_1 + \cdots + f_r$, where f_i is a homogenous polynomial/form of degree i and $r = deg(f)$.
(2) If $f(p) = 0$, then $f_i(p) = 0$ for any homogenous coordinates of p.

Proof. (1) is obvious from just writing f as a sum of monomials. We prove (2). Suppose $f(p) = 0$. Then, $f(\lambda p) = 0$ for $\lambda \neq 0$. But $f(\lambda p) = \sum_i \lambda^i f_i(p)$. Now since $f(\lambda p) = 0$ for all $\lambda \neq 0$. Let $\varphi(\lambda) = f(\lambda p) = \sum_i \lambda^i f_i(p)$. We see then that φ has infinitely many zeros which is possible if and only if φ is the zero polynomial i.e $f_i(p) = 0$ for all i. □

Definition 89. (Zero set of a set of homogenous polynomials). The zeros of a homoygenous polynomial is $Z(f) = \{P \in \mathbb{P}^n | f(P) = 0\}$. If T is any set of homogenous elements of $k[x_1, \cdots, x_n]$, we define the zero set of T to be $Z(T) = \{P \in \mathbb{P}^n | f(P) = 0, \forall f \in T\}$.

If I is a homogenous ideal of $k[x_1, \cdots, x_n]$, we define $Z(I) = Z(T)$ where T is the set of all homogenous elements in I. Since $k[x_1, \cdots, x_n]$ is a Noetherian ring, any set of homogenous elements T has a finite subset $f_1, \cdots, f_r$ such that $Z(T) = Z(f_1, \cdots, f_r)$.

Definition 90. (Algebraic Set). A subset Y of $\mathbb{P}^n$ is an algebraic set if there exists a set T of homogenous elements of $k[x_1, \cdots, x_n]$ such that $Y = Z(T)$.

In particular, if f is a *linear homogenous polynomial,* then $Z(f)$ is called a hyperplane.

Once again, we have that the union of finitely many algebraic sets is an algebraic set, intersection of any family of algebraic sets is an algebraic set, the empty set and all of $\mathbb{P}^n$ are algebraic sets.

Definition 91. (Zariski topology on $\mathbb{P}^n$). The Zariski topology on $\mathbb{P}^n$ is defined by letting the closed sets be algebraic sets in $\mathbb{P}^n$.

Definition 92. (Projective algebraic variety and quasi-projective variety). A projective algebraic variety is an irreducible algebraic set in $\mathbb{P}^n$. An open subset of a projective variety is called a quasi-projective variety.

Definition 93. (Homogenous ideal). If Y is any subset of $\mathbb{P}^n$, we define the homogenous ideal of Y in $k[x_1, \cdots, x_n]$, denoted $I(Y)$, to be the ideal *generated by*

$$\{f \in S | f \text{ is homogenous and } f(P) = 0, \forall P \in Y\}.$$

Definition 94. (Homogenous coordinate ring). If Y is an algebraic set, we define the homogenous coordinate ring of Y is (with $I(Y)$ the homogenous ideal of Y)

$$S(Y) = k[x_1, \cdots, x_n]/I(Y).$$

Definition 95. (H_i and U_i). We denote the zero set of x_i to be H_i for $i = 0, ..., n$. We define the open set $U_I := \mathbb{P}^n - H_i$ i.e.

$$U_i := \{[x_0 : \cdots : x_n] \in \mathbb{P}^n | x_i \neq 0\}.$$

Open cover of $\mathbb{P}^n$: We now have an open cover of $\mathbb{P}^n$ by the open sets U_i, for $i = 0, \cdots, n$.

Map to affine n-space. We now define the map $\varphi_i : U_i \to \mathbb{A}^n$ such that if $P = (a_0, ..., a_n) \in U_i$, then $\varphi_i(P) = Q$ where Q is the point with affine coordinates

$$\left(\frac{a_0}{a_i}, \cdots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \cdots, \frac{a_n}{a_i}\right).$$

Proposition 95. The map $\varphi_i : U_i \to \mathbb{A}^n$ is a homeomorphism of U_i with its induced topology to $\mathbb{A}^n$ with its Zariski topology.

Proof. One can easily check that φ is bijective. We now show that the map takes closed sets to closed sets. Consider φ_0. We define the map $\alpha : S^h \to k[y_1, \cdots, y_n]$ where S^h is the set of homogenous elements of $k[x_0, \cdots, x_n]$ and the map $\beta : k[y_1, \cdots, y_n] \to S^h$. Let $f \in S^h$, then $\alpha(f) = f(1, y_1, \cdots, y_n)$. On the other hand, for $g \in k[y_1, \cdots, y_n]$ of degree e, we let $\beta(g) = x_0^e g(x_1/x_0, \cdots, x_n/x_0)$. Let $Y \subseteq U$ be a closed subset. Let $\bar{Y}$ be the closure in $\mathbb{P}^n$. Since this is a closed set, this is an algebraic set and so $\bar{Y} = Z(T)$ for some $T \subseteq S^h$. Define $T' := \alpha(T)$. One can check that $\varphi(Y) = Z(T')$. Conversely, let W be a closed subset of $\mathbb{A}^n$. Then, $W = Z(T')$ for some subset T' of $k[y_1, \cdots, y_n]$ and $\varphi^{-1}(W) = Z(\beta(T')) \cap U$. Thus, φ and φ^{-1} are both closed maps, so φ is a homeomorphism. □

We will require some of these constructions in the proof, so we standardize them:

Definition 96. (Homogenization and dehomogenization). For any polynomial $g \in k[x_1, \cdots, x_n]$ of degree $deg(g)$, the homogenization of g is $\beta(g) = x_0^{deg(g)} g(x_1/x_0, \cdots, x_n/x_0)$. On the other hand, for any homogenous polynomial/form $f \in k[x_0, \cdots, x_n]$, the dehomogenization is the polynomial $\alpha(f) = f(1, x_1, \cdots, x_n) \in k[x_1, \cdots, x_n]$.

Corollary 96. If Y is a projective (respectively, quasi-projective) variety, then Y is covered by the open sets $Y \cap U_i$, $i = 0, \cdots, n$ which are homeomorphic to affine (respectively, quasi-affine) varieties via the mapping φ_i defined above.

4.2 Projective Nullstellensatz

Theorem 97. (Projective Nullstellensatz).
Let I be a homogenous ideal in $k[x_0, \cdots, x_n]$. Then:
(1) $Z(I) = \emptyset$ if and only if there exists an integer N such that I contains all homogenous polynomials/forms of degree $\geq N$.
(2) If $Z(I) \neq \emptyset$, then $I(Z(I)) = \sqrt{I}$.

Alternatively, we can phrase this as:

Theorem 98. (Homogenous Nullstellensatz). if $I \subseteq k[x_0, \cdots, x_n]$ is a homogenous ideal and if $f \in k[x_0, \cdots, x_n]$ is a homogenous polynomial/form with $deg(f) > 0$ such that $f(p) = 0$ for all $p \in Z(I)$ in $\mathbb{P}^n$, then $f^q \in I$ for some $q > 0$.

4.3 Preliminary properties

We now look at some immediate properties.

Theorem 99. For a homogenous ideal $I \subseteq k[x_0, \cdots, x_n]$, the following are equivalent:
(1) $Z(I) = \emptyset$
(2) $\sqrt{I} =$ either S or the ideal $S_+ = \oplus_{d>0} S_d$
(3) $S_d \subseteq a$ for some $d > 0$.

Proof. (1) implies (2): Suppose $Z(I) = \emptyset$. Consider the affine algebraic set of this ideal: $Z_a(I) = \{x \in \mathbb{A}^{n+1} | f(x) = 0, \forall f \in I\}$. Consider any $x \in Z_a(I)$ such that $x \neq 0$. Since I is a homogenous ideal and $Z(I) = \emptyset$ such an x does not exist. Thus, $Z_a(I)$ is either the emptyset or $\{0\}$. In the former case, $\sqrt{I} = S$. In the latter case, $\sqrt{I} = I(Z(I)) = I(\{0\}) = S_+$.

(2) implies (3): Suppose $\sqrt{I} = k[x_0, \cdots, x_n]$. Then, for all $f \in k[x_0, \cdots, x_n]$, $f^q \in I$ for some $q > 0$. Then, $x_i^{q_i} \in I$ for some $q_i > 0$ for each i. Let $r := q_0 + \cdots + q_n$. Then, we claim $S_r \subseteq I$. This is because if $x_0^{s_0} \cdots x_n^{s_n} \in S_r$, then at least one $s_i \geq q_i$ and so $x_0^{s_0} \cdots x_n^{s_n} \in I$. The proof for $\sqrt{I} = S_+$ is similar.

(3) implies (1). Suppose $S_d \subseteq I$ for some $d > 0$. Then $Z(I) \subseteq Z(S_d)$. If $s = (s_0, \cdots, s_n) \in Z(I)$, then there is at least one $s_i \neq 0$. but $x_i^d \in S_d \in I$ while clearly x_i^d does not vanish at $s \in Z(I)$. So $Z(I) = \emptyset$. $\square$

Theorem 100. If $T_1 \subseteq T_2$ are subsets of S^h (the set of homogenous polynomials in $k[x_0, \cdots, x_n]$, then $Z(T_1) \subseteq Z(T_2)$. If $Y_1 \subseteq Y_2$ are subsets of $\mathbb{P}^n$, then $I(Y_1) \subseteq I(Y_2)$. Furthermore $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.

Theorem 101. $\mathbb{P}^n$ is a Noetherian topological space i.e. a decreasing chain of closed sets in $\mathbb{P}^n$ must stabilize.

Proof. The proof following from the fact that $k[x_0, \cdots, x_n]$ is a Noetherian ring and that $I(Y_1) \subseteq I(Y_2)$ if $Y_2 \subseteq Y_2$. $\square$

Proposition 102. Every algebraic set in $\mathbb{P}^n$ can be written uniquely as a finite union of irreducible algebraic sets that do not contain one another. An algebraic set Y in $\mathbb{P}^n$ is irreducible if and only if $I(Y)$ is a prime ideal.

4.4 Segre Embedding

We now look at a construction that will become important later on.

Definition 97. (Segre Embedding). Let $\psi : \mathbb{P}^r \times \mathbb{P}^s \to \mathbb{P}^N$, where $N = rs + r + s$, such that ψ maps $((a_0, \cdots, a_r), (b_0, \cdots, b_s))$ to $(a_0b_0, \cdots, a_ib_j, \cdots, a_rb_s)$ in a lexicographic order. Then, ψ is well-defined and injective and is called the Segre Embedding.

Proposition 103. The image of Segre embedding is a subvariety of $\mathbb{P}^n$.

Proof. We explicitly construct the ideal whose algebraic set is the image of this embedding. Denote the homogenous coordinates of $\mathbb{P}^N$ by $(z_{00}, \cdots, z_{rs})$. Define

$$\gamma : k[z_{00}, \cdots, z_{rs}] \to k[x_0, \cdots, x_r, y_0, \cdots, y_s]$$

by

$$\gamma(z_i j) = x_i y_j.$$

Now, define $I = \ker(\gamma)$. Note that I is generated by polynomials of the form $z_{ij}z_{kl} - z_{il}z_{kj}$ for $i, k \in \{0, \cdots, r\}$ and $j, l \in \{0, \cdots, s\}$. This is because $\gamma(z_{ij}z_{kl} - z_{il}z_{kj}) = x_i y_j x_k y_l - x_i y_l x_k y_j = 0$.

We claim $Z(I) = \mathrm{Im}(\psi)$. First, we show $Z(I) \subset \mathrm{Im}(\psi)$. Let $p \in Z(I)$ and denote it by $p = (p_{00}, \cdots, p_{ij}, \cdots, p_{rs})$. Since all its coordinates cannot be 0 (it is in $\mathbb{P}^N$) afterall), let $p_{ij} \neq 0$. First, we show how to determine all the other coordinates of p using $\{p_{0j}, \cdots, p_{rj}, p_{i0}, \cdots, p_{is}\}$. This can be done by simply noting that, for all k and l, $p_{ij}p_{kl} - p_{il}p_{kj} = 0$ implies $p_{kl} = \frac{p_{il}p_{kj}}{p_{ij}}$. As such,

$$\psi\left((p_{0j}, \cdots, p_{rj}), \left(\frac{p_{i0}}{p_{ij}}, \cdots, \frac{p_{is}}{p_{ij}}\right)\right) = (p_{00}, \cdots, p_{rs}) = p.$$

Next, we show $\mathrm{Im}(\psi) \subset Z(I)$. This is straightforward - if $(a_0b_0, \cdots, a_rb_s) \in \mathrm{Im}(\psi)$. But then, at these coordinates, polynomials in I are all 0 and so we are done. $\square$

Now, one can easily show the following:

Proposition 104. Let $X \subseteq \mathbb{P}^n$ and $Y \subseteq \mathbb{P}^m$ be two quasi-projective varieties. Then, $X \times Y \subseteq \mathbb{P}^n \times \mathbb{P}^m$ is a quasi-projective variety. If X and Y are both projective, then $X \times Y$ is projective.

5 Morphisms

5.1 Regular functions and morphisms

Definition 98. (Regular functions on a quasi-affine variety). Let Y be a quasi-affine variety in $\mathbb{A}^n$ (i.e., Y is an open subset of an affine variety). A function $f : Y \to k$ is regular at point $p \in Y$ if there exists an open neighbourhood of p, $U \subseteq Y$, and polynomials $g, h \in k[x_1, \cdots, x_n]$ such that $h(x) \neq 0$ for any $x \in U$ and $f = \frac{g}{h}$ on U. We say f is regular on Y if it is regular at every point of Y.

Definition 99. (Regular functions on a quasi-projective variety). Let Y be a quasi-projective variety in $\mathbb{P}^n$ (i.e. Y is an open subset of a projective variety). A function $f : Y \to k$ is regular at point $p \in Y$ if there exists an open neighbourhood of p, $U \subseteq Y$, and *homogenous* polynomials $g, h \in k[x_0, \cdots, x_n]$ of the *same degree* such that $h(x) \neq 0$ for any $x \in U$ and $f = \frac{g}{h}$ on U. We say f is regular on Y if it is regular at every point of Y.

Lemma 105. A regular function (on both quasi-affine and quasi-projective varieties) is continuous (letting k be $\mathbb{A}^1_k$ in Zariski topology).

Proof. A closed set in $\mathbb{A}^1_k$ is a finite set of points. So, we show $f^{-1}(a)$ is closed for $a \in \mathbb{A}^1_k$. Suppose $f = \frac{g}{h}$ on U as in the definition of regular functions. Then, $f^{-1}(a) \cap U = Z(g - ah) \cup U$ - because $f(x) = g(x)/h(x) = a$ implies $(g - ah)(x) = 0$. Thus, $f^{-1}(a) \cap U$ is closed and so $f^{-1}(a)$ is closed. The proof for the case of quasi-projective varieties is similar. $\square$

So far, we have looked at functions that take elements of a quasi-affine/quasi-projective variety to the field k. Next, we look at functions from one variety to another.

Definition 100. (Variety). Let k be an algebraically closed field. A variety over k is any affine/quasi-affine/projective/quasi-projective variety.

Definition 101. (Morphism). Let X and Y be two varieties. Then, a morphism $\varphi : X \to Y$ is a *continuous map* such that for any open set $V \subseteq Y$ and for any regular function $f : V \to k$, the function $(f \circ \varphi) : \varphi^{-1}(V) \to k$ is a regular function.

Definition 102. (Pullback). With the set-up as in the definition of morphisms, the function $\varphi^*(f) = f \circ \varphi$ is called the pullback. So, $\varphi^* : \mathcal{O}(Y) \to \mathcal{O}(X)$.

Definition 103. (Isomorphism). An isomorphism is a morphism $\varphi : X \to Y$ such that there exists a morphism $\psi : Y \to X$ with $\varphi \circ \psi = \mathrm{id}_Y$ and $\psi \circ \varphi = \mathrm{id}_X$.

A composition of morphisms is a morphism and a composition of isomorphisms is an isomorphism.

5.2 Ring of regular functions, local ring of a point and function field.

Definition 104. (Ring of regular functions). Let Y be a variety. Then, $\mathcal{O}(Y)$ is the ring of regular functions on Y.

While $\mathcal{O}(Y)$ consists of functions that are regular on all of Y, we can look at just the functions that are regular at p.

Definition 105. (Local ring of p). Let Y be a variety and let $p \in Y$ be a point. The local ring of p on Y is the ring of germs of regular functions near p:

$$\mathcal{O}(p) := \{(U, f) | p \in U, U \text{ is open, } f \text{ is regular on } U, \text{ and } (U, f) \sim (V, g) \text{ if } f = g \text{ on } U \cap V\}.$$

Lastly, we define the function field:

Definition 106. (Function field and rational functions). Let Y be a variety. The *function field* $K(Y)$ of Y is

$$K(Y) := \{(U, f) | U \subseteq Y \text{ open, } f \text{ regular on } U, \text{ and } (U, f) \sim (V, g) \text{ if } f = g \text{ on } U \cap V\}.$$

The elements of $K(Y)$ are called *rational functions* on Y.

The function field $K(Y)$ is a field. The operations are defined as $(U, f) + (V, g) = (U \cap V, f + g)$ and $(U, f) \cdot (V, g) = (U \cap V, fg)$. Also, for any element (U, f), there exists a multiplicative inverse with $V = U - (U \cap Z(f))$ and then, $(V, \frac{1}{f})$ is the inverse.

The following propositions motivate the emphasis on intersections of open sets to define equivalence:

Proposition 106. Let Y be a variety. Then, for any open subsets U and V of Y, we have $U \cap V \neq \emptyset$.

Proof. Y is irreducible but if $U \cap V$ is empty, then $Y = (U \cap V)^C = U^C \cup V^C$ is a decomposition into algebraic sets. □

Proposition 107. Let f and g be regular functions on a variety X and if $f = g$ on some non-empty open subset U of X, then $f = g$ on all of X.

Proof. Let $U = Z(f - g)$. Then, U is closed since it is an algebraic set. Also U is dense. This is because X is irreducible, U is defined to be open (and suppose U is non-empty), so $U^C \subsetneq X$ is closed. Then, $X = U \cup U^C$ is a decomposition. But X is irreducible so U must be equal to all of X. □

5.3 Preliminary properties

Proposition 108. There exists the natural, injective maps

$$\mathcal{O}(Y) \to \mathcal{O}_p \to K(Y)$$

and so we treat $\mathcal{O}(Y$ and $\mathcal{O}_p$ as subrings of $K(Y)$.

Proof. The maps are natural and the injectivity follows from Proposition 107. □

Now, we recall an important construction from algebra:

Definition 107. (Localization). Let A be a ring. A multiplicative subset $S \subseteq A$ is a subset that is closed under multiplication and $1 \in S$. Then, define $S^{-1}A = \{a/s \mid a \in A, s \in S, s \neq 0\}/\sim$ where the equivalent relation is $a_1/s_1 = a_2/s_2$ if there exists $s \in S$ such that $s(s_2a_1 - s_1a_2) = 0$. The operations of addition and multiplication are similar to the ones for rational numbers.

Here are some important localizations:
(1) Let p be a prime ideal and let $S = A - p$. Then,

$$A_p = S^{-1}A.$$

(2) Given A an integral domain and $S = A - \{0\}$, the *fractional field* of A is

$$K(A) = S^{-1}(A).$$

(3) Given $S = \{1, f, f^2, \cdots\}$ where $f \in A$, define

$$A_f = S^{-1}A.$$

We will requite the following example in particular:

Definition 108. (Localization of a graded ring). Let A be a graded ring and let p be a prime homogenous ideal in A. Then, $A_{(p)}$ is the subring of *degree 0* elements in the localization, $S^{-1}A$, of A w.r.t the $S = A - p$ of homogenous elements. So,

$$A_{(p)} = \{f/g \mid f \in A, g \in A - p, g \text{ homogenous}, deg(f) = deg(g)\}.$$

If A is an integral domain, then for $p = (0)$, we get the *field* $S_{((0))}$. If $f \in A$ is a homogenous element, then $A_{(f)}$ is the subring of elements of degree 0 in the localized ring $A_f = T^{-1}A$ where $T = \{1, f, f^2, ..\}$.

Now, we look at some relationships between these constructions in the affine space.

Theorem 109. Let $Y \subseteq \mathbb{A}^n$ be an affine variety with the affine coordinate ring $A(Y) = k[x_1, \cdots, x_n]/I(Y)$. Then,
(1) $\mathcal{O}(Y) \cong A(Y)$.
(2) For each point $p \in Y$, define the ideal $m_p \subseteq A(Y)$ of functions vanishing at p i.e.

$$m_p := \{f \in A(Y) | f(p) = 0\}.$$

Then, there exists a 1-1 correspondence between the points of Y and the maximal ideals of $A(Y)$.
(3) For each point $p \in Y$, $\mathcal{O}_p \cong A(Y)_{m_p}$ and $dim(\mathcal{O}_p) = dim(Y)$.
(4) $K(Y)$ is isomorphic to the quotient field of $A(Y)$ and, so, $K(Y$ is a finitely generated field extension of k.

Proof. Define $\alpha : A(Y) \to \mathcal{O}(Y)$. Then, α is an injective homomorphism as $k[x_1, \cdots, x_n] \to \mathcal{O}(Y)$ is a homomorphism and its kernel is $I(Y)$. We need to show that the map is surjective. Before we do so, we prove (2) and (3).

We proved (2) when we proved Hilbert's Nullstellensatz.

Now, for (3), for each $p \in Y$, there exists a natural map $i : A(Y)_{m_p} = S^{-1}A(Y) \to \mathcal{O}_p$ (where $S = A(Y) - m_p$), because $A(Y)_{m_p}$ consists of functions $f = \frac{g}{h}$ such that h does not vanish at p. Note that i is an injective map. Also, i is a surjective map: for any function $f \in \mathcal{O}_p$ that is regular on U containing p, we can write it as an element in $A(Y)_{m_p}$. The map is of course a homomorphism which allows us to conclude $A(Y)_{m_p} \cong \mathcal{O}_p$. Now, $dim(\mathcal{O}_p = \text{height} m_p$. But m_p is maximal and so $A(Y)/m_p \cong k$. Therefore, $dim(\mathcal{O}_p) = dim(Y)$.

Now, we prove (1). Note that $\mathcal{O}(Y) \subseteq \cap_{p \in Y} \mathcal{O}_p$ since a regular function is regular at every point in Y. Also, note that $A(Y) \subseteq \mathcal{O}(Y)$ since every function $f \in A(Y)$ can be expressed as $f = \frac{f}{/}1$ and thus a regular function in $\mathcal{O}(Y)$. Also note $\mathcal{O}(Y) \subseteq \cap_m A(Y)_m$ where m runs over all the maximal ideals of $A(Y)$, because $\mathcal{O}(Y) \subseteq \cap_{p \in Y} \mathcal{O}_p = \cap_m A(Y)_m$ by (3) and using the fact that points are in direct 1-1 correspondence with maximal ideals. So, we have

$$A(Y) \subseteq \mathcal{O}(Y) \subseteq \cap_m A(Y)_m.$$

Claim: If B is an integral domain, then B is equal to the intersection of its localizations at all maximal ideals i.e. $B = \cap_m B_m$.

Proof of claim: $B \subseteq \cap_m B_m$ because each $b \in B$ can be represented as $b/1$ and $1 \notin m$ for any maximal ideal m. Also $\cap_m B_m \subseteq B$. Suppose $x \in B_m$ for every maximal ideal m. Then, write $x = b/s$ for $s \neq 0$, and $b, s \in B$. Note that $s \notin m$ for any maximal ideal m and so, s must be a unit and thus, $x = bs^{-1}$ is an element of B.

Then, using this claim, $A(Y) = \cap_m A(Y)_m$ and so $A(Y) \cong \mathcal{O}(Y)$. $\square$

Next, we show that $U_i \subset \mathbb{P}^n$ is isomorphic to $\mathbb{A}^n$. We previously only showed that they are homeomorphic.

Proposition 110. Let $U_i \subset \mathbb{P}^n$ be the open sets $U_i = \{(x_0, \cdots, x_n) \in \mathbb{P}^n \mid x_i \neq 0\}$. Then, the mapping $\varphi : U_i \to \mathbb{A}^n$ defined by $\varphi(x_0, \cdots, x_n) = (\frac{x_0}{x_i}, \cdots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \cdots, \frac{x_n}{x_i})$ is an isomorphism of varieties.

Proof. We already know it is bijective since we previously showed that this map is a homeomorphism. So, now we need to show the pullback of any regular function is regular (as per the definition of morphisms).

For simplicity, consider $i = 0$.

Consider a regular function on an open set in $V \subseteq \mathbb{A}^n$. Then, for any $(x_1, ..., x_n) \in V$, we can find $(1, x_0, \cdots, x_n) \in \mathbb{P}^n$ and then, $f \circ \varphi$ is regular on $\varphi^{-1}(V)$.

On the other hand, consider a regular function f on open set $V \subseteq \mathbb{P}^n$. Note that $f = g/h$ where g and h are homogenous of the same degree. Then, $(x_0, \cdots, x_n)$ is mapped to $(\frac{x_0}{x_i}, \cdots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \cdots, \frac{x_n}{x_i})$. Then, g and h becomes polynomials in the affine coordinates. □

Theorem 111. Let $Y \subseteq \mathbb{P}^n$ be a projective variety with the homogenous coordinate ring $S(Y)$ where $S = [x_0, \cdots, x_n]$. Then,
(1) $\mathcal{O}(Y) = k$
(2) for any point $p \in Y$, let $m_p \subseteq S(Y)$ be the homogenous ideal generated by the set of homogenous $f \in S(Y)$ s.t $f(p) = 0$ i..e

$$m_p := \{f \in S(Y) | f \text{ homogenous, } f(p) = 0\}.$$

Then, $\mathcal{O}_p = S(Y)_{m_p}$.
(3) $K(Y) \cong S(Y)_{((0))}$.

Proof. Define U_i as in the previous proposition and we know that $U_i \cong \mathbb{A}^n$. Then, $Y_i := Y \cap U_i$ is a variety.

Claim: $A(Y_i) \cong S(Y)_{(x_i)}$.
To show this, first note that $k[y_1, \cdots, y_n] \cong k[x_0, \cdots, x_n]_{(x_i)}$ by the map sending

$$\varphi^* : f(y_1, \cdots, y_n) \to f\left(\frac{x_0}{x_i}, \cdots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \cdots, \frac{x_n}{x_i}\right).$$

Note that

$$\varphi^*(f) = f \circ \varphi.$$

This map sends $I(Y_i)$ to $I(Y)k[x_0, \cdots, x_n]_{(x_i)}$. Then,
$A(Y_i) \cong k[x_0, \cdots, x_n]_{(x_i)}/I(Y) = (k[x_0, \cdots, x_n]/I(Y))_{(x_i)} = S(Y)_{(x_i)}$.

Now, we prove (2). Let $p \in Y$ be a point. Then $p \in Y_i$ for some i since a point in projetive space cannot have all 0s. By Proposition 109, $\mathcal{O}_p \cong A(Y_i)_{m_p}$, where m_p is the maximal ideal in $A(Y_i)$ corresponding to p. Then, $\varphi^*(m_p) = m_p S(Y)_{(x_i)}$. Since $x_i \notin m_p$, so $A(Y_i)_{m_p} \cong S(Y)_{(m_p)}$.

Next, we prove (3).

Claim: $K(Y)$ is equal to $K(Y_i)$. Suppose $< U, f >\in K(Y)$. Then, f is regular on U. Then, $< U, f >\in K(Y_i)$ since $U \cap Y_i$ is open and f is regular on it. On the other hand, if $< U, f >\in K(Y_i)$, clearly it is in $K(Y)$. Now, we know that $K(Y_i)$ is the quotient field of $A(Y_i)$ and so by the pullback φ^*, the quotient field of $A(Y_i)$ is isomorphic to $S(Y)_{((0))}$. So, $K(Y) \cong S(Y)_{((0))}$.

The proof of (1) can be found in Harshorne's "Algebraic Geometry". □

Definition 109. ($\mathrm{Hom}(X, Y)$). Let X and Y be varieties. Then, $\mathrm{Hom}(X, Y)$ is the set of all morphisms from X to Y.

Definition 110. ($\mathrm{Hom}(S, T)$). Let S and T be rings. Then, by $\mathrm{Hom}(S, T)$, we denote the set of all homomorphisms from ring S to ring T.

Proposition 112. Let X be a variety and let Y be an affine variety. Then, there exists a natural bijective mapping of sets

$$\alpha : \mathrm{Hom}(X, Y) \to \mathrm{Hom}(A(Y), \mathcal{O}(X)).$$

Proof. Given $\varphi : X \to Y$ is a morphism, φ takes regular functions on Y to regular functions on X via the pullback, $\varphi^* : \mathcal{O}(Y) \to \mathcal{O}(X)$. This map is a homomorphism of k-algebras. But $\mathcal{O}(Y) \cong A(Y)$, so φ^* induces a map from $A(Y)$ to $\mathcal{O}(X)$. Let this map be $\alpha : A(Y) \to \mathcal{O}(X)$.

Conversely, suppose $h : A(Y) \to \mathcal{O}(X)$ is a homomorphism. Let $Y \subseteq \mathbb{A}^n$ be a closed subset, so $A(Y)$ is defined. Let $\bar{x}_i$ be the image of x_i in $A(Y)$ (via the natural projection) and define $\gamma_i := h(\bar{x}_i) \in \mathcal{O}(X)$. Since each γ_i is a global function on X, we can define a mapping

$$\psi : X \to \mathbb{A}^n$$

by

$$\psi(p) = (\gamma_1(p), \cdots, \gamma_n(p))$$

for $p \in X$.

Claim: $\mathrm{Im}(\psi)$ is contained in Y.
Note $Y = Z(I(Y))$, so we only need to show that for any $p \in X$ and $f \in I(Y)$, $f(\psi(p)) = 0$. But $f(\psi(p)) = f(\gamma_1(p), \cdots, \gamma_n(p))$. Now, since f is a polynomial and h is a homomorphism, $f(\psi(p)) = f(\gamma_1(p), \cdots, \gamma_n(p)) = h(f(\bar{x}_1, \cdots, \bar{x}_n))(p) = 0$ as $f \in I(Y)$.

Lastly, we claim ψ is a morphism. This follows from the following lemma: □

Lemma 113. Let X be any variety and let $Y \subseteq \mathbb{A}^n$ be an affine variety. A map of sets $\psi : X \to Y$ is a morphism if and only if $x_i \circ \psi$ is a regular function on X for each i, where $x_1, \cdots, x_n$ are the coordinates functions on $\mathbb{A}^n$.

Proof. Suppose $\psi : X \to Y$ is a morphism. Then, $x_i \circ \psi$ is a regular function using the definition of morphisms. Conversely, suppose $x_i \circ \psi$ are regular for each i. Then, for any polynomial $f(x_1, \cdots, x_n)$, $f \circ \psi$ is also regular on X. Clearly, ψ is continuous. Lastly, regular functions on open subsets of Y are locally quotients of polynomials. So $g \circ \psi$ is regular for any regular ufntion g on any open subset of Y. Thus, ψ is a morphism. □

Corollary 114. Let X and Y be two affine varieties. Then, X and Y are isomorphic if and only if $A(X) \cong A(Y)$ i.e., $A(X)$ and $A(Y)$ are isomorphic as k-algebras.

References

[1] R. Vakil, *The Rising Sea: Foundations of Algebraic Geometry*. Stanford, 2024, available at http://math.stanford.edu/~vakil/216blog/.

[2] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed. John Wiley & Sons, 2004.

[3] R. Hartshorne, *Algebraic Geometry*, ser. Graduate Texts in Mathematics. Springer-Verlag, 1977, vol. 52.

[4] T. Leinster, "Basic category theory," 2016. [Online]. Available: https://arxiv.org/abs/1612.09375

[5] M. S. E. Community, "Showing exact functors preserve exact sequences (abelian categories, additive functors)," 2014. [Online]. Available: https://math.stackexchange.com/questions/803578/showing-exact-functors-preserve-exact-sequences-abelian-categories-additive-fu

A Ring Theory

All the material here is from Dummit and Foote's "Abstract Algebra". Detailed proofs of the theorems can be found in the text.

A.1 Rings

Definition: Rings. A ring R is a set with binary operations $\times$ and $+$ such that
(1) $(R, +)$ is an abelian group (i.e has identity, inverses and associativity).
(2) $\times$ is associatve i.e $(a \times b) \times c = a \times (b \times c)$
(3) distributive laws hold in R i.e $\forall a, b, c \in R$, we have $(a+b) \cdot c = a \cdot c + b \cdot c$ and $a \cdot (b+c) = a \cdot b + a \cdot c$.

Note: Rings that are commutative under multiplication are called **commutative rings**.

Example: Ring without identity The set of even integers $2\mathbb{Z}$ since 1 is not even.

Example: Ring of functions. For X a non-empty set and A any ring, the set of functions $f : X \to A$ forms a ring R with operations $(f + g)(x) = f(x) + g(x), (fg)(x) = f(x)g(x)$. R is commutative if and only if A is commutative. R has identity 1 if and only if A has 1.

Example: Some other easy rings. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all commutative rings. $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity 1.

Example: Trivial and Zero ring. Any abelian group is a trivial ring with the operation $x \cdot y = 0$ for any $x, y \in R$.

Definition: Division Ring. A ring R with identity $1 \neq 0$ such that every $x \in R$ has a multiplicative inverse $x^{-1} \in R$ with $xx^{-1} = x^{-1}x = 1$ is a division ring.

Definition: Field. A field is a commutative division ring.

Proposition: Immediate properties of rings For any ring R:
(1) $0x = x0 = 0, \forall x \in R$
(2) $(-x)y = x(-y) = -(xy), \forall x, y \in R$
(3) $(-x)(-y) = xy, \forall x, y \in R$
(4) if $\exists 1 \in R$, then 1 is unique and $-x = (-1)x, \forall x \in R$.

Proposition: A finite division ring is a field.

Definition: Zero divisor. Let R be a ring. Let $x \neq 0$. Then, x is a zero divisor if $\exists y \in R, y \neq 0$ such that $xy = 0$ or $yx = 0$.

Definition: Unit. Let R be a ring with identity 1. Then, $x \in R$ is called a unit if there exists $y \in R$ such that $xy = yx = 1$.
$R^{\times}$ is the set of units in ring R. $(R^{\times}, \times)$ is a group under multiplication called the group of units.

Example of zero divisor: Let $x \neq 0$ be an integer and suppose x is relatively prime to $n \in \mathbb{Z}$. Then, x is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$.

Lemma: If $x \in R$ is a zero divisor then x is not a unit. If $x \in R$ is a unit, then x is not a zero divisor.

Corollary: Fields have no zero divisors.

Example: zero divisor. Let $x \neq 0, x \in \mathbb{Z}$ and suppose x is relatively prime to $n \in \mathbb{Z}$. Then, $\bar{x}$ is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$.

A.2 Integral Domains and Subrings

Definition: Integral Domain. A commutative ring with identity $1 \neq 0$ such that it has no zero divisor.

Proposition: Cancellation laws hold in integral domains. Let $a, b, c \in R$ such that a is not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$. In other words, if a, b, c are elements in an integral domain, then, $ab = ac \implies a = 0$ or $b = c$.

Proposition: Any finite integral domain is a field.

Proof. Let R be a finite integral domain. Let $a \in R$ s.t. $a \neq 0$. We find a multiplicative inverse for a. Consider the map $\varphi(x) = ax$ for all $x \in R$. This map is injective by the previous proposition. Since R is finite and the map is injective, this map must also be surjective. Thus, there exists x such that $ax = 1$. □

Definition: Subring. A subring of the ring R is a subgroup of R that is closed under multiplication i.e $S \neq \emptyset$ is closed under addition, for each $x \in S$, there exists an additive inverse in S, $0 \in S$ and S is closed under multiplication.

Definition: Polynomial Rings. Let R be a commutative ring with identity 1. Let x be an indeterminate. Then, $R[x]$ is the ring of polynomials $\sum_{i=1}^{n} a_i x^i, n \geq 0, a_i \in R$. If $a_n \neq 0$, degree of the polynomial is n. Monic polynomials are those with $a_n = 1$. $R \subset R[x]$ is the set of constant polynomials. $R[x]$ is itself a commutative ring with identity (where 1 is the same identity as in R).

Note: if S is a subring of R, then $S[x]$ is a subring of $R[x]$.

Proposition: immediate properties of polynomial rings. Let R be an integral domain. Let $p(x), q(x)$ be non-zero elements of $R[x]$. Then,
(1) degree $p(x)q(x) =$ degree $p(x)+$ degree $q(x)$.
(2) the units of $R[x]$ are the same as the units of R
(3) $R[x]$ is an integral domain.

Definition: Ring homomorphisms. Let R and S be rings. A ring homomorphism $f : R \to S$ is a map such that $f(x + y) = f(x) + f(y), f(xy) = f(x)f(y), \forall x, y \in R$. A bijective ring homomorphism is called an **isomorphism** and we say $R \cong S$.

Lemma: Let $f : R \to S$ be a ring homomorphism. Then, $Im(f)$ be a subring of S and $ker(f)$ is a subring of R.

Examples of subrings: $\mathbb{Z}$ is a subring of $\mathbb{Q}$ which is a subring of $\mathbb{R}$. $2\mathbb{Z}$ and $n\mathbb{Z}$ are subrings of $\mathbb{Z}$.

A.3 Ideals

Definition: Ideals. Let R be a ring, let $r \in R$ and let I be a subset of R. Then, $rI := \{rx : x \in I\}$. $Ir := \{xr : x \in I\}$. A subset I of R is a left ideal of R if $\underline{I \text{ is a subring of } R}$ and $\underline{rI \subseteq I, \forall r \in R}$. A subset I of R is a right ideal of R if I is a subring of R and $Ir \subseteq I, \forall r \in R$. If I is both a left and right ideal, it is called an ideal of R.

Definition (Quotient ring of R by an ideal). Let I be an ideal of the ring R. Then, R/I is the quotient ring of R by I. The elements of this quotient ring are of the form $r + I$ for $r \in R$ and $r + I = s + I$ if $r - s \in I$.

Proposition: Quotient ring is a ring. Let R be a ring and let I be an ideal of R. Then the additive quotient group R/I is a ring under the binary operations $(r + I) + (s + I) = (r + s) + I, (r + I)(s + I) = (rs + I), \forall r, s \in R$. Conversely, if I is any subgroup of R such that these two operations are well-defined, then I is an ideal of R.

Proposition: Isomorphism Theorems for Rings.
(1) (First Isomorphism Theorem for Rings) If $\psi : R \to S$ is a ring homomorphism, then $ker(\psi)$ is an ideal of R, $Im(\psi)$ is a subring of S and $R/ker(\psi) \cong \psi(R)$.
(2) If I is an ideal of R, then the map $R \to R/I$ defined by $r \to r + I$ is a surjective ring homomorphism with kernel I. This is the natural projection of R onto R/I. Every ideal is the kernel of a ring homomorphism and vice-versa.
(3) (Second Isomorphism Theorem for Rings) Let A be a subring and B be an ideal of the ring R. Then, $A + B = \{a + b | a \in A, b \in B\}$ is a subring of R and $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)$.
(4) (Third Isomorphism Theorem for Rings) Let I and J be ideals of the ring R with $I \subseteq J$. Then, J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.
(5) (Lattice/Fourth Isomorphism Theorem for Rings) Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion-preserving bijection between the set of subrings of R that contain I and the set of subrings of R/I (in other words, if $A \subseteq B$ and both contain I, then $A/I \subseteq B/I$ + if $J \subseteq K$ are ideals containing I, then $J/I \subseteq K/I$). Also, A (a subring containing I) is an ideal of R if and only if A/I is an ideal of R/I.

Definition: Proper ideal. An ideal I is proper if $I \neq R$.

Example: R and $\{0\}$ are ideals of R. $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for any $n \in \mathbb{Z}$.

Definition (Ideals generated by a set). Let R be a ring with identity 1. Let A be a subset of R. Let (A) be the smallest ideal of R containing A. Then,
(1) (A) is the smallest ideal of R containing A, called the ideal generated by A:

$$(A) = \cap_{(\text{I is an ideal, A} \subseteq \text{I})} I$$

.
(2) Define $RA = \{\sum_i r_i a_i : r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$. Define RA and RAR similarly. We say RA is the left ideal generated by A, AR is the right ideal generated by A and RAR is the ideal generated by A. **If R is commutative, $RA = AR = RAR = (A)$.**
(3) Principle ideals are ideals generated by a single element.
(4) A finitely general ideal is an ideal generated by a finite set.

Proposition (conditions for proper ideal and fields): Let I be an ideal of R, where R is a ring with identity 1. (1) $I = R$ if and only if I contains a unit. (2) If R is commutative, then R is a field if and only if its only ideals are the zero ideal $\{0\}$ and R.

Corollary: If R is a field, then any non-zero ring homomorphism from R into another ring is an injection.

A.4 Maximal Ideals

Definition: Maximal Ideals Let R be a ring with identity $1 \in R$. An ideal M in R is called a maximal ideal if $M \neq R$ and the only ideals containing M are M and R.

Proposition: In a ring with identity 1, every proper ideal is contained in a maximal ideal.

Sketch of proof: Suppose I is a proper ideal. Let S be the set of proper ideals containing I(S is clearly non-empty and has partial order by inclusion). Let C be a chain in S and let J be the union of all ideals in C. Show that J is an ideal - $0 \in J$ and elements are closed under subtraction and left/ring multiplication by elements of R. Then, show that J is a proper ideal since otherwise $1 \in J$ and therefore, 1 is in at least one of the ideals in C making that ideal not proper. Then, each chain has an upper bound in S. Use Zorn's lemma to conclude S has a maximal element which is our maximal proper ideal containing I

Proposition: Let R be a commutative ring with identity 1. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.

Sketch of proof: ideal M is maximal iff there are no ideals I st $M \subset I \subset R$. By lattice isomorphism, ideals of R containing M correspond bijectively with the ideals of R/M, so M is maximal if and only if the only ideals of R/M are 0 and R/M. But by a proposition above, R/M is a field iff the only ideals are 0 and R/M.

A.5 Prime Ideals

Definition: Prime ideal. Suppose R is a commutative ring with identity 1. An ideal P is called a prime ideal if $P \neq R$ and whenever $xy \in P$, we have $x \in P$ and/or $y \in P$.

Proposition: Suppose R is commutative with identity $1 \neq 0$. Then, the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

Proof: P is a prime ideal if and only if $\bar{R} \neq \bar{0}$ (since $P \neq R$) and $\bar{ab} = \bar{a}\bar{b} = 0$ implies either $\bar{a} = 0$ or $\bar{b} = 0$ which is if and only if R/P is an integral domain.

Proposition: Assume R is commutative. Every maximal ideal of R is a prime ideal.

Proof: M is maximal implies R/M is a field and a field is an integral domain so M must be prime.

Example: The ideal (x) is a prime ideal in $\mathbb{Z}[x]$ since $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$.

A.6 Rings of Fractions and Fields of Fractions

Let R be a commutative ring. We want to show that R is a subring of a larger ring Q in which every non-zero element of R that is not a zero divisor is a unit in Q.

First, we define the equivalence relation $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$. Define addition and multiplication of fractions as is normally done with rational numbers.

Definition: Let R be a commutative ring and let D be a non-empty subset of R such that $0 \notin D$, D contains no zero divisors and D is closed under multiplication. Then, there exists a commutative ring Q, denoted $Q = D^{-1}R$, with $1 \in Q$ such that Q contains R as a subring and every element of D is a unit in Q. This ring Q has the following properties:
(1) every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$.
(2) If $D = R - \{0\}$, then Q is a field. We call Q the field of fractions or the quotient field of R.
(3) The ring Q is the smallest ring containing R in which all elements of D are units. In other words, let S be any commutative ring with identity and let $\varphi : R \to S$ be any injective ring homomorphism s.t. $\varphi(d)$ is a unit in S for all $d \in D$. Then, there is an injective ring homomorphism $\phi : Q \to S$ s.t. $\phi|_R = \varphi$.

A.7 Euclidean Domains and Discrete Valuation Rings

Definition (Norm/Positive Norm). Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a norm on the integral domain R. If $N(a) > 0$ for all $a \neq 0$, then N is called a positive norm.

Definition (Euclidean Domains). An integral domain R is called a Euclidean Domain (or possess a Division Algorithm) if there exists a norm N on R such that for any two elements

$a, b \in R$ with $b \neq 0$, there exists elements $q, r \in R$ s.t.

$$a = bq + r$$

with $r = 0$ or $N(r) < N(b)$. We call q the quotient and r the remainder.

Examples of Euclidean domains:
(1) All fields are trivial examples of Euclidean Domains.
(2) $\mathbb{Z}$ is a Euclidean Domain with $N(a) = |a|$.
(3) If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain with norm $N(p(x)) = deg(p(x))$.

Proposition: Every ideal in a Euclidean domain is a principal ideal. So, Euclidean domains are principal ideal domains.

Proof. If $I = 0$, we are done. Let $d \in I$ s.t. $N(d) \leq N(x)$ for all $x \in I$. Then, $(d) \subseteq I$. Consider any $a \in I$, where $a = qd + r$ (here, $r = 0$ or $N(r) \leq N(d)$). Then, $r = a - qd \in I$. By minimality of norm of d, $r = 0$, so $a = qd \in (d)$. So $I \subseteq (d)$. $\square$

Examples:
(1) Every ideal in $\mathbb{Z}$ is a principal ideal.

Definition (Discrete Valuation): Let K be a field. A discrete valuation on K is a function

$$v : K^{\times} \to \mathbb{Z}$$

such that (1) $v(ab) = v(a) + v(b)$ (2) v is surjective and (3) $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K^{\times}$ with $x + y \neq 0$.

Definition (Valuation Ring): The valuation ring of v is

$$\{x \in K^{\times} | v(x) \geq 0\} \cup \{0\}.$$

Definition(Discrete Valuation Ring). An integral domain R is a discrete valuation ring if there exists a valuation v on its field of fractions such that R is the valuation ring of v.

Note: **A discrete valuation ring is a Euclidean Domain** with the norm $N(0) = 0$ and $N = v$ on non-zero elements.

A.8 Principal Ideal Domains

Definition: Principal Ideal Domain (PID). A PID is an integral domain in which every ideal is principal.

Example: $\mathbb{Z}$ is a PID.

Proposition: Let R be a PID and let $a, b \in R$ such that $a \neq 0$, $b \neq 0$. Let d be a generator for the principal ideal generated by a and b. Then,
(1) d is the greatest common divisor of a and b.
(2) d can be written as an R-linear combination of a and b i.e. there exists $x, y \in R$ such that $d = ax + by$ and
(3) d is unique up to multiplication by a unit of R.

Proposition: Every non-zero prime ideal in a PID is a maximal ideal.

Proof. Let (p) be a prime ideal in a PID. Let $I = (m)$ contain (p). We want to show $I = (p)$ or $I = R$. Since $(p) \subset (m) = I$, $p = rm$ for some $r \in R$. Now, (p) is prime, so either $r \in (p)$ or $m \in (p)$. If $m \in (p)$, then $(p) = (m) = 1$. If $r \in (p)$, write $r = ps$ so $p = rm = psm$. So $sm = 1$ so m is a unit and $I = R$. $\square$

Corollary: If R is any commutative ring such that the polynomial ring $R[x]$ is a PID or a Euclidean domain, then R is necessarily a field.

Proof. Suppose, $R[x]$ is a PID. Now, R is a subring of $R[x]$, then R must be an integral domain. The ideal (x) is a non-zero prime ideal in $R[x]$ as $R[x]/(x) \cong R$. Then, (x) is a maximal ideal by previous proposition, so R is a field. $\square$

A.9 Irreducible elements and Prime elements

Definition: Irreducible, prime and associate. Let R be an integral domain.
(1) Let $x \in R$ such that x is not a unit. Then x is irreducible in R if $x = ab$ where $a, b \in R$ implies either a or b is a unit in R.
(2) A non-zero element $x \in R$ is called a prime in R if the ideal (x) generated by x is a prime ideal. Equivalently, $x \neq 0$ is a prime if it is not a unit and whenever x divides $ab \in R$, either x divides a or x divides b.
(3) Two elements x and y of R are associate if $x = uy$ for some unit $u \in R$.

Proposition: In an integral domain, a prime element is always irreducible.

Proof. Suppose (p) is a non-zero prime ideal and $p = ab$. Then, $ab \in (p)$ implies either $a \in (p)$ or $b \in (p)$. Assume the former WLOG. Then, $a = pr$ for some $r \in R$. Now, $p = ab = prb$ so $rb = 1$ so b is a unit. Thus, p is irreducible. $\square$

Proposition: prime = irreducible in PID. In a PID, a non-zero element x is a prime if and only if it is irreducible.

Proof. We already know prime implies irreducible, so we show the converse. Suppose M is an ideal containing (p). Then, $M = (m)$ is a principal ideal and since $p \in (m)$, $p = rm$ for some r. Since p is irreducible, either r or m is a unit. So, either $(p) = (m)$ or $(m) = (1)$. Thus, the only ideals containing (p) are (p) or (1). So (p) is a maximal ideal. We know maximal ideals are prime ideals, so p is a prime. $\square$

A.10 Unique Factorization Domain

Definition: Unique factorization domain (UFD) A unique factorization domain is an integral domain R in which every non-zero $x \in R$ which is not a unit has the following properties:
(1) x is a finite product of irreducible p_i (not necessarily distinct) of R; $x = p_1 \cdots p_r$
(2) The decomposition is unique up to associates i.e $x = q_1 \cdots q_m$ is another decomposition, then $m = r$ and after renumpering p_i is associate to q_i for all i.

Example: **A field F is a UFD since every element is a unit.**

Example: **When R is a UFD, R[x] is also a UFD.**

Proposition: prime = irreducible in UFD. In a UFD, a non-zero element x is a prime if and only if it is irreducible.

Proof. Let R be a UFD. We need to show irreducible implies prime. Suppose $p \in R$ is irreducible and suppose $p|ab$ for some $a, b \in R$. Then, $ab = pc$ for some c. Write a and b as their irreducible decomposition. Then p must be associate to some irreducible either in the decomposition of a or b - assume the former WLOG. Then, $a = (up)p_2 \cdots p_n$ where u is a unit. Then, p divides a and so p is a prime. $\square$

Proposition: Let $a, b \in R$ be non-zero and let R be a UFD. Suppose, $a = up_1^{e_1} \cdots p_n^{e_n}$ and $b = vp_1^{f_1} \cdots p_n^{f_n}$ are their prime factorizations for a and b with u, v units. Here the primes p_i are distinct and $e_i, f_i \geq 0$ for all i. Then, $d = p_1^{\min e_1, f_1} \cdots p_n^{\min e_n, f_n}$ is the greatest common divisor of a and b.

Proposition: Every Principal Ideal Domain is a Unique Factorization Domain. In particular, every Euclidean Domain is a Unique Factorization Domain.

A.11 Polynomial Rings

Definition (Polynomial Ring). $R[x]$ consists of formal sums $a_n x^n + \cdots + a_1 x + a_0$, where $a_i \in R$ and $n \geq 0$. If $a_n \geq 0$, then the degree of the polynomial is n. A monic polynomial is one where $a_n = 1$.

We already saw the following before:

Proposition 1: Let R be an integral domain. Then:
(a) $deg(p(x)q(x)) = deg(p(x)) + deg(q(x))$ given $p(x), q(x)$ are non-zero.
(b) The units of $R[x]$ are the units of R.
(c) $R[x]$ is an integral domain.

Proposition 2: Quotient of polynomial ring. Let I be an ideal of the ring R. Then, $R[x]/I[x] \cong (R/I)[x]$. In particular, if I is a prime ideal of R, then $I[x]$ is a prime ideal of $R[x]$.

Proof. Consider map $\varphi : R[x] \to (R/I)[x]$ by taking each coefficient mod $I/$; this is easily seen to be a ring homomorphism. Then, $ker(\varphi) = I[x]$ proves first part. For the second, since I is prime, R/I is integral domain (by previous proposition) so $(R/I)[x]$ is an integral domain and so $I[x]$ is a prime ideal of $R[x]$. □

Note: It is *not* true that if I is a maximal ideal of R, then $I[x]$ is a maximal ideal of $R[x]$. However, if I is maximal in R, then the ideal of $R[x]$ generated by I and x is maximal in $R[x]$.

Definition: Polynomial ring of more than one variables. The polynomial ring in the variables $x_1, \cdots, x_n$ with coefficients in R denoted by $R[x_1, \cdots, x_n]$ is defined inductively by $R[x_1, \cdots, x_n] = R[x_1, \cdots, x_{n-1}][x_n]$.

A polynomial in a polynomial ring of more than one variable is a finite sum of elements of the form $ax_1^{d_1} \cdots x_n^{d_n}$ where $a \in R, d_i \geq 0$ which are called the monomial terms. For a monomial term, if $a = 1$, we call it a monic term. A monomial term of this form is of degree $d = d_1 + \cdots + d_n$ and the n-tuple $(d_1, \cdots, d_n)$ is the multidegree of the term.

If f is a non-zero polynomial in n variables, the sum of all monomial terms in f of degree k is called the homogenous component of f of degree k. If f has degree d, then f may be written uniquely as the sum $f_0 + \cdots + f_d$ where f_k is the homogenous component of f of degree k.

A.12 Polynomial Rings over Fields

Theorem 3: Polynomial rings that are Euclidean Domains. Let F be a field. The polynomial ring $F[x]$ is a Euclidean Domain. If $a(x), b(x)$ are two polynomials in $F[x]$ with $b(x) \neq 0$, then there are unique polynomials $q(x), r(x) \in F[x]$ such that $a(x) = q(x)b(x) + r(x)$ with $r(x) = 0$ or *degree* r$(x) <$ *degree* b(x).

Sketch of proof: Use induction. Let $deg(a(x)) = n, deg(b(x)) = m$. If $a(x) = 0$, then $q(x) = r(x) = 0$. If $n < m$, let $q(x) = 0, r(x) = a(x)$. So let $n \geq m$. Construct $q(x)$ - if $a(x) = \sum_{i=0}^{n} a_i x^i, b(x) = \sum_{i=0}^{m} b_i x^i$. Define $a'(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$ designed to subtract leading term from $a(x)$. By inductive hypothesis, $a'(x) = q'(x)b(x) + r(x)$. With $q(x) = q'(x) + \frac{a_n}{b_m} x^{n-m}$. To prove uniqueness, assume there is another decomposition with $q_1(x), r_1(x)$ and leverage the fact that degree of $f(x)g(x)$ is the sum of degree $f(x)$ and degree $g(x)$.

Corollary 4: If F is a field, then $F[x]$ is a Principal Ideal Domain (PID) and a Unique Factorization Domain (UFD).

Now we look at polynomial rings that UFDs.

Proposition 5: Gauss's Lemma. Let R be a UFD with a field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$, then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some non-constant polynomials $A(x), B(x) \in F[x]$, then there are non-zero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

Sketch of proof for R a field: Let $p(x) = A(x)B(x)$ where on RHS, coefficients are in F. Multiply both sides by a common denominator for all coefficients to get $dp(x) = a'(x)b'(x)$ where on RHS we have elements in R[x], $d \neq 0 \in R$. If d is unit, we are done with $a(x) = d^{-1}a'(x)b'(x)$. Check Dummit and Foote for the proof in the case where d is not a unit.

Corollary: Let R be a UFD. Let F be its field of fractions and let $p(x) \in R[x]$. Suppose the greatest common divisor of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic poynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

Proof: By Gauss's Lemma, if $p(x)$ is reducible in $F[x]$, then it is reducible in $R[x]$. Conversely, suppose the gcd of coefficients of $p(x)$ is 1. If p is reducible with $p(x) = a(x)b(x)$, then neither $a(x)$ nor $b(x)$ are constant polynomials - this factorization also shows $p(x)$ is reducible in $F[x]$.

Theorem: R is a UFD if and only if $R[x]$ is a UFD.

Corollary: If R is a UFD, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a UFD.

A.13 Irreducibility Criteria

Now we look at **irreducible criteria** of polynomials.

We will require the following throughout the AG notes:

Proposition: Let R be a field. The prime ideals of $R[y]$ are the zero ideal (0), the ideals $(f(y))$ where f is irreducible.

Proof: Given R is a field, $R[x]$ is a PID. If (f) is a prime ideal in $R[x]$, then f is prime which means f is irreducible.

Proposition: Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in R i.e there is an $\alpha \in F$ with $p(\alpha) = 0$.

Proof: If $p(x)$ has a factor of degree 1, then since F is a field, we may assume the factor is of the *form $(x-a), a \in F$. Then, $p(a) = 0$. Conversely, if $p(a) = 0$, then by division algorithm in $F[x]$ - theorem 3 in this section - $p(x) = q(x)(x-a) + r$ where r is constant and since $p(a) = 0, r = 0$ so $(x-a)$ is a factor.*

Proposition: A polynomial of degree two or three over a field F is reducible if and only if has a root in F.

Proposition: Let $p(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial of degree n with integer coefficients. If $r/s \in \mathbb{Q}$ is in its lowest term (i.e r and s are relatively prime integers) and r/s is a root of $p(x)$, then r divides the constant term and s divides the leading coefficient of $p(x)$ i.e $r|a_0$ and $s|a_n$. In particular, if $p(x)$ is a monic polynomial with integer coefficients and $p(d) \neq 0$ for all integers d dividing the constant term of $p(x)$, then $p(x)$ has no roots in $\mathbb{Q}$.

The following are very important results:

Proposition: Let I be a proper ideal in the integer domain R and let $p(x)$ be a nonconstant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.

Proof: Suppose p(x) cannot be factored in (R/I)[x] but p(x) is reducible in R[x] so $p(x) = a(x)b(x)$ where both a(x) and b(x) are monic, nonconstant in R[x]. But then reducing the coefficients modulo I gives a factorization in (R/I)[x] - contradiction.

Proposition: Einsenstein's Criterion. Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial in $R[x]$ $(n \geq 1)$. Suppose $a_{n-1}, a_n, \cdots, a_1, a_0$ are all elements of P and suppose a_0 is not an element of P^2. Then $f(x)$ is irreducible in $R[x]$.

Proposition: The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials in $f(x)$. In particular, $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proposition: Let $g(x)$ be a nonconstant element of $F[x]$ and let $g(x) = f_1(x)^{n_1}f_2(x)^{n_2}\cdots f_k(x)^{n_k}$ be its factorization into irreducibles, where the $f_i(x)$ are distinct. Then, we have the following isomorphism of things:

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times \cdots \times F[x]/(f_k(x)^{n_k})$$

Proposition: I the polynomial $f(x)$ has roots $a_1, ..., a_k \in F$ (not necessarily distinct), then $f(x)$ has $(x-a_1)\cdots(x-a_k)$ as a factor. In particular, a polynomial of degree n in one variable over a field F has at most n roots in R, even counted with multiplicity.

B Module Theory

(Review from Dummit and Foote)

B.1 Modules and Submodules

Definition 111. (**Modules**). Let R be a ring. Then, a left R-module (or, in short, a module) is a set M such that $(M, +)$ is an abelian group and there exists a map $R \times M \to M$ such that for any $r, r' \in R$ and $m, m' \in M$, we have $(r + r')m = rm + r'm$, $(rr')m = r(r'm)$, $r(m+m') = rm+rm'$. If $1 \in R$, then $1\dot{y} = y$ for any $y \in M$ and we call M a **unitary module**.

A right R-module is defined similarly. If R is commutative and M is a left R-module, we can make this a right R-module by defining $mr = rm$ for all $r \in R, m \in M$.

Definition 112. (Submodules). Let R be a ring and let M be a R-module. An R-submodule of M is a subgroup N is closed under the action of ring elements $rn \in N$ for any $r \in R, n \in N$.

Examples of modules and submodules:
(1) M and $\{0\}$ are submodules of the module M.
(2) Every ring can be made into a module i.e., $M = R$. Here, the submodules are the left ideals of R.
(3) The affine n-space is a module: let n be a positive integer and let F be a field. Then, $F^n := \{(x_1, \cdots, x_n) \mid x_i \in F \forall i\}$ is an R-module where the operations (addition and multiplication by a scalar from F) are defined similar to $\mathbb{R}^n$.
(4) **Free module of rank n over R:** R is a ring with $1 \in R$ and let n be a positive integer. Then, $R^n := \{(x_1, \cdots, x_n) \mid x_i \in R, \forall i\}$ is an R-module. The operations are, again, defined similar to $\mathbb{R}^n$.

Now, we look at $\mathbb{Z}$-modules. Importantly, ***any abelian group can be made into a $\mathbb{Z}$-module.***

Definition 113. ($\mathbb{Z}$-modules) Let $R = \mathbb{Z}$ and let $(A, +)$ be any abelian group. Then, A can be made into a $\mathbb{Z}$-module by letting (for any $n \in \mathbb{Z}$ and any $a \in A$) $na = a + \cdots + a$ (if $n > 0$), $na = 0$ (if $n = 0$) and $na = -a - a \cdots - a$ (if $n < 0$). $\mathbb{Z}$-modules are unital modules. Every abelian group is a $\mathbb{Z}$-module using this construction and of course every $\mathbb{Z}$-module is an abeliagn group - therefore, there is the following bijections:

$$\mathbb{Z}\text{-modules} \leftrightarrow \{\text{abelian group}\}$$
$$\mathbb{Z}\text{-submodules} \leftrightarrow \{\text{subgroups of abelian group}\}.$$

If A is an abeliagn group such that $x \in A$ is of finite order n, then $nx = 0$ (i.e., x is a zero divisor) and if A is a group of order m then $mx = 0$ for all $x \in A$.

Proposition 115 (Submodule criterion)**.** Let R be a ring and let M be an R-module. Subset N of M is a submodule of M if and only if (a) $N \neq \emptyset$ (b) $x + ry \in N$ for any $x, y \in N$ and $r \in R$.

B.2 R-algebra and R-algebra homomorphisms

An R-module is an abelian group that a ring R acts on. An R-algebra is a commutative ring A that contains the image of R in its center.

Definition 114. (R-algebra) Let R be a commutative ring with $1 \in R$. An R-algebra is a ring A with $1 \in A$ and a ring homomorphism $f : R \to A$ such that $f(1_R) = 1_A$ such that the subring $f(R) \subset Z(A)$ ($Z(A)$ is the center of A).

Properties:
(1) If A is an R-algebra, then A has a natural left and right unital module structure defined by $r \cdot a = a \cdot r = f(r)a$.

Definition 115. (R-algebra homomorphism) Let A and B be two R-algebras. An R-algebra homomorphism (isomorphism) is a ring homomorphism (isomorphism) $\varphi : A \to B$ such that (1) $\varphi(1_A) = 1_B$ (2) $\varphi(r \cdot a) = r \cdot \varphi(a)$ for any $r \in R$ and $a \in A$ – note that here $r \cdot a = f(r) \cdot a$ and $r \cdot \varphi(a) = f(r) \cdot \varphi(a)$.

Examples:
Let R be a commutative ring with $1 \in R$.
(1) Any ring with identity 1 is a $\mathbb{Z}$-algebra.
(2) For any ring R with $1 \in R$, if $A \subseteq Z(R)$ is a subring and $1 \in R$, then A is an R-algebra. For example, $R[x]$ **is an** R**-algebra.**

Important property:
Let A be an R-algebra. Then, the R-module structure of A depends on $f(R) \subseteq Z(A)$. So, *up to a ring homomorphism*, every algebra A arises from a subring of $Z(A)$ with 1_A in it.

In particular, when $R = F$ a field and A is an R-algebra, then F is isomorphic to its image $f(R) = f(F)$ (since any non-zero ring homomorphism, which it has to be since it takes multiplicative identities to multiplicative identities, from R to its image is a bijection).

B.3 R-module homomorphisms and isomorphisms

Definition 116. (R-module homomorphisms and isomorphisms) Let R be a ring and let M and N be R-modules. Then, a map $\varphi : M \to N$ is an R-module homomorphism if it satisfies the following two: (1) $\varphi(x + y) = \varphi(x) + \varphi(y)$ for al $x, y \in M$ and (2) $\varphi(rx) = r\varphi(x)$. If φ is bijective, we call this an R-module isomorphism and write $M \cong N$.

We call $\mathrm{Hom}_R(M, N)$ the space of all R-module homomorphisms from M to N.

Our dictionary can be kept intact: $ker(\varphi) = \{m \in M \mid \varphi(m) = 0\}$ is a submodule and $\varphi(M) = \{n \in N \mid \exists m \in M, \varphi(m) = n\}$ is also a submodule.

Example: $\mathbb{Z}$-module homomorphisms are abelian group homomorphisms.

Proposition 116. Let M, N and L be R-modules.
(1) A map $\varphi : M \to N$ is an R-module homomorphism if and only if $\varphi(rx+y) = r\varphi(x) + \varphi(y)$ for all $x, y \in M$ and $r \in R$.
(2) Let $\varphi, \psi \in \mathrm{Hom}_R(M, N)$. Define $\varphi + \psi$ by letting $(\varphi+\psi)(m) = \varphi(m) + \psi(m)$ for any $m \in M$. Then, $(\varphi+\psi) \in \mathrm{Hom}_R(M, N)$. If R is a commutative ring, then for any $r \in R$, define $(r\varphi)(m) = r\varphi(m)$ for any $m \in M$. Then, $r\varphi \in \mathrm{Hom}_R(M, N)$. Thus, $\mathrm{Hom}_R(M, N)$ is an R-module itself.
(3) If $\varphi \in \mathrm{Hom}_R(M, N)$ and $\psi \in \mathrm{Hom}_R(N, L)$, then $\varphi \circ \psi \in \mathrm{Hom}_R(M, L)$.
(4) $\mathrm{Hom}_R(M, M)$ is a ring with $1 \in \mathrm{Hom}_R(M, M)$. When R is commutative, $\mathrm{Hom}_R(M, M)$ is an R-algebra.

Definition 117. (Endomorphism ring and endomorphisms) $\mathrm{Hom}_R(M, M)$ is called the endomorphism ring and each element in this ring is called an endomorphism. We denote the ring by $\mathrm{End}_R(M)$ or, simply, $\mathrm{End}(M)$.

Examples:
(1) When R is a commutative ring, there is the map $R \to \mathrm{End}_R(M)$ by sending each $r \in R$ to $r \cdot I$ (here, $(rI)(m) = rm$ for any $m \in M$). We require R to be commutative so that the image of this map in $\mathrm{End}_R(M)$ is an abelian group.
(2) If R has the identity 1_R, then $\mathrm{End}_R(M)$ is an R-algebra.

Proposition 117. Let R be a ring, M be an R-module and N be a submodule of M. Then, the abelian group $(M/N, +)$ can be made into an R-module by defining $r(x+N) = (rx) + N$ for any $x + N \in M/N$ and $r \in R$. The natural projection map $\pi : M \to M/N$ by $\pi(x) = x + N$ for $x \in M$ is an R-module homomorphism with $\ker(\pi) = N$ i.e., $\pi \in \mathrm{Hom}\big(M, N\big)$.

Theorem 118 (Isomorphism Theorems)**.**

1. **(The First Isomorphism Theorem for Modules)** Let M, N be R-modules and let $\varphi : M \to N$ be an R-module homomorphism. Then $\ker\varphi$ is a submodule of M and $M/\ker\varphi \cong \varphi(M)$.

2. **(The Second Isomorphism Theorem)** Let A, B be submodules of the R-module M. Then $(A+B)/B \cong A/(A\cap B)$.

3. **(The Third Isomorphism Theorem)** Let M be an R-module, and let A and B be submodules of M with $A \subseteq B$. Then $(M/A)/(B/A) \cong M/B$.

4. **(The Fourth or Lattice Isomorphism Theorem)** Let N be a submodule of the R-module M. There is a bijection between the submodules of M which contain N and the submodules of M/N. The correspondence is given by $A \mapsto A/N$, for all $A \supseteq N$. This correspondence commutes with the processes of taking sums and intersections (i.e., is a lattice isomorphism between the lattice of submodules of M/N and the lattice of submodules of M which contain N).

B.4 Generators

Definition 118. Let R be a ring with $1 \in R$. Let M be an R-module. Let $N_1, \cdots, N_n$ be sub-modules of M. Then,

$$N_1 + \cdots + N_n := \{x_1 + \cdots x_n \mid x_i \in N_i \forall i\}$$

and, with A a subset of M,

$$RA = \{r_1 a_1 + \cdots + r_m a_m \mid r_i \in R, a_i \in A, m \in \mathbb{Z}\}.$$

We call RA the **submodule of** M **generated by** A**.**

1. $RA = \emptyset$ if $A = \emptyset$.
2. If A is finite with $A = \{a_1, \cdots, a_n\}$, we write $RA = Ra_1 + \cdots + Ra_n$.
3. If $N = RA$ for some $A \subset M$, we call A the set of generators of N. N is a finitely generated submodule of M if there exists $A \subseteq M$ such that $N = RA$ and A is finite.
4. N is called a cyclic submodule if there exists $a \in M$ such that $N = Ra = \{ra \mid r \in R\}$.

If N is finitely generated by d elements, the smallest set of size d that generates N is called the minimal set of generators for N.

Examples:

1. Let $R = \mathbb{Z}$ and let M be an R-module. Then, if $a \in M$, $\mathbb{Z}a$ is the cyclic group of M generated by a i.e. $\mathbb{Z}a =< a >\subseteq M$.
2. If R is a ring with $1 \in R$ and M is an R-module, then R is a finitely generated, cyclic R-module as $R = R1_R$. Here, the submodules of R are the left ideals of R.

B.5 Direct product and direct sums of modules

Definition 119. (Direct Product). Let $M_1, \cdots, M_k$ be a collection of R-modules. Then,

$$M_1 \times \cdots \times M_k = \{(x_1, \cdots, x_k) \mid x_i \in M_i, \forall i\}$$

is called the direct product of $M_1, \cdots, M_k$. The direct product is also an R-module.

Proposition 119. Let $N_1, \cdots, N_k$ be submodules of the R-module M. Then, the following are equivalent:

1. $\pi : N_1 \times N_2 \times \cdots \times N_k \to N_1 + \cdots + N_k$ by $\pi(x_1 \cdots, x_k) = x_1 + \cdots + x_k$ is an isomorphism of R-modules, so $N_1 \times N_2 \times \cdots \times N_k \cong N_1 + \cdots + N_k$.

2. $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$ for all $j \in \{1, \cdots, k\}$.

3. For any $x \in N_1 + \cdots + N_k$, x can be uniquely written as $x = x_1 + \cdots + x_k$ where $x_i \in N_i$.

Definition 120. (Direct sum) If an R-module $M = N_1 + \cdots + N_k$ where N_i are submodules of M, then, we say M is the direct sum of $N_1, \cdots, N_k$ and write it as

$$M = N_1 \oplus \cdots \oplus N_k.$$

Notably, each $x \in M$ can be uniquely written as $x = x_1 + \cdots + x_k$ for $x_i \in N_i$.

B.6 Free R-modules

Definition 121. (Free module on subset A). An R-module F is *free* on the subset $A \subseteq F$ if for any $x \in F$, *unique* non-zero elements $r_1, \cdots, r_n$ in R and unique $a_1, \cdots, a_n \in A$ such that $x = r_1 a_1 + \cdots + r_n a_n$ and $n \in \mathbb{Z}^+$. Then, A is the basis or *the set of free generators* for F.

Note that the elements $a_1, \ldots, a_n$ need not be the same for every $x \in F$. In particular, n could be different for each element x in the free R-module, F.

Notation: We denote the free R module, F, on the subset $A \subseteq F$ as $F(A)$.

Proposition 120. For any set A, there exists a free R-module $F(A)$ on A such that $F(A)$ satisfies the universal property:

if M is any R-module and $\varphi : A \to M$ is a map of sets, then there exists a unique R-module homomorphism $\phi : F(A) \to M$ such that $\phi(a) = \varphi(a)$ for any $a \in A$ and the following diagram commutes:

$$\begin{tikzcd}
A \arrow[r, "inclusion"] \arrow[dr, "\varphi"'] & F(A) \arrow[d, "\Phi"] \\
& M
\end{tikzcd}$$

When $A = \{a_1, \cdots, a_n\}$ is finite,

$$F(A) = Ra_1 \oplus \cdots \oplus Ra_n \cong R^n.$$

Proof: Define $F(A) = \{0\}$ if A is empty and otherwise define

$$F(A) = \{f : A \to R \mid f(x) = 0 \text{ for all but finitely many } x \in A\}.$$

$F(A)$ is a module: This becomes an R-module by $(f+g)(x) = f(x) + g(x), (rf)(x) = rf(x)$ for any $x \in A, r \in R, f, g \in F(A)$.

A is a subset of $F(A)$: Identify A as a subset of $F(A)$ by $a \to f_a$ which is 1 at a and 0 elsewhere.

$F(A)$ is free on A: Then any $f \in F(A)$ can be uniquely written as $f = r_1a_1 + \cdots + r_na_n$ given $f(a_i) = r_i$.

To show the universal property, define $\phi : F(A) \to M$ by $\phi\left(\sum_{i=1}^n r_ia_i\right) = \sum_{i=1}^n r_i\varphi(a_i)$. Therefore, $\varphi|_A = \phi|_A$. Use the previous proposition to prove the result for when A is finite.

If A is finite: any $f \in F(A)$ can be uniquely written as $\sum_i r_ia_i$ and so, $F(A) = Ra_1 \oplus \cdots \oplus Ra_n$. Given $R \cong Ra_i$, $F(A) \cong R^n$.

Corollary 121. If F_1 and F_2 are free modules on the same set A, then there exists a unique isomorphism between F_1 and F_2 which is identity on A. If F is any free R-module with the set of generators being A, $F \cong F(A)$.

Example: **Free abelian group on A.** When $R = \mathbb{Z}$, if $F(A)$ is the free module on subset A, we call $F(A)$ the free abelian group on A. When A is finite with cardinality n, $F(A)$ is said to have rank n and we write

$$F(A) \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$$

where the direct sum is n times.

B.7 Tensor Products of Modules

Goal: We want to construct a product of modules M and N over a ring that contains 1. This will be done by constructing a new module where mn, for any $m \in M, n \in N$, is defined.

We start with a special case of this construction before moving on to the general case.

Special case: N is an R-module and R is a subring of S. Goal is to make N something like a S-module.

Step 1: Constructing the group. We define a map $\phi : S \times N \to N$ and we will denote $\phi(s, n)$ as sn. Consider the free $\mathbb{Z}$-module/free abelian group on $S \times N$ (i.e., for any $(s, n) \in S \times N$, there exists unique $(s_1, n_1), \ldots, (s_x, n_x)$ and unique $n_1, \ldots, n_x \in \mathbb{Z}$ such that $(s, n) = \sum_{i=1}^x n_i(s_i, n_i)$ – such a free $\mathbb{Z}$-module exists by the universal property of free modules). Next, we quotient this group $F(S \times N)$ by the subgroup H generated by elements of the form:

- $(s_1 + s_2, n) - (s_1, n) - (s_2, n)$
- $(s, n_1 + n_2) - (s, n_1) - (s, n_2)$
- $(sr, n) - (s, rn)$

for all $s, s_1, s_2 \in S, r \in R, n, n_1, n_2 \in N$.

We then have the Abelian group $S \otimes_R N := (S \times N)/H$ called the tensor product of S and N over R.

We denote the coset $(s, n) + H$ by $s \otimes n$. One can easily check that these cosets satisfy:

- $(s_1 + s_2) \otimes n = s_1 \otimes n + s_2 \otimes n$
- $s \otimes (n_1 + n_2) = s \otimes n_1 + s \otimes n_2$
- $sr \otimes n = s \otimes rn$.

Step 2: Constructing the S-module. We turn $S \otimes_R N$ into an S-module by defining $s(\sum_{\text{finite}} s_i \otimes n_i) = \sum_{\text{finite}} (ss_i) \otimes n_i$.

Then, we call $S \otimes_R N$ the left S-module obtained by extending the scalars from the left R-module N.

Immediate properties:

- There exists the map $\iota : N \to S \otimes_R N$ by $\iota(n) = 1 \otimes n$ by first mapping n to $(1, n)$ and then quotienting by H.
- $\iota : N \to S \otimes_R N$ is an R-module homomorphism from N to $S \otimes_R N$. However, ι is not injective in general as we are quotienting by H. Therefore, $S \otimes_R N$ ***need not contain an isomorphic copy of*** N.

Theorem 122. Let R be a subring of the ring S. Let N be a left R-module. Let $\iota : N \to S \otimes_R N$ be the left R-module homomorphism defined by $\iota(n) = 1 \otimes n$. Let L be any left S-module and let $\varphi : N \to L$ be an R-module homomorphism. Then, there exists a unique S-module homomorphism $\Phi : S \otimes_R N \to L$ such that $\varphi = \Phi \circ \iota$ and the following diagram commutes:

$$\begin{tikzcd} N \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & S \otimes_R N \arrow[d, "\Phi"] \\ & L \end{tikzcd}$$

Conversely, if $\Phi : S \otimes_R N \to L$ is an S-module homomorphism, then $\varphi = \Phi \circ \iota$ is an R-module homomorphism from N to L.

Note: $R \otimes_R N \cong N$. One can see this by letting φ be the identity map.

General construction:

Let N be a left R-module and let M be a right R-module.

Step 1: Constructing the group. We quotient the free $\mathbb{Z}$-module on the set $M \times N$ by the subgroup H generated by elements

- $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$
- $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$
- $(mr, n) - (m, rn)$

for all $m, m_1, m_2 \in M, n, n_1, n_2 \in N, r \in R$.

Denote this group by $M \otimes_R N = F(M \times N)/H$ called the tensor product of M and N over the ring R. The elements of $M \otimes_R N$ are called tensors. The coset, $m \otimes n$, of (m, n) in $M \otimes_R N$ is called a **simple tensor** and they satisfy

- $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$
- $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$
- $mr \otimes n = m \otimes rn$.

Immediate properties:

- We can define the map $\iota : M \times N \to M \otimes_R N$ by $\iota(m, n) = m \otimes n$. Here ι is additive in both m and n and $\iota(mr, n) = mr \otimes n = m \otimes rn = \iota(m, rn)$. Such
- Such maps are given a special definition.

  Definition 122. Let M be a right R-module and let N be a left R-module. Let L be an additive, abelian group. The map $\varphi : M \times N \to L$ is called R-balanced or middle linear w.r.t R if $\varphi(m_1 + m_2, n) = \varphi(m_1, n) + \varphi(m_2, n)$ and $\varphi(m, rn) = \varphi(mr, n)$.

Theorem 123. Suppose R is a ring with 1, M is a right R-module and N is a left R-module. Let $M \otimes_R N$ be the tensor product of M and N over R and let $\iota : M \times N \to M \otimes_R N$ be an R-balanced map.

- If $\Phi : M \otimes_R N \to L$ is any group homomorphism from $M \otimes_R N$ to an abelian group L, then the composite map $\varphi = \Phi \circ \iota$ is an R-balanced map from $M \times N$ to L.
- Conversely, suppose L is an abelian group and $\varphi : M \times N \to L$ is any R-balanced map. Then, there exists a unique homomorphism $\Phi : M \otimes_R N \to L$ such that φ factors through ι i.e., $\varphi = \Phi \circ \iota$.

Equivalently, the correspondence $\phi \leftrightarrow \Phi$ in the diagram establishes a bijection:

$$\begin{tikzcd} M \times N \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & M \otimes_R N \arrow[d, "\Phi"] \\ & L \end{tikzcd}$$

$$\{R\text{-balanced maps } \phi : M \times N \to L\} \quad \longleftrightarrow \quad \{\text{group homomorphisms } \Phi : M \otimes_R N \to L\}.$$

Definition 123. Let R and S be rings with 1. An abelian group M is called an (S, R)-bimodule if M is a left S-module, a right R-module and $s(mr) = (sm)r$ for any $s \in S, r \in R, m \in M$.

Examples of (S, R)*-bimodules*:

- Let S be a ring with R a subring of S. Then, S is a (S, R)-bimodule.
- If $f : R \to S$ is a ring homomorphism with $f(1_R) = 1_S$, then S can be considered as a right R-module with the action $s \cdot r = s \cdot f(r)$ and this makes S a (S, R)-bimodule.
- **(Standard structure)**Let R be a commutative ring. Let M be a left R-module. We can make M into a right R-module by defining $mr = rm$ for any $m \in M, r \in R$. Then, M becomes a (R, R)-bimodule. This is called the standard R-module structure on M.

Step 2: Constructing the module structure. N is a left R-module. Suppose M is a (S, R)-bimodule. Then, define

$$s\left(\sum_{\text{finite}} m_i \otimes n_i\right) = \sum_{\text{finite}} (sm_i) \otimes n_i.$$

Note: When $S = R$, we have that $M \otimes_R N$ is a left R-module because M is a $(R, R$-bimodule.

Definition 124. Let R be a commutative ring with 1. Let M, N and L be left R-modules. The map $\varphi : M \times N \to L$ is called R-bilinear if $\varphi(r_1m_1 + r_2m_2, n) = r_1\varphi(m_1, n) + r_2\varphi(m_2, n)$ and if $\varphi(m, r_1n_1 + r_2n_2) = r_1\varphi(m, n_1) + r_2\varphi(m, n_2)$.

Proposition 124. Let R be a commutative ring. Let M and N be left R-modules with M having the standard R-module structure (i.e. $rm = mr$). Then, $M \otimes_R N$ is a left R-module with $r(m \otimes n) = (rm) \otimes n = (mr) \otimes n = m \otimes (rn)$.

The map $\iota : M \times N \to M \otimes_R N$ with $\iota(m, n) = m \otimes n$ is an R-bilinear map.

If L is any left R-module, then the following diagram commutes:

$$\begin{tikzcd} M \times N \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & M \otimes_R N \arrow[d, "\Phi"] \\ & L \end{tikzcd}$$

B.8 Exact Sequences

Definition 125. (Extension). Let A and C be modules. Let B be the module either containing A or containing an isomorphic copy of A (call it $\varphi(A)$) such that $B/A \cong C$ or $B/\varphi(A) \cong C$. Then, B is called an extension of C by A.

Definition 126. (Exact pair of homomorphisms). Let X, Y and Z be modules. Then, the pair of homomorphisms

$$X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$$

is *exact* at Y if $\mathrm{Im}(\alpha) = \ker(\beta)$.

Note: Given the pair α and β are exact at Y, we see that $Z \cong Y/\ker(\beta)$. Also $Z \cong Y/\mathrm{Im}(\alpha)$ and so Y is an extension of Z by X.

Definition 127. (Exact Sequence). A sequence $\cdots \to X_{n-1} \to X_n \to X_{n+1} \to \cdots$ of homomorphisms is exact if it is exact at every X_n between a pair of homomorphisms.

Now, we look at some preliminary properties.

Proposition 125. Let A, B and C be R-modules over the ring R. Then,

1. The sequence $0 \to A \xrightarrow{\alpha} B$ is exact at A if and only if α is injective.
2. The sequence $B \xrightarrow{\beta} C \to 0$ is exact at C if and only if β is surjective.

Corollary 126. The sequence $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is exact if and only if α is injective, β is surjective, and $\mathrm{Im}(\alpha) = \ker(\beta)$.

Definition 128. (Short exact sequence). The exact sequence $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is called a short exact sequence.

Correspondence between exact sequence and short exact sequence: Given the exact sequence $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$, we can extract the short exact sequence $0 \to \alpha(X) \to Y \to Y/\ker(\beta) \to 0$.

Examples:

1. Let A and C be modules. Let $B = A \oplus C$ be the direct sum of A and C. Recall that each $x \in B$ can be uniquely written as $x = x_A + x_C$ where $x_A \in A, x_C \in C$. Then, the following is a short exact sequence:

   $$0 \to A \xrightarrow{i} A \oplus C \xrightarrow{\pi} C \to 0$$

   is a short exact sequence. Here, $i(x) = (x, 0)$ for any x in A and $\pi(x, y) = y$ for all $(x, y) \in A \oplus C$. Therefore, for any modules A and C, there exists at least one extension of C by A which is the direct sum.

(a) In particular, if $A = \mathbb{Z}$ and $C = \mathbb{Z}/n\mathbb{Z}$, then the following is a short exact sequence:

$$0 \to \mathbb{Z} \xrightarrow{i} \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0.$$

Another short exact sequence is the following:

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0$$

where $n(x) = nx$.

Definition 129. (Homomorphism of short exact sequences, equivalent extensions). Let

$$0 \to A \to B \to C \to 0$$

and

$$0 \to A' \to B' \to C' \to 0$$

be two short exact sequences.

1. A homomorphism of short exact sequences is the triple α, β, γ of module homomorphisms such that the following diagram commutes:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

2. If α, β and γ are isomorphisms, then the two exact sequences are said to be isomorphic and we say B and B' are isomorphic extensions.

3. The two exact sequences are *equivalent* if $A = A'$, $C = C'$ and there exists an isomorphism between them.

Proposition 127. (Short Five Lemma). Let α, β, γ be a homomorphism of short exact sequences:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

1. If α and γ are injective, then so is β.

2. If α and γ are surjective, then so is γ.

3. If α and γ are isomorphisms, then so is β.

Proof. We prove the first. Let α and γ be injective. Now suppose for some $b \in B$, we have that $\beta(b) = 0$. We want to show that $b = 0$ and so β is injective.

Let $\psi : A \to B$ and $\varphi : B \to C$ be the homomorphisms in the diagram. Since $\beta(b) = 0$, therefore the image of $\beta(b)$ in C' is also 0 (by property of module homomorphism). Then, by the commutativity of the diagram, $\gamma(\varphi(b)) = 0$. Since γ is injective by hypothesis, $\gamma(b) = 0$. Therefore, $b \in \ker(\varphi)$ and, by the exactness, $b \in \mathrm{Im}(\psi)$. So, $b = \psi(a)$ for some $a \in A$. Now, the image of $\alpha(a)$ in B' is the same as $\beta(\psi(a)) = \beta(b) = 0$. Given α is injective (by hypothesis) and the map from A' to B' (since the sequence is exact), therefore, $a = 0$ and so $b = \psi(a) = \psi(0) = 0$. $\square$