Algebraic Construction

Huyi Chen

Latest Update: January 17, 2026

Contents

Notation Conventions

In this book, we use the following notation conventions:

- $\mathbb{N}$: the set of natural numbers $\{0, 1, 2, \cdots\}$.

We use sans-serif font for categories. Some common categories are

- FinSet: the category of finite sets.
- Set: the category of sets.
- Mon: the category of monoids.
- Grp: the category of groups.
- Ab: the category of abelian groups.
- Ring: the category of rings.
- CRing: the category of commutative rings.
- Field: the category of fields.
- R-Mod: the category of left R-modules, where $R \in \mathrm{Ob}\,(\mathsf{Ring})$.
- K-Vect: the category of K-vector spaces, where $K \in \mathrm{Ob}\,(\mathsf{Field})$.
- R-Alg: the category of associative R-algebras, where $R \in \mathrm{Ob}\,(\mathsf{CRing})$.
- R-CAlg: the category of commutative R-algebras, where $R \in \mathrm{Ob}\,(\mathsf{CRing})$.
- Top: the category of topological spaces.

Chapter 1

Set Theory

1.1 Construction

1.1.1 Basic Operations

Definition 1.1.1 Family of Sets

Let I be some index set. A **family of sets index by** I is a function that maps each index $i \in I$ to a set A_i, denoted by $(A_i)_{i\in I}$.

Definition 1.1.2 Union and Intersection

Let I be some index set and $(A_i)_{i\in I}$ be a family of sets. The **union** and **intersection** of $(A_i)_{i\in I}$ are defined as follows

$$\bigcup_{i\in I} A_i := \{x : \exists\, i \in I, x \in A_i\}$$
$$\bigcap_{i\in I} A_i := \{x : \forall\, i \in I, x \in A_i\}$$

Definition 1.1.3 Difference and Complement

Let A, B be subsets of X. The **complement** of A is defined as follows

$$A^{\complement} := \{x \in X : x \notin A\}.$$

The **difference** of A and B is defined as follows

$$A - B := \{x : x \in A \text{ and } x \notin B\}.$$

We have

$$A^{\complement} = X - A, \qquad A - B = A \cap B^{\complement}.$$

Proposition 1.1.4 Distribution Law

Suppose that A_α, A, B_α, B are sets and I is some index set. We have the following distribution law:

- $A \cup \left(\bigcap_{\alpha\in I} B_\alpha\right) = \bigcap_{\alpha\in I} (A \cup B_\alpha)$
- $A \cap \left(\bigcup_{\alpha\in I} B_\alpha\right) = \bigcup_{\alpha\in I} (A \cap B_\alpha)$

Proposition 1.1.5 De Morgan Law

Suppose that A_α, A are sets and I is some index set. We have

- $\left(\bigcup_{\alpha\in I} A_\alpha\right)^{\complement} = \bigcap_{\alpha\in I} A_\alpha^{\complement}$, $\left(\bigcap_{\alpha\in I} A_\alpha\right)^{\complement} = \bigcup_{\alpha\in I} A_\alpha^{\complement}$
- $E - \bigcup_{\alpha\in I} A_\alpha = \bigcap_{\alpha\in I} (E - A_\alpha)$, $E - \bigcap_{\alpha\in I} A_\alpha = \bigcup_{\alpha\in I} (E - A_\alpha)$

1.1.2 Limit of Sequence of Sets

Definition 1.1.6 Upper Limit of Sequence of Sets

Let $(A_n)_{n=1}^{\infty}$ be a sequence of sets. The **upper limit** of $(A_n)_{n=1}^{\infty}$ is defined as follows

$$\overline{\lim_{n\to\infty}} A_n := \bigcap_{n=1}^{\infty}\bigcup_{k=n}^{\infty} A_k = \{x : x \text{ belongs to infinitely many sets in } (A_n)_{n=1}^{\infty}\}$$

We have

$$x \in \overline{\lim_{n\to\infty}} A_n \iff \forall n \geq 1, \exists k \geq n, x \in A_k.$$

Definition 1.1.7 Lower Limit of Sequence of Sets

Let $(A_n)_{n=1}^{\infty}$ be a sequence of sets. The **lower limit** of $(A_n)_{n=1}^{\infty}$ is defined as follows

$$\underline{\lim_{n\to\infty}} A_n := \bigcup_{n=1}^{\infty}\bigcap_{k=n}^{\infty} A_k = \{x : x \text{ belongs to all but finitely many sets in } (A_n)_{n=1}^{\infty}\}$$

Proposition 1.1.8 Property of Upper Limit and Lower limit

$$\bigcap_{n=1}^{\infty} A_n \subseteq \underline{\lim_{n\to\infty}} A_n \subseteq \overline{\lim_{n\to\infty}} A_n \subseteq \bigcup_{n=1}^{\infty} A_n.$$

Definition 1.1.9 Limit of Sequence of Sets

Let $(A_n)_{n=1}^{\infty}$ be a sequence of sets. If $\underline{\lim_{n\to\infty}} A_n = \overline{\lim_{n\to\infty}} A_n$, we define the **limit** of $(A_n)_{n=1}^{\infty}$ as follows

$$\lim_{n\to\infty} A_n := \underline{\lim_{n\to\infty}} A_n = \overline{\lim_{n\to\infty}} A_n$$

Proposition 1.1.10

Let $(A_n)_{n=1}^{\infty}$ be a sequence of sets.

1. If $(A_n)_{n=1}^{\infty}$ is nondecreasing, then it has limit

$$\lim_{n\to\infty} A_n = \bigcup_{n=1}^{\infty} A_n.$$

2. If $(A_n)_{n=1}^{\infty}$ is nonincreasing, then it has limit

$$\lim_{n\to\infty} A_n = \bigcap_{n=1}^{\infty} A_n.$$

1.1.3 Cartesian Product

Proposition 1.1.11 Cartesian Product of Intersections of Sets

$$\left(\prod_{i\in I} A_i\right) \cap \left(\prod_{i\in I} B_i\right) = \prod_{i\in I} (A_i \cap B_i)\,.$$

1.2 Relation

Definition 1.2.1 Relation

An n-**ary relation** R over sets $X_1, \cdots, X_n$ is a subset of the Cartesian product $X_1 \times \cdots \times X_n$. A **binary relation** R over sets X and Y is a subset of $X \times Y$. We write xRy to denote that $(x, y) \in R$.

Definition 1.2.2 Homogeneous Relation

A **homogeneous relation** R over a set X is a binary relation between X and itself, i.e. a subset of $X \times X$.

Here are some important properties that a homogeneous relation R over a set X may have:

- **Reflexivity**: $\forall x \in X$, xRx.
- **Irreflexivity**: $\forall x \in X$, not xRx.
- **Transitivity**: $\forall x, y, z \in X$, xRy and $yRz \implies xRz$.
- **Symmetry**: $\forall x, y \in X$, $xRy \implies yRx$.
- **Antisymmetry**: $\forall x, y \in X$, xRy and $yRx \implies x = y$.
- **Asymmetry**: $\forall x, y \in X$, $xRy \implies$ not yRx.
- **Strong Connectedness**: $\forall x, y \in X$, xRy or yRx.
- **Connectedness**: $\forall x, y \in X$, $x \neq y \implies xRy$ or yRx.

Definition 1.2.3 Filtered Set

A **filtered set** or **directed set** is a preorder set $(X, \leq)$ with an additional property that every pair of elements has an upper bound. In other words, for every $x, y \in X$, there exists $z \in X$ such that $x \leq z$ and $y \leq z$.

Proposition 1.2.4 Intersection of equivalence relations is an equivalence relation

The intersection of a family of equivalence relations on a set X is an equivalence relation on X.

Proof. Suppose $(R_i)_{i\in i}$ is a family of equivalence relations on X. We can check that $\bigcap_{i\in I} R_i$ is an equivalence relation on X by checking the three properties of equivalence relation:

(i) Reflexivity: For any $x \in X$, since $(x, x) \in R_i$ for all $i \in I$, we have $(x, x) \in \bigcap_{i\in I} R_i$.

(ii) Symmetry: For any $x, y \in X$,

$$(x, y) \in \bigcap_{i\in I} R_i \implies \forall i \in I, (x, y) \in R_i \implies \forall i \in I, (y, x) \in R_i \implies (y, x) \in \bigcap_{i\in I} R_i$$

Homogeneous Relation	Reflexivity	Symmetry	Transitivity	Connectedness
Directed graph				
Undirected graph		Symmetric		
Dependency	Reflexive	Symmetric		
Tournament	Irreflexive	Asymmetric		
Preorder	Reflexive		Transitive	
Total preorder	Reflexive		Transitive	Strongly Connected
Partial order	Reflexive	Antisymmetric	Transitive	
Strict partial order	Irreflexive	Asymmetric	Transitive	
Total order	Reflexive	Antisymmetric	Transitive	Strongly Connected
Strict total order	Irreflexive	Asymmetric	Transitive	Connected
Partial equivalence		Symmetric	Transitive	
Equivalence	Reflexive	Symmetric	Transitive	

(iii) Transitivity: For any $x, y, z \in X$,

$$\begin{aligned}(x,y) \in \bigcap_{i\in I} R_i \text{ and } (y,z) \in \bigcap_{i\in I} R_i &\implies \forall i \in I, (x,y) \in R_i \text{ and } (y,z) \in R_i \\ &\implies \forall i \in I, (x,z) \in R_i \\ &\implies (x,z) \in \bigcap_{i\in I} R_i\end{aligned}$$

□

Definition 1.2.5 Generated Equivalence Relation

Let X be a set and $R \subseteq X \times X$ be a relation on X. The **generated relation** $\langle R \rangle$ is defined as the smallest equivalence relation on X that contains R, or equivalently, the intersection of all equivalence relations on X that contain R.

1.3 Function

Proposition 1.3.1 Image and Preimage Laws for Set Operations

Let $f : X \to Y$ be a map. Suppose that $A_\alpha, A, E \subseteq X$ and $B_\alpha, B, F \subseteq Y$. We have

(i) $f\left(\bigcup_{\alpha\in I} A_\alpha\right) = \bigcup_{\alpha\in I} f(A_\alpha)$, $f\left(\bigcap_{\alpha\in I} A_\alpha\right) \subseteq \bigcap_{\alpha\in I} f(A_\alpha)$, $f(E-A) \supseteq f(E) - f(A)$.

(ii) $f^{-1}\left(\bigcup_{\alpha\in I} B_\alpha\right) = \bigcup_{\alpha\in I} f^{-1}(B_\alpha)$, $f^{-1}\left(\bigcap_{\alpha\in I} B_\alpha\right) = \bigcap_{\alpha\in I} f^{-1}(B_\alpha)$, $f^{-1}(F-B) = f^{-1}(F) - f^{-1}(B)$, $f^{-1}\left(B^{\complement}\right) = f^{-1}(B)^{\complement}$.

(iii) $A \subseteq f^{-1}(f(A))$, $B \supseteq f(f^{-1}(B))$.

(iv) If f is surjective, then $f\left(f^{-1}(B)\right) = B$.

(v) If f is injective, then $f\left(\bigcap_{\alpha\in I} A_\alpha\right) = \bigcap_{\alpha\in I} f\left(A_\alpha\right)$, where the indexed set I is nonempty.

(vi) $f\left(A \cap f^{-1}(B)\right) = f(A) \cap B$.

(vii) $A \subseteq f^{-1}(B) \iff f(A) \subseteq B$.

(viii) $(f \circ g)^{-1}(U) = g^{-1}\left(f^{-1}(U)\right)$.

Proof. (i) Omited.

(ii) Omited.

(iii) Omited.

(iv) Omited.

(v) Omited.

(vi) On the one hand,

$$f\left(A \cap f^{-1}(B)\right) \subseteq f(A) \cap f\left(f^{-1}(B)\right) \subseteq f(A) \cap B.$$

On the other hand, if $y \in f(A) \cap B$, then there exists $x \in A$ such that $f(x) = y$. Since $f(x) \in B$, we have $x \in f^{-1}(B)$, which implies $x \in A \cap f^{-1}(B)$. Therefore, $y \in f\left(A \cap f^{-1}(B)\right)$. Hence, $f(A) \cap B \subseteq f\left(A \cap f^{-1}(B)\right)$.

(vii)

$$A \subseteq f^{-1}(B) \implies f(A) \subseteq f(f^{-1}(B)) \subseteq B, \quad f(A) \subseteq B \implies A \subseteq f^{-1}(f(A)) \subseteq f^{-1}(B).$$

(viii)

$$\begin{aligned} x \in (f \circ g)^{-1}(U) &\iff (f \circ g)(x) \in U \\ &\iff f(g(x)) \in U \\ &\iff g(x) \in f^{-1}(U) \\ &\iff x \in g^{-1}(f^{-1}(U)). \end{aligned}$$

□

Proposition 1.3.2 Equivalent Characterization of Injections

Let $f : X \to Y$ be a map. The following are equivalent:

(i) f is injective.

(ii) f has a left inverse: there exists a map $h : Y \to X$ such that $h \circ f = \mathrm{id}_X$.

(iii) f is left-cancellable: if $f \circ g_1 = f \circ g_2$, then $g_1 = g_2$.

Proposition 1.3.3 Equivalent Characterization of Surjections

Let $f : X \to Y$ be a map. The following are equivalent:

(i) f is surjective.

(ii) f has a right inverse: there exists a map $h : Y \to X$ such that $f \circ h = \mathrm{id}_Y$.

(iii) f is right-cancellable: if $g_1 \circ f = g_2 \circ f$, then $g_1 = g_2$.

Proposition 1.3.4

Suppose $f : X \to Y$ and $g : Y \to Z$ are maps. We have

(i) If $g \circ f$ is injective, then f is injective.

(ii) If $g \circ f$ is surjective, then g is surjective.

1.4 Grothendieck Universe

Definition 1.4.1 Grothendieck Universe

A **Grothendieck universe** is a set $\mathscr{U}$ such that

(i) $\mathscr{U}$ is transitive: $\forall x \in \mathscr{U}, \forall y \in x,\ (y \in \mathscr{U})$. Or equivalently, $\forall x \in \mathscr{U}, x \subseteq \mathscr{U}$.

(ii) $\mathscr{U}$ is closed under power set: $\forall x \in \mathscr{U}, \mathscr{P}(x) \in \mathscr{U}$.

(iii) $\mathscr{U}$ is closed under union: $\forall x \in \mathscr{U}, \bigcup x \in \mathscr{U}$.

(iv) $\mathscr{U}$ is closed under replacement: $\forall x \in \mathscr{U}, \forall f \in \mathrm{Hom}(x, \mathscr{U}), f(x) \in \mathscr{U}$.

(v) $\mathscr{U}$ contains all the natural numbers: $\mathbb{N} \in \mathscr{U}$.

Definition 1.4.2 $\mathscr{U}$-Small Set

Let $\mathscr{U}$ be a Grothendieck universe. A set X is called a **$\mathscr{U}$-small set** if there exists $Y \in \mathscr{U}$ such that X and Y have the same cardinality.

Chapter 2

Category Theory

2.1 Category

Definition 2.1.1 Small Category and Locally Small Category

Suppose $\mathscr{U}$ is a Grothendieck universe and C is a category. We say

- C is **locally $\mathscr{U}$-small** if $\mathrm{Hom}_{\mathsf{C}}(X, Y)$ is a $\mathscr{U}$-small set for all $X, Y \in \mathrm{Ob}(\mathsf{C})$.
- C is **$\mathscr{U}$-small** if C is locally $\mathscr{U}$-small and $\mathrm{Ob}(\mathsf{C})$ is a $\mathscr{U}$-small set,

We can simply say C is **small** or **locally small** if the choice of $\mathscr{U}$ can be inferred from the context.

Definition 2.1.2 Isomorphism of Categories

Suppose C and D are two categories. A **functor** $F : \mathsf{C} \to \mathsf{D}$ is called an **isomorphism** if there exists a functor $G : \mathsf{D} \to \mathsf{C}$ such that $F \circ G = \mathrm{id}_{\mathsf{D}}$ and $G \circ F = \mathrm{id}_{\mathsf{C}}$. In this case, we say C and D are **isomorphic** and write $\mathsf{C} \cong \mathsf{D}$.

Definition 2.1.3 Section of a Morphism

A **section** of a morphism $f : E \to X$ in some category is a right-inverse of f, i.e. a morphism $\sigma : X \to E$ such that

$$f \circ \sigma : X \xrightarrow{\sigma} E \xrightarrow{f} X$$

equals id_X.

Definition 2.1.4 Retraction of a Morphism

A **retraction** of a morphism $f : S \to X$ in some category is a left-inverse of f, i.e. a morphism $\rho : X \to S$ such that

$$\rho \circ f : S \xrightarrow{f} X \xrightarrow{\rho} S$$

equals id_S.

Definition 2.1.5 Category of Categories

$\mathscr{U}$-Cat is defined as a category whose objects are all $\mathscr{U}$-small categories and morphisms are all functors between small categories.
$\mathscr{U}$-CAT is defined as a category whose objects are all locally $\mathscr{U}$-small categories and morphisms are all functors between locally small categories.

Proposition 2.1.6 Size of Functor Category

Suppose C, D are two categories.

- If C and D are small, then $[\mathsf{C}, \mathsf{D}]$ is small.
- If C is small and D is locally small, then $[\mathsf{C}, \mathsf{D}]$ is locally small.
- If C and D are locally small, then $[\mathsf{C}, \mathsf{D}]$ is generally not locally small.

Suppose C_i and D_i are locally $\mathscr{U}_i$-small categories, and that c_i and d_i are $\mathscr{U}_i$-small categories. We have the following table

Category	$\mathscr{U}_1$-Cat	$\mathscr{U}_1$-CAT	$\mathscr{U}_2$-CAT
Object	$[\mathsf{c}_1, \mathsf{d}_1]$	$\mathscr{U}_1$-Set $\mathscr{U}_1$-Cat $[\mathsf{c}_1, \mathsf{D}_1]$	$\mathscr{U}_2$-Set $[\mathsf{C}_1, \mathsf{D}_1]$

Definition 2.1.7 Subcategory

Suppose C is a category. A **subcategory** D of C is a category such that

- $\mathrm{Ob}(\mathsf{D}) \subseteq \mathrm{Ob}(\mathsf{C})$.
- For any $X, Y \in \mathrm{Ob}(\mathsf{D})$, $\mathrm{Hom}_{\mathsf{D}}(X, Y) \subseteq \mathrm{Hom}_{\mathsf{C}}(X, Y)$.
- For any $X \in \mathrm{Ob}(\mathsf{D})$, the identity morphism id_X of D is the same as the identity morphism id_X of C.
- For any $X, Y, Z \in \mathrm{Ob}(\mathsf{D})$ and $g \in \mathrm{Hom}_{\mathsf{D}}(X, Y)$, $f \in \mathrm{Hom}_{\mathsf{D}}(Y, Z)$, $f \circ_{\mathsf{D}} g = f \circ_{\mathsf{C}} g$.

A subcategory D of C is called a **full subcategory** if for any $X, Y \in \mathrm{Ob}(\mathsf{D})$, $\mathrm{Hom}_{\mathsf{D}}(X, Y) = \mathrm{Hom}_{\mathsf{C}}(X, Y)$.

There is a looser way to think about a subcategory: D is a subcategory of C if there exists a fully faithful functor $F : \mathsf{D} \to \mathsf{C}$ that is injective on objects.

Example 2.1.1 Examples of Full Subcategories

Here are some examples of full subcategories:

- $\mathsf{Ab} \subseteq \mathsf{Grp} \subseteq \mathsf{Mon}$
- $\mathsf{Field} \subseteq \mathsf{CRing} \subseteq \mathsf{Ring}$
- K-$\mathsf{Vect} \subseteq K$-$\mathsf{Mod}$
- R-$\mathsf{CAlg} \subseteq R$-$\mathsf{Alg}$

Definition 2.1.8 Opposite Category

Suppose C is a category. The **opposite category** C^{op} is defined as follows

- Objects: $\mathrm{Ob}(\mathsf{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathsf{C})$
- Morphisms: $\mathrm{Hom}_{\mathsf{C}^{\mathrm{op}}}(X, Y) = \mathrm{Hom}_{\mathsf{C}}(Y, X)$
- Composition: $f \circ_{\mathsf{C}^{\mathrm{op}}} g = g \circ_{\mathsf{C}} f$
- Identity: $\mathrm{id}_{\mathsf{C}^{\mathrm{op}}} = \mathrm{id}_{\mathsf{C}}$

It is easy to see that $(\mathsf{C}^{\mathrm{op}})^{\mathrm{op}} = \mathsf{C}$.

Definition 2.1.9 Opposite Functor

Suppose C and D are two categories and $F : \mathsf{C} \to \mathsf{D}$ is a functor. The **opposite functor** $F^{\mathrm{op}} : \mathsf{C}^{\mathrm{op}} \to \mathsf{D}^{\mathrm{op}}$

is defined by

$$\begin{array}{ccc} \mathsf{C}^{\mathrm{op}} & & \mathsf{D}^{\mathrm{op}} \\ X & & F(X) \\ {\scriptstyle f}\downarrow & \overset{F^{\mathrm{op}}}{\rightsquigarrow} & \downarrow{\scriptstyle F(f)} \\ Y & & F(Y) \end{array}$$

It is easy to see that $(F^{\mathrm{op}})^{\mathrm{op}} = F$.

Example 2.1.2

Define a functor ${}^{\mathrm{op}} : \mathsf{CAT} \to \mathsf{CAT}$ as follows

$$\begin{array}{ccc} \mathsf{CAT} & & \mathsf{CAT} \\ \mathsf{C} & & \mathsf{C}^{\mathrm{op}} \\ {\scriptstyle F}\downarrow & \overset{{}^{\mathrm{op}}}{\rightsquigarrow} & \downarrow{\scriptstyle F^{\mathrm{op}}} \\ \mathsf{D} & & \mathsf{D}^{\mathrm{op}} \end{array}$$

The functor ${}^{\mathrm{op}}$ is an involution, i.e. ${}^{\mathrm{op}} \circ {}^{\mathrm{op}} = \mathrm{id}_{\mathsf{CAT}}$. Hence ${}^{\mathrm{op}} \in \mathrm{Aut}(\mathsf{CAT})$.

Definition 2.1.10 Hom Functors

Let C be a locally small category. We can define a functor $\mathrm{Hom}_{\mathsf{C}}(-,-)$ as follows

$$\begin{array}{ccccc} \mathsf{C}^{\mathrm{op}} \times \mathsf{C} & & & & \mathsf{Set} \\ (X_1, Y_1) & & & & \mathrm{Hom}_{\mathsf{C}}(X_1, Y_1) \ni h \\ {\scriptstyle (f,g)}\downarrow & & \overset{\mathrm{Hom}_{\mathsf{C}}(-,-)}{\rightsquigarrow} & & \downarrow{\scriptstyle f^* \circ g_*} \\ (X_2, Y_2) & & & & \mathrm{Hom}_{\mathsf{C}}(X_2, Y_2) \ni g \circ h \circ f \end{array}$$

By partial application, we obtain the following two functors:

- $\mathrm{Hom}_{\mathsf{C}}(X,-) : \mathsf{C} \to \mathsf{Set}$

$$\begin{array}{ccccc} \mathsf{C} & & & & \mathsf{Set} \\ Y_1 & & & & \mathrm{Hom}_{\mathsf{C}}(X, Y_1) \ni h \\ {\scriptstyle g}\downarrow & & \overset{\mathrm{Hom}_{\mathsf{C}}(X,-)}{\rightsquigarrow} & & \downarrow{\scriptstyle g_*} \\ Y_2 & & & & \mathrm{Hom}_{\mathsf{C}}(X, Y_2) \ni g \circ h \end{array}$$

  where g_* is called **pushforward by** g.

- $\mathrm{Hom}_{\mathsf{C}}(-,Y) : \mathsf{C}^{\mathrm{op}} \to \mathsf{Set}$

$$\begin{array}{ccccc} \mathsf{C}^{\mathrm{op}} & & & & \mathsf{Set} \\ X_1 & & & & \mathrm{Hom}_{\mathsf{C}}(X_1, Y) \ni h \\ {\scriptstyle f}\downarrow & & \overset{\mathrm{Hom}_{\mathsf{C}}(-,Y)}{\rightsquigarrow} & & \downarrow{\scriptstyle f^*} \\ X_2 & & & & \mathrm{Hom}_{\mathsf{C}}(X_2, Y) \ni h \circ f \end{array}$$

  where f^* is called **pullback by** f.

Proposition 2.1.11 Natural Isomorphism $[\mathsf{C},\mathsf{D}]^{\mathrm{op}} \cong [\mathsf{C}^{\mathrm{op}},\mathsf{D}^{\mathrm{op}}]$

We have a natural isomorphism $[\mathsf{C},\mathsf{D}]^{\mathrm{op}} \cong [\mathsf{C}^{\mathrm{op}},\mathsf{D}^{\mathrm{op}}]$. The isomorphism is given by the functor $O_{\mathsf{C},\mathsf{D}} : [\mathsf{C},\mathsf{D}]^{\mathrm{op}} \to [\mathsf{C}^{\mathrm{op}},\mathsf{D}^{\mathrm{op}}]$ defined as follows

$$\begin{array}{ccc} [\mathsf{C},\mathsf{D}]^{\mathrm{op}} & & [\mathsf{C}^{\mathrm{op}},\mathsf{D}^{\mathrm{op}}] \\ F & & F^{\mathrm{op}} \\ \theta \Downarrow & \overset{O_{\mathsf{C},\mathsf{D}}}{\rightsquigarrow} & \Downarrow \theta^{\mathrm{op}} \\ G & & G^{\mathrm{op}} \end{array} \qquad \begin{array}{ccc} F^{\mathrm{op}}(X) & \xrightarrow{F^{\mathrm{op}}(f)} & F^{\mathrm{op}}(Y) \\ {\scriptstyle\theta_X}\downarrow & & \downarrow{\scriptstyle\theta_Y} \\ G^{\mathrm{op}}(X) & \xrightarrow[G^{\mathrm{op}}(f)]{} & G^{\mathrm{op}}(Y) \end{array}$$

The inverse of $O_{\mathsf{C},\mathsf{D}}$ is $O^{\mathrm{op}}_{\mathsf{C}^{\mathrm{op}},\mathsf{D}^{\mathrm{op}}}$. The naturality means the following diagram commutes

$$\begin{array}{ccc} [\mathsf{C}_1,\mathsf{D}_1]^{\mathrm{op}} & \xrightarrow{O_{\mathsf{C}_1,\mathsf{D}_1}} & [\mathsf{C}_1^{\mathrm{op}},\mathsf{D}_1^{\mathrm{op}}] \\ {\scriptstyle(S^*T_*)^{\mathrm{op}}}\downarrow & & \downarrow{\scriptstyle(S^{\mathrm{op}})^*\circ(T^{\mathrm{op}})_*} \\ [\mathsf{C}_2,\mathsf{D}_2]^{\mathrm{op}} & \xrightarrow{O_{\mathsf{C}_2,\mathsf{D}_2}} & [\mathsf{C}_2^{\mathrm{op}},\mathsf{D}_2^{\mathrm{op}}] \end{array}$$

Proposition 2.1.12 Opposite Preserves Products, Functors, and Slices

- Opposite preserves products: $(\mathsf{C}\times\mathsf{D})^{\mathrm{op}} \cong \mathsf{C}^{\mathrm{op}}\times\mathsf{D}^{\mathrm{op}}$.
- Opposite preserves functors: $[\mathsf{C},\mathsf{D}]^{\mathrm{op}} \cong [\mathsf{C}^{\mathrm{op}},\mathsf{D}^{\mathrm{op}}]$.
- Opposite preserves slices: $(F\downarrow G)^{\mathrm{op}} \cong (G^{\mathrm{op}}\downarrow F^{\mathrm{op}})$.

Definition 2.1.13 Product Category

Let C and D be categories. The **product category** $\mathsf{C}\times\mathsf{D}$ is defined as follows

- Objects: $\mathrm{Ob}(\mathsf{C}\times\mathsf{D}) = \mathrm{Ob}(\mathsf{C})\times\mathrm{Ob}(\mathsf{D})$.
- Morphisms: $\mathrm{Hom}_{\mathsf{C}\times\mathsf{D}}((C,D),(C',D')) = \mathrm{Hom}_{\mathsf{C}}(C,C')\times\mathrm{Hom}_{\mathsf{D}}(D,D')$.
- Composition: $(f',g')\circ(f,g) = (f'\circ f, g'\circ g)$.
- Identity: $\mathrm{id}_{(C,D)} = (\mathrm{id}_C,\mathrm{id}_D)$.

Definition 2.1.14 Initial Object

Let C be a category. An object $c\in\mathrm{Ob}(\mathsf{C})$ is called an **initial object** if for any object $X\in\mathrm{Ob}(\mathsf{C})$, there exists a unique morphism $c\to X$, or equivalently, $\mathrm{Hom}_{\mathsf{C}}(c,X)$ is a singleton set.

Definition 2.1.15 Terminal Object

Let C be a category. An object $c\in\mathrm{Ob}(\mathsf{C})$ is called a **terminal object** or **final object** if for any object $X\in\mathrm{Ob}(\mathsf{C})$, there exists a unique morphism $X\to c$, or equivalently, $\mathrm{Hom}_{\mathsf{C}}(X,c)$ is a singleton set.

Proposition 2.1.16

Let C be a category. If $c\in\mathrm{Ob}(\mathsf{C})$ is an initial (or terminal) object then any object isomorphic to c is also an initial (or terminal) object.

Proof. Suppose $c\in\mathrm{Ob}(\mathsf{C})$ is an initial object and $c'\in\mathrm{Ob}(\mathsf{C})$ is isomorphic to c. Then there exists an isomorphism $f: c\to c'$. For any object $X\in\mathrm{Ob}(\mathsf{C})$, there exists a unique morphism $g: c\to X$. Hence there exists a morphism

$c' \to X$ given by $g \circ f^{-1}$. We assert $\mathrm{Hom}_{\mathsf{C}}(c', X) = g \circ f^{-1}$. If there exists a morphism $h : c' \to X$, then $h \circ f : c \to X$ is morphism. $\mathrm{Hom}_{\mathsf{C}}(c, X) = g$ forces $h \circ f = g$, which implies $h = g \circ f^{-1}$. Hence c' is an initial object. The proof for terminal object is similar. □

Definition 2.1.17 Zero Object

Let C be a category. An object $0 \in \mathrm{Ob}(\mathsf{C})$ is called a **zero object** if it is both initial and terminal. In other words, 0 is a zero object if for any object $X \in \mathrm{Ob}(\mathsf{C})$, there exists unique morphisms $0 \to X$ and $X \to 0$. These morphisms are the **zero morphisms** of C.

Definition 2.1.18 Evaluation Functor

Let A be a small category and C be a category. The **evaluation functor** $\mathrm{ev} : \mathsf{A} \times [\mathsf{A}, \mathsf{C}] \to \mathsf{C}$ is defined by

$$\begin{array}{ccc} \mathsf{A} \times [\mathsf{A}, \mathsf{C}] & & \mathsf{C} \\ (X, F) & & F(X) \\ {\scriptstyle f\times\theta}\downarrow & \rightsquigarrow^{\mathrm{ev}} & \downarrow{\scriptstyle \theta_Y \circ F(f) = G(f) \circ \theta_X} \\ (Y, G) & & G(Y) \end{array}$$

From the following diagram, we can see that ev preserves composition.

$$\begin{array}{ccccc} F(X) & \xrightarrow{F(f)} & F(Y) & \xrightarrow{F(g)} & F(Z) \\ {\scriptstyle \theta_X}\downarrow & \searrow^{\mathrm{ev}(f\times\theta)} & \downarrow{\scriptstyle \theta_Y} & & \downarrow{\scriptstyle \theta_Z} \\ G(X) & \xrightarrow[G(f)]{} & G(Y) & \xrightarrow{G(g)} & G(Z) \\ {\scriptstyle \eta_X}\downarrow & & {\scriptstyle \eta_Y}\downarrow & \searrow^{\mathrm{ev}(g\times\eta)} & \downarrow{\scriptstyle \eta_Z} \\ H(X) & \xrightarrow[H(f)]{} & H(Y) & \xrightarrow[H(g)]{} & H(Z) \end{array}$$

If we fix $X \in \mathsf{A}$, then we have a functor $\mathrm{ev}_X : [\mathsf{A}, \mathsf{C}] \to \mathsf{C}$ defined by $\mathrm{ev}_X(F) = F(X)$. This functor is called the **evaluation functor at** X.

Definition 2.1.19 Constant Functor

Suppose C, D be categories and $d \in \mathrm{Ob}(\mathsf{D})$. The **constant functor** $\boxslash d : \mathsf{C} \to \mathsf{D}$ is defined by

$$\begin{array}{ccc} \mathsf{C} & & \mathsf{D} \\ x & & d \\ {\scriptstyle f}\downarrow & \rightsquigarrow^{\boxslash d} & \downarrow{\scriptstyle \mathrm{id}_d} \\ y & & d \end{array}$$

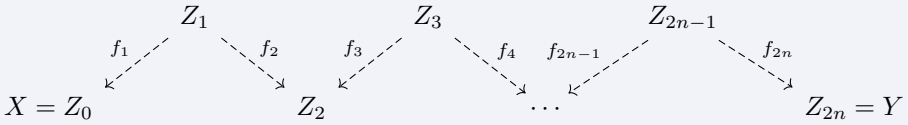
Definition 2.1.20 Diagonal Functor

Suppose J, C are categories. The **diagonal functor** $\boxslash : \mathsf{C} \to [\mathsf{J}, \mathsf{C}]$ is defined by

$$\begin{array}{ccccc} \mathsf{C} & & [\mathsf{J}, \mathsf{C}] & & \\ x & & \boxslash x & & x \xrightarrow{\mathrm{id}_x} x \\ {\scriptstyle f}\downarrow & \rightsquigarrow^{\boxslash} & \Downarrow{\scriptstyle f_\bullet} & & {\scriptstyle f}\downarrow \quad\quad \downarrow{\scriptstyle f} \\ y & & \boxslash y & & y \xrightarrow[\mathrm{id}_y]{} y \end{array}$$

Definition 2.1.21 Connected Category

A category C is **connected** if it is nonempty and for any pair of objects $X, Y \in \mathrm{Ob}(\mathsf{C})$, there exists a zigzag of morphisms $(f_1, f_2, \cdots, f_{2n})$ connecting X and Y as follows



Definition 2.1.22 Comma Category

Suppose that A, B, and C are categories, and S and T (for source and target) are functors:

$$\mathsf{A} \xrightarrow{S} \mathsf{C} \xleftarrow{T} \mathsf{B}$$

We can form the comma category $(S \downarrow T)$ as follows:

- The objects are all triples (A, B, h) with $A \in \mathrm{Ob}(\mathsf{A})$, $B \in \mathrm{Ob}(\mathsf{B})$, and $h : S(A) \to T(B)$ a morphism in C.
- The morphisms from (A, B, h) to (A', B', h') are all pairs (f, g) where $f : A \to A'$ and $g : B \to B'$ are morphisms in A and B respectively, such that the following diagram commutes:

$$\begin{array}{ccc} S(A) & \xrightarrow{h} & T(B) \\ {\scriptstyle S(f)}\downarrow & & \downarrow{\scriptstyle T(g)} \\ S(A') & \xrightarrow[h']{} & T(B') \end{array}$$

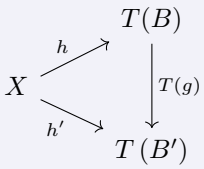
  Morphisms are composed by taking $(f', g') \circ (f, g)$ to be $(f' \circ f, g' \circ g)$, whenever the latter expression is defined. The identity morphism on an object (A, B, h) is $(\mathrm{id}_A, \mathrm{id}_B)$.

Definition 2.1.23 Universal Morphism

Suupose A, B, and C are categories and $X \in \mathrm{Ob}(\mathsf{C})$. The comma category $(\boxslash X \downarrow T)$ for the following pair of functors

$$\mathbb{1} \xrightarrow{\boxslash X} \mathsf{C} \xleftarrow{T} \mathsf{B}$$

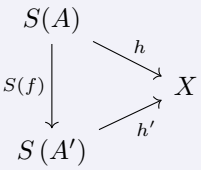
can be written as $(X \downarrow T)$ for short. Morphisms in $(X \downarrow \mathsf{B})$ can be simplified to commutative triangles



We say $\left(Y, X \xrightarrow{u} T(Y)\right)$ is a **universal morphism from X to T** if it is initial in $(X \downarrow T)$.
Similarly, the comma category $(\mathsf{A} \downarrow \boxslash X)$ for the following pair of functors

$$\mathsf{A} \xrightarrow{S} \mathsf{C} \xleftarrow{\boxslash X} \mathbb{1}$$

can be written as $(\mathsf{A} \downarrow X)$ for short. Morphisms in $(\mathsf{A} \downarrow X)$ can be simplified to commutative triangles



We say $\left(Y, S(Y) \xrightarrow{u} X\right)$ is a **universal morphism from S to X** if it is terminal in $(\mathsf{A} \downarrow X)$.

Example 2.1.3 Disc Functor

Given a set X, we can define a functor $\mathsf{Disc} : \mathsf{Set} \to \mathsf{Cat}$ as follows

$$\begin{array}{ccc} \mathsf{Set} & & \mathsf{Cat} \\ X & & \mathsf{Disc}(X) \\ {\scriptstyle f}\downarrow & \rightsquigarrow^{\mathsf{Disc}} & \downarrow{\scriptstyle \mathsf{Disc}(f)} \\ Y & & \mathsf{Disc}(Y) \end{array}$$

where $\mathsf{Disc}(X)$ is the discrete category with object set $\mathrm{Ob}\left(\mathsf{Disc}(X)\right) = X$ and morphism set

$$\mathrm{Hom}_{\mathsf{Disc}(X)}(x, y) = \begin{cases} \{\mathrm{id}_x\} & \text{if } x = y, \\ \varnothing & \text{if } x \neq y, \end{cases}$$

and $\mathsf{Disc}(f)$ is the functor defined by $\mathsf{Disc}(f)(x) = f(x)$ and $\mathsf{Disc}(f)(\mathrm{id}_x) = \mathrm{id}_{f(x)}$ for each $x \in X$.
It is easy to check that the functor Disc is fully faithful.

Definition 2.1.24 Grothendieck Construction

Let C be a category and let $F : \mathsf{C} \to \mathsf{Cat}$ be a functor from any small category to the category of small categories. The **Grothendieck construction** of F is a category $\int_{\mathsf{C}} F$ (also written $\Gamma(F)$) defined as follows:

- Objects are pairs (A, a) where $A \in \mathrm{Ob}(\mathsf{C})$ and $a \in F(A)$.
- Morphisms $(A, a) \to (B, b)$ are pairs (f, g) where $f : A \to B$ is a morphism in C and $g : F(f)(a) \to b$ is a morphism in $F(B)$.

The composition of morphisms is defined as follows:

$$(f', g') \circ (f, g) = (f' \circ f, g' \circ (F(f')(g)))$$

where $F(f')(g) : F(f')(F(f)(a)) \to F(f')(b)$ is the morphism induced by g under the functor $F(f')$.

Definition 2.1.25 Category of Elements

Let C be a category and let $F : \mathsf{C} \to \mathsf{Set}$ be a functor. The **category of elements of F** is the the comma category $(\{*\} \downarrow F)$ where functors are illustrated as follows

$$\mathbb{1} \xrightarrow{\boxtimes\{*\}} \mathsf{Set} \xleftarrow{F} \mathsf{C}$$

This category is denoted by $\int_{\mathsf{C}} F$ and can be explicitly described as follows

- Objects are pairs (A, a) where $A \in \mathrm{Ob}(\mathsf{C})$ and $a \in F(A)$.
- Morphisms $(A, a) \to (B, b)$ are arrows $f : A \to B$ of C such that $F(f)(a) = b$.

The category of elements of F is naturally equipped with a projection functor $\pi : \int_{\mathsf{C}} F \to \mathsf{C}$

$$\begin{array}{ccc} \int_{\mathsf{C}} F & & \mathsf{C} \\ (A, a) & & A \\ {\scriptstyle f}\downarrow & \rightsquigarrow^{\pi} & \downarrow{\scriptstyle f} \\ (B, b) & & B \end{array}$$

By viewing sets in Set as discrete categories, we have an inclusion $\mathsf{Set} \hookrightarrow \mathsf{Cat}$. Hence the category of elements of F is a special case of the Grothendieck construction.

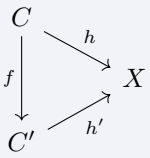
2.1.1 Slice Category

Definition 2.1.26 Slice Category

Suppose C is a category and $X \in \mathrm{Ob}(\mathsf{C})$. The **slice category** or **over category** (C/X) is the comma category $(\mathrm{id}_{\mathsf{C}} \downarrow X)$, where functors are illustrated as follows

$$\mathsf{C} \xrightarrow{\mathrm{id}_{\mathsf{C}}} \mathsf{C} \xleftarrow{\boxslash X} \mathbb{1}$$

Morphims in (C/X) are commutative triangles shown as follows



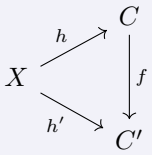
If C has a terminal object $\top_{\mathsf{C}}$, then the slice category $(\mathsf{C}/\top_{\mathsf{C}})$ is isomorphic to C.

Definition 2.1.27 Coslice Category

Suppose C is a category and $X \in \mathrm{Ob}(\mathsf{C})$. The **coslice category** (X/C) is the comma category $(X \downarrow \mathrm{id}_{\mathsf{C}})$, where functors are illustrated as follows

$$\mathbb{1} \xrightarrow{\boxslash} \mathsf{C} \xleftarrow{\mathrm{id}_{\mathsf{C}}} \mathsf{C}$$

Morphims in (X/C) are commutative triangles shown as follows



If C has an initial object $\varnothing$, then the coslice category $(\varnothing/\mathsf{C})$ is isomorphic to C.

Definition 2.1.28 Category of Pointed Objects

Suppose C is a category with terminal object $\bullet$. The coslice category $(\bullet/\mathsf{C})$ is called the **category of pointed objects** of C and is denoted by $\mathsf{C}_{\bullet}$.

Proposition 2.1.29 Limits and Colimits in Slice Categories

Let C be a category. Fix some object $X \in \mathrm{Ob}\,(\mathsf{C})$. Then

(i) The forgetful functor $U : \mathsf{C}/X \to \mathsf{C}$ strictly creates all colimits. If $\varinjlim(U \circ F)$ exists for some diagram $F : \mathsf{J} \to X/\mathsf{C}$, then $\varinjlim F$ exists and we have natural isomorphism

$$U\left(\varinjlim F\right) \cong \varinjlim(U \circ F).$$

(ii) The forgetful functor $U : \mathsf{C}/X \to \mathsf{C}$ strictly creates all connected limits. If $\varprojlim(U \circ F)$ exists for some connected diagram $F : \mathsf{J} \to \mathsf{C}/X$, then $\varprojlim F$ exists and we have natural isomorphism

$$U\left(\varprojlim F\right) \cong \varprojlim(U \circ F).$$

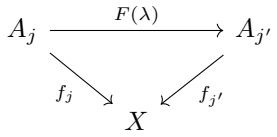
(iii) If

$$\left(\varprojlim U \circ F\right) \times_{\varprojlim_{j\in \mathsf{J}} X} X$$

exists for some diagram $F : \mathsf{J} \to \mathsf{C}/X$, then $\varprojlim F$ exists and can be given as

$$\left(\varprojlim U \circ F\right) \times_{\varprojlim_{j\in \mathsf{J}} X} X \longrightarrow X.$$

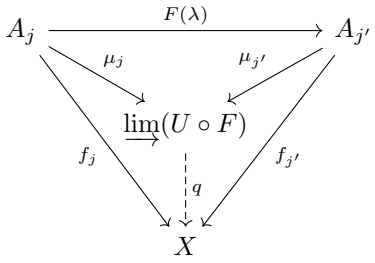
Proof. (i) Let $F : \mathsf{J} \to \mathsf{C}/X$ be a diagram. Write $F(j) = (f_j : A_j \to X)$ for each object $j \in \mathrm{Ob}(\mathsf{J})$. For each morphism $\lambda : j \to j'$ in J, we have $F(\lambda) : A_j \to A_{j'}$ such that the following diagram commutes



Lift the Limit Cocone. Suppose the colimit of $U \circ F$ exists and the cocone

$$C := \left(\varinjlim U \circ F, \left(\mu_j : A_j \longrightarrow \varinjlim U \circ F\right)_{j\in \mathrm{Ob}(\mathsf{J})}\right)$$

is initial in $\mathsf{Cocone}\,(U \circ F, \mathsf{C})$. Then by the universal property of colimits, there exists a unique morphism $q : \varinjlim(U \circ F) \to X$ such that for each morphism $\lambda : j \to j'$ in J the following diagram commutes



This commutative diagram implies

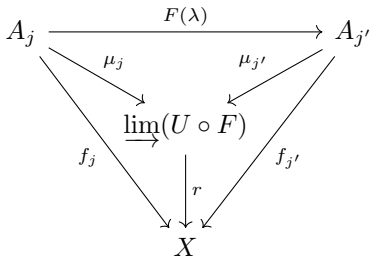
$$Q := \left(q : \varinjlim(U \circ F) \longrightarrow X, \left(\mu_j : A_j \longrightarrow \varinjlim U \circ F\right)_{j\in \mathrm{Ob}(\mathsf{J})}\right)$$

is a cocone in $\mathsf{Cocone}\,(F, \mathsf{C}/X)$ and the pushforward cocone U_*Q is exactly C.

Uniqueness of Lift. To show Q is the unique cocone in $\mathsf{Cocone}\,(F, \mathsf{C}/X)$ such that $U_*Q = C$, let

$$R = \left(r : \varinjlim(U \circ F) \longrightarrow X, \left(\mu_j : A_j \longrightarrow \varinjlim U \circ F\right)_{j\in \mathrm{Ob}(\mathsf{J})}\right)$$

be any cocone in $\mathsf{Cocone}\,(F, \mathsf{C}/X)$ such that $U_*R = C$. The cocone condition implies for each morphism $\lambda : j \to j'$ in J the following diagram commutes

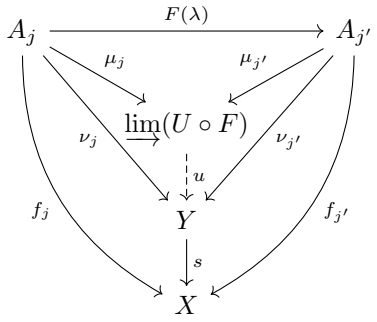


By the uniqueness part of the universal property of colimits, we have $r = q$. Hence Q is the unique cocone in $\mathsf{Cocone}\,(F, \mathsf{C}/X)$ such that $U_*Q = C$.

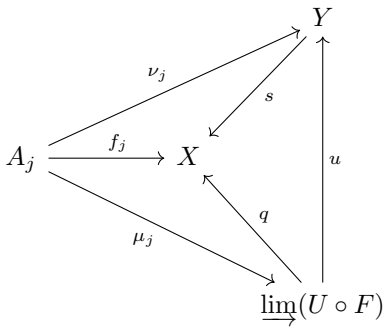
Lifted Cocone is Initial. To show Q is initial in $\mathsf{Cocone}\,(F, \mathsf{C}/X)$, let

$$S = \left(s : Y \longrightarrow X, (\nu_j : A_j \longrightarrow Y)_{j \in \mathrm{Ob}(\mathsf{J})}\right)$$

be any cocone in $\mathsf{Cocone}\,(F, \mathsf{C}/X)$. Since for each morphism $\lambda : j \to j'$ in J, the following diagram commutes

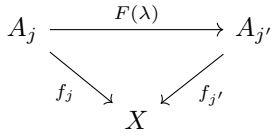


where $u : \varinjlim(U \circ F) \to Y$ is the morphism induced by the universal property of colimits such that $u \circ \mu_j = \nu_j$ for each $j \in \mathrm{Ob}(\mathsf{J})$. By the uniqueness part of the universal property of colimits, we have $s \circ u = q$. Thus we have the following commutative diagram



which implies $u : \varinjlim(U \circ F) \to Y$ is a morphism in $\mathsf{Cocoone}(F, \mathsf{C}/X)$ from Q to S. To show uniqueness of such morphism, let $u' : \varinjlim(U \circ F) \to Y$ be any morphism in $\mathsf{Cocoone}(F, \mathsf{C}/X)$ from Q to S. Then for each $j \in \mathrm{Ob}(\mathsf{J})$, we have $u' \circ \mu_j = \nu_j$. By the uniqueness part of the universal property of colimits, we have $u' = u$. Hence Q is initial in $\mathsf{Cocone}\,(F, \mathsf{C}/X)$.

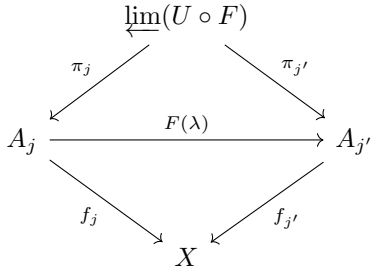
(ii) Let $F : \mathsf{J} \to \mathsf{C}/X$ be a diagram with J being connected. Write $F(j) = (f_j : A_j \to X)$ for each object $j \in \mathrm{Ob}(\mathsf{J})$. For each morphism $\lambda : j \to j'$ in J, we have $F(\lambda) : A_j \to A_{j'}$ such that the following diagram commutes



Lift the Limit Cone. Suppose the limit of $U \circ F$ exists and the cone

$$L := \left(h : \varprojlim(U \circ F), \left(\pi_j : \varprojlim(U \circ F) \to A_j\right)_{j \in \mathrm{Ob}(\mathsf{J})}\right)$$

is final in $\mathsf{Cone}\,(\mathsf{C}, U \circ F)$. Then by the universal property of limits, for each morphism $\lambda : j \to j'$ in J, the following diagram commutes



and we have

$$f_j \circ \pi_j = f_{j'} \circ \pi_{j'}.$$

Since J is connected, $f_j \circ \pi_j = f_{j'} \circ \pi_{j'}$ holds for any $j, j' \in \mathrm{Ob}(\mathsf{J})$. Since connected category is nonempty, there exists $j_0 \in \mathrm{Ob}(\mathsf{J})$. Define $h := f_{j_0} \circ \pi_{j_0}$. Then

$$H = \left(h : \varprojlim(U \circ F) \longrightarrow X, (\pi_j)_{j \in \mathrm{Ob}(\mathsf{J})}\right)$$

is a cone in $\mathsf{Cone}\,(\mathsf{C}/X, F)$ and the pushforward cone $U_* H$ is exactly L.

Uniqueness of Lift. To show H is the unique cone in $\mathsf{Cone}\,(\mathsf{C}/X, F)$ such that $U_* H = L$, let

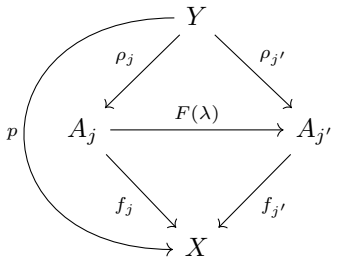
$$H' = \left(h' : \varprojlim(U \circ F) \longrightarrow X, (\pi_j)_{j \in \mathrm{Ob}(\mathsf{J})}\right)$$

be any cone in $\mathsf{Cone}\,(\mathsf{C}/X, F)$ such that $U_* H' = L$. Since $h' : \varprojlim(U \circ F) \to X$ is a morphism in C/X, we have $h' = f_{j_0} \circ \pi_{j_0} = h$. Hence $H' = H$.

Lifted Cone is Final. To show H is final in $\mathsf{Cone}\,(\mathsf{C}/X, F)$, let

$$P = \left(p : Y \longrightarrow X, (\rho_j : Y \longrightarrow A_j)_{j \in \mathrm{Ob}(\mathsf{J})}\right)$$

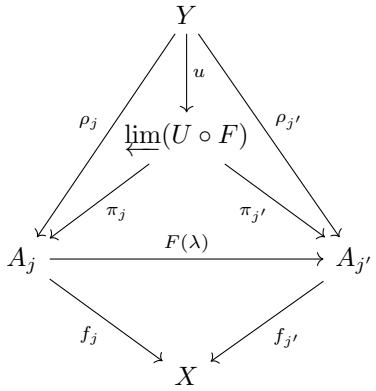
be any cone in $\mathsf{Cone}\,(\mathsf{C}/X, F)$. Since for each morphism $\lambda : j \to j'$ in J, the following diagram commutes



we see

$$(\rho_j : Y \longrightarrow A_j)_{j \in \mathrm{Ob}(\mathsf{J})}$$

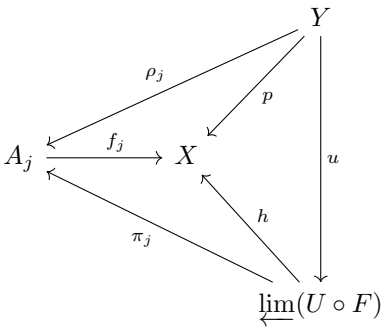
is a cone in $\mathsf{Cone}\,(\mathsf{C}, F)$. By universal property of $\varprojlim(U \circ F)$, there exists a unique morphism $u : Y \to \varprojlim(U \circ F)$ such that the following diagram commutes



for each $j \in \mathrm{Ob}(\mathsf{J})$. Since

$$h \circ u = f_{j_0} \circ \pi_{j_0} \circ u = f_{j_0} \circ \rho_{j_0} = p,$$

we see $u : Y \to \varprojlim(U \circ F)$ is a morphism in C/X such that the following diagram commutes



for each $j \in \mathrm{Ob}(\mathsf{J})$. Hence $u : Y \to \varprojlim(U \circ F)$ is a morphism in $\mathsf{Cone}\,(\mathsf{C}/X, F)$ from P to H.

If $u' : Y \to \varprojlim(U \circ F)$ is a morphism in $\mathsf{Cone}\,(\mathsf{C}/X, F)$ from P to H, then by forgetting the morphism to C, we see u' is also a morphism in $\mathsf{Cone}\,(\mathsf{C}, U \circ F)$ from

$$\left(Y, (\rho_j)_{j \in \mathrm{Ob}(\mathsf{J})}\right)$$

to

$$\left(\varprojlim(U \circ F), (\pi_j)_{j \in \mathrm{Ob}(\mathsf{J})}\right).$$

Thus we have $u' = u$ by the universal property of $\varprojlim(U \circ F)$. Therefore H is final in $\mathsf{Cone}\,(\mathsf{C}/X, F)$. □

Corollary 2.1.30 Initial and Terminal Objects in Slice Categories

Let C be a category and fix some object $X \in \mathrm{Ob}\,(\mathsf{C})$.

- If C has an initial object $\bot$, then the slice category C/X has an initial object $(\bot \to X)$.
- The slice category C/X has a terminal object $\mathrm{id}_X : X \to X$.
- If C has a terminal object $\top$, then we have a natural isomorphism of categories $\mathsf{C}/\top \cong \mathsf{C}$.

Corollary 2.1.31

Let C be a category and fix some object $X \in \mathrm{Ob}\,(\mathsf{C})$.

- If C is complete, then the slice category C/X is also complete.
- If C is cocomplete, then the slice category C/X is also cocomplete.

Proof. According to Proposition 2.1.29, the equalizers and products in C/X can be constructed from limits in C. By Theorem 2.4.31, C/X is also complete. The dual argument shows that if C is cocomplete, then C/X is also cocomplete. □

2.2 String Diagram

String diagrams are a convenient way to represent the composition of natural transformations. From top to bottom, a string diagram represents a series of vertical compositions of natural transformations.

Suppose $\varphi : F \Rightarrow G$ is a natural transformation between functors $F, G : \mathsf{C} \to \mathsf{D}$. The string diagram for φ is just the Poincare dual of its 2-cell diagram.

When we say two string diagrams are equal, we mean that the vertical compositions of natural transformations they represent are equal.

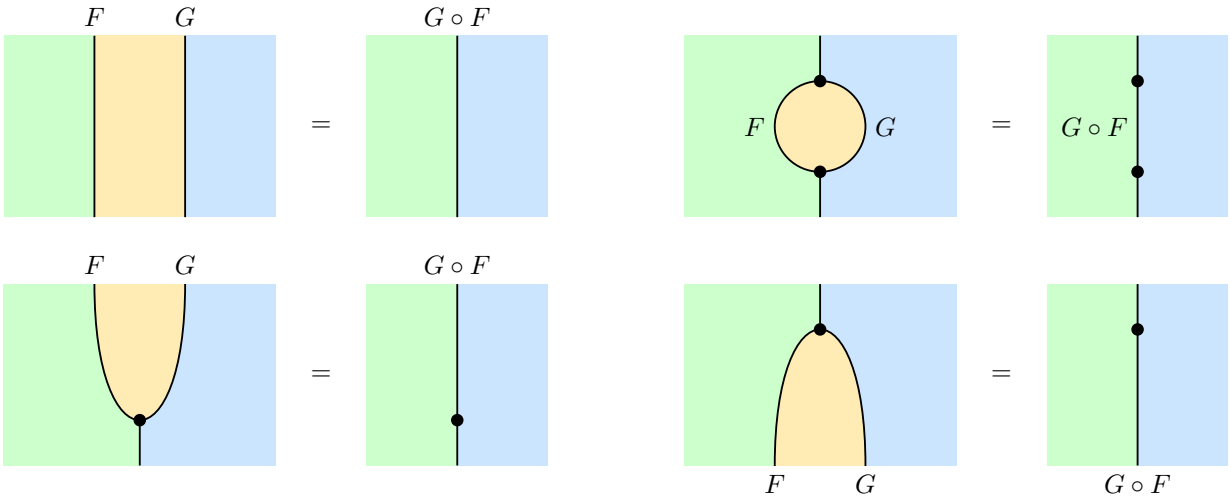
The point(0-cells), strings(1-cells), and 2-cells in a string diagram can be interpreted as follows

- 2-cells: categories. 2-cells with different colors represent different categories.
- 1-cells: functors. Each 1-cell has exactly two adjacent 2-cells. The left and right adjacent 2-cells are the domain and codomain of the functor respectively. We can think each 1-cell has two end points connected to either a natural transformation or the point at infinity ∞. If an end point is connected to ∞, then we say that it is a **free end**. The end point on the top of a string and the end point on the bottom of a string are called the **top end** and **bottom end** respectively.
- 0-cells: natural transformations. Each 0-cell has exactly two adjacent 1-cells. The top and bottom adjacent 1-cells are the domain and codomain of the natural transformation respectively.

2.2.1 Basic Operations

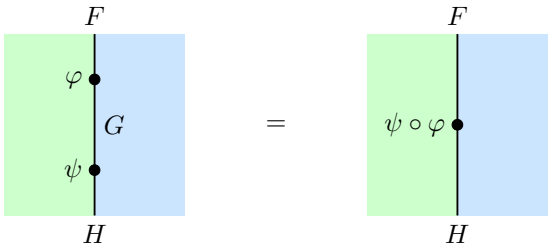
Composition of Functors

If two string $F : \mathsf{C} \to \mathsf{D}$ and $G : \mathsf{D} \to \mathsf{F}$ has the same top ends and bottom ends, then we can glue them together to form a new string $G \circ F$. Depending on whether the top ends and bottom ends are free or not, we can illustrate the following cases



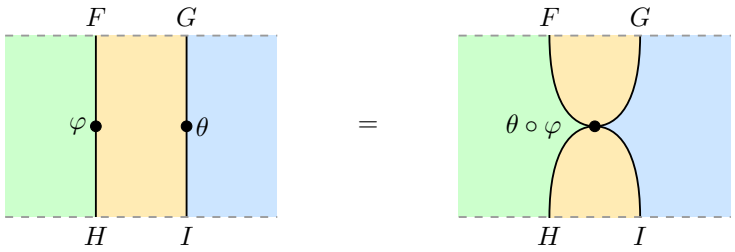
Vertical Composition

The vertical composition of natural transformations $\varphi : F \Rightarrow H$ and $\psi : G \Rightarrow I$ collapses two adjacent points in a string into one single point and "eats" the intermediate segment, which is illustrated as follows

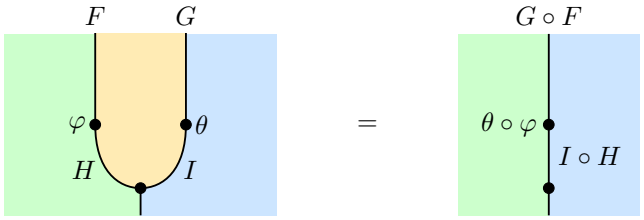


Horizontal Composition

To do horizontal composition for natural transformations $\varphi : F \Rightarrow H$ and $\theta : G \Rightarrow I$ on a horizontal line. First we can stick these two points together, which is illustrated as follows



Then we can composite the functors F and G to get a new functor $G \circ F$. Also we can composite the functors H and I to get a new functor $I \circ H$. By gluing these strings together, we get a new natural transformation $\theta \circ \varphi : G \circ F \Rightarrow I \circ H$. This is illustrated as follows

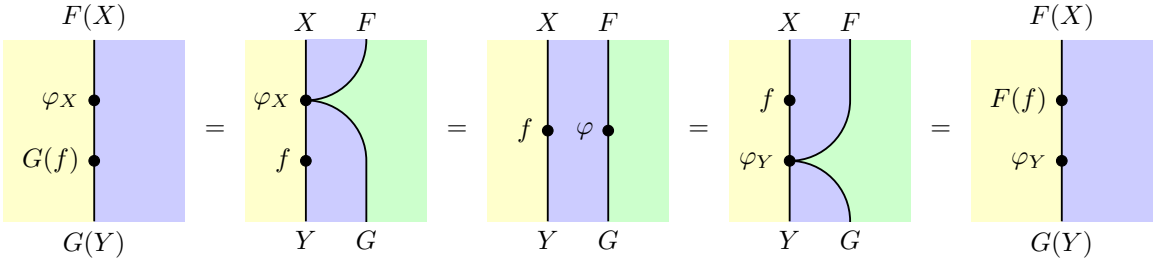


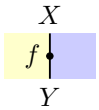
2.2.2 Morphism as Natural Transformation

If $f : X \to Y$ is a morphism in C, then the following string diagram should be understood as follows

Naturality

Suppose $\varphi : F \Rightarrow G$ is a natural transformation between functors $F, G : \mathsf{C} \to \mathsf{D}$. Then the functoriality of φ can be described by the following string diagram

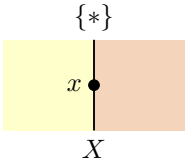


Note that appending the string diagram 

to the left of the string diagram of φ is equivalent to evaluating φ at $f : X \to Y$.

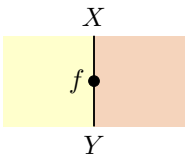
Elements of Sets

Let X be a set and $x \in X$ be an element of X. Then we represents x as a morphism $x : \{*\} \to X$ in Set, which is illustrated as follows

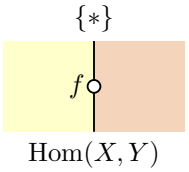


Function as Element or Morphism

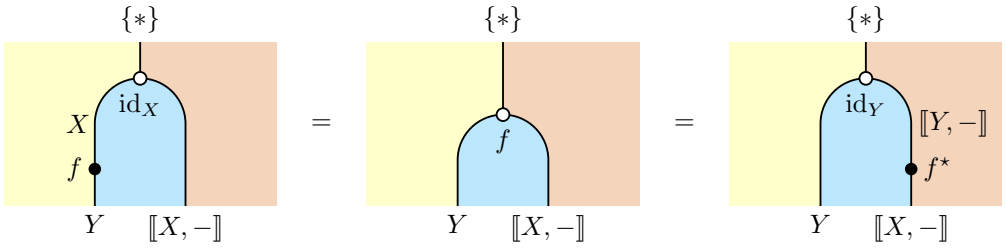
If we have a function $f : X \to Y$, then we can represent f as morphism $f : X \to Y$ in Set, which is illustrated as follows



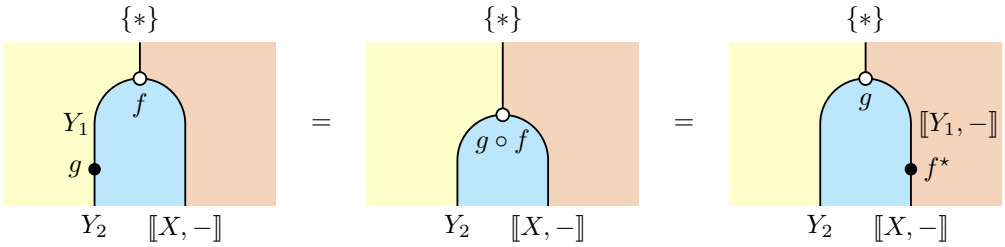
And we can also represent f as an element $f \in \mathrm{Hom}_{\mathsf{Set}}(X, Y)$, which is illustrated as follows



Then we have the following equalities for Hom functor $[\![X, -]\!] : \mathsf{C} \to \mathsf{Set}$



Generally, given $X \xrightarrow{f} Y_1 \xrightarrow{g} Y_2$ in Set, we have the following equalities



2.3 Representable Functor

Definition 2.3.1 Presheaf

Let C be a category. A **presheaf** on C is a functor $F : \mathsf{C}^{\mathrm{op}} \to \mathsf{Set}$.

Definition 2.3.2 Yoneda Embedding Functor

Let C be a category. The **Yoneda embedding functor** is the functor $Y_{\mathsf{C}} : \mathsf{C} \to [\mathsf{C}^{\mathrm{op}}, \mathsf{Set}]$ defined as follows

$$\begin{array}{ccc} \mathsf{C} & & [\mathsf{C}^{\mathrm{op}}, \mathsf{Set}] \\ Y_1 & \overset{Y_{\mathsf{C}}}{\rightsquigarrow} & \mathrm{Hom}_{\mathsf{C}}(-, Y_1) \\ {\scriptstyle g}\downarrow & & \Downarrow {\scriptstyle g_\star} \\ Y_2 & & \mathrm{Hom}_{\mathsf{C}}(-, Y_2) \end{array} \qquad \begin{array}{ccc} \mathrm{Hom}_{\mathsf{C}}(X_1, Y_1) & \xrightarrow{f^*} & \mathrm{Hom}_{\mathsf{C}}(X_2, Y_1) \\ {\scriptstyle g_*}\downarrow & & \downarrow{\scriptstyle g_*} \\ \mathrm{Hom}_{\mathsf{C}}(X_1, Y_2) & \xrightarrow[f^*]{} & \mathrm{Hom}_{\mathsf{C}}(X_2, Y_2) \end{array}$$

where the natural transformation $g_\star$ is defined pointwise as follows: $(g_\star)_X = g_*$ for any $X \in \mathrm{Ob}(\mathsf{C}^{\mathrm{op}})$. The contravariant version is $Y_{\mathsf{C}^{\mathrm{op}}} : \mathsf{C}^{\mathrm{op}} \to [\mathsf{C}, \mathsf{Set}]$, which is defined as follows

$$\begin{array}{ccc} \mathsf{C}^{\mathrm{op}} & & [\mathsf{C}, \mathsf{Set}] \\ X_1 & \overset{Y_{\mathsf{C}^{\mathrm{op}}}}{\rightsquigarrow} & \mathrm{Hom}_{\mathsf{C}}(X_1, -) \\ {\scriptstyle f}\downarrow & & \Downarrow {\scriptstyle f^*} \\ X_2 & & \mathrm{Hom}_{\mathsf{C}}(X_2, -) \end{array} \qquad \begin{array}{ccc} \mathrm{Hom}_{\mathsf{C}}(X_1, Y_1) & \xrightarrow{g_*} & \mathrm{Hom}_{\mathsf{C}}(X_1, Y_2) \\ {\scriptstyle f^*}\downarrow & & \downarrow{\scriptstyle f^*} \\ \mathrm{Hom}_{\mathsf{C}}(X_2, Y_1) & \xrightarrow[g_*]{} & \mathrm{Hom}_{\mathsf{C}}(X_2, Y_2) \end{array}$$

Here we use the fact $\mathrm{Hom}_{\mathsf{C}^{\mathrm{op}}}(-, X) = \mathrm{Hom}_{\mathsf{C}}(X, -)$.

Theorem 2.3.3 Yoneda Lemma

Let C be a locally small category. For any functor $F : \mathsf{C}^{\mathrm{op}} \to \mathsf{Set}$ and any $A \in \mathrm{Ob}(\mathsf{C})$, there is a natural bijection

$$q_{A,F} : \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}\left(\mathrm{Hom}_{\mathsf{C}}(-, A), F\right) \xrightarrow{\sim} F(A)$$
$$\left[\ \mathsf{C}^{\mathrm{op}} \ \underset{F}{\overset{\mathrm{Hom}_{\mathsf{C}}(-,A)}{\Downarrow \phi}} \ \mathsf{Set}\ \right] \longmapsto \phi_A(\mathrm{id}_A)$$

The naturality of $q_{A,F}$ means that

$$\begin{array}{ccc} \mathsf{C}^{\mathrm{op}} \times [\mathsf{C}^{\mathrm{op}}, \mathsf{Set}] & & \mathsf{Set} \\ (A_1, F_1) & & \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(\mathrm{Hom}_{\mathsf{C}}(-, A_1), F_1) \ni \phi \\ {\scriptstyle (g,\eta)}\downarrow & \overset{\mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(Y_{\mathsf{C}}(-),-)}{\rightsquigarrow} & \downarrow \\ (A_2, F_2) & & \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(\mathrm{Hom}_{\mathsf{C}}(-, A_2), F_2) \ni \eta \circ \phi \circ g_\star \end{array}$$

is a functor isomorphic to the evaluation functor

$$\begin{aligned} \mathrm{ev} : \mathsf{C}^{\mathrm{op}} \times [\mathsf{C}^{\mathrm{op}}, \mathsf{Set}] &\longrightarrow \mathsf{Set} \\ (A, F) &\longmapsto F(A) \end{aligned}$$

Covariant version

For any functor $F : \mathsf{C} \to \mathsf{Set}$ and any $A \in \mathrm{Ob}(\mathsf{C})$, there is a natural bijection

$$\mathrm{Hom}_{[\mathsf{C},\mathsf{Set}]}\left(\mathrm{Hom}_{\mathsf{C}}(A, -), F\right) \xrightarrow{\sim} F(A)$$
$$\left[\ \mathsf{C} \ \underset{F}{\overset{\mathrm{Hom}_{\mathsf{C}}(A,-)}{\Downarrow \phi}} \ \mathsf{Set}\ \right] \longmapsto \phi_A(\mathrm{id}_A)$$

Proof. We break the proof into following steps.

- ϕ **is determined by** $\phi_A(\mathrm{id}_A)$.
  Suppose $\phi : \mathrm{Hom}_{\mathsf{C}}(-, A) \Rightarrow F$ is a natural transformation. Given any morphism $f : X \to A$ in C, the naturality of ϕ gives the following commutative diagram

$$\begin{array}{ccccccc} \mathrm{id}_A & \in & \mathrm{Hom}_{\mathsf{C}}(A,A) & \xrightarrow{f^*} & \mathrm{Hom}_{\mathsf{C}}(X,A) & \ni & f \\ \downarrow & & \downarrow{\scriptstyle \phi_A} & & \downarrow{\scriptstyle \phi_X} & & \downarrow \\ \phi_A(\mathrm{id}_A) & \in & F(A) & \xrightarrow[F(f)]{} & F(X) & \ni & \phi_X(f) \end{array}$$

  Thus we see ϕ is determined by $\phi_A(\mathrm{id}_A)$ as follows

$$\phi_X(f) = F(f)(\phi_A(\mathrm{id}_A)), \quad \forall X \in \mathrm{Ob}(\mathsf{C}), \forall f \in \mathrm{Hom}_{\mathsf{C}}(X, A).$$

  This implies that the injectivity of $q_{A,F}$.

- **Construct the inverse of** $q_{A,F}$.
  Define

$$\begin{aligned} r_{A,F} : F(A) &\longrightarrow \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}\left(\mathrm{Hom}_{\mathsf{C}}\left(-, A\right), F\right) \\ u &\longmapsto \phi^u : \begin{bmatrix} \phi^u_X : \mathrm{Hom}_{\mathsf{C}}(X, A) \longrightarrow F(X) \\ f \longmapsto F(f)(u) \end{bmatrix} \end{aligned}$$

  To ensure $r_{A,F}$ is well-defined, we need to check that $r_{A,F}(u) = \phi^u$ is always a natural transformation. In fact, given any morphism $h : X_1 \to X_2$ in C, it is easy to check the following diagram commutes

$$\begin{array}{ccccccc} g & \in & \mathrm{Hom}_{\mathsf{C}}(X_2,A) & \xrightarrow{h^*} & \mathrm{Hom}_{\mathsf{C}}(X_1,A) & \ni & g \circ h \\ \downarrow & & \downarrow{\scriptstyle \phi^u_{X_2}} & & \downarrow{\scriptstyle \phi^u_{X_1}} & & \downarrow \\ F(g)(u) & \in & F(X_2) & \xrightarrow[F(h)]{} & F(X_1) & \ni & F(g \circ h)(u) \end{array}$$

  because the functoriality of F gives the identity $F(g \circ h) = F(h) \circ F(g)$.

  For any $u \in F(A)$, we have

$$\begin{aligned} \left(q_{A,F} \circ r_{A,F}\right)(u) &= q_{A,F}(\phi^u) \\ &= \phi^u_A(\mathrm{id}_A) \\ &= F(\mathrm{id}_A)(u) \\ &= \mathrm{id}_{F(A)}(u) \\ &= u, \end{aligned}$$

  which implies that $q_{A,F}$ is surjective. Therefore, $q_{A,F}$ is a bijection and $r_{A,F}$ is the inverse of $q_{A,F}$.

  We can also manually check that $\left(r_{A,F} \circ q_{A,F}\right)(\phi) = \phi$ for any natural transformation $\phi : \mathrm{Hom}_{\mathsf{C}}\left(-, A\right) \Rightarrow F$, by evaluating the natural transformations at id_A,

$$\begin{aligned} \left(\left(r_{A,F} \circ q_{A,F}\right)(\phi)\right)_A(\mathrm{id}_A) &= \left(r_{A,F}(\phi_A(\mathrm{id}_A))\right)_A(\mathrm{id}_A) \\ &= F(\mathrm{id}_A)(\phi_A(\mathrm{id}_A)) \\ &= \mathrm{id}_{F(A)}(\phi_A(\mathrm{id}_A)) \\ &= \phi_A(\mathrm{id}_A). \end{aligned}$$

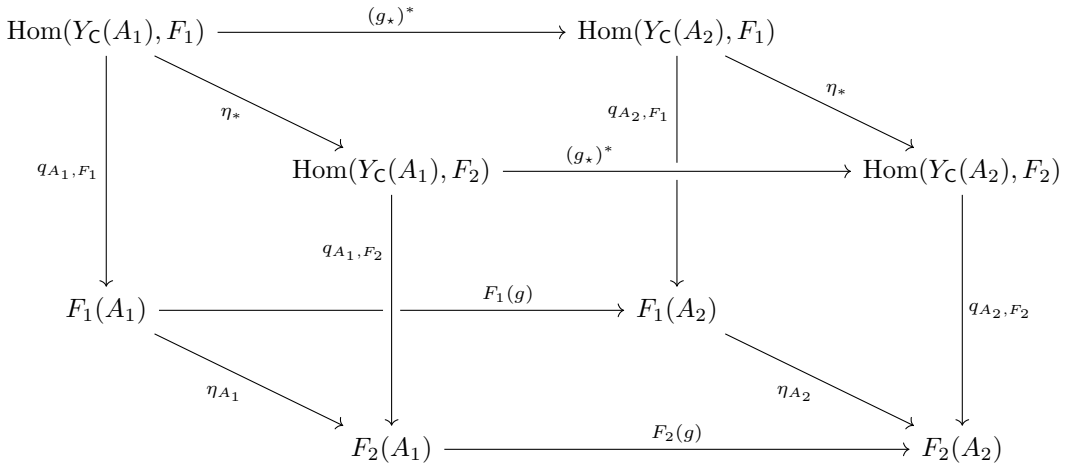
- $q_{A,F}$ **is natural in** A **and** F.
  $\mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}\left(Y_{\mathsf{C}}(-), -\right)$ is a functor obtained by the composition

$$\mathsf{C}^{\mathrm{op}} \times [\mathsf{C}^{\mathrm{op}}, \mathsf{Set}] \xrightarrow{\left(Y_{\mathsf{C}}^{\mathrm{op}}, \mathrm{id}\right)} [\mathsf{C}^{\mathrm{op}}, \mathsf{Set}]^{\mathrm{op}} \times [\mathsf{C}^{\mathrm{op}}, \mathsf{Set}] \xrightarrow{\mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(-,-)} \mathsf{Set}$$

Given any $g : A_2 \to A_1$ and $\eta : F_1 \to F_2$, we should check the following diagram commutes

$$\begin{array}{ccc} \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(Y_{\mathsf{C}}(A_1), F_1) & \xrightarrow{(g_\star)^* \circ \eta_*} & \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(Y_{\mathsf{C}}(A_2), F_2) \\ \downarrow{\scriptstyle q_{A_1,F_1}} & & \downarrow{\scriptstyle q_{A_2,F_2}} \\ F_1(A_1) & \xrightarrow[F_2(g)\circ\eta_{A_1}]{} & F_2(A_2) \end{array}$$

It suffices to check that the following diagram commutes



To check the commutativity of the left square

$$\begin{array}{ccc} \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(Y_{\mathsf{C}}(A_1), F_1) & \xrightarrow{\eta_*} & \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(Y_{\mathsf{C}}(A_1), F_2) \\ \downarrow{\scriptstyle q_{A_1,F_1}} & & \downarrow{\scriptstyle q_{A_1,F_2}} \\ F_1(A_1) & \xrightarrow[\eta_{A_1}]{} & F_2(A_1) \end{array}$$

we can verify that for any $\phi \in \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(Y_{\mathsf{C}}(A_1), F_1)$,

$$\begin{aligned} q_{A_1,F_2} \circ \eta_*(\phi) &= q_{A_1,F_2}(\eta \circ \phi) \\ &= (\eta \circ \phi)_{A_1}(\mathrm{id}_{A_1}) \\ &= \eta_{A_1}(\phi_{A_1}(\mathrm{id}_{A_1})) \\ &= \eta_{A_1} \circ q_{A_1,F_1}(\phi). \end{aligned}$$

To check the commutativity of the front square

$$\begin{array}{ccc} \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(Y_{\mathsf{C}}(A_1), F_2) & \xrightarrow{(g_\star)^*} & \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(Y_{\mathsf{C}}(A_2), F_2) \\ \downarrow{\scriptstyle q_{A_1,F_2}} & & \downarrow{\scriptstyle q_{A_2,F_2}} \\ F_2(A_1) & \xrightarrow[F_2(g)]{} & F_2(A_2) \end{array}$$

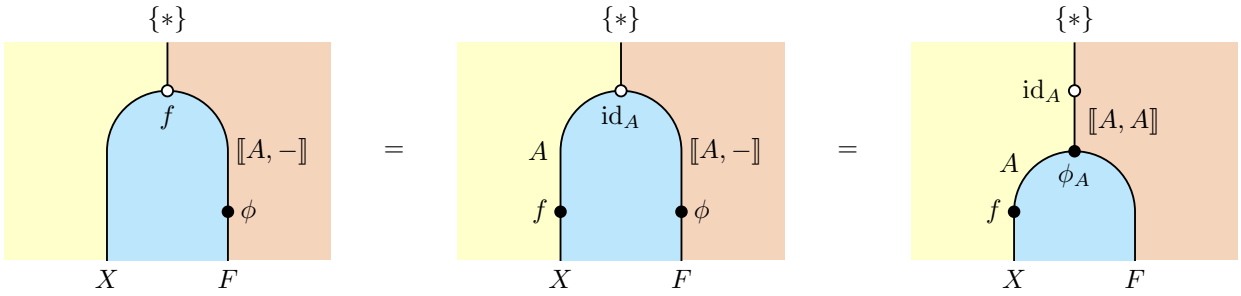
we can verify that for any $\psi \in \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(Y_{\mathsf{C}}(A_1), F_2)$, we have

$$\begin{aligned} q_{A_2,F_2} \circ (g_\star)^*(\psi) &= q_{A_2,F_2}(\psi \circ g_\star) \\ &= (\psi \circ g_\star)_{A_2}(\mathrm{id}_{A_2}) \\ &= \psi_{A_2} \circ g_*(\mathrm{id}_{A_2}) \\ &= \psi_{A_2}(g) \\ &= F_2(g)(\psi_{A_1}(\mathrm{id}_{A_1})) \\ &= F_2(g) \circ q_{A_1,F_2}(\psi). \end{aligned}$$

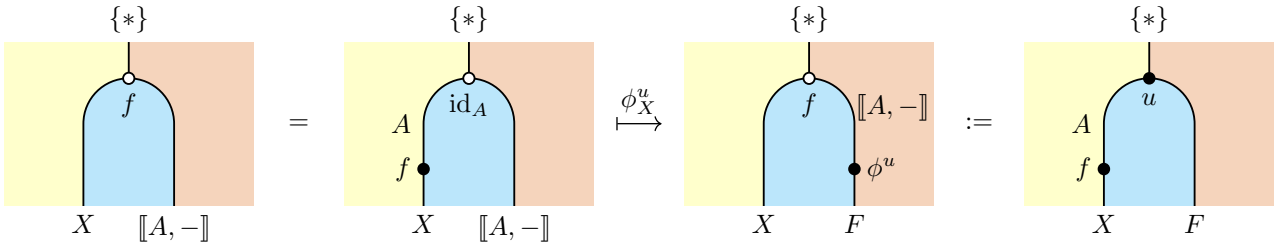
□

For the covariant version, the following string diagram shows ϕ is determined by $\phi_A(\mathrm{id}_A)$

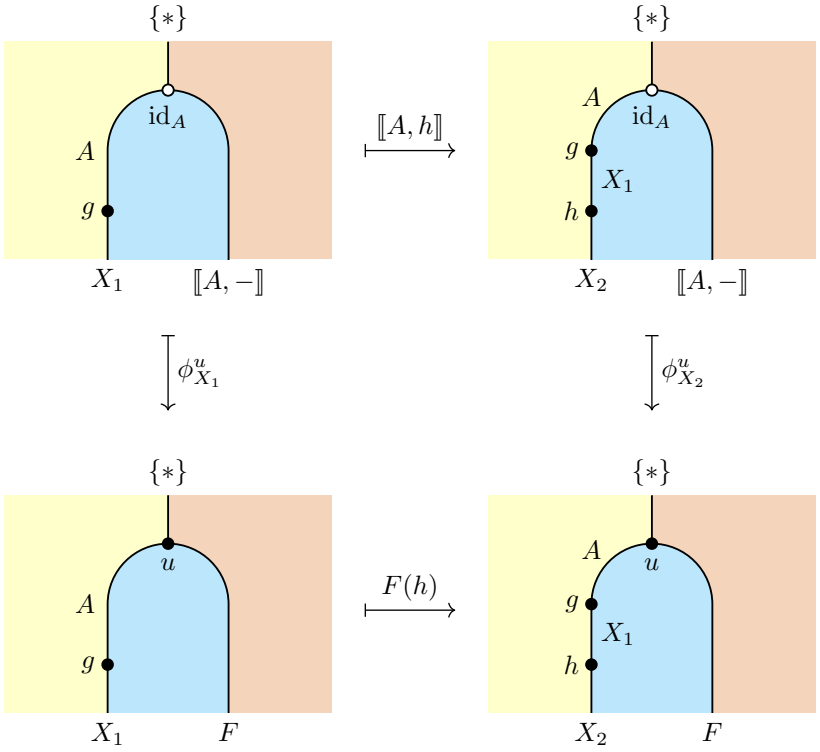
$$\phi_X(f) = F(f)(\phi_A(\mathrm{id}_A)), \quad \forall X \in \mathrm{Ob}(\mathsf{C}), \forall f \in \mathrm{Hom}_{\mathsf{C}}(A, X).$$



For any $u \in F(A)$, we can define $\phi^u : \mathrm{Hom}_{\mathsf{C}}(A, -) \Rightarrow F$ by



and check that the naturality of ϕ^u as follows



Then it is straightforward to see $\phi^u_A(\mathrm{id_A}) = u$ and $\phi^{\phi_A(\mathrm{id}_A)} = \phi$.

Corollary 2.3.4 Yoneda Embedding

Let C be a locally small category. The Yoneda embedding functor $Y_{\mathsf{C}} : \mathsf{C} \to [\mathsf{C}^{\mathrm{op}}, \mathsf{Set}]$ is fully faithful. That is, for any $A_1, A_2 \in \mathrm{Ob}(\mathsf{C})$, the morphism set map

$$\begin{aligned} Y_{\mathsf{C}}|_{\mathrm{Hom}_{\mathsf{C}}(A_1,A_2)} : \mathrm{Hom}_{\mathsf{C}}(A_1, A_2) &\longrightarrow \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(\mathrm{Hom}_{\mathsf{C}}(-, A_1), \mathrm{Hom}_{\mathsf{C}}(-, A_2)) \\ f &\longmapsto f_\star \end{aligned}$$

is a bijection. That justifies the name "embedding" because C is embedded into $\mathsf{Psh}(\mathsf{C})$ via Y_{C} as a full subcategory.

Proof. By Yoneda lemma, there is a natural bijection

$$\mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(\mathrm{Hom}_{\mathsf{C}}(-, A_1), \mathrm{Hom}_{\mathsf{C}}(-, A_2)) \cong \mathrm{Hom}_{\mathsf{C}}(A_1, A_2),$$

which is given by

$$\begin{aligned} r_{A_1, Y_{\mathsf{C}}(A_2)} : \mathrm{Hom}_{\mathsf{C}}(A_1, A_2) &\xrightarrow{\sim} \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(\mathrm{Hom}_{\mathsf{C}}(-, A_1), \mathrm{Hom}_{\mathsf{C}}(-, A_2)) \\ f \longmapsto f_\star : &\begin{bmatrix} (f_\star)_X : \mathrm{Hom}_{\mathsf{C}}(X, A_1) \longrightarrow \mathrm{Hom}_{\mathsf{C}}(X, A_2) \\ g \longmapsto f_*(g) = f \circ g \end{bmatrix} \end{aligned}$$

and

$$q_{A_1, Y_{\mathsf{C}}(A_2)} : \mathrm{Hom}_{\mathsf{Psh}(\mathsf{C})}(\mathrm{Hom}_{\mathsf{C}}(-, A_1), \mathrm{Hom}_{\mathsf{C}}(-, A_2)) \xrightarrow{\sim} \mathrm{Hom}_{\mathsf{C}}(A_1, A_2)$$

$$\begin{bmatrix} \mathsf{C}^{\mathrm{op}} \xrightarrow[\mathrm{Hom}_{\mathsf{C}}(-,A_2)]{\mathrm{Hom}_{\mathsf{C}}(-,A_1)} \mathsf{Set} \ \text{(with } \phi \text{ between)} \end{bmatrix} \longmapsto \phi_{A_1}(\mathrm{id}_{A_1})$$

Note that $r_{A_1, Y_{\mathsf{C}}(A_2)}$ is exactly the morphism set map $Y_{\mathsf{C}}|_{\mathrm{Hom}_{\mathsf{C}}(A_1,A_2)}$. □

Yoneda embedding allows us to regard any category C as a full subcategory of $\mathsf{Psh}(\mathsf{C})$. So in the sense of categorical isomorphism, we can identify any object $A \in \mathrm{Ob}(\mathsf{C})$ with a presheaf $\mathrm{Hom}_{\mathsf{C}}(-, A)$.

An object in a category is equivalent to the collection of all arrows pointing to that object. In other words, the information we care about is which arrows from an object itself and other objects would point to this object, while the object's internals are completely regarded as a black box.

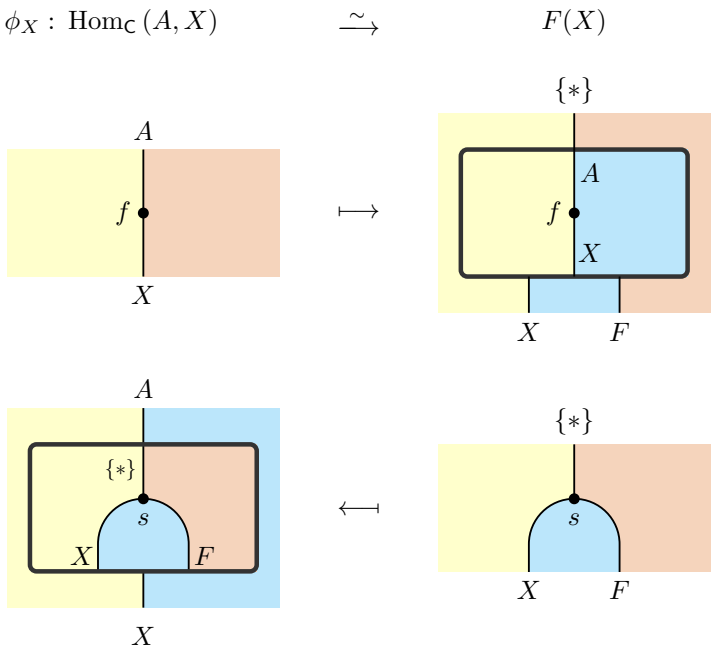
The arrows between objects in a category are equivalent to the transformations between sets of arrows pointing to objects. Specifically, suppose f is an arrow from object A to object B, then any arrow pointing to A can be transformed into an arrow pointing to B by appending an f, which is exactly what $f_\star$ does. Conversely, if there is a way to naturally transform all arrows pointing to A into arrows pointing to B, then this transformation must be realized by appending an arrow between A and B.

Definition 2.3.5 Representable Functor

Let C be a locally small category.

- A functor $F : \mathsf{C} \to \mathsf{Set}$ is called **representable** if it is naturally isomorphic to $\mathrm{Hom}_{\mathsf{C}}(A, -)$ for some $A \in \mathrm{Ob}(\mathsf{C})$.
- A functor $F : \mathsf{C}^{\mathrm{op}} \to \mathsf{Set}$ is called **representable** if it is naturally isomorphic to $\mathrm{Hom}_{\mathsf{C}}(-, A)$ for some $A \in \mathrm{Ob}(\mathsf{C})$.

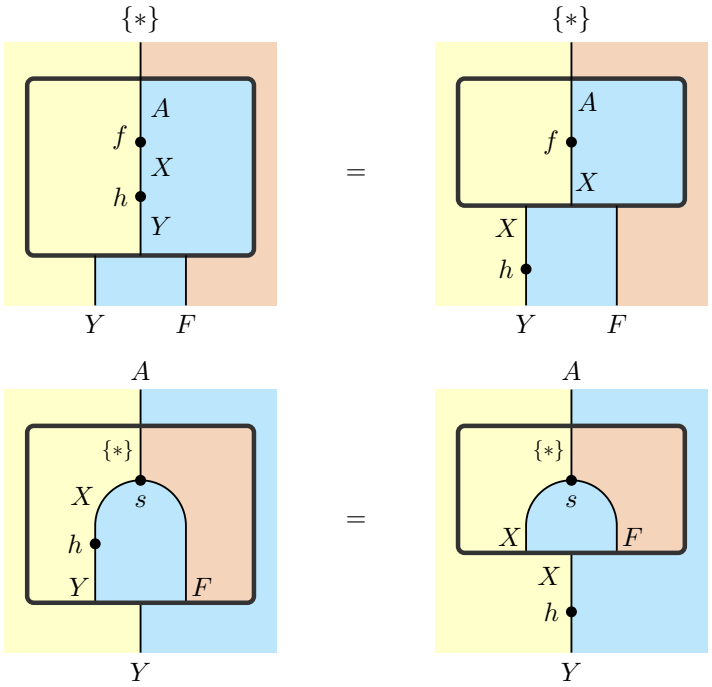
A **representation of** F is a pair (A, ϕ), where $A \in \mathrm{Ob}(\mathsf{C})$ and $\phi : \mathrm{Hom}_{\mathsf{C}}(A, -) \xRightarrow{\sim} F$ is a natural isomorphism.
According to Yoneda lemma, $\phi : \mathrm{Hom}_{\mathsf{C}}(A, -) \Rightarrow F$ is 1-1 correspondence with an element $\phi_A(\mathrm{id}_A) \in F(A)$. We define an **universal element of** F is a pair (A, u) where $A \in \mathrm{Ob}(\mathsf{C})$ and $u \in F(A)$ such that u corresponds to a natural isomorphism $\phi : \mathrm{Hom}_{\mathsf{C}}(A, -) \xRightarrow{\sim} F$. Specifying a universal element of F is equivalent to specifying a representation of F.



The naturality diagram of ϕ

$$\begin{array}{ccc} \mathrm{Hom}_{\mathsf{C}}(A,X) & \xrightarrow{h_*} & \mathrm{Hom}_{\mathsf{C}}(A,Y) \\ \downarrow{\scriptstyle \phi_X}\ \sim & & \sim\ \downarrow{\scriptstyle \phi_Y} \\ F(X) & \xrightarrow[F(h)]{} & F(Y) \end{array}$$

can be translated into the following calculus rules



Proposition 2.3.6 Equivalent Characterizations of Representable Functor

Suppose $F : \mathsf{C} \to \mathsf{Set}$ is a functor. Then the following statements are equivalent:

(i) F is representable by universal element (A, u)

(ii) (A, u) is initial in the category $\int_{\mathsf{C}} F = (\{*\} \downarrow F)$, which corresponds to $\mathbb{1} \xrightarrow{\boxtimes\{*\}} \mathsf{Set} \xleftarrow{F} \mathsf{C}$.

(iii) (A, ϕ^u) is initial in the category $(Y_{\mathsf{C}^{\mathrm{op}}} \downarrow F)$, which corresponds to $\mathsf{C}^{\mathrm{op}} \xrightarrow{Y_{\mathsf{C}^{\mathrm{op}}}} [\mathsf{C}, \mathsf{Set}] \xleftarrow{\boxtimes F} \mathbb{1}$.

(iv) $(A, \boxtimes u : \{*\} \to F(A))$ is a universal morphism from $\{*\}$ to F.

(v) For any $(X, x) \in \mathrm{Ob}(\int_{\mathsf{C}} F)$, there is a unique morphism $(A, u) \to (X, x)$ in $\int_{\mathsf{C}} F$ (which is a morphism $f : A \to X$ in C such that $F(f)(u) = x$).

Suppose $F : \mathsf{C}^{\mathrm{op}} \to \mathsf{Set}$ is a functor. Then the following statements are equivalent:

(i) F is representable by universal element (A, u)

(ii) (A, u) is initial in the category $\int_{\mathsf{C}^{\mathrm{op}}} F = (\{*\} \downarrow F)$, which corresponds to $\mathbb{1} \xrightarrow{\boxtimes\{*\}} \mathsf{Set} \xleftarrow{F} \mathsf{C}^{\mathrm{op}}$.

(iii) (A, ϕ^u) is terminal in the category $(Y_{\mathsf{C}} \downarrow F)$, which corresponds to $\mathsf{C} \xrightarrow{Y_{\mathsf{C}}} [\mathsf{C}^{\mathrm{op}}, \mathsf{Set}] \xleftarrow{\boxtimes F} \mathbb{1}$.

(iv) $(A, \boxtimes u : \{*\} \to F(A))$ is a universal morphism from $\{*\}$ to F.

(v) For any $(X, x) \in \mathrm{Ob}\left(\int_{\mathsf{C}^{\mathrm{op}}} F\right)$, there is a unique morphism $(A, u) \to (X, x)$ in $\int_{\mathsf{C}^{\mathrm{op}}} F$ (which is a morphism $f : X \to A$ in C such that $F(f)(x) = u$).

Proof. (i) $\iff$ (ii). Suppose (A, u) is an object of $\int_{\mathsf{C}} F$ and $\phi^u : \mathrm{Hom}_{\mathsf{C}}(A, -) \Rightarrow F$ be the natural transformation

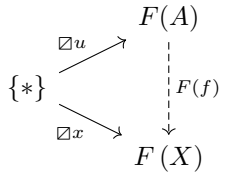
$$\phi^u_X(f) = F(f)(u), \quad \forall f \in \mathrm{Hom}_{\mathsf{C}}(A, X),$$

which can be illustrated by the following diagram

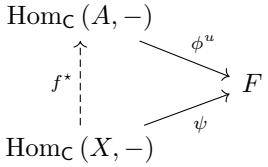
$$\begin{array}{ccccccc} \mathrm{id}_A & \in & \mathrm{Hom}_{\mathsf{C}}(A, A) & \xrightarrow{f_*} & \mathrm{Hom}_{\mathsf{C}}(A, X) & \ni & f \\ \downarrow & & \downarrow{\scriptstyle \phi^u_A} & & \downarrow{\scriptstyle \phi^u_X} & & \downarrow \\ u = \phi^u_A(\mathrm{id}_A) & \in & F(A) & \xrightarrow[F(f)]{} & F(X) & \ni & \phi^u_X(f) \end{array}$$

Thus we have

$$\begin{aligned} (A, u) \text{ is initial in } \int_{\mathsf{C}} F &\iff \forall (X, x) \in \mathrm{Ob}\left(\int_{\mathsf{C}} F\right),\ \exists! f \in \mathrm{Hom}_{\mathsf{C}}(A, X),\ F(f)(u) = x \\ &\iff \forall X \in \mathrm{Ob}(\mathsf{C}),\ \forall x \in F(X),\ \exists! f \in \mathrm{Hom}_{\mathsf{C}}(A, X),\ \phi^u_X(f) = x \\ &\iff \forall X \in \mathrm{Ob}(\mathsf{C}),\ \phi^u_X \text{ is bijective} \\ &\iff \phi^u \text{ is a natural isomorphism} \\ &\iff (A, u) \text{ is a universal element of } F. \end{aligned}$$



(i) $\iff$ (iii). (A, ϕ^u) is initial in $(Y_{\mathsf{C}^{\mathrm{op}}} \downarrow F)$ if and only if for any $X \in \mathrm{Ob}(\mathsf{C})$ and any natural transformation $\psi : \mathrm{Hom}_{\mathsf{C}}(X, -) \implies F$, there is a unique $f \in \mathrm{Hom}_{\mathsf{C}}(A, X)$ such that $\phi^u \circ f^\star = \psi$



or equivalently

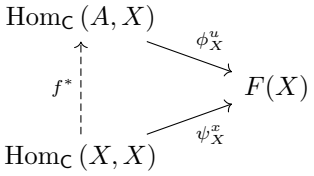
$$\psi_X(\mathrm{id}_X) = (\phi^u \circ f^\star)_X(\mathrm{id}_X) = \phi^u_X(f).$$

Suppose F is representable by universal element (A, u). Then $\phi^u : \mathrm{Hom}_{\mathsf{C}}(A, -) \xRightarrow{\sim} F$ is a natural isomorphism. Since

$$\begin{aligned} Y_{\mathsf{C}^{\mathrm{op}}}|_{\mathrm{Hom}_{\mathsf{C}}(A,X)} : \mathrm{Hom}_{\mathsf{C}}(A, X) &\xrightarrow{\sim} \mathrm{Hom}_{[\mathsf{C},\mathsf{Set}]}(\mathrm{Hom}_{\mathsf{C}}(X, -), \mathrm{Hom}_{\mathsf{C}}(A, -)) \\ f &\longmapsto f^\star \end{aligned}$$

is a bijection, there is a unique $f \in \mathrm{Hom}_{\mathsf{C}}(A, X)$ such that $f^\star = (\phi^u)^{-1} \circ \psi$ or equivalently $\phi^u \circ f^\star = \psi$.

Conversely, suppose (A, ϕ^u) is initial in $(Y_{\mathsf{C}^{\mathrm{op}}} \downarrow F)$. Then for any $X \in \mathrm{Ob}(\mathsf{C})$ and any $x \in F(X)$, there exist natural transformation $\psi^x : \mathrm{Hom}_{\mathsf{C}}(X, -) \Longrightarrow F$ and unique $f \in \mathrm{Hom}_{\mathsf{C}}(A, X)$ such that $x = \psi^x_X(\mathrm{id}_X) = \phi^u_X(f)$,



which implies ϕ^u_X is bijective. Thus ϕ^u is a natural isomorphism and (A, u) is a universal element of F. □

Corollary 2.3.7 Initial Object Characterized by Representable Functor

Suppose C is a locally small category.

- $A \in \mathrm{Ob}(\mathsf{C})$ is initial in C if and only if the functor $\not\square\{*\} : \mathsf{C} \to \mathsf{Set}$ is representable and naturally isomorphic to $\mathrm{Hom}_{\mathsf{C}}(A, -)$.
- $A \in \mathrm{Ob}(\mathsf{C})$ is terminal in C if and only if the functor $\not\square\{*\} : \mathsf{C}^{\mathrm{op}} \to \mathsf{Set}$ is representable and naturally isomorphic to $\mathrm{Hom}_{\mathsf{C}}(-, A)$.

Proof. Let $\not\square\{*\} : \mathsf{C} \to \mathsf{Set}$ be a constant functor. It is easy to see that the category $\int_{\mathsf{C}} \not\square\{*\}$ is isomorphic to C through the functor

$$\begin{aligned} p : \int_{\mathsf{C}} \not\square\{*\} &\longrightarrow \mathsf{C} \\ (C, *) &\longmapsto C \end{aligned}$$

As established in Proposition 2.3.6, $(A, *) \in \mathrm{Ob}(\mathsf{C})$ is initial in $\int_{\mathsf{C}} \not\square\{*\}$ if and only if $\not\square\{*\}$ is a representable functor with a universal element $(A, *)$, which proves the first statement. The second statement can be obtained by applying the first statement to C^{op}.

In addition, an alternative ad-hoc proof is conceivable. If $\not\square\{*\}$ is naturally isomorphic to $\mathrm{Hom}_{\mathsf{C}}(A, -)$ through $\theta : \mathrm{Hom}_{\mathsf{C}}(A, -) \xRightarrow{\sim} \not\square\{*\}$, we have no choice but to define $\theta_X(\mathrm{id}_X) = *$. Note that $\not\square\{*\}(A) = \{*\}$. Yoneda lemma also implies that θ must correspond to $* \in \not\square\{*\}(A)$ and accordingly θ is the unique natural isomorphism from $\mathrm{Hom}_{\mathsf{C}}(A, -)$ to $\not\square\{*\}$. □

Lemma 2.3.8

Let $F : \mathsf{C} \to \mathsf{D}$ be a functor and $X \in \mathrm{Ob}(\mathsf{D})$. Consider functors

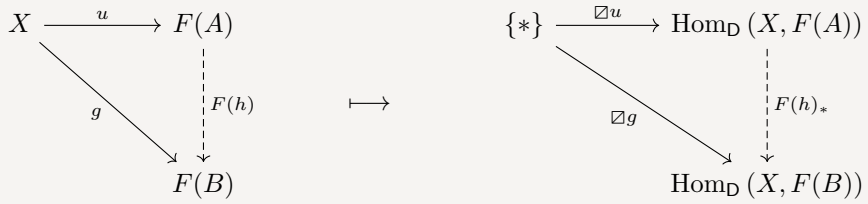
$$\mathbb{1} \xrightarrow{\not\square X} \mathsf{D} \xleftarrow{F} \mathsf{C}$$

$$\mathbb{1} \xrightarrow{\not\square\{*\}} \mathsf{Set} \xleftarrow{\mathrm{Hom}_{\mathsf{D}}(X, F(-))} \mathsf{C}$$

We have the following category isomorphism

$$(X \downarrow F) \cong (\{*\} \downarrow \mathrm{Hom}_{\mathsf{D}}(X, F(-))) = \int_{\mathsf{C}} \mathrm{Hom}_{\mathsf{D}}(X, F(-))$$

through the functor $(A, u) \mapsto (A, \boxslash u)$, whose action on commutative diagrams is illustrated as follows



Proposition 2.3.9 Equivalent Characterizations of Universal Morphism

Let $F : \mathsf{C} \to \mathsf{D}$ be a functor, $A, X \in \mathrm{Ob}(\mathsf{D})$ and $u : X \to F(A)$ be a morphism. Then the following statements are equivalent:

(i) (A, u) is initial in the category $(X \downarrow F)$.

(ii) $\mathrm{Hom}_{\mathsf{D}}(X, F(-))$ is representable by universal element (A, u).

(iii) $(A, \boxslash u)$ is initial in the category $\int_{\mathsf{C}} \mathrm{Hom}_{\mathsf{D}}(X, F(-)) = (\{*\} \downarrow \mathrm{Hom}_{\mathsf{D}}(X, F(-)))$.

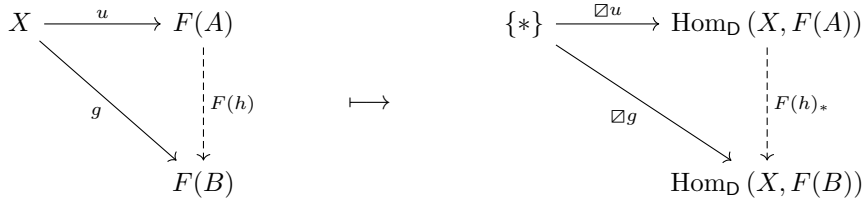
Dually, the following statements are equivalent:

(i) (A, u) is terminal in the category $(F \downarrow X)$.

(ii) $\mathrm{Hom}_{\mathsf{D}}(F(-), X)$ is representable by universal element (A, u).

(iii) $(A, \boxslash u)$ is initial in the category $\int_{\mathsf{C}^{\mathrm{op}}} \mathrm{Hom}_{\mathsf{D}}(F(-), X) = (\{*\} \downarrow \mathrm{Hom}_{\mathsf{D}}(F(-), X))$.

Proof. It suffices to show (i) $\iff$ (iii). The category $(X \downarrow F)$ is isomorphic to $\int_{\mathsf{C}} \mathrm{Hom}_{\mathsf{D}}(X, F(-))$ through the functor



We can also verify it directly.

$$
\begin{aligned}
(A, u) \text{ is initial in } (X \downarrow F) &\iff \forall (B, g) \in \mathrm{Ob}(X \downarrow F),\ \exists! h \in \mathrm{Hom}_{\mathsf{C}}(A, B),\ F(h) \circ u = g \\
&\iff \forall B \in \mathrm{Ob}(\mathsf{C}),\ \forall g \in \mathrm{Hom}_{\mathsf{C}}(X, F(B)),\ \exists! h \in \mathrm{Hom}_{\mathsf{C}}(A, B),\ F(h) \circ u = g \\
&\iff \forall (B, \boxslash g) \in \mathrm{Ob}\left(\int_{\mathsf{C}} \mathrm{Hom}_{\mathsf{D}}(X, F(-))\right),\ \exists! h \in \mathrm{Hom}_{\mathsf{C}}(A, B),\ F(h)_* \circ \boxslash u = \boxslash g \\
&\iff (A, u) \text{ is initial in } \int_{\mathsf{C}} \mathrm{Hom}_{\mathsf{D}}(X, F(-))
\end{aligned}
$$

The dual version is similar. □

Example 2.3.1 Identity Functor $\mathrm{id}_{\mathsf{Set}}$ is Representable

The identity functor $\mathrm{id}_{\mathsf{Set}} : \mathsf{Set} \to \mathsf{Set}$ is representable by $\left(\{*\}, \mathrm{id}_{\{*\}}\right)$. The natural isomorphism $\phi : \mathrm{Hom}_{\mathsf{Set}}(\{*\}, -) \xRightarrow{\sim} \mathrm{id}_{\mathsf{Set}}$ is defined by

$$
\begin{aligned}
\phi_X : \mathrm{Hom}_{\mathsf{Set}}(\{*\}, X) &\xrightarrow{\sim} X \\
f &\longmapsto f(*)
\end{aligned}
$$

Naturality of ϕ means that for any function $h : X \to Y$, the following diagram commutes

$$\begin{array}{ccc} \mathrm{Hom}_{\mathsf{Set}}(\{*\}, X) & \xrightarrow{h_*} & \mathrm{Hom}_{\mathsf{Set}}(\{*\}, Y) \\ \downarrow{\scriptstyle \phi_X} & & \downarrow{\scriptstyle \phi_Y} \\ X & \xrightarrow[h]{} & Y \end{array}$$

Example 2.3.2 Ob : Cat → Set is Representable

The functor

$$\begin{array}{ccc} \mathsf{Cat} & & \mathsf{Set} \\ \mathsf{C} & & \mathrm{Ob}(\mathsf{C}) \\ \downarrow{\scriptstyle F} & \rightsquigarrow^{\mathrm{Ob}} & \downarrow{\scriptstyle F^{\mathrm{Ob}}} \\ \mathsf{D} & & \mathrm{Ob}(\mathsf{D}) \end{array}$$

$\mathrm{Ob} : \mathsf{Cat} \to \mathsf{Set}$ is representable by $\left(\mathbb{1}, \mathrm{id}_{\{*\}}\right)$. The natural isomorphism $\phi : \mathrm{Hom}_{\mathsf{Cat}}(\mathbb{1}, -) \xRightarrow{\sim} \mathrm{Ob}$ is defined by

$$\begin{aligned} \phi_{\mathsf{C}} : \mathrm{Hom}_{\mathsf{Cat}}(\mathbb{1}, \mathsf{C}) &\xrightarrow{\sim} \mathrm{Ob}(\mathsf{C}) \\ F &\longmapsto F^{\mathrm{Ob}}(\bullet) \end{aligned}$$

Naturality of ϕ means that for any functor $H : \mathsf{C} \to \mathsf{D}$, the following diagram commutes

$$\begin{array}{ccc} \mathrm{Hom}_{\mathsf{Cat}}(\mathbb{1}, \mathsf{C}) & \xrightarrow{H_\star} & \mathrm{Hom}_{\mathsf{Cat}}(\mathbb{1}, \mathsf{D}) \\ \downarrow{\scriptstyle \phi_{\mathsf{C}}} & & \downarrow{\scriptstyle \phi_{\mathsf{D}}} \\ \mathrm{Ob}(\mathsf{C}) & \xrightarrow[H^{\mathrm{Ob}}]{} & \mathrm{Ob}(\mathsf{D}) \end{array}$$

Example 2.3.3 Mor : C → Set is Representable

The functor

$$\begin{array}{ccc} \mathsf{Cat} & & \mathsf{Set} \\ \mathsf{C} & & \mathrm{Mor}(\mathsf{C}) \\ \downarrow{\scriptstyle F} & \rightsquigarrow^{\mathrm{Mor}} & \downarrow{\scriptstyle F^{\mathrm{Mor}}} \\ \mathsf{D} & & \mathrm{Mor}(\mathsf{D}) \end{array}$$

$\mathrm{Mor} : \mathsf{Cat} \to \mathsf{Set}$ is representable by $(2, \bullet \to \bullet)$. The natural isomorphism $\phi : \mathrm{Hom}_{\mathsf{Cat}}(2, -) \xRightarrow{\sim} \mathrm{Mor}$ is defined by

$$\begin{aligned} \phi_{\mathsf{C}} : \mathrm{Hom}_{\mathsf{Cat}}(2, \mathsf{C}) &\xrightarrow{\sim} \mathrm{Mor}(\mathsf{C}) \\ F &\longmapsto F^{\mathrm{Mor}}(\bullet \to \bullet) \end{aligned}$$

Naturality of ϕ means that for any functor $H : \mathsf{C} \to \mathsf{D}$, the following diagram commutes

$$\begin{array}{ccc} \mathrm{Hom}_{\mathsf{Cat}}(2, \mathsf{C}) & \xrightarrow{H_\star} & \mathrm{Hom}_{\mathsf{Cat}}(2, \mathsf{D}) \\ \downarrow{\scriptstyle \phi_{\mathsf{C}}} & & \downarrow{\scriptstyle \phi_{\mathsf{D}}} \\ \mathrm{Mor}(\mathsf{C}) & \xrightarrow[H^{\mathrm{Mor}}]{} & \mathrm{Mor}(\mathsf{D}) \end{array}$$

2.4 Limit and Colimit

Definition 2.4.1 Cone

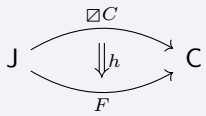
Let J, C be categories and $F : \mathsf{J} \to \mathsf{C}$ be a functor. Consider functors

$$\mathsf{C} \xrightarrow{\boxslash} [\mathsf{J}, \mathsf{C}] \xleftarrow{\boxslash F} \mathbb{1}$$

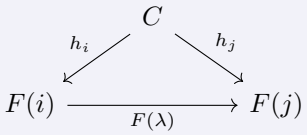
The comma category $(\boxslash \downarrow \boxslash F)$ is called the **cone category from C to** F, denoted by $\mathsf{Cone}(\mathsf{C}, F)$. According to Lemma 2.3.8, we have category isomorphism

$$\mathsf{Cone}(\mathsf{C}, F) = (\boxslash \downarrow \boxslash F) \cong \left(\{*\} \downarrow \mathrm{Hom}_{[\mathsf{J},\mathsf{C}]}\left(\boxslash(-), F\right)\right) = \int_{\mathsf{C}^{\mathrm{op}}} \mathrm{Hom}_{[\mathsf{J},\mathsf{C}]}\left(\boxslash(-), F\right).$$

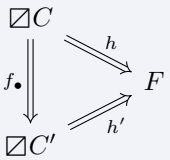
- Objects: The objects in $\mathsf{Cone}(\mathsf{C}, F)$ are all natural transformations



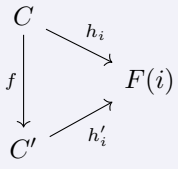
  where $C \in \mathrm{Ob}(\mathsf{C})$. Such $h : \boxslash C \Rightarrow F$ is called a **cone from C to F** because it can be viewed as a family of morphisms $(h_i : C \to F(i))_{i \in \mathrm{Ob}(\mathsf{J})}$ in C such that the following diagram commutes for each morphism $\lambda : i \to j$ in J



- Morphisms: The morphisms in $\mathsf{Cone}(\mathsf{C}, F)$ are commutative triangles shown as follows



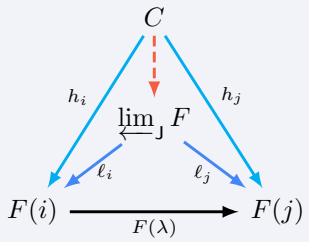
  Equivalently, a morphism from cone $(h_i : C \to F(i))_{i \in \mathrm{Ob}(\mathsf{J})}$ to cone $(h'_i : C' \to F(i))_{i \in \mathrm{Ob}(\mathsf{J})}$ is a morphism $f : C \to C'$ in C such that the following diagram commutes for each $i \in \mathrm{Ob}(\mathsf{J})$



Definition 2.4.2 Limit

Let J, C be categories and $F : \mathsf{J} \to \mathsf{C}$ be a functor. The **limit** of F, denoted by $\varprojlim_{\mathsf{J}} F$, is the terminal

object of $\mathsf{Cone}(\mathsf{C}, F)$. For each morphism $\lambda : i \to j$ in J, we have the following commutative diagram



For simplicity, we may write $\varprojlim F$ instead of $\varprojlim_{\mathsf{J}} F$.

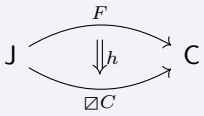
Definition 2.4.3 Cocone

Let J, C be categories and $F : \mathsf{J} \to \mathsf{C}$ be a functor. Consider functors

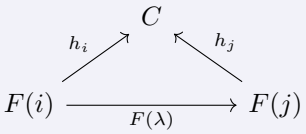
$$\mathbb{1} \xrightarrow{\boxslash F} [\mathsf{J}, \mathsf{C}] \xleftarrow{\boxslash} \mathsf{C}$$

The comma category $(\boxslash F \downarrow \boxslash)$ is called the **cocone category from F to C**, denoted by $\mathsf{Cocone}(F, \mathsf{C})$.

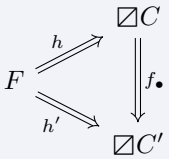
- Objects: The objects in $\mathsf{Cocone}(F, \mathsf{C})$ are all natural transformations



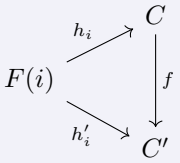
  where $C \in \mathrm{Ob}(\mathsf{C})$. Such $h : F \Rightarrow \boxslash C$ is called a **cocone from F to C** because it can be viewed as a family of morphisms $(h_i : F(i) \to C)_{i \in \mathrm{Ob}(\mathsf{J})}$ in C such that the following diagram commutes for each morphism $\lambda : i \to j$ in J



- Morphisms: The morphisms in $\mathsf{Cocone}(F, \mathsf{C})$ are commutative triangles shown as follows



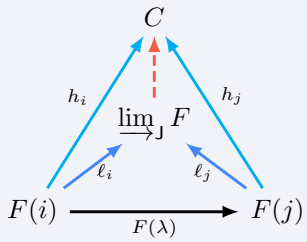
Equivalently, a morphism from cocone $(h_i : F(i) \to C)_{i \in \mathrm{Ob}(\mathsf{J})}$ to cocone $(h'_i : F(i) \to C')_{i \in \mathrm{Ob}(\mathsf{J})}$ is a morphism $f : C \to C'$ in C such that the following diagram commutes for each $i \in \mathrm{Ob}(\mathsf{J})$



Definition 2.4.4 Colimit

Let J, C be categories and $F : \mathsf{J} \to \mathsf{C}$ be a functor. The **colimit** of F, denoted by $\varinjlim F$, is the initial object

of $\mathsf{Cocone}(F, \mathsf{C})$. For each morphism $\lambda : i \to j$ in J, we have the following commutative diagram



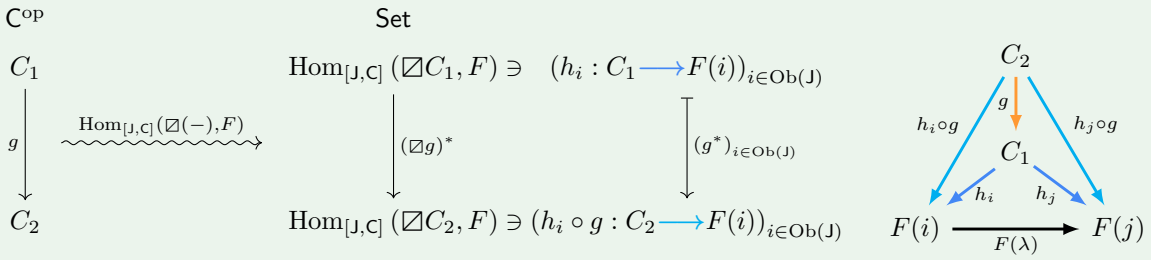
For simplicity, we may write $\varinjlim F$ instead of $\varinjlim_{\mathsf{J}} F$.

Definition 2.4.5 Connected Limit

Let J be a category. Then a J-shaped limit (resp. colimit) is called a **connected limit** (resp. **connected colimit**) if the category J is connected.

Proposition 2.4.6 Limit Characterized by Representability

Let J, C be categories and $F : \mathsf{J} \to \mathsf{C}$ be a functor. The limit of F exists if and only if the functor $\mathrm{Hom}_{[\mathsf{J},\mathsf{C}]}(\boxslash(-), F)$



is representable. In this case, the universal element coincides with $\left(\varprojlim F, \left(\ell_i : \varprojlim F \to F(i)\right)_{i \in \mathrm{Ob}(\mathsf{J})}\right)$ and we have

$$\mathrm{Hom}_{[\mathsf{J},\mathsf{C}]}(\boxslash(-), F) \cong \mathrm{Hom}_{\mathsf{C}}\left(-, \varprojlim F\right).$$

Dually, the colimit of F exists if and only if the functor $\mathrm{Hom}_{[\mathsf{J},\mathsf{C}]}(F, \boxslash(-)) : \mathsf{C} \to \mathsf{Set}$ is representable. In this case, the universal element coincides with $\left(\varinjlim F, \left(\ell_i : F(i) \to \varinjlim F\right)_{i \in \mathrm{Ob}(\mathsf{J})}\right)$ and we have

$$\mathrm{Hom}_{[\mathsf{J},\mathsf{C}]}(F, \boxslash(-)) \cong \mathrm{Hom}_{\mathsf{C}}\left(\varinjlim F, -\right).$$

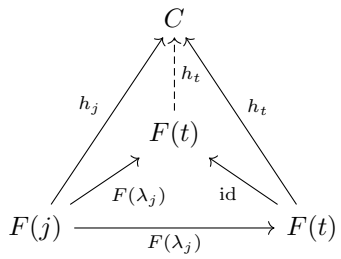
Proof. According to Proposition 2.3.6, $\mathrm{Hom}_{[\mathsf{J},\mathsf{C}]}(\boxslash(-), F)$ is representable by the universal element (A, u) if and only if (A, u) is initial in $\int_{\mathsf{C}^{\mathrm{op}}} \mathrm{Hom}_{[\mathsf{J},\mathsf{C}]}(\boxslash(-), F)$, which is equivalent to saying that for any $C \in \mathrm{Ob}(\mathsf{C})$ and $(h_i) \in \mathrm{Hom}_{[\mathsf{J},\mathsf{C}]}(\boxslash C, F)$, there is a unique morphism $f : C \to A$ in C such that $h_i = f^*(u_i) = u_i \circ f$ for each $i \in \mathrm{Ob}(\mathsf{J})$. This is exactly the universal property of limit. □

Lemma 2.4.7

If J is a small category with a terminal object t, then for any functor $F : \mathsf{J} \to \mathsf{C}$, we have $\varinjlim F \cong F(t)$.

Proof. Since for every $j \in \mathrm{Ob}(\mathsf{J})$, there is a unique morphism $\lambda_j : j \to t$, $\left(F(t), (F(\lambda_j) : F(j) \to F(t))_{j \in \mathrm{Ob}(\mathsf{J})}\right)$ is a cocone from F to $F(t)$. We need to show that it is initial. Note that $F(\lambda_t) = F(\mathrm{id}_t) = \mathrm{id}_{F(t)}$. For any cocone $\left(C, (h_j : F(j) \to C)_{j \in \mathrm{Ob}(\mathsf{J})}\right)$, there is a morphism $h_t : F(t) \to C$ such that for any $j \in \mathrm{Ob}(\mathsf{J})$, $h_t \circ F(\lambda_j) = h_j$,

which means the following diagram commutes



If there is another morphism $g : F(t) \to C$ such that for any $j \in \mathrm{Ob}(\mathsf{J})$, $g \circ F(\lambda_j) = h_j$. Take $j = t$, and we have $g = h_t$. Therefore, $\left(F(t), (F(\lambda_j) : F(j) \to F(t))_{j \in \mathrm{Ob}(\mathsf{J})}\right)$ is the colimit of F.

□

Example 2.4.1

Let C be a category and $X \in \mathrm{Ob}(\mathsf{C})$. Consider the hom functor $\mathrm{Hom}_{\mathsf{C}}(X, -) : \mathsf{C} \to \mathsf{Set}$. We have

$$\varinjlim \mathrm{Hom}_{\mathsf{C}}(X, -) \cong \{*\}.$$

Proof. Let $h^X = \mathrm{Hom}_{\mathsf{C}}(X, -)$. By Proposition 2.4.6, we have

$$\mathrm{Hom}_{[\mathsf{C},\mathsf{Set}]}\left(h^X, \boxslash(-)\right) \cong \mathrm{Hom}_{\mathsf{Set}}\left(\varinjlim h^X, -\right).$$

where $\boxslash : \mathsf{Set} \to [\mathsf{C}, \mathsf{Set}]$ is the diagonal functor. By Yoneda Lemma, we have natural isomorphism

$$\mathrm{Hom}_{[\mathsf{C},\mathsf{Set}]}\left(h^X, \boxslash(-)\right) \cong \mathrm{Hom}_{[\mathsf{C},\mathsf{Set}]}\left(h^X, -\right) \circ \boxslash \cong \mathrm{ev}_X \circ \boxslash \cong \mathrm{id}_{\mathsf{Set}} \cong \mathrm{Hom}_{\mathsf{Set}}\left(\{*\}, -\right).$$

The last isomorphism has been proved in Example 2.3.1. Therefore, we have

$$\mathrm{Hom}_{\mathsf{Set}}\left(\varinjlim h^X, -\right) \cong \mathrm{Hom}_{\mathsf{Set}}\left(\{*\}, -\right).$$

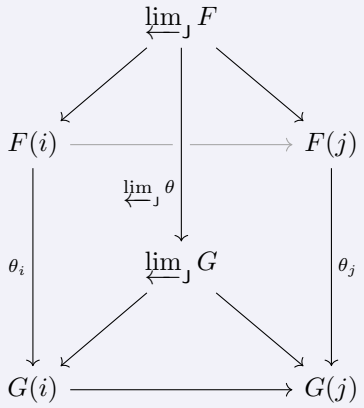
Since Yoneda embedding is full and faithful, we have $\varinjlim h^X \cong \{*\}$. □

Definition 2.4.8 $\varprojlim_{\mathsf{J}}$ **Functor**

Let J be a small category and C be a category. If for any functor $F : \mathsf{J} \to \mathsf{C}$, $\varprojlim_{\mathsf{J}} F$ exists, then we have a functor

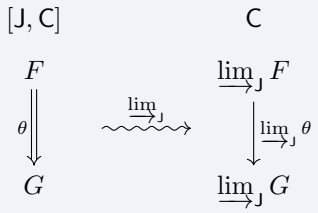
$$\begin{array}{ccc} [\mathsf{J}, \mathsf{C}] & & \mathsf{C} \\ F & & \varprojlim_{\mathsf{J}} F \\ \theta \Downarrow & \overset{\varprojlim_{\mathsf{J}}}{\rightsquigarrow} & \downarrow \varprojlim_{\mathsf{J}} \theta \\ G & & \varprojlim_{\mathsf{J}} G \end{array}$$

where $\varprojlim_{\mathsf{J}} \theta$ is induced by the universal property of $\varprojlim_{\mathsf{J}} G$

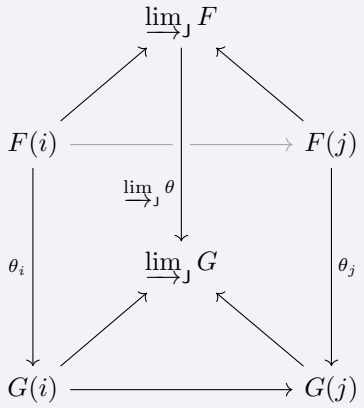


Definition 2.4.9 $\varinjlim_{\mathsf{J}}$ Functor

Let J be a small category and C be a category. If for any functor $F : \mathsf{J} \to \mathsf{C}$, $\varinjlim_{\mathsf{J}} F$ exists, then we have a functor

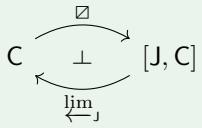


where $\varinjlim_{\mathsf{J}} \theta$ is induced by the universal property of $\varinjlim_{\mathsf{J}} F$



Proposition 2.4.10 Diagonal is Left Adjoint to Limit: $\boxslash \dashv \varprojlim_{\mathsf{J}}$

Let J be a small category and C be a category. If for any functor $F \in [\mathsf{J}, \mathsf{C}]$, $\varprojlim_{\mathsf{J}} F$ exists, then the functor $\varinjlim_{\mathsf{J}} : [\mathsf{J}, \mathsf{C}] \to \mathsf{C}$ is right adjoint to the diagonal functor $\boxslash : \mathsf{C} \to [\mathsf{J}, \mathsf{C}]$



We have a natural isomorphism

$$\mathrm{Hom}_{[\mathsf{J},\mathsf{C}]}\left(\boxslash C, F\right) \cong \mathrm{Hom}_{\mathsf{C}}\left(C, \varprojlim_{\mathsf{J}} F\right)$$

Proposition 2.4.11 Diagonal is Right Adjoint to Colimit: $\varinjlim_{\mathsf{J}} \dashv \boxslash$

Let J be a small category and C be a category. If for any functor $F \in [\mathsf{J}, \mathsf{C}]$, $\varprojlim_{\mathsf{J}} F$ exists, then the functor $\varinjlim_{\mathsf{J}} : [\mathsf{J}, \mathsf{C}] \to \mathsf{C}$ is right adjoint to the diagonal functor $\boxslash : \mathsf{C} \to [\mathsf{J}, \mathsf{C}]$

$$[\mathsf{J}, \mathsf{C}] \underset{\boxslash}{\overset{\varinjlim_{\mathsf{J}}}{\perp}} \mathsf{C}$$

We have a natural isomorphism

$$\mathrm{Hom}_{[\mathsf{J},\mathsf{C}]}\left(F, \boxslash C\right) \cong \mathrm{Hom}_{\mathsf{C}}\left(\varinjlim_{\mathsf{J}} F, C\right)$$

Definition 2.4.12 Complete Category

A category C is **complete** if it has all small limits. That is, for any functor $F : \mathsf{J} \to \mathsf{C}$ with J small, $\varprojlim F$ exists.

Definition 2.4.13 Cocomplete Category

A category C is **cocomplete** if it has all small colimits. That is, for any functor $F : \mathsf{J} \to \mathsf{C}$ with J small, $\varinjlim F$ exists.

Definition 2.4.14 Bicomplete Category

A category C is **bicomplete** if it is both complete and cocomplete.

Example 2.4.2 Examples of Bicomplete Categories

The following categories are bicomplete: Set, Grp, Ab, Ring, R-Mod, K-Vect, Top.

Definition 2.4.15 Finitely Complete category

A category C is **finitely complete** if it has all finite limits. That is, for any functor $F : \mathsf{J} \to \mathsf{C}$ with J a finite category, $\varprojlim F$ exists.

Definition 2.4.16 Finitely Cocomplete category

A category C is **finitely cocomplete** if it has all finite colimits. That is, for any functor $F : \mathsf{J} \to \mathsf{C}$ with J a finite category, $\varinjlim F$ exists.

Definition 2.4.17 Filtered Category

A category J is **filtered** if

- J is nonempty.
- For any pair of objects $j_1, j_2 \in \mathrm{Ob}(\mathsf{J})$, there exists an object $j_3 \in \mathrm{Ob}(\mathsf{J})$ and morphisms $j_1 \to j_3$ and $j_2 \to j_3$.
- For any pair of morphisms $f, g : j_1 \to j_2$, there exists an object $j_3 \in \mathrm{Ob}(\mathsf{J})$ and a morphism $h : j_2 \to j_3$ such that $h \circ f = h \circ g$.

Definition 2.4.18 Cofiltered Category

A category J is **cofiltered** if J^{op} is filtered. Equivalently, J is cofiltered if

- J is nonempty.
- For any pair of objects $j_1, j_2 \in \mathrm{Ob}(\mathsf{J})$, there exists an object $j_3 \in \mathrm{Ob}(\mathsf{J})$ and morphisms $j_3 \to j_1$ and $j_3 \to j_2$.
- For any pair of morphisms $f, g : j_1 \to j_2$, there exists an object $j_3 \in \mathrm{Ob}(\mathsf{J})$ and a morphism $h : j_3 \to j_2$ such that $f \circ h = g \circ h$.

Lemma 2.4.19

Let C be a filtered category. Then

(i) Given a finite family of objects $(c_i)_{i=1}^n \subseteq \mathrm{Ob}(\mathsf{C})$, there exists an object $c \in \mathrm{Ob}(\mathsf{C})$ and morphisms $c_i \to c$ for each $i = 1, 2, \cdots, n$.

(ii) Given a finite family of morphisms $(f_i : c \to c')_{i=1}^n \subseteq \mathrm{Hom}(c, c')$, there exists an object $c'' \in \mathrm{Ob}(\mathsf{C})$ and a morphism $g : c' \to c''$ such that $g \circ f_i = g \circ f_j$ for each $i, j = 1, 2, \cdots, n$.

Proof. (i) We prove this by induction on n. For $n = 1$, we can take $c = c_1$ and $f_i = \mathrm{id}_{c_1}$. Suppose the result is valid in the case of $n = k - 1$. Then we can find an object $c' \in \mathrm{Ob}(\mathsf{C})$ and morphisms $g_i : c_i \to c'$ for each $i = 1, 2, \cdots, k-1$. By the definition of filtered category, there exists an object $c \in \mathrm{Ob}(\mathsf{C})$ and morphisms $h' : c' \to c$ and $h : c_k \to c$. Take $f_i = h' \circ g_i$ for each $i = 1, 2, \cdots, k-1$ and $f_n = h$. Then we prove the case of $n = k$.

(ii) We prove this by induction on n. For $n = 1$, this holds trivially. Suppose the result is valid in the case of $n = k - 1$. Then we can find a morphism $h : c' \to c^*$ such that $h \circ f_i = h \circ f_j$ for each $i, j = 1, 2, \cdots, k-1$. By the definition of filtered category, there exists an object $c'' \in \mathrm{Ob}(\mathsf{C})$ and a morphism $h^* : c^* \to c''$ such that $h^* \circ h \circ f_1 = h^* \circ h \circ f_k$. Take $g = h^* \circ h$, then we prove the case of $n = k$.

□

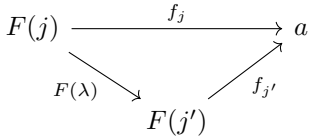
Proposition 2.4.20 Equivalent Characterizations of Filtered Category

The following are equivalent for a category C.

(i) C is filtered.

(ii) For any finite category J and functor $F : \mathsf{J} \to \mathsf{C}$, the exists a cocone from F to an object $c \in \mathrm{Ob}(\mathsf{C})$.

Proof. (i) $\Longrightarrow$ (ii). By Lemma 2.4.19, there exists an object $a \in \mathrm{Ob}(\mathsf{C})$ and morphisms $f_j : F(j) \to a$ for each $j \in \mathrm{Ob}(\mathsf{J})$. For each morphism $\lambda : j \to j'$ in J, we have a pair of parallel morphisms



By Lemma 2.4.19, there exists an object $a_\lambda \in \mathrm{Ob}(\mathsf{C})$ and a morphism $g_\lambda : a \to a_\lambda$ such that

$$g_\lambda \circ f_j = g_\lambda \circ f_{j'} \circ F(\lambda).$$

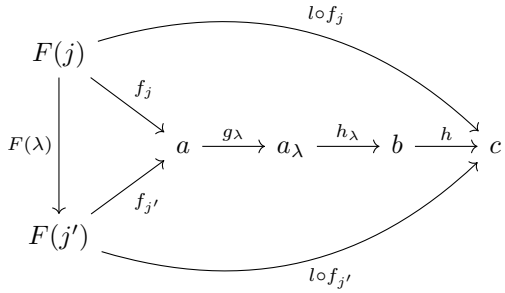
Again by Lemma 2.4.19, we can find an object $b \in \mathrm{Ob}(\mathsf{C})$ and morphisms $h_\lambda : a_\lambda \to b$. Now we have a family of parallel morphisms

$$(h_\lambda \circ g_\lambda : a \longrightarrow b)_{\lambda \in \mathrm{Mor}(\mathsf{J})}.$$

Again by Lemma 2.4.19, there exists an object $c \in \mathrm{Ob}(\mathsf{C})$ and morphisms $h : b \to c$ such that

$$h \circ h_\lambda \circ g_\lambda = h \circ h_{\lambda'} \circ g_{\lambda'}.$$

Hence $l := h \circ h_\lambda \circ g_\lambda$ is a well-defined morphism from a to c. Since the following diagram commutes for any $\lambda \in \mathrm{Mor}(\mathsf{J})$



we have constructed a cocone from F to c

$$(l \circ f_j : F(j) \longrightarrow c)_{j \in \mathrm{Ob}(\mathsf{J})} .$$

□

Definition 2.4.21 Cofiltered limit

A **cofiltered limit** is a limit of a functor $F : \mathsf{J}^{\mathrm{op}} \to \mathsf{C}$ where J is a filtered category.

Definition 2.4.22 Filtered Colimit

A **filtered colimit** is a colimit of a functor $F : \mathsf{J} \to \mathsf{C}$ where J is a filtered category.

Definition 2.4.23 Thin Category

A **thin category** or $(0,1)$**-category** is a category in which any two objects have at most one morphism between them.
A preordered set $(X, \leq)$ can be regarded as a thin category X with objects being elements of X and morphisms being

$$\mathrm{Hom}(x,y) = \begin{cases} \{*\} & \text{if } x \leq y \\ \varnothing & \text{otherwise} \end{cases}$$

Therefore, we obtain a category isomorphism between the category of preordered sets and the category of thin categories

$$\begin{aligned} F : \mathsf{PreOrdSet} &\longrightarrow (0,1)\text{-}\mathsf{Cat} \\ (X, \leq) &\longmapsto \mathsf{X} \end{aligned}$$

Example 2.4.3 Directed Set

A **directed set** (or **filtered set**) is a preordered set in which every finite subset has an upper bound.
A directed set $(X, \leq)$ can be regarded as a filtered (0,1)-category with objects being elements of the set X and morphisms being

$$\mathrm{Hom}(x,y) = \begin{cases} \{*\} & \text{if } x \leq y \\ \varnothing & \text{otherwise} \end{cases}$$

Definition 2.4.24 Inverse Limit

A **inverse system** is a functor $F : \mathsf{J}^{\mathrm{op}} \to \mathsf{C}$ where J is a filtered thin category.
According to Example 2.4.3, J can be regarded as a directed set $(J, \leq)$. Thus inverse system F can be equivalently defined as a family of objects $(F_j)_{j \in J}$ in C together with a family of morphisms $(f_{j,j'} : F_j \leftarrow F_{j'})_{j \leq j'}$ such that

(i) for any $j \in J$, $f_{j,j} = \mathrm{id}_{F_j}$,

(ii) for any $j \leq j' \leq j''$, $f_{j,j''} = f_{j,j'} \circ f_{j',j''}$.

Here, $j \leq j'$ is a short notation for $(j, j') \in \{(j, j') \in J \times J \mid j \leq j'\}$.
A **inverse limit** is a limit of a inverse system.

Example 2.4.4 Pushforward Cone by Functor

Let $\mathsf{J}, \mathsf{C}, \mathsf{D}$ be categories and $K : \mathsf{J} \to \mathsf{C}$, $F : \mathsf{C} \to \mathsf{D}$ be a functor. F induces the following pushforward functor between cone categories

$$\begin{array}{ccc} \mathsf{Cone}(\mathsf{C}, K) & & \mathsf{Cone}(\mathsf{D}, F \circ K) \\ \nabla C \xRightarrow{h} K & & \nabla F(C) \xRightarrow{\mathrm{id}_F \circ h} F \circ K \\ {\scriptstyle \nabla f}\downarrow & \overset{F_*}{\rightsquigarrow} & \downarrow{\scriptstyle \nabla F(f)} \\ \nabla C' \xRightarrow{h'} K & & \nabla F(C') \xRightarrow{\mathrm{id}_F \circ h'} F \circ K \end{array}$$

Definition 2.4.25 Preserve, Reflect, Create Limits

Suppose J, C, D are categories and $K : \mathsf{J} \to \mathsf{C}$ is a diagram. A functor $F : \mathsf{C} \to \mathsf{D}$ is said to

- **preserves** the limit of K if for any cone $\mu \in \mathsf{Cone}(\mathsf{C}, K)$,
$$\mu \text{ is terminal in } \mathsf{Cone}(\mathsf{C}, K) \implies F_*\mu \text{ is terminal in } \mathsf{Cone}(\mathsf{D}, F \circ K)$$
- **reflects** the limit of K if for any cone $\mu \in \mathsf{Cone}(\mathsf{C}, K)$,
$$F_*\mu \text{ is terminal in } \mathsf{Cone}(\mathsf{D}, F \circ K) \implies \mu \text{ is terminal in } \mathsf{Cone}(\mathsf{C}, K)$$
- **creates** the limit of K if
  - F reflects the limit of K, and
  - if η is terminal in $\mathsf{Cone}(\mathsf{D}, F \circ K)$, then there exists a cone μ in $\mathsf{Cone}(\mathsf{C}, K)$ such that $F_*\mu$ is terminal in $\mathsf{Cone}(\mathsf{D}, F \circ K)$.
- **strictly creates** the limit of K if for any terminal object $\eta \in \mathsf{Cone}(\mathsf{D}, F \circ K)$,
  - there exists a unique cone μ in $\mathsf{Cone}(\mathsf{C}, K)$ such that $F_*\mu = \eta$, and
  - moreover, μ is terminal in $\mathsf{Cone}(\mathsf{C}, K)$.

Suppose $\mathcal{K} \subseteq \mathrm{Ob}([\mathsf{J}, \mathsf{C}])$ is a class of diagrams valued in C. We say that F preserves (reflects, creates, strictly creates) limits for $\mathcal{K}$ if it preserves (reflects, creates, strictly creates) limits for each diagram $K : \mathsf{J} \to \mathsf{C}$ in $\mathcal{K}$.
We say that F preserves (reflects, creates, strictly creates) limits of shape J if it preserves (reflects, creates, strictly creates) limits for all diagrams $K : \mathsf{J} \to \mathsf{C}$.

It is clear from the definition that if a functor F strictly creates the limit of a diagram K, then it creates the limit of K.

Proposition 2.4.26

Suppose J, C, D are categories and $\mathcal{K} \subseteq \mathrm{Ob}([\mathsf{J}, \mathsf{C}])$ is a class of diagrams valued in C. If $F : \mathsf{C} \to \mathsf{D}$ creates limits for $\mathcal{K}$ and $\varprojlim_{\mathsf{J}} F \circ K$ exists for each $K \in \mathcal{K}$, then $\varprojlim_{\mathsf{J}} K$ exists for each $K \in \mathcal{K}$ and F preserves them.

Proof. For any diagram $K : \mathsf{J} \to \mathsf{C}$ in $\mathcal{K}$, the hypothesis asserts that there is a cone $\mu : \nabla d \Rightarrow F \circ K$ in $\mathsf{Cone}(\mathsf{D}, F \circ K)$. As F creates these limits, there must be a limit cone $\lambda : \nabla c \Rightarrow K$ in $\mathsf{Cone}(\mathsf{C}, K)$ such that

$F_*\lambda : \nabla F(c) \Rightarrow F \circ K$ is a limit cone. Since F reflects limits, λ is a limit cone, which means that C admits limits for $\mathcal{K}$. To see that F preserves them, consider another limit cone $\lambda' : \nabla c' \Rightarrow K$. The two limit cones in $\mathsf{Cone}(\mathsf{C}, K)$ are isomorphic and by composing isomorphisms we see that the cone $F\lambda' : \nabla Fc' \Rightarrow F \circ K$ is isomorphic to the limit cone $\mu : \nabla d \Rightarrow F \circ K$. This implies that $F\lambda' : Fc' \Rightarrow FK$ is again a limit cone, proving that F preserves these limits. □

Definition 2.4.27 Conservative Functor

A functor $F : \mathsf{C} \to \mathsf{D}$ is **conservative** if it reflects isomorphisms. Equivalently, F is a conservative functor if for any morphism f in C,

$$f \text{ is an isomorphism in } \mathsf{C} \iff F(f) \text{ is an isomorphism in } \mathsf{D}.$$

Proposition 2.4.28

Suppose $K : \mathsf{J} \to \mathsf{C}$ is a diagram and $F : \mathsf{C} \to \mathsf{D}$ is a conservative functor. If $\varprojlim K$ exists, and F preserves $\varprojlim K$, then F reflects $\varprojlim K$.

Proposition 2.4.29 Fully Faithful Functor Reflects Limits

Any full and faithful functor reflects all limits and colimits.

Proof. Let $F : \mathsf{C} \to \mathsf{D}$ be a full and faithful functor. Suppose $K : \mathsf{J} \to \mathsf{C}$ is a diagram,

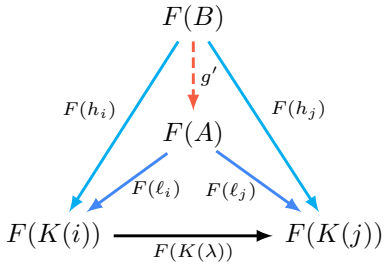
$$(\ell_i : A \to K(i))_{i \in \mathrm{Ob}(\mathsf{J})} \in \mathsf{Cone}\,(\mathsf{C}, K)$$

is a cone over K, and $(F(\ell_i) : F(A) \to F \circ K(i))_{i \in \mathrm{Ob}(\mathsf{J})}$ is a limit cone over $F \circ K$. We want to show that $(\ell_i)_{i \in \mathrm{Ob}(\mathsf{J})}$ is initial in $\mathsf{Cone}\,(\mathsf{C}, K)$.

Suppose $(h_i : B \to K(i))_{i \in \mathrm{Ob}(\mathsf{J})} \in \mathsf{Cone}\,(\mathsf{C}, K)$ is another cone over K. Then

$$(F(h_i) : F(B) \longrightarrow F \circ K(i))_{i \in \mathrm{Ob}(\mathsf{J})} \in \mathsf{Cone}\,(\mathsf{D}, F \circ K)$$

is a cone over $F \circ K$. By the universal property of $F(A)$, there exists a unique morphism $g' : F(B) \to F(A)$ such that $F(\ell_i) \circ g' = F(h_i)$ for each $i \in \mathrm{Ob}(\mathsf{J})$



Since F is full and faithful, there exists a unique morphism $g : B \to A$ such that $F(g) = g'$. We can check that

$$F(\ell_i \circ g) = F(\ell_i) \circ F(g) = F(\ell_i) \circ g' = F(h_i) \implies \ell_i \circ g = h_i.$$

If there exists another morphism $q : B \to A$ such that $\ell_i \circ q = h_i$ for all $i \in \mathrm{Ob}(\mathsf{J})$, then we have

$$\forall i \in \mathrm{Ob}(\mathsf{J}),\ F(\ell_i \circ q) = F(\ell_i) \circ F(q) = F(h_i) \implies F(q) = g' \implies q = g.$$

Thus we show that $(\ell_i : A \to K(i))_{i \in \mathrm{Ob}(\mathsf{J})}$ is initial in $\mathsf{Cone}\,(\mathsf{C}, K)$. □

Proposition 2.4.30

Suppose $\mathcal{K} \subseteq \mathrm{Ob}([\mathsf{J}, \mathsf{C}])$. If $F : \mathsf{C} \to \mathsf{D}$ creates limits for $\mathcal{K}$ and $\varprojlim F \circ K$ exists for all $K \in \mathcal{K}$, then $\varprojlim K$ exists for all $K \in \mathcal{K}$ and F preserves limits for $\mathcal{K}$.

Proof. For any $K \in \mathcal{K}$, since $\varprojlim F \circ K$ exists and F creates limits for $\mathcal{K}$, there exists a limit cone

$$\left(\ell_i : \varprojlim K \to K(i)\right)_{i \in \mathrm{Ob}(\mathsf{J})} \in \mathsf{Cone}\left(\mathsf{C}, K\right)$$

such that

$$\left(F(\ell_i) : F\left(\varprojlim K\right) \to F \circ K(i)\right)_{i \in \mathrm{Ob}(\mathsf{J})} \in \mathsf{Cone}\left(\mathsf{D}, F \circ K\right)$$

is terminal in $\mathsf{Cone}\left(\mathsf{D}, F \circ K\right)$, i.e it is a limit cone over $F \circ K$. Given any limit cone in $\mathsf{Cone}\left(\mathsf{C}, K\right)$, it is isomorphic to $(\ell_i)_{i \in \mathrm{Ob}(\mathsf{J})}$, which implies that its image under F is isomorphic to $(F(\ell_i))_{i \in \mathrm{Ob}(\mathsf{J})}$. Thus we show F preserves limits for $\mathcal{K}$. □

Theorem 2.4.31 Existance Theorem for Limits

Let C be a category and $F : \mathsf{J} \to \mathsf{C}$ be a functor. If a category C has equalizers and all products indexed by the classes $\mathrm{Ob}(\mathsf{J})$ and $\mathrm{Hom}(\mathsf{J})$, then C has all limits of shape J.

Proposition 2.4.32

Suppose A is a small category. Denote $\mathsf{Ob}(\mathsf{A}) = \mathsf{Disc}\left(\mathrm{Ob}\left(\mathsf{A}\right)\right)$. Then the forgetful functor $U : [\mathsf{A}, \mathsf{C}] \to [\mathsf{Ob}(\mathsf{A}), \mathsf{C}] \cong \prod_{a \in \mathrm{Ob}(\mathsf{A})} \mathsf{C}$

$$\begin{array}{ccc} [\mathsf{A}, \mathsf{C}] & & \prod\limits_{a \in \mathsf{Ob}(\mathsf{A})} \mathsf{C} \\ F & & (F(a))_{a \in \mathrm{Ob}(\mathsf{A})} \\ \theta \Downarrow & \overset{U}{\rightsquigarrow} & \downarrow \prod\limits_{a \in \mathrm{Ob}(\mathsf{A})} \theta_a \\ G & & (G(a))_{a \in \mathrm{Ob}(\mathsf{A})} \end{array}$$

strictly creates all limits and colimits that exist in C. These limits are defined objectwise, meaning that for each $a \in \mathrm{Ob}(\mathsf{A})$, the evaluation functor $\mathrm{ev}_a : [\mathsf{A}, \mathsf{C}] \to \mathsf{C}$ preserves all limits and colimits existing in C.

Proof. Given a diagram $F : \mathsf{J} \to [\mathsf{A}, \mathsf{C}]$, suppose the limit $\varprojlim U \circ F$ exists and can be written as

$$\left((L(a))_{a \in \mathrm{Ob}(\mathsf{A})}, \left(\ell_j = (\ell_{j,a} : L(a) \to F(j)(a))_{a \in \mathrm{Ob}(\mathsf{A})}\right)_{j \in \mathrm{Ob}(\mathsf{J})}\right).$$

□

The next result shows that functor categories inherit limits and colimits, defined "objectwise" in the target category: that is, given a J-indexed diagram in $[\mathsf{A}, \mathsf{C}]$ whose objects are functors $F_j : \mathsf{A} \to \mathsf{C}$, the value of the limit functor $\varprojlim_{j \in J} F_j : \mathsf{A} \to \mathsf{C}$ at an object $a \in \mathsf{A}$ is the limit of the J-indexed diagram in C whose objects are the objects $F_j(a) \in \mathrm{Ob}(\mathsf{C})$, which reads as follows:

$$\left(\varprojlim_{j \in J} F_j\right)(a) = \varprojlim_{j \in J} F_j(a).$$

Proposition 2.4.33 Evaluation Functor Preserves Limits

Let A be a small category and C be a category. Given a diagram $F : \mathsf{J} \to [\mathsf{A}, \mathsf{C}]$ with J small, if for any $a \in \mathsf{A}$, the diagram

$$\mathrm{ev}_a \circ F : \mathsf{J} \xrightarrow{F} [\mathsf{A}, \mathsf{C}] \xrightarrow{\mathrm{ev}_a} \mathsf{C}$$

has a limit, then

(i) $\varprojlim F$ exists.

(ii) For any $a \in \mathsf{A}$, ev_a preserves $\varprojlim F$.

Definition 2.4.34 Exact Functor

Let F be a functor between finitely complete categories categories C and D.

- F is **left exact** if it preserves finite limits.
- F is **right exact** if it preserves finite colimits.
- F is **exact** if it is both left and right exact.

Example 2.4.5 Limit in Set

Let $F : \mathsf{J} \to \mathsf{Set}$ be a functor. Then

$$\varprojlim F \cong \left\{ (x_i)_{i\in \mathrm{Ob}(\mathsf{J})} \in \prod_{i\in \mathrm{Ob}(\mathsf{J})} F(i) \;\middle|\; \forall \lambda : i \to j \text{ in } \mathrm{Hom}_{\mathsf{J}}(i,j),\ F(\lambda)(x_i) = x_j \right\}$$

where α and β are defined by and the map $\ell_i : \varprojlim F \to F(i)$ is given by the composition

$$\varprojlim F \xrightarrow{\ \iota\ } \prod_{i\in \mathrm{Ob}(\mathsf{J})} F(i) \xrightarrow{\ \pi_i\ } F(i).$$

$\varprojlim F$ also can be constructed from product and equalizer

$$\varprojlim F \cong \ker \left[\prod_{i\in \mathrm{Ob}(\mathsf{J})} F(i) \underset{\beta}{\overset{\alpha}{\rightrightarrows}} \prod_{\lambda\in \mathrm{Mor}(\mathsf{J})} F(\mathrm{codom}\,(\lambda)) \right]$$

where α and β are induced by the following diagrams

$$\begin{array}{ccccc}
F(\mathrm{dom}\,(\lambda)) & \xleftarrow{\ \pi_{\mathrm{dom}(\lambda)}\ } & \prod_{i\in \mathrm{Ob}(\mathsf{J})} F(i) & \ni & (x_i)_{i\in \mathrm{Ob}(\mathsf{J})} \\
\downarrow{\scriptstyle F(\lambda)} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} \\
F(\mathrm{codom}\,(\lambda)) & \xleftarrow[\ \pi_\lambda\ ]{} & \prod_{\lambda\in \mathrm{Mor}(\mathsf{J})} F(\mathrm{codom}\,(\lambda)) & \ni & (F(\lambda)(x_i))_{\lambda : i\to j \in \mathrm{Mor}(\mathsf{J})}
\end{array}$$

$$\begin{array}{ccccc}
 & & \prod_{i\in \mathrm{Ob}(\mathsf{J})} F(i) & \ni & (x_i)_{i\in \mathrm{Ob}(\mathsf{J})} \\
 & \overset{\pi_{\mathrm{codom}(\lambda)}}{\swarrow} & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \beta} \\
F(\mathrm{codom}\,(\lambda)) & \xleftarrow[\ \pi_\lambda\ ]{} & \prod_{\lambda\in \mathrm{Mor}(\mathsf{J})} F(\mathrm{codom}\,(\lambda)) & \ni & (x_j)_{\lambda : i\to j \in \mathrm{Mor}(\mathsf{J})}
\end{array}$$

Example 2.4.6 Colimit in Set

Let $F : \mathsf{J} \to \mathsf{Set}$ be a functor. Define a relation $\sim^*$ on $\coprod_{i\in \mathrm{Ob}(\mathsf{J})} F(i)$: for any $(i,x),(j,y) \in \coprod_{i\in \mathrm{Ob}(\mathsf{J})} F(i)$,

$$(i,x) \sim^* (j,y) \iff \text{there exists } \lambda : i \to j \text{ in } \mathrm{Hom}_{\mathsf{J}}(i,j) \text{ such that } F(\lambda)(x) = y.$$

Let $\sim$ denote the equivalence relation generated by $\sim^*$. Then

$$\varinjlim F \cong \coprod_{i\in \mathrm{Ob}(\mathsf{J})} F(i)/\sim$$

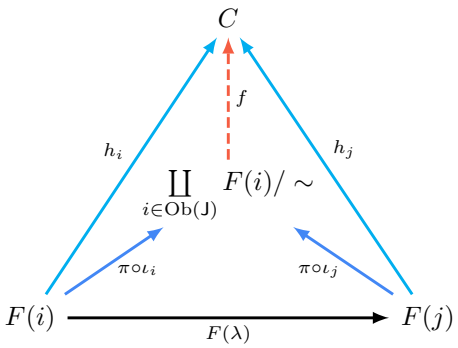
and the map $\ell_i : F(i) \to \varinjlim F$ is given by the composition

$$F(i) \xrightarrow{\iota_i} \coprod_{i\in \mathrm{Ob(J)}} F(i) \xrightarrow{\pi} \coprod_{i\in \mathrm{Ob(J)}} F(i)/\sim .$$

Proof. It is straightforward to show

$$\varinjlim F \cong \coprod_{i\in \mathrm{Ob(J)}} F(i)/\sim$$

by checking the universal property of $\varinjlim F$



First, we check that for any morphism $\lambda : i \to j$ in J and any $x \in F(i)$, we have

$$\ell_i(x) = \pi \circ \iota_i(x) = [(i, x)]_\sim = [(j, F(\lambda)(x))]_\sim = \pi \circ \iota_j(F(\lambda)(x)) = \ell_j \circ F(\lambda)(x).$$

Suppose $(C, (h_i)_{i\in \mathrm{Ob(J)}})$ is a cone over F, then by the universal property of coproduct, there a unique map $g : \coprod_{i\in \mathrm{Ob(J)}} F(i) \to C$ defined by $g(i, x) = h_i(x)$ such that $g \circ \iota_i = h_i$. Note that if $(i, x) \sim (j, y)$, then we can suppose there exists $\lambda : i \to j$ such that $F(\lambda)(x) = y$. Hence $h(i, x) = h_i(x) = h_j(F(\lambda)(x)) = h_j(y) = h(j, y)$. Then by the universal property of quotient set, there exists a unique map $f : \coprod_{i\in \mathrm{Ob(J)}} F(i)/\sim \to C$ such that $f \circ \pi = g$. Thus we have

$$f \circ \ell_i = f \circ \pi \circ \iota_i = g \circ \iota_i = h_i.$$

What is left is to show that f is unique. Suppose there exists another map $f' : \coprod_{i\in \mathrm{Ob(J)}} F(i)/\sim \to C$ such that

$$f' \circ \ell_i = f' \circ \pi \circ \iota_i = g \circ \iota_i = h_i.$$

By the universal property of coproduct, we have $f' \circ \pi = g = f \circ \pi$. Since π is surjective, there must be $f' = f$. □

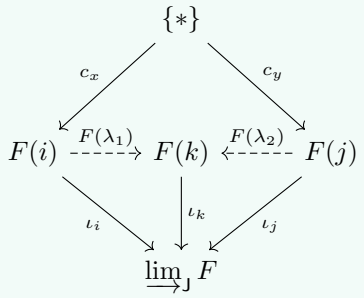
Example 2.4.7 Filtered Colimit in Set

Let $F : \mathsf{J} \to \mathsf{Set}$ be a functor and J is a filtered category, then the colimit $\varinjlim_{\mathsf{J}} F$ has an explicit description

$$\varinjlim_{\mathsf{J}} F \cong \left(\coprod_{j\in \mathrm{Ob(J)}} F(j) \right) / \sim$$

where the equivalence relation $\sim$ is defined as follows: for any $(i, x), (j, y) \in \coprod_{i\in \mathrm{Ob(J)}} F(i)$,

$$(i, x) \sim (j, y) \iff \text{there exists } \lambda_1 : i \to k \text{ and } \lambda_2 : j \to k \text{ such that } F(\lambda_1)(x) = F(\lambda_2)(y).$$



Proof. If J is a filtered category, first we can check

$$(i,x) \approx (j,y) \iff \text{there exists } \lambda_1 : i \to k \text{ and } \lambda_2 : j \to k \text{ such that } F(\lambda_1)(x) = F(\lambda_2)(y).$$

is an equivalence relation that $\approx$ contains $\sim^*$. It is clear an equivalence relation. If $(i,x) \sim^* (j,y)$, then there exists $\lambda : i \to j$ such that $F(\lambda)(x) = y$. Hence there exists $\lambda_1 = \lambda$ and $\lambda_2 = \mathrm{id}_j$ such that $F(\lambda_1)(x) = F(\lambda_2)(y)$. Thus we have $\sim^* \subseteq \approx$.

To show $\approx = \sim$, let's assume $\backsimeq$ is any equivalence relation containing $\sim^*$. If $(i,x) \approx (j,y)$, then there exists $\lambda_1 : i \to k$ and $\lambda_2 : j \to k$ such that $F(\lambda_1)(x) = F(\lambda_2)(y) = z$. Hence

$$(i,x) \sim^* (k,z) \text{ and } (j,y) \sim^* (k,z) \implies (i,x) \backsimeq (k,z) \text{ and } (j,y) \backsimeq (k,z) \implies (i,x) \backsimeq (j,y).$$

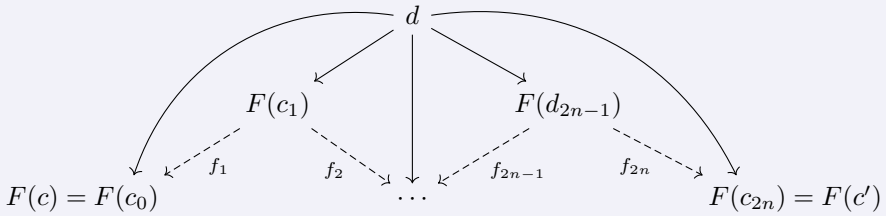
This implies $\backsimeq$ contains $\approx$. Therefore, $\approx$ is the smallest equivalence relation containing $\sim^*$, which means $\approx$ coincides with $\sim$. □

Definition 2.4.35 Final Functor

A functor $F : \mathsf{C} \to \mathsf{D}$ is **final** if for every object $d \in \mathsf{D}$, the comma category $(d \downarrow F)$ obtained from

$$\mathbb{1} \xrightarrow{\mathrm{const}_d} \mathsf{D} \xleftarrow{F} \mathsf{C}$$

is connected. That is, given any $d \in \mathrm{Ob}(\mathsf{D})$, $(d \downarrow F)$ is nonempty, and for any morphisms $d \to F(c)$ and $d \to F(c')$ there exists a zigzag of morphisms $(f_1, f_2, \cdots, f_{2n})$ such that the following diagram commutes

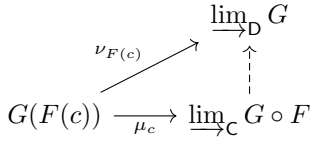


Lemma 2.4.36

Let $F : \mathsf{C} \to \mathsf{D}$ and $G : \mathsf{D} \to \mathsf{E}$ be functors. If both $\varinjlim G \circ F$ and $\varinjlim G$ exist, then there exists a natural morphism between colimits

$$\varinjlim G \circ F \longrightarrow \varinjlim G$$

Proof. Suppose $\mu : G \circ F \Rightarrow \triangle \varinjlim_{\mathsf{C}} G \circ F$ is a colimit cone in $\mathsf{Cocone}(G \circ F, \mathsf{E})$ and $\nu : G \Rightarrow \triangle \varinjlim_{\mathsf{D}} G$ is a colimit cone in $\mathsf{Cocone}(G, \mathsf{E})$. Then by universal property of $\varinjlim G \circ F$, we can get the following commutative diagram



□

Proposition 2.4.37 Equivalent Characterization of Final Functor

Let $F : \mathsf{C} \to \mathsf{D}$ be a functor. The following are equivalent:

(i) F is final.

(ii) For any functor $G : \mathsf{D} \to \mathsf{E}$, the natural morphism between colimits

$$\varinjlim G \circ F \longrightarrow \varinjlim G$$

is an isomorphism.

Note that $d \in \mathrm{Ob}(\mathsf{D})$ is a final object in D if and only if the functor $\mathrm{const}_d : \mathbb{1} \to \mathsf{D}$ is final.

Definition 2.4.38 Initial Functor

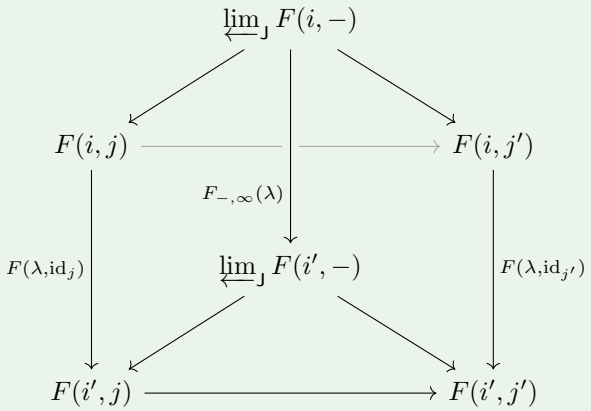
A functor $F : \mathsf{C} \to \mathsf{D}$ is **initial** if the opposite functor $F^{\mathrm{op}} : \mathsf{C}^{\mathrm{op}} \to \mathsf{D}^{\mathrm{op}}$ is final.

Proposition 2.4.39 Limits Commute with Limits

Let $F : \mathsf{I} \times \mathsf{J} \to \mathsf{C}$ be a functor. Suppose for each $i \in \mathrm{Ob}(\mathsf{I})$, the limit of the diagram $F(i, -) : \mathsf{J} \to \mathsf{C}$ exists and is denoted by $F_{i,\infty} := \varprojlim_{\mathsf{J}} F(i, -)$. Define a diagram $F_{-,\infty} : \mathsf{I} \to \mathsf{C}$ as follows

$$\begin{array}{ccc} \mathsf{I} & & \mathsf{C} \\ i & & \varprojlim_{\mathsf{J}} F(i,-) \\ {\scriptstyle\lambda}\downarrow & \overset{F_{-,\infty}}{\rightsquigarrow} & \downarrow{\scriptstyle F_{-,\infty}(\lambda)} \\ i' & & \varprojlim_{\mathsf{J}} F(i',-) \end{array}$$

where $F_{-,\infty}(\lambda)$ is induced by the universal property of $\varprojlim_{\mathsf{J}} F(i', -)$



Then $\varprojlim_{\mathsf{I}} F_{-,\infty}$ exists $\iff$ $\varprojlim_{\mathsf{I}\times\mathsf{J}} F$ exists. Moreover, if either $\varprojlim_{\mathsf{I}} F_{-,\infty}$ or $\varprojlim_{\mathsf{I}\times\mathsf{J}} F$ exists, we have natural isomorphism

$$\varprojlim_{\mathsf{I}\times\mathsf{J}} F \cong \varprojlim_{\mathsf{I}} F_{-,\infty}.$$

Similarly, Suppose for each $j \in \mathrm{Ob}(\mathsf{J})$, the limit of the diagram $F(-, j) : \mathsf{I} \to \mathsf{C}$ exists and is denoted by $F_{\infty,j} := \varprojlim_{\mathsf{I}} F(-, j)$. Then $\varprojlim_{\mathsf{J}} F_{\infty,-}$ exists if and only if $\varprojlim_{\mathsf{I}\times\mathsf{J}} F$ exists. Moreover, if either $\varprojlim_{\mathsf{J}} F_{\infty,-}$ or $\varprojlim_{\mathsf{I}\times\mathsf{J}} F$ exists, we have natural isomorphism

$$\varprojlim_{\mathsf{I}\times\mathsf{J}} F \cong \varprojlim_{\mathsf{J}} F_{\infty,-}.$$

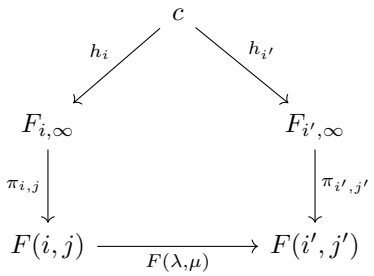
Proof. For any cone

$$h = \left(c \xrightarrow{h_i} F_{i,\infty}\right)_{i\in \mathrm{Ob}(\mathsf{I})} \in \mathrm{Ob}\left(\mathsf{Cone}\left(\mathsf{C}, \varprojlim F_{-,\infty}\right)\right),$$

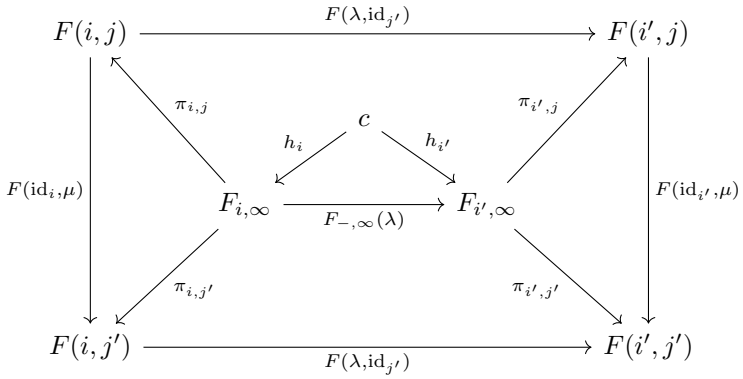
we can construct a cone

$$\phi(h) := \left(c \xrightarrow{h_i} F_{i,\infty} \xrightarrow{\pi_{i,j}} F(i,j)\right)_{(i,j)\in \mathrm{Ob}(\mathsf{I}\times\mathsf{J})} \in \mathrm{Ob}\left(\mathsf{Cone}\left(\mathsf{C}, \varprojlim F\right)\right).$$

To verify it is a cone, we need to check for any morphism $(\lambda, \mu) : (i, j) \to (i', j)$ in $\mathsf{I} \times \mathsf{J}$, the following diagram commutes



Note that $F(\lambda, \mu) = F(\mathrm{id}_{i'}, \mu) \circ F(\lambda, \mathrm{id}_{j'})$. It is sufficient to show the following diagram commutes



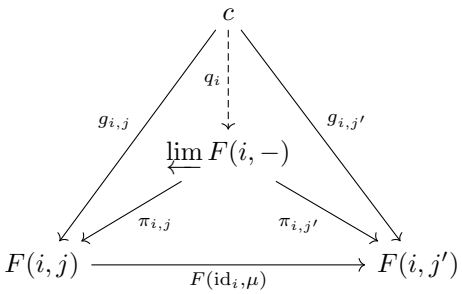
Conversely, for any cone

$$g = \left(c \xrightarrow{g_{i,j}} F(i,j)\right)_{(i,j)\in \mathrm{Ob}(\mathsf{I}\times\mathsf{J})} \in \mathrm{Ob}\left(\mathsf{Cone}\left(\mathsf{C}, \varprojlim F\right)\right),$$

we can construct a cone

$$\psi(g) := \left(c \xrightarrow{q_i} F_{i,\infty}\right)_{i\in \mathrm{Ob}(\mathsf{I})} \in \mathrm{Ob}\left(\mathsf{Cone}\left(\mathsf{C}, \varprojlim F_{-,\infty}\right)\right).$$

through the universal property of $\varprojlim F(i,-)$



□

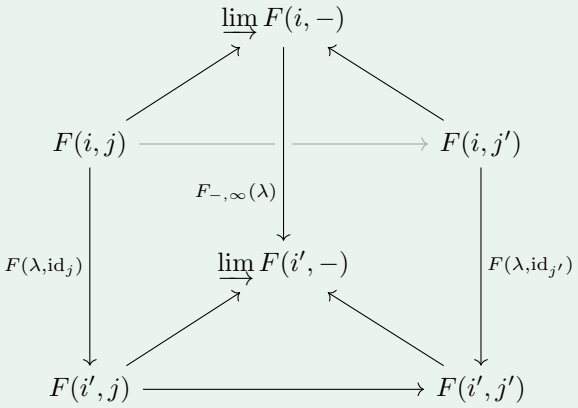
Proposition 2.4.40 Colimits Commute with Colimits

Let $F : \mathsf{I} \times \mathsf{J} \to \mathsf{C}$ be a functor. Suppose for each $i \in \mathrm{Ob}(\mathsf{I})$, the colimit of the diagram $F(i,-) : \mathsf{J} \to \mathsf{C}$

exists and is denoted by $F_{i,\infty} := \varinjlim F(i,-)$. Define a diagram $F_{-,\infty} : \mathsf{I} \to \mathsf{C}$ as follows

$$\begin{array}{ccc} \mathsf{I} & & \mathsf{C} \\ i & & \varinjlim F(i,-) \\ {\scriptstyle\lambda}\downarrow & \overset{F_{-,\infty}}{\rightsquigarrow} & \downarrow{\scriptstyle F_{-,\infty}(\lambda)} \\ i' & & \varinjlim F(i',-) \end{array}$$

where $F_{-,\infty}(\lambda)$ is induced by the universal property of $\varinjlim F(i,-)$



Then $\varinjlim F_{-,\infty}$ exists if and only if $\varinjlim F$ exists. Moreover, if $\varinjlim F$ exists, we have natural isomorphism

$$\varinjlim F \cong \varinjlim F_{-,\infty}.$$

Proof. This can be proved by duality. Here we give another proof.

$$\begin{array}{ccccc} [\mathsf{I},\mathsf{C}] & \xleftarrow{\nabla_{\mathsf{I}}} & \mathsf{C} & \xrightarrow{\nabla_{\mathsf{J}}} & [\mathsf{J},\mathsf{C}] \\ {\scriptstyle\nabla_{\mathsf{J}}}\downarrow & & {\scriptstyle\nabla_{\mathsf{I}\times\mathsf{J}}}\downarrow & & \downarrow{\scriptstyle\nabla_{\mathsf{I}}} \\ [\mathsf{J},[\mathsf{I},\mathsf{C}]] & \xrightarrow{\cong} & [\mathsf{I}\times\mathsf{J},\mathsf{C}] & \xleftarrow{\cong} & [\mathsf{I},[\mathsf{J},\mathsf{C}]] \end{array}$$

Using the adjunction between $\varprojlim$ and ∇

$$[\mathsf{J},\mathsf{C}] \underset{\nabla_{\mathsf{J}}}{\overset{\varinjlim_{\mathsf{J}}}{\rightleftarrows}} \mathsf{C} \quad (\perp)$$

we have

$$\begin{array}{ccccc} [\mathsf{I},\mathsf{C}] & \xrightarrow{\varinjlim_{\mathsf{I}}} & \mathsf{C} & \xleftarrow{\varinjlim_{\mathsf{J}}} & [\mathsf{J},\mathsf{C}] \\ {\scriptstyle\varinjlim_{\mathsf{J}}}\uparrow & & {\scriptstyle\varinjlim_{\mathsf{I}\times\mathsf{J}}}\uparrow & & \uparrow{\scriptstyle\varinjlim_{\mathsf{I}}} \\ [\mathsf{J},[\mathsf{I},\mathsf{C}]] & \xleftarrow{\cong} & [\mathsf{I}\times\mathsf{J},\mathsf{C}] & \xrightarrow{\cong} & [\mathsf{I},[\mathsf{J},\mathsf{C}]] \end{array}$$

□

Definition 2.4.41 I-colimits commute with J-limits in C

Let I, J, C be categories. Suppose C has all I-shaped colimits and all J-shaped limits. Then for any functor

$F : \mathsf{I} \times \mathsf{J} \to \mathsf{C}$, there is canonical morphism

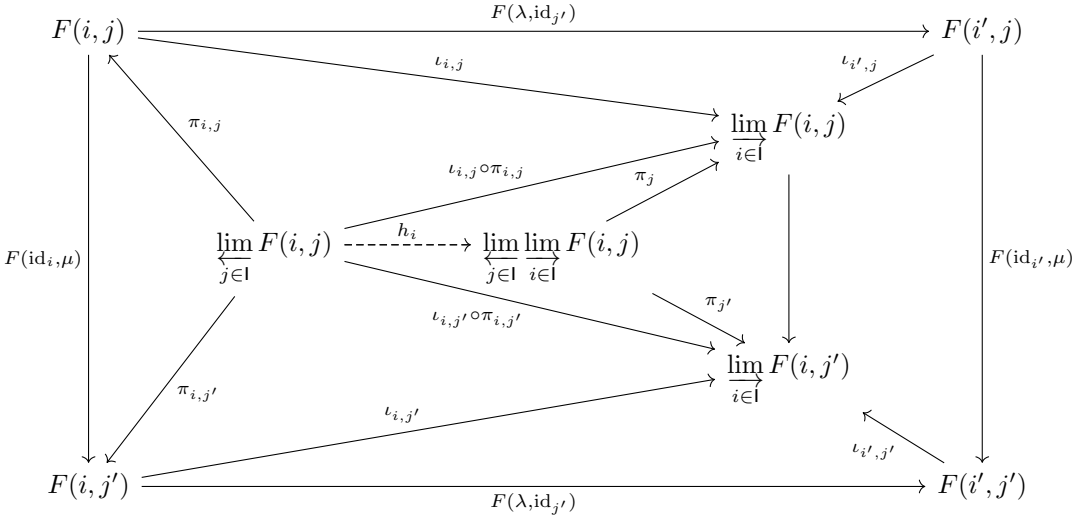
$$h : \varinjlim_{i\in\mathsf{I}} \varprojlim_{j\in\mathsf{J}} F(i,j) \longrightarrow \varprojlim_{j\in\mathsf{J}} \varinjlim_{i\in\mathsf{I}} F(i,j)$$

If this morphism is an isomorphism, we say **I-colimits commute with J-limits in C**.

Proof. First for any $i \in \mathrm{Ob}(\mathsf{I})$, we can construct a cone

$$\left(\varprojlim_{j\in\mathsf{I}} F(i,j) \xrightarrow{\pi_{i,j}} F(i,j) \xrightarrow{\iota_{i,j}} \varinjlim_{i\in\mathsf{I}} F(i,j)\right)_{j\in\mathrm{Ob}(\mathsf{J})} \in \mathrm{Ob}\left(\mathsf{Cone}\left(\mathsf{C}, \varinjlim_{j\in\mathsf{I}} F(i,j)\right)\right).$$

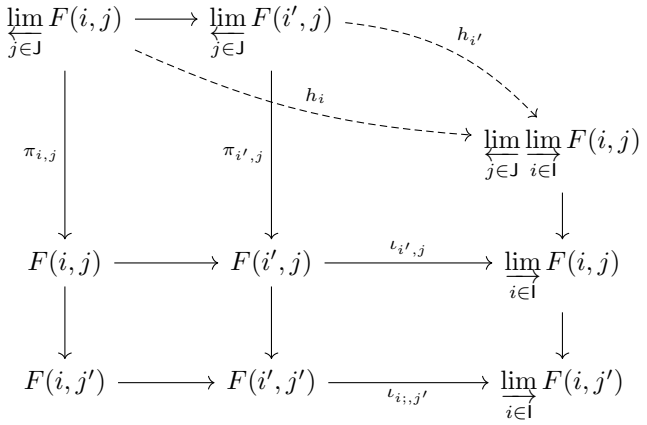
And by the universal property of $\varinjlim_{j\in\mathsf{I}} \varprojlim_{i\in\mathsf{I}} F(i,j)$, we can induce a morphism $h_i : \varprojlim_{j\in\mathsf{I}} F(i,j) \to \varinjlim_{j\in\mathsf{I}} \varprojlim_{i\in\mathsf{I}} F(i,j)$ such that the following diagram commutes



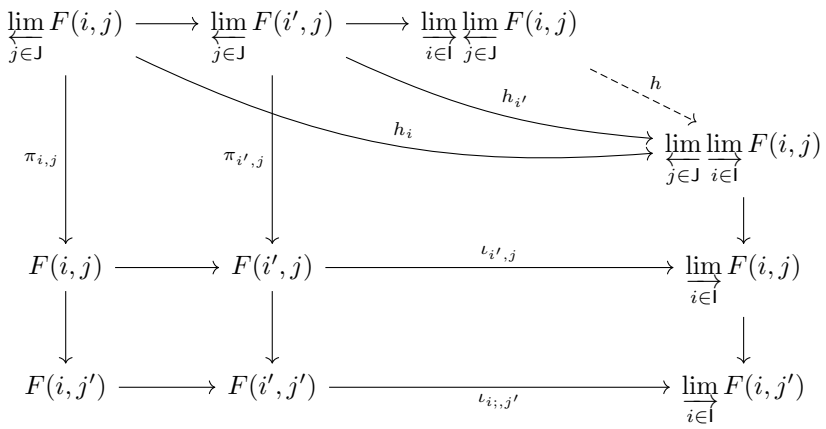
Doing this for each $i \in \mathrm{Ob}(\mathsf{I})$, we can get a cocone

$$\left(\varprojlim_{j\in\mathsf{I}} F(i,j) \xrightarrow{h_i} \varinjlim_{j\in\mathsf{J}} \varprojlim_{i\in\mathsf{I}} F(i,j)\right)_{i\in\mathrm{Ob}(\mathsf{I})} \in \mathrm{Ob}\left(\mathsf{Cocone}\left(\mathsf{C}, \varinjlim_{j\in\mathsf{J}} \varprojlim_{i\in\mathsf{I}} F(i,j)\right)\right),$$

which is shown in the following commutative diagram



Finally, by the universal property of $\varinjlim_{i\in\mathsf{I}}\varprojlim_{j\in\mathsf{J}} F(i,j)$, we can induce a morphism



□

Proposition 2.4.42

Let I, J, C be categories. Suppose C has all I-shaped colimits and all J-shaped limits. Then the following are equivalent:

(i) I-colimits commute with J-limits in C.

(ii) The functor $\varinjlim_{\mathsf{I}} : [\mathsf{I},\mathsf{C}] \to \mathsf{C}$ preserves all J-shaped limits.

(iii) The functor $\varprojlim_{\mathsf{J}} : [\mathsf{J},\mathsf{C}] \to \mathsf{C}$ preserves all I-shaped colimits.

Proposition 2.4.43

In Set, we have

(i) Filtered colimits commute with finite limits.

(ii) Coproducts commute with connected limits.

Proof. (i) Let I be a filtered category and J be a finite category. Let $F : \mathsf{I}\times\mathsf{J} \to \mathsf{Set}$ be a functor.

First we prove the canonical map

$$\begin{aligned} h : \varinjlim_{i\in\mathsf{I}}\varprojlim_{j\in\mathsf{J}} F(i,j) &\longrightarrow \varprojlim_{j\in\mathsf{J}}\varinjlim_{i\in\mathsf{I}} F(i,j) \\ \left[(a_j)_{j\in\mathrm{Ob}(\mathsf{J})}\right] &\longmapsto ([a_j])_{j\in\mathrm{Ob}(\mathsf{J})} \end{aligned}$$

is injective. Let $a = \left[(a_j)_{j\in\mathrm{Ob}(\mathsf{J})}\right]$ with $a_j \in F(i,j)$ and $b = \left[(b_j)_{j\in\mathrm{Ob}(\mathsf{J})}\right]$ with $b_j \in F(i',j)$. If $h(a) = h(b)$, then for each $j \in \mathrm{Ob}(\mathsf{J})$, we have $[a_j] = [b_j]$ in $\varinjlim_{i\in\mathsf{I}} F(i,j)$, which implies there exists morphisms $\varphi_j : i \to i_j$ and $\psi_j : i' \to i_j$ in I such that

$$F(\varphi_j, \mathrm{id}_j)(a_j) = F(\psi_j, \mathrm{id}_j)(b_j)$$

holds in $F(i_j, j)$. Consider the subcategory W of I consisting of φ_j and ψ_j for all $j \in \mathrm{Ob}(\mathsf{J})$. By Proposition 2.4.20, there exists a cocone from $H : \mathsf{W} \hookrightarrow \mathsf{I}$ to $m \in \mathrm{Ob}(\mathsf{J})$.

$$\left(\begin{array}{ccccc} & & m & & \\ & \overset{\varphi}{\nearrow} & \uparrow{\scriptstyle \eta_j} & \overset{\psi}{\nwarrow} & \\ i & \xrightarrow[\varphi_j]{} & i_j & \xleftarrow[\psi_j]{} & i' \end{array}\right)_{j\in\mathrm{Ob}(\mathsf{J})} \in \mathrm{Ob}\left(\mathsf{Cocone}\left(H, \mathsf{I}\right)\right).$$

This implies for any $j \in \mathrm{Ob}(\mathsf{J})$,

$$\begin{aligned} F(\varphi, \mathrm{id}_j)(a_j) &= F(\eta_i \circ \varphi_j, \mathrm{id}_j)(a_j) \\ &= F(\eta_i, \mathrm{id}_j) \circ F(\varphi_j, \mathrm{id}_j)(a_j) \\ &= F(\eta_i, \mathrm{id}_j) \circ F(\psi_j, \mathrm{id}_j)(b_j) \\ &= F(\eta_i \circ \psi_j, \mathrm{id}_j)(b_j) \\ &= F(\psi, \mathrm{id}_j)(b_j) \end{aligned}$$

holds in $F(m, j)$. Consider the functor

$$\begin{array}{ccc} \mathsf{I} & & \mathsf{Set} \\ i_1 & & \varinjlim_{j \in \mathsf{J}} F(i_1, j) \\ {\scriptstyle\lambda}\downarrow & \overset{F_{-,\infty}}{\rightsquigarrow} & \downarrow{\scriptstyle F_{-,\infty}(\lambda)} \\ i_2 & & \varinjlim_{j \in \mathsf{J}} F(i_2, j) \end{array}$$

Then there exist morphisms $\varphi : i \to m$ and $\psi : i' \to m$ in I such that

$$F_{-,\infty}(\varphi)\left((a_j)_{j \in \mathrm{Ob}(\mathsf{J})}\right) = \varinjlim_{j \in \mathsf{J}} F(\varphi, \mathrm{id}_j)(a_j) = \varinjlim_{j \in \mathsf{J}} F(\psi, \mathrm{id}_j)(b_j) = F_{-,\infty}(\psi)\left((b_j)_{j \in \mathrm{Ob}(\mathsf{J})}\right),$$

which implies $a = b$. So the map h is injective.

To Specify an element a in the filtered colimit $\varinjlim_{i \in \mathsf{I}} \varprojlim_{j \in \mathsf{J}} F(i, j)$, it is sufficient to specify a map $\{*\} \to \varprojlim_{j \in \mathsf{J}} F(i, j)$ or alternatively a cone

$$v := \left(\{*\} \xrightarrow{v_j} F(i, j)\right)_{j \in \mathrm{Ob}(\mathsf{J})} \in \mathrm{Ob}\left(\mathsf{Cone}\left(\mathsf{Set}, \varprojlim_{j \in \mathsf{J}} F(i, -)\right)\right).$$

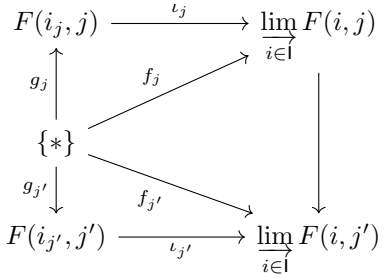
Let w be another cone over $\varprojlim_{j \in \mathsf{J}} F(i', -)$ correponding to $b \in \varinjlim_{i \in \mathsf{I}} \varprojlim_{j \in \mathsf{J}} F(i, j)$. Suppose $h(a) = h(b)$. Then there exists a morphism $\lambda : i \to i'$ in I such that the following diagram commutes

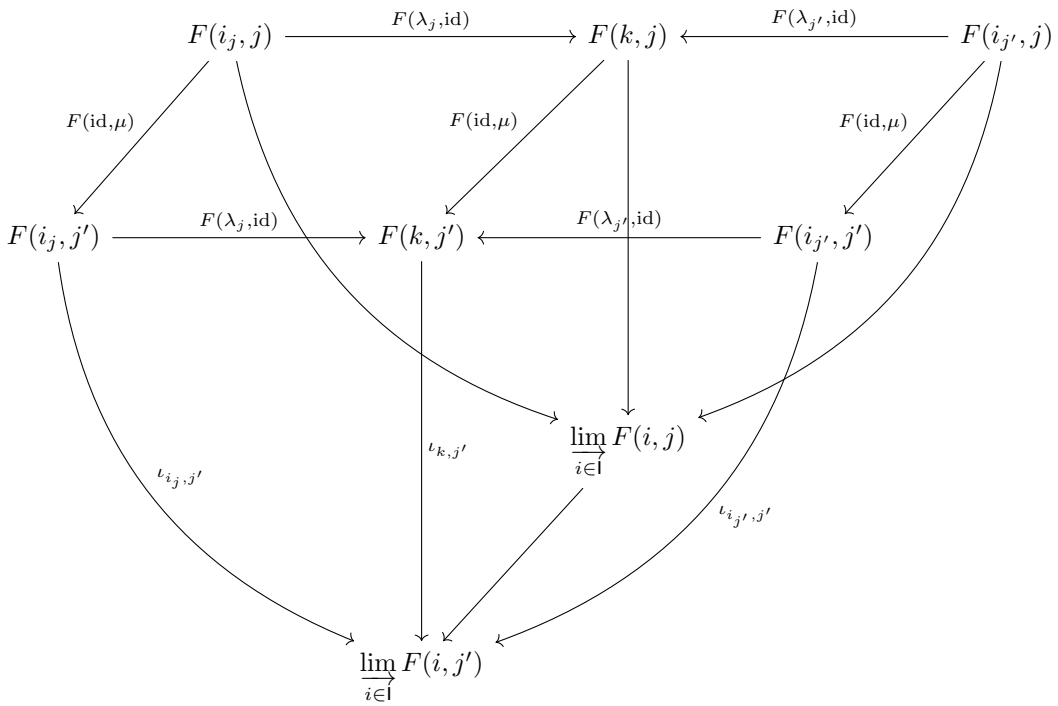
Giving an element $x \in \varprojlim_{j \in \mathsf{J}} \varinjlim_{i \in \mathsf{I}} F(i, j)$ is equivalent to giving a map $c_x : \{*\} \to \varprojlim_{j \in \mathsf{J}} \varinjlim_{i \in \mathsf{I}} F(i, j)$. By Proposition 2.4.6, this is equivalent to specifying a cone over $\varinjlim_{i \in \mathsf{I}} F(i, -)$

$$\left(\{*\} \xrightarrow{f_j} \varinjlim_{i \in \mathsf{I}} F(i, j)\right)_{j \in \mathrm{Ob}(\mathsf{J})} \in \mathrm{Ob}\left(\mathsf{Cone}\left(\mathsf{Set}, \varinjlim_{i \in \mathsf{I}} F(i, -)\right)\right).$$

By the construction filtered colimits in Set, for each $j \in \mathrm{Ob}(\mathsf{J})$, there exists a $i_j \in \mathrm{Ob}(\mathsf{I})$ and a morphism $g_j : \{*\} \to F(i_j, j)$ such that $f_j = \iota_{i_j, j} \circ g_j$, where $\iota_{i_j, j} : F(i_j, j) \to \varinjlim_{i \in \mathsf{I}} F(i, j)$ are the morphisms in the cocone of colimit. Since I is filtered and J is finite, there exists $k \in \mathrm{Ob}(\mathsf{I})$ with morphisms $\lambda_j : i_j \to k$ for each $j \in \mathrm{Ob}(\mathsf{J})$.

Given any morphism $\mu : j \to j'$ in J, the following two diagrams commutes





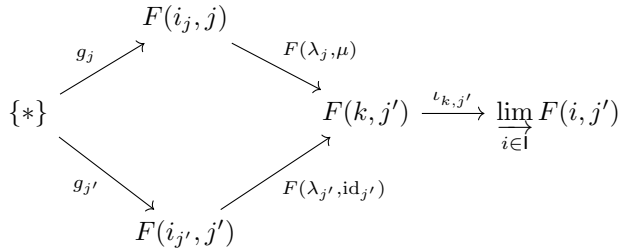
Combining these two commutative diagrams, we obtain

$$\iota_{k,j'} \circ F(\lambda_j, \mathrm{id}_{j'}) \circ F(\mathrm{id}_{i_j}, \mu) \circ g_j = \iota_{k,j'} \circ F(\lambda_{j'}, \mathrm{id}_{j'}) \circ g_{j'},$$

or equivalently

$$\iota_{k,j'} \circ F(\lambda_j, \mu) \circ g_j = \iota_{k,j'} \circ F(\lambda_{j'}, \mathrm{id}_{j'}) \circ g_{j'},$$

which is illustrated in the following diagram



By the property of filtered colimits in Set, there exists an object $k_\mu \in \mathrm{Ob}(\mathsf{I})$ and morphisms $\alpha_\mu : k \to k_\mu$ and $\beta_\mu : k \to k_\mu$ such that

$$F(\alpha_\mu, \mathrm{id}_{j'}) \circ F(\lambda_j, \mu) \circ g_j = F(\beta_\mu, \mathrm{id}_{j'}) \circ F(\lambda_{j'}, \mathrm{id}_{j'}) \circ g_{j'},$$

namely

$$F(\alpha_\mu \circ \lambda_j, \mu) \circ g_j = F(\beta_\mu \circ \lambda_{j'}, \mathrm{id}_{j'}) \circ g_{j'}.$$

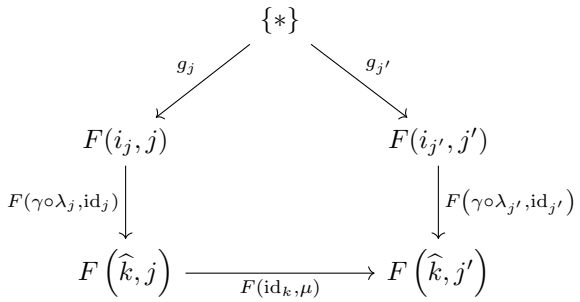
Consider the subcategory K of I consisting of k, $(k_\mu)_{\mu \in \mathrm{Mor}(\mathsf{I})}$ and morphisms α_μ, β_μ for each $\mu \in \mathrm{Mor}(\mathsf{I})$. By Proposition 2.4.6, since the inclusion functor $G : \mathsf{K} \hookrightarrow \mathsf{I}$ is a finite diagram, there exists a cocone from G to $\widehat{k} \in \mathrm{Ob}(\mathsf{I})$

$$\left(\begin{array}{ccc} & \widehat{k} & \\ {\scriptstyle \gamma}\nearrow & & \nwarrow{\scriptstyle \xi_\mu} \\ k & \overset{\alpha_\mu}{\underset{\beta_\mu}{\rightrightarrows}} & k_\mu \end{array} \right)_{\mu \in \mathrm{Mor}(\mathsf{I})} \in \mathrm{Ob}\left(\mathsf{Cocone}\left(G, \mathsf{I}\right)\right).$$

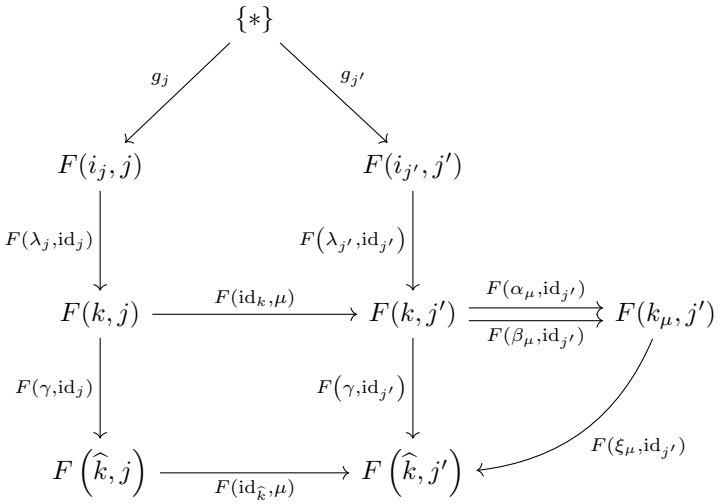
Then we can define a cone over $F\left(\widehat{k}, -\right)$ as follows

$$\left(r_j : \{*\} \xrightarrow{g_j} F(i_j, j) \xrightarrow{F(\gamma \circ \lambda_j, j)} F\left(\widehat{k}, j\right)\right)_{j \in \mathrm{Ob}(\mathsf{J})} \in \mathrm{Ob}\left(\mathsf{Cone}\left(\mathsf{Set}, F\left(\widehat{k}, -\right)\right)\right).$$

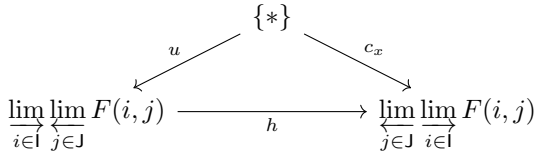
To verify it is a cone, we need to check for any morphism $\mu : j \to j'$ in J, the following diagram commutes



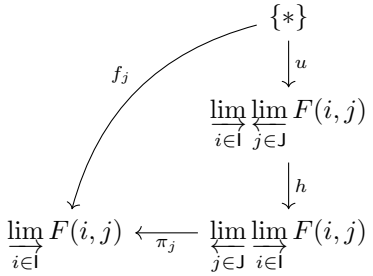
This can be derived from the following diagram



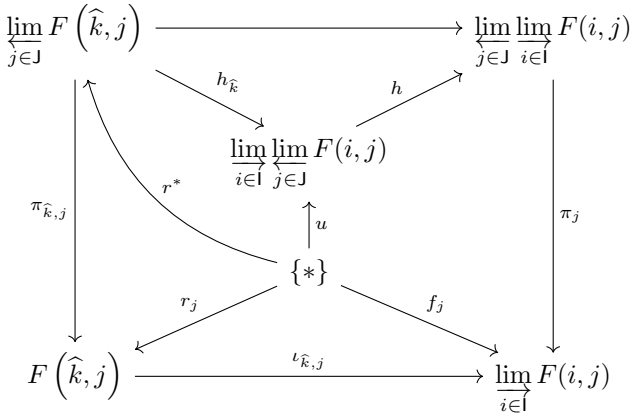
By the universal property of $\varprojlim_{j \in \mathsf{J}} F\left(\widehat{k}, j\right)$, there exists a unique morphism $r^* : \{*\} \to \varprojlim_{j \in \mathsf{J}} F\left(\widehat{k}, j\right)$. Compose r^* with the canonical morphism $\varprojlim_{j \in \mathsf{J}} F\left(\widehat{k}, j\right) \to \varinjlim_{i \in \mathsf{I}} \varprojlim_{j \in \mathsf{J}} F(i, j)$, we obtain a morphism $v : \{*\} \to \varprojlim_{j \in \mathsf{J}} \varinjlim_{i \in \mathsf{I}} F(i, j)$. To prove h is surjective, it is sufficient to verify that the following diagram commutes



We need to check that for any $j \in \mathrm{Ob}(\mathsf{J})$, the following diagram commutes



This follows from the commutativity of the outer square and all inter loops but the right one in the following diagram



By the universal property of $\varprojlim_{j\in\mathsf{J}}\varinjlim_{i\in\mathsf{I}} F(i,j)$, c_x is the uniqueness morphism such that $\pi_j \circ c_x = f_j$ for any $j \in \mathrm{Ob}(\mathsf{J})$. So we have $c_x = h \circ u$.

(ii) Let I be a discrete category and J be a connected category. Let $F : \mathsf{I} \times \mathsf{J} \to \mathsf{Set}$ be a functor.

First we prove the canonical map

$$\begin{aligned} h : \coprod_{i\in\mathsf{I}} \varprojlim_{j\in\mathsf{J}} F(i,j) &\longrightarrow \varprojlim_{j\in\mathsf{J}} \coprod_{i\in\mathsf{I}} F(i,j) \\ \left(i, (a_j)_{j\in\mathrm{Ob}(\mathsf{J})}\right) &\longmapsto \left((i,a_j)\right)_{j\in\mathrm{Ob}(\mathsf{J})} \end{aligned}$$

is injective. Let $a = \left(i, (a_j)_{j\in\mathrm{Ob}(\mathsf{J})}\right)$ with $a_j \in F(i,j)$ and $b = \left(i', (b_j)_{j\in\mathrm{Ob}(\mathsf{J})}\right)$ with $b_j \in F(i',j)$. If $h(a) = h(b)$, then for each $j \in \mathrm{Ob}(\mathsf{J})$, we have $(i, a_j) = (i', b_j)$ in $\coprod_{i\in\mathsf{I}} F(i,j)$, which implies $i = i'$ and $a_j = b_j$. So the map h is injective.

Next we prove h is surjective. Let $x = \left((i_j, a_j)\right)_{j\in\mathrm{Ob}(\mathsf{J})}$ be an element in $\varprojlim_{j\in\mathsf{J}} \coprod_{i\in\mathsf{I}} F(i,j)$, where $a_j \in F(i_j, j)$. Define the map

$$\begin{aligned} \coprod_{i\in\mathsf{I}} F(i,\mu) : \coprod_{i\in\mathsf{I}} F(i,j) &\longrightarrow \coprod_{i\in\mathsf{I}} F(i,j') \\ (i,a) &\longmapsto (i, F(i,\mu)(a)) . \end{aligned}$$

For any morphism $\mu : j \to j'$ in J, compatibility requires

$$(i_{j'}, a_{j'}) = \coprod_{i\in\mathsf{I}} F(i,\mu)\,(i_j, a_j) = (i_j, F(i_j,\mu)(a_j))$$

which forces

$$i_{j'} = i_j \text{ and } a_{j'} = F(i_j,\mu)(a_j).$$

Since J is connected, we can assume $i_j = i^*$ for all $j \in \mathrm{Ob}(\mathsf{J})$. And we get $(a_j)_{j\in\mathrm{Ob}(\mathsf{J})} \in \varprojlim_{j\in\mathsf{J}} F(i^*, j)$ by checking the compatibility condition

$$a_{j'} = F(i^*,\mu)(a_j), \text{ for any morphism } \mu : j \to j'.$$

Thus we have

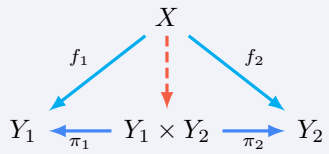
$$h\left(i^*, (a_j)_{j\in\mathrm{Ob}(\mathsf{J})}\right) = \left((i_j, a_j)\right)_{j\in\mathrm{Ob}(\mathsf{J})} = x.$$

This proves the surjectivity of h and hence h is a bijection.

□

2.4.1 Product and Coproduct

Definition 2.4.44 Binary Product



In the diagram $Y_1 \xleftarrow{f_1} X \xrightarrow{f_2} Y_2$, the information in X is coarsened through f_1 and reinterpreted in Y_1, while the same information in X is processed in another coarsening manner through f_2 and reinterpreted differently in Y_2.

$Y_1 \xleftarrow{\pi_1} Y_1 \times Y_2 \xrightarrow{\pi_2} Y_2$ is the most refined way to combine the information in Y_1 and Y_2 such that $Y_1 \times Y_2$ exactly captures the mixture of information in Y_1 and Y_2 and the projections π_1 and π_2 can coarsen the information in $Y_1 \times Y_2$ exactly to recover the information in Y_1 and Y_2 respectively.

Example 2.4.8 Binary Product in Set

Let Y_1 and Y_2 be sets. The binary product $Y_1 \times Y_2$ can be constructed as follows

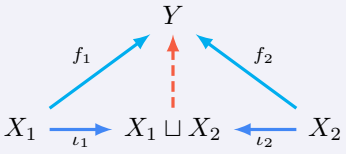
$$\begin{aligned} Y_1 \times Y_2 &= \{(y_1, y_2) \,|\, y_1 \in Y_1 \text{ and } y_2 \in Y_2\}. \\ \pi_1 &: (y_1, y_2) \longmapsto y_1, \\ \pi_2 &: (y_1, y_2) \longmapsto y_2. \end{aligned}$$

Given any $Y_1 \xleftarrow{f_1} X \xrightarrow{f_2} Y_2$, there exists a unique map

$$\begin{aligned} f_1 \times f_2 : X &\longrightarrow Y_1 \times Y_2 \\ x &\longmapsto (f_1(x), f_2(x)) \end{aligned}$$

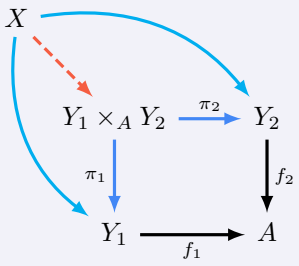
such that $\pi_1 \circ (f_1 \times f_2) = f_1$ and $\pi_2 \circ (f_1 \times f_2) = f_2$.

Definition 2.4.45 Binary Coproduct



2.4.2 Fibered Product and Fibered Coproduct

Definition 2.4.46 Fibered Product / Pullback



Example 2.4.9 Pullback in Set

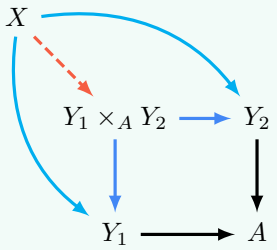
Let Y_1, Y_2, and A be sets and $f_1 : Y_1 \to A$, $f_2 : Y_2 \to A$ be maps. The fibered product $Y_1 \times_A Y_2$ can be constructed as follows

$$Y_1 \times_A Y_2 = \{(y_1, y_2) \,|\, y_1 \in Y_1 \text{ and } y_2 \in Y_2 \text{ such that } f_1(y_1) = f_2(y_2)\}.$$

Given any $X \xrightarrow{f} Y_1 \xleftarrow{g} Y_2$, there exists a unique map

$$\begin{aligned} X &\longrightarrow Y_1 \times_A Y_2 \\ x &\longmapsto (f(x), g(x)) \end{aligned}$$

such that the following diagram commutes



Proposition 2.4.47 Diagonal Base Change for Fibered Products

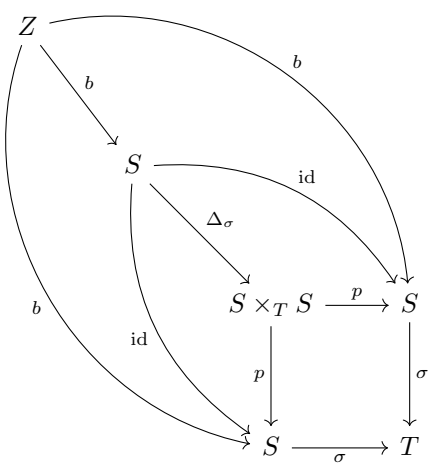
Let C be a category which admits fibered products. Let $\sigma : S \to T$, $f : X \to S$, and $g : Y \to S$ be morphisms in C. Then there is an isomorphism

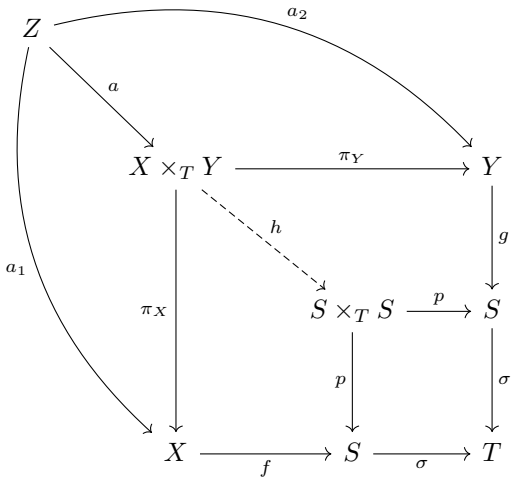
$$X \times_S Y \cong (X \times_T Y) \times_{(S \times_T S)} S.$$

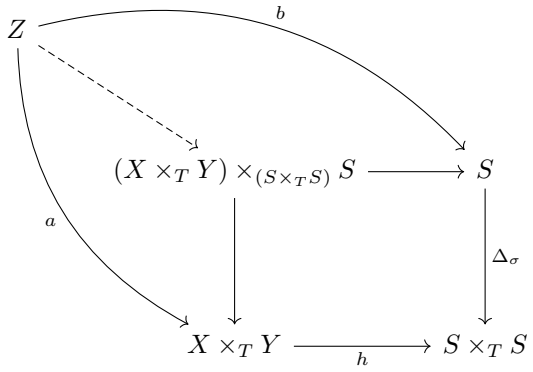
Dually, let C be a category which admits fibered coproducts. Let $\sigma : T \to S$, $f : S \to X$, and $g : S \to Y$ be morphisms in C. Then there is an isomorphism

$$X \sqcup_S Y \cong (X \sqcup_T Y) \sqcup_{(S \sqcup_T S)} S.$$

Proof.







We have the following isomorphisms natural in Z:

$$
\begin{aligned}
&\operatorname{Hom}(Z, (X \times_T Y) \times_{S \times_T S} S) \\
\cong\ &\operatorname{Hom}(Z, X \times_T Y) \times_{\operatorname{Hom}(Z, S \times_T S)} \operatorname{Hom}(Z, S) \\
\cong\ &\{(a, b) \,|\, a \in \operatorname{Hom}(Z, X \times_T Y),\ b \in \operatorname{Hom}(Z, S),\ h \circ a = \Delta_\sigma \circ b\} \\
\cong\ &\left\{(a, b) \,\middle|\, a \in \operatorname{Hom}(Z, X) \times_{\operatorname{Hom}(Z,T)} \operatorname{Hom}(Z, Y),\ b \in \operatorname{Hom}(Z, S),\ h \circ a = \Delta_\sigma \circ b\right\} \\
\cong\ &\{(a_1, a_2, b) \,|\, a_1 \in \operatorname{Hom}(Z, X),\ a_2 \in \operatorname{Hom}(Z, Y),\ b \in \operatorname{Hom}(Z, S),\ \sigma \circ f \circ a_1 = \sigma \circ g \circ a_2,\ f \circ a_1 = g \circ a_2 = b\} \\
\cong\ &\{(a_1, a_2) \,|\, a \in \operatorname{Hom}(Z, X),\ b \in \operatorname{Hom}(Z, Y),\ f \circ a_1 = g \circ a_2\} \\
\cong\ &\operatorname{Hom}(Z, X) \times_{\operatorname{Hom}(Z, S)} \operatorname{Hom}(Z, Y) \\
\cong\ &\operatorname{Hom}(Z, X \times_S Y)
\end{aligned}
$$

where the forth isomorphism follows from the natural isomorphism

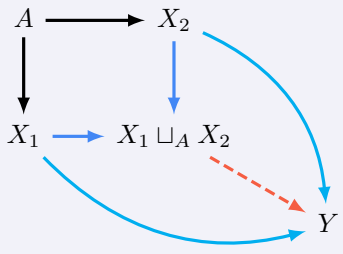
$$
\begin{aligned}
\operatorname{Hom}(Z, S \times_T S) &\xrightarrow{\sim} \operatorname{Hom}(Z, S) \times_{\operatorname{Hom}(Z,T)} \operatorname{Hom}(Z, S) \\
\phi &\longmapsto (p \circ \phi, p \circ \phi)\,.
\end{aligned}
$$

By Yoneda lemma, we have the desired isomorphism

$$X \times_S Y \cong (X \times_T Y) \times_{(S \times_T S)} S.$$

□

Definition 2.4.48 Fibered Coproduct / Pushout

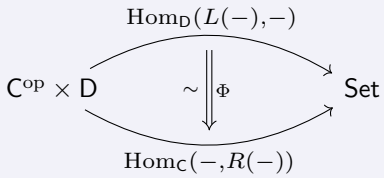


2.5 Adjoint Functor

Definition 2.5.1 Adjoint Pair of Functors

An **adjoint pair of functors** is a tuple (L, R, Φ) consisting of a pair of functors $\mathsf{C} \underset{R}{\overset{L}{\rightleftarrows}} \mathsf{D}$ and a natural

isomorphism



which means for any $X \in \mathrm{Ob}(\mathsf{C})$ and $Y \in \mathrm{Ob}(\mathsf{D})$, there is a bijection

$$\begin{aligned} \Phi_{X,Y} : \mathrm{Hom}_{\mathsf{D}}\left(L(X), Y\right) &\xrightarrow{\sim} \mathrm{Hom}_{\mathsf{C}}\left(X, R(Y)\right) \\ \left(L(X) \xrightarrow{f} Y\right) &\longmapsto \left(X \xrightarrow{f^{\triangleright}} R(Y)\right) \end{aligned}$$

natural in X and Y. L is called the **left adjoint** of R, and R is called the **right adjoint** of L. We write $L \dashv R$ to denote that L is left adjoint to R.

The naturality square of Φ means that for any morphism $g : X_2 \to X_1$ in C and $h : Y_1 \to Y_2$ in D, the following diagram commutes

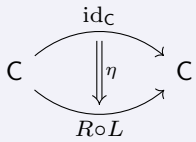
$$\begin{array}{ccc} \mathrm{Hom}_{\mathsf{D}}\left(L(X_1), Y_1\right) & \xrightarrow{\mathrm{Hom}_{\mathsf{D}}(L(g),h)} & \mathrm{Hom}_{\mathsf{D}}\left(L(X_2), Y_2\right) \\ \Phi_{X_1,Y_1} \downarrow \sim & & \sim \downarrow \Phi_{X_2,Y_2} \\ \mathrm{Hom}_{\mathsf{C}}\left(X_1, R(Y_1)\right) & \xrightarrow[\mathrm{Hom}_{\mathsf{C}}(g,R(h))]{} & \mathrm{Hom}_{\mathsf{C}}\left(X_2, R(Y_2)\right) \end{array}$$

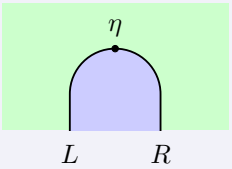
which in turn can be explicitly written as for any $f : L(X_1) \to Y_1$ in D,

$$\Phi_{X_2,Y_2}\left(h \circ f \circ L(g)\right) = R(h) \circ \Phi_{X_1,Y_1}(f) \circ g.$$

Definition 2.5.2 Adjunction Unit and Counit

Let (L, R, Φ) be an adjoint pair of functors. The **adjunction unit** η of this adjunction is a natural transformation

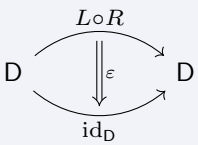


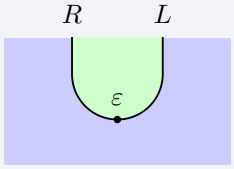


defined by $\eta_X := \Phi_{X,L(X)}\left(\mathrm{id}_{L(X)}\right)$ for any $X \in \mathrm{Ob}(\mathsf{C})$, where $\Phi_{X,L(X)}$ is the natural bijection

$$\begin{aligned} \Phi_{X,L(X)} : \mathrm{Hom}_{\mathsf{D}}\left(L(X), L(X)\right) &\xrightarrow{\sim} \mathrm{Hom}_{\mathsf{C}}(X, RL(X)) \\ \mathrm{id}_{F(X)} &\longmapsto \eta_X \end{aligned}$$

The **adjunction counit** ε of this adjunction is a natural transformation





defined by $\varepsilon_Y := \Phi^{-1}_{R(Y),Y}\left(\mathrm{id}_{R(Y)}\right)$ for any $Y \in \mathrm{Ob}(\mathsf{D})$, where $\Phi^{-1}_{R(Y),Y}$ is the natural bijection

$$\begin{aligned} \Phi^{-1}_{R(Y),Y} : \mathrm{Hom}_{\mathsf{D}}\left(R(Y), R(Y)\right) &\xrightarrow{\sim} \mathrm{Hom}_{\mathsf{C}}(LR(Y), R(Y)) \\ \mathrm{id}_{R(Y)} &\longmapsto \varepsilon_Y \end{aligned}$$

Proof. By naturality of Φ, for any morphism $g : X_2 \to X_1$ in C, we have the following commutative diagram

$$\begin{array}{ccccccc}
\mathrm{id}_{L(X_1)} & \ni & \mathrm{Hom}_{\mathsf{D}}\left(L(X_1), L(X_1)\right) & \xrightarrow{(L(g))^*} & \mathrm{Hom}_{\mathsf{D}}\left(L(X_2), L(X_1)\right) & \xleftarrow{(L(g))_*} & \mathrm{Hom}_{\mathsf{D}}\left(L(X_2), L(X_2)\right) \ni \mathrm{id}_{L(X_2)} \\
\downarrow & & \downarrow{\scriptstyle \Phi_{X_1, L(X_1)}} & & \downarrow{\scriptstyle \Phi_{X_2, L(X_1)}} & & \downarrow{\scriptstyle \Phi_{X_2, L(X_2)}} \quad \downarrow \\
\eta_{X_1} & \ni & \mathrm{Hom}_{\mathsf{C}}(X_1, RL(X_1)) & \xrightarrow{g^*} & \mathrm{Hom}_{\mathsf{C}}(X_2, RL(X_1)) & \xleftarrow{(RL(g))_*} & \mathrm{Hom}_{\mathsf{C}}(X_2, RL(X_2)) \ni \eta_{X_2}
\end{array}$$

Since

$$(L(g))^*\left(\mathrm{id}_{L(X_1)}\right) = L(g) = (L(g))_*\left(\mathrm{id}_{L(X_2)}\right),$$

we have

$$g^*(\eta_{X_1}) = \Phi_{X_2, L(X_1)}(L(g)) = (RL(g))_*(\eta_{X_2}),$$

which implies the naturality square of η commutes

$$\begin{array}{ccc}
X_2 & \xrightarrow{g} & X_1 \\
\downarrow{\scriptstyle \eta_{X_2}} & & \downarrow{\scriptstyle \eta_{X_1}} \\
RL(X_2) & \xrightarrow[RL(g)]{} & RL(X_1)
\end{array}$$

Similarly, we can show that for any morphism $h : Y_1 \to Y_2$ in D, the naturality square of ε commutes

$$\begin{array}{ccc}
LR(Y_1) & \xrightarrow{LR(h)} & LR(Y_2) \\
\downarrow{\scriptstyle \varepsilon_{Y_1}} & & \downarrow{\scriptstyle \varepsilon_{Y_2}} \\
Y_1 & \xrightarrow[h]{} & Y_2
\end{array}$$

□

Proposition 2.5.3 Adjunction Isomorphism Determined by Unit or Counit

Let (L, R, Φ) be an adjoint pair of functors and η and ε be the adjunction unit and counit respectively. Then

$$\begin{aligned}
&\Phi_{X,Y}(f) = R(f) \circ \eta_X : X \to R(Y), \quad \forall f : L(X) \to Y, \\
&\Phi^{-1}_{X,Y}(g) = \varepsilon_Y \circ L(g) : L(X) \to Y, \quad \forall g : X \to R(Y).
\end{aligned}$$

Proof. For any object $X \in \mathrm{Ob}(\mathsf{C})$ and any morphism $f : L(X) \to Y$ in D, we have the following commutative diagram

$$\begin{array}{ccccccc}
\mathrm{id}_{L(X)} & \in & \mathrm{Hom}_{\mathsf{C}}(L(X), L(X)) & \xrightarrow{f_*} & \mathrm{Hom}_{\mathsf{C}}(L(X), Y) & \ni & f \\
\downarrow & & \downarrow{\scriptstyle \Phi_{X, L(X)}} & & \downarrow{\scriptstyle \Phi_{X,Y}} & & \downarrow \\
\eta_X & \in & \mathrm{Hom}_{\mathsf{C}}(X, RL(X)) & \xrightarrow[(R(f))_*]{} & \mathrm{Hom}_{\mathsf{C}}(X, R(Y)) & \ni & \Phi_{X,Y}(f)
\end{array}$$

For any object $Y \in \mathrm{Ob}(\mathsf{D})$ and any morphism $g : X \to R(Y)$ in C, we have the following commutative diagram

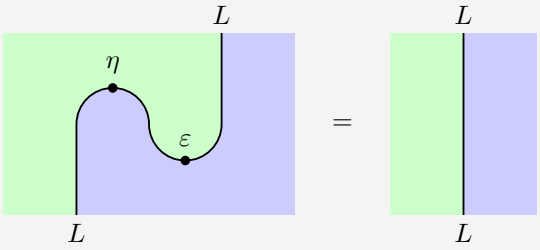
$$\begin{array}{ccccccc}
\mathrm{id}_{R(Y)} & \in & \mathrm{Hom}_{\mathsf{D}}(R(Y), R(Y)) & \xrightarrow{g^*} & \mathrm{Hom}_{\mathsf{D}}(X, R(Y)) & \ni & g \\
\downarrow & & \downarrow{\scriptstyle \Phi^{-1}_{R(Y),Y}} & & \downarrow{\scriptstyle \Phi^{-1}_{R(Y),Y}} & & \downarrow \\
\varepsilon_Y & \in & \mathrm{Hom}_{\mathsf{C}}(LR(Y), Y) & \xrightarrow[(L(g))^*]{} & \mathrm{Hom}_{\mathsf{C}}(L(X), Y) & \ni & \Phi^{-1}_{X,Y}(g)
\end{array}$$

□

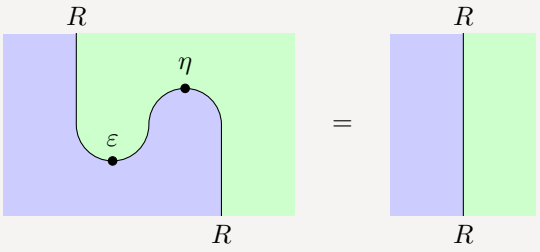
Lemma 2.5.4 Snake Equations

Let (L, R, Φ) be an adjoint pair of functors and η and ε be the adjunction unit and counit respectively. Then we have the following equalities of natural transformations

$$\left[L \xRightarrow{L\eta} LRL \xRightarrow{\varepsilon L} L\right] = \mathrm{id}_L$$



$$\left[R \xRightarrow{\eta R} RLR \xRightarrow{R\varepsilon} R\right] = \mathrm{id}_R$$



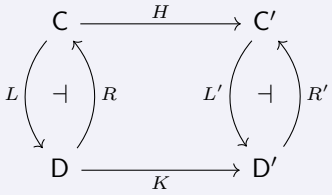
Proposition 2.5.5

If $F : \mathsf{C} \to \mathsf{D}$ and $G : \mathsf{D} \to \mathsf{C}$ are inverse functors, which means $F \circ G = \mathrm{id}_{\mathsf{D}}$ and $G \circ F = \mathrm{id}_{\mathsf{C}}$, then we have $F \dashv G$ and $G \dashv F$.

Proof. The snake equations of the adjunction unit and counit holds trivially because the unit $\eta : \mathrm{id}_{\mathsf{C}} \Rightarrow G \circ F$ and counit $\varepsilon : F \circ G \Rightarrow \mathrm{id}_{\mathsf{D}}$ are identity natural transformations. □

Definition 2.5.6 Wire Bending

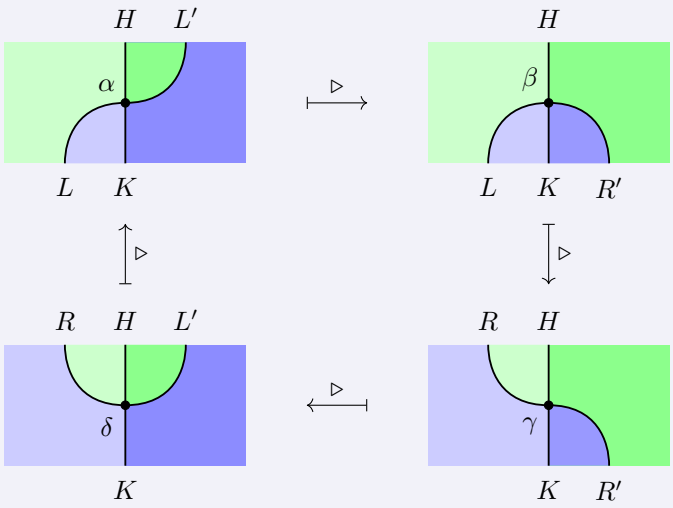
Let C, D, C', D' be categories and L, R, L', R', H, K be functors shown in the following diagram



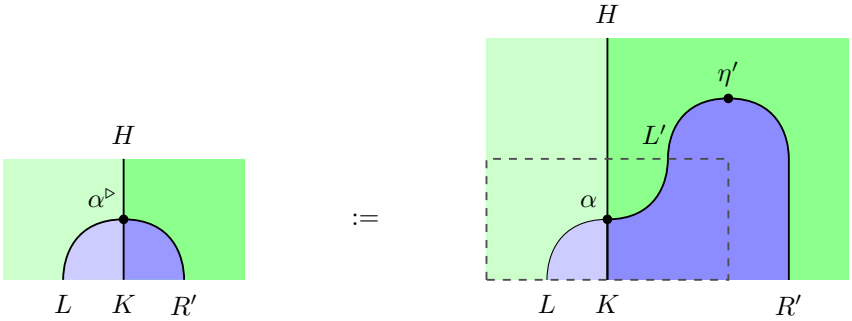
There are bijections between the following sets of natural transformations

$$\begin{array}{ccc} \mathrm{Hom}_{[\mathsf{C},\mathsf{D}']}(L'H, KL) & \underset{\triangleleft}{\overset{\triangleright}{\rightleftharpoons}} & \mathrm{Hom}_{[\mathsf{C},\mathsf{C}']}(H, R'KL) \\ \triangleright \Big\| \triangleleft & & \triangleleft \Big\| \triangleright \\ \mathrm{Hom}_{[\mathsf{D},\mathsf{D}']}(L'HR, K) & \underset{\triangleright}{\overset{\triangleleft}{\rightleftharpoons}} & \mathrm{Hom}_{[\mathsf{D},\mathsf{C}']}(HR, R'K) \end{array}$$

natural in both H and K such that $\triangleleft = \triangleright^{-1}$ and $\triangleright\triangleright\triangleright\triangleright = \triangleright^4 = \mathrm{id}$. $\triangleright$ is called **wire bending** because its action can be visualized as bending the wires of adjoint pairs in the following string diagrams



We only explicit define $\alpha^{\triangleright}$ here. The other wire bendings are defined similarly using the unit or counit of the adjunctions.



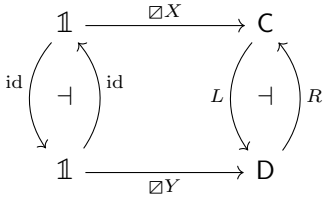
The fact that $\triangleleft$ is the inverse of $\triangleright$ follows from the snake equations.

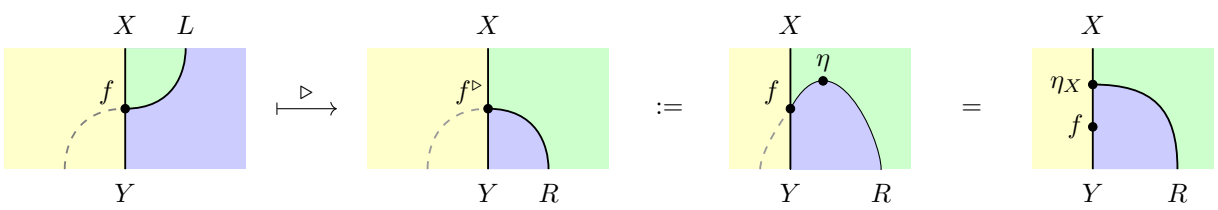
Proposition 2.5.7 Equivalent Definition of Adjoint Functor Using Unit and Counit

Given pair of functors $\mathsf{C} \underset{R}{\overset{L}{\rightleftarrows}} \mathsf{D}$ there is a bijection between the following sets

$$T : \{\text{adjoint pair } (L, R, \Phi)\} \xrightleftharpoons{\sim} \{(L, R, \eta, \varepsilon) \text{ that satisfies snake equations}\}$$
$$\Phi \longmapsto \left(\eta_X := \Phi\left(\mathrm{id}_{L(X)}\right), \varepsilon_Y := \Phi^{-1}\left(\mathrm{id}_{R(Y)}\right)\right)$$
$$\Phi_{X,Y}(f) := R(f) \circ \eta_X \longmapsfrom (\eta, \varepsilon)$$

Proof. Suppose $(L, R, \eta, \varepsilon)$ satisfies snake equations. Consider the diagram





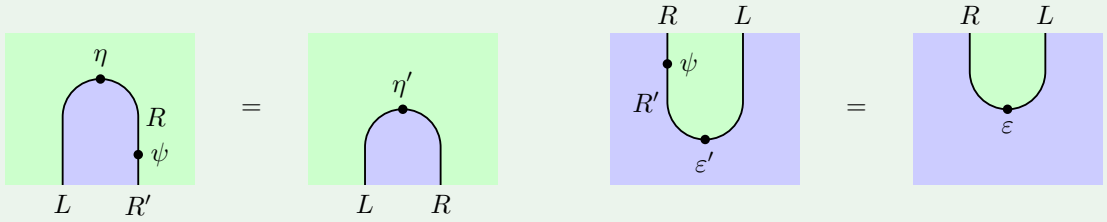
As the string diagram shows, we find $\Phi_{X,Y}$ conincides with the wire bending map

$$\triangleright : \mathrm{Hom}_{\mathsf{D}}\left(L(X), Y\right) \xrightarrow{\sim} \mathrm{Hom}_{\mathsf{C}}(X, R(Y))$$

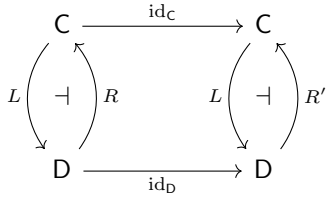
which is natural in both X and Y. Hence Φ is a natural isomorphism. It is straightforward to check that T is a bijection. □

Proposition 2.5.8 Uniqueness of Adjunction

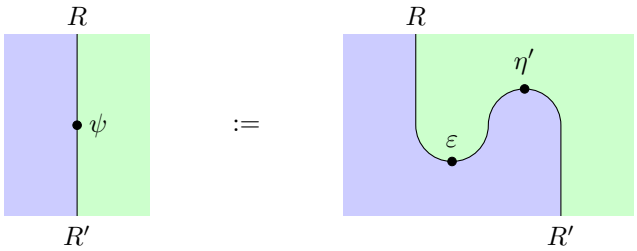
If $(L, R, \eta, \varepsilon)$ and $(L, R', \eta', \varepsilon)$ are two adjoint pairs of functors, then there is a unique natural isomorphism $\psi : R \xRightarrow{\sim} R'$ such that



Proof. Consider the diagram



Define $\psi := \mathrm{id}_L^{\triangleright\triangleright}$, which is illustrated by the following string diagram



ψ is a natural isomorphism since it has inverse $\mathrm{id}_L^{\triangleleft\triangleleft}$. The first equality in the statement of the proposition follows from $\psi^{\triangleleft} = \psi^{\triangleright\triangleright\triangleright} = \mathrm{id}_L^{\triangleright} = \eta'$. The uniqueness of ψ follows from the injectivity of

$$\triangleleft : \mathrm{Hom}_{[\mathsf{D},\mathsf{C}]}\left(R, R'\right) \xrightarrow{\sim} \mathrm{Hom}_{[\mathsf{C},\mathsf{C}]}\left(\mathrm{id}_{\mathsf{C}}, R'L\right).$$

Similarly, the second equality follows from $\psi^{\triangleright} = \psi^{\triangleleft\triangleleft\triangleleft} = \mathrm{id}_L^{\triangleleft} = \varepsilon$. And the uniqueness of ψ follows from the injectivity of

$$\triangleright : \mathrm{Hom}_{[\mathsf{C},\mathsf{D}]}\left(L', L\right) \xrightarrow{\sim} \mathrm{Hom}_{[\mathsf{D},\mathsf{D}]}\left(LR, \mathrm{id}_{\mathsf{D}}\right).$$

□

Proposition 2.5.9 Equivalent Definition of Adjoint Functor Using Representable Functor

(i) A functor $L : \mathsf{C} \to \mathsf{D}$ has right adjoint if and only for each $Y \in \mathrm{Ob}(\mathsf{D})$, $\mathrm{Hom}_{\mathsf{D}}\left(L(-), Y\right)$ is representable. If so, the universal element of $\mathrm{Hom}_{\mathsf{D}}\left(L(-), Y\right)$ is $(R(Y), \varepsilon_Y)$.

(ii) A functor $R : \mathsf{D} \to \mathsf{C}$ has left adjoint if and only for each $X \in \mathrm{Ob}(\mathsf{C})$, $\mathrm{Hom}_{\mathsf{C}}\left(X, R(-)\right)$ is representable. If so, the universal element of $\mathrm{Hom}_{\mathsf{C}}\left(X, R(-)\right)$ is $(L(X), \eta_X)$.

Proof. We only prove (i) here. The proof of (ii) is similar. If (L, R, Φ) is an adjoint pair of functors, then for each $Y \in \mathrm{Ob}(\mathsf{D})$, we have an isomorphism

$$\Phi_{\text{-},Y} : \mathrm{Hom}_{\mathsf{D}}\left(L(-), Y\right) \xRightarrow{\sim} \mathrm{Hom}_{\mathsf{D}}\left(-, R(Y)\right).$$

where $\Phi_{\text{-},Y}$ is the horizontal composition

$$\mathsf{C}^{\mathrm{op}} \times \mathbb{1} \xrightarrow{\mathrm{id}\times \boxtimes Y} \mathsf{C}^{\mathrm{op}} \times \mathsf{D} \underset{\mathrm{Hom}_{\mathsf{C}}(-,R(-))}{\overset{\mathrm{Hom}_{\mathsf{D}}(L(-),-)}{\Downarrow \Phi}} \mathsf{Set}$$

Since

$$\left(\Phi^{-1}_{-,Y}\right)_{R(Y)}\left(\mathrm{id}_{R(Y)}\right) = \Phi^{-1}_{R(Y),Y}\left(\mathrm{id}_{R(Y)}\right) = \varepsilon_Y,$$

we see $\mathrm{Hom}_{\mathsf{D}}\left(L(-), Y\right)$ is representable by $(R(Y), \varepsilon_Y)$.

Conversely, suppose for each $Y \in \mathrm{Ob}(\mathsf{D})$, $\mathrm{Hom}_{\mathsf{D}}\left(L(-), Y\right)$ is representable. Then for each $Y \in \mathrm{Ob}(\mathsf{D})$, there exist a natural isomorphism

$$\phi(Y) : \mathrm{Hom}_{\mathsf{D}}\left(-, R_Y\right) \xRightarrow{\sim} \mathrm{Hom}_{\mathsf{D}}\left(L(-), Y\right)$$

for some $R_Y \in \mathrm{Ob}(\mathsf{D})$. Proposition 2.3.6 implies that $(R_Y, \phi(Y))$ is terminal in the category $(Y_{\mathsf{C}} \downarrow \mathrm{Hom}_{\mathsf{D}}\left(L(-), Y\right))$, which corresponds to

$$\mathsf{C} \xrightarrow{Y_{\mathsf{C}}} [\mathsf{C}^{\mathrm{op}}, \mathsf{Set}] \xleftarrow{\boxtimes \mathrm{Hom}_{\mathsf{D}}(L(-),Y)} \mathbb{1}$$

Given any morphism $h : Y_1 \to Y_2$ in D, since $(R_{Y_2}, \phi(Y_2))$ is terminal in $(Y_{\mathsf{C}} \downarrow \mathrm{Hom}_{\mathsf{D}}\left(L(-), Y\right))$, there exists a unique morphism $R_h : R_{Y_1} \to R_{Y_2}$ in C such that the following diagram commutes

$$\begin{array}{ccc} Y_{\mathsf{C}}\left(R_{Y_1}\right) & \xrightarrow{\phi(Y_1)} & \mathrm{Hom}_{\mathsf{D}}\left(L(-), Y_1\right) \\ {\scriptstyle Y_{\mathsf{C}}(R_h)}\downarrow & & \downarrow{\scriptstyle h_\star} \\ Y_{\mathsf{C}}\left(R_{Y_2}\right) & \xrightarrow[\phi(Y_2)]{} & \mathrm{Hom}_{\mathsf{D}}\left(L(-), Y_2\right) \end{array} = \begin{array}{ccc} \mathrm{Hom}_{\mathsf{C}}\left(-, R_{Y_1}\right) & \xrightarrow{\phi(Y_1)} & \mathrm{Hom}_{\mathsf{D}}\left(L(-), Y_1\right) \\ {\scriptstyle (R_h)_\star}\downarrow & & \downarrow{\scriptstyle h_\star} \\ \mathrm{Hom}_{\mathsf{C}}\left(-, R_{Y_2}\right) & \xrightarrow[\phi(Y_2)]{} & \mathrm{Hom}_{\mathsf{D}}\left(L(-), Y_2\right) \end{array}$$

Thus we can define a functor $R : \mathsf{D} \to \mathsf{C}$ by $R(Y) := R_Y$ and $R(h) := R_h$. We can also define a natural isomorphism $\Phi : \mathrm{Hom}_{\mathsf{D}}\left(L(-), -\right) \xRightarrow{\sim} \mathrm{Hom}_{\mathsf{D}}\left(-, R(-)\right)$ by

$$\begin{aligned} \Phi_{X,Y} : \mathrm{Hom}_{\mathsf{D}}\left(L(X), Y\right) &\xrightarrow{\sim} \mathrm{Hom}_{\mathsf{C}}\left(X, R(Y)\right) \\ \left(L(X) \xrightarrow{f} Y\right) &\longmapsto \left(X \xrightarrow{(\phi(Y)_X)^{-1}(f)} R(Y)\right) \end{aligned}$$

The naturality of Φ can be check as follows: for any morphism $g : X_2 \to X_1$ in C and $h : Y_1 \to Y_2$ in D, the following diagram commutes

$$\begin{array}{ccccc} \mathrm{Hom}_{\mathsf{D}}\left(L(X_1), Y_1\right) & \xrightarrow{L(g)^*} & \mathrm{Hom}_{\mathsf{D}}\left(L(X_2), Y_1\right) & \xrightarrow{h_*} & \mathrm{Hom}_{\mathsf{D}}\left(L(X_2), Y_2\right) \\ {\scriptstyle \Phi_{X_1,Y_1}}\downarrow{\scriptstyle \left(\phi(Y_1)_{X_1}\right)^{-1}} & & {\scriptstyle \Phi_{X_2,Y_1}}\downarrow{\scriptstyle \left(\phi(Y_1)_{X_2}\right)^{-1}} & & {\scriptstyle \Phi_{X_2,Y_2}}\downarrow{\scriptstyle \left(\phi(Y_2)_{X_2}\right)^{-1}} \\ \mathrm{Hom}_{\mathsf{C}}\left(X_1, R(Y_1)\right) & \xrightarrow[g^*]{} & \mathrm{Hom}_{\mathsf{C}}\left(X_2, R(Y_1)\right) & \xrightarrow[R(h)_*]{} & \mathrm{Hom}_{\mathsf{C}}\left(X_2, R(Y_2)\right) \end{array}$$

Therefore, (L, R, Φ) is an adjoint pair of functors. □

Corollary 2.5.10 Equivalent Definition of Adjoint Functor Using Universal Morphism

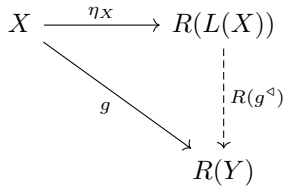
Given pair of functors $\mathsf{C} \underset{R}{\overset{L}{\rightleftarrows}} \mathsf{D}$, then the following are equivalent

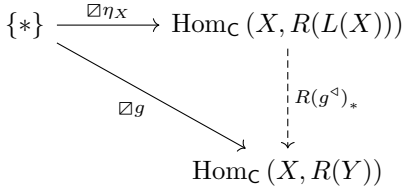
(i) $L \dashv R$.

(ii) For every object $X \in \mathrm{Ob}(\mathsf{C})$, there exists $\left(L(X), X \xrightarrow{\eta_X} R(L(X))\right)$ initial in $(X \downarrow R)$, i.e. there exists a universal morphism from X to R.

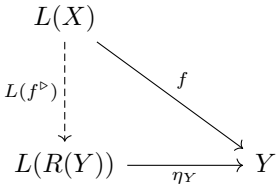
(iii) For every object $Y \in \mathrm{Ob}(\mathsf{D})$, there exists $\left(R(Y), L(R(Y)) \xrightarrow{\varepsilon_Y} Y\right)$ terminal in $(L \downarrow Y)$, i.e. there exists a universal morphism from L to Y.

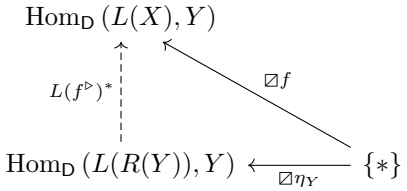
Proof. This is a direct consequence of Proposition 2.5.9. According to Proposition 2.3.9, for each $X \in \mathrm{Ob}(\mathsf{C})$, $\mathrm{Hom}_{\mathsf{C}}(X, R(-))$ is representable by $(L(X), \eta_X)$ is equivalent to that $\left(L(X), X \xrightarrow{\eta_X} R(L(X))\right)$ is initial in $(X \downarrow R)$.





Similarly, for each $Y \in \mathrm{Ob}(\mathsf{D})$, $\mathrm{Hom}_{\mathsf{D}}(L(-), Y)$ is representable by $(R(Y), \varepsilon_Y)$ is equivalent to that $(R(Y), \varepsilon_Y)$ is terminal in $(L \downarrow Y)$.





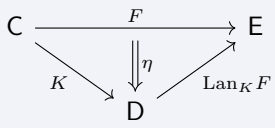
□

2.6 Kan Extension

Definition 2.6.1 Kan Extension

Let C, D, E be categories and $K : \mathsf{C} \to \mathsf{D}$, $F : \mathsf{C} \to \mathsf{E}$ be functors. A **left Kan extension** of F along K is a pair $(\mathrm{Lan}_K F, \eta)$ consisting of

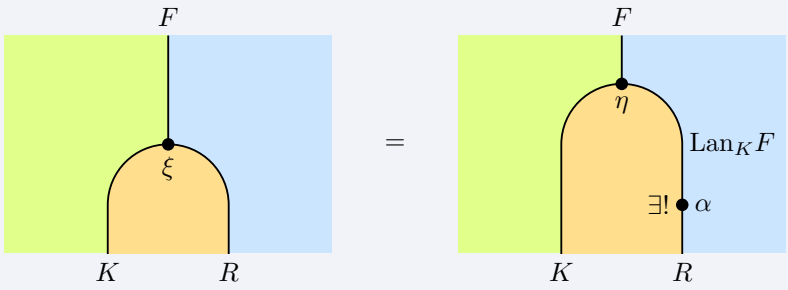
- a functor $\mathrm{Lan}_K F : \mathsf{D} \to \mathsf{E}$,
- a natural transformation $\eta : F \Rightarrow (\mathrm{Lan}_K F) \circ K$



such that for any pair (R, ξ) consisting of

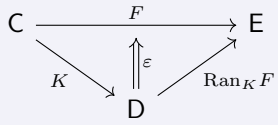
- a functor $R : \mathsf{D} \to \mathsf{E}$,
- a natural transformation $\xi : F \Rightarrow R \circ K$,

there exists a unique natural transformation $\alpha : \mathrm{Lan}_K F \Rightarrow R$ such that



A **right Kan extension** of K along F is a pair $(\mathrm{Ran}_K F, \varepsilon)$ consisting of

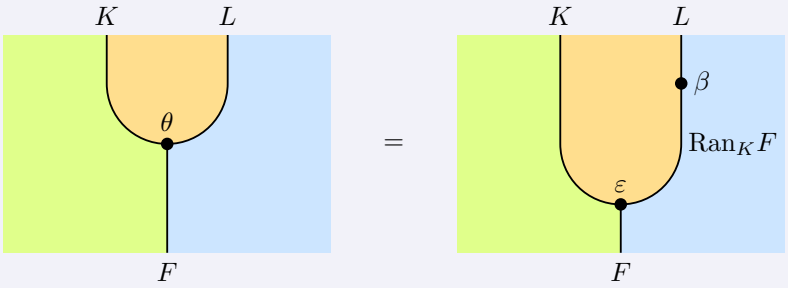
- a functor $\mathrm{Ran}_K F : \mathsf{D} \to \mathsf{E}$,
- a natural transformation $\varepsilon : (\mathrm{Ran}_K F) \circ K \Rightarrow F$



such that for any pair (L, θ) consisting of

- a functor $L : \mathsf{D} \to \mathsf{E}$,
- a natural transformation $\theta : L \circ K \Rightarrow F$,

there exists a unique natural transformation $\beta : L \Rightarrow \mathrm{Ran}_K F$ such that



2.7 Monoidal Category

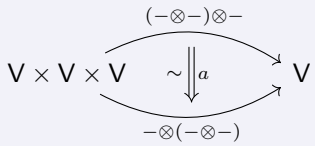
Definition 2.7.1 Monoidal Category

A monoidal category is a category V equipped with

(i) Tensor product: a functor $\otimes : \mathsf{V} \times \mathsf{V} \to \mathsf{V}$.

$$\begin{array}{ccc} \mathsf{V} \times \mathsf{V} & & \mathsf{V} \\ (X_1, Y_1) & \overset{\otimes}{\rightsquigarrow} & X_1 \otimes Y_1 \\ {\scriptstyle f \times g}\downarrow & & \downarrow{\scriptstyle f \otimes g} \\ (X_2, Y_2) & & X_2 \otimes Y_2 \end{array}$$

(ii) Associator: a natural isomorphism a

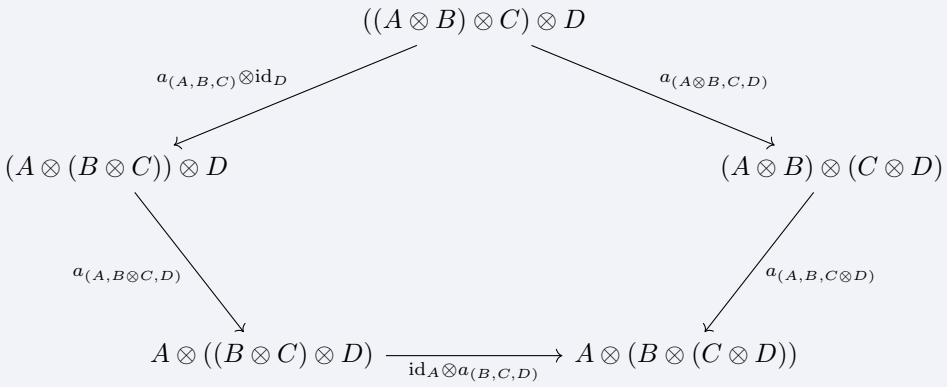


(iii) Unit object: an object $1 \in \mathrm{Ob}(\mathsf{V})$

(iv) An isomorphism in V: $\iota : 1 \otimes 1 \to 1$

such that the following two conditions holds

(i) The pentagon axiom: the following diagram commutes



(ii) Unit axiom: the functors $1 \otimes - : \mathsf{V} \to \mathsf{V}$ and $- \otimes 1 : \mathsf{V} \to \mathsf{V}$ are category equivalences.

A strict monoidal category is one for which the natural isomorphisms a, λ and ρ are identities. Every monoidal category is monoidally equivalent to a strict monoidal category.

Definition 2.7.2 Cartesian/Cocartesian Monoidal Category

- A **cartesian monoidal category** is a monoidal category with finite products endowed with a where the tensor product is the categorical product and the unit object is the terminal object. If a category has all finite products, then we say it is **cartesian monoidal**.
- A **cocartesian monoidal category** is a monoidal category where the tensor product is the categorical coproduct and the unit object is the initial object. If a category has all finite coproducts, then we say it is **cocartesian monoidal**.

Example 2.7.1 Category of Endofunctors is a Monoidal Category

Let C be a category. The **category of endofunctors** $[\mathsf{C}, \mathsf{C}]$ is a monoidal category with the following structure

(i) Tensor product: composition of functors.

(ii) Associator: the natural isomorphism a is the identity.

(iii) Unit object: the identity functor id_{C}.

(iv) Unit isomorphism: the natural isomorphism ι is the identity.

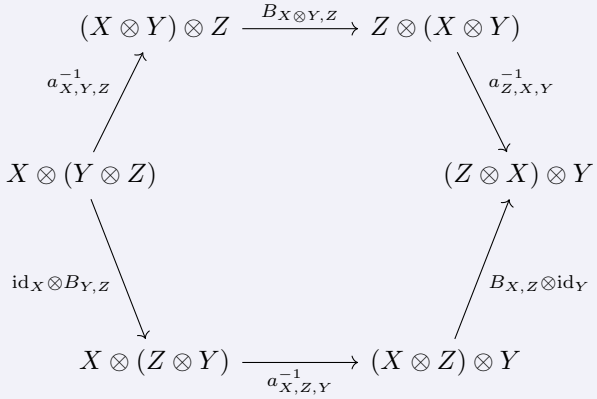
Definition 2.7.3 Braided Monoidal Category

A **braided monoidal category** is a monoidal category V equipped with an isomorphism natural in $X, Y \in \mathrm{Ob}(\mathsf{V})$

$$B_{X,Y} : X \otimes Y \to Y \otimes X$$

called the **braiding** such that the following two conditions hold:

(i) The hexagon axiom: the following diagram commutes



Definition 2.7.4 Symmetric Monoidal Category

A **symmetric monoidal category** is a braided monoidal category V satisfying the following condition:

$$B_{Y,X} \circ B_{X,Y} = \mathrm{id}_{X\otimes Y}.$$

2.8 Enriched Category

Definition 2.8.1 Enriched Category

Let V be a monoidal category. An **V-enriched category** C consists of

(i) Object set: a set of objects $\mathrm{Ob}(\mathsf{C})$.

(ii) Hom-object: for each pair of objects $A, B \in \mathrm{Ob}(\mathsf{C})$, an object $\mathrm{Hom}_{\mathsf{C}}(A, B) \in \mathrm{Ob}(\mathsf{V})$.

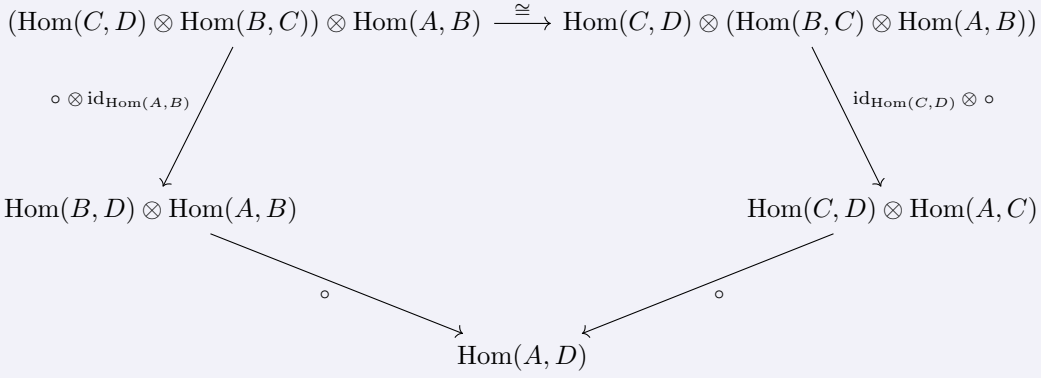
(iii) Composition: for each triple of objects $A, B, C \in \mathrm{Ob}(\mathsf{C})$, a morphism in V

$$\circ : \mathrm{Hom}_{\mathsf{C}}(B, C) \otimes \mathrm{Hom}_{\mathsf{C}}(A, B) \longrightarrow \mathrm{Hom}_{\mathsf{C}}(A, C)$$

(iv) Identity: for each object $A \in \mathrm{Ob}(\mathsf{C})$, a morphism $\mathcal{I}d_A : 1 \to \mathrm{Hom}_{\mathsf{C}}(A, A)$ in V.

such that the following conditions hold

(i) For each quadruple of objects $A, B, C, D \in \mathrm{Ob}(\mathsf{C})$, the following diagram in V commutes



(ii) For each pair of objects $A, B \in \mathrm{Ob}(\mathsf{C})$, the following diagrams in V commute

$$\begin{array}{ccc} 1 \otimes \mathrm{Hom}_{\mathsf{C}}(A,B) & \xrightarrow{\mathcal{I}d_B \otimes \mathrm{id}_{\mathrm{Hom}_{\mathsf{C}}(A,B)}} & \mathrm{Hom}_{\mathsf{C}}(B,B) \otimes \mathrm{Hom}_{\mathsf{C}}(A,B) \\ & \searrow^{\cong} \quad \swarrow_{\circ} & \\ & \mathrm{Hom}_{\mathsf{C}}(A,B) & \end{array}$$

$$\begin{array}{ccc} \mathrm{Hom}_{\mathsf{C}}(A,B) \otimes 1 & \xrightarrow{\mathrm{id}_{\mathrm{Hom}_{\mathsf{C}}(A,B)} \otimes \mathcal{I}d_A} & \mathrm{Hom}_{\mathsf{C}}(A,B) \otimes \mathrm{Hom}_{\mathsf{C}}(A,A) \\ & \searrow^{\cong} \quad \swarrow_{\circ} & \\ & \mathrm{Hom}_{\mathsf{C}}(A,B) & \end{array}$$

Definition 2.8.2 Enriched Functor

Let V be a monoidal category and C and D be V-enriched categories. An **V-enriched functor** $F : \mathsf{C} \to \mathsf{D}$ consists of

(i) Object map: a map $F^{\mathrm{Ob}} : \mathrm{Ob}(\mathsf{C}) \to \mathrm{Ob}(\mathsf{D})$,

(ii) Hom-object morphisms: for each pair of objects $A, B \in \mathrm{Ob}(\mathsf{C})$, a morphism $F^{\mathrm{Mor}}_{A,B} : \mathrm{Hom}_{\mathsf{C}}(A,B) \to \mathrm{Hom}_{\mathsf{D}}(F(A), F(B))$ in V, such that for any triple of objects $A, B, C \in \mathrm{Ob}(\mathsf{C})$, the following diagram in V commutes

$$\begin{array}{ccc} \mathrm{Hom}\,(Y,Z) \otimes \mathrm{Hom}\,(X,Y) & \xrightarrow{\circ} & \mathrm{Hom}\,(X,Z) \\ \downarrow{\scriptstyle F^{\mathrm{Mor}}_{Y,Z} \otimes F^{\mathrm{Mor}}_{X,Y}} & & \downarrow{\scriptstyle F^{\mathrm{Mor}}_{X,Z}} \\ \mathrm{Hom}\,(FY,FZ) \otimes \mathrm{Hom}\,(FX,FY) & \xrightarrow[\circ]{} & \mathrm{Hom}\,(FX,FZ) \end{array}$$

$$\begin{array}{ccc} \mathrm{Hom}(X,X) & \xrightarrow{F^{\mathrm{Mor}}_{X,X}} & \mathrm{Hom}(FX,FX) \\ & \nwarrow \quad \nearrow & \\ & 1 & \end{array}$$

2.9 2-Category

Definition 2.9.1 Strict 2-Category

Let Cat be the Cartesian monoidal category consisting of all small categories. A **strict 2-category** is a Cat-enriched category. We define the following sets

- 0-morphism set: $\mathrm{Ob}(\mathsf{C})$
- 1-morphism set: $\mathrm{Hom}_{\mathsf{C}}(X,Y)$ for any $X, Y \in \mathrm{Ob}(\mathsf{C})$
- 2-morphism set: $\mathrm{Hom}_{\mathsf{C}}(f,g)$ for any $X, Y \in \mathrm{Ob}(\mathsf{C})$ and $f, g \in \mathrm{Hom}_{\mathsf{C}}(X,Y)$

For any $X, Y, Z \in \mathrm{Ob}(\mathsf{C})$, we have the following composition bifunctor

$$\begin{array}{ccc} \mathrm{Hom}_{\mathsf{C}}(Y,Z) \times \mathrm{Hom}_{\mathsf{C}}(X,Y) & & \mathrm{Hom}_{\mathsf{C}}(X,Z) \\ (f',f) & & f' \circ f \\ {\scriptstyle (\theta',\theta)}\Downarrow & \rightsquigarrow^{\Theta} & \Downarrow{\scriptstyle \theta' \circ \theta} \\ (g',g) & & g' \circ g \end{array}$$

which are called the horizontal composition of 2-morphisms. The functoriality of Θ means that given any vertical composition of 2-morphisms

$$\begin{array}{c} (f', f) \\ {\scriptstyle (\theta', \theta)}\Downarrow \\ (g', g) \\ {\scriptstyle (\psi', \psi)}\Downarrow \\ (h', h) \end{array}$$

we have the following equality

$$\Theta\left(\left(\psi' \circ \theta'\right), (\psi \circ \theta)\right) = (\psi' \circ \theta') \circ (\psi \circ \theta) = \Theta\left(\psi', \psi\right) \circ \Theta\left(\theta', \theta\right) = (\psi' \circ \psi) \circ (\theta' \circ \theta)$$

which is called the **interchange law**.

Example 2.9.1 Cat as 2-category

The category Cat is a strict 2-category with the following structure

- 0-morphism set: $\mathrm{Ob}(\mathsf{Cat})$
- 1-morphism set: $\mathrm{Hom}_{\mathsf{Cat}}(\mathsf{C}, \mathsf{D}) := [\mathsf{C}, \mathsf{D}]$ for any $\mathsf{C}, \mathsf{D} \in \mathrm{Ob}(\mathsf{Cat})$
- 2-morphism set: $\mathrm{Hom}_{\mathsf{Cat}}(F, G) := \mathrm{Hom}_{[\mathsf{C},\mathsf{D}]}(F, G)$ for any $\mathsf{C}, \mathsf{D} \in \mathrm{Ob}(\mathsf{Cat})$ and $F, G \in [\mathsf{C}, \mathsf{D}]$

2.10 Internalization

Traditional Bourbaki-style mathematical structures are formulated within set theory, or put differently, within the ambient category Set. The concept of **Internalization** entails reformulating these mathematical structures in a broader ambient category C, which typically need some extra structures to express the correponding mathematics. The extra structure required on an ambient category C is referred to as a **doctrine** for internalization.

2.10.1 Monoid Object

Monoids can be internalized in the doctrine of monoidal categories.

Example 2.10.1 Monoid Objects in Monoidal Categories

Monoid objects internal to Cartesian monoidal categories

- Set: traditional monoid.
- Cat: (small) strict monoidal category.
- Top: topological monoid.
- Mon: commutative monoid.

Monoid objects internal to general monoidal categories

- $(R\text{-}\mathsf{Mod}, \otimes_R, R)$ for $R \in \mathrm{Ob}(\mathsf{CRing})$: associative R-algebra.
- $(\mathsf{Ab}, \otimes_{\mathbb{Z}}, \mathbb{Z})$: ring.
- $\left(\mathsf{Ch}\left(R\text{-}\mathsf{Mod}\right), \otimes_R, (R)_{n\in\mathbb{Z}}\right)$ for $R \in \mathrm{Ob}(\mathsf{CRing})$: differential graded R-algebra.
- $([\mathsf{C}, \mathsf{C}], \circ, \mathrm{id}_{\mathsf{C}})$ for $\mathsf{C} \in \mathrm{Ob}(\mathsf{Cat})$: monad on C.

Commutative monoids can be internalized in the doctrine of symmetric monoidal categories.

2.10.2 Internal Category

Definition 2.10.1 Internal Category

Let C be a category with pullbacks. A **category internal to** C consists of

(i) Object of 0-morphisms: an object $C_0 \in \mathrm{Ob}(\mathsf{C})$.

(ii) Object of 1-morphisms: an object $C_1 \in \mathrm{Ob}(\mathsf{C})$.

(iii) Source and target morphisms: two morphisms $s, t : C_1 \to C_0$.

(iv) Identity assignment: a morphism $e : C_0 \to C_1$.

(v) Composition: a morphism $c : C_1 \times_{C_0} C_1 \to C_1$.

such that the following diagrams commute

(i) Source and target of identity morphisms

$$\begin{array}{ccccc} & & C_0 & & \\ & \swarrow^{\mathrm{id}_{C_0}} & \downarrow{\scriptstyle e} & \searrow^{\mathrm{id}_{C_0}} & \\ C_0 & \xleftarrow[s]{} & C_1 & \xrightarrow[t]{} & C_0 \end{array}$$

(ii) Source and target of composition

$$\begin{array}{ccccc} C_1 & \xleftarrow{\pi_1} & C_1 \times_{C_0} C_1 & \xrightarrow{\pi_2} & C_1 \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle t} \\ C_0 & \xleftarrow[s]{} & C_1 & \xrightarrow[t]{} & C_0 \end{array}$$

(iii) Associativity of composition

(iv) Left and right unit laws

Definition 2.10.2 Double Category

A **double category** D is a category internal to Cat.

Chapter 3

Homological Algebra

3.1 Abelian Category

3.1.1 Ab-enriched Category

We will refer to Ab-enriched functors as **additive functors**. Some literature refers to Ab-categories as preadditive categories. We will not use this term in this note.

Definition 3.1.1 Biproduct

Let C be an Ab-category and X_1, X_2 be objects in C. A **biproduct** of X_1 and X_2 is a diagram

$$X_1 \underset{p_1}{\overset{i_1}{\rightleftarrows}} X_1 \oplus X_2 \underset{p_2}{\overset{i_2}{\leftrightarrows}} X_2$$

such that

- $p_1 \circ i_1 = \mathrm{id}_{X_1}$, $p_2 \circ i_2 = \mathrm{id}_{X_2}$.
- $i_1 \circ p_1 + i_2 \circ p_2 = \mathrm{id}_{X_1 \oplus X_2}$.

Empty biproduct is defined to be the zero object.

Proposition 3.1.2 Equivalent Conditions of Existance of Biproduct

Let C be an Ab-category and X_1, X_2 be objects in C. Then the following are equivalent

(i) Product $X_1 \times X_2$ exists.

(ii) Coproduct $X_1 \amalg X_2$ exists.

(iii) Biproduct $X_1 \oplus X_2$ exists.

Proposition 3.1.3 Equivalent Conditions of Existance of Zero Object

Let C be an Ab-category. Then the following are equivalent

(i) Initial object (empty product) exists.

(ii) Terminal object (empty coproduct) exists.

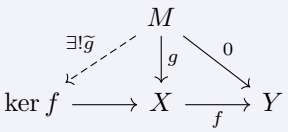
(iii) Zero object (empty biproduct) exists.

Proposition 3.1.4 Ab-enriched Functors Preserve Biproducts

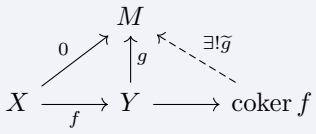
Ab-enriched functors preserve finite biproducts.

Definition 3.1.5 Kernel and Cokernel

Suppose C is a category with zero object and $f : X \to Y$ is a morphism in C. The **kernel** of f is the equalizer of f and the zero morphism, which is denoted by $\ker f$. The universal property of kernel is given by the following diagram



The **cokernel** of f is the coequalizer of f and the zero morphism, which is denoted by $\operatorname{coker} f$. The universal property of cokernel is given by the following diagram



3.1.2 Additive Category

Definition 3.1.6 Additive Category

An Ab-category is **additive** if it has all finite biproducts.

3.1.3 Abelian Category

Definition 3.1.7 Abelian Category

An additive category A is **abelian** if

(i) Every morphism has both a kernel and a cokernel.

(ii) Every monomorphism and every epimorphism is normal. This means that every monomorphism is a kernel of some morphism, and every epimorphism is a cokernel of some morphism.

Proposition 3.1.8

If A is an abelian category, then $[\mathsf{C}, \mathsf{A}]$ is abelian for any small category C.

Proposition 3.1.9 Exact Functors in Abelian Category

Let A and B be abelian categories and $F : \mathsf{A} \to \mathsf{B}$ be an additive functor. Then

(i) F is left exact if and only if F preserves kernels, or equivalently,

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \text{ is exact} \quad \Longrightarrow \quad 0 \longrightarrow F(X) \xrightarrow{F(f)} F(Y) \xrightarrow{F(g)} F(Z) \text{ is exact.}$$

(ii) F is right exact if and only if F preserves cokernels, or equivalently,

$$X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0 \text{ is exact} \quad \Longrightarrow \quad F(X) \xrightarrow{F(f)} F(Y) \xrightarrow{F(g)} F(Z) \longrightarrow 0 \text{ is exact.}$$

(iii) F is exact if and only if F preserves kernels and cokernels, or equivalently,

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0 \text{ is exact} \quad \Longrightarrow \quad 0 \longrightarrow F(X) \xrightarrow{F(f)} F(Y) \xrightarrow{F(g)} F(Z) \longrightarrow 0 \text{ is exact.}$$

Definition 3.1.10 Cohomology Functor

Let A be an abelian category and

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

be an exact sequence in A. The **cohomology functor** $\mathrm{H} : \mathsf{Ch}(\mathsf{A}) \to \mathsf{Ab}$ is defined by

$$\mathrm{H}(X \xrightarrow{f} Y \xrightarrow{g} Z) := \operatorname{coker}[\operatorname{im}(f) \to \ker(g)].$$

Proposition 3.1.11 Exact Functor Preserve Cohomology

Let $F : \mathsf{A} \to \mathsf{B}$ be an exact functor between abelian categories. Suppose

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

is an exact sequence in A. Then we have the following natural isomorphism

$$F\left(\mathrm{H}\left[X \xrightarrow{f} Y \xrightarrow{g} Z\right]\right) \cong \mathrm{H}\left[F(X) \xrightarrow{F(f)} F(Y) \xrightarrow{F(g)} F(Z)\right].$$

Proof.

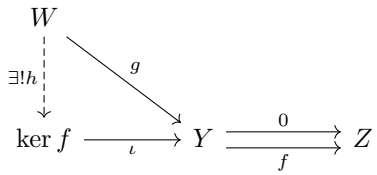
$$\begin{aligned} F\left(\mathrm{H}\left[X \xrightarrow{f} Y \xrightarrow{g} Z\right]\right) &= F \operatorname{coker}[\operatorname{im}(f) \to \ker(g)] \\ &\cong \operatorname{coker}[F \operatorname{im}(f) \to F \ker(g)] \\ &\cong \operatorname{coker}[\operatorname{im}(Ff) \to \ker(Fg)] \\ &= \mathrm{H}\left[FX \xrightarrow{Ff} FY \xrightarrow{Fg} Z\right] \end{aligned}$$

□

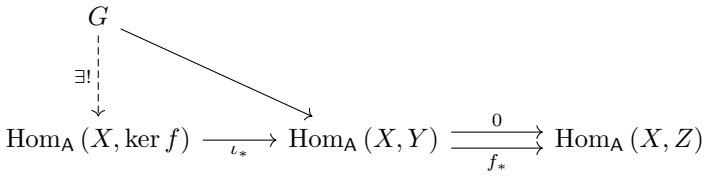
Proposition 3.1.12 Hom Functors are Left Exact

Let A be an abelian category. Then given any $X \in \mathrm{Ob}(\mathsf{A})$, $\mathrm{Hom}_{\mathsf{A}}(X, -) : \mathsf{A} \to \mathsf{Ab}$ and $\mathrm{Hom}_{\mathsf{A}}(-, X) : \mathsf{A}^{\mathrm{op}} \to \mathsf{Ab}$ are left exact functors.

Proof. To prove that $\mathrm{Hom}_{\mathsf{A}}(X, -)$ is left exact, we need to prove that it preserves kernels. Let $f : Y \to Z$ be a morphism in A, the universal property of $\ker f$ is illustrated by the following diagram



It suffices to show that $\iota_* : \mathrm{Hom}_{\mathsf{A}}(X, \ker f) \hookrightarrow \mathrm{Hom}_{\mathsf{A}}(X, Y)$ satisfies the universal property of $\ker f_*$.



This reduces to checking that $\ker f_* = \iota_*(\mathrm{Hom}_{\mathsf{A}}(X, \ker f))$.

If $\iota_*(h) \in \iota_*(\mathrm{Hom}_{\mathsf{A}}(X, \ker f))$, then $f_*(\iota_*(h)) = f \circ \iota \circ h = 0$, which means that $h \in \ker f_*$. Conversely, if $g \in \ker f_*$, then $f_*(g) = f \circ g = 0$. By the universal property of $\ker f$, there exists a unique morphism $h : W \to \ker f$ such that $\iota \circ h = g$. This means that $g = \iota_*(h) \in \iota_*(\mathrm{Hom}_{\mathsf{A}}(X, \ker f))$.

The proof for left-exactness of $\mathrm{Hom}_{\mathsf{A}}(-, X)$ can be obtained by duality. □

Definition 3.1.13 Split Exact Sequence

Let A be an abelian category and

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$$

be an exact sequence in A. The sequence is said to be **split** if there exists morphisms $r : Y \to X$ and $s : Z \to Y$ such that Y is the biproduct of X and Z, which is illustrated by the following diagram

$$X \underset{r}{\overset{f}{\rightleftarrows}} Y \underset{g}{\overset{s}{\rightleftarrows}} Z$$

Proposition 3.1.14 Equivalent Characterizations of Split Exact Sequence

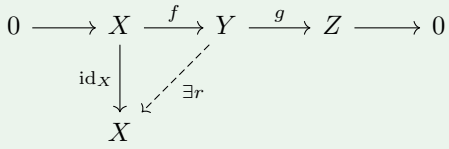
Let A be an abelian category and

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$$

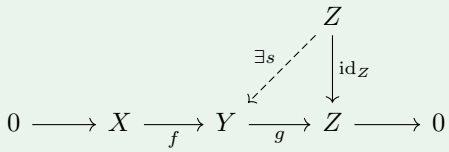
be an exact sequence in A. Then the following statements are equivalent

(i) The sequence is split.

(ii) f has left inverse, i.e. there exists a morphism $r : Y \to X$ such that $r \circ f = \mathrm{id}_X$.



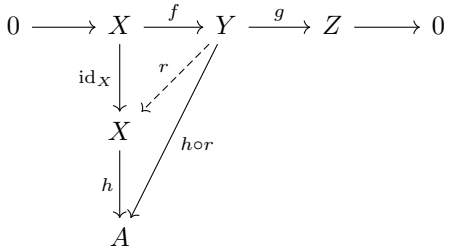
(iii) g has right inverse, i.e. there exists a morphism $s : Z \to Y$ such that $g \circ s = \mathrm{id}_Z$.



(iv) The homomorphism $f^* : \mathrm{Hom}_{\mathsf{A}}(Y, A) \to \mathrm{Hom}_{\mathsf{A}}(X, A)$ is surjective for any $A \in \mathrm{Ob}(\mathsf{A})$.

(v) The homomorphism $g_* : \mathrm{Hom}_{\mathsf{A}}(A, Y) \to \mathrm{Hom}_{\mathsf{A}}(A, Z)$ is surjective for any $A \in \mathrm{Ob}(\mathsf{A})$.

Proof. (ii) $\implies$ (iv). Suppose $r : Y \to X$ is a left inverse of f. Given any $h \in \mathrm{Hom}_{\mathsf{A}}(X, A)$, there exists $h \circ r \in \mathrm{Hom}_{\mathsf{A}}(Y, A)$ such that $f^*(h \circ r) = h \circ r \circ f = h$, which means that f^* is surjective.



(iv) $\implies$ (ii). Suppose f^* is surjective. Given any $h \in \mathrm{Hom}_{\mathsf{A}}(X, A)$, there exists $h' \in \mathrm{Hom}_{\mathsf{A}}(Y, A)$ such that $f^*(h') = h$. This means that $h' \circ f = h$. Let $r := h'$, then $r \circ f = h$. □

3.2 Complex

3.2.1 Complex in Additive Category

Cochain Complex

Definition 3.2.1 S-graded Object of a Category

Let C be a category and S be a set. The category of **S-graded object of C** is defined as the functor category $[\mathsf{Disc}(S), \mathsf{C}]$, denoted by $\mathsf{Gr}_S(\mathsf{C})$. The explicit description of the category is given as follows

- Object: a collection of objects $\{X_s\}_{s\in S}$ in C.
- Morphism: a collection of morphisms $\{f_s : X_s \to Y_s\}_{s\in S}$ in C.

Definition 3.2.2 Category with Translation

A **category with translation** is a category C equipped with an auto-equivalence functor

$$T : \mathsf{C} \longrightarrow \mathsf{C}$$

called the **shift functor** or **translation functor** or suspension functor.

Example 3.2.1 Shift Functors on $\mathbb{Z}$-graded Category

Let C be a category. Given $k \in \mathbb{Z}$, the **k-th shift functor** on $\mathsf{Gr}_{\mathbb{Z}}(\mathsf{C})$ is an endofunctor $[k]$ defined by

$$\begin{array}{ccc} \mathsf{Gr}_{\mathbb{Z}}(\mathsf{C}) & & \mathsf{Gr}_{\mathbb{Z}}(\mathsf{C}) \\ X = (X^i) & & X[k] = (X[k]^i) = (X^{k+i}) \\ {\scriptstyle f=(f^i)}\downarrow & \overset{[k]}{\rightsquigarrow} & \downarrow{\scriptstyle f[k]=(f^{k+i})} \\ Y = (Y^i) & & Y[k] = (Y[k]^i) = (Y^{k+i}) \end{array}$$

Example 3.2.2 Shift Functors on $\mathbb{Z}^m$-graded Category

Let C be a category. In a similar manner, given $k_1, \cdots, k_m \in \mathbb{Z}$, the **$(k_1, \cdots, k_m)$-th shift functor** on $\mathsf{Gr}_{\mathbb{Z}^m}(\mathsf{C})$ is an endofunctor $[k_1, \cdots, k_m]$ defined by

$$\begin{array}{ccc} \mathsf{Gr}_{\mathbb{Z}^m}(\mathsf{C}) & & \mathsf{Gr}_{\mathbb{Z}^m}(\mathsf{C}) \\ A = (A^{i_1,\cdots,i_m}) & & A[k_1,\cdots,k_m] = (A[k_1,\cdots,k_m]^{i_1,\cdots,i_m}) = (A^{i_1+k_1,\cdots,i_m+k_m}) \\ {\scriptstyle f=(f^{i_1,\cdots,i_m})}\downarrow & \overset{[k_1,\cdots,k_m]}{\rightsquigarrow} & \downarrow{\scriptstyle (f^{i_1+k_1,\cdots,i_m+k_m})} \\ B = (B^{i_1,\cdots,i_m}) & & B[k_1,\cdots,k_m] = (B[k_1,\cdots,k_m]^{i_1,\cdots,i_m}) = (B^{i_1+k_1,\cdots,i_m+k_m}) \end{array}$$

Lemma 3.2.3

If C is an additive category, then $\mathsf{Gr}_{\mathbb{Z}^m}(\mathsf{C}) = [\mathsf{Disc}(\mathbb{Z}^m), \mathsf{C}]$ is an additive category.

Definition 3.2.4 General Differential Object in a Category with Translation

A **general differential object** in a category C with translation T is a pair (X, d_X) consisting of an object X in C and a morphism $d_X : X \to T(X)$ in C.

Definition 3.2.5 Differential Object in an Additive Category with Translation

A **differential object** in an additive category C with translation T is a pair (X, d_X) consisting of an object X in C and a morphism $d_X : X \to T(X)$ in C such that $T(d_X) \circ d_X = 0$.

Definition 3.2.6 Differential $\mathbb{Z}$-Graded Object

Let A be an additive category. The category of **differential $\mathbb{Z}$-graded objects** of A consists of the following data

- Object: differential objects (X, d_X) in the additive category $\mathsf{Gr}_{\mathbb{Z}}(\mathsf{A})$ with translation $[1]$.
- Morphism: morphisms $f : (X, d_X) \to (Y, d_Y)$ are morphisms $f : X \to Y$ in $\mathsf{Gr}_{\mathbb{Z}}(\mathsf{A})$ such that $f[1] \circ d_X = d_Y \circ f$.

Definition 3.2.7 Cochain Complex

Let A be an additive category. The category of **cochain complexes** of A, denoted by $\mathsf{Ch}(\mathsf{A})$, consists of the following data

- Object: **cochain complex** of A, which consists of a collection of objects $X^\bullet = (X^n)_{n\in\mathbb{Z}}$ in A and a collection of morphisms $d_X^\bullet = \left(d^n : X^n \to X^{n+1}\right)_{n\in\mathbb{Z}}$ in A

$$\cdots \longrightarrow X^n \xrightarrow{d_X^n} X^{n+1} \xrightarrow{d_X^{n+1}} X^{n+2} \longrightarrow \cdots$$

  such that $d_X^{n+1} \circ d_X^n = 0$ for all $n \in \mathbb{Z}$.

- Morphism: a collection of morphisms $(f^n : X^n \to Y^n)_{n\in\mathbb{Z}}$ in A such that $f^{n+1} \circ d_X^n = d_Y^n \circ f^n$ for all $n \in \mathbb{Z}$

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & X^n & \xrightarrow{d_X^n} & X^{n+1} & \xrightarrow{d_X^{n+1}} & X^{n+2} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f^n} & & \downarrow{\scriptstyle f^{n+1}} & & \downarrow{\scriptstyle f^{n+2}} & & \\
\cdots & \longrightarrow & Y^n & \xrightarrow[d_Y^n]{} & Y^{n+1} & \xrightarrow[d_Y^{n+1}]{} & Y^{n+2} & \longrightarrow & \cdots
\end{array}$$

$\mathsf{Ch}(\mathsf{A})$ is isomorphic to the category of differential $\mathbb{Z}$-graded objects of A.

Chain Complex

Definition 3.2.8 Homotopy between Morphisms of Chain Complexes

A homotopy h between a pair of morphisms of chain complexes $f, g : X_\bullet \to Y_\bullet$ is a collection of morphisms $h_i : X_i \to Y_{i+1}$ such that we have

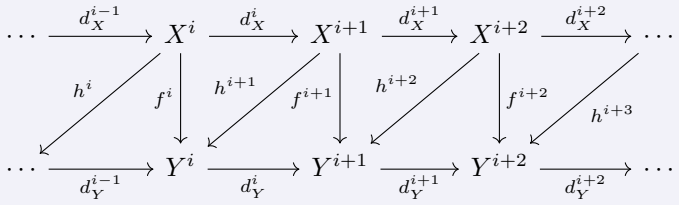
$$f_i - g_i = d_{i+1} \circ h_i + h_{i-1} \circ d_i$$

for all i. Two morphisms $f, g : X_\bullet \to Y_\bullet$ are said to be homotopic if a homotopy between f and g exists.

3.2.2 Chain Homotopy

Definition 3.2.9 Homotopy between Morphisms of Cochain Complexes

A **homotopy h between a pair of morphisms of cochain complexes** $f, g : X^\bullet \to Y^\bullet$ is a collection of morphisms $h^i : X^i \to Y^{i-1}$



such that

$$f^i - g^i = d_Y^{i-1} \circ h^i + h^{i+1} \circ d_X^i$$

for all $i \in \mathbb{Z}$. Two morphisms $f, g : X^\bullet \to Y^\bullet$ are said to be **homotopic** if there exists a homotopy between f and g. A morphism $f : X^\bullet \to Y^\bullet$ is said to be **null homotopic** if it is homotopic to the zero morphism $0 : X^\bullet \to Y^\bullet$.

Proposition 3.2.10 Additive Functor Preserves Cochain Homotopy

Let $F : \mathsf{A} \to \mathsf{B}$ be an additive functor between additive categories. Suppose h is a homotopy between a pair of morphisms $f, g : X^\bullet \to Y^\bullet$ in $\mathsf{Ch}(\mathsf{A})$. Then $(F(h^i))_{i\in\mathbb{Z}}$ is a homotopy between $F(f), F(g) : F(X^\bullet) \to F(Y^\bullet)$ in B.

Definition 3.2.11 Homotopy Equivalence between Cochain Complexes

A morphism $f : X^\bullet \to Y^\bullet$ of cochain complexes is a **homotopy equivalence** if there exists a morphism $g : Y^\bullet \to X^\bullet$ such that $f \circ g$ and $g \circ f$ are homotopic to the identity morphisms of $X^\bullet$ and $Y^\bullet$, respectively. We say that $X^\bullet$ and $Y^\bullet$ are **homotopy equivalent** if there exists a homotopy equivalence between $X^\bullet$ and $Y^\bullet$.

3.2.3 Cohomology

Definition 3.2.12 n-th Cohomology Functor

Let A be an abelian category. Given any $n \in \mathbb{Z}$, the **n-th cohomology functor** of a cochain complex $X^\bullet$ is defined to be the functor

$$\mathrm{H}^n(X^\bullet) := \ker d^n / \operatorname{im} d^{n-1}.$$

Definition 3.2.13 Quasi-isomorphism

A morphism $f : X^\bullet \to Y^\bullet$ of cochain complexes is a **quasi-isomorphism** if the induced morphism $\mathrm{H}^n(f) : \mathrm{H}^n(X^\bullet) \to \mathrm{H}^n(Y^\bullet)$ is an isomorphism for all $n \in \mathbb{Z}$.

Lemma 3.2.14

If $f : X^\bullet \to Y^\bullet$ is null homotopic, then $\mathrm{H}^n(f) = 0$ for all $n \in \mathbb{Z}$.

Proof. Let h be a homotopy between f and the zero morphism. Then we have

$$f^n = d_Y^{n-1} \circ h^n + h^{n+1} \circ d_X^n$$

for all $n \in \mathbb{Z}$. This implies that f^n induces the zero morphism on cohomology for all $n \in \mathbb{Z}$. □

Proposition 3.2.15 Homotopic Morphisms Induce the Same Morphisms on Cohomology

Let $f, g : X^\bullet \to Y^\bullet$ be homotopic morphisms of cochain complexes. Then the induced morphisms $\mathrm{H}^n(f)$ and $\mathrm{H}^n(g)$ on cohomology are the same for all $n \in \mathbb{Z}$.

Proof. Let h be a homotopy between f and g. Then we have

$$f^n - g^n = d_Y^{n-1} \circ h^n + h^{n+1} \circ d_X^n$$

for all $n \in \mathbb{Z}$. This implies that f^n and g^n induce the same morphism on cohomology for all $n \in \mathbb{Z}$. □

Corollary 3.2.16 Homotopy Equivalences are Quasi-Isomorphisms

A homotopy equivalence of cochain complexes is a quasi-isomorphism.

Definition 3.2.17 Acyclic Complex

A cochain complex $X^\bullet$ is **acyclic** if $\mathrm{H}^n(X^\bullet) = 0$ for all $n \in \mathbb{Z}$.

Proposition 3.2.18

Let A be an abelian category and $X^\bullet \in \mathrm{Ob}\,(\mathsf{Ch}(\mathsf{A}))$ be a cochain complex. Then the following are equivalent

(i) $X^\bullet$ is acyclic.

(ii) $X^\bullet$ is exact, that is, exact at each X^n.

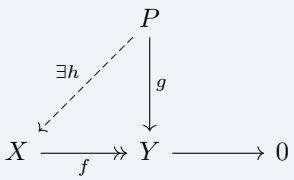
(iii) The zero morphism $0 \to X^\bullet$ is a quasi-isomorphism.

3.3 Resolution

3.3.1 Projective and Injective Objects

Definition 3.3.1 Projective Object

An object P in an abelian category A is **projective** if for any epimorphism $f : X \to Y$ and any morphism $g : P \to Y$, there exists a morphism $h : P \to X$ such that $f \circ h = g$.



Proposition 3.3.2 Equivalent Characterizations of Projective Objects

Let A be an abelian category and P be an object in A. Then the following are equivalent

(i) P is projective.

(ii) $\mathrm{Hom}_{\mathsf{A}}(P, -)$ is exact.

(iii) Every short exact sequence

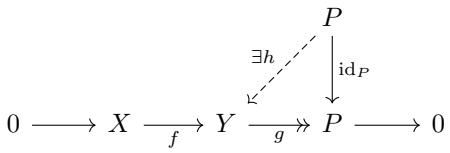
$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} P \longrightarrow 0$$

in A splits.

(iv) $\mathrm{Ext}_{\mathsf{A}}(P, X) = 0$ for all $X \in \mathsf{A}$.

Proof. (i) $\implies$ (ii). Since $\mathrm{Hom}_{\mathsf{A}}(P, -)$ is a left exact functor, it suffices to show that $\mathrm{Hom}_{\mathsf{A}}(P, -)$ preserves epimorphisms. Let $f : X \to Y$ be an epimorphism in A. We need to show that $f_* : \mathrm{Hom}_{\mathsf{A}}(P, X) \to \mathrm{Hom}_{\mathsf{A}}(P, Y)$ is surjective. Let $g : P \to Y$ be a morphism in A. Since P is projective, there exists a morphism $h : P \to X$ such that $f_*(h) = f \circ h = g$. This means that f_* is surjective.

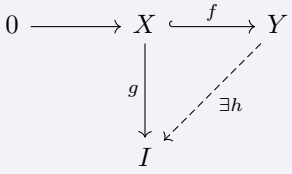
(i) $\implies$ (iii). If P is projective, then for any short exact sequence $0 \to X \xrightarrow{f} Y \xrightarrow{g} P \to 0$, there exists a morphism $h : P \to Y$ such that $h \circ g = \mathrm{id}_P$.



By Proposition 3.1.14, this implies that the short exact sequence splits. □

Definition 3.3.3 Injective Object

An object I in an abelian category A is **injective** if for any monomorphism $f : X \to Y$ and any morphism $g : X \to I$, there exists a morphism $h : Y \to I$ such that $h \circ f = g$.



Proposition 3.3.4 Equivalent Characterizations of Injective Objects

Let A be an abelian category and I be an object in A. Then the following are equivalent

(i) I is injective.

(ii) $\mathrm{Hom}_{\mathsf{A}}(-, I)$ is exact.

(iii) Every short exact sequence

$$0 \longrightarrow I \longrightarrow X \xrightarrow{f} Y \longrightarrow 0$$

in A splits.

(iv) $\mathrm{Ext}_{\mathsf{A}}(I, X) = 0$ for all $X \in \mathsf{A}$.

Chapter 4

Group

4.1 Basic Concepts

Definition 4.1.1 Group

A **group** is a set G together with a binary operation $\cdot : G \times G \to G$ such that

(i) (Associativity) $\forall x, y, z \in G$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

(ii) (Identity) $\exists e \in G$ such that $\forall x \in G$, $e \cdot x = x \cdot e = x$.

(iii) (Inverse) $\forall x \in G$, $\exists x^{-1} \in G$ such that $x \cdot x^{-1} = x^{-1} \cdot x = e$.

Since the identity of a group is unique, we denote it by 1_G or simply 1.

Definition 4.1.2 Opposite Group

Let $G = (G, *)$ be a group. The **opposite group** of G is the group $G^{\mathrm{op}} = (G, *^{\mathrm{op}})$, where $*^{\mathrm{op}} : G \times G \to G$ is defined by $x *^{\mathrm{op}} y = y \cdot x$. If we consider G as a category $\mathsf{B}G$, then we have category isomorphism

$$\mathsf{B}G^{\mathrm{op}} \cong (\mathsf{B}G)^{\mathrm{op}}.$$

Proposition 4.1.3 Group is Isomorphic to Its Opposite group

G is isomorphic to G^{op} through the isomorphism $x \mapsto x^{-1}$. This is same as saying that $\mathsf{B}G$ is isomorphic to $(\mathsf{B}G)^{\mathrm{op}}$ through the functor $^{\mathrm{op}}$ defined in Definition 2.1.8.

Definition 4.1.4 Subgroup

Let G be a group. A subset H of G is called a **subgroup** of G if H is a group with respect to the binary operation of G. In this case, we write $H \leq G$.

4.2 Group Homomorphism

Definition 4.2.1 Group Homomorphism

Let G, H be groups. A **group homomorphism** from G to H is a function $\varphi : G \to H$ such that

$$\forall x, y \in G, \quad \varphi(xy) = \varphi(x)\varphi(y).$$

Definition 4.2.2 Isomorphism

Let G, H be groups. A group homomorphism $\varphi : G \to H$ is called an **isomorphism** if φ is bijective. In

this case, we say that G and H are **isomorphic** and write $G \cong H$.

Proposition 4.2.3 Properties of Group Homomorphisms

Let G, H be groups and $\varphi : G \to H$ be a group homomorphism. Then

(i) $\varphi(1_G) = 1_H$.

(ii) $\forall x \in G$, $\varphi(x^{-1}) = \varphi(x)^{-1}$.

(iii) $\forall n \in \mathbb{Z}$, $\varphi(x^n) = \varphi(x)^n$.

(iv) If $K \leq G$, then $\varphi(K) \leq H$.

(v) If $K \leq H$, then $\varphi^{-1}(K) \leq G$.

Definition 4.2.4 Kernel of Group Homomorphism

Let $\varphi : G \to H$ be a group homomorphism. The **kernel** of φ is defined by

$$\ker \varphi = \{x \in G \mid \varphi(x) = 1_H\}.$$

Proposition 4.2.5 Property of Kernel

Let G be a group. Then

(i) Let $\varphi : G \to H$ be a group homomorphism. Then φ is injective if and only if $\ker \varphi = \{1_G\}$.

Definition 4.2.6 Normal Subgroup

Let G be a group. A subgroup H of G is called a **normal subgroup** if $gHg^{-1} = H$ for all $g \in G$. In this case, we write $H \lhd G$.

Proposition 4.2.7 Equivalent Definition of Normal Subgroup

Let G be a group and H be a subgroup of G. Then the following are equivalent:

(i) H is a normal subgroup of G.

(ii) $\forall \gamma_g \in \mathrm{Inn}(G)$, $\gamma_g(H) \subseteq H$.

(iii) $gHg^{-1} \subseteq H$ for all $g \in G$.

(iv) $gHg^{-1} = H$ for all $g \in G$.

(v) $gH = Hg$ for all $g \in G$.

(vi) H is a union of conjugacy classes.

(vii) $H = \ker \varphi$ for some group homomorphism $\varphi : G \to K$.

Proposition 4.2.8 Properties of Normal Subgroup

Let G be a group.

(i) $\{1_G\}$ and G are normal subgroups of G.

(ii) If $H \leq K \leq G$ and $H \lhd G$, then $H \lhd K$.

(iii) If $H \lhd_{\text{char}} K \lhd G$, then $H \lhd G$.

(iv) Normality is preserved under surjective homomorphisms: if $f : G \to H$ is a surjective group homomorphism and $N \lhd G$, then $f(N) \lhd H$.

(v) Normality is preserved by taking inverse images of homomorphisms: if $f : G \to H$ is a group homomorphism and $N \lhd H$, then $f^{-1}(N) \lhd G$.

(vi) Normality is preserved on taking finite products: if $N_1 \lhd G_1$ and $N_2 \lhd G_2$, then $N_1 \times N_2 \lhd G_1 \times G_2$.

(vii) Given two normal subgroups, N and M, of G, their intersection $N \cap M$ and their product $NM = \{nm : n \in N \text{ and } m \in M\}$ are also normal subgroups of G.

Definition 4.2.9 Simple Group

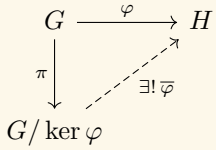
A group G is called **simple** if G is nontrivial and the only normal subgroups of G are $\{1_G\}$ and G.

Theorem 4.2.10 Fundamental Theorem on Homomorphisms

Let G, H be groups and $\varphi : G \to H$ be a group homomorphism. Define natural projection

$$\begin{aligned} \pi : G &\longrightarrow G/\ker\varphi \\ g &\longmapsto g\ker\varphi \end{aligned}$$

Then there exists a unique group homomorphism $\overline{\varphi} : G/\ker\varphi \to H$ such that the following diagram commutes



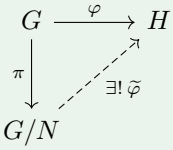
Moreover, $\overline{\varphi}$ is injective and we have $G/\ker\varphi \cong \mathrm{im}\varphi$.

Corollary 4.2.11 First isomorphism theorem

Let G, H be groups and $\varphi : G \to H$ be surjective group homomorphism. Then $G/\ker\varphi \cong H$.

Proposition 4.2.12 Universal Property of Quotient Group

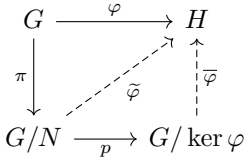
Let G be a group and $N \lhd G$ be a normal subgroup. Suppose $\pi : G \to G/N$ is the natural projection. Then π is initial in the category of group homomorphisms $\varphi : G \to H$ such that $N \subseteq \ker\varphi$.
That is, for any group H and group homomorphism $\varphi : G \to H$ such that $N \subseteq \ker\varphi$, there exists a unique group homomorphism $\widetilde{\varphi} : G/N \to H$ such that the following diagram commutes



Proof. Since $N \subseteq \ker\varphi$, there is a canonical projection

$$\begin{aligned} p : G/N &\longrightarrow G/\ker\varphi \\ gN &\longmapsto g\ker\varphi \end{aligned}$$

According to the following diagram, we can define $\widetilde{\varphi}$ by $\widetilde{\varphi} = \overline{\varphi} \circ p$.



Theorem 4.2.13 Second Isoomorphism Theorem

Let G be a group and H, K be subgroups of G. Then HK is a subgroup of G and $H \cap K$ is a normal subgroup of H. Moreover, we have

$$HK/H \cong K/(H \cap K).$$

4.3 Construction

4.3.1 Free Object

Let A be set. Define a **string** over the A to be a finite sequence of elements of A. The **concatenation** of two strings $\overline{a_1 \cdots a_n}$ and $\overline{b_1 \cdots b_m}$ is a binary operation $\diamond$ defined by

$$\overline{a_1 \cdots a_n} \diamond \overline{b_1 \cdots b_m} = \overline{a_1 \cdots a_n b_1 \cdots b_m}.$$

Definition 4.3.1 Word

Let S be a set. Define $S^{-1} = \left\{ s^{-1} \,\middle|\, s \in S \right\}$. A **word** on S is a string over $S \sqcup S^{-1} \sqcup \{1\}$. $\overline{1}$ is called an **empty word**. The **length** of a word w is the number of letters in w.

Definition 4.3.2 Reduced Word

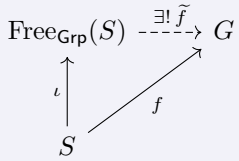
Let $W(S)$ be the set of all words on S. Define a relation $\approx$ on $W(S)$ as follows: for any $s \in S$

$$\overline{s^{-1}s} \approx \overline{1}, \quad \overline{ss^{-1}} \approx \overline{1}, \quad \overline{1s} \approx s, \quad \overline{s1} \approx \overline{1}$$

Define $\sim$ to be the equivalence relation generated by $\approx$. Let $\pi : W(S) \to W(S)/\sim, w \mapsto [w]_\sim$ denote the quotient map. It is easy to see that for any $[w]_\sim \in W(S)/\sim$, there exists a unique representative element $\rho(w) \in W(S)$ which has shortest length among all representatives of $[w]_\sim$. A word w is called **reduced** if $\rho(w) = w$.

Definition 4.3.3 Free Group

Let S be a set. The **free group** on S, denoted by $\mathrm{Free}_{\mathsf{Grp}}(S)$, together with a function $\iota : S \to \mathrm{Free}_{\mathsf{Grp}}(S)$, is defined by the following universal property: for any group G and any function $f : S \to G$, there exists a unique group homomorphism $\widetilde{f} : \mathrm{Free}_{\mathsf{Grp}}(S) \to G$ such that the following diagram commutes



The free group $\mathrm{Free}_{\mathsf{Grp}}(S)$ can be contructed as follows: as a set it consists of all reduced words on S. The binary operation $\cdot$ is concatenation with reduction defined by

$$w_1 \cdot w_2 = \rho(w_1 \diamond w_2).$$

The identity element is the empty word. The inverse of a word is obtained by reversing the order of the letters and replacing each letter by its inverse.

Example 4.3.1 Forgetful Functor $U : \mathsf{Grp} \to \mathsf{Set}$

The forgetful functor $U : \mathsf{Grp} \to \mathsf{Set}$ forgets the group structure of a group and returns the underlying set.

(i) U is representable by $(\mathbb{Z}, 1)$. The natural isomorphism $\phi : \mathrm{Hom}_{\mathsf{Grp}}(\mathbb{Z}, -) \xRightarrow{\sim} U$ is given by

$$\begin{aligned} \phi_G : \mathrm{Hom}_{\mathsf{Grp}}(\mathbb{Z}, G) &\xrightarrow{\sim} U(G) \\ f &\longmapsto f(1). \end{aligned}$$

A group homomorphism from $\mathbb{Z}$ to G is uniquely determined by its action on 1.

(ii) U is faithful but not full.

Proof. (i) $\phi : \mathrm{Hom}_{\mathsf{Grp}}(\mathbb{Z}, -) \xRightarrow{\sim} U$ is the composition of the following natural isomorphisms

$$\mathrm{Hom}_{\mathsf{Grp}}(\mathbb{Z}, -) \cong \mathrm{Hom}_{\mathsf{Grp}}(\mathrm{Free}_{\mathsf{Grp}}(\{*\}), -) \cong \mathrm{Hom}_{\mathsf{Set}}(\{*\}, U(-)) \cong U.$$

(ii) U is not full because not every mapping $f : \mathbb{Z} \to G$ is a group homomorphism. □

Proposition 4.3.4 Free-Forgetful Adjunction $\mathrm{Free}_{\mathsf{Grp}} \dashv U$

The free group functor $\mathrm{Free}_{\mathsf{Grp}}$ is left adjoint to the forgetful functor $U : \mathsf{Grp} \to \mathsf{Set}$

$$\mathsf{Set} \underset{U}{\overset{\mathrm{Free}_{\mathsf{Grp}}}{\rightleftarrows}} \mathsf{Grp} \quad (\perp)$$

The adjunction isomorphism is given by

$$\begin{aligned} \varphi_{S,G} : \mathrm{Hom}_{\mathsf{Grp}}(\mathrm{Free}_{\mathsf{Grp}}(S), G) &\xrightarrow{\sim} \mathrm{Hom}_{\mathsf{Set}}(S, U(G)) \\ g &\longmapsto g \circ \iota \end{aligned}$$

Proof. First we show that $\varphi_{S,G}$ is injective. Suppose $g_1, g_2 : \mathrm{Free}_{\mathsf{Grp}}(S) \to G$ are two group homomorphisms such that $g_1 \circ \iota = g_2 \circ \iota$. By the universal property of free group, we have $g_1 = g_2$. Then we show that $\varphi_{S,G}$ is surjective. Suppose $f : S \to U(G)$ is a function. By the universal property there exists a group homomorphism $\widetilde{f} : \mathrm{Free}_{\mathsf{Grp}}(S) \to G$ such that $\varphi_{S,G}(\widetilde{f}) = \widetilde{f} \circ \iota = f$. Finally, we show that $\varphi_{S,G}$ is natural in S and G. Suppose $h : S_1 \to S_2$ is a function and $q : G_1 \to G_2$ is a group homomorphism. Then we can check that for any $g \in \mathrm{Hom}_{\mathsf{Grp}}(\mathrm{Free}_{\mathsf{Grp}}(S_2), G_2)$,

$$\begin{aligned} \varphi_{S_1,G_1}(q \circ g \circ \iota_{S_1}) &= (q \circ g \circ \iota_{S_1}) \circ \iota_{S_1} \\ &= q \circ g \circ (\iota_{S_1} \circ \iota_{S_1}) \\ &= q \circ g \circ \iota_{S_2} \\ &= \varphi_{S_2,G_2}(g \circ \iota_{S_2}). \end{aligned}$$

□

4.3.2 Inverse Limit

Definition 4.3.5 Inverse Limit in Grp

Let I be a filtered thin category and $F : \mathsf{I}^{\mathrm{op}} \to \mathsf{Grp}$ be a functor. To unpack the information of F, denote $I := \mathrm{Ob}(\mathsf{I})$, $G_i := F(i)$ and $f_{ij} := F(i \to j)$. An **inverse system** is a pair $\left((G_i)_{i \in I}, (f_{ij})_{i \le j \in I}\right)$ where $f_{ij} : G_j \to G_i$ is a group homomorphism for each $i \le j$ such that

(i) $f_{ii} = \mathrm{id}_{G_i}$ for all $i \in I$.

(ii) $f_{ik} = f_{ij} \circ f_{jk}$ for all $i \le j \le k$.

The **inverse limit** of $\left((G_i)_{i \in I}, (f_{ij})_{i \le j \in I}\right)$ is the cofiltered limit $\varprojlim F$, also denoted by $\varprojlim_{i \in I} G_i$, which can be constructed as a subgroup of $\prod_{i \in I} G_i$ as follows

$$\varprojlim_{i \in I} G_i \cong \left\{ (x_i)_{i \in I} \in \prod_{i \in I} G_i \;\middle|\; x_i = f_{ij}(x_j) \text{ for all } i \le j \in I \right\}$$

equipped with natural projections $\pi_i : \varprojlim_{i \in I} G_i \to G_i$.

Example 4.3.2 Inverse Limit $\varprojlim_{i\geq 1} G_i$

Let $\mathsf{I} = (\mathbb{Z}_{\geq 1}, \leq)$ be a filtered thin category and $F : \mathsf{I}^{\mathrm{op}} \to \mathsf{Grp}$ be a functor. To determine an inverse system, it is sufficient to specify G_i and $f_{i,i+1} : G_{i+1} \to G_i$ for all $i \in \mathbb{Z}_{\geq 1}$. The inverse limit of this inverse system is denoted by $\varprojlim_{i\geq 1} G_i$, which we now write as G for simplicity.

G can be imaged as a tree with root layer being $G_0 = \{1\}$ and i-th layer being G_i. Each node in G_i has a unique parent node in G_{i-1}, which is determined by $f_{i,i-1}$. An element in G is a path starting from the root and passing through each G_i exactly once along the edges of the tree. The i-th component x_i of an element $x \in G$ includes all information of its history path from G_0 to G_i, which makes $x_1, x_2, \cdots, x_{i-1}$ redundant.

4.4 Group Action

4.4.1 Definitions

Definition 4.4.1 Symmetric Group

The **symmetric group** on a set X is the group whose elements are all bijections from X to X, with the group operation of function composition. The symmetric group on X is denoted by $\mathrm{Sym}(X)$ or $\mathrm{Aut}_{\mathsf{Set}}(X)$. If $X = \{1, 2, \cdots, n\}$, then we denote $\mathrm{Sym}(X)$ by S_n.

Definition 4.4.2 Group Action

Let G be a group and X be a set. A **group action** of G on X is a group homomorphism

$$\begin{aligned} \sigma : G &\longrightarrow \mathrm{Aut}_{\mathsf{Set}}(X) \\ g &\longmapsto \sigma_g \end{aligned}$$

If G acts on X by σ, we say (X, σ) is a G**-set**. If there is no ambiguity, we simply say X is a G-set.

Proposition 4.4.3 Equivalent Definition of Group Actions

Let G be a group and X be a set. A group action of G on X can be alternatively defined as a map

$$\begin{aligned} \cdot : G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

such that

(i) $\forall x \in X,\ e \cdot x = x$.

(ii) $\forall g, h \in G, \forall x \in X,\ (gh) \cdot x = g \cdot (h \cdot x)$.

The equivalence of the two definitions is given by

$$\sigma_g(x) = g \cdot x.$$

We say X is a right G-set if X is a left G^{op}-set.

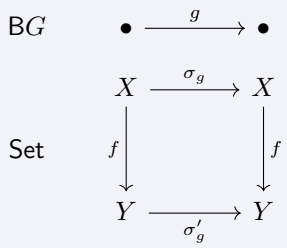
Definition 4.4.4 G-equivariant Map

Let G be a group and (X, σ), (Y, σ') be G-sets. A map $f : X \to Y$ is called G**-equivariant** if for all $g \in G$ and $x \in X$, we have

$$f(g \cdot x) = g \cdot f(x).$$

Equivalently, f is G-equivariant if it is a natural transformation $f : \sigma(-) \implies \sigma'(-)$ such that for any

$g \in G$, the following naturality diagram commutes



Definition 4.4.5 Category of G-sets

The categories of left G-sets, denoted by G-Set, are defined as follows:

- Objects: G-sets.
- Morphisms: G-equivariant maps.
- Composition of morphisms is the composition of functions.

G-Set can be identified with the functor category $[\mathsf{B}G, \mathsf{Set}]$, given by the following isomorphism of categories

$$\begin{aligned} G\text{-}\mathsf{Set} &\xrightarrow{\sim} [\mathsf{B}G, \mathsf{Set}] \\ (X, \sigma) &\longmapsto (\bullet \to X,\ \ \sigma : G \to \mathrm{Aut}_{\mathsf{Set}}(X)) \end{aligned}$$

Example 4.4.1 Trivial Group Action

Let G be a group and X be a set. The **trivial group action** of G on X is defined as $\sigma_g = \mathrm{id}_X$ for all $g \in G$.

Example 4.4.2 Actions on X Induce Actions on 2^X

If a group G acts on a set X, then G acts on the power set 2^X by

$$g \cdot A = \{g \cdot x \mid x \in A\}.$$

Definition 4.4.6 Product of G-Sets

The **product** of two G-sets X and Y is defined as the set $X \times Y$ with the G-action

$$g \cdot (x, y) = (g \cdot x, g \cdot y).$$

Alternatively, the product of two G-sets can be defined as the product of two functors, cf. Proposition 2.4.33.

Definition 4.4.7 Coproduct of G-Sets

The **coproduct** of two G-sets X and Y is defined as the set $X \sqcup Y$ with the G-action

$$g \cdot a = \begin{cases} g \cdot a & a \in X \\ g \cdot a & a \in Y \end{cases}$$

Alternatively, the coproduct of two G-sets can be defined as the coproduct of two functors, cf. Proposition 2.4.33.

Example 4.4.3 $\mathrm{Aut}_{\mathsf{C}}(X)$ acts on $\mathrm{Hom}_{\mathsf{C}}(X, Y)$ and $\mathrm{Hom}_{\mathsf{C}}(Y, X)$

Let X and Y be objects in a category C. Then $\mathrm{Aut}_{\mathsf{C}}(X)$ acts on $\mathrm{Hom}_{\mathsf{C}}(X, Y)$ by the composition of

functors

$$\mathsf{BAut}_{\mathsf{C}}(X) \xrightarrow{(-)^{-1}} \mathsf{BAut}_{\mathsf{C}}(X)^{\mathrm{op}} \hookrightarrow \mathsf{C}^{\mathrm{op}} \xrightarrow{\mathrm{Hom}_{\mathsf{C}}(-,Y)} \mathsf{Set}$$

$$\begin{array}{ccccccc}
\bullet & \longmapsto & \bullet & \longmapsto & X & \longmapsto & \mathrm{Hom}(X,Y) \\
\downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g^{-1}} & & \downarrow{\scriptstyle g^{-1}} & & \downarrow{\scriptstyle (g^{-1})^*} \\
\bullet & \longmapsto & \bullet & \longmapsto & X & \longmapsto & \mathrm{Hom}(X,Y)
\end{array}$$

Writing explicily, the action is given by

$$\begin{aligned}
\mathrm{Aut}_{\mathsf{C}}(X) \times \mathrm{Hom}_{\mathsf{C}}(X,Y) &\longrightarrow \mathrm{Hom}_{\mathsf{C}}(X,Y) \\
(g,f) &\longmapsto f \circ g^{-1}
\end{aligned}$$

Similarly, $\mathrm{Aut}_{\mathsf{C}}(Y)$ acts on $\mathrm{Hom}_{\mathsf{C}}(Y,X)$ by

$$\mathsf{BAut}_{\mathsf{C}}(X) \hookrightarrow \mathsf{C} \xrightarrow{\mathrm{Hom}_{\mathsf{C}}(Y,-)} \mathsf{Set}$$

$$\begin{array}{ccccc}
\bullet & \longmapsto & X & \longmapsto & \mathrm{Hom}(Y,X) \\
\downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g_*} \\
\bullet & \longmapsto & X & \longmapsto & \mathrm{Hom}(X,Y)
\end{array}$$

Writing explicily, the action is given by

$$\begin{aligned}
\mathrm{Aut}_{\mathsf{C}}(Y) \times \mathrm{Hom}_{\mathsf{C}}(Y,X) &\longrightarrow \mathrm{Hom}_{\mathsf{C}}(Y,X) \\
(g,f) &\longmapsto g \circ f
\end{aligned}$$

Example 4.4.4 Actions on X Induce Actions on $\mathrm{Hom}_{\mathsf{Set}}(X,Y)$

If G acts on X through a functor $\sigma(-) : \mathsf{B}G \to \mathsf{Set}$, then it also acts on $\mathrm{Hom}_{\mathsf{Set}}(X,Y)$ for any set Y by the composition of functors

$$\mathsf{B}G \xrightarrow{(-)^{-1}} \mathsf{B}G^{\mathrm{op}} \xrightarrow{\sigma(-)^{\mathrm{op}}} \mathsf{Set}^{\mathrm{op}} \xrightarrow{\mathrm{Hom}_{\mathsf{Set}}(-,Y)} \mathsf{Set}$$

The left action on $\mathrm{Hom}_{\mathsf{Set}}(X,Y)$ is given explicitly as follows: for all $g \in G$, $f \in \mathrm{Hom}_{\mathsf{Set}}(X,Y)$ and $x \in X$,

$$(g \cdot f)(x) = f(g^{-1} \cdot x).$$

Equivalently, the right action $\star$ on $\mathrm{Hom}_{\mathsf{Set}}(X,Y)$ is given by

$$(f \star g)(x) = f(g \cdot x).$$

Proof. We can check that

$$\begin{aligned}
(g_1 \cdot (g_2 \cdot f))(x) &= (g_2 \cdot f)\left(g_1^{-1} \cdot x\right) \\
&= (g_2 \cdot f)\left(g_1^{-1} \cdot x\right) \\
&= f\left(g_2^{-1} \cdot \left(g_1^{-1} \cdot x\right)\right) \\
&= f\left(\left(g_2^{-1} g_1^{-1}\right) \cdot x\right) \\
&= \left((g_1 g_2) \cdot f\right)(x).
\end{aligned}$$

and also check that

$$\begin{aligned}((f \star g_1) \star g_2)(x) &= (f \star g_1)(g_2 \cdot x) \\ &= f(g_1 \cdot (g_2 \cdot x)) \\ &= f((g_1 g_2) \cdot x) \\ &= (f \star (g_1 g_2))(x).\end{aligned}$$

□

Definition 4.4.8 Orbit of a Group Action

Let G be a group acting on a set X. For $x \in X$, the **orbit** of x is defined as

$$Gx = \{g \cdot x \mid g \in G\}.$$

Definition 4.4.9 Orbit Space

Let G be a group acting on a set X. The **orbit space** of G acting on X is defined as

$$G\backslash X = \{Gx \mid x \in X\}.$$

If G acts on X, then G acts on $G\backslash X$ trivially by $g \cdot Gx = Gx$.

Proposition 4.4.10 Orbit Decomposition

Let G be a group acting on a set X. We define a equivalence relation $\sim$ on X by

$$x \sim y \iff Gx = Gy.$$

Then the equivalence class of x is exactly Gx. The quotient set $X/\sim$ is exactly the orbit space $G\backslash X$. And we have a partition of X by the orbits of G acting on X

$$X = \bigsqcup_{Gx \in G\backslash X} Gx.$$

Proof. We can check that the equivalence class of x is Gx. If $y \sim x$, then $y \in Gy = Gx$. If $y \in Gx$, then $Gy \subseteq Gx$ and $x \in Gy$. Note $x \in Gy$ implies $Gx \subseteq Gy$. We have $Gx = Gy$, i.e. $x \sim y$. □

If G acts on X, then G acts on $G\backslash X$ trivially.

Definition 4.4.11 G-invariant element

Let G be a group acting on a set X. An element $x \in X$ is called **G-invariant** if $Gx = \{x\}$ or equivalently $|Gx| = 1$. The set of all G-invariant elements is denoted by X^G

$$X^G = \{x \in X \mid Gx = \{x\}\} = \{x \in X \mid \forall g \in G, g \cdot x = x\}.$$

Definition 4.4.12 Stabilizer Subgroup

Let G be a group acting on a set X. For $x \in X$, the **stabilizer subgroup** of of G with respect to x is defined as

$$\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}.$$

It is easy to see that $\mathrm{Stab}_G(x)$ is a subgroup of G.

Proposition 4.4.13 Properties of Stabilizer Subgroup

Let G be a group acting on a set X. For $x \in X$, the stabilizer subgroup $\mathrm{Stab}_G(x)$ has the following properties

(i) $x \in X^G \iff \mathrm{Stab}_G(x) = G$.

(ii) $\ker(G \to \mathrm{Aut}_{\mathsf{Set}}(X)) = \bigcap_{x \in X} \mathrm{Stab}_G(x)$.

(iii) $\mathrm{Stab}_G(gx) = g\mathrm{Stab}_G(x)g^{-1}$ for any $g \in G$. Hence, we have a bijection between the G-orbit of x and the conjugacy class of stabilizer subgroup $\mathrm{Stab}_G(x)$

$$\begin{aligned} Gx &\xrightarrow{\sim} \mathrm{Cl}(\mathrm{Stab}_G(x)) \\ gx &\longmapsto g\mathrm{Stab}_G(x)g^{-1} \end{aligned}$$

(iv) $\mathrm{Stab}_G(gx) = \mathrm{Stab}_G(x) \iff g \in \mathrm{N}_G(\mathrm{Stab}_G(x))$.

If $X \curvearrowleft G$ is a right action, then we have $\mathrm{Stab}_G(xg) = g^{-1}\mathrm{Stab}_G(x)g$ for any $g \in G$.

Proof. (i)

$$x \in X^G \iff \forall g \in G, gx = x \iff \mathrm{Stab}_G(x) = G.$$

(ii)

$$g \in \ker(G \to \mathrm{Aut}_{\mathsf{Set}}(X)) \iff \forall x \in X,\ gx = x \iff g \in \bigcap_{x \in X} \mathrm{Stab}_G(x).$$

(iii) Let $h \in \mathrm{Stab}_G(gx)$, meaning $h(gx) = gx$. Applying g^{-1} to both sides, we get $g^{-1}h(gx) = g^{-1}(gx) = x$. Thus, $g^{-1}hg \in \mathrm{Stab}_G(x)$, meaning $h \in g\mathrm{Stab}_G(x)g^{-1}$. Conversely, if $h \in g\mathrm{Stab}_G(x)g^{-1}$, then $h = gkg^{-1}$ for some $k \in \mathrm{Stab}_G(x)$. Therefore, $h(gx) = g(kx) = gx$, so $h \in \mathrm{Stab}_G(gx)$. Thus, $\mathrm{Stab}_G(gx) = g\mathrm{Stab}_G(x)g^{-1}$.

(iv)

$$\mathrm{Stab}_G(gx) = \mathrm{Stab}_G(x) \iff g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(x) \iff g \in \mathrm{N}_G(\mathrm{Stab}_G(x)).$$

□

Definition 4.4.14 Faithful Group Action

Let G be a group acting on a set X. The action is called **faithful** if any of the following equivalent conditions holds

(i) $G \to \mathrm{Aut}_{\mathsf{Set}}(X)$ is injective.

(ii) $\bigcap_{x \in X} \mathrm{Stab}_G(x) = \{1_G\}$.

(iii) $\forall x \in X,\ g \cdot x = x \implies g = 1_G$.

For any group action, we can always make it faithful by quotienting out the kernel of $G \to \mathrm{Aut}_{\mathsf{Set}}(X)$.

Definition 4.4.15 Free Group Action

Let G be a group acting on a set X. The action is called **free** if any of the following equivalent conditions holds

(i) For all $x \in X$, $\mathrm{Stab}_G(x) = \{1_G\}$.

(ii) $\exists x \in X,\ g \cdot x = x \implies g = 1_G$.

It is clear that a free action is faithful, but the converse does not hold in general. For example, the dihedral group D_3 acts on an equilateral triangle faithfully but not freely, since the reflections fix one vertex and swap the other two.

Definition 4.4.16 Transitive Group Action

Let G be a group acting on a set X. The action is called **transitive** if any of the following equivalent conditions holds

(i) For any $x, y \in X$, there exists $g \in G$ such that $g \cdot x = y$.

(ii) X has only one orbit, i.e. $X = Gx$ for any $x \in X$.

If G acts transitively on X, then X is called a **transitive G-set** or **homogeneous space for G**.

The following proposition shows that we can understand a group action on a set X by studying the group action on each G-orbit Gx separately.

Proposition 4.4.17 G Acts on Orbit Gx Transitively

Let G be a group acting on a set X and $x \in X$. Then G acts on the orbit Gx by left multiplication transitively. And we have a G-set isomorphism

$$X \cong \bigsqcup_{Gx \in G\backslash X} Gx,$$

which decomposes any G-set into coproduct of transitive G-sets.

Proposition 4.4.18 Properties of G-equivariant Maps between Transitive G-sets

Let G be a group acting on a set X and Y transitively. Then we have

(i) Any G-equivariant map $f : X \to Y$ is uniquely determined by its value at one point $x \in X$:

$$f(g \cdot x) = g \cdot f(x), \quad \forall g \in G.$$

(ii) If $X \neq \varnothing$, then any G-equivariant map $f : X \to Y$ is surjective.

(iii) Assume $x \in X$ and $y \in Y$. Then the following are equivalent:

a) There exists a unique G-equivariant map $f : X \to Y$ such that $f(x) = y$.

b) There exists a unique G-equivariant map $p : G/\mathrm{Stab}_G(x) \to G/\mathrm{Stab}_G(y)$ such that $p(\mathrm{Stab}_G(x)) = \mathrm{Stab}_G(y)$.

c) $\mathrm{Stab}_G(x) \subseteq \mathrm{Stab}_G(y)$.

Proof. (i) For any $x' \in X$, we can assume $x' = g \cdot x$ for some $g \in G$. Since f is G-equivariant, we have

$$f(g \cdot x) = g \cdot f(x).$$

(ii) Suppose $x \in X$, and $y = f(x) \in Y$. For any $y' \in Y$, we can assume $y' = g \cdot y$ for some $g \in G$. And we have

$$f(g \cdot x) = g \cdot f(x) = g \cdot y = y'.$$

(iii) a) $\Longrightarrow$ c). Suppose $f : X \to Y$ is a G-equivariant map such that $f(x) = y$. For any $g \in \mathrm{Stab}_G(x)$, we have

$$gy = gf(x) = f(gx) = f(x) = y,$$

which implies $g \in \mathrm{Stab}_G(y)$. Thus we show that $\mathrm{Stab}_G(x) \subseteq \mathrm{Stab}_G(y)$.

c) $\Longrightarrow$ a). suppose $\mathrm{Stab}_G(x) \subseteq \mathrm{Stab}_G(y)$. We can define $f : X \to Y$ by $f(g \cdot x) = g \cdot y$. It is well-defined since

$$g_1 \cdot x = g_2 \cdot x \implies g_2^{-1} g_1 \in \mathrm{Stab}_G(x) \implies g_2^{-1} g_1 \in \mathrm{Stab}_G(y) \implies g_1 \cdot y = g_2 \cdot y.$$

a) $\Longleftrightarrow$ b). It is a direct consequence of Proposition 4.4.26.

□

Corollary 4.4.19 G-maps between Left Coset Spaces

Suppose H, K are subgroups of G. Then we know G left acts on G/H and G/K.

(i) If $\alpha : G/H \longrightarrow G/K$ is a G-map, then α has the form $\alpha(gH) = grK$, where the element $r \in G$ satisfies $H \subseteq rKr^{-1}$.

(ii) If there exists $r \in G$ such that $H \subseteq rKr^{-1}$, then the map $\alpha : G/H \longrightarrow G/K$ defined by $\alpha(gH) = grK$ is a G-map.

Proof. (i) Suppose $\alpha : G/H \longrightarrow G/K$ is a G-map and $\alpha(H) = rK$. The equivariance condition gives $\alpha(gH) = grK$. And By Proposition 4.4.18, we have

$$H = \mathrm{Stab}_G(H) \subseteq \mathrm{Stab}_G(rK) = r\mathrm{Stab}_G(K)r^{-1} = rKr^{-1}.$$

(ii) If there exists $r \in G$ such that

$$H = \mathrm{Stab}_G(H) \subseteq r\mathrm{Stab}_G(K)r^{-1} = \mathrm{Stab}_G(rK),$$

then by Proposition 4.4.18, there exists a unique G-map $\alpha : G/H \to G/K$ such that $\alpha(H) = rK$. Thus $\alpha(gH) = grK$ for all $g \in G$.

□

Proposition 4.4.20 Transitive G-set Isomorphism Criterion

Suppose X, Y are transitive G-sets and $x \in X$, $y \in Y$. Then we have

(i) There exists a G-set isomorphism $f : X \xrightarrow{\sim} Y$ such that $f(x) = y$ if and only if $\mathrm{Stab}_G(x) = \mathrm{Stab}_G(y)$.

(ii) $X \cong Y$ as G-sets if and only if $\mathrm{Stab}_G(x)$ and $\mathrm{Stab}_G(y)$ are conjugate subgroups in G.

Proof. (i) Suppose there exists a G-set isomorphism $f : X \xrightarrow{\sim} Y$ such that $f(x) = y$. Then $f^{-1} : Y \xrightarrow{\sim} X$ is also a G-set isomorphism such that $f^{-1}(y) = x$. By Proposition 4.4.18, we have both $\mathrm{Stab}_G(x) \subseteq \mathrm{Stab}_G(y)$ and $\mathrm{Stab}_G(y) \subseteq \mathrm{Stab}_G(x)$, which implies $\mathrm{Stab}_G(x) = \mathrm{Stab}_G(y)$.

Conversely, suppose $\mathrm{Stab}_G(x) = \mathrm{Stab}_G(y)$. By the previous proposition, there exists a unique G-equivariant map $f : X \to Y$ such that $f(x) = y$. There also exists a unique G-equivariant map $h : Y \to X$ such that $h(y) = x$. Since for any $g \in G$, we have

$$h \circ f(g \cdot x) = h(g \cdot y) = g \cdot h(y) = g \cdot x, \quad f \circ h(g \cdot y) = f(g \cdot x) = g \cdot f(x) = g \cdot y,$$

we know $h \circ f = \mathrm{id}_X$ and $f \circ h = \mathrm{id}_Y$. Thus f is a G-set isomorphism.

(ii) Suppose $X \cong Y$ as G-sets. Then there exists a G-set isomorphism $f : X \xrightarrow{\sim} Y$. We can assume $f(x) = g \cdot y$ for some $g \in G$. By the previous proposition, we have

$$\mathrm{Stab}_G(x) = \mathrm{Stab}_G(f(x)) = \mathrm{Stab}_G(g \cdot y) = g\mathrm{Stab}_G(y)g^{-1}.$$

Conversely, suppose $\mathrm{Stab}_G(x)$ and $\mathrm{Stab}_G(y)$ are conjugate subgroups in G. Then there exists $g \in G$ such that

$$\mathrm{Stab}_G(x) = g\mathrm{Stab}_G(y)g^{-1} = \mathrm{Stab}_G(g \cdot y).$$

By the previous proposition, we have a G-set isomorphism $f : X \xrightarrow{\sim} Y$ such that $f(x) = g \cdot y$. Thus $X \cong Y$ as G-sets.

□

Example 4.4.5 The Orbit Decomposition of Subgroup Action

Let G be a group acting on a set X with orbit decomposition

$$X = \bigsqcup_{i \in I} Gx_i$$

Suppose H be a subgroup of G and G has right coset decomposition

$$G = \bigsqcup_{j \in J} Hg_j$$

Then H also acts on X and each G-orbit is disjoint union of some H-orbits, which can written as

$$Gx_i = \bigsqcup_{k\in K} Hs_{ik}.$$

More concretely, Gx_i is the union of the cosets $H(g_jx_i)$ $(j \in J)$,

$$Gx_i = \bigcup_{j\in J} Hg_jx_i.$$

But $H(g_jx_i)$ may coincide with $H(g_{j'}x_i)$ for $j \neq j'$. We can duplicate $H(g_jx_i)$ $(j \in J)$ by checking if there exists $h \in H$ such that $hg_js_i = g_{j'}s_i$. Suppose $a \sim_H b$ iff a and b in the same H-orbit. Then we get

$$\{s_{ik} \mid k \in K\} = \{g_jx_i \mid j \in J\}/\sim_H .$$

Definition 4.4.21 Regular Group Action

Let G be a group acting on a set X. The action is called **regular** if any of the following equivalent conditions holds

(i) The action is transitive and free.

(ii) For any $x, y \in X$, there exists unique $g \in G$ such that $g \cdot x = y$.

If G acts regularly on X, then X is called a **principal homogeneous space for** G or a G**-torsor**.

4.4.2 Coset

Example 4.4.6 Left Multiplication Action

Let G be a group. The **left multiplication action** of G on itself is defined as

$$\begin{aligned} m^L : G &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto (x \longmapsto gx) \end{aligned}$$

Example 4.4.7 Right Multiplication Action

Let G be a group. The **right multiplication action** of G on itself is defined as

$$\begin{aligned} m^R : G^\circ &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto (x \longmapsto xg) \end{aligned}$$

Definition 4.4.22 Left Cosets

Let G be a group and H be a subgroup of G. H° can act on G through $H^\circ \hookrightarrow G^\circ \xrightarrow{m^R} \mathrm{Aut}(G)$, namely

$$\begin{aligned} H^\circ &\longrightarrow \mathrm{Aut}(G) \\ h &\longmapsto (g \longmapsto gh) \end{aligned}$$

The orbit of g under H° is called the **left coset** of H containing g, denoted by gH

$$gH = H^\circ g = \{gh \mid h \in H\}.$$

The set of all left cosets of H is denoted by G/H, called the left coset space of G modulo H. G/H is the orbit space of G under the right multiplication action of H.

Example 4.4.8 G Acts on G/H Transitively

Let G be a group and H be a subgroup of G. G acts on G/H through

$$\begin{aligned} G &\longrightarrow \mathrm{Aut}(G/H) \\ g &\longmapsto (xH \longmapsto gxH) \end{aligned}$$

For any $xH, yH \in G/H$, we have $yH = gxH$ for some $g = yx^{-1} \in G$. Thus G acts on G/H transitively. The stabilizer subgroup of xH is given by

$$\mathrm{Stab}_G(xH) = xHx^{-1}.$$

Definition 4.4.23 Right Cosets

Let G be a group and H be a subgroup of G. H can act on G through $H \hookrightarrow G \xrightarrow{m^L} \mathrm{Aut}(G)$, namely

$$\begin{aligned} H &\longrightarrow \mathrm{Aut}(G) \\ h &\longmapsto (g \longmapsto hg) \end{aligned}$$

The orbit of g under H is called the **right coset** of H containing g, denoted by Hg

$$Hg = \{hg \mid h \in H\},$$

which matches notation of orbit. The set of all right cosets of H is denoted by $H\backslash G$, called the right coset space of G modulo H.

Definition 4.4.24 Index of Subgroup

Let G be a group and H be a subgroup of G. The **index** of H in G is defined as the cardinality of G/H or $H\backslash G$, denoted by $[G : H]$.

Theorem 4.4.25 Lagrange's Theorem

Let G be a finite group and H be a subgroup of G. Then $|G| = |H|[G : H]$.

Proposition 4.4.26 G-Set Isomorphism $G/\mathrm{Stab}_G(x) \cong Gx$

Let G be a group acting on a set X and $x \in X$. Then the map

$$\begin{aligned} F : G/\mathrm{Stab}_G(x) &\longrightarrow Gx \\ g\mathrm{Stab}_G(x) &\longmapsto g \cdot x \end{aligned}$$

is a G-set isomorphism. The transitive G-set $G/\mathrm{Stab}_G(x)$ is defined in Example 4.4.8.

Proof. The map is well-defined since for any $h \in \mathrm{Stab}_G(x)$, we have $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x$. The map is a G-set homomorphism since for any $g_1, g_2 \in G$,

$$F\left(g_1 \cdot g_2\mathrm{Stab}_G(x)\right) = (g_1g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot F\left(g_2\mathrm{Stab}_G(x)\right).$$

The map is injective since for any $g, h \in G$, if $g \cdot x = h \cdot x$, then $h^{-1}g \in \mathrm{Stab}_G(x)$. Hence $g\mathrm{Stab}_G(x) = h\mathrm{Stab}_G(x)$. The map is surjective because for any $g \cdot x \in Gx$, we have $F\left(g\mathrm{Stab}_G(x)\right) = g \cdot x$. □

Theorem 4.4.27 Orbit-Stabilizer Theorem

Let G be a group acting on a set X. For $x \in X$, we have

$$|G| = |Gx| \cdot |\mathrm{Stab}_G(x)|.$$

Proof. According to Proposition 4.4.26, we have

$$|Gx| = |G/\mathrm{Stab}_G(x)| = |G|/\left|\mathrm{Stab}_G(x)\right|.$$

□

Theorem 4.4.28 Burnside's Lemma

Let G be a finite group acting on a finite set X. Then the number of orbits of G on X is equal to

$$|G\backslash X| = \frac{1}{|G|}\sum_{g\in G}|X^g|,$$

where $X^g = \{x \in X \mid g \cdot x = x\}$ is the set of fixed points of g.

Proof.

$$\begin{aligned}
\sum_{g\in G}|X^g| &= |\{(g,x) \in G \times X \mid g\cdot x = x\}| \\
&= \sum_{x\in X}|\mathrm{Stab}_G(x)| \\
&= \sum_{x\in X}\frac{|G|}{|Gx|} \quad \text{by Orbit-Stabilizer Theorem} \\
&= |G|\sum_{Gy\in G\backslash X}\sum_{x\in Gy}\frac{1}{|Gx|} \\
&= |G|\sum_{Gy\in G\backslash X}|Gy|\,\frac{1}{|Gy|} \\
&= |G|\sum_{Gy\in G\backslash X}1 \\
&= |G|\cdot|G\backslash X|.
\end{aligned}$$

□

4.4.3 Conjugacy Action

Definition 4.4.29 Conjugacy Action and Inner Automorphism Group

Let G be a group. The **conjugacy action** of G on itself is defined as a group homomorphism

$$\begin{aligned}
\gamma : G &\longrightarrow \mathrm{Aut}_{\mathsf{Grp}}(G) \\
g &\longmapsto (\gamma_g : x \longmapsto gxg^{-1})
\end{aligned}$$

The **inner automorphism group** of G is defined as the image of γ

$$\mathrm{Inn}(G) = \mathrm{im}\,\gamma = \{\gamma_g \mid g \in G\}.$$

And we have inclusion relation $\mathrm{Inn}(G) \hookrightarrow \mathrm{Aut}_{\mathsf{Grp}}(G) \hookrightarrow \mathrm{Aut}_{\mathsf{Set}}(G)$.

Definition 4.4.30 Conjugate Subgroups

From Example 4.4.2, we see conjugacy action on G induces an action on its power set 2^G:

$$\begin{aligned}
G \times 2^G &\longrightarrow 2^G \\
(g, E) &\longmapsto gEg^{-1}
\end{aligned}$$

If H is a subgroup of G, then gHg^{-1} is also a subgroup of G. We say H and gHg^{-1} are **conjugate subgroups** of G.

Proposition 4.4.31 Equivalent Characterization of Inner Automorphisms

Let G be a group and $\varphi \in \mathrm{Aut}(G)$. Then $\varphi \in \mathrm{Inn}(G)$ if and only if φ satisfies the property:

$$G \text{ is embedded in a group } H \implies \varphi \text{ extends to an automorphism of } H.$$

To be specific, the property can be stated as: for any monomophism $\iota : G \hookrightarrow H$, there exists $\psi \in \mathrm{Aut}(H)$ such that the following diagram commutes

$$\begin{array}{ccc} G & \xhookrightarrow{\iota} & H \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ G & \xhookrightarrow[\iota]{} & H \end{array}$$

Definition 4.4.32 Outer Automorphism Group

Let G be a group. Then we have $\mathrm{Inn}(G) \lhd \mathrm{Aut}_{\mathsf{Grp}}(G)$. And the **outer automorphism group** of G is defined as

$$\mathrm{Out}(G) = \mathrm{coker}\,\gamma = \mathrm{Aut}_{\mathsf{Grp}}(G)/\mathrm{Inn}(G).$$

Definition 4.4.33 Characteristic Subgroup

Let G be a group. A subgroup $H \leq G$ is called a **characteristic subgroup** if

$$\forall \varphi \in \mathrm{Aut}_{\mathsf{Grp}}(G),\ \varphi(H) \subseteq H.$$

It would be equivalent to require the stronger condition that $\forall \varphi \in \mathrm{Aut}_{\mathsf{Grp}}(G)$, $\varphi(H) = H$, because

$$\varphi(H) \subseteq H \implies \varphi^{-1}(H) \subseteq H \implies H \subseteq \varphi(H).$$

Definition 4.4.34 Fully Characteristic Subgroup

Let G be a group. A subgroup $H \leq G$ is called a **fully characteristic subgroup** if

$$\forall \varphi \in \mathrm{End}_{\mathsf{Grp}}(G),\ \varphi(H) \subseteq H.$$

Definition 4.4.35 Word Map

Suppose G is a group and

$$x = x_{i_1}^{\alpha_1} \cdots x_{i_m}^{\alpha_m} \in F\langle x_1, \cdots, x_n \rangle$$

is a reduced word in a free group of rank n, where $\alpha_k \in \mathbb{Z} - \{0\}$ for $k = 1, 2, \cdots, m$. The **word map** induced by x is defined as a map

$$\begin{aligned} w_x : G^m &\longrightarrow G \\ (g_1, \cdots, g_m) &\longmapsto g_{i_1}^{\alpha_1} \cdots g_{i_m}^{\alpha_m}. \end{aligned}$$

Definition 4.4.36 Verbal Subgroup

Let G be a group and $\mathcal{W}$ be a collection of word maps. A subgroup $H \leq G$ is called a **verbal subgroup** if H is the subgroup generated by

$$\{w(g_1, \cdots, g_n) \mid w \in \mathcal{W},\ g_i \in G\}.$$

Definition 4.4.37 Commutator

Let G be a group. The word map induced by $xyx^{-1}y^{-1}$ is a binary operation defined on G, denoted by

$$\begin{aligned}[\cdot,\cdot] : G \times G &\longrightarrow G \\ (x,y) &\longmapsto [x,y] = xyx^{-1}y^{-1}\end{aligned}$$

$[x,y]$ is called the **commutator** of x and y.

Proposition 4.4.38 Properties of Commutator

Let G be a group. Then

(i) x commutes with y if and only if $[x,y] = 1_G$.

(ii) $[x,y]^{-1} = [y,x]$.

(iii) For any homomorphism $f : G \to H$, $f([x,y]) = [f(x), f(y)]$.

Proposition 4.4.39

According to the extent that a subgroup is preserved by endomorphisms, we have the following inclusions

$$\{\text{verbal subgroups}\} \subseteq \{\text{fully characteristic subgroups}\} \subseteq \{\text{characteristic subgroups}\} \subseteq \{\text{normal subgroups}\}.$$

Definition 4.4.40 Commutator Subgroup

Let G be a group. The **commutator subgroup** or **derived subgroup** of G is the subgroup generated by all the commutators, denoted by

$$[G,G] = \langle \{[x,y] \mid x,y \in G\} \rangle.$$

Proposition 4.4.41 Properties of Commutator Subgroup

Let G be a group. Then

(i) $[G,G]$ is a verbal subgroup with $\mathcal{W} = \{[\cdot,\cdot]\}$. Hence $[G,G] \lhd G$.

(ii) $[G,G]$ is the smallest normal subgroup of G such that $G/[G,G]$ is abelian.

(iii) $[G,G] = \{1_G\}$ if and only if G is abelian.

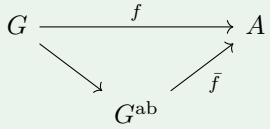
Definition 4.4.42 Abelianization

Let G be a group. The **abelianization** of G is defined as the quotient group

$$G^{\mathrm{ab}} = G/[G,G].$$

Proposition 4.4.43 Universal Property of Abelianization

Let G be a group and A be an abelian group. Then any group homomorphism $f : G \to A$ factors through G^{ab} uniquely, that is, there exists a unique homomorphism $\bar{f} : G^{\mathrm{ab}} \to A$ such that the following diagram commutes



Definition 4.4.44 Normalizer

Let G be a group and S be a subset of G. The **normalizer** of S in G is defined as

$$\mathrm{N}_G(S) = \left\{g \in G \mid gSg^{-1} = S\right\}.$$

Let G acts on 2^G by conjugation (c.f. Definition 4.4.29). Then $\mathrm{N}_G(S) = \mathrm{Stab}_G(S) \leq G$.

Proposition 4.4.45 Normalizer of a Subgroup is the Largest Subgroup in which the Subgroup is Normal

Let G be a group and H be a subgroup of G. Then $H \lhd \mathrm{N}_G(H)$. Moreover, $\mathrm{N}_G(H)$ is the largest subgroup of G in which H is normal, i.e.

$$H \lhd K \leq G \implies H \lhd K \leq \mathrm{N}_G(H) \leq G.$$

Proof. For all $n \in \mathrm{N}_G(H)$, we have $nHn^{-1} = H$, which implies $H \lhd \mathrm{N}_G(H)$. Suppose $H \lhd K \leq G$. Then $\forall k \in K$, $kHk^{-1} = H$. Hence $k \in \mathrm{N}_G(H)$. Therefore we prove the maximality of $\mathrm{N}_G(H)$. □

Definition 4.4.46 Centralizer

Let G be a group and S be a subset of G. The **centralizer** of S in G is defined as

$$\mathrm{C}_G(S) = \{g \in G \mid \forall s \in S,\ gs = sg\}.$$

The centralizer of $\{x\}$ is the stabilizer subgroup of x under conjugacy action, denoted by

$$\mathrm{C}_G(x) = \{g \in G \mid gx = xg\} = \{g \in G \mid gxg^{-1} = x\} = \mathrm{Stab}_G(x) = \mathrm{N}_G(x).$$

Definition 4.4.47 Center of a Group

Let G be a group. The **center** of G is defined as the centralizer of G in G, denoted by

$$Z_G = \mathrm{C}_G(G) = \{g \in G \mid \forall x \in G,\ gx = xg\}.$$

Proposition 4.4.48 Normalizer $\mathrm{N}_G(S)$ Acts on S by Conjugation

Let G be a group and $S \subseteq G$. Then $\mathrm{N}_G(S)$ acts on S by conjugation, i.e. by the group homomorphism

$$\begin{aligned}\Psi_S : \mathrm{N}_G(S) &\longrightarrow \mathrm{Aut}_{\mathsf{Set}}(S)\\ g &\longmapsto \gamma_g|_S\end{aligned}$$

where $\gamma_g|_S(s) = gsg^{-1}$ for all $s \in S$. Moreover, we have $\ker \Psi_S = \mathrm{C}_G(S) \lhd \mathrm{N}_G(S)$.

Proof. Ψ_S is obtained from restriction $\Psi_S : \mathrm{N}_G(S) \hookrightarrow G \xrightarrow{\gamma} \mathrm{Aut}_{\mathsf{Set}}(G)$. Since for any $g \in \mathrm{N}_G(S)$, $\gamma_g|_S(S) = \left\{gsg^{-1} \in G \mid s \in S\right\} \subseteq S$, we see $\Psi_S(g) = \gamma_g|_S \in \mathrm{Aut}_{\mathsf{Set}}(S)$. The kernel of Ψ_S is

$$\ker \Psi_S = \{n \in \mathrm{N}_G(S) \mid \gamma_n|_S = \mathrm{id}_S\} = \left\{n \in \mathrm{N}_G(S) \mid \forall s \in S, nsn^{-1} = s\right\} = \mathrm{N}_G(S) \cap \mathrm{C}_G(S) = \mathrm{C}_G(S).$$

Theorem 4.4.49 N/C Theorem

Let G be a group and H be a subgroup of G. By Proposition 4.4.48, $\mathrm{N}_G(H)$ acts on H by conjugation through the group homomorphism $\Psi_H : \mathrm{N}_G(H) \to \mathrm{Aut}_{\mathsf{Set}}(H)$. We assert that

$$\mathrm{N}_G(H)/\mathrm{C}_G(H) \cong \mathrm{Im}\Psi_H \leq \mathrm{Aut}_{\mathsf{Grp}}(H).$$

Hence it is legal to define

$$\begin{aligned}\Psi_H : \mathrm{N}_G(H) &\longrightarrow \mathrm{Aut}_{\mathsf{Grp}}(H)\\ g &\longmapsto \gamma_g|_H\end{aligned}$$

Corollary 4.4.50 Kernel and Cokernel of Conjugation Action $\gamma : G \to \mathrm{Aut}_{\mathsf{Grp}}(G)$

Let G be a group. Then $G/Z_G \cong \mathrm{Inn}(G)$. That means the conjugation action of a central element is trivial. The kernel and cokernel of the conjugation $\gamma : G \to \mathrm{Aut}_{\mathsf{Grp}}(G)$ can be connected by the following exact sequence

$$1 \longrightarrow Z_G \longrightarrow G \xrightarrow{\gamma} \mathrm{Aut}_{\mathsf{Grp}}(G) \longrightarrow \mathrm{Out}(G) \longrightarrow 1.$$

Proof. Take $H = G$ in Theorem 4.4.49 we can get $G/Z_G \cong \mathrm{Inn}(G)$. □

Proposition 4.4.51 Properties of Centralizer

Let G be a group and S be a subset of G. Then

(i) $S \subseteq \mathrm{C}_G(\mathrm{C}_G(S))$.

Proposition 4.4.52 Properties of Center

Let G be a group. Then

(i) $Z_G = \bigcap_{g \in G} C_G(g)$.

(ii) $Z_G \lhd_{\mathrm{char}} G$.

(iii) A group is Abelian if and only if $Z_G = G$.

Proof. (i) According to Corollary 4.4.50 and Proposition 4.4.13 (ii), we have

$$x \in Z_G \iff x \in \ker \gamma \iff x \in \bigcap_{g \in G} \mathrm{C}_G(g).$$

□

Definition 4.4.53 Conjugacy Class

Let G be a group. The orbit of a under conjugacy action is called the **conjugacy class** of a, denoted by

$$\mathrm{Cl}(a) = \{gag^{-1} \mid x \in G\}.$$

Two elements $a, b \in G$ are called **conjugate** if $\mathrm{Cl}(a) = \mathrm{Cl}(b)$.

Proposition 4.4.54 Conjugacy Class of Element of Center is Singleton

Consider a group G under conjugacy action. The G-invariant elements under conjugacy action are elements in the center of G:

$$a \in Z_G \iff \mathrm{Cl}(a) = \{a\} \iff \mathrm{C}_G(a) = \mathrm{Stab}_G(a) = G.$$

Proof. According to Proposition 4.4.13 (i), $\mathrm{Cl}(a) = \{a\} \iff \mathrm{Stab}_G(a) = G$.

$$\begin{aligned} a \in Z_G &\iff \forall g \in G,\ ga = ag \\ &\iff \forall g \in G,\ gag^{-1} = a \\ &\iff \mathrm{C}_G(a) = \{a\} \end{aligned}$$

□

Proposition 4.4.55 Conjugacy Class Equation

Suppose G is a finite group. If the distinct conjugacy classes of G which are not singletons are

$\mathrm{Cl}(x_1), \cdots, \mathrm{Cl}(x_m)$, then we have the **conjugacy class equation**

$$|G| = |Z(G)| + \sum_{j=1}^{m} [G : Z_G(x_j)]$$

Proof. With the orbit decomposition of G under conjugacy action, then by orbit-stabilizer theorem we have

$$|G| = \sum_{Gx \in G\backslash G} |\mathrm{Cl}(x)| = \sum_{Gx \in G\backslash G} [G : \mathrm{Stab}_G(x)] = |Z(G)| + \sum_{j=1}^{m} [G : Z_G(x_j)].$$

□

Proposition 4.4.56

Let G acts transitively on a set S. Choose $s \in S$, and let $H = \mathrm{Stab}_G(s)$. Then we have group isomorphism $\mathrm{N}_G(H)/H \cong \mathrm{Aut}_{G\text{-}\mathsf{Set}}(S)$.

Proof. For any $n \in \mathrm{N}_G(H)$ with image $\bar{n} \in \mathrm{N}_G(H)/H$, since G acts transitively on S, we can define a map

$$\begin{aligned} \phi(\bar{n}) : S &\longrightarrow S \\ g \cdot s &\longmapsto gn^{-1} \cdot s \end{aligned}$$

and check $\phi(\bar{n}) \in \mathrm{Aut}_{G\text{-}\mathsf{Set}}(S)$ by

- $\phi(\bar{n}) \in \mathrm{Aut}_{G\text{-}\mathsf{Set}}(S)$. $\phi(\bar{n})$ is well-defined:

$$\begin{aligned} & \bar{m} = \bar{n} \in \mathrm{N}_G(H)/H \\ \Longrightarrow\ & m^{-1} \in n^{-1}H \\ \Longrightarrow\ & \exists h \in H, m^{-1} = n^{-1}h \\ \Longrightarrow\ & \phi(\bar{m})(s) = gm^{-1} \cdot s = gn^{-1}h \cdot s = gn^{-1} \cdot s = \phi(\bar{n})(s). \end{aligned}$$

- $\phi(\bar{n})$ is a G-set morphism: $\phi(\bar{n})(g \cdot s) = gn^{-1} \cdot s = g \cdot \phi(\bar{n})(s)$
- $\phi(\bar{n})$ is a bijection: $\phi(\bar{n}^{-1})$ is the inverse of $\phi(\bar{n})$.

For any automorphism $\psi \in \mathrm{Aut}_{G\text{-}\mathsf{Set}}(S)$, by transitivity we have $\psi(s) = n^{-1} \cdot s$ for some $n \in G$. For $h \in H$, $hn^{-1} \cdot s = h \cdot \psi(s) = \psi(h \cdot s) = \psi(s) = n^{-1} \cdot s$, hence $nhn^{-1} \in H$ and $n \in \mathrm{N}_G(H)$. This gives a well-defined map

$$\begin{aligned} \eta : \mathrm{Aut}_{G\text{-}\mathsf{Set}}(S) &\longrightarrow \mathrm{N}_G(H)/H \\ \psi &\longmapsto \bar{n} \end{aligned}$$

Clearly $\eta(\phi(\bar{n})) = \bar{n}$. Suppose $\psi \in \mathrm{Aut}_{G\text{-}\mathsf{Set}}(S)$ and $\psi(s) = n^{-1} \cdot s$. Then $\phi(\eta(\psi))(g \cdot s) = gn^{-1} \cdot s = g\psi(s) = \psi(g \cdot s)$, which imples $\phi(\eta(\psi)) = \psi$. Therefore, $\phi : \mathrm{N}_G(H)/H \to \mathrm{Aut}_{G\text{-}\mathsf{Set}}$ is bijective. And it is easy to check that this ϕ is an isomorphism of groups,

$$\phi(\bar{n}\bar{m})(g \cdot s) = \phi(\overline{nm})(g \cdot s) = g(nm)^{-1} \cdot s = gm^{-1}n^{-1} \cdot s = \phi(\bar{n})(gm^{-1} \cdot s) = \phi(\bar{n}) \circ \phi(\bar{m})(g \cdot s).$$

□

4.5 Symmetric Groups

Definition 4.5.1 Symmetric Group

The **symmetric group** on a set X is the group of all permutations of X, denoted by $S_X = \mathrm{Aut}_{\mathsf{Set}}(X)$. If $X = \{1, 2, \cdots, n\}$, then we denote S_X by S_n.

Definition 4.5.2 k-Cycle

Let $n \geq 2$ and $k \geq 1$ be integers. A **k-cycle** in S_n is a permutation $\sigma \in S_n$ such that there exist a subset of $P_n = \{1, 2, \cdots, n\}$, denoted by $A = \{a_1, a_2, \cdots, a_k\}$, satisfying

(i) $\sigma(a_i) = a_{i+1}$ for $i = 1, 2, \cdots, k-1$,

(ii) $\sigma(a_k) = a_1$,

(iii) $\sigma(x) = x$ for $x \in P_n - A$.

Definition 4.5.3 Cycle Decomposition

Let $n \geq 2$ and $\sigma \in S_n$. A **cycle decomposition** of σ is a product of disjoint cycles $\sigma = \sigma_1\sigma_2\cdots\sigma_r$ such that σ_i is a k_i-cycle for $i = 1, 2, \cdots, r$ and $k_1 + k_2 + \cdots + k_r = n$. $(k_1, k_2, \cdots, k_r)$ is called the **cycle type** of σ. Equivalently, a **cycle decomposition** of σ is the decomposition of P_n into orbits under the action of $\langle\sigma\rangle$.

Theorem 4.5.4 Pólya Enumeration Theorem (Unweighted)

Let X, Y be finite sets, where $X = \{1, 2, \cdots, n\}$ is the set of points to be colored and Y is the set of colors. Suppose a group G acts on X through $\sigma : G \to \mathrm{Aut}_{\mathsf{Set}}(X)$. Then it also acts on Y^X by Example 4.4.4. Define that a coloring configuration of (X, Y, σ) is an orbit in Y^X/G. Then the number of essentially distinct coloring configurations is

$$\left|Y^X/G\right| = \frac{1}{|G|}\sum_{g\in G}|Y|^{c(g)},$$

where $c(g) := |\langle g\rangle\backslash X| = |\langle\sigma_g\rangle\backslash X|$ denotes the number of cycles in the cycle decomposition of $\sigma_g \in S_n$.

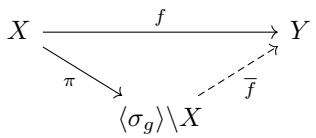
Proof. We apply Burnside's lemma 4.4.28, which states that

$$\left|Y^X/G\right| = \frac{1}{|G|}\sum_{g\in G}\left|\left(Y^X\right)^g\right|$$

where

$$\begin{aligned}\left(Y^X\right)^g &= \left\{f \in Y^X \mid f(g\cdot x) = f(x) \text{ for all } x \in X\right\}\\ &= \left\{f \in Y^X \mid \langle g\rangle x = \langle g\rangle y \implies f(x) = f(y)\right\}.\end{aligned}$$

Define an equivalence relation $\sim_g$ on X by $x \sim_g y \iff \langle g\rangle x = \langle g\rangle y$. Then we have $X/\sim_g = \langle g\rangle\backslash X$. By the universal property of the quotient set, for any map $f : X \to Y$ satisfying $x \sim y \implies f(x) = f(y)$, there exists a unique map $\overline{f} : \langle\sigma_g\rangle\backslash X \to Y$ such that the following diagram commutes



And we have a natural bijection between $\left(Y^X\right)^g$ and $Y^{\langle g\rangle\backslash X}$, which implies that $\left|\left(Y^X\right)^g\right| = |Y|^{c(g)}$. □

Definition 4.5.5 Cycle Index Polynomial

Let G be a subgroup of S_n. The **cycle index polynomial** of G is defined as

$$Z(t_1, t_2, \cdots, t_n; G) = \frac{1}{|G|}\sum_{g\in G} t_1^{c_1(g)}t_2^{c_2(g)}\cdots t_n^{c_n(g)},$$

where $c_k(g)$ denotes the number of k-cycles in the cycle decomposition of σ_g. $|G|Z(t_1, t_2, \cdots, t_n; G)$ can be seen as a generating function, where the coefficient of $t_1^{c_1}t_2^{c_2}\cdots t_n^{c_n}$ represents the number of permutations in G with excatly c_k k-cycles for $k = 1, 2, \cdots, n$.

Theorem 4.5.6 Pólya Enumeration Theorem (Weighted)

Let X, Y be finite sets, where $X = \{1, 2, \cdots, n\}$ is the set of points to be colored and Y is the set of colors. Suppose $w : Y \to \mathbb{Z}_{\geq 0}^m$ is a weight function which assigns a weight $w(y) = (w_1(y), w_2(y), \cdots, w_m(y))$ to each color $y \in Y$. Consider the genrating function

$$q(x_1, \cdots, x_m) = \sum_{y \in Y} x_1^{w_1(y)} x_2^{w_2(y)} \cdots x_m^{w_m(y)},$$

where the coefficient of the term $x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}$ is the number of colors with weight $(a_1, a_2, \cdots, a_m)$. For each coloring map $f : X \to Y$, define the its weight as $W(f)$, where

$$\begin{aligned} W : Y^X &\longrightarrow \mathbb{Z}_{\geq 0}^m \\ f &\longmapsto \sum_{x \in X} w(f(x)) \end{aligned}$$

Let G be a subgroup of S_n. Given any $g \in G$ and $f \in X^Y$, we can check the action of g on f does not change its weight

$$W(f \star g) = \sum_{x \in X} w((f \star g)(x)) = \sum_{x \in X} w(f(g \cdot x)) = \sum_{x \in X} w(f(x)) = W(f),$$

which implies that for each $\omega = (\omega_1, \cdots, \omega_m) \in \mathbb{Z}_{\geq 0}^m$, the fiber $W^{-1}(\omega)$ is G-invariant.
Define a coloring configuration of (X, Y, G) as an orbit in Y^X/G. The generating function for the number of essentially distinct coloring configurations with weight ω can be expressed as

$$\begin{aligned} \operatorname{CGF}(x_1, \cdots, x_m) &= \sum_{\omega \in \mathbb{Z}_{\geq 0}^m} \left| G \backslash W^{-1}(\omega) \right| x_1^{\omega_1} \cdots x_m^{\omega_m} \\ &= Z\left(q(x_1, \cdots, x_m), q\left(x_1^2, \cdots, x_m^2\right), \cdots, q\left(x_1^n, \cdots, x_m^n\right); G\right). \end{aligned}$$

Proof. For any $\omega = (\omega_1, \cdots, \omega_m) \in \mathbb{Z}_{\geq 0}^m$, by applying Burnside's lemma 4.4.28 to the G-set $W^{-1}(\omega)$, we have

$$\left| G \backslash W^{-1}(\omega) \right| = \frac{1}{|G|} \sum_{g \in G} \left| W^{-1}(\omega)^g \right|.$$

Similar to Theorem 4.5.4, we have a bijection between

$$W^{-1}(\omega)^g = \left\{ f \in \left(Y^X\right)^g \mid W(f) = \omega \right\} \quad \text{and} \quad \left\{ \overline{f} \in Y^{\langle g \rangle \backslash X} \mid W\left(\overline{f} \circ \pi\right) = \omega \right\},$$

Suppose $\langle g \rangle \backslash X = \{\langle g \rangle x_1, \cdots, \langle g \rangle x_r\}$. We can give a coloring configuration by r consecutive steps. In the i-th step, we just need to choose a color in $y \in Y$ for the i-orbit $\langle g \rangle \backslash x_i$, which will contribute a term

$$x_1^{|\langle g \rangle x_i| w_1(y)} x_2^{|\langle g \rangle x_i| w_2(y)} \cdots x_m^{|\langle g \rangle x_i| w_m(y)}.$$

Thus we have

$$\begin{aligned} \sum_{\omega \in \mathbb{Z}_{\geq 0}^m} \left| W^{-1}(\omega)^g \right| x_1^{\omega_1} \cdots x_m^{\omega_m} &= \prod_{\langle g \rangle x_i \in \langle g \rangle \backslash X} \left(\sum_{y \in Y} x_1^{|\langle g \rangle x_i| w_1(y)} x_2^{|\langle g \rangle x_i| w_2(y)} \cdots x_m^{|\langle g \rangle x_i| w_m(y)} \right) \\ &= \prod_{\langle g \rangle x_i \in \langle g \rangle \backslash X} q\left(x_1^{|\langle g \rangle x_i|}, x_2^{|\langle g \rangle x_i|}, \cdots, x_m^{|\langle g \rangle x_i|} \right) \\ &= q(x_1, \cdots, x_m)^{c_1(g)} q\left(x_1^2, \cdots, x_m^2\right)^{c_2(g)} \cdots q\left(x_1^n, \cdots, x_m^n\right)^{c_n(g)}. \end{aligned}$$

where

$$c_k(g) = \sum_{\langle g \rangle x_i \in \langle g \rangle \backslash X} \mathbf{1}_{|\langle g \rangle x_i| = k}$$

denotes the number of orbits with size k. With this equality, we can rewrite the generating function as

$$\begin{aligned}
\operatorname{CGF}(x_1, \cdots, x_m) &= \sum_{\omega \in \mathbb{Z}_{\geq 0}^m} \left|G \backslash W^{-1}(\omega)\right| x_1^{\omega_1} \cdots x_m^{\omega_m} \\
&= \sum_{\omega \in \mathbb{Z}_{\geq 0}^m} \frac{1}{|G|} \sum_{g \in G} \left|W^{-1}(\omega)^g\right| x_1^{\omega_1} \cdots x_m^{\omega_m} \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{\omega \in \mathbb{Z}_{\geq 0}^m} \left|W^{-1}(\omega)^g\right| x_1^{\omega_1} \cdots x_m^{\omega_m} \\
&= \frac{1}{|G|} \sum_{g \in G} q(x_1, \cdots, x_m)^{c_1(g)} q\left(x_1^2, \cdots, x_m^2\right)^{c_2(g)} \cdots q\left(x_1^n, \cdots, x_m^n\right)^{c_n(g)} \\
&= Z\left(q(x_1, \cdots, x_m), q\left(x_1^2, \cdots, x_m^2\right), \cdots, q\left(x_1^n, \cdots, x_m^n\right); G\right).
\end{aligned}$$

□

Example 4.5.1 Counting the Isomers of Chlorobenzene

Replacing the H in a benzene ring with Cl, one can consider coloring the 6 vertices of the benzene ring with two colors: H and Cl. The group action is D_{12}, which includes 6 rotations: 0°, 60°, ..., 300°, and 6 reflections: 3 along the opposing sides and 3 along the opposing diagonals.
Compute the cycle decomposition for each g:

- Identity: 6 1-cycles, corresponding to t_1^6.
- Rotation by 1 or 5 times 60°: 1 6-cycle, corresponding to t_6^1.
- Rotation by 2 or 4 times 60°: 2 3-cycles, corresponding to t_3^2.
- Rotation by 3 times 60°: 3 2-cycles, corresponding to t_2^3.
- 3 kinds of opposing side reflections: 3 2-cycles, corresponding to t_2^3.
- 3 kinds of opposing diagonal reflections: 2 1-cycles and 2 2-cycles, corresponding to $t_1^2 t_2^2$.

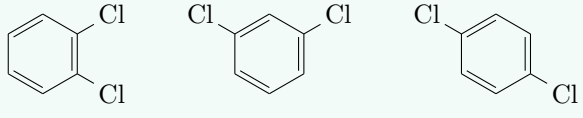
Writing out $Z(t_1, \cdots, t_6; D_{12})$:

$$Z(t_1, \cdots, t_6; D_{12}) = \frac{1}{12}\left(t_1^6 + 3t_1^2 t_2^2 + 4t_2^3 + 2t_3^2 + 2t_6\right)$$

Assigning a weight of (1,0) to H and a weight of (0,1) to Cl, the corresponding generating function is $q(\mathrm{H}, \mathrm{Cl}) = \mathrm{H} + \mathrm{Cl}$. Finally, the generating function for the number of essentially distinct coloring configurations is:

$$\begin{aligned}
&\operatorname{CGF}(\mathrm{H}, \mathrm{Cl}) \\
&= \frac{1}{12}\left((\mathrm{H}+\mathrm{Cl})^6 + 3(\mathrm{H}+\mathrm{Cl})^2\left(\mathrm{H}^2+\mathrm{Cl}^2\right)^2 + 4\left(\mathrm{H}^2+\mathrm{Cl}^2\right)^3 + 2\left(\mathrm{H}^3+\mathrm{Cl}^3\right)^2 + 2\left(\mathrm{H}^6+\mathrm{Cl}^6\right)\right) \\
&= \mathrm{H}^6 + \mathrm{H}^5\mathrm{Cl} + 3\mathrm{H}^4\mathrm{Cl}^2 + 3\mathrm{H}^3\mathrm{Cl}^3 + 3\mathrm{H}^2\mathrm{Cl}^4 + \mathrm{HCl}^5 + \mathrm{Cl}^6
\end{aligned}$$

The coefficients give the number of isomers for various chlorobenzene compounds. For instance, looking at the term $3\mathrm{H}^4\mathrm{Cl}^2$, with a weight of $(4, 2)$, it can only be achieved using 4 H atoms and 2 Cl atoms. The coefficient 3 indicates that there are 3 isomers for dichlorobenzene. The 3 isomers are 1,2-dichlorobenzene, 1,3-dichlorobenzene, and 1,4-dichlorobenzene, plotted as follows:



4.6 Abelian Group

Definition 4.6.1 Abelian Group

An **abelian group** is a group G such that G is commutative. That is, for all $a, b \in G$, $ab = ba$.

An Abelian group is a $\mathbb{Z}$-module and we have category isomorphism $\mathsf{Ab} \cong \mathbb{Z}\text{-}\mathsf{Mod}$.

Example 4.6.1 Forgetful Functor $U_{\mathsf{Grp}} : \mathsf{Ab} \to \mathsf{Grp}$

The forgetful functor $U_{\mathsf{Grp}} : \mathsf{Ab} \to \mathsf{Grp}$ is a functor that sends an abelian group to its underlying group. It is a fully faithful functor.

Example 4.6.2 Forgetful Functor $U : \mathsf{Ab} \to \mathsf{Set}$

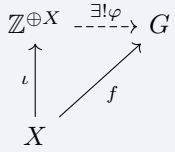
The forgetful functor $U : \mathsf{Ab} \to \mathsf{Set}$ forgets the group structure and sends an abelian group to its underlying set.

(i) U is representable by $(\mathbb{Z}, 1_{\mathbb{Z}})$.

(ii) U is full but not faithful.

Definition 4.6.2 Free Abelian Group

A **free abelian group** generated by a set X is an abelian group denoted by $\mathbb{Z}^{\oplus X}$ which satisfies the following universal property: for any group G and any funtion $f : X \to G$, there exists a unique group homomorphism $\varphi : \mathbb{Z}^{\oplus X} \to G$ such that the following diagram commutes



where $\iota : X \to \mathbb{Z}^{\oplus X}$ is the canonical injection.

Chapter 5

Ring

5.1 Basic Concepts

Definition 5.1.1 Ring

A **ring** is a set R together with two binary operations $+$ and $\cdot$ on R such that

(i) $(R, +)$ is an abelian group.

(ii) $(R, \cdot)$ is a monoid.

(iii) $\cdot$ is distributive over $+$,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

A ring is a monoid object in the category Ab. In other words, a ring is an Ab-enriched category with only one object.
A ring R is an R-module over itself.
A ring R is a $Z(R)$-algebra and also a $\mathbb{Z}$-algebra. In fact, we have the following category isomorphism

$$\mathsf{Ring} \cong \mathbb{Z}\text{-}\mathsf{Alg}.$$

Definition 5.1.2 Unit Group of a Ring

Let R be a ring. The **unit group** of R is the group of invertible elements of R under multiplication, denoted by $R^\times$. We can define a functor $(-)^\times : \mathsf{Ring} \to \mathsf{Grp}$ that sends a ring to its unit group

$$\begin{array}{ccc} \mathsf{Ring} & & \mathsf{Grp} \\ R & \overset{(-)^\times}{\rightsquigarrow} & R^\times \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f|_{R^\times}} \\ S & & S^\times \end{array}$$

Proposition 5.1.3 Adjunction $\mathbb{Z}[-] \dashv (-)^\times$

$(-)^\times : \mathsf{Ring} \to \mathsf{Grp}$ has a left adjoint which sends each group G to the group ring $\mathbb{Z}[G]$.

Next we define the morphisms in the category Ring.

Definition 5.1.4 Ring Homomorphism

Let R, S be rings. A **ring homomorphism** from R to S is a map $f : R \to S$ such that

(i) $f(a + b) = f(a) + f(b)$ for all $a, b \in R$.

(ii) $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in R$.

(iii) $f(1_R) = 1_S$.

Definition 5.1.5 Zero Divisor

Assume that a is an element of a ring R.

- a is called a **left zero divisor** if there exists a nonzero x in R such that $ax = 0$.
- a is called a **right zero divisor** if there exists a nonzero x in R such that $xa = 0$.
- a is called a **zero divisor** if there exists a nonzero x in R such that $ax = xa = 0$.
- a is called a **regular element** if it is neither a left zero divisor nor a right zero divisor.

0 is never a regular element.

Proposition 5.1.6 Set of Regular Elements is a Multiplicative Set

The set of regular elements in a ring R is a multiplicative set.

Proof. Let a, b be regular elements in R. We are to show that ab is also a regular element. Suppose that there exists a nonzero $x \in R$ such that $(ab)x = 0$. Then $a(bx) = 0$. Since a is a regular element, we have $bx = 0$. Since b is also a regular element, we have $x = 0$. This is a contradiction.

Similarly, if there exists a nonzero $y \in R$ such that $y(ab) = 0$, then we can deduce that $(ya)b = 0$. Since b is a regular element, we have $ya = 0$. Since a is also a regular element, we have $y = 0$. This is also a contradiction. Therefore, ab is a regular element. □

Definition 5.1.7 Domain

A nonzero ring R is called a **domain** if one of the following equivalent conditions holds:

(i) 0 is the only left zero divisor in R.

(ii) 0 is the only right zero divisor in R.

Definition 5.1.8 Ideal

Let R be a ring and $I \subseteq R$ be an additive subgroup.

- **Left ideal**: If for every $r \in R$, $rI \subseteq I$, then I is called a left ideal of R.
- **Right ideal**: If for every $r \in R$, $Ir \subseteq I$, then I is called a right ideal of R.
- **Two-sided ideal**: If I is both a left and a right ideal, then it is called a two-sided ideal.

A left, right, or two-sided ideal I that satisfies $I \neq R$ is called a **proper ideal**. In commutative rings, left and right ideals are the same and are simply called ideals.

Sometimes we just say ideal to mean two-sided ideal.

Proposition 5.1.9 Equivalent Characterizations of Ideals

Let R be a ring. Then

(i) Submodules of the left R-module R are precisely the left ideals of R.

(ii) Submodules of the right R-module R are precisely the right ideals of R.

(iii) Sub-bimodules of the R-R bimodule R are precisely the two-sided ideals of R.

Especially, if R is commutative, then the ideals of R are precisely the submodules of the R-module R.

Definition 5.1.10 Kernel of a Ring Homomorphism

Let $f : R \to S$ be a ring homomorphism. The **kernel** of f is the set

$$\ker f = f^{-1}(0_S) = \{r \in R \mid f(r) = 0_S\}.$$

Proposition 5.1.11 Kernel of a Ring Homomorphism is an Ideal

Let $f : R \to S$ be a ring homomorphism. Then $\ker f$ is a two-sided ideal of R. If S is not a zero ring, then $\ker f$ is a proper ideal of R.

Proof. Let $a, b \in \ker f$ and $r \in R$. Then $f(a) = f(b) = 0_S$. Hence $f(a + b) = f(a) + f(b) = 0_S$, $f(ra) = f(r)f(a) = 0_S$ and $f(ar) = f(a)f(r) = 0_S$. Therefore, $a + b, ra, , ar \in \ker f$.
If S is not a zero ring, then $1_S \neq 0_S$. Hence $f(1_R) = 1_S \neq 0_S$, which implies $1_R \notin \ker f$. Therefore, $\ker f$ is a proper ideal of R. □

Proposition 5.1.12 Surjective Ring Homomorphisms Map Ideals to Ideals

A ring homomorphism $f : R \to S$ is surjective if and only if maps two-sided ideals to two-sided ideals.

Proof. First, assume that f is surjective. Let I be any two-sided ideal of R. Since f is a homomorphism between addition group $(R, +)$ and $(S, +)$, $(f(I), +)$ is a subgroup of $(S, +)$. Now take any element $y \in f(I)$ and any $s \in S$, we are to show $sy \in f(I)$ and $ys \in I$. Since f is surjective, there exists an $r \in R$ such that $s = f(r)$. Also, since $y \in f(I)$, there exists an $x \in I$ with $y = f(x)$. Then

$$sy = f(r)f(x) = f(rx).$$

Because I is a two-sided ideal in R, we have $rx \in I$, hence $f(rx) \in f(I)$. Similarly,

$$ys = f(x)f(r) = f(xr) \in f(I).$$

Thus, $f(I)$ is a two-sided ideal of S.

Conversely, suppose that for every two-sided ideal I of R, the set $f(I)$ is a two-sided ideal in S. In particular, consider the two-sided ideal $I = R$. Then $f(R)$ is a two-sided ideal of S. Note that $1_S \in f(R)$. We have $f(R) = S$, so f is surjective.

□

Definition 5.1.13 Reduced Ring

A ring R is called **reduced** if it has no nonzero nilpotent elements, or equivalently, if for any $x \in R$, $x^2 = 0 \implies x = 0$.

Proposition 5.1.14 Examples of Reduced Ring

(i) Subrings, products, and localizations of reduced commutative rings are again reduced rings.

(ii) Every integral domain is reduced.

(iii) $\mathbb{Z}/n\mathbb{Z}$ is reduced if and only if $n = 0$ or n is square-free.

Proof. (i) Let R be a reduced ring and S be a multiplicative subset of R. For any $\frac{f}{s} \in S^{-1}R$, if $\left(\frac{f}{s}\right)^n = \frac{f^n}{s^n} = 0$, then there exists $t \in S$ such that $tf^n = 0$, which implies $(tf)^n = 0$. Since R is reduced, we have $tf = 0$, which means $\frac{f}{s} = 0$. Hence $S^{-1}R$ is reduced.

□

Definition 5.1.15 Local Ring

A ring R is called **local** if it has a unique maximal ideal.

Definition 5.1.16 Local Ring Homomorphism

Let $f : R \to S$ be a ring homomorphism and $\mathfrak{m}_R$ and $\mathfrak{m}_S$ be the unique maximal ideals of R and S respectively. Then f is called a **local ring homomorphism** if $f(\mathfrak{m}_R) \subseteq \mathfrak{m}_S$ or equivalently $f^{-1}(\mathfrak{m}_S) = \mathfrak{m}_R$.

5.2 Construction

5.2.1 Initial Object and Terminal Object

Proposition 5.2.1 Initial Object in Ring

The ring $\mathbb{Z}$ is an initial object in Ring. That is, for any ring R, there exists a unique ring homomorphism

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow R \\ n &\longmapsto n \cdot 1_R \end{aligned}$$

Proof. If $\psi : \mathbb{Z} \to R$ is a ring homomorphism, then $\psi(1) = 1_R$ implies

$$\psi(n) = \psi(1 + \cdots + 1) = \psi(1) + \cdots + \psi(1) = n \cdot 1_R.$$

Therefore, $\psi = \varphi$. □

Definition 5.2.2 Characteristic of a Ring

Let R be a ring and $\varphi : \mathbb{Z} \to R$ be the unique ring homomorphism. Then $\ker \varphi = n\mathbb{Z}$ and $\mathrm{im}\varphi = \mathbb{Z}/n\mathbb{Z}$, where $n \in \mathbb{Z}_{\geq 0}$. The **characteristic** of R is defined to be n, denoted by $\mathrm{char}(R)$.
Equivalently, $\mathrm{char}(R)$ is the smallest positive integer n such that $n \cdot 1_R = 0_R$ if such an integer exists. Otherwise, the characteristic of R is 0.

Proposition 5.2.3 Terminal Object in Ring

The ring $\mathbb{Z}$ is an initial object in $\{0\}$.

Since the forgetful functor Ring $\to$ Set is a right adjoint, it preserves all limits. Hence the underlying set of the terminal object in Ring is the terminal object in Set, which is the singleton set $\{*\}$.

5.2.2 Quotient Object

Definition 5.2.4 Quotient Ring

Let R be a ring and I be a two-sided ideal of R. Equip the additive group R/I with the following multiplication operation:

$$(r + I) \cdot (s + I) := (rs + I), \quad r, s \in R.$$

Then R/I forms a ring, which is called the **quotient ring of R modulo I**. The quotient map $R \to R/I$ is called the quotient homomorphism.

Proposition 5.2.5 Universal Property of Quotient Rings

Let R be a ring and I be a two-sided ideal of R. Then the quotient map $\pi : R \to R/I$ is a surjective ring homomorphism with kernel I. Moreover, for any ring S and any ring homomorphism $f : R \to S$ such that $I \subseteq \ker f$, or equivalently $f(I) = \{0\}$, there exists a unique ring homomorphism $\bar{f} : R/I \to S$ such that the following diagram commutes

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ {\scriptstyle\pi}\downarrow & \nearrow_{\exists!\bar{f}} & \\ R/I & & \end{array}$$

Moreover, $\bar{f}$ is injective if and only if $\ker f = I$. $\bar{f}$ is surjective if and only if f is surjective.

Proposition 5.2.6 Kernel of a Ring Homomorphism is a Two-sided Ideal
Let $f : R \to S$ be a ring homomorphism. Then $\ker f$ is an two-sided ideal of R.

Proposition 5.2.7 Image of a Ring Homomorphism is a Subring
Let $f : R \to S$ be a ring homomorphism. Then $\mathrm{im} f$ is a subring of S.

Theorem 5.2.8 The Fundamental Theorem of Ring Homomorphisms
Let $f : R \to S$ be a ring homomorphism. Then $R/\ker f \cong \mathrm{im} f$.

Proposition 5.2.9
Let $f : R \to S$ be a ring homomorphism. Then we have the following map

$$\begin{aligned} \{\text{two-sided ideals of } S\} &\longrightarrow \{\text{two-sided ideals of } R \text{ containing } \ker f\} \\ I_2 &\longmapsto f^{-1}(I_2) \end{aligned}$$

Furthermore, if f is surjective, then we obtain a bijection

$$\begin{aligned} \{\text{two-sided ideals of } S\} &\xrightarrow{\sim} \{\text{two-sided ideals of } R \text{ containing } \ker f\} \\ I_2 &\longmapsto f^{-1}(I_2) \\ f(I_1) &\longmapsfrom I_1 \end{aligned}$$

Corollary 5.2.10
Let R be a ring and I be a two-sided ideal of R. Then we have the following bijection

$$\begin{aligned} \{\text{two-sided ideals of } R/I\} &\xrightarrow{\sim} \{\text{two-sided ideals of } R \text{ containing } I\} \\ J/I := \{j + I \mid j \in J\} &\longmapsfrom J \end{aligned}$$

Example 5.2.1
Let R be a commutative ring and $a_1, \cdots, a_n \in R$ be elements in R. Then

$$(a_1, \cdots, a_n)/(a_1) = (a_2 + (a_1), \cdots, a_n + (a_1))$$

is a ideal of $R/(a_1)$.

Proof. For any $x = r_1a_1 + \cdots + r_na_n + (a_1) \in (a_1, \cdots, a_n)/(a_1)$, we have

$$x = r_1a_1 + \cdots + r_na_n + (a_1) = r_2(a_2 + (a_1)) + \cdots + r_n(a_n + (a_1)) \in (a_2 + (a_1), \cdots, a_n + (a_1)).$$

This implies $(a_1, \cdots, a_n)/(a_1) \subseteq (a_2 + (a_1), \cdots, a_n + (a_1))$.
Conversely, for any $y = r_2(a_2 + (a_1)) + \cdots + r_n(a_n + (a_1)) \in (a_2 + (a_1), \cdots, a_n + (a_1))$, we have

$$y = r_2a_2 + \cdots + r_na_n + (a_1) \in (a_1, \cdots, a_n)/(a_1).$$

This implies $(a_2 + (a_1), \cdots, a_n + (a_1)) \subseteq (a_1, \cdots, a_n)/(a_1)$. Therefore, we prove the equality. □

Theorem 5.2.11 Third Isomorphism Theorem
Let R be a ring and I and J be two-sided ideals of R such that $I \subseteq J$. Then J/I is a two-sided ideal of R/I and we have the following isomorphism

$$\frac{R/I}{J/I} \cong R/J.$$

5.2.3 Free Object

Definition 5.2.12 Free Ring

Let S be a set. The **free ring** on S, denoted by $\mathrm{Free}_{\mathsf{Ring}}(S)$, together with a function $\iota : S \to \mathrm{Free}_{\mathsf{Ring}}(S)$, is defined by the following universal property: for any ring R and any function $f : S \to R$, there exists a unique ring homomorphism $\widetilde{f} : \mathrm{Free}_{\mathsf{Ring}}(S) \to R$ such that the following diagram commutes

$$\begin{array}{ccc} \mathrm{Free}_{\mathsf{Ring}}(S) & \xrightarrow{\exists!\, \widetilde{f}} & R \\ {\scriptstyle \iota}\uparrow & \nearrow_{f} & \\ S & & \end{array}$$

The free ring $\mathrm{Free}_{\mathsf{Ring}}(S)$ can be contructed as the free $\mathbb{Z}$-algebra on $\mathrm{Free}_{\mathsf{Mon}}(S)$

$$\mathrm{Free}_{\mathsf{Ring}}(S) \cong \bigoplus_{w \in \mathrm{Free}_{\mathsf{Mon}}(S)} \mathbb{Z} w.$$

Example 5.2.2 Forgetful Functor $U : \mathsf{Ring} \to \mathsf{Set}$

The forgetful functor $U : \mathsf{Ring} \to \mathsf{Set}$ forgets the ring structure and retains only the underlying set.

(i) U is representable by $(\mathbb{Z}[x], x)$.

(ii) U is faithful but not full.

Proposition 5.2.13 Free-Forgetful Adjunction $\mathrm{Free}_{\mathsf{Ring}} \dashv U$

The free ring functor $\mathrm{Free}_{\mathsf{Ring}}$ is left adjoint to the forgetful functor $U : \mathsf{Ring} \to \mathsf{Set}$.

5.2.4 Graded Object

Definition 5.2.14 I-Graded Ring (Internal Definition)

Let $(I, +)$ be a monoid. An **I-graded ring** is a ring $(R, +, \cdot)$ together with a family of subgroups $(R_i)_{i \in I}$ of $(R, +)$ such that

(i) $R = \bigoplus_{i \in I} R_i$.

(ii) $R_i R_j \subseteq R_{i+j}$ for all $i, j \in I$.

Elements in $R_i - \{0\}$ are called **homogeneous elements of degree** i.

Definition 5.2.15 Graded Ideal

Let R be an I-graded ring with grading $(R_i)_{i \in I}$. An ideal J of R is called **graded** if

$$J = \bigoplus_{i \in I} J \cap R_i.$$

Proposition 5.2.16 Homogeneous Elements Generate Graded Ideal

Let R be a I-graded ring with grading $(R_i)_{i \in I}$ and $\mathfrak{a}$ be a two-sided ideal of R. Then $\mathfrak{a}$ is a graded ideal if and only if $\mathfrak{a}$ is generated by homogeneous elements. That is,

$$\mathfrak{a} \text{ is a graded ideal} \iff \mathfrak{a} = \left\langle \bigcup_{i \in I} H_i \right\rangle, \quad H_i \subseteq R_i.$$

Proof. If $\mathfrak{a}$ is a graded ideal, then

$$\mathfrak{a} = \bigoplus_{i\in I} \mathfrak{a} \cap R_i = \left\langle \bigcup_{i\in I} (\mathfrak{a} \cap R_i) \right\rangle,$$

which means $\mathfrak{a}$ is generated by homogeneous elements.

Assume $\mathfrak{a}$ is generated by homogeneous elements, say $\mathfrak{a} = \left\langle \bigcup_{i\in I} H_i \right\rangle$, where $H_i \subseteq R_i$. Let $H = \bigcup_{i\in I} H_i$. Then for any $a \in \mathfrak{a}$, it can be written as

$$a = \sum_{k=1}^{n} r_k h_k s_k.$$

where $r_k, s_k \in R$, $h_k \in H$. Assume that r_k, s_k have the following decomposition

$$r_k = \sum_{i\in I} r_{k,i}, \quad r_{k,i} \in R_i,$$
$$s_k = \sum_{j\in I} s_{k,j}, \quad s_{k,j} \in R_j,$$

Then we have

$$a = \sum_{k=1}^{n} \left(\sum_{i\in I} r_{k,i} \right) h_k \left(\sum_{j\in I} s_{k,j} \right) = \sum_{k=1}^{n} \sum_{i\in I} \sum_{j\in I} r_{k,i} h_k s_{k,j}.$$

Suppose $h_k \in R_m$, then $r_{k,i} h_k s_{k,j} \in R_{i+m+j}$. Also we note $h_k \in \mathfrak{a}$ implies $r_{k,i} h_k s_{k,j} \in \mathfrak{a}$. Hence

$$a = \sum_{k=1}^{n} \sum_{i\in I} \sum_{j\in I} r_{k,i} h_k s_{k,j} \in \sum_{i\in I} \mathfrak{a} \cap R_i = \bigoplus_{i\in I} \mathfrak{a} \cap R_i.$$

It is clear that $\bigoplus_{i\geq 0} (\mathfrak{a} \cap R_i) \subseteq \mathfrak{a}$. Therefore, we show that

$$\mathfrak{a} = \bigoplus_{i\geq 0} (\mathfrak{a} \cap R_i),$$

which means $\mathfrak{a}$ is a graded ideal. □

Proposition 5.2.17 Membership Criterion for Graded Ideals

Let R be a I-graded ring with grading $(R_i)_{i\in I}$ and $\mathfrak{a}$ be a graded ideal of R. Assume $x = \sum_{i\in I} x_i \in R$ with $x_i \in R_i$. Then

$$x \in \mathfrak{a} \iff x_i \in \mathfrak{a} \text{ for all } i \in I.$$

Proof. Suppose $x \in \mathfrak{a}$. Since $\mathfrak{a} = \bigoplus_{i\in I} \mathfrak{a} \cap R_i$, there exists $y_i \in \mathfrak{a} \cap R_i$ such that

$$x = \sum_{i\in I} y_i.$$

Since $R = \bigoplus_{i\in I} R_i$, the decomposition of x is unique. Hence $x_i = y_i \in \mathfrak{a}$ for all $i \in I$. The converse is clear. □

5.3 Category Properties

The category Ring is both complete and cocomplete.

Proposition 5.3.1 Equivalence Chracaterization of Monomorphisms in Ring

Let $f : R \to S$ be a ring homomorphism. Then the following are equivalent:

(i) f is a monomorphism.

(ii) f is injective.

(iii) $\ker f = \{0_R\}$.

Proposition 5.3.2 Sujective Ring Homomorphisms are Epimorphisms

Every surjective homomorphism of rings is an epimorphism. However, the converse is not true in general.

Proposition 5.3.3 Equivalence Chracaterization of Isomorphisms in Ring

Let $f : R \to S$ be a ring homomorphism. Then the following are equivalent:

(i) f is an isomorphism.

(ii) f is bijective.

(iii) $\ker f = \{0_R\}$ and $\mathrm{im} f = S$.

Chapter 6

Commutative Ring

6.1 Basic Concepts

A commutative ring R is a commutative R-algebra and accordingly a commutative $\mathbb{Z}$-algebra. Furthermore we have a categorical isomorphism

$$\mathsf{CRing} \cong \mathbb{Z}\text{-}\mathsf{CAlg}.$$

Definition 6.1.1 Noetherian Commutative Ring

Let R be a commutative ring. We say R is **Noetherian** if one of following conditions holds:

(i) R as an R-module is Noetherian.

(ii) Every ideal of R is finitely generated.

(iii) Every prime ideal of R is finitely generated.

(iv) Every ascending chain of ideals of R is eventually constant. That is, if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is a chain of ideals of R, then there exists $n \in \mathbb{N}$ such that $I_n = I_{n+1} = \cdots$.

Proposition 6.1.2 Properties of Noetherian rings

(i) If R is a Noetherian ring, then the polynomial ring $R[X_1, X_2, \cdots, X_n]$ is also Noetherian.

(ii) If R is a Noetherian ring, then the formal power series ring $R[[X_1, X_2, \cdots, X_n]]$ is also Noetherian.

Definition 6.1.3 Frobenius Endomorphism of a Commutative Ring

Let R be a commutative ring with prime characteristic p. The **Frobenius endomorphism** of R is the ring homomorphism defined by

$$\begin{aligned} \varphi : R &\longrightarrow R \\ r &\longmapsto r^p. \end{aligned}$$

Remark. The Frobenius endomorphism is a ring homomorphism since

$$\begin{aligned} \varphi(r+s) = (r+s)^p = \sum_{k=0}^{p} \binom{p}{k} r^k s^{p-k} = r^p + s^p = \varphi(r) + \varphi(s), \\ \varphi(rs) = (rs)^p = r^p s^p = \varphi(r)\varphi(s). \end{aligned}$$

□

6.1.1 Ideals

Definition 6.1.4 Ideal

Let R be a ring. A subset $I \subseteq R$ is called an **ideal** if

(i) I is a subgroup of $(R, +)$.

(ii) I is closed under multiplication, i.e. $a \in I$ and $b \in R$ implies $ab \in I$.

Proposition 6.1.5 Ideal as Submodule

Let R be a ring and $I \subseteq R$ be a subset of R. Then I is an ideal of R if and only if I is a submodule of R as an R-module.

Definition 6.1.6 Prime Ideal

Let R be a commutative ring. An ideal $I \subseteq R$ is called **prime** if

(i) $I \neq R$, i.e. I is a proper ideal.

(ii) $ab \in I \implies a \in I$ or $b \in I$, i.e. there exist no two elements in R whose product is in I but neither of them is in I.

Proposition 6.1.7

Let R be a commutative ring and $\mathfrak{p}$ be a prime ideal of R. If $x_1 \cdots x_n \in \mathfrak{p}$, then there exists some $i \in \{1, 2 \cdots, n\}$ such that $x_i \in \mathfrak{p}$.

Proof. We prove this by induction on n. The case $n = 1$ is trivial. Suppose the statement holds for $n = k$. If $x_1 \cdots x_{k+1} \in \mathfrak{p}$, then $x_1 \cdots x_k \in \mathfrak{p}$ or $x_{k+1} \in \mathfrak{p}$. If $x_1 \cdots x_k \in \mathfrak{p}$, then there exists some $i \in \{1, 2, \cdots, k\}$ such that $x_i \in \mathfrak{p}$. If $x_{k+1} \in \mathfrak{p}$, then we are done. Hence the statement holds for $n = k + 1$. □

Proposition 6.1.8 Preimage of a Prime Ideal is a Prime Ideal

Let $f : R \to S$ be a commutative ring homomorphism and $\mathfrak{p} \subseteq S$ be a prime ideal. Then $f^{-1}(\mathfrak{p})$ is a prime ideal of R.

Corollary 6.1.9 Contraction of a Prime Ideal is Prime

Let R be a commutative ring and $S \subseteq R$ be a subring. If $\mathfrak{p} \subseteq R$ is a prime ideal, then $\mathfrak{p} \cap S$ is a prime ideal of S.

Proof. Let $\iota : S \hookrightarrow R$ be the inclusion map. Then $\iota^{-1}(\mathfrak{p}) = \mathfrak{p} \cap S$ is a prime ideal of S. □

Proposition 6.1.10 Prime Ideal Equivalent Definition

Let R be a commutative ring and $I \subseteq R$ be an ideal. Then I is prime if and only if R/I is an integral domain.

Definition 6.1.11 Maximal Ideal

Let R be a commutative ring. An ideal $I \subseteq R$ is called **maximal** if

(i) $I \neq R$, i.e. I is a proper ideal.

(ii) There exists no ideal $J \subseteq R$ such that $I \subsetneq J \subsetneq R$.

Proposition 6.1.12 Maximal Ideal Equivalent Definition

Let R be a commutative ring and $I \subseteq R$ be an ideal. Then I is maximal if and only if R/I is a field.

Proposition 6.1.13

If R is a ring and I an ideal of R such that $I \neq R$, then R contains a maximal ideal $\mathfrak{m}$ such that $I \subseteq \mathfrak{m}$.

Proof. Let $\mathcal{A}$ be the set of ideals of R not equal to R, ordered by inclusion. We must show that whenever $\mathcal{C}$ is a chain in $\mathcal{A}$ it has an upper bound in $\mathcal{A}$, since then the result follows immediately from Zorn's lemma. So let's take such a chain $\mathcal{C}$.

Let $I = \bigcup_{J \in \mathcal{C}} J$. Now suppose x_1, x_2 are in I. Then there are J_1, J_2 in $\mathcal{C}$ such that $x_i \in J_i$. Either $J_1 \subseteq J_2$ or $J_2 \subseteq J_1$. Without loss of generality, we assume the former follows. Then $x_1 \in J_2$, so $x_1 + x_2 \in J_2 \subset I$. Also if $a \in R$ then $ax_i \in J_2 \subseteq I$ for each i. It follows that I is an ideal.

It now just remains to check that $I \neq A$. But $1 \notin J$ for each $J \in \mathcal{C}$, so $1 \notin I$ and $I \neq R$ as required. □

Proposition 6.1.14 Non-Unit Elements Lies in Maximal Ideals

Let R be a commutative ring. Then the following are equivalent:

(i) $x \notin R^\times$.

(ii) $(x) \neq R$.

(iii) x lies in a maximal ideal of R.

Proof. (i) $\implies$ (ii). If $(x) \neq R$, then there exists $r \in R$ such that $rx = 1$. Hence $x \in R^\times$.

(ii) $\implies$ (iii). If $(x) \neq R$, by the proposition above, there exists a maximal ideal $\mathfrak{m}$ such that $(x) \subseteq \mathfrak{m}$.

(iii) $\implies$ (i). If $x \in R^\times$, then $(x) = R$ and there exists no maximal ideal containing (x). □

Corollary 6.1.15

Let R be a commutative ring. Then

$$R - R^\times = \bigcup_{\mathfrak{m} \in \mathrm{MaxSpec} R} \mathfrak{m}.$$

Proof. This is a direct consequence of Proposition 6.1.14. □

Definition 6.1.16 Ideal generated from subset

Let R be a commutative ring and $\mathcal{I}(R)$ be the set of all ideals of R. Suppose $S \subseteq R$ be a subset. The **ideal generated by** S, denoted by (S), is the smallest ideal of R containing S, i.e.

$$(S) = \bigcap_{\substack{I \in \mathcal{I}(R) \\ S \subseteq I}} I = \left\{ \sum_{i=1}^{n} r_i s_i \mid n \in \mathbb{Z}_+, r_i \in R, s_i \in S \right\}.$$

If $S = \{a_1, \ldots, a_n\}$, we write

$$(S) = (a_1, \ldots, a_n) = \left\{ \sum_{i=1}^{n} r_i a_i \,\middle|\, r_i \in R \right\}.$$

If $S = \mathfrak{p}$ is a prime ideal, we write

$$(\mathfrak{p}) = \mathfrak{p}R = \left\{ \sum_{i=1}^{n} r_i p \,\middle|\, r_i \in R, p \in \mathfrak{p}, n \in \mathbb{Z}_+ \right\}.$$

Definition 6.1.17 Ideal Operations

(i) Sum:

$$I + J = \{a + b \mid a \in I, b \in J\} = (I \cup J),$$

$$\sum_{t\in T} I_t = \{a_{t_1} + \cdots + a_{t_n} \mid n \in \mathbb{Z}_+, t_i \in T, a_{t_i} \in I_{t_i}\}.$$

(ii) Product:

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i \,\middle|\, n \in \mathbb{Z}_+, a_i \in I, b_i \in J \right\} = (\{ab \mid a \in I, b \in J\}).$$

(iii) Power: $I^0 = R$,

$$I^n = \underbrace{I \cdots I}_{n \text{ times}} = (\{a^n \mid a \in I\}),$$

(iv) Radical:

$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}_+\} = \bigcap_{\substack{\mathfrak{p}\in \operatorname{Spec} R \\ I\subseteq\mathfrak{p}}} \mathfrak{p}$$

.

Proposition 6.1.18 Sum of Generated Ideals

Let R be a commutative ring and S be a subset of R. Then

$$(S) = \sum_{s\in S}(s).$$

As a result,

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_m) = (a_1, \ldots, a_n, b_1, \ldots, b_m).$$

Proof.

$$\begin{aligned}\sum_{s\in S}(s) &= \{a_{s_1} + \cdots + a_{s_n} \mid n \in \mathbb{Z}_+, s_i \in S, a_{s_i} \in (s_i)\} \\ &= \{r_1 s_1 + \cdots + r_n s_n \mid n \in \mathbb{Z}_+, s_i \in S, r_i \in R\} \\ &= (S).\end{aligned}$$

□

Proposition 6.1.19 Product of Generated Ideals

Let R be a commutative ring and S, T be subsets of R. Then

$$(S)(T) = (ST).$$

As a result,

$$(a_1, \ldots, a_n)(b_1, \ldots, b_m) = (a_1 b_1, \ldots, a_1 b_m, \ldots, a_n b_1, \ldots, a_n b_m).$$

Proposition 6.1.20 Properties of Ideal Operations

(i) $(I \cap J)^2 \subseteq IJ \subseteq I \cap J \subseteq I + J$

(ii) $I \cap (J + K) \supseteq I \cap J + I \cap K$

(iii) $I(J + K) = IJ + IK$

(iv)

$$J \sum_{t\in T} I_t = \sum_{t\in T} J I_t.$$

(v) $I(JK) = (IJ)K$

(vi) $(a)^n = (a^n)$

(vii) $I^0 \supseteq \sqrt{I} \supseteq I \supseteq I^2 \supseteq I^3 \supseteq \cdots$

(viii) $\sqrt{\sqrt{I}} = \sqrt{I}$,

(ix) $\sqrt{I^n} = \sqrt{I}$, $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

Proof. (i) Since $\{ab \mid a \in I, b \in J\} \subseteq I \cap J$, we see $IJ = (\{ab \mid a \in I, b \in J\}) \subseteq I \cap J$. Also we can check $I \cap J \subseteq I \cup J \subseteq (I \cup J) = I + J$.

(vi) If $x \in (a)^n$, then $x = r_1(r_2 a)^n = r_1 r_2^n a^n \in (a^n)$. If $y \in (a^n)$, then $y = ra^n \in (a)^n$.

□

Definition 6.1.21 Semiring of Ideals of a Commutative Ring

Let R be a commutative ring. Then the set of all ideals of R forms a semiring under the operations of addition and multiplication. The zero ideal (0) is the additive identity and the unit ideal R is the multiplicative identity.

Proposition 6.1.22 Surjective Ring Homomorphism Induces Semiring Homomorphism of Ideals

If $\varphi : R \to S$ is a surjective ring homomorphism, then φ induces a semiring homomorphism from the semiring of ideals of R to the semiring of ideals of S.

Proof. First, we show φ preserves addition of ideals. Let I, J be ideals of R. Then

$$\begin{aligned}
\varphi(I + J) &= \varphi\left(\{a + b \mid a \in I, b \in J\}\right) \\
&= \{\varphi(a + b) \mid a \in I, b \in J\} \\
&= \{\varphi(a) + \varphi(b) \mid a \in I, b \in J\} \\
&= \{x + y \mid x \in \varphi(I), y \in \varphi(J)\} \\
&= \varphi(I) + \varphi(J).
\end{aligned}$$

Then we show φ preserves multiplication of ideals. Let I, J be ideals of R. We have

$$\begin{aligned}
\varphi(IJ) &= \varphi\left(\left\{\sum_{i=1}^{n} a_i b_i \,\middle|\, n \in \mathbb{Z}_+, a_i \in I, b_i \in J\right\}\right) \\
&= \left\{\varphi\left(\sum_{i=1}^{n} a_i b_i\right) \,\middle|\, n \in \mathbb{Z}_+, a_i \in I, b_i \in J\right\} \\
&= \left\{\sum_{i=1}^{n} \varphi(a_i)\varphi(b_i) \,\middle|\, n \in \mathbb{Z}_+, a_i \in I, b_i \in J\right\} \\
&= \left\{\sum_{i=1}^{n} x_i y_i \,\middle|\, n \in \mathbb{Z}_+, x_i \in \varphi(I), y_i \in \varphi(J)\right\} \\
&= \varphi(I)\varphi(J).
\end{aligned}$$

Finally, we show φ preserves the multiplicative identity. This follows immediately from the fact that φ is surjective.

□

Proposition 6.1.23

Let I and J be ideals of a commutative ring R and $\mathfrak{p}$ be a prime ideal of R. Then

$$I \cap J \subseteq \mathfrak{p} \iff IJ \subseteq \mathfrak{p} \iff I \subseteq \mathfrak{p} \text{ or } J \subseteq \mathfrak{p}.$$

Proof. We have the following chain of implications:

- $I \cap J \subseteq \mathfrak{p} \implies IJ \subseteq \mathfrak{p}$. Note that $IJ \subseteq I \cap J$. The result follows immediately.

- $IJ \subseteq \mathfrak{p} \implies I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$. Assume $IJ \subseteq \mathfrak{p}$. Suppose $I \subsetneq \mathfrak{p}$ and $J \subsetneq \mathfrak{p}$. Then there exist $a \in I - \mathfrak{p}$ and $b \in J - \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $ab \in IJ \subseteq \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, which is a contradiction. Hence $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$.
- $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p} \implies I \cap J \subseteq \mathfrak{p}$. Note that $I \cap J \subseteq I$. The result follows immediately.

□

Definition 6.1.24 Radical Ideal

An ideal I is called a **radical ideal** if $I = \sqrt{I}$.

Proposition 6.1.25 Radical Ideal Equivalent Definition

Let R be a commutative ring and $I \subseteq R$ be an ideal. Then I is radical if and only if R/I is reduced.

Definition 6.1.26 Nilradical

The **nilradical** of R, denoted by $\mathfrak{N}_R$, is the radical ideal $\sqrt{0}$ consisting of all the nilpotent elements of R. We have

$$\mathfrak{N}_R = \sqrt{0} = \{r \in R \mid r^n = 0 \text{ for some } n \in \mathbb{Z}_+\} = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$$

Proposition 6.1.27 Properties of Radical Ideal

(i) For any ideal I, $\sqrt{0} \subseteq \sqrt{I}$.

(ii) $\sqrt{I}$ is the smallest radical ideal containing I.

(iii) $\sqrt{\mathfrak{p}^n} = \sqrt{\mathfrak{p}} = \mathfrak{p}$ for any prime ideal $\mathfrak{p}$, which means prime ideals are radical.

(iv) Suppose the natural projection $\pi : R \to R/I$ induces a bijection between the set of ideals of R containing I and the set of ideals of R/I, denoted by $\tilde{\pi} : \mathcal{I}(R) \to \mathcal{I}(R/I)$. Then $\tilde{\pi}$ maps $\sqrt{I}$ to $\mathfrak{N}_{R/I}$.

(v) A commutative ring R is reduced if and only if $\mathfrak{N}_R = (0)$.

In summary, we have the following chain of inclusions:

$$\{\text{maximal ideals of } R\} \subseteq \{\text{prime ideals of } R\} \subseteq \{\text{radical ideals of } R\} \subseteq \{\text{ideals of } R\}.$$

Proposition 6.1.28 Quotient Preserves Radical, Prime, Maximal Ideals

Let R be a commutative ring and $I \subseteq R$ be a proper ideal. Then we have bijections between the following sets:

$$\begin{aligned} \{\text{ideals of } R \text{ containing } I\} &\longleftrightarrow \{\text{ideals of } R/I\} \\ J &\longmapsto J/I \end{aligned}$$

The ideal $J \supseteq I$ is radical, prime, or maximal if and only if J/I is radical, prime, or maximal respectively.

Definition 6.1.29 Jacobson Radical

Let R be a commutative ring and $\mathfrak{m}$ be a maximal ideal of $\mathfrak{m}$. The **Jacobson radical** of R, denoted by $\mathfrak{J}_R$, is the intersection of all maximal ideals of R, denoted by

$$\mathfrak{J}_R = \bigcap_{\mathfrak{m} \in \operatorname{MaxSpec} R} \mathfrak{m}.$$

6.1.2 Prime Elements

Definition 6.1.30 Divisibility

Let R be a commutative ring and $a, b \in R$. We say a **divides** b if there exists $c \in R$ such that $b = ac$, denoted by $a \mid b$. If $a \mid b$. a is called a **divisor** of b, and b is called a **multiple** of a.

Proposition 6.1.31

Let R be a commutative ring.

(i) $a \mid b \iff (b) \subseteq (a)$.

(ii) $u \in R^\times \iff (u) = R \iff \forall r \in R,\ u \mid r$.

Definition 6.1.32 Prime Element

Let R be a commutative ring. An element $a \in R$ is called **prime** if

(i) $a \neq 0$.

(ii) $a \notin R^\times$, i.e. a is not a unit.

(iii) $a \mid bc \implies a \mid b$ or $a \mid c$.

Proposition 6.1.33 Prime Element and Nonzero Prime Ideal

Suppose R is a commutative ring and $a \in R$. Then

$$a \text{ is prime} \iff (a) \text{ is a nonzero prime ideal.}$$

Proof.

$$\begin{aligned} a \text{ is prime} &\iff a \neq 0 \text{ and } a \notin R^\times \text{ and } a \mid bc \implies a \mid b \text{ or } a \mid c \\ &\iff (a) \neq 0 \text{ and } (a) \neq R \text{ and } bc \in (a) \implies b \in (a) \text{ or } c \in (a) \\ &\iff (a) \text{ is a nonzero prime ideal.} \end{aligned}$$

□

6.1.3 Local Commutative Ring

Definition 6.1.34 Local Commutative Ring

Let R be a commutative ring. Then the following are equivalent:

(i) R is a local ring.

(ii) R has a unique maximal ideal.

(iii) R has a maximal ideal $\mathfrak{m}$ and $R - \mathfrak{m} = R^\times$.

(iv) R is not the zero ring and for every $x \in R$, $x \in R^\times$ or $1 - x \in R^\times$.

(v) R is not the zero ring and if $\sum_{i=1}^n r_i \in R^\times$, then there exist some i such that $r_i \in R^\times$.

(vi) R is not the zero ring and the sum of any two non-units in R is a non-unit.

Lemma 6.1.35 Nakayama's Lemma

Let R be a commutative ring and M be a finitely generated R-module. If the image of $m_1, \cdots, m_n$ in $M/\mathfrak{J}_R M$ generates $M/\mathfrak{J}_R M$ as an $R/\mathfrak{J}_R$-module, then $m_1, \cdots, m_n$ generates M as an R-module.

Proposition 6.1.36

Let $(R, \mathfrak{m})$ be a local commutative ring and M be a finitely generated R-module. Let

$$\mathfrak{m}M = \left\{ \sum_{i=1}^{n} r_i m_i \;\middle|\; r_i \in \mathfrak{m}, m_i \in M, n \in \mathbb{N} \right\}$$

denote the submodule of M generated by $\mathfrak{m}$-action and $\pi : M \to M/\mathfrak{m}M$ be the natural projection. Then we have

- $M/\mathfrak{m}M$ is an $R/\mathfrak{m}$-vector space.
- If $(v_1, \ldots, v_n)$ is a $R/\mathfrak{m}$-basis for $M/\mathfrak{m}M$, then $(\pi^{-1}(v_1), \ldots, \pi^{-1}(v_n))$ is a minimal generating set for M.
- If $(m_1, \ldots, m_k)$ is a minimal generating set for M, then $(\pi(m_1), \ldots, \pi(m_k))$ is a $R/\mathfrak{m}$-basis for $M/\mathfrak{m}M$.

As a result, the minimal number of generators of M is equal to $\dim_{R/\mathfrak{m}}(M/\mathfrak{m}M)$.

Proof. The action of $R/\mathfrak{m}$ on $M/\mathfrak{m}M$ is defined by

$$\overline{r} \cdot \pi(m) = \pi(rm).$$

This is well-defined since if $\overline{r_1} = \overline{r_2}$, then $r_1 - r_2 = s \in \mathfrak{m}$. For any $m \in M$, we have

$$r_1 m - r_2 m = sm \in \mathfrak{m}M \implies \pi(r_1 m) = \pi(r_2 m).$$

Suppose $(v_1, \ldots, v_n)$ is a $R/\mathfrak{m}$-basis for $M/\mathfrak{m}M$. The rest of the proof is a direct application of Nakayama's lemma. □

6.2 Integral Domain

Definition 6.2.1 Integral Domain

A commutative ring R is called an **integral domain** if

(i) the only zero divisor of R is 0,

(ii) R is not the zero ring.

Remark. Or equivalently, we can define an integral domain as a commutative domain. □

Proposition 6.2.2 Cancellation Laws in Integral Domain

Let R be an integral domain. Then the following cancellation laws hold: given any $a, b, c \in R$, if $a \neq 0$, then $ab = ac$ implies $b = c$.

Proposition 6.2.3 Nonzero Subring of Integral Domain is Integral Domain

Let R be an integral domain and $S \subseteq R$ be a nonzero subring. Then S is an integral domain.

Proof. Let $a, b \in S$ be nonzero elements. Since $a, b \in R$, we have $ab = 0 \implies a = 0$ or $b = 0$. Hence S is an integral domain. □

Definition 6.2.4 Associate

Let R be an integral domain. Two elements $a, b \in R$ are called **associates** if one of the following equivalent conditions holds:

(i) $a = ub$ for some $u \in R^\times$.

(ii) $a \mid b$ and $b \mid a$, i.e. $(a) = (b)$.

If R is a general commutative ring, then we only have the implication (i) $\implies$ (ii). The converse is not true in general. For example, in $\mathbb{C}[x, y, z]/(x - xyz)$, $\overline{x} \mid \overline{xy}$ and $\overline{xy} \mid \overline{x}$, but there exists no unit u such that $\overline{x} = u\overline{xy}$.

Associatedness can also be described in terms of the action of $R^\times$ on R via multiplication: two elements of R are associates if they are in the same $R^\times$-orbit.

Definition 6.2.5 Irreducible Element

Let R be an integral domain. An non-zero element $a \in R$ is called **irreducible** if

(i) $a \notin R^\times$, i.e. a is not a unit.

(ii) $a = bc \implies b \in R^\times$ or $c \in R^\times$.

0 is never an irreducible element.

Proposition 6.2.6 Dividing Irreducible Element in PID Implies Associate or Unit

Let R be an integral domain and $f, g \in R$. If f is irreducible and $f \in (g)$, then one of the following holds:

(i) $g \in R^\times$, i.e. $(g) = R$.

(ii) g is an associate of f, i.e. $(g) = (f)$.

Proof. Since $f \in (g)$, there exists $h \in R$ such that $f = gh$. Since f is irreducible, we have $g \in R^\times$ or $h \in R^\times$. If $g \in R^\times$, then $(g) = R$. If $h \in R^\times$, then g is an associate of f and $(g) = (f)$. □

Proposition 6.2.7 Prime Element $\implies$ Irreducible Element in Integral Domain

Let R be an integral domain. Then every prime element in R is irreducible.

Proof. Let $a \in R$ be a prime element. Suppose $a = bc$ for some $b, c \in R$. Then $a \mid bc$. Since a is prime, there must be $a \mid b$ or $a \mid c$. Without loss of generality, we can assume $a \mid b$. Then $b = ad$ for some $d \in R$. Thus we have

$$a = bc = adc \implies a(1 - dc) = 0 \implies dc = 1 \implies c \in R^\times.$$

That implies a is irreducible. □

Proposition 6.2.8 Prime Ideal Equivalent Definition

Let R be a commutative ring. An ideal $I \subseteq R$ is prime if and only if R/I is an integral domain.

6.3 Unique Factorization Domain

Definition 6.3.1 Unique Factorization Domain

An integral domain R is called a **unique factorization domain** (UFD) if

(i) every nonzero nonunit element of R can be written as a product of irreducible elements of R.

(ii) if $p_1 \cdots p_n = q_1 \cdots q_m$ for some irreducible elements $p_1, \cdots, p_n, q_1, \cdots, q_m \in R$, then $n = m$ and there exists a permutation $\sigma \in S_n$ such that p_i is an associate of $q_{\sigma(i)}$ for all $i = 1, \cdots, n$.

Proposition 6.3.2 Irreducible Element $\iff$ Prime Element in UFD

Let R be a UFD and $a \in R$. Then

$$a \text{ is an irreducible element} \iff a \text{ is a prime element.}$$

Proof. Let $a \in R$ be an irreducible element. Suppose $a \mid bc$ for some $b, c \in R$. Then $bc = ad$ for some $d \in R$. Since R is a UFD, we can write $b = p_1 \cdots p_n$ and $c = q_1 \cdots q_m$ for some irreducible elements $p_1, \cdots, p_n, q_1, \cdots, q_m \in R$. Then we have

$$ad = bc = p_1 \cdots p_n q_1 \cdots q_m.$$

Since a is irreducible, a must be an associate of one of the p_i's or q_j's. Without loss of generality, we can assume $a \sim p_1$. Then $a \mid b$. That implies a is prime.

Proposition 6.2.7 shows the converse. □

Proposition 6.3.3 UFD $\implies$ Normal Domain

Every UFD is a normal domain.

Proof. Let R be a UFD and $K = \mathrm{Frac}(R)$ be the field of fractions of R. Suppose $a/b \in K$ is integral over R and $\gcd(a, b) = 1$. Then a/b satisfies a monic polynomial $f(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0$ with $r_i \in R$. Multiplying by b^n, we have

$$a^n + r_{n-1}a^{n-1}b + \cdots + r_0 b^n = 0 \implies b \mid a^n.$$

Since R is a UFD, both a and b can be uniquely written as a product of irreducible elements. Either b is a unit or b has an irreducible factor in common with a. Since $\gcd(a, b) = 1$, the latter is impossible. Hence $b \in R^\times$ and $a/b \in R$. □

6.4 Principal Ideal Domain

Definition 6.4.1 Principal Ideal Domain

An integral domain R is called a **principal ideal domain** (PID) if every ideal of R is principal.

Proposition 6.4.2

Let R be a commutative ring. Then the following are equivalent:

(i) R is a PID.

(ii) R is a UFD with Krull dimension $\dim R \leq 1$.

Corollary 6.4.3 PID $\implies$ UFD

Every PID is a UFD.

Proposition 6.4.4 Nonzero Prime Ideal $\iff$ Maximal Ideal in PID

Let R be a PID and $p \in R$. Then the following are equivalent:

(i) p is a prime element.

(ii) p is an irreducible element.

(iii) (p) is a nonzero prime ideal.

(iv) (p) is a maximal ideal.

Proof. By Proposition 6.1.33, (i) $\iff$ (iii). Since in UFD, prime elements are irreducible elements, (i) $\iff$ (ii). Since maximal ideals are prime, (iv) $\implies$ (iii).

To show (ii) $\implies$ (iv), suppose p is irreducible. Let I be an ideal of R such that

$$(p) \subseteq I \subseteq R.$$

Since R is a PID, there exists some $a \in R$ such that $I = (a)$. Then we have $(p) \subseteq (a)$, which implies there exists $r \in R$ such that $p = ra$ by Proposition 6.1.31. Because p is irreducible, by definition we have $a \in R^\times$ or $r \in R^\times$.

- If $a \in R^\times$, then $I = (a) = R$.
- If $r \in R^\times$, then $a = r^{-1}p$, which implies $(a) \subseteq (p)$ and thus $I = (a) = (p)$.

This shows that there are no ideals strictly between (p) and R. Hence (p) is maximal. □

6.5 Construction

6.5.1 Product

Definition 6.5.1 Product of Commutative Rings

Let $(R_i)_{i\in I}$ be a family of commutative rings. The **product** of the family $(R_i)_{i\in I}$ is the set of all families $(r_i)_{i\in I}$ where $r_i \in R_i$ for all $i \in I$. The addition and multiplication are defined componentwise:

$$(r_i)_{i\in I} + (s_i)_{i\in I} = (r_i + s_i)_{i\in I},$$
$$(r_i)_{i\in I} \cdot (s_i)_{i\in I} = (r_i \cdot s_i)_{i\in I}.$$

Proposition 6.5.2 Ideals of Finite Product of Commutative Rings

Let $R_1, R_2, \cdots, R_n$ be commutative rings. Then I is an ideal of the product $R_1 \times R_2 \times \cdots \times R_n$ if and only if $I = I_1 \times I_2 \times \cdots \times I_n$ where I_i is an ideal of R_i for all $i = 1, 2, \cdots, n$.

Proof. It is sufficient to show this for $n = 2$. Let I be an ideal of $R_1 \times R_2$. Let $\mathrm{pr}_1 : R_1 \times R_2 \to R_1$ and $\mathrm{pr}_2 : R_1 \times R_2 \to R_2$ be the natural projections. Then $\mathrm{pr}_1(I)$ and $\mathrm{pr}_2(I)$ are ideals of R_1 and R_2 respectively. It is easy to check that $I \subseteq \mathrm{pr}_1(I) \times \mathrm{pr}_2(I)$. To show the reverse inclusion, let $(a, b) \in \mathrm{pr}_1(I) \times \mathrm{pr}_2(I)$. Then there exist $(a, y) \in I$ such that $\mathrm{pr}_1((a, y)) = a$ and $(x, b) \in I$ such that $\mathrm{pr}_2((x, b)) = b$. Then

$$(a, b) = (1, 0)(a, y) + (0, 1)(x, b) \in I.$$

This implies $I = \mathrm{pr}_1(I) \times \mathrm{pr}_2(I)$.

Conversely, let I_1 and I_2 be ideals of R_1 and R_2 respectively. Then $I_1 \times I_2$ is an additive subgroup of $R_1 \times R_2$. For any $(a, b) \in I_1 \times I_2$ and $(x, y) \in R_1 \times R_2$, we have

$$(x, y)(a, b) = (xa, yb) \in I_1 \times I_2.$$

This implies $I_1 \times I_2$ is an ideal of $R_1 \times R_2$. □

6.5.2 Coproduct

Since we have the isomorphisms of categories

$$\mathsf{CRing} \cong (\mathsf{CRing}/\mathbb{Z}) \cong \mathbb{Z}\text{-}\mathsf{CAlg},$$

the coproduct in the category of commutative rings is given by the tensor product of commutative $\mathbb{Z}$-algebras.

Definition 6.5.3 Coproduct of Commutative Rings

Let R, S be commutative rings. The **coproduct** of R and S, denoted by $R \otimes_{\mathbb{Z}} S$, is the tensor product of R and S over $\mathbb{Z}$. The addition and multiplication are defined as follows:

$$(r_1 \otimes s_1) + (r_2 \otimes s_2) = (r_1 + r_2) \otimes (s_1 + s_2) - r_1 \otimes s_2 - r_2 \otimes s_1,$$
$$(r_1 \otimes s_1) \cdot (r_2 \otimes s_2) = (r_1 r_2) \otimes (s_1 s_2).$$

6.5.3 Quotient Ring

Definition 6.5.4 Quotient Ring

Let R be a commutative ring and $I \subseteq R$ be an ideal. The **quotient ring** of R by I, denoted by R/I, is the set of equivalence classes of the relation $\sim$ on $R \times R$ defined by

$$(a,b) \sim (c,d) \iff a - d \in I.$$

The equivalence class of (a,b) is denoted by $a+I$. The addition and multiplication on R/I are defined as follows:

$$(a+I)+(b+I) = (a+b)+I$$
$$(a+I)\cdot(b+I) = (ab)+I$$

The addition identify is $0+I$ and the multiplication identity is $1+I$.

Proposition 6.5.5 Universal Property of Quotient Ring

Let R be a commutative ring and $I \subseteq R$ be an ideal. The natural projection $\pi : R \to R/I$ satisfies the following universal property: for any ring homomorphism $f : R \to S$ such that $I \subseteq \ker f$ or equivalently $f(I) = \{0_S\}$, there exists a unique ring homomorphism

$$\begin{aligned} \overline{f} : R/I &\longrightarrow S \\ r+I &\longmapsto f(r) \end{aligned}$$

such that the following diagram commutes

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{f}} & \\ R/I & & \end{array}$$

Moreover, $\overline{f}$ is surjective exactly when f is surjective. $\overline{f}$ is injective exactly when $I = \ker f$.

Proof. If $\overline{f}$ is surjective, then $f = \overline{f} \circ \pi$ is surjective. If f is surjective, then for any $s \in S$, there exists $r \in R$ such that $f(r) = s$. Thus $\overline{f}(r+I) = f(r) = s$. That implies $\overline{f}$ is surjective.

If $\overline{f}$ is injective, then $\ker f = \ker \overline{f} \circ \pi = \ker \pi = I$. If $I = \ker f$, then

$$\ker \overline{f} = \left\{ r+I \in R/I \mid \overline{f}(r+I) = 0 \right\} = \{ r+I \in R/I \mid f(r) = 0 \} = \{ r+I \in R/I \mid r \in I \} = \{0+I\} = \left\{0_{R/I}\right\}$$

which implies $\overline{f}$ is injective. □

6.5.4 Free Object

Proposition 6.5.6

Define the following free functor

$$\begin{array}{ccc} \textsf{Set} & & \textsf{CRing} \\ \mathcal{X} & & \mathbb{Z}[\mathcal{X}] \ni \sum_\alpha n_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n} \\ {\scriptstyle f}\downarrow & \overset{\text{Free}}{\rightsquigarrow} & \downarrow{\scriptstyle \text{Free}(f)} \qquad\qquad \downarrow \\ \mathcal{Y} & & \mathbb{Z}[\mathcal{Y}] \ni \sum_\alpha n_\alpha f(X_1)^{\alpha_1} \cdots f(X_n)^{\alpha_n} \end{array}$$

We have a pair of adjoint functors

$$\mathsf{CRing} \underset{U}{\overset{\text{Free}}{\rightleftarrows}} \mathsf{Set} \quad (\perp)$$

and natural isomorphism

$$\mathrm{Hom}_{\mathsf{CRing}}(\mathrm{Free}\,(\mathcal{X})\,, R) \cong \mathrm{Hom}_{\mathsf{Set}}(\mathcal{X}, U(R)).$$

Definition 6.5.7 Free Commutative Ring

Since $\mathsf{CRing} \cong \mathbb{Z}\text{-}\mathsf{CAlg}$, the **free commutative ring** on a set X is isomorphic to the polynomial ring $\mathbb{Z}[X]$, which coincides with the free commutative $\mathbb{Z}$-algebra on X.

6.5.5 Localization

Definition 6.5.8 Multuplicative Subset

Let R be a commutative ring. A subset $S \subseteq R$ is called **multiplicative** if S is monoid under the multiplication of R, i.e.

(i) $1 \in S$.

(ii) $a, b \in S \implies ab \in S$.

Proposition 6.5.9

Let $\varphi : R \to R'$ be a ring homomorphism and $S \subseteq R$ be a multiplicative subset. Then $\varphi(S)$ is a multiplicative subset of $\subseteq R'$.

Proof. Since $1 \in S$, we have $1' = \varphi(1) \in \varphi(S)$. For any $a', b' \in \varphi(S)$, there exist $a, b \in S$ such that $a' = \varphi(a)$ and $b' = \varphi(b)$. Since S is multiplicative, we have $ab \in S$. Thus $a'b' = \varphi(a)\varphi(b) = \varphi(ab) \in \varphi(S)$. That implies $\varphi(S)$ is a multiplicative subset of R'. □

Definition 6.5.10 Localization of a Ring

Let R be a commutative ring and $S \subseteq R$ be a multiplicative subset. The **localization** of R at S is the ring $S^{-1}R$ defined as the set of equivalence classes of the relation $\sim$ on $R \times S$ defined by

$$(a, s) \sim (b, t) \iff \exists u \in S \text{ such that } u(at - bs) = 0.$$

The equivalence class of (a, s) is denoted by $\frac{a}{s}$. The addition and multiplication on $S^{-1}R$ are defined as follows:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$
$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

The addition identify is $\frac{0}{1}$ and the multiplication identity is $\frac{1}{1}$.

The localization of a commutative ring R at a multiplicative subset S is a commutative ring $S^{-1}R$. If we consider R as an R-module, then the localization of the R-module R at S is an $S^{-1}R$-module $S^{-1}R$. The underlying sets of $S^{-1}R$ as a commutative ring and as an $S^{-1}R$-module are the same. Furthermore, the ring structure of $S^{-1}R$ is compatible with the $S^{-1}R$-module structure, which makes $S^{-1}R$ a commutative $S^{-1}R$-algebra. By composing the localization map $R \to S^{-1}R$, $S^{-1}R$ can also be viewed as a commutative R-algebra.

Next we introduce the universal property of localization. It says localization is the most economical way to make a multiplicative subset invertible.

Proposition 6.5.11 Universal Property of Localization

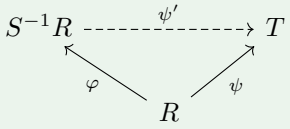
Let R be a commutative ring and $S \subseteq R$ be a multiplicative subset. The ring homomorphism

$$\begin{aligned} \varphi : R &\longrightarrow S^{-1}R \\ r &\longmapsto \frac{r}{1} \end{aligned}$$

satisfies the following universal property: for any ring homomorphism $\psi : R \to T$ such that $\psi(S) \subseteq T^\times$ or equivalently $S \subseteq \psi^{-1}(T^\times)$, there exists a unique ring homomorphism

$$\begin{aligned} \psi' : S^{-1}R &\longrightarrow T \\ \frac{a}{s} &\longmapsto \psi(a)(\psi(s))^{-1} \end{aligned}$$

such that the following diagram commutes



Moreover, if ψ is injective, then ψ' is injective. If ψ is surjective, then ψ' is surjective.

Proof. First let's check ψ' is well-defined. Suppose $\frac{a}{s} = \frac{b}{t}$. Then there exists $u \in S$ such that $u(at - bs) = 0$. Since ψ is a ring homomorphism, we have

$$0 = \psi(u(at - bs)) = \psi(u)\left(\psi(a)\psi(t) - \psi(b)\psi(s)\right).$$

Since $u \in S$ and $\psi(S) \subseteq T^\times$, we have $\psi(u) \in T^\times$. Thus

$$\psi'\left(\frac{a}{s}\right) = \psi(a)(\psi(t))^{-1} = \psi(b)(\psi(s))^{-1} = \psi'\left(\frac{b}{t}\right).$$

That implies ψ' is well-defined. It is easy to check ψ' is a ring homomorphism

$$\psi'\left(\frac{a}{s} + \frac{b}{t}\right) = \psi'\left(\frac{at + bs}{st}\right) = \psi(at + bs)(\psi(st))^{-1} = \psi(a)(\psi(s))^{-1} + \psi(b)(\psi(t))^{-1} = \psi'\left(\frac{a}{s}\right) + \psi'\left(\frac{b}{t}\right).$$

The multiplication is similar. The diagram commutes since

$$\psi' \circ \varphi(r) = \psi'\left(\frac{r}{1}\right) = \psi(r)(\psi(1))^{-1} = \psi(r).$$

Now we show ψ' is unique. Suppose there exists another ring homomorphism $\psi'' : S^{-1}R \to T$ such that the diagram commutes. Then for any $\frac{a}{s} \in S^{-1}R$, we have

$$\psi''\left(\frac{a}{s}\right) = \psi''\left(\frac{a}{1}\frac{1}{s}\right) = \psi''\left(\frac{a}{1}\right)\psi''\left(\frac{1}{s}\right) = \psi''\left(\frac{a}{1}\right)\left(\psi''\left(\frac{s}{1}\right)\right)^{-1} = \psi\left(a\right)\left(\psi(s)\right)^{-1} = \psi'\left(\frac{a}{s}\right).$$

That implies $\psi'' = \psi'$. Thus ψ' is unique.
Now suppose ψ is injective. Then

$$\ker\psi' = \left\{\frac{a}{s} \in S^{-1}R \,\middle|\, \psi(a)(\psi(s))^{-1} = 0\right\} = \left\{\frac{a}{s} \in S^{-1}R \,\middle|\, \psi(a) = 0\right\} = \left\{\frac{0}{s} \,\middle|\, s \in S\right\} = \{0\},$$

which implies ψ' is injective. □

Proposition 6.5.12 Localization of Commutative Rings as a Functor

Let CRingM be the category, whose objects and morphisms defined as follows:

- The objects are pairs (R, S) where R is a commutative ring and $S \subseteq R$ is a multiplicative subset.
- The morphisms from (R, S) to (R', S') are ring homomorphisms $f : R \to R'$ such that $f(S) \subseteq S'$.

Localization of commutative rings is a functor

$$\begin{array}{ccc} \mathsf{CRingM} & & \mathsf{CRing} \\ (R,S) & \overset{L}{\rightsquigarrow} & S^{-1}R \ni \frac{a}{s} \\ \downarrow f & & \downarrow L(f) \quad \downarrow \\ (R',S') & & S'^{-1}R' \ni \frac{f(a)}{f(s)} \end{array}$$

Let $G : \mathsf{CRing} \to \mathsf{CRingM}$ be functor that sends R to $(R, R^\times)$ and $f : R \to R'$ to $(f, f|_{R^\times})$. Then we have a pair of adjoint functors

$$\mathsf{CRingM} \underset{G}{\overset{L}{\rightleftarrows}} \mathsf{CRing} \quad (\perp)$$

and natural isomorphism

$$\mathrm{Hom}_{\mathsf{CRing}}(S^{-1}R, T) \cong \mathrm{Hom}_{\mathsf{CRingM}}((R,S),(T,T^\times)).$$

Proposition 6.5.13 Localization Functor for R-CAlg

Let R be a commutative ring, S be a multiplicative set in R, and M be an R-module. Define the localization functor as follows

$$\begin{array}{ccc} R\text{-}\mathsf{CAlg} & & S^{-1}R\text{-}\mathsf{CAlg} \\ A & \overset{S^{-1}}{\rightsquigarrow} & S^{-1}A \ni \frac{a}{s} \\ \downarrow f & & \downarrow S^{-1}(f) \quad \downarrow \\ B & & S^{-1}B \ni \frac{f(a)}{s} \end{array}$$

Let $\mathrm{Res}_{R \to S^{-1}R} : S^{-1}R\text{-}\mathsf{CAlg} \to R\text{-}\mathsf{CAlg}$ be the functor that regards $S^{-1}R$-algebras as R-algebras. Then we have a pair of adjoint functors

$$R\text{-}\mathsf{CAlg} \underset{\mathrm{Res}}{\overset{S^{-1}}{\rightleftarrows}} S^{-1}R\text{-}\mathsf{CAlg} \quad (\perp)$$

and natural isomorphism

$$\mathrm{Hom}_{S^{-1}R\text{-}\mathsf{CAlg}}(S^{-1}A, B) \cong \mathrm{Hom}_{R\text{-}\mathsf{CAlg}}(A, \mathrm{Res}_{R \to S^{-1}R}(B)).$$

And we have the following commutative diagram in R-CAlg

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow l_1 & & \downarrow l_2 \\ S^{-1}A & \underset{S^{-1}(f)}{\dashrightarrow} & S^{-1}B \end{array}$$

Proposition 6.5.14 Properties of Localization of Rings

Let R be a commutative ring and $S \subseteq R$ be a multiplicative subset. Then

(i) $S^{-1}R = \{0\}$ if and only if $0 \in S$.

(ii) If $0 \notin S$, then $\frac{a}{s}$ is invertible in $S^{-1}R$ if and only if there exists $r \in R$ such that $ra \in S$.

(iii) If $0 \notin S$, the localization map $\varphi : R \to S^{-1}R$ is injective if and only if S contains no zero divisors.

(iv) Localization preserves nilradical: $\mathfrak{N}_{S^{-1}R} = S^{-1}\mathfrak{N}_R$. Especially, R is reduced $\implies$ $S^{-1}R$ is reduced.

Proof. (i)

$$S^{-1}R = 0 \iff \frac{1}{1} = \frac{0}{1} \iff \exists s \in S \text{ such that } s \cdot 1 = 0 \iff 0 \in S.$$

(ii) Suppose $0 \notin S$. If $\frac{a}{s}$ is invertible in $S^{-1}R$, then there exists $\frac{b}{t} \in S^{-1}R$ such that $\frac{a}{s} \cdot \frac{b}{t} = \frac{1}{1}$, which implies there exists $u \in S$ such that $u(ab - st) = 0$. Let $r = ub \in R$ and then we see $ra = ust \in S$. Conversely, suppose there exists $r \in R$ such that $ra \in S$. Then $\frac{a}{s} \cdot \frac{rs}{ra} = \frac{1}{1}$, which implies $\frac{a}{s}$ is invertible.

(iii) Suppose $0 \notin S$. Given the localization map $\varphi : R \to S^{-1}R$, we have

$$\varphi(r) = 0 \iff \frac{r}{1} = \frac{0}{1} \iff \exists s \in S \text{ such that } s \cdot r = 0.$$

Thus

$$\varphi \text{ is injective} \iff \ker\varphi = \{0\} \iff \forall s \in S, \forall r \in R - \{0\}, sr \neq 0 \iff S \text{ contains no zero divisors.}$$

(iv) By Proposition 6.5.19, localization commutes with taking radical. Thus we have $\mathfrak{N}_{S^{-1}R} = \sqrt{0(S^{-1}R)} = S^{-1}\sqrt{0R} = S^{-1}\mathfrak{N}_R$. If R is reduced, then the nilradical of R is $\mathfrak{N}_R = (0)$. Thus we have $\mathfrak{N}_{S^{-1}R} = S^{-1}\mathfrak{N}_R = S^{-1}(0) = (0)$, which implies $S^{-1}R$ is reduced.

□

Definition 6.5.15 Total Ring of Fractions

Let R be a commutative ring. Then $S = \{r \in R - \{0\} \mid r \text{ is not a zero divisor}\}$ is a multiplicative subset. The **total ring of fractions** of R is the localization $S^{-1}R$, denoted by $\mathrm{Frac}(R)$. The localization map $\varphi : R \hookrightarrow \mathrm{Frac}(R)$ is an injective ring homomorphism.

Proof. Since $0 \notin S$ and S contains no zero divisors, φ is injective by (iii) of Proposition 6.5.14. □

Proposition 6.5.16 Properties of Total Ring of Fractions

Let R be a commutative ring and $S \subseteq R$ be a multiplicative subset. Then $S^{-1}R$ can be regarded as a subring of $\mathrm{Frac}(R)$.

Proof. By the universal property of localization, there exists a unique ring homomorphism $\psi : S^{-1}R \to \mathrm{Frac}(R)$. Since $\varphi : R \hookrightarrow \mathrm{Frac}(R)$ is injective, ψ is also injective. □

Definition 6.5.17 Field of Fractions

If R be an integral domain, then $S = R - \{0\}$ is a multiplicative subset. The total ring of fractions $\mathrm{Frac}(R) = S^{-1}R = R_{(0)}$ is a field, call the **field of fractions** of R.

Definition 6.5.18 Localization of an Ideal

Let R be a commutative ring, S be a multiplicative set in R, and I be an ideal of R. If we regard I as a R-module, the **localization of the ideal** I by S, denoted $S^{-1}I$, is the localization of the module I by S. That is,

$$S^{-1}I = \left\{ \frac{a}{s} \,\middle|\, a \in I, s \in S \right\}.$$

$S^{-1}I$ is a $S^{-1}R$-submodule of $S^{-1}R$. Suppose the localization map is $l_S : R \to S^{-1}R$, $S^{-1}I$ can also

defined as the ideal generated by $l_S(I)$ in $S^{-1}R$

$$S^{-1}I = \langle l_S(I) \rangle = \left\{ \frac{r}{s}\frac{a}{1} \,\middle|\, a \in I, \frac{r}{s} \in S^{-1}R \right\}.$$

Proposition 6.5.19 Properties of Localization of Ideals

Let R be a commutative ring, S be a multiplicative set in R, and $0 \notin S$. Suppose the localization map is $l_S : R \to S^{-1}R$. Then we have maps between the sets of ideals of R and $S^{-1}R$:

$$\mathcal{I}(R) = \{\text{ideals of } R\} \underset{l_S^{-1}}{\overset{S^{-1}}{\rightleftarrows}} \{\text{ideals of } S^{-1}R\} = \mathcal{I}(S^{-1}R)$$

(i) $S^{-1} \circ l_S^{-1} = \mathrm{id}_{\mathcal{I}(S^{-1}R)}$. As a result, S^{-1} is surjective and l_S^{-1} is injective.

(ii) For any ideal J of $S^{-1}R$, there exists an ideal I of R such that $S^{-1}I = J$.

(iii) If I is a ideal of R, then $S^{-1}I = S^{-1}R \iff I \cap S \neq \varnothing$.

(iv) l_S induces a bijection between the set of prime ideals of R that do not intersect S and the set of prime ideals of $S^{-1}R$. That is, the following restriction of S^{-1} and l_S^{-1} are bijections:

$$\{I \in \mathrm{Spec}\,(R) : I \cap S = \varnothing\} \underset{l_S^{-1}}{\overset{S^{-1}}{\rightleftarrows}} \mathrm{Spec}\left(S^{-1}R\right)$$

(v) If I is an ideal of R, then $S^{-1}\sqrt{I} = \sqrt{S^{-1}I}$.

Proof. (i) Let J be an ideal of $S^{-1}R$. We have

$$S^{-1}l_S^{-1}(J) = \left\{ \frac{x}{s} \,\middle|\, x \in l_S^{-1}(J), s \in S \right\} = \left\{ \frac{x}{s} \,\middle|\, \frac{x}{1} \in J, s \in S \right\} = \left\{ \frac{1}{s}\frac{x}{1} \,\middle|\, \frac{x}{1} \in J, s \in S \right\} = J.$$

(ii) It is a direct consequence of the surjectivity of S^{-1}.

(iii) Let I be an ideal of R. We have

$$S^{-1}I = S^{-1}R \iff \frac{1}{1} \in S^{-1}I \iff \exists t, s \in S, a \in I, t(a-s) = 0 \iff ta = ts \in I \cap S \neq \varnothing \iff I \cap S \neq \varnothing.$$

(iv) Omitted.

(v) For any $\frac{a}{s} \in S^{-1}\sqrt{I}$, there exists $n \in \mathbb{N}$ such that $a^n \in I$. Since $s^n \in S$, we have $\left(\frac{a}{s}\right)^n \in S^{-1}I$, which implies $\frac{a}{s} \in \sqrt{S^{-1}I}$. Hence $S^{-1}\sqrt{I} \subseteq \sqrt{S^{-1}I}$.

Conversely, for any $x \in \sqrt{S^{-1}I}$, since $\sqrt{S^{-1}I}$ is an ideal of $S^{-1}R$, there exists $a \in r$ and $s \in S$ such that $x = \frac{a}{s}$. $\frac{a}{s} \in \sqrt{S^{-1}I}$ means there exists $n \in \mathbb{N}$ such that $\left(\frac{a}{s}\right)^n \in S^{-1}I$. Thus there exists $t \in S$ and $b \in I$ such that $\left(\frac{a}{s}\right)^n = \frac{b}{t}$. And this is equivalent to $uta^n = ubs^n$ for some $u \in S$. Note $(uta)^n = u^n t^{n-1} s^n b \in I$, we have $uta \in \sqrt{I}$. Now we get $x = \frac{a}{s} = \frac{uta}{uts} \in S^{-1}\sqrt{I}$. Hence $\sqrt{S^{-1}I} \subseteq S^{-1}\sqrt{I}$.

□

Proposition 6.5.20 Localization Respects Quotients

Let R be a commutative ring, S be a multiplicative set in R, and I be an ideal of R. Let $\pi_I : R \to R/I$ be the projection and $\overline{S} = \pi_I(S)$. Then we have an R-algebra isomorphism $\overline{S}^{-1}(R/I) \cong (S^{-1}R)/(S^{-1}I)$ and

the following commutative diagram in R-CAlg (and accordingly in CRing)

$$\begin{array}{ccc} R & \xrightarrow{\pi_I} & R/I \\ {\scriptstyle l_S}\downarrow & & \downarrow{\scriptstyle l_S} \\ S^{-1}R & \xrightarrow[\pi_{S^{-1}I}]{} & \overline{S}^{-1}(R/I) \cong (S^{-1}R)/(S^{-1}I) \end{array}$$

Proof. From Proposition 7.2.26 we get the commutative diagram in R-Mod. Since localization map and quotient map are both ring homomorphisms, the commutative diagram holds in R-CAlg. □

Definition 6.5.21 Localization at a Prime Ideal

Let R be a commutative ring and $\mathfrak{p}$ be a prime ideal of R. Then $S = R - \mathfrak{p}$ is a multiplicative set. The localization $S^{-1}R$ is called the **localization of R at $\mathfrak{p}$**, denoted by $R_{\mathfrak{p}}$. $R_{\mathfrak{p}}$ is a local ring with unique maximal ideal

$$\mathfrak{p}R_{\mathfrak{p}} = S^{-1}\mathfrak{p} = \left\{ \frac{x}{s} \,\middle|\, x \in \mathfrak{p}, s \in R - \mathfrak{p} \right\}.$$

And we have field isomorphism $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \cong \mathrm{Frac}(R/\mathfrak{p})$. We call the field $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ the **residue field** of R at $\mathfrak{p}$ and denote it by $\kappa(\mathfrak{p})$.

Proof. Note

$$\{I \in \operatorname{Spec} R : I \cap S = \varnothing\} = \{I \in \operatorname{Spec} R : I \cap (R - \mathfrak{p}) = \varnothing\} = \{I \in \operatorname{Spec} R : I \subseteq \mathfrak{p}\}.$$

For any ideal $S^{-1}I \in \operatorname{Spec} S^{-1}R$, where $I \in \{I \in \operatorname{Spec} R : I \cap S = \varnothing\}$, we have $I \subseteq \mathfrak{p}$, which implies $S^{-1}I \subseteq S^{-1}\mathfrak{p}$. Thus we see $S^{-1}\mathfrak{p}$ is the unique maximal ideal of $S^{-1}R$.

According to Proposition 6.5.20, we have an isomorphism $(R/\mathfrak{p})_{\mathfrak{p}} \cong R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ and the following commutative diagram in R-CAlg

$$\begin{array}{ccc} R & \xrightarrow{\pi_{\mathfrak{p}}} & R/\mathfrak{p} \\ {\scriptstyle l_{R-\mathfrak{p}}}\downarrow & & \downarrow{\scriptstyle l_{R-\mathfrak{p}}} \\ R_{\mathfrak{p}} & \xrightarrow[\pi_{\mathfrak{p}R_{\mathfrak{p}}}]{} & \mathrm{Frac}(R/\mathfrak{p}) \cong R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \end{array}$$

□

Lemma 6.5.22

Let R be a commutative ring and $\mathfrak{p}$ be a prime ideal of R. Suppose $l : R \to R_{\mathfrak{p}}$ is the localization map. Then we have

$$l^{-1}\left(R_{\mathfrak{p}}^{\times}\right) = l^{-1}\left(R_{\mathfrak{p}} - \mathfrak{p}R_{\mathfrak{p}}\right) = R - \mathfrak{p}.$$

Proof. Since

$$\mathfrak{p}R_{\mathfrak{p}} = \left\{ \frac{x}{s} \,\middle|\, x \in \mathfrak{p}, s \in R - \mathfrak{p} \right\},$$

we have

$$l^{-1}\left(R_{\mathfrak{p}}^{\times}\right) = l^{-1}\left(R_{\mathfrak{p}} - \mathfrak{p}R_{\mathfrak{p}}\right) = \left\{ a \in R \,\middle|\, \frac{a}{1} \notin \mathfrak{p}R_{\mathfrak{p}} \right\} = \{a \in R \,|\, a \notin \mathfrak{p}\} = R - \mathfrak{p}.$$

□

Proposition 6.5.23

Suppose $\varphi : R \to S$ is a commutative ring homomorphism. Let $\mathfrak{q}$ be a prime ideal of S. Then $\mathfrak{p} := \varphi^{-1}(\mathfrak{q})$

is a prime ideal of R. And we have the following commutative diagram in CRing:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle l_{\mathfrak{p}}}\downarrow & & \downarrow{\scriptstyle l_{\mathfrak{q}}} \\ R_{\mathfrak{p}} & \xrightarrow[\psi]{} & S_{\mathfrak{q}} \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} & \xrightarrow[\eta]{} & S_{\mathfrak{q}}/\mathfrak{q}S_{\mathfrak{q}} \end{array}$$

Proof. Note that

$$(l_{\mathfrak{q}} \circ \varphi)^{-1}(S_{\mathfrak{q}}^{\times}) = \varphi^{-1}(l_{\mathfrak{q}}^{-1}(S_{\mathfrak{q}}^{\times})) = \varphi^{-1}(S - \mathfrak{q}) = R - \varphi^{-1}(\mathfrak{q}) = R - \mathfrak{p}.$$

By the universal property of localization, since $R - \mathfrak{p} \subseteq (l_{\mathfrak{q}} \circ \varphi)^{-1}(S_{\mathfrak{q}}^{\times})$, there exists a unique ring homomorphism

$$\begin{aligned} \psi : R_{\mathfrak{p}} &\longrightarrow S_{\mathfrak{q}} \\ \frac{a}{s} &\longmapsto \frac{\varphi(a)}{\varphi(s)} \end{aligned}$$

such that $l_{\mathfrak{q}} \circ \varphi = \psi \circ l_{\mathfrak{p}}$.

Since $\varphi(\mathfrak{p}) = \varphi(\varphi^{-1}(\mathfrak{q})) \subseteq \mathfrak{q}$ and $\varphi(R - \mathfrak{p}) = \varphi(\varphi^{-1}(S - \mathfrak{q})) \subseteq S - \mathfrak{q}$, we have

$$\psi(\mathfrak{p}R_{\mathfrak{p}}) = \left\{ \frac{\varphi(x)}{\varphi(s)} \,\middle|\, x \in \mathfrak{p}, s \in R - \mathfrak{p} \right\} \subseteq \left\{ \frac{y}{t} \,\middle|\, y \in \mathfrak{q}, t \in S - \mathfrak{q} \right\} = \mathfrak{q}S_{\mathfrak{q}},$$

which means ψ is a local ring homomorphism. Note that

$$\psi(\mathfrak{p}R_{\mathfrak{p}}) \subseteq \mathfrak{q}S_{\mathfrak{q}} = \ker \pi_2 \implies \mathfrak{p}R_{\mathfrak{p}} \subseteq \psi^{-1}(\ker \pi_2) = \ker(\pi_2 \circ \psi).$$

By the universal property of quotient ring, there exists a unique ring homomorphism

$$\begin{aligned} \eta : R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} &\longrightarrow S_{\mathfrak{q}}/\mathfrak{q}S_{\mathfrak{q}} \\ \frac{a}{s} + \mathfrak{p}R_{\mathfrak{p}} &\longmapsto \frac{\varphi(a)}{\varphi(s)} + \mathfrak{q}S_{\mathfrak{q}} \end{aligned}$$

such that $\eta \circ \pi_1 = \pi_2 \circ \psi$. Hence we obtain the commutative diagram. □

Proposition 6.5.24 Localization of Integral Domain at a Prime Ideal

Let R be an integral domain and $\mathfrak{p}$ be a prime ideal of R. Then $R_{\mathfrak{p}}$ is an integral domain and we have

$$R = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} R_{\mathfrak{p}} = \bigcap_{\mathfrak{m} \in \operatorname{MaxSpec} R} R_{\mathfrak{m}}.$$

Proof. First we need to show $R_{\mathfrak{p}}$ is an integral domain. Suppose $\frac{a}{s}, \frac{b}{t} \in R_{\mathfrak{p}}$ such that $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} = \frac{0}{1}$. Then there exists $u \in R - \mathfrak{p}$ such that $uab = 0$. Since R is an integral domain and $u \neq 0$, either $a = 0$ or $b = 0$, which implies $R_{\mathfrak{p}}$ is an integral domain.

□

Example 6.5.1

Let R be a commutative ring and $f \in R$. Let $S = \{1, f, f^2, \cdots\}$ be the monoid generated by f. Then S is a multiplicative set. The localization $S^{-1}R$ is called the **localization of R at f**, denoted by R_f or $R\left[\frac{1}{f}\right]$. The notation can be justified by the fact that $R\left[\frac{1}{f}\right] \cong R[t]/(ft - 1)$. $R_f = \{0\}$ if and only if f is nilpotent.

Proof. $R_f = \{0\} \iff 0 \in S \iff \exists n \in \mathbb{Z}_{\geq 0},\ f^n = 0.$ □

6.6 Commutative Ring Homomorphism

6.6.1 Commutative Ring Homomorphism of Finite Type

Definition 6.6.1 Finite-type Commutative Algebra

Let $R \to A$ be a commutative ring homomorphism. We say A is a **finite-type R-algebra**, or that $R \to A$ is **of finite type**, if one of the following equivalent conditions holds:

(i) there exists a finite set of elements $a_1, \cdots, a_n$ of A such that every element of A can be expressed as a polynomial in $a_1, \cdots, a_n$, with coefficients in R.

(ii) there exists a finite set X such that $A \cong R[X]/I$ as R-algebra where I is an ideal of $R[X]$.

6.6.2 Integral Commutative Ring Homomorphism

Recall the polynomial ring functor. Let $\varphi : R \to S$ be a ring homomorphism between two commutative rings. Since $\varphi : R \to S$ induces a ring homomorphism

$$\begin{aligned} \widetilde{\varphi} : R[T] &\longrightarrow S[T] \\ \sum_{k=0}^{n} r_k T^k &\longmapsto \sum_{k=0}^{n} \varphi(r_k) T^k \end{aligned}$$

we can define ${}^{\varphi}f := \widetilde{\varphi}(f)$ for any $f \in R[T]$.

Definition 6.6.2 Integral Element

Let $\varphi : R \to S$ be a ring homomorphism between two commutative rings. An element $x \in S$ is called **integral** over R if there exists a monic polynomial $f \in R[T]$ such that ${}^{\varphi}f(x) = 0$.

Definition 6.6.3 Generated Subalgebra

Let $\varphi : R \to A$ be a ring homomorphism between two commutative rings and $(a_i)_{i \in I}$ where $a_i \in A$. Let $\mathcal{T} = (T_i)_{i \in I}$. Define

$$\begin{aligned} \theta : \mathcal{T} &\longrightarrow A \\ T_i &\longmapsto a_i \end{aligned}$$

By the universal property of polynomial ring, there exists a unique ring homomorphism $\psi : R[\mathcal{T}] \to A$ such that $\psi(T_i) = a_i$ for all $i \in I$, that is, the following diagram commutes

$$\begin{array}{ccc} R[\mathcal{T}] & \overset{\exists! \, \psi}{\dashrightarrow} & A \\ {\scriptstyle \iota}\uparrow & \nearrow_{\theta} & \\ \mathcal{T} & & \end{array}$$

The **R-subalgebra of A generated by** $(a_i)_{i \in I}$ is defined as

$$R[\mathcal{T}] := \psi\left(R[\mathcal{T}]\right) = \left\{ \sum_{|\alpha| \leq n} r_\alpha a^\alpha \in A \;\middle|\; r_\alpha \in R \right\}.$$

The **R-subalgebra of A generated by** a is defined as

$$R[a] := \psi\left(R[T]\right) = \left\{ \sum_{k=0}^{n} r_k a^k \in A \;\middle|\; r_k \in R \right\}.$$

Proposition 6.6.4 Equivalent Definition of Integral Element

Let $\varphi : R \to S$ be a ring homomorphism between two commutative rings and $a \in S$. Let $R[a]$ be the R-subalgebra of S generated by a. Then S is an $R[a]$-module. And the following statements are equivalent:

(i) a is integral over R.

(ii) $R[a]$ is a finitely generated R-module.

(iii) There exists a faithful $R[a]$-submodule of S that is finitely generated as an R-module and contains x.

Suppose $a_1, \cdots, a_n \in S$. Let $R[a_1, \cdots, a_n]$ be the R-subalgebra of S generated by $a_1, \cdots, a_n$. Then the following statements are equivalent:

(i) $a_1, \cdots, a_n$ are integral over R.

(ii) $R[a_1, \cdots, a_n]$ is a finitely generated R-module.

Proof. The first part is a special case of Proposition 8.3.3. □

Definition 6.6.5 Integral Extension

Let $\varphi : R \to S$ be a ring homomorphism between two commutative rings. If every element of S is integral over R, then we say φ is **integral** and S is an **integral extension** of R.

Proposition 6.6.6 Descent of Integrality along Ring Homomorphisms

Let $A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ be ring homomorphisms between commutative rings.

(i) If $x \in C$ is integral over A, then x is integral over B.

(ii) If $A \to C$ is integral, then $B \to C$ is integral.

Proof. (i) Let $f \in A[T]$ be a monic polynomial such that ${}^{\psi\circ\varphi}f(x) = 0$. We have ${}^{\varphi}f \in B[T]$ and ${}^{\psi}({}^{\varphi}f)(x) = {}^{\psi\circ\varphi}f(x) = 0$. Hence x is integral over B.

(ii) Since $A \to C$ is integral, every element of C is integral over A. By (i), every element of C is integral over B. Hence $B \to C$ is integral.

□

Definition 6.6.7 Integral Closure

Let $\varphi : R \to S$ be a ring homomorphism between two commutative rings. The set of all elements in S that are integral over R is called the **integral closure of R in S**. The integral closure of R in S is an R-subalgebra of S, denoted by $\overline{R}^S$. If φ is injective, we say that R is **integrally closed in S** if $\varphi(R) = \overline{R}^S$.

Remark. Since for any $b \in \varphi(R)$, there exists $a \in R$ such that $b = \varphi(a)$. Let $P(X) = X - a \in R[X]$. Then

$$ {}^{\varphi}P(X) = X - \varphi(a) \implies {}^{\varphi}P(b) = b - \varphi(a) = 0. $$

Hence b is integral over R. Since $\varphi(R) \subseteq \overline{R}^S$, we can define a ring homomorphism $u : R \to \overline{R}^S$ as the composition of φ and the inclusion map $\varphi(R) \hookrightarrow \overline{R}^S$.

$$ u := \iota \circ \varphi : R \longrightarrow \overline{R}^S. $$

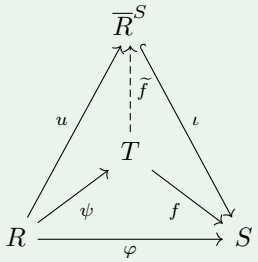
Therefore, integral closure is a ring extension. Furthermore, if φ is injective, then $u : R \to \overline{R}^S$ is also injective. □

Proposition 6.6.8 Universal Properties of Integral Closure

Let $\varphi : R \to S$ be a ring homomorphism between two commutative rings. Then for any integral extension $\psi : R \to T$ and any ring homomorphism $f : T \to S$, there exists a unique ring homomorphism

$$\begin{aligned} \widetilde{f} : T &\longrightarrow \overline{R}^S \\ t &\longmapsto f(t) \end{aligned}$$

such that the following diagram commutes



That is, $R \to \overline{R}^S \hookrightarrow S$ is terminal.

Proof. First we show $f(T) \subseteq \overline{R}^S$. For any $b \in f(T)$, there exists $a \in T$ such that $b = f(a)$. Since a is integral over R, there exists a monic polynomial $P(X) = X^n + r_{n-1}X^{n-1} + \cdots + r_0 \in R[X]$ such that ${}^{\psi}P(a) = 0$. By applying f to both sides of the equation, we get

$$f\left({}^{\psi}P(a)\right) = {}^{f\circ\psi}P(f(a)) = {}^{\varphi}P(b) = 0,$$

which implies b is integral over R. Hence $f(T) \subseteq \overline{R}^S$. So we can define a ring homomorphism

$$\begin{aligned} \widetilde{f} : T &\longrightarrow \overline{R}^S \\ t &\longmapsto f(t) \end{aligned}$$

such that $\iota \circ \widetilde{f} = f$. Since ι is injective,

$$\iota \circ \widetilde{f} \circ \psi = f \circ \psi = \varphi = \iota \circ u \implies \widetilde{f} \circ \psi = u.$$

Thus we obtain the commutative diagram.

Suppose there exists another ring homomorphism $g : T \to \overline{R}^S$ such that $\iota \circ g = f$. Since ι is injective, we have $g = \widetilde{f}$. This means $\widetilde{f}$ is unique. □

Definition 6.6.9 Integral Closure of Integal Domain in Field of Fractions

Let R be an integral domain. The **integral closure of** R or **normalization of** R is defined to be the integral closure of R in $\mathrm{Frac}(R)$.

Remark. We say R is **integrally closed** or **normal** if R is integrally closed in $\mathrm{Frac}(R)$. See Definition 6.7.1 □

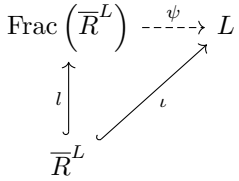
Proposition 6.6.10 Fraction Field of Integral Closure of Integral domain

Let R be an integral domain and $\mathrm{Frac}(R)$ be its field of fractions. If L/K is a finite field extension, and $\overline{R}^L$ is the integral closure of R in L, then L is a field of fractions of $\overline{R}^L$.

Proof. $\overline{R}^L$ is an integral domain because it is a subring of integral domain L. Let $l : \overline{R}^L \hookrightarrow \mathrm{Frac}\left(\overline{R}^L\right)$ be the localization map and $\iota : \overline{R}^L \hookrightarrow L$ be the inclusion. According to the universal property of field of fractions, there exists a unique field homomorphism

$$\begin{aligned} \psi : \mathrm{Frac}\left(\overline{R}^L\right) &\longrightarrow L \\ \frac{a}{b} &\longmapsto \frac{a}{b} \end{aligned}$$

such that the following diagram commutes



For any $x \in L$, suppose the minimal polynomial of x is

$$f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0 \in K[T].$$

By multiplying $f(T)$ by the product of the denominators of the coefficients of $f(T)$, we get a polynomial $g(T) \in R[T]$ such that

$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = 0.$$

Multiplying this equation by b_n^{n-1}, we get

$$(b_n x)^n + b_{n-1}(b_n x)^{n-1} + \cdots + b_1 b_n^{n-2}(b_n x) + b_0 = 0,$$

which implies $b_n x$ is integral over R. Since $\overline{R}^L$ is the integral closure of R in L, we have $b_n x \in \overline{R}^L$. Hence

$$x = \psi\left(\frac{b_n x}{b_n}\right) \in \psi\left(\text{Frac}\left(\overline{R}^L\right)\right).$$

Therefore, ψ is a isomorphism between $l : \overline{R}^L \hookrightarrow \text{Frac}\left(\overline{R}^L\right)$ and $\iota : \overline{R}^L \hookrightarrow L$. Since any object isomorphic to an initial object is also initial, we see L is a field of fractions of $\overline{R}^L$.

□

Proposition 6.6.11 Quotient and Localization Respect Integral Extensions

Let $R \subseteq T$ be an integral extension of commutative rings. Then

(i) If $\mathfrak{b}$ is an ideal of T, then $\mathfrak{a} := R \cap \mathfrak{b}$ is an ideal of R and $S/\mathfrak{b}$ is integral over $R/\mathfrak{a}$.

(ii) If S is a multiplicative set in R, then $S^{-1}T$ is integral over $S^{-1}R$.

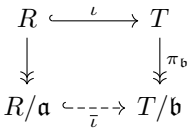
Proof. (i) Since

$$\ker(\pi_\mathfrak{b} \circ \iota) = \iota^{-1}(\ker \pi_\mathfrak{b}) = \iota^{-1}(\mathfrak{b}) = R \cap \mathfrak{b} = \mathfrak{a},$$

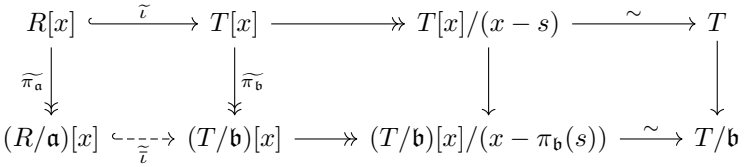
by the universal property of quotient ring, there is an injective ring homomorphism

$$\begin{aligned} \bar{\iota} : R/\mathfrak{a} &\hookrightarrow T/\mathfrak{b} \\ r + \mathfrak{a} &\longmapsto r + \mathfrak{b}. \end{aligned}$$

such that the following diagram commutes



For any $s + \mathfrak{b} \in T/\mathfrak{b}$, there exists a monic polynomial $f \in R[x]$ such that $\iota f(s) = 0_T$. So we have the following commutative diagram



By evaluating this diagram at $f \in R[x]$, we see there exists a monic polynomial $g := {}^{\pi_{\mathfrak{a}}}f \in (R/\mathfrak{a})[x]$ such that

$$\bar{\iota}g(s+\mathfrak{b}) = {}^{\iota}f(s) + \mathfrak{b} = 0_{S/\mathfrak{b}},$$

which implies $s+\mathfrak{b}$ is an integral element over $R/\mathfrak{a}$.

(ii) Regard R, T as R-modules. Since the localization functor $S^{-1} : R\text{-}\mathsf{Mod} \to S^{-1}R\text{-}\mathsf{Mod}$ is exact, from the exact sequence in R-Mod

$$0 \longrightarrow R \longrightarrow T$$

we get the exact sequence in $S^{-1}R$-Mod

$$0 \longrightarrow S^{-1}R \longrightarrow S^{-1}T.$$

Note that the underlying sets of the $S^{-1}R$-module $S^{-1}T$ and the commutative ring $S^{-1}T$ coincide and the two algebraic structures on the same underlying set are compatible, which makes $S^{-1}T$ an $S^{-1}R$-algebra. For any $\frac{a}{s} \in S^{-1}T$, there exists a monic polynomial

$$f(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0 \in R[x]$$

such that

$${}^{\iota}f(a) = a^n + r_{n-1}a^{n-1} + \cdots + r_0 = 0_T.$$

This equation can be rewritten as

$$\left(\frac{a}{s}\right)^n + \frac{r_{n-1}}{s}\left(\frac{a}{s}\right)^{n-1} + \cdots + \frac{r_0}{s^n} = 0_{S^{-1}T},$$

which implies $\frac{a}{s}$ is an integral element over $S^{-1}R$.

□

The following proposition shows that the property of being integral is preserved under field extension.

Proposition 6.6.12 Injective Ring Extension Preserves Integral Elements

Suppose $A \xrightarrow{\varphi} B \xhookrightarrow{\iota} C$ are ring homomorphisms between commutative rings and ι is injective. For any $b \in B$, b is integral over A if and only if $\iota(b)$ is integral over A.

Proof. Let $c = \iota(b)$. We have the following commutative diagram

$$\begin{array}{ccccc}
C[X] & \xrightarrow{\pi_2} & C[X]/(X-c) & \xrightarrow{\mathrm{ev}_c} & C \\
\tilde{\iota}\uparrow & & \uparrow & & \uparrow\iota \\
B[X] & \xrightarrow{\pi_1} & B[X]/(X-b) & \xrightarrow{\mathrm{ev}_b} & B \\
\tilde{\varphi}\uparrow & & & & \\
A[X] & & & &
\end{array}$$

If c is integral over A, there exists a monic polynomial $f \in A[X]$ such that

$$\mathrm{ev}_c \circ \pi_2 \circ \tilde{\iota} \circ \tilde{\varphi}(f) = {}^{\varphi\circ\iota}f(c) = 0_C,$$

which implies

$$\iota \circ \mathrm{ev}_b \circ \pi_1 \circ \tilde{\varphi}(f) = \iota(\mathrm{ev}_b \circ \pi_1 \circ \tilde{\varphi}(f)) = 0_C.$$

Since ι is injective, we have $\mathrm{ev}_b \circ \pi_1 \circ \tilde{\varphi}(f) = 0_B$, which implies b is integral over A.

Conversely, if b is integral over A, there exists a monic polynomial $f \in A[X]$ such that

$$\mathrm{ev}_b \circ \pi_1 \circ \tilde{\varphi}(f) = {}^{\varphi}f(b) = 0_B.$$

Thus we have

$${}^{\varphi\circ\iota}f(c) = \mathrm{ev}_c \circ \pi_2 \circ \tilde{\iota} \circ \tilde{\varphi}(f) = \iota \circ \mathrm{ev}_b \circ \pi_1 \circ \tilde{\varphi}(f) = \iota(\mathrm{ev}_b \circ \pi_1 \circ \tilde{\varphi}(f)) = \iota(0_B) = 0_C,$$

which implies c is integral over A. □

Proposition 6.6.13 Surjectivity of Spectrum Map of Integral Extension

Let $R \subseteq S$ be an integral extension of commutative rings and $\varphi : R \hookrightarrow S$ be the inclusion. Then the map $\varphi^{-1} : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is surjective.

Proposition 6.6.14

Let $R \subseteq K$ be an extension of commutative rings and K be a field.

- If K is integral over R, then R is a field. The field extension K/R is algebraic.
- If K is finite over R, then R is a field. The field extension K/R is finite.

Proof.

- According to Proposition 6.6.13, the map $\varphi^{-1} : \mathrm{Spec}(K) \to \mathrm{Spec}(R)$ is surjective. Since $\mathrm{Spec}(K)$ is a singleton, $\mathrm{Spec}(R)$ is also a singleton. It is clear that R is a Noetherian ring. According to Proposition 6.9.11, R is an Artinian ring. Since R is a subring of a field, R is an integral domain. Since Artinian integral domain is a field, R is a field.

□

Proposition 6.6.15

Let $\varphi : K \to S$ be a ring homomorphism of integral domains and K be a field.

- If S is integral over K, then S is a field.

Corollary 6.6.16

Let $R \subseteq S$ be an integral extension of integral domains. Then R is a field if and only if S is a field.

Proof. This is a direct consequence of Proposition 6.6.14 and Proposition 6.6.15. □

Corollary 6.6.17

Let $R \subseteq S$ be an integral extension of commutative rings. Let $\mathfrak{q}$ be a prime ideal of S and $\mathfrak{p} := R \cap \mathfrak{q}$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.

Proof. From Proposition 6.6.11 we see $R/\mathfrak{p} \hookrightarrow S/\mathfrak{q}$ is an integral extension of integral domains. By Corollary 6.6.16 we know $R/\mathfrak{p}$ is a field if and only if $S/\mathfrak{q}$ is a field. This implies $\mathfrak{p}$ is maximal if and only if $\mathfrak{q}$ is maximal. □

Definition 6.6.18

Let $R \subseteq S$ be an extension of commutative rings.

- **lying over property**: If there exist $\mathfrak{p} \in \mathrm{Spec}\, R$ and $\mathfrak{q} \in \mathrm{Spec}\, S$ such that $\mathfrak{q} \cap R = \mathfrak{p}$, we say $\mathfrak{q}$ **lies over** $\mathfrak{p}$ and $\mathfrak{p}$ **lies under** $\mathfrak{q}$. We say the extension $R \subseteq S$ satisfies the **lying over property** if every prime ideal of R lies under some prime ideal of S.
- **incomparability property**: we say the extension $R \subseteq S$ satisfies the **incomparability property** if for any two distinct prime ideals $\mathfrak{q}_1, \mathfrak{q}_2$ of S lying over $\mathfrak{p} \in \mathrm{Spec}\, R$, we have $\mathfrak{q}_1 \not\subseteq \mathfrak{q}_2$ and $\mathfrak{q}_2 \not\subseteq \mathfrak{q}_1$.
- **going-up property**: we say the extension $R \subseteq S$ satisfies the **going-up property** if for any prime ideals $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ of R and any prime ideal $\mathfrak{q}_1$ of S lying over $\mathfrak{p}_1$, there exists a prime ideal $\mathfrak{q}_2$ of S lying over $\mathfrak{p}_2$ such that $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$.
- **going-down property**: we say the extension $R \subseteq S$ satisfies the **going-down property** if for any prime ideals $\mathfrak{p}_1 \supseteq \mathfrak{p}_2$ of R and any prime ideal $\mathfrak{q}_1$ of S lying over $\mathfrak{p}_1$, there exists a prime ideal $\mathfrak{q}_2$ of S lying over $\mathfrak{p}_2$ such that $\mathfrak{q}_1 \supseteq \mathfrak{q}_2$.

Proposition 6.6.19

if an extension $R \subseteq T$ satisfies the going-up property, then it also satisfies the lying-over property.

The following theorems are also called the Cohen-Seidenberg theorems.

Theorem 6.6.20 Going-up and Going-down Theorems

Let $R \subseteq T$ be an extension of commutative rings. Then the following hold:

(i) **Going-up Theorem**: If $R \subseteq T$ is an integral extension, then it satisfies the going-up property and and the incomparability property.

(ii) **Going-down Theorem**: If $R \subseteq T$ is an integral extension, T is an integral domain, and R is integrally closed in T, then it satisfies the going-down property.

Proof. (i) First we prove the incomparability property. It is sufficient to show if $\mathfrak{q}_1, \mathfrak{q}_2$ are prime ideals of S lying over $\mathfrak{p} \in \operatorname{Spec} R$ such that $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$, then $\mathfrak{q}_1 = \mathfrak{q}_2$. Let $S = R - \mathfrak{p}$. According to Proposition 6.6.11, we obtain an integral extension

$$\begin{aligned} \iota : R_{\mathfrak{p}} &\hookrightarrow S^{-1}T \\ \frac{r}{s} &\longmapsto \frac{r}{s}. \end{aligned}$$

$\mathfrak{p}R_{\mathfrak{p}}$ is a maximal ideal of $R_{\mathfrak{p}}$. Let

$$\begin{aligned} \mathfrak{a}_1 := S^{-1}\mathfrak{q}_1 &= \left\{ \frac{q}{s} \in S^{-1}T \,\middle|\, q \in \mathfrak{q}_1, s \in S \right\}, \\ \mathfrak{a}_2 := S^{-1}\mathfrak{q}_2 &= \left\{ \frac{q}{s} \in S^{-1}T \,\middle|\, q \in \mathfrak{q}_2, s \in S \right\}. \end{aligned}$$

Since

$$\mathfrak{q}_1 \cap S = \mathfrak{q}_1 \cap (R - \mathfrak{p}) = \mathfrak{q}_1 \cap (R - (\mathfrak{q}_1 \cap R)) = \mathfrak{q}_1 \cap (R - \mathfrak{q}_1) = \varnothing,$$

$\mathfrak{a}_1$ and $\mathfrak{a}_2$ are prime ideals of $S^{-1}T$. And we can check that

$$\begin{aligned} \mathfrak{a}_1 \cap R_{\mathfrak{p}} &= \iota^{-1}(\mathfrak{a}_1) \\ &= \left\{ \frac{q}{s} \in R_{\mathfrak{p}} \,\middle|\, q \in \mathfrak{q}_1, s \in S \right\} \\ &= \left\{ \frac{q}{s} \in R_{\mathfrak{p}} \,\middle|\, q \in \mathfrak{q}_1 \cap R, s \in S \right\} \\ &= \left\{ \frac{q}{s} \in R_{\mathfrak{p}} \,\middle|\, q \in \mathfrak{p}, s \in S \right\} \\ &= \mathfrak{p}R_{\mathfrak{p}}. \end{aligned}$$

Similarly we have $\mathfrak{a}_2 \cap R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$. So $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are prime ideals of $S^{-1}T$ lying over $\mathfrak{p}R_{\mathfrak{p}}$. By Corollary 6.6.17, both $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are maximal ideals of $S^{-1}T$. Since $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$, we have $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$. By the maximality of $\mathfrak{a}_1$ and $\mathfrak{a}_2$, we have $\mathfrak{a}_1 = \mathfrak{a}_2$. Since

$$\begin{aligned} S^{-1} : \{\mathfrak{q} \in \operatorname{Spec}(T) : \mathfrak{q} \cap S = \varnothing\} &\longrightarrow \operatorname{Spec}\left(S^{-1}T\right) \\ \mathfrak{q} &\longmapsto S^{-1}\mathfrak{q} \end{aligned}$$

is a bijection, we have $\mathfrak{q}_1 = \mathfrak{q}_2$.

□

Corollary 6.6.21

Let $R \subseteq S$ be an integral extension of integral domains. Then the unique prime ideal of S which lies over (0) is (0).

Proof. By Theorem 6.6.20, the extension $R \subseteq S$ satisfies the incomparability property. Suppose there exists a nonzero prime ideal $\mathfrak{q}$ of S lying over (0). Since (0) is another prime ideal of S lying over (0), we have $(0) \nsubseteq \mathfrak{q}$, which is a contradiction. □

Proposition 6.6.22 Composition of Integral Ring Homomorphisms is Integral

Let $\varphi : R \to S$ and $\psi : S \to T$ be two integral homomorphisms between commutative rings. Then $\psi \circ \varphi : R \to T$ is also integral.

Proof. Let $t \in T$. Since ψ is integral, there exists a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in S[X]$ such that $f(t) = 0_T$. Let $S' = R[a_0, \cdots, a_{n-1}] \subseteq S$. Since S is integral over R, we see $a_0, \cdots, a_{n-1} \in S$ are integral over R. By Proposition 6.6.4, this implies S' is finite over R. Since t is integral over S', again by Proposition 6.6.4 $S'[t]$ is finite over S'. Thus by Proposition 6.6.26, $S'[t]$ is finite over R, which implies $S'[t]$ is integral over R. Therefore, t is integral over R. □

6.6.3 Finite Commutative Ring Homomorphism

Definition 6.6.23 Finite Commutative Ring Homomorphism

Let $\varphi : R \to S$ be a homomorphism between two commutative rings. We say φ is **finite** if S as an R-module is finitely generated.

Definition 6.6.24 Finitely Generated Commutative Algebra

Let $R \to A$ be a commutative ring homomorphism. We say A is a **finitely generated R-algebra** or A is **finite** over R if one of the following equivalent conditions holds:

(i) $R \to A$ is finite.

(ii) A as an R-module is finitely generated.

Proposition 6.6.25

Let $\varphi : R \to S$ be a finite homomorphism between two commutative rings. Let M be an S-module. Then M is a finitely generated R-module if and only if M is a finitely generated S-module.

Proof. Suppose M is a finitely generated R-module. According to Proposition 7.2.9, M is a finitely generated S-module.

Conversely, suppose M is a finitely generated S-module. Then we have exact sequence of S-modules

$$S^m \longrightarrow M \longrightarrow 0.$$

Since the functor: φ_* is exact, the above exact sequence is also exact when we regard S^m as an R-module. Since S is a finitely generated R-module, we have an exact sequence of R-modules

$$R^n \longrightarrow S \longrightarrow 0.$$

Since direct sum is exact, we have an exact sequence of R-modules

$$R^{nm} \longrightarrow S^m \longrightarrow 0.$$

By composing $R^{nm} \longrightarrow S^m$ with $S^m \longrightarrow M$, we get a surjective R-linear map $R^{nm} \longrightarrow M$. Therefore, M is a finitely generated R-module. □

Proposition 6.6.26 Composition of Finite Ring Homomorphisms is Finite

Let $\varphi : R \to S$ and $\psi : S \to T$ be two finite homomorphisms between commutative rings. Then $\psi \circ \varphi : R \to T$ is also finite.

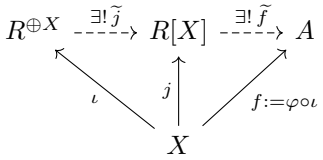
Proof. If $\varphi : R \to S$ and $\psi : S \to T$ are finite, according to Proposition 6.6.25, T is also finite over R. □

Proposition 6.6.27 Finite Generation Implies Finite Type

Let A be a R-algebra. If A is finitely generated as an R-module, then A is a finite-type R-algebra.

Proof. This holds because if each element of A can be expressed as an R-linear combination of finitely many elements of A, then each element of A can also be expressed as a polynomial in finitely many elements of A with coefficients in R.

An alternative proof can be given by utilizing the universal property of the free contruction. Suppose A is finitely generated as an R-module. Then there exists some a finite set $X = \{x_1, \cdots, x_n\}$ and a surjective R-linear map $\varphi : R^{\oplus X} \to A$. Define $f = \varphi \circ \iota$, where $\iota : X \to R^{\oplus X}$ is the inclusion map.



The universal property of free R-module induces a unique R-linear map $\widetilde{j} : R^{\oplus} \to R[X]$ such that $j = \widetilde{j} \circ \iota$. And the universal property of free commutative R-algebra induces a unique R-algebra homomorphism $\widetilde{f} : R[X] \to A$ such that $f = \widetilde{f} \circ j$. Note $f = \varphi \circ \iota = \left(\widetilde{f} \circ \widetilde{j}\right) \circ \iota$. By the uniqueness of the universal property of $R^{\oplus}$, we have $\widetilde{f} \circ \widetilde{j} = \varphi$. Since $\widetilde{f} \circ \widetilde{j}$ is surjective, $\widetilde{f}$ must be surjective, which implies A is a finite-type R-algebra. □

Corollary 6.6.28 Finite $\implies$ Finite Type

Let $\varphi : R \to A$ be a finite homomorphism between two commutative rings. Then φ is of finite type.

Proof. This is a reformulation of Proposition 6.6.27. □

Proposition 6.6.29 Quotient Respect Finiteness

Let $\varphi : R \to T$ be an finite homomorphism of commutative rings. Then

(i) Suppose $\mathfrak{b}$ is an ideal of S, and $\mathfrak{a} := \varphi^{-1}(\mathfrak{b})$. Then $\overline{\varphi} : R/\mathfrak{a} \to T/\mathfrak{b}$ is finite.

(ii) Suppose S is a multiplicative set of R, and $\widetilde{S} = \varphi(S)$. Then $\widetilde{\varphi} : S^{-1}R \to \widetilde{S}^{-1}T$ is finite.

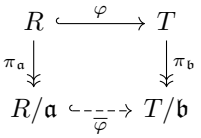
Proof. (i) Let $\mathfrak{a} := \varphi^{-1}(\mathfrak{b})$. Since

$$\ker(\pi_{\mathfrak{b}} \circ \varphi) = \varphi^{-1}\left(\ker \pi_{\mathfrak{b}}\right) = \varphi^{-1}\left(\mathfrak{b}\right) = \mathfrak{a},$$

by the universal property of quotient ring, there is an injective ring homomorphism

$$\begin{aligned} \overline{\varphi} : R/\mathfrak{a} &\hookrightarrow T/\mathfrak{b} \\ r + \mathfrak{a} &\longmapsto \varphi(r) + \mathfrak{b}. \end{aligned}$$

such that the following diagram commutes



Since T is a finitely generated R-module, we can suppose the generating set of T is $\{t_1, \cdots, t_n\}$. Then for any $t + \mathfrak{b} \in T/\mathfrak{b}$, there exists $r_1, \cdots, r_n \in R$ such that $t = \sum_{i=1}^{n} \varphi(r_i)t_i$. Thus we have

$$t + \mathfrak{b} = \left(\sum_{i=1}^{n} \varphi(r_i)t_i\right) + \mathfrak{b} = \sum_{i=1}^{n} \left(\varphi(r_i)t_i + \mathfrak{b}\right) = \sum_{i=1}^{n} (\varphi(r_i) + \mathfrak{b})\left(t_i + \mathfrak{b}\right) = \sum_{i=1}^{n} \overline{\varphi}(r_i + \mathfrak{a})\left(t_i + \mathfrak{b}\right).$$

Hence $\{t_1 + \mathfrak{b}, \cdots, t_n + \mathfrak{b}\}$ generates $T/\mathfrak{b}$. Therefore we proved $T/\mathfrak{b}$ is a finitely generated $R/\mathfrak{a}$-module, which implies $\overline{\varphi}$ is finite.

(ii) Regard R, T as R-modules. Since the localization functor $S^{-1} : R\text{-Mod} \to S^{-1}R\text{-Mod}$ is exact, from the exact sequence in R-Mod

$$0 \longrightarrow R \longrightarrow T$$

we get the exact sequence in $S^{-1}R$-Mod

$$0 \longrightarrow S^{-1}R \longrightarrow S^{-1}T.$$

Note that the underlying sets of the $S^{-1}R$-module $S^{-1}T$ and the commutative ring $S^{-1}T$ coincide and the two algebraic structures on the same underlying set are compatible, which makes $S^{-1}T$ an $S^{-1}R$-algebra. For any $\frac{a}{s} \in S^{-1}T$, there exists a monic polynomial

$$f(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0 \in R[x]$$

such that

$$\iota f(a) = a^n + r_{n-1}a^{n-1} + \cdots + r_0 = 0_T.$$

This equation can be rewritten as

$$\left(\frac{a}{s}\right)^n + \frac{r_{n-1}}{s}\left(\frac{a}{s}\right)^{n-1} + \cdots + \frac{r_0}{s^n} = 0_{S^{-1}T},$$

which implies $\frac{a}{s}$ is an integral element over $S^{-1}R$.

□

Lemma 6.6.30 Finite $\implies$ Integral

Let $\varphi : R \to S$ be a finite homomorphism between two commutative rings. Then φ is integral.

Proposition 6.6.31 Equivalent Definition of Finite Ring Homomorphism

Let $\varphi : R \to S$ be a ring homomorphism between two commutative rings. The following are equivalent:

(i) φ is finite.

(ii) φ is integral and of finite type.

(iii) there exist $x_1, \cdots, x_n \in S$ such that $S = R[x_1, \cdots, x_n]$ and each x_i is integral over R.

6.7 Normal Ring

Recall the remark in Definition 6.6.9.

Definition 6.7.1 Normal Domain

Suppose R is an integral domain, $\mathrm{Frac}(R)$ be a field of fractions and $l : R \hookrightarrow \mathrm{Frac}(R)$ is the localization map. R is called **normal** or **integrally closed** if $l(R)$ equals the integral closure of R in $\mathrm{Frac}(R)$.

Proposition 6.7.2 Equivalent Definition of Normal Domain

Let R be an integral domain. The following are equivalent:

(i) R is normal.

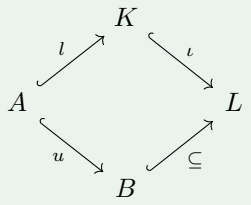
(ii) For each $x \in \mathrm{Frac}(R)$ integral over R, $x \in l(R)$.

(iii) For every prime ideal $\mathfrak{p}$ of R, the localization $R_{\mathfrak{p}}$ is normal.

(iv) For every maximal ideal $\mathfrak{m}$ of R, the localization $R_{\mathfrak{m}}$ is normal.

Proposition 6.7.3

Suppose A is integrally closed commutative ring with fraction field $K = \mathrm{Frac}(A)$ and $l : A \hookrightarrow K$ is the localization map. Let $\iota : K \hookrightarrow L$ be a finite field extension. If $B = \overline{A}^L$ is the integral closure of A in L, then we have commutative diagram



and

$$B \cap \iota(K) = \iota(l(A)).$$

Especially, if we have $A \subseteq K \subseteq L$, then $B \cap K = A$.

Proof. Since for any $a \in A$, there exists monic polynomial $f(x) = x - c \in A[x]$ such that $f(a) = 0$, we have $\iota(l(A)) \subseteq B$. Since $l(A) \subseteq K$, we have $\iota(l(A)) \subseteq \iota(K)$, which implies $\iota(l(A)) \subseteq B \cap \iota(K)$.

For any $b \in B \cap \iota(K)$, since B is the integral closure of A in L, b is integral over A. Since $\iota(K)$ is a field of fractions of A with the localization map $\iota \circ l : A \hookrightarrow \iota(K)$, by the integral closed property of A, any integral element over A in $\iota(K)$ must be in $\iota \circ l(A)$. Hence we have $b \in \iota \circ l(A)$, which implies $B \cap \iota(K) \subseteq \iota \circ l(A)$. Therefore, $B \cap \iota(K) = \iota \circ l(A)$. □

Proposition 6.7.4

Let $\varphi : R \to S$ be a commutative ring homomorphism and $\overline{R}^S$ be the integral closure of R in S. If S is a normal integral domain, then $\overline{R}^S$ is a normal integral domain.

Proof. Let $\overline{R}^S$ be the integral closure of R in S. $\overline{R}^S$ is an integral domain because it is a subring of integral domain S. Suppose $\mathrm{Frac}\left(\overline{R}^S\right)$ is a field of fractions that contains $\overline{R}^S$ and $l : \overline{R}^S \hookrightarrow \mathrm{Frac}\left(\overline{R}^S\right)$ be the localization map. To show $\overline{R}^S$ is normal, by Proposition 6.7.2 it is sufficient to show that for each $x \in \mathrm{Frac}\left(\overline{R}^S\right)$ integral over $\overline{R}^S$, $x \in \overline{R}^S$.

Suppose $x \in \mathrm{Frac}\left(\overline{R}^S\right)$ is integral over $\overline{R}^S$. Let $\mathrm{Frac}\,(S)$ be a field of fractions that contains S. By the universal property of the field of fractions, there exists a unique ring homomorphism

$$\begin{aligned} \overline{\iota} : \mathrm{Frac}\left(\overline{R}^S\right) &\longrightarrow \mathrm{Frac}\,(S) \\ \frac{a}{b} &\longmapsto \frac{a}{b} \end{aligned}$$

such that the following diagram commutes

$$\begin{array}{ccc} \overline{R}^S & \xhookrightarrow{\ \iota\ } & S \\ {\scriptstyle l_1}\downarrow & & \downarrow{\scriptstyle l_2} \\ \mathrm{Frac}\left(\overline{R}^S\right) & \xhookrightarrow[\overline{\iota}]{} & \mathrm{Frac}(S) \end{array}$$

Since l_1 and $l_2 \circ \iota$ are injective, $\overline{\iota}$ is injective. According to Proposition 6.6.12, $\overline{\iota}(x)$ is integral over $\overline{R}^S$ through $\overline{\iota} \circ l_1$, namely $\overline{\iota}(x)$ is integral over $\overline{R}^S$ through $l_2 \circ \iota$. According to Proposition 6.6.6, $\overline{\iota}(x)$ is integral over S. Since S is normal, $\overline{\iota}(x) \in S$. Since $\overline{R}^S$ is integral over S, we have $\overline{\iota}(x)$ is integral over R. Since $\overline{R}^S$ is the integral closure of R in S, we have $\overline{\iota}(x) \in \overline{R}^S$. Therefore, $x \in \overline{R}^S$, which completes the proof. □

Proposition 6.7.5 Characterization of Integrality via Minimal Polynomials

Let R be a normal integral domain and $K = \mathrm{Frac}(R)$ be a field of fractions of R that contains R. If L/K is a field extension, then $\alpha \in L$ is integral over R if and only if the minimal polynomial of α over K has coefficients in R.

Proof. Suppose $\alpha \in L$ is integral over R. Then $\alpha \in L$ is algebraic over K. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ be the minimal polynomial of α over K. Since α is integral over R, there exists a monic polynomial $g(X) = X^m + b_{m-1}X^{m-1} + \cdots + b_0 \in R[X]$ such that $g(\alpha) = 0$. By the definition of the minimal polynomial, $f(X)$ divides $g(X)$ in $K[X]$. Suppose $M = \overline{K(\alpha)}$ is an algebraic closure of $K(\alpha)$ such that $K(\alpha) \subseteq M$. Then f splits into linear factors over M as

$$f(X) = \prod_{i=1}^{n} (X - \alpha_i) \in M[X],$$

with $\alpha = \alpha_k$ for some k. Thus we have $g(\alpha_i) = 0$ for $i = 1, \cdots, n$, which implies $\alpha_1, \cdots, \alpha_n$ are integral over R. By Vieta's formulas, a_i is a symmetric polynomial of $\alpha_1, \cdots, \alpha_n$ for $i = 1, \cdots, n$. Hence a_i are also integral over R. Since R is normal, we have $a_i \in R$ for $i = 1, \cdots, n$, which implies $a \in R$.

Conversely, suppose the minimal polynomial of α over K has coefficients in R. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in R[X]$ be the minimal polynomial of α over K. Since $f(\alpha) = 0$, α is integral over R. □

Definition 6.7.6 Normal Ring

An commutative R is called **normal** if for every prime ideal $\mathfrak{p}$ of R, the localization $R_{\mathfrak{p}}$ is a normal integral domain.

Proposition 6.7.7

A normal ring is integrally closed in its total ring of fractions.

6.8 Japanese Rings

Definition 6.8.1 Japanese Ring

Let R be an integral domain with field of fractions $K = \mathrm{Frac}(R)$.

(i) We say R is **N-1** if the integral closure of R in K is a finitely generated R-module.

(ii) We say R is **N-2** or **Japanese** if for any finite extension L/K, the integral closure of R in L is finite over R.

Remark. By definition, a N-2 ring is N-1. □

Proposition 6.8.2 N-1 and N-2 are Preserved under Localization

Let R be an integral domain and S be a multiplicative set in R. If R is N-1 (resp. N-2), then $S^{-1}R$ is N-1 (resp. N-2).

Proposition 6.8.3

Let R be a Noetherian normal domain with fraction field $K = \mathrm{Frac}(R)$. Let L/K be a finite separable field extension. Then the integral closure of R in L is finite over R.

Proposition 6.8.4

A Noetherian integral domain whose fraction field has characteristic zero is N-1 if and only if it is N-2.

Example 6.8.1 Examples of Japanese Rings

The following types of rings are Nagata rings:

- Dedekind domains with fraction field of characteristic zero.
- $\mathbb{Z}$.
- Fields.
- Noetherian complete local integral domains.
- Polynomial rings over any of the above.

Proof. Proposition 9.2.2 and Example 6.8.2. □

Definition 6.8.5 Nagata Ring

We say a commutative ring R is a **Nagata ring** if R is Noetherian and for every prime ideal $\mathfrak{p}$ of R, $R/\mathfrak{p}$ is a Japanese ring.

Definition 6.8.6 Universally Japanese Ring

We say a commutative ring R is **universally Japanese** if for any finite type ring homomorphism $R \to S$ with S being an integral domain, S is a Japanese ring.

Proposition 6.8.7 Equivalent Characterization of Nagata Ring

Let R be a Noetherian ring. The following are equivalent:

(i) R is a Nagata ring.

(ii) any finite type R-algebra is a Nagata ring.

(iii) R is Noetherian and universally Japanese.

Corollary 6.8.8 Nataga Domain is Japanese

Suppose R is a Nagata ring. Then R is a Japanese ring if and only if it is an integral domain.

Example 6.8.2 Examples of Nagata Rings

The following types of rings are Nagata rings:

- Dedekind domains with fraction field of characteristic zero.
- $\mathbb{Z}$.
- Fields.
- Noetherian complete local rings.
- Finite type ring extensions of any of the above.

6.9 Krull Dimension

Definition 6.9.1 Length of a Chain of Prime Ideals

Let R be a commutative ring and $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ be a chain of prime ideals of R. The **length** of the chain is defined to be n.

Definition 6.9.2 Height of a Prime Ideal

Let R be a commutative ring and $\mathfrak{p}$ be a prime ideal of R. The **height** of $\mathfrak{p}$ is defined to be the supremum of the lengths of all chains of prime ideals of R contained in $\mathfrak{p}$

$$\operatorname{ht}(\mathfrak{p}) = \sup\{n \in \mathbb{N} \mid \exists \text{ a chain of prime ideals } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}\}.$$

Definition 6.9.3 Krull Dimension

Let R be a commutative ring. The **Krull dimension** of R, denoted by $\dim R$, is defined to be the supremum of the heights of all prime ideals of R

$$\dim R = \sup\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec}(R)\} = \sup\{\operatorname{ht}(\mathfrak{m}) \mid \mathfrak{m} \text{ is a maximal ideal of } R\}.$$

Proposition 6.9.4

Let R be a commutative ring and $\mathfrak{p}$ be a prime ideal of R. Then

$$\operatorname{ht}(\mathfrak{p}) = \dim R_{\mathfrak{p}}.$$

Proof. Let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$ be a chain of prime ideals of R. Since $R_{\mathfrak{p}}$ is a local ring, $\mathfrak{p}R_{\mathfrak{p}}$ is the unique maximal ideal of $R_{\mathfrak{p}}$. Then we have a chain of prime ideals of $R_{\mathfrak{p}}$

$$\mathfrak{p}_0R_{\mathfrak{p}} \subsetneq \mathfrak{p}_1R_{\mathfrak{p}} \subsetneq \cdots \subsetneq \mathfrak{p}_nR_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}.$$

That implies $\dim R_{\mathfrak{p}} \geq n$. Since the chain is arbitrary, we have $\dim R_{\mathfrak{p}} \geq \operatorname{ht}(\mathfrak{p})$.

On the other hand, any prime ideal of $R_{\mathfrak{p}}$ is of the form $\mathfrak{q}R_{\mathfrak{p}}$ for some prime ideal $\mathfrak{q}$ of R such that $\mathfrak{q} \subseteq \mathfrak{p} \neq \varnothing$. Suppose $\dim R_{\mathfrak{p}} = m$ and

$$\mathfrak{q}_0R_{\mathfrak{p}} \subsetneq \mathfrak{q}_1R_{\mathfrak{p}} \subsetneq \cdots \subsetneq \mathfrak{q}_{m-1}R_{\mathfrak{p}} \subsetneq \mathfrak{p}R_{\mathfrak{p}}$$

is a chain of prime ideals of $R_{\mathfrak{p}}$. Then we have a chain of prime ideals of R

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_{m-1} \subsetneq \mathfrak{p}$$

That implies $\operatorname{ht}(\mathfrak{p}) \geq m = \dim R_{\mathfrak{p}}$. Thus we have $\dim R_{\mathfrak{p}} = \operatorname{ht}(\mathfrak{p})$. □

6.9.1 Noetherian Local Rings

Definition 6.9.5 Ideal of Definition

Let $(R, \mathfrak{m})$ be a Noetherian local commutative ring. An **ideal of definition** of R is an ideal $\mathfrak{a}$ of R such that $\sqrt{\mathfrak{a}} = \mathfrak{m}$.

Proposition 6.9.6 Krull Dimension of Noetherian Local Rings

Let R be a Noetherian local commutative ring and $d \geq 0$ be an integer. Then the following statements are equivalent:

(i) $\dim R = d$.

(ii) There exists an ideal of definition $\mathfrak{a} = (a_1, \cdots, a_d)$ of R, and no ideal of definition of R is generated by fewer than d elements.

Definition 6.9.7 System of Parameters

Let $(R, \mathfrak{m})$ be a Noetherian local commutative ring. A **system of parameters** of R is a sequence of elements $a_1, \cdots, a_d \in \mathfrak{m}$ such that

$$\sqrt{(a_1, \cdots, a_d)} = \mathfrak{m},$$

that is, $(a_1, \cdots, a_d)$ is an ideal of definition of R.

Definition 6.9.8 Regular Local Ring

Let $(R, \mathfrak{m})$ be a Noetherian local commutative ring of dimension d. R is called a **regular local ring** if there $a_1, \cdots, a_d \in \mathfrak{m}$ such that $(a_1, \cdots, a_d) = \mathfrak{m}$. In this case, $a_1, \cdots, a_d$ is called a **regular system of parameters** of R.

A regular local ring is a field if and only if it has Krull dimension 0. A regular local ring is a DVR if and only if it has Krull dimension 1.

Definition 6.9.9 Regular Ring

Let R be a commutative ring. R is called a **regular ring** if R is a Noetherian ring and for every prime ideal $\mathfrak{p}$ of R, the localization $R_{\mathfrak{p}}$ is a regular local ring.

6.9.2 Artinian Rings

Definition 6.9.10 Artinian Ring

A commutative ring R is called **Artinian** if R satisfies the descending chain condition for ideals: for every chain of ideals

$$\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \mathfrak{a}_3 \supseteq \cdots$$

there exists an integer n such that $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots$.

Proposition 6.9.11 Equivalent Characterization of Artinian Rings

Let R be a Noetherian commutative ring. The following are equivalent:

(i) R is Artinian.

(ii) R has Krull dimension 0.

(iii) $\mathrm{Spec}(R)$ is discrete and finite.

(iv) $\mathrm{Spec}(R)$ is finite.

(v) R is a finite product of Artinian local commutative rings.

Proposition 6.9.12 Artinian Integral Domain is a Field

Let R be an Artinian ring. Then R is a field if and only if R is an integral domain.

Proof. Suppose R is an Artinian integral domain. Suppose $a \in R - \{0\}$ is any nonzero element of R. Then the chain of ideals

$$(a) \supseteq (a^2) \supseteq (a^3) \supseteq \cdots$$

must stabilize at some point, say $(a^n) = (a^{n+1}) = \cdots$. Therefore, there exists $r \in R$ such that $a^n = ra^{n+1}$. Since R is an integral domain, we have $a^n \neq 0$ and $1 = ra$. Thus $a \in R^\times$. This implies R is a field. □

6.10 Dedekind Domain

Definition 6.10.1 Fractional Ideal

Let R be an integral domain. A **fractional ideal** of R is an R-submodule I of $\mathrm{Frac}(R)$ such that there exists a nonzero $r \in R$ such that $rI \subseteq R$.

Proposition 6.10.2 Equivalent Characterization of Fractional Ideal

Let R be an integral domain and I be a subset of $K := \mathrm{Frac}(R)$. The following are equivalent:

(i) I is a fractional ideal of R.

(ii) there exists a nonzero $r \in R$ and an ideal J such that $I = r^{-1}J$.

Proof. (i) $\implies$ (ii). Suppose I is a fractional ideal of R. Then there exists a nonzero $r \in R$ such that $rI \subseteq R$. Let $J = rI$. Since $rI = (r)I$, J is also an ideal of R. And by Lemma 10.1.2 we have $I = (r^{-1}r)I = r^{-1}J$.

(ii) $\implies$ (i). Suppose there exists a nonzero $r \in R$ and an ideal J such that $I = r^{-1}J$. By Proposition 7.3.11 we see $r^{-1}J$ is an R-submodule of K. Since $rI = r(r^{-1}J) = J \subseteq R$, I is a fractional ideal of R.

□

Definition 6.10.3 Dedekind Domain

An integral domain R is called a **Dedekind domain** if every nonzero ideal I of R can be written as a product of prime ideals of R

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

uniquely up to permutation of the $\mathfrak{p}_i$.

Proposition 6.10.4 Equivalent Definition of Dedekind Domain

Let R be a commutative ring. The following are equivalent:

(i) R is a Dedekind domain.

(ii) R is Noetherian domain and for every nonzero maximal ideal $\mathfrak{m}$ of R, the localization $R_{\mathfrak{m}}$ is a DVR.

(iii) R a Noetherian, normal domain, and $\dim R \leq 1$.

(iv) Every non-zero fractional ideal of R is invertible.

(v) For any two ideals I and J,

$$I \subseteq J \iff J \text{ divides } I.$$

Here J divides I means there exists an ideal H such that $I = JH$.

Corollary 6.10.5 Containment and Divisibility of Prime Powers

Let R be a Dedekind domain, $\mathfrak{p}$ be a nonzero prime ideal of R and $n \in \mathbb{Z}_{\geq 1}$. If I is a ideal Then we have

$$\mathfrak{p}^n \subseteq I \iff I = \mathfrak{p}^m \text{ for some } 0 \leq m \leq n$$

and

$$I \subseteq \mathfrak{p}^n \iff I = \mathfrak{p}^m \text{ for some } m \geq n.$$

Here $\mathfrak{p}^0 := (1_R) = R$.

Proof. Suppose $\mathfrak{p}^n \subseteq I$. By Proposition 6.10.4 we have

$$\mathfrak{p}^n = IJ$$

for some ideal J. Suppose I and J has prime ideal factorization,

$$I = \mathfrak{a}_1^{e_1} \cdots \mathfrak{a}_r^{e_r}$$

$$J = \mathfrak{b}_1^{v_1} \cdots \mathfrak{b}_s^{v_s}$$

By the uniqueness of prime ideal factorization, we have $r = s = 1$, $\mathfrak{a}_1 = \mathfrak{b}_1 = \mathfrak{p}$. Thus

$$\mathfrak{p}^n = \mathfrak{p}^{e_1}\mathfrak{p}^{v_1} = \mathfrak{p}^{e_1+v_1} \implies n = e_1 + v_1 \implies 0 \leq e_1 \leq n.$$

□

Proposition 6.10.6 Properties of Dedekind Domains

Let R be a Dedekind domain.

(i) Every nonzero prime ideal of R is maximal.

(ii) If $\mathfrak{p}$ is a maximal ideal of R, then $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ is 1-dimensional $R/\mathfrak{p}$-vector space.

Proof. (i) Suppose $\mathfrak{p}$ is a nonzero prime ideal of R, In an integral domain, (0) is a prime ideal, and we have chain of ideals

$$(0) \subseteq \mathfrak{p}.$$

Since the Krull dimension of R is at most 1, there is no prime ideal strictly between (0) and $\mathfrak{p}$. Thus $\mathfrak{p}$ is maximal.

(ii) Since $\mathfrak{p}^{n+1}$ is an R-submodule of $\mathfrak{p}^n$, the quotient module $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ is an R-module. We need to show that $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ is an $R/\mathfrak{p}$-module.

For any $a \in \mathfrak{p}$ and $x + \mathfrak{p}^{n+1} \in \mathfrak{p}^n/\mathfrak{p}^{n+1}$, we have

$$a\left(x + \mathfrak{p}^{n+1}\right) = ax + \mathfrak{p}^{n+1} = 0 + \mathfrak{p}^{n+1},$$

which implies

$$\mathfrak{p} \subseteq \operatorname{Ann}_R\left(\mathfrak{p}^n/\mathfrak{p}^{n+1}\right).$$

Thus according to Proposition 7.1.7, $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ is an $R/\mathfrak{p}$-module. Since $R/\mathfrak{p}$ is a field, $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ is an $R/\mathfrak{p}$-vector space. Let $W \subseteq \mathfrak{p}^n/\mathfrak{p}^{n+1}$ be any $R/\mathfrak{p}$-subspace. W is also an R-submodule of $\mathfrak{p}^n/\mathfrak{p}^{n+1}$. Since we have the following bijection of sets

$$\begin{aligned}
&\left\{W \,\middle|\, W \text{ is an } R\text{-submodules of } \mathfrak{p}^n/\mathfrak{p}^{n+1}\right\} \\
\longleftrightarrow &\left\{V \,\middle|\, V \text{ is an } R\text{-submodules of } \mathfrak{p}^n \text{ and } \mathfrak{p}^{n+1} \subseteq V\right\} \\
\longleftrightarrow &\left\{V \,\middle|\, V \text{ is an } R\text{-submodules of } R \text{ and } \mathfrak{p}^{n+1} \subseteq V \subseteq \mathfrak{p}^n\right\} \\
\longleftrightarrow &\left\{I \mid I \text{ is an ideal of } R \text{ and } \mathfrak{p}^{n+1} \subseteq I \subseteq \mathfrak{p}^n\right\}
\end{aligned}$$

W corresponds to an ideal I of R such that $\mathfrak{p}^{n+1} \subseteq I \subseteq \mathfrak{p}^n$. By the Corollary 6.10.5, we have $I = \mathfrak{p}^n$ or $I = \mathfrak{p}^{n+1}$. Thus $W = \mathfrak{p}^n/\mathfrak{p}^{n+1}$ or $W = 0$. This implies that $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ is a 1-dimensional $R/\mathfrak{p}$-vector space. □

6.10.1 Extensions of Dedekind Domains

Theorem 6.10.7 Krull-Akizuki Theorem

Let o be a one-dimensional Noetherian integral domain and $K = \operatorname{Frac}(o)$ be its field of fractions. Let L/K be a finite field extension and $\mathcal{O}$ be the integral closure of o in L. Then $\mathcal{O}$ is a Dedekind domain.

Proof. We can prove that $\mathcal{O}$ is integrally closed and that every nonzero prime ideal is maximal. It remains to show that $\mathcal{O}$ is Noetherian. Let $\omega_1, \ldots, \omega_n$ be a basis of L/K which is contained in $\mathcal{O}$. Then the ring $\mathcal{O}_0 = \mathcal{O}[\omega_1, \ldots, \omega_n]$ is a finitely generated $\mathcal{O}$-module and in particular is Noetherian since $\mathcal{O}$ is Noetherian. We argue as before that $\mathcal{O}_0$ is one-dimensional and are thus reduced to the case $L = K$. So let $\mathfrak{A}$ be an ideal of $\mathcal{O}$ and $a \in \mathfrak{A} \cap \mathcal{O}, a \neq 0$; then by the above lemma $\mathcal{O}/a\mathcal{O}$ is a finitely generated $\mathcal{O}$-module. Since $\mathcal{O}$ is Noetherian, so is the $\mathcal{O}$-submodule $\mathfrak{A}/a\mathcal{O}$, and also the $\mathcal{O}$-module $\mathfrak{A}$. □

Proposition 6.10.8

Let o be a Dedekind domain and $K = \operatorname{Frac}(o)$ be its field of fractions. Let L/K be a finite field extension and $\mathcal{O}$ be the integral closure of o in L. If $\mathfrak{p}$ is a prime ideal of o, then $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$, where $\mathfrak{p}\mathcal{O}$ is the ideal of $\mathcal{O}$ generated by $\mathfrak{p}$.
Therefore, if $\mathfrak{p} \neq (0)$, then $\mathfrak{p}\mathcal{O}$ can be factored into a product of prime ideals of $\mathcal{O}$ in a unique way

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

where $\mathfrak{P}_i$ are prime ideals of $\mathcal{O}$. Moreover, $\mathfrak{P}_i$ are exactly those prime ideals of $\mathcal{O}$ lying over $\mathfrak{p}$.

Remark. In other words, $\mathfrak{P}_i$ are exactly those prime ideals in $\operatorname{Spec}(\mathcal{O})$ such that $\iota^{-1}(\mathfrak{P}_i) = \mathfrak{p}$, where $\iota : \mathcal{o} \hookrightarrow \mathcal{O}$ is the embedding. Consider the morphism of affine schemes $\iota^{-1} : \operatorname{Spec}(\mathcal{O}) \to \operatorname{Spec}(\mathcal{o})$. By Proposition 6.6.13 we see ι^{-1} is surjective as a map between the underlying sets. This is equivalent to say the fiber over $\mathfrak{p}$ is $\{\mathfrak{P}_1, \cdots, \mathfrak{P}_n\}$. □

Proof. Since $\mathcal{o} \subseteq \mathcal{O}$ is an integral extension, by the going-up theorem, if $\mathfrak{p}$ is a prime ideal of $\mathcal{o}$, then there exists a prime ideal $\mathfrak{P}$ of $\mathcal{O}$ such that $\mathfrak{P} \cap \mathcal{o} = \mathfrak{p}$. Thus we have

$$\mathfrak{p}\mathcal{O} \subseteq \mathfrak{P}\mathcal{O} = \mathfrak{P} \subsetneq \mathcal{O}.$$

By Theorem 6.10.7, $\mathcal{O}$ is a Dedekind domain. If $\mathfrak{p} \neq 0$, $\mathfrak{p}\mathcal{O}$ is a nonzero proper ideal of $\mathcal{O}$ and $\mathfrak{p}\mathcal{O}$ is a product of prime ideals of $\mathcal{O}$

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

Since we have

$$\mathfrak{p} \subseteq \mathfrak{p}\mathcal{O} \subseteq \mathfrak{P}_k$$

for $1 \leq k \leq r$, we have $\mathfrak{p} \subseteq \mathfrak{P}_k \cap \mathcal{o}$ for $1 \leq k \leq r$. From Corollary 6.1.9 we see $\mathfrak{P}_k \cap \mathcal{o}$ are prime ideals of $\mathcal{o}$. Since nonzero prime ideals of $\mathcal{o}$ are maximal, we have $\mathfrak{P}_k \cap \mathcal{o} = \mathfrak{p}$ for $1 \leq k \leq r$. Thus $\mathfrak{P}_k$ are prime ideals of $\mathcal{O}$ lying over $\mathfrak{p}$.

Conversely, if $\mathfrak{q}$ is any prime ideal of $\mathcal{O}$ lying over $\mathfrak{p}$, then $\mathfrak{q} \cap \mathcal{o} = \mathfrak{p}$, which implies

$$\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} = \mathfrak{p}\mathcal{O} \subseteq \mathfrak{q}\mathcal{O} = \mathfrak{q}.$$

According to Proposition 6.1.23, there exists some $1 \leq k \leq r$ such that $\mathfrak{P}_k \subseteq \mathfrak{q}$. Since $\mathfrak{P}_k$ is maximal, we have $\mathfrak{q} = \mathfrak{P}_k$. □

Definition 6.10.9 Ramification Index

Let $\mathcal{o}$ be a Dedekind domain and $K = \operatorname{Frac}(\mathcal{o})$ be its field of fractions. Let L/K be a finite field extension and $\mathcal{O}$ be the integral closure of $\mathcal{o}$ in L. Suppose $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{o}$, and $\mathfrak{p}\mathcal{O}$ can be factored into a product of prime ideals of $\mathcal{O}$

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

then e_i is called the **ramification index** of $\mathfrak{P}_i$ over $\mathfrak{p}$. For each $1 \leq m \leq r$, we have a canonical field extension

$$\begin{aligned} \mathcal{o}/\mathfrak{p} &\hookrightarrow \mathcal{O}/\mathfrak{P}_m \\ a + \mathfrak{p} &\mapsto a + \mathfrak{P}_m. \end{aligned}$$

Let $\kappa(\mathfrak{p}) = \mathcal{o}/\mathfrak{p}$, $\kappa(\mathfrak{P}_m) = \mathcal{O}/\mathfrak{P}_m$. The degree of the field extension $\kappa(\mathfrak{P}_m)/\kappa(\mathfrak{p})$ is called the **inertia degree** of $\mathfrak{P}_m$ over $\mathfrak{p}$, denoted by

$$f_m = [\kappa(\mathfrak{P}_m) : \kappa(\mathfrak{p})] = [\mathcal{O}/\mathfrak{P}_m : \mathcal{o}/\mathfrak{p}].$$

- The prime ideal $\mathfrak{P}_m$ is called **unramified over** $\mathcal{o}$ if $e_m = 1$ and the field extension $\mathcal{o}/\mathfrak{p} \hookrightarrow \mathcal{O}/\mathfrak{P}_m$ is separable.
- The prime ideal $\mathfrak{P}_m$ is called **ramified over** $\mathcal{o}$ if it is not unramified.
- The prime ideal $\mathfrak{P}_m$ is called **totally ramified over** $\mathcal{o}$ if it is ramified and $f_m = 1$.
- The prime ideal $\mathfrak{p}$ is called **unramified in** L if all $\mathfrak{P}_m$ are unramified.
- The prime ideal $\mathfrak{p}$ is called **ramified in** L if it is not unramified in L.
- The field extension L/K is called **unramified** if all prime ideals of $\mathcal{o}$ are unramified in L.

Remark. By Proposition 6.6.29, if $\mathcal{o} \hookrightarrow \mathcal{O}$ is a finite ring homomorphism, then $\kappa(\mathfrak{P}_m)/\kappa(\mathfrak{p})$ is a finite field extension. □

Proof. By the universal property of quotient ring, since

$$\ker(\pi_k \circ \iota) = \iota^{-1}(\mathfrak{P}_k) = \mathfrak{P}_k \cap \mathcal{o} = \mathfrak{p},$$

there exists a unique ring homomorphism $\mathfrak{o}/\mathfrak{p} \to \mathcal{O}/\mathfrak{P}_k$ such that the following diagram commutes

$$\begin{array}{ccc} \mathfrak{o} & \xhookrightarrow{\iota} & \mathcal{O} \\ \downarrow & & \downarrow{\scriptstyle \pi_k} \\ \mathfrak{o}/\mathfrak{p} & \dashrightarrow & \mathcal{O}/\mathfrak{P}_k \end{array}$$

Since both $\mathfrak{o}/\mathfrak{p}$ and $\mathcal{O}/\mathfrak{P}_k$ are fields, $\mathfrak{o}/\mathfrak{p} \to \mathcal{O}/\mathfrak{P}_k$ is a field extension. □

Proposition 6.10.10 Fundamental Identity

Let $\mathfrak{o}$ be a Dedekind domain with field of fractions $K = \mathrm{Frac}(\mathfrak{o})$. Let L/K be a finite separable field extension and $\mathcal{O}$ be the integral closure of $\mathfrak{o}$ in L. Suppose $\mathfrak{p}$ is a nonzero prime ideal of $\mathfrak{o}$, and $\mathfrak{p}\mathcal{O}$ can be factored into a product of prime ideals of $\mathcal{O}$

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

then we have the fundamental identity

$$\sum_{i=1}^{r} e_i f_i = [L : K].$$

Definition 6.10.11 Split Completely

Let $\mathfrak{o}$ be a Dedekind domain with field of fractions $K = \mathrm{Frac}(\mathfrak{o})$. Let L/K be a finite separable field extension and $\mathcal{O}$ be the integral closure of $\mathfrak{o}$ in L. Suppose $\mathfrak{p}$ is a nonzero prime ideal of $\mathfrak{o}$, and $\mathfrak{p}\mathcal{O}$ can be factored into a product of prime ideals of $\mathcal{O}$

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

- $\mathfrak{p}$ is said to **split completely in** L if $[L : K] = r$, or equivalently, $e_m = 1$ and $f_m = 1$ for all $m = 1, \cdots, r$.
- $\mathfrak{p}$ is called **nonsplit in** L if $r = 1$.
- $\mathfrak{p}$ is called **inert in** L if $r = e_1 = 1$.

Proposition 6.10.12

Let $\mathfrak{o}$ be a Dedekind domain with field of fractions $K = \mathrm{Frac}(\mathfrak{o})$. Let L/K be a finite separable field extension and $\mathcal{O}$ be the integral closure of $\mathfrak{o}$ in L. Then there are only finitely many prime ideals of $\mathfrak{o}$ which are ramified in L.

6.10.2 Ramification Theory

Lemma 6.10.13 Galois Group Maps Integral Elements to Integral Elements

Let $\mathfrak{o}$ be a Dedekind domain with field of fractions $K = \mathrm{Frac}(\mathfrak{o})$. Let L/K be a finite Galois extension and $\mathcal{O}$ be the integral closure of $\mathfrak{o}$ in L. For any $\sigma \in \mathrm{Gal}(L/K)$, we have $\sigma(\mathcal{O}) \subseteq \mathcal{O}$.

Proof. Take any $\alpha \in \mathcal{O}$, α is integral over $\mathfrak{o}$. So there exists a monic polynomial $f(x) \in \mathfrak{o}[x]$ such that $f(\alpha) = 0$. Since σ is a ring homomorphism, we have

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0.$$

Thus $\sigma(\alpha)$ is integral over $\mathfrak{o}$, which means $\sigma(\alpha) \in \mathcal{O}$. □

Proposition 6.10.14 Galois Group Acts on $\mathcal{O}$

Let $\mathfrak{o}$ be a Dedekind domain with field of fractions $K = \mathrm{Frac}(\mathfrak{o})$. Let L/K be a finite Galois extension and $\mathcal{O}$ be the integral closure of $\mathfrak{o}$ in L. Then the Galois group $G := \mathrm{Gal}(L/K)$ acts on $\mathcal{O}$ through the

following group homomorphism

$$\begin{aligned} \mathrm{Gal}(L/K) &\longrightarrow \mathrm{Aut}_{\mathcal{O}\text{-}\mathsf{Alg}}(\mathcal{O}) \\ \sigma &\longmapsto \sigma|_{\mathcal{O}}, \end{aligned}$$

which makes $\mathcal{O}$ an $\mathcal{O}[G]$-module.

Proof. For any $\sigma \in \mathrm{Gal}(L/K)$, we have $\sigma(\mathcal{O}) \subseteq \mathcal{O}$ and $\sigma^{-1}(\mathcal{O}) \subseteq \mathcal{O}$ by the Lemma 6.10.13. Thus $\mathcal{O} = \sigma(\sigma^{-1}(\mathcal{O})) \subseteq \sigma(\mathcal{O})$, which implies $\sigma(\mathcal{O}) = \mathcal{O}$. Since σ is an $\mathcal{O}$-algebra automorphism of L, $\sigma|_{\mathcal{O}}$ is an $\mathcal{O}$-algebra ring automorphism of $\mathcal{O}$. Suppose $\iota : \mathcal{O} \hookrightarrow L$ is the inclusion map. For any $\sigma, \tau \in \mathrm{Gal}(L/K)$, we have

$$(\sigma \circ \tau)|_{\mathcal{O}} = \sigma \circ \tau \circ \iota = \sigma|_{\mathcal{O}} \circ \tau \circ \iota = \sigma|_{\mathcal{O}} \circ \tau|_{\mathcal{O}},$$

which means the map is a group homomorphism. □

Lemma 6.10.15 Prime Avoidance Lemma

Let R be a commutative ring and $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be ideals of R. Suppose E is a additive subgroup of R such that for any $x, y \in E$, $xy \in E$. If

(i) all but two of $\mathfrak{p}_1$ are prime ideals of R,

(ii) $E \not\subseteq \mathfrak{p}_m$ for $1 \leq m \leq n$,

then we have

$$E \not\subseteq \bigcup_{m=1}^{n} \mathfrak{p}_m,$$

which means there exists $x \in E$ such that $x \notin \mathfrak{p}_m$ for any $m = 1, \cdots, n$.

Since we have category isomorphism

$$\mathcal{O}\text{-}\mathsf{CAlg} \cong \mathcal{O}\text{-}\mathsf{AffSch}^{\mathrm{op}},$$

we can also view the action of $\mathrm{Gal}(L/K)$ on $\mathcal{O}$ as an action on $\mathrm{Spec}(\mathcal{O})$.

Proposition 6.10.16 Galois Group Acts on $\mathrm{Spec}(\mathcal{O})$

Let $\mathcal{O}$ be a Dedekind domain with field of fractions $K = \mathrm{Frac}(\mathcal{O})$. Let L/K be a finite Galois extension and $\mathcal{O}$ be the integral closure of $\mathcal{O}$ in L. Then the Galois group $\mathrm{Gal}(L/K)$ acts on $\mathrm{Spec}(\mathcal{O})$ through the following group homomorphism

$$\begin{aligned} \mathrm{Gal}(L/K) &\longrightarrow \mathrm{Aut}_{\mathcal{O}\text{-}\mathsf{AffSch}}(\mathrm{Spec}(\mathcal{O})) \\ \sigma &\longmapsto (\mathfrak{P} \longmapsto \sigma(\mathfrak{P})) \end{aligned}$$

The orbits of this action are the prime ideals of $\mathcal{O}$ lying over the same prime ideal $\mathfrak{p}$ of $\mathcal{O}$. This means the action is transitive on all prime ideals of $\mathcal{O}$ lying over the same prime ideal $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$.

Proof. For any $\sigma, \tau \in \mathrm{Gal}(L/K)$ and any prime ideal $\mathfrak{P}$ of $\mathcal{O}$, we have

$$\sigma(\tau(\mathfrak{P})) = (\sigma \circ \tau)(\mathfrak{P}),$$

which means the map is a group homomorphism. If $\mathfrak{P}$ is a prime ideal of $\mathcal{O}$ lying over a prime ideal $\mathfrak{p}$ of $\mathcal{O}$, then by Proposition 1.3.1 we have

$$\sigma(\mathfrak{P}) \cap \mathcal{O} = \sigma(\mathfrak{P}) \cap \sigma(\mathcal{O}) = \sigma(\mathfrak{P} \cap \mathcal{O}) = \sigma(\mathfrak{p}) = \mathfrak{p},$$

which means each orbit of this action can only contain prime ideals of $\mathcal{O}$ lying over the same prime ideal $\mathfrak{p}$ of $\mathcal{O}$.

Use the incomparability property of integral extensions, we see (0) is the only prime ideal of $\mathcal{O}$ lying over (0). Thus the action of $\mathrm{Gal}(L/K)$ on (0) is trivial.

Every nonzero prime ideal of a Dedekind domain is a maximal ideal. Let $\mathfrak{P}$ and $\mathfrak{P}'$ be maximal ideals of $\mathcal{O}$ lying over maximal ideal $\mathfrak{p} \in \mathrm{Spec}\,\mathcal{O}$. Suppose $\mathfrak{P}$ and $\mathfrak{P}'$ are not in the same orbit. Then for any $\sigma \in \mathrm{Gal}(L/K)$,

we have $\sigma(\mathfrak{P}) \neq \mathfrak{P}'$. Note ring isomorphism maps maximal ideals to maximal ideals. By maximality of $\sigma(\mathfrak{P})$, we have $\mathfrak{P}' \not\subseteq \sigma(\mathfrak{P})$ for all $\sigma \in \mathrm{Gal}(L/K)$. By the Lemma 6.10.15, there exists $x \in \mathfrak{P}'$ such that $x \notin \sigma(\mathfrak{P})$ for all $\sigma \in \mathrm{Gal}(L/K)$.

Since $\mathrm{id} \in \mathrm{Gal}(L/K)$,

$$N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) = x \prod_{\sigma \in \mathrm{Gal}(L/K) - \{\mathrm{id}\}} \sigma(x) \in \mathfrak{P}'.$$

By the property of norm we see $N_{L/K}(x) \in K$. Since Dedekind domains are integral closed, by Proposition 6.7.3 we have $\mathcal{O} \cap K = \mathcal{o}$. Combining with $\mathfrak{P}' \subseteq \mathcal{O}$ we get $N_{L/K}(x) \in \mathcal{O} \cap K = \mathcal{o}$. Hence we get

$$N_{L/K}(x) \in \mathfrak{P}' \cap \mathcal{o} = \mathfrak{p} \subseteq \mathfrak{P}.$$

Since $\mathfrak{P}$ is a prime ideal, there exists some $\tau \in \mathrm{Gal}(L/K)$ such that $\tau(x) \in \mathfrak{P}$, which means $x \in \tau^{-1}(\mathfrak{P})$. This contradicts the fact that $x \notin \sigma(\mathfrak{P})$ for all $\sigma \in \mathrm{Gal}(L/K)$. Thus $\mathfrak{P}$ and $\mathfrak{P}'$ are in the same orbit. □

Definition 6.10.17 Decomposition Group

Let $\mathcal{o}$ be a Dedekind domain with field of fractions $K = \mathrm{Frac}(\mathcal{o})$. Let L/K be a finite Galois extension and $\mathcal{O}$ be the integral closure of $\mathcal{o}$ in L. According to Proposition 6.10.16, the Galois group $\mathrm{Gal}(L/K)$ acts on $\mathrm{Spec}\,(\mathcal{O})$. Suppose $\mathfrak{P} \in \mathrm{Spec}\,(\mathcal{O})$, then the stabilizer subgroup of $\mathfrak{P}$ under this action is called the **decomposition group** of $\mathfrak{P}$, denoted by

$$D_{\mathfrak{P}} := \mathrm{Stab}_{\mathrm{Gal}(L/K)}(\mathfrak{P}) = \{\sigma \in \mathrm{Gal}(L/K) \,|\, \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

$D_{\mathfrak{P}}$ as a subgroup of $\mathrm{Gal}(L/K)$ also acts on L, and the $D_{\mathfrak{P}}$-invariant elements of L form a subfield of L, called the **decomposition field** of $\mathfrak{P}$, denoted by

$$L^{D_{\mathfrak{P}}} = \{x \in L \,|\, \sigma(x) = x \text{ for all } \sigma \in D_{\mathfrak{P}}\}.$$

Proposition 6.10.18 Decomposition Groups for Prime Ideals over $\mathfrak{p}$ are Conjugate

Let $\mathcal{o}$ be a Dedekind domain with field of fractions $K = \mathrm{Frac}(\mathcal{o})$. Let L/K be a finite Galois extension and $\mathcal{O}$ be the integral closure of $\mathcal{o}$ in L. For any $\sigma \in \mathrm{Gal}(L/K)$ and any $\mathfrak{P} \in \mathrm{Spec}\,(\mathcal{O})$, we have

$$D_{\sigma(\mathfrak{P})} = \sigma D_{\mathfrak{P}} \sigma^{-1}.$$

Proof. This is a direct consequence of Proposition 4.4.13. □

Lemma 6.10.19 Galois Action Induces Isomorphism of Residue Fields

Let $\mathcal{o}$ be a Dedekind domain with field of fractions $K = \mathrm{Frac}(\mathcal{o})$. Let L/K be a finite Galois extension and $\mathcal{O}$ be the integral closure of $\mathcal{o}$ in L. Suppose $\mathfrak{P}$ is a maximal ideal over $\mathfrak{p} \in \mathrm{Spec}\,(\mathcal{o})$.

(i) If $\sigma \in \mathrm{Gal}(L/K)$, then there exists a unique field isomorphism

$$\begin{aligned} \widetilde{\sigma} : \mathcal{O}/\mathfrak{P} &\longrightarrow \mathcal{O}/\sigma\mathfrak{P} \\ a + \mathfrak{P} &\longmapsto \sigma(a) + \sigma\mathfrak{P} \end{aligned}$$

such that the following diagram commutes

$$\begin{array}{ccc} \mathcal{O} & \xrightarrow{\sigma|_{\mathcal{o}}} & \mathcal{O} \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \pi'} \\ \mathcal{O}/\mathfrak{P} & \xrightarrow[\widetilde{\sigma}]{} & \mathcal{O}/\sigma\mathfrak{P} \end{array}$$

(ii) If $\sigma \in D_{\mathfrak{P}}$, then there exists a unique $\mathcal{o}/\mathfrak{p}$-field automorphism

$$\begin{aligned} \widetilde{\sigma} : \mathcal{O}/\mathfrak{P} &\longrightarrow \mathcal{O}/\mathfrak{P} \\ a + \mathfrak{P} &\longmapsto \sigma(a) + \mathfrak{P} \end{aligned}$$

such that the following diagram commutes

$$\begin{array}{ccc} \mathcal{O} & \xrightarrow{\sigma|_{\mathcal{O}}} & \mathcal{O} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ \mathcal{O}/\mathfrak{P} & \xrightarrow[\widetilde{\sigma}]{} & \mathcal{O}/\mathfrak{P} \end{array}$$

Proof. (i) Suppose $\sigma \in \mathrm{Gal}(L/K)$. Since

$$\ker\left(\pi' \circ \sigma|_{\mathcal{O}}\right) = \sigma^{-1}(\sigma\mathfrak{P}) = \mathfrak{P},$$

by the universal property of quotient ring $\mathcal{O}/\mathfrak{P}$, there exists a unique ring homomorphism

$$\begin{aligned} \widetilde{\sigma} : \mathcal{O}/\mathfrak{P} &\longrightarrow \mathcal{O}/\sigma\mathfrak{P} \\ a + \mathfrak{P} &\longmapsto \sigma(a) + \sigma\mathfrak{P} \end{aligned}$$

such that the following diagram commutes

$$\begin{array}{ccc} \mathcal{O} & \xrightarrow{\sigma|_{\mathcal{O}}} & \mathcal{O} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ \mathcal{O}/\mathfrak{P} & \xrightarrow[\widetilde{\sigma}]{} & \mathcal{O}/\sigma\mathfrak{P} \end{array}$$

Furthermore, the surjectivity of $\pi' \circ \sigma|_{\mathcal{O}}$ and $\ker\left(\pi' \circ \sigma|_{\mathcal{O}}\right) = \mathfrak{P}$ implies $\widetilde{\sigma}$ is a an isomorphism of fields.

(ii) If $\sigma \in D_{\mathfrak{P}}$, then $\sigma(\mathfrak{P}) = \mathfrak{P}$. For any $x \in \mathcal{O}$, we have

$$\widetilde{\sigma}\left(x + \mathfrak{P}\right) = \sigma(x) + \sigma\mathfrak{P} = x + \mathfrak{P},$$

which means $\widetilde{\sigma}$ is an $\mathcal{O}/\mathfrak{p}$-automorphism of $\mathcal{O}/\mathfrak{P}$, namely $\widetilde{\sigma} \in \mathrm{Aut}_{(\kappa(\mathfrak{p})/\mathsf{Field})}\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right)$.

□

Proposition 6.10.20 Ramification Index and Inertia Degree for finite Galois Extension

Let $\mathcal{O}$ be a Dedekind domain with field of fractions $K = \mathrm{Frac}(\mathcal{O})$. Let L/K be a finite Galois extension and $\mathcal{O}$ be the integral closure of $\mathcal{O}$ in L. Suppose $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}$, and $\mathfrak{p}\mathcal{O}$ can be factored as

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

Let $G = \mathrm{Gal}(L/K)$. Then we have

$$e_1 = e_2 = \cdots = e_r = e, \quad f_1 = f_2 = \cdots = f_r = f, \quad [L:K] = efr,$$

and

$$\mathfrak{p}\mathcal{O} = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e = \left(\prod_{G\cdot\mathfrak{P}\in G\backslash\mathrm{Spec}(\mathcal{O})} \mathfrak{P}\right)^e.$$

For any $m \in \{1, \cdots, r\}$, by orbit-stabilizer theorem, we have

$$\frac{|G|}{|D_{\mathfrak{P}_m}|} = |G \cdot \mathfrak{P}_m| = r \text{ and } |D_{\mathfrak{P}_m}| = ef.$$

So the decomposition group $D_{\mathfrak{P}_m}$ characterizes splitting behavior of $\mathfrak{p}$ in L:

$$\begin{aligned} D_{\mathfrak{P}_m} = \{\mathrm{id}\} &\iff L^{D_{\mathfrak{P}_m}} = L \iff \mathfrak{p} \text{ splits completely in } L, \\ D_{\mathfrak{P}_m} = G &\iff L^{D_{\mathfrak{P}_m}} = K \iff \mathfrak{p} \text{ is nonsplit in } L. \end{aligned}$$

Proof. According to Lemma 6.10.19, $[\mathcal{O}/\sigma\mathfrak{P} : \mathfrak{o}/\mathfrak{p}]$ is independent of σ, which implies

$$f_1 = f_2 = \cdots = f_r = f.$$

According to Proposition 6.1.22, for any $\sigma \in \mathrm{Gal}(L/K)$, we have

$$\sigma(\mathfrak{p}\mathcal{O}) = \sigma\left(\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}\right) = \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_r)^{e_r}.$$

Since σ fix K, we have

$$\begin{aligned}
\sigma(\mathfrak{p}\mathcal{O}) &= \sigma\left(\left\{\sum_{i=1}^{n} a_i x_i \,\middle|\, n \in \mathbb{Z}_+, a_i \in \mathfrak{p}, x_i \in \mathcal{O}\right\}\right) \\
&= \left\{\sum_{i=1}^{n} \sigma(a_i)\sigma(x_i) \,\middle|\, n \in \mathbb{Z}_+, a_i \in \mathfrak{p}, x_i \in \mathcal{O}\right\} \\
&= \left\{\sum_{i=1}^{n} a_i \sigma(x_i) \,\middle|\, n \in \mathbb{Z}_+, a_i \in \mathfrak{p}, x_i \in \mathcal{O}\right\} \\
&\subseteq \mathfrak{p}\mathcal{O}.
\end{aligned}$$

Note

$$\sigma^{-1}(\mathfrak{p}\mathcal{O}) \subseteq \mathfrak{p}\mathcal{O} \implies \mathfrak{p}\mathcal{O} \subseteq \sigma(\mathfrak{p}\mathcal{O}).$$

We have

$$\sigma(\mathfrak{p}\mathcal{O}) = \mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} = \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_r)^{e_r}.$$

For any $1 \leq m \leq r$, there exists some $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}_m) = \mathfrak{P}_1$. By the uniqueness of prime factorization, there must be $e_m = e_1$. Thus we proved

$$e_1 = e_2 = \cdots = e_r = e.$$

□

Proposition 6.10.21

Let $\mathfrak{o}$ be a normal integral domain with fraction field K. Let L/K be a (possibly infinite) Galois extension. Let $G = \mathrm{Gal}(L/K)$ and let $\mathcal{O}$ be the integral closure of $\mathfrak{o}$ in L.

(i) For any two primes $\mathfrak{P}, \mathfrak{P}' \in \mathrm{Spec}(\mathcal{O})$ lying over the same prime in $\mathfrak{o}$, there exists a $\sigma \in G$ with $\sigma(\mathfrak{P}) = \mathfrak{P}'$.

(ii) Let $\mathfrak{P} \in \mathrm{Spec}(\mathcal{O})$ be a prime lying over $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{o})$. Then $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is an algebraic normal field extension and the map

$$D_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{q}\} \longrightarrow \mathrm{Aut}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$$

is surjective.

Proof. https://stacks.math.columbia.edu/tag/0BRK □

This proposition enables us to define the inertia group.

Definition 6.10.22 Inertia Group

Let $\mathfrak{o}$ be a Dedekind domain with field of fractions $K = \mathrm{Frac}(\mathfrak{o})$. Let L/K be a finite Galois extension and $\mathcal{O}$ be the integral closure of $\mathfrak{o}$ in L. Suppose $\mathfrak{P}$ is a maximal ideal over $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{o})$. The **inertia group** of $\mathfrak{P}$ is defined as the kernel of the surjective group homomorphism

$$\begin{aligned}
\xi : D_{\mathfrak{P}} &\longrightarrow \mathrm{Aut}_{(\kappa(\mathfrak{p})/\mathsf{Field})}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \\
\sigma &\longmapsto \widetilde{\sigma}.
\end{aligned}$$

denote by $I_{\mathfrak{P}} := \ker \xi$. And we have the following exact sequence

$$1 \longrightarrow I_{\mathfrak{P}} \longrightarrow D_{\mathfrak{P}} \longrightarrow \mathrm{Aut}\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right) \longrightarrow 1.$$

Therefore, the decomposition group $D_{\mathfrak{P}}$ controls the splitting behavior of $\mathfrak{p}$ in L, with size $|D_{\mathfrak{P}}| = ef$. If we further assume that $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is a finite separable extension, then $\mathrm{Aut}\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right) = \mathrm{Gal}\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right)$ and $|\mathrm{Gal}\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right)| = f$. Thus by the exact sequence, the inertia group $I_{\mathfrak{P}}$ has size $|I_{\mathfrak{P}}| = e$. In this case, the inertia group $I_{\mathfrak{P}}$ measures the ramification of $\mathfrak{p}$ in L, while $\mathrm{Gal}\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right)$ measures the inertia.

Definition 6.10.23 Frobenius Element

Let $\mathcal{o}$ be a Dedekind domain with field of fractions $K = \mathrm{Frac}(\mathcal{o})$. Let L/K be a finite Galois extension and $\mathcal{O}$ be the integral closure of $\mathcal{o}$ in L. Suppose $\mathfrak{P}$ is a maximal ideal over $\mathfrak{p} \in \mathrm{Spec}\left(\mathcal{o}\right)$ and $\kappa(\mathfrak{p})$ is a finite field isomorphic to $\mathbb{F}_q$. Then $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is a finite Galois extension and we have the following exact sequence

$$1 \longrightarrow I_{\mathfrak{P}} \longrightarrow D_{\mathfrak{P}} \xrightarrow{\xi} \mathrm{Gal}\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right) \longrightarrow 1.$$

- The set of **Frobenius elements** for $\mathfrak{P}$ is defined as the preimage of the Frobenius automorphism of $\mathrm{Fr}_q : x \mapsto x^q$ in $\mathrm{Gal}\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right)$, denoted by $\mathrm{Frob}_{\mathfrak{p},\mathfrak{P}} := \xi^{-1}\left(\mathrm{Fr}_q\right)$.
- The **Frobenius conjugacy class** for a Frobenius element $\sigma \in \mathrm{Frob}_{\mathfrak{p},\mathfrak{P}}$ is defined as the conjugacy class of σ in $\mathrm{Gal}(L/K)$. $\sigma \in \mathrm{Frob}_{\mathfrak{p},\mathfrak{P}}$ if and only if $\tau\sigma\tau^{-1} \in \mathrm{Frob}_{\mathfrak{p},\tau\mathfrak{P}}$ for some $\tau \in \mathrm{Gal}(L/K)$.
- If $I_{\mathfrak{P}}$ is trivial, then $\mathfrak{p}$ is unramified in L and the Frobenius element $\mathrm{Frob}_{\mathfrak{p},\mathfrak{P}}$ is unique. We denote the Frobenius conjugacy class of $\mathrm{Frob}_{\mathfrak{p},\mathfrak{P}}$ by $\mathrm{Frob}_{\mathfrak{p},L}$ or $\mathrm{Frob}_{\mathfrak{p}}$ for short.
- If $I_{\mathfrak{P}}$ is trivial and L/K is Abelian, then the Frobenius conjugacy class $\mathrm{Frob}_{\mathfrak{p},L}$ has only one element, which is called the **Frobenius element** of $\mathfrak{p}$ in L.

6.11 Absolute Value

Definition 6.11.1 Absolute Value on an Integral Ring

Let R be an integral ring. An **absolute value** on R is a function $|\cdot| : R \to \mathbb{R}_{\geq 0}$ satisfying the following properties:

(i) (positive definiteness) $|a| = 0 \iff a = 0$.

(ii) (multiplicativity) $|ab| = |a||b|$.

(iii) (triangle inequality) $|a + b| \leq |a| + |b|$.

An absolute value on R induces a metric (and thus a topology) by

$$d(a, b) = |a - b|,$$

which makes $(R, |\cdot|)$ a topological ring.

Definition 6.11.2 Equivalent Absolute Value

Let R be an integral ring and $|\cdot|, |\cdot|'$ be two absolute values on R. $|\cdot|$ and $|\cdot|'$ are called **equivalent** if they induce the same topology on R.

Definition 6.11.3 Trivial Absolute Value

Let R be an integral ring. The **trivial absolute value** on R is defined by

$$|a| = \begin{cases} 0, & a = 0_R \\ 1, & a \neq 0_R \end{cases}$$

On a finite field, the trivial absolute value is the only absolute value.

Definition 6.11.4 Archimedean Absolute Value

If an absolute value $|\cdot|$ satisfies the stronger property

$$|a+b| \leq \max\{|a|, |b|\},$$

then $|\cdot|$ is called an **non-Archimedean absolute value**. Otherwise, $|\cdot|$ is called an **Archimedean absolute value**.

Proposition 6.11.5

Let R be an integral ring and $|\cdot|$ be an absolute value on R. Then $|\cdot|$ is non-Archimedean if and only if $\{|n1_R| : n \in \mathbb{Z}\}$ is bounded.

Proof. Suppose $|\cdot|$ is non-Archimedean. Then for any $n \in \mathbb{Z}$, we have

$$|n1_R| = |1_R + \cdots + 1_R| \leq \max\{|1_R|, \cdots, |1_R|\} = |1_R| = 1.$$

Thus $\{|n1_R| : n \in \mathbb{Z}\}$ is bounded.
Conversely, suppose $\{|n1_R| : n \in \mathbb{Z}\}$ is bounded by M. Then for any $a, b \in R$, we have

$$\begin{aligned}
|a+b|^n &= |(a+b)^n| \\
&= \left|\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}\right| \\
&\leq \sum_{i=0}^{n} \left|\binom{n}{i} 1_R\right| |a|^i |b|^{n-i} \\
&\leq \sum_{i=0}^{n} M \max\{|a|, |b|\}^i \max\{|a|, |b|\}^{n-i} \\
&= (n+1) M \max\{|a|, |b|\}^n.
\end{aligned}$$

As $n \to \infty$, we have

$$|a+b| \leq ((n+1)M)^{\frac{1}{n}} \max\{|a|, |b|\} \to \max\{|a|, |b|\}.$$

Thus $|\cdot|$ is non-Archimedean. □

6.12 Valuation Ring

Definition 6.12.1 Dominance of Local Rings

A local ring S is said to **dominate** another local ring R if one of the following equivalent condition holds

(i) $R \subseteq S$ and $\mathfrak{m}_R = \mathfrak{m}_S \cap R$, where $\mathfrak{m}_R$ and $\mathfrak{m}_S$ are the maximal ideals of R and S respectively.

(ii) The inclusion map $i : R \hookrightarrow S$ is a local ring homomorphism.

Definition 6.12.2 Valuation Ring

Suppose R is an integral domain and has field of fractions $K = \mathrm{Frac}\,(R)$. We say R is a **valuation ring** if R satisfies one of the following equivalent conditions:

(i) For every $x \in K^\times$, either $x \in R$ or $x^{-1} \in R$.

(ii) The ideals of R are totally ordered by inclusion.

(iii) The principal ideals of R are totally ordered by inclusion (i.e. the elements in R are, up to units, totally ordered by divisibility.)

(iv) R is a local ring and R is maximal among all local rings contained in K partially ordered by dominance.

(v) There is a totally ordered abelian group $(\Gamma, \leq)$ and a valuation $v : K \to \Gamma \cup \{\infty\}$ such that R is the valuation ring of v, i.e.
$$R = \mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}.$$

Proof. The equivalence of these conditions can be shown as follows.

- (i) $\Longrightarrow$ (ii). Suppose I, J are two distinct ideals of R. Without loss of generality, we can assume $I \subsetneq J$ and there exists $a \in I - J$. Suppose $b \in J$. Since $a \notin J$, there must be $ab^{-1} \notin R$, which forces $ba^{-1} \in R$. Thus there exists $r \in R$ such that $b = ra$, implying $b \in I$. Therefore, we show $J \subseteq I$.
- (ii) $\Longrightarrow$ (iii). Trivial.
- (iii) $\Longrightarrow$ (i). Given any $x \in K^\times$, there exists $a, b \in R$ such $x = ab^{-1}$. Then we have
$$(a) \subseteq (b) \text{ or } (b) \subseteq (a) \implies ab^{-1} \in R \text{ or } ba^{-1} \in R \implies x \in R \text{ or } x^{-1} \in R.$$
- (i) $\Longrightarrow$ (v). Take $\Gamma = K^\times / R^\times$. Define a binary relation $\leq$ on Γ by $xR^\times \leq yR^\times \iff yx^{-1} \in R$. Then we can check $(\Gamma, \leq)$ is a totally ordered abelian group:
  (a) (reflexivity) For any $xR^\times \in \Gamma$, we have $xx^{-1} = 1 \in R$, which implies $xR^\times \leq xR^\times$.
  (b) (antisymmetry) Suppose $xR^\times \leq yR^\times$ and $yR^\times \leq xR^\times$. Then $yx^{-1} \in R$ and $\left(yx^{-1}\right)^{-1} = xy^{-1} \in R$, implying $yx^{-1} \in R^\times$. Therefore, $xR^\times = yR^\times$.
  (c) (transitivity) If $xR^\times \leq yR^\times$ and $yR^\times \leq zR^\times$, then $yx^{-1} \in R$ and $zy^{-1} \in R$, so $zx^{-1} = \left(zy^{-1}\right)\left(yx^{-1}\right) \in R$, implying $xR^\times \leq zR^\times$.
  (d) (strong connectivity) For any $xR^\times, yR^\times \in \Gamma$, either $xy^{-1} \in R$ or $y^{-1}x \in R$, which means $xR^\times \leq yR^\times$ or $yR^\times \leq xR^\times$.
  (e) (order preservation) For any $xR^\times, yR^\times, zR^\times \in \Gamma$, we have
$$xR^\times \leq yR^\times \implies yx^{-1} \in R \implies (yz)(xz)^{-1} \in R \implies xzR^\times \leq yzR^\times.$$
  Take v to be the natural projection
$$\begin{aligned} v : K &\longrightarrow \Gamma \cup \{\infty\} \\ x &\longmapsto \begin{cases} xR^\times, & \text{if } x \neq 0 \\ \infty, & \text{if } x = 0 \end{cases} \end{aligned}$$
  Then we can check that v is a valuation of K. For any $x, y \in K$, if $x = 0$ or $y = 0$ or $x + y = 0$, then it is clear to see $v(x + y) = \min\{v(x), v(y)\}$. If $x \neq 0$, $y \neq 0$ and $x + y \neq 0$, then we have
$$\begin{aligned} v(x) \leq v(x+y) &\iff (x+y)y^{-1} \in R \iff xy^{-1} + 1 \in R \iff xy^{-1} \in R, \\ v(y) \leq v(x+y) &\iff (x+y)x^{-1} \in R \iff yx^{-1} + 1 \in R \iff yx^{-1} \in R. \end{aligned}$$
  which implies either $v(x + y) \geq v(x)$ or $v(x + y) \geq v(y)$. Therefore, we show $v(x + y) \geq \min\{v(x), v(y)\}$.
- (ii) $\Longrightarrow$ (iv). Since ideals of R are totally ordered by inclusion, there exists a unique maximal ideal $\mathfrak{m}$ of R. Hence R is a local ring.

□

Proposition 6.12.3

Let K be a field. Let $R \subseteq K$ be a local subring. Then there exists a valuation ring with fraction field K dominating R.

Definition 6.12.4 Discrete Valuation Ring

Suppose R is an integral domain and has field of fractions $K = \mathrm{Frac}\,(R)$. We say R is a **discrete valuation ring** if R satisfies one of the following equivalent conditions:

(i) R is a valuation ring such that the induced valuation $v : K \to \Gamma \cup \{\infty\}$ is a discrete valuation.

(ii) R is a local PID, and not a field.

(iii) R is a PID with a unique non-zero prime ideal.

(iv) R is a PID with a unique irreducible element (up to multiplication by units).

(v) R is a UFD with a unique irreducible element (up to multiplication by units).

(vi) R is a local Dedekind domain and not a field.

(vii) R is a Noetherian local domain whose maximal ideal is principal, and not a field.

(viii) R is an integrally closed Noetherian local ring with Krull dimension one.

(ix) R is Noetherian, not a field, and every nonzero fractional ideal of R is irreducible in the sense that it cannot be written as a finite intersection of fractional ideals properly containing it.

Proposition 6.12.5

A valuation ring is Noetherian if and only if it is a discrete valuation ring or a field.

Chapter 7

Module

7.1 Basic Concepts

Definition 7.1.1 Module

Let R be a ring. An left R**-module** is an abelian group M with a binary operation $R \times M \to M$ such that

(i) $r(m+n) = rm + rn$ for all $r \in R$ and $m, n \in M$.

(ii) $(r+s)m = rm + sm$ for all $r, s \in R$ and $m \in M$.

(iii) $(rs)m = r(sm)$ for all $r, s \in R$ and $m \in M$.

(iv) $1m = m$ for all $m \in M$.

If R is a commutative ring, then M is called a **commutative R-module**.

Definition 7.1.2 Homomorphism of R-modules

Let R be a ring and M, N be R-modules. A map $f : M \to N$ is called an R**-module homomorphism** if

(i) $f(m+n) = f(m) + f(n)$ for all $m, n \in M$.

(ii) $f(rm) = rf(m)$ for all $r \in R$ and $m \in M$.

If f is bijective, then f is called an R**-module isomorphism**. If $M = N$, then f is called an R**-module endomorphism**. If f is bijective, then f is called an R**-module automorphism**. Another name for a homomorphism of R-modules is an R**-linear map**.

Proposition 7.1.3 Ring Action on an Abelian Group

From the perspective of representation theory, a module is a ring action on an abelian group. To be more precise, a ring R can be regarded as an Ab-enriched category with only one object, called the delooping of R, denoted $\mathsf{B}R$. Ab itself is an Ab-enriched category. Thus a left R-module M is a functor between Ab-enriched categories $\mathcal{M} : \mathsf{B}R \to \mathsf{Ab}$.

$$\begin{array}{ccc} \mathsf{B}R & & \mathsf{Ab} \\ * & & M \\ {\scriptstyle r\in R}\downarrow & \overset{\mathcal{M}}{\rightsquigarrow} & \downarrow{\scriptstyle r\cdot(-)\in \mathrm{End}_{\mathsf{Ab}}(M)} \\ * & & M \end{array}$$

As a map between objects, $\mathcal{M}$ assigns an abelian group for $\{*\}$. As a map between morphisms, $\mathcal{M}$ specifies a ring homomorphism $\sigma_M : R \to \mathrm{End}_{\mathsf{Ab}}(M)$. Define the ring representation category to be the category of

all Ab-enriched functors between Ab-enriched categories $\mathsf{B}R$ and Ab, denoted by

$$\mathrm{Rep}_{\mathsf{Ab}}(R) := [\mathsf{B}R, \mathsf{Ab}]_{\mathsf{Ab\text{-}Cat}}.$$

Then we have category isomorphism

$$\mathrm{Rep}_{\mathsf{Ab}}(R) \cong R\text{-}\mathsf{Mod}.$$

Proposition 7.1.4 Ring Homomorphism $f : R \to S$ Induces Functor $f_* : S\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$

Let R and S be rings with a ring homomorphism $f : R \to S$. Then every S-module M is an R-module by defining the scalar multiplication as

$$\begin{aligned} R \times M &\longrightarrow M \\ (r, m) &\longmapsto f(r)m \end{aligned}$$

or equivalently through $R \to S \to \mathrm{End}_{\mathsf{Ab}}(M)$. This defines a functor $f_* : S\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$, which is identify map on objects and morphisms.

$$\begin{array}{ccc} S\text{-}\mathsf{Mod} & & R\text{-}\mathsf{Mod} \\ M & & f_*M \\ \downarrow{\scriptstyle g} & \overset{f_*}{\rightsquigarrow} & \downarrow{\scriptstyle g} \\ N & & f_*N \end{array}$$

The functor $f_* : S\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$ can also be denoted as $\mathrm{Res}_{R\to S} : S\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$. We have the following adjunction

$$R\text{-}\mathsf{Mod} \underset{f_*=\mathrm{Res}_{R\to S}}{\overset{f^*=S\otimes_R -}{\perp}} S\text{-}\mathsf{Mod}$$

Also we have the following adjunction

$$R\text{-}\mathsf{Mod} \underset{f^!=\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(S,M)}{\overset{f^*=S\otimes_R -}{\overset{\perp}{\underset{f_*=\mathrm{Res}_{R\to S}}{\longleftarrow}}}} S\text{-}\mathsf{Mod}, \quad \perp \text{ (between the two arrows)}$$

Since f_* has both left and right adjoint, it is an exact functor.

Remark. The notation f_* comes from the case when R and S are commutative rings. f induces a morphism of affine schemes $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$. Let $\widetilde{M}$ be the associated quasi-coherent sheaf on $\mathrm{Spec}(S)$. Then the global section of $\widetilde{M}$ is the S-module M

$$\Gamma\left(\mathrm{Spec}(S), \widetilde{M}\right) = M$$

Consider the direct image sheaf $f_*\widetilde{M}$ on $\mathrm{Spec}(R)$. The global section of $f_*\widetilde{M}$ is the R-module f_*M

$$\Gamma\left(\mathrm{Spec}(R), f_*\widetilde{M}\right) = f_*M$$

□

In particular, ring homomorphism $R \to S$ makes S an R-module.

Definition 7.1.5 Noetherian Module

Let R be a commutative ring, and let M be an R-module. We say M is **Noetherian** if one of the following equivalent conditions holds:

(i) Every submodule of M is finitely generated.

(ii) Every ascending chain of submodules of M stabilizes; that is, if

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$$

is a chain of submodules of M, then $\exists i$ such that $N_i = N_{i+1} = N_{i+2} = \ldots$.

(iii) Every nonempty family of submodules of M has a maximal element w.r.t. inclusion.

Definition 7.1.6 Annihilator

Let R be a ring, and let M be a left R-module. Suppose S is a non-empty subset of M. The **annihilator** of S, denoted $\mathrm{Ann}_R(S)$, is a left ideal of R defined by

$$\mathrm{Ann}_R(S) = \{r \in R \mid rs = 0 \text{ for all } s \in S\}.$$

If $S = \{x\}$, then we write $\mathrm{Ann}_R(x)$ instead of $\mathrm{Ann}_R(\{x\})$. We have

$$\mathrm{Ann}_R(S) = \bigcap_{s \in S} \mathrm{Ann}_R(s).$$

Proposition 7.1.7 Annihilator and Induced Module Structures

If N is a submodule of M, then

$$\mathrm{Ann}_R(N) = \{r \in R \mid rs = 0 \text{ for all } s \in N\} = \ker\left(R \longrightarrow \mathrm{End}_{\mathsf{Ab}}(N)\right)$$

is a two-sided ideal of R. Through $R/\mathrm{Ann}_R(N) \to \mathrm{End}_{\mathsf{Ab}}(N)$, we can regard N as an $R/\mathrm{Ann}_R(N)$-module. In general, if I is a two-sided ideal of R such that $I \subseteq \mathrm{Ann}_R(N)$, we can regard N as an R/I-module.

Proof. By the universal property of quotient module, we have the following commutative diagram

$$\begin{array}{ccc} R & \longrightarrow & \mathrm{End}_{\mathsf{Ab}}(N) \\ {\scriptstyle\pi}\downarrow & \nearrow & \\ R/I & & \end{array}$$

□

Definition 7.1.8 Faithful Module

Let R be a ring, and let M be a left R-module. We say M is **faithful** if $\mathrm{Ann}_R(M) = 0$, or equivalently, the map $R \to \mathrm{End}_{\mathsf{Ab}}(M)$ is injective.

Proposition 7.1.9 Properties of Annihilator

Let R be a ring, and let M be a left R-module.

(i) If $x \in M$, then $\mathrm{Ann}_R(x) = R$ if and only if $x = 0$.

(ii) If S is a non-empty subset of M and N is the submodule generated by S, then $\mathrm{Ann}_R(N) \subseteq \mathrm{Ann}_R(S)$. If R is commutative, then $\mathrm{Ann}_R(N) = \mathrm{Ann}_R(S)$.

(iii) M as an $R/\mathrm{Ann}_R(M)$-module is faithful.

Definition 7.1.10 Cyclic Module

Let R be a ring, and let M be a left R-module. We say M is a **cyclic module** if there exists an element

$m \in M$ such that

$$M = Rm := \{rm \mid r \in R\}.$$

Definition 7.1.11 Simple Module

Let R be a ring, and let M be a left R-module. We say M is a **simple module** if $M \neq 0$ and the only submodules of M are $\{0\}$ and M itself.

Proposition 7.1.12

Let R be a ring, and let I be a left ideal of R. Then

(i) I is a simple left R-module if and only if I is a minimal nonzero left ideal.

(ii) R/I is a simple left R-module if and only if I is a maximal left ideal.

Proof. (i) Suppose that I is a simple left R-module. Then $I \neq 0$ and the only submodules of I are $\{0\}$ and I itself. Hence, I is a minimal nonzero left ideal.

Conversely, if I is a minimal nonzero left ideal, and J is a R-submodule of I, then J is an left ideal of R. By the minimality of I, J must be either $\{0\}$ or I. Hence, I is a simple left R-module.

(ii) Suppose that R/I is a simple left R-module. Let J be a left ideal of R such that $I \subseteq J$. Then J/I is a left ideal of R/I. Since R/I is simple, we have either $J/I = \{0\}$ or $J/I = R/I$. If $J/I = \{0\}$, then $J = I$. If $J/I = R/I$, then $J = R$. Hence, I is a maximal left ideal.

Suppose that R/I is not a simple left R-module. Then there exists a left ideal $\overline{J} = J/I$ of R/I such that $I \subseteq J \subsetneq R$. Hence, I is not a maximal left ideal.

□

Proposition 7.1.13 Equivalent Characterizations of Simple Module

Let R be a ring, and let M be a left R-module. The following are equivalent:

(i) M is a simple module.

(ii) For any $m \in M - \{0\}$, the cyclic submodule generated by m is equal to M, namely

$$M = Rm.$$

(iii) There exists a maximal left ideal $\mathfrak{m}$ of R such that $M \cong R/\mathfrak{m}$.

Proof. We prove (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i).

$(i) \Rightarrow (ii)$ Assume M is simple and let $0 \neq m \in M$. The set Rm is a submodule of M containing m, hence non–zero. By simplicity, the only non–zero submodule is M itself; therefore $Rm = M$.

$(ii) \Longrightarrow (iii)$ Choose any non–zero $m \in M$ and consider the R–homomorphism

$$\varphi : R \longrightarrow M, \qquad r \longmapsto rm.$$

Because $m \neq 0$ and $Rm = M$ by assumption, φ is surjective. Set $\mathfrak{m} := \ker \varphi$ (a left ideal). By the first isomorphism theorem, $M \cong R/\mathfrak{m}$.

It remains to show that $\mathfrak{m}$ is maximal. Let I be a left ideal with $\mathfrak{m} \subsetneq I \subsetneq R$. Pick $r \in I \setminus \mathfrak{m}$; then $\bar{r} := r + \mathfrak{m} \neq 0$ in $R/\mathfrak{m} \cong M$. Property (ii) transfers through isomorphisms, so $\bar{r}$ must generate all of $R/\mathfrak{m}$:

$$R\bar{r} \;=\; R/\mathfrak{m}.$$

But $R\bar{r} = I/\mathfrak{m}$ (by definition of I), hence $I/\mathfrak{m} = R/\mathfrak{m}$, which forces $I = R$. Therefore no left ideal lies strictly between $\mathfrak{m}$ and R; $\mathfrak{m}$ is maximal.

$(iii) \Rightarrow (i)$ Suppose $M \cong R/\mathfrak{m}$ with $\mathfrak{m}$ a maximal left ideal. Submodules of $R/\mathfrak{m}$ correspond one-to-one with left ideals I satisfying $\mathfrak{m} \subseteq I \subseteq R$:

$$I \longmapsto I/\mathfrak{m}.$$

Because $\mathfrak{m}$ is maximal, the only such I are $\mathfrak{m}$ and R, yielding only the zero submodule and all of $R/\mathfrak{m}$. Hence $R/\mathfrak{m}$, and therefore M, is simple.

Thus $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$, completing the proof. □

7.2 Construction

7.2.1 Free Object

Definition 7.2.1 Free Module

Let R be a ring and S be a set. The **free R-module** on S, denoted by $\mathrm{Free}_{R\text{-}\mathsf{Mod}}(S)$, together with a map $\iota : S \to \mathrm{Free}_{R\text{-}\mathsf{Mod}}(S)$, is defined by the following universal property: for any R-module M and any map $f : S \to M$, there exists a unique R-linear map $\widetilde{f} : \mathrm{Free}_{R\text{-}\mathsf{Mod}}(S) \to M$ such that the following diagram commutes

$$\begin{array}{ccc} \mathrm{Free}_{R\text{-}\mathsf{Mod}}(S) & \xrightarrow{\exists!\, \widetilde{f}} & M \\ {\scriptstyle \iota}\uparrow & \nearrow_{f} & \\ S & & \end{array}$$

The free R-module $\mathrm{Free}_{R\text{-}\mathsf{Mod}}(S)$ can be contructed as the direct sum of copies of R indexed by S, i.e.

$$\mathrm{Free}_{R\text{-}\mathsf{Mod}}(S) \cong \bigoplus_{s \in S} R.$$

Example 7.2.1 Forgetful Functor U

Let R be a ring. Then the forgetful functor $U : R\text{-}\mathsf{Mod} \to \mathsf{Set}$ forgets the R-module structure of an R-module.

(i) U is representable by $(R, 1_R)$. The natural isomorphism $\phi : \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R, -) \xRightarrow{\sim} U$ is given by

$$\begin{aligned} \phi_M : \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R, M) &\longrightarrow U(M) \\ f &\longmapsto f(1_R). \end{aligned}$$

An R-linear map $f : R \to M$ is uniquely determined by $f(1_R)$, and vice versa.

(ii) U is faithful but not full.

Proposition 7.2.2 Free-Forgetful Adjunction $\mathrm{Free}_{R\text{-}\mathsf{Mod}} \dashv U$

Let R be a ring. Then the free R-module functor $\mathrm{Free}_{R\text{-}\mathsf{Mod}}$ is left adjoint to the forgetful functor U.

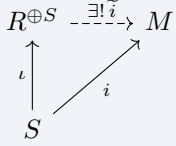
$$R\text{-}\mathsf{Mod} \underset{U}{\overset{\mathrm{Free}_{R\text{-}\mathsf{Mod}}}{\rightleftarrows}} \mathsf{Set} \quad (\perp)$$

For any set S and any R-module M, we have a natural isomorphism

$$\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(\mathrm{Free}_{R\text{-}\mathsf{Mod}}(S), M) \cong \mathrm{Hom}_{\mathsf{Set}}(S, U(M)).$$

Definition 7.2.3 Basis of a Module

Let R be a ring, M be an R-module and $S \subseteq M$ be a subset. The inclusion map $i : S \hookrightarrow M$ induces a map $\widetilde{i} : R^{\oplus S} \to M$ by the universal property of free R-module.



- If $\widetilde{i}$ is injective, then S is called a **linearly independent subset of** M. If $\widetilde{i}$ is not injective, then S is called a **linearly dependent subset of** M.
- If $\widetilde{i}$ is surjective, then S is called a **generating set of** M.
- If $\widetilde{i}$ is bijective, then S is called a **basis of** M.

Proposition 7.2.4

A R-module M has a basis if and only if M is a free R-module.

Definition 7.2.5 Invariant Basis Number

A ring R is said to have the **invariant basis number** property if

$$R^{\oplus S} \cong R^{\oplus T} \iff |S| = |T|.$$

Proposition 7.2.6 Commutative Ring Has IBN Property

Every nonzero commutative ring has the invariant basis number property.

Definition 7.2.7 Rank of a Free Module over Commutative Ring

Let R be a nonzero commutative ring and M be a free R-module. Suppose $M \cong R^{\oplus S}$ for some set S. Then the **rank of** M, denoted by $\mathrm{rk}_R(M)$, is defined as the cardinality of S.

Definition 7.2.8 Finitely Generated Module

We say M is a **finitely generated R-module** if one of the following equivariant conditions holds:

(i) there exist $x_1, \ldots, x_n \in M$ such that every element of M is an R-linear combination of the x_i.

(ii) there exists an epimorphism $R^{\oplus n} \to M$ for some $n \in \mathbb{Z}_+$.

(iii) there exists an exact sequence

$$R^{\oplus n} \longrightarrow M \longrightarrow 0$$

for some $n \in \mathbb{N}$.

(iv) $S \cong R^{\oplus n}/M$ for some $n \in \mathbb{Z}_+$ and some submodule M of $R^{\oplus n}$.

Proposition 7.2.9

Let $R \to S$ be a ring homomorphism and M be an S-module. If M as an R-module is finitely generated, then M as an S-module is also finitely generated.

Proof. Since M is finitely generated as an R-module, there exists an epimorphism $h : R^n \to M$ for some $n \in \mathbb{Z}_+$.

Define

$$\begin{aligned} \iota_1 : \{1, \cdots, n\} &\longrightarrow R^n, \\ i &\longmapsto e_i, \end{aligned}$$

where e_i is the i-th standard basis of R^n and

$$\begin{aligned} i : \{1, \cdots, n\} &\longrightarrow M, \\ i &\longmapsto h(e_i). \end{aligned}$$

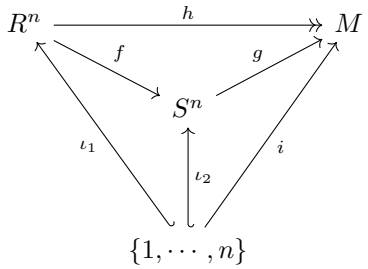
Then we have $h \circ \iota_1 = i$. Define

$$\begin{aligned} \iota_2 : \{1, \cdots, n\} &\longrightarrow S^n, \\ i &\longmapsto e'_i, \end{aligned}$$

where e'_i is the i-th standard basis of S^n. By the universal property of free S-module, there exists a unique S-linear map $g : S^n \to M$ such that $g \circ \iota_2 = i$. By the universal property of free R-module, there exists a unique R-linear map $f : R^n \to S^n$ such that $f \circ \iota_1 = \iota_2$. Therefore, we have

$$(g \circ f) \circ \iota_1 = g \circ \iota_2 = i = h \circ \iota_1.$$

By the universal property of free R-module, we have $g \circ f = h$. Since h is surjective, g is surjective. Therefore, M is finitely generated as an S-module.



□

Definition 7.2.10 Finitely Presented Module

We say M is a **finitely presented R-module** if there exists an exact sequence

$$R^{\oplus m} \longrightarrow R^{\oplus n} \longrightarrow M \longrightarrow 0$$

for some $m, n \in \mathbb{Z}_+$.

7.2.2 Tensor Product

Definition 7.2.11 Bimodule

Let R and S be rings. An (R, S)-**bimodule** is an abelian group M together with a structure of left R-module and a structure of right S-module such that

$$r(ms) = (rm)s$$

for all $r \in R$, $s \in S$, and $m \in M$.

Example 7.2.2 Examples of Bimodule

Let R and S be rings.

- If M is a left R-module, then M is an $(R, \mathbb{Z})$-bimodule.

- If M is a right S-module, then M is a $(\mathbb{Z}, S)$-bimodule.
- If R is a commutative ring, then every left R-module is an (R, R)-bimodule, and every right R-module is also an (R, R)-bimodule. In particular, every abelian group is a $\mathbb{Z}$-module, hence a $(\mathbb{Z}, \mathbb{Z})$-bimodule.
- Any two-sided ideal of a ring R is an (R, R)-bimodule, with the ring multiplication both as the left and as the right multiplication. In particular, R itself is an (R, R)-bimodule.
- If M is a right R-module, then M is an $(\mathrm{End}_{\mathsf{Mod}\text{-}R}(M), R)$-bimodule, where the left multiplication is given by function application.
- If M is a left R-module, then M is an $(R, \mathrm{End}_{R\text{-}\mathsf{Mod}}(M)^{\mathrm{op}})$-bimodule, where the right multiplication is given by function application.

Definition 7.2.12 Balanced Product

Let R be a ring, M be a right R-module, N be a left R-module and G be an abelian group. A map $b : M \times N \to G$ is called a **R-balanced product** if

(i) $b(m_1 + m_2, n) = b(m_1, n) + b(m_2, n)$ for all $m_1, m_2 \in M$ and $n \in N$.

(ii) $b(m, n_1 + n_2) = b(m, n_1) + b(m, n_2)$ for all $m \in M$ and $n_1, n_2 \in N$.

(iii) $b(mr, n) = b(m, rn)$ for all $r \in R$, $m \in M$, and $n \in N$.

The set of all R-balanced products from $M \times N$ to G is denoted by $\mathrm{Bal}_R(M, N; G)$, which is an abelian group with respect to pointwise addition:

$$(b_1 + b_2)(m, n) = b_1(m, n) + b_2(m, n).$$

Proposition 7.2.13 Functor $\mathrm{Bal}_R(M, N; -) : \mathsf{Ab} \to \mathsf{Ab}$

For M and N fixed, we can define a functor $\mathrm{Bal}_R(M, N; -) : \mathsf{Ab} \to \mathsf{Ab}$ by

$$\begin{array}{ccc} \mathsf{Ab} & & \mathsf{Ab} \\ G & & \mathrm{Bal}_R(M,N;G) \ni b \\ \downarrow{\scriptstyle f} & \overset{\mathrm{Bal}_R(M,N;-)}{\rightsquigarrow} & \downarrow{\scriptstyle f_*} \qquad \downarrow \\ H & & \mathrm{Bal}_R(M,N;H) \ni f \circ b \end{array}$$

Definition 7.2.14 Category $\mathsf{Bal}_R(M, N)$

Let R be a ring, M be a right R-module, and N be a left R-module. The **category of R-balanced products** from M and N, denoted by $\mathsf{Bal}_R(M, N)$, is defined as follows:

- The objects of $\mathsf{Bal}_R(M, N)$ are R-balanced products from $M \times N$ to G

$$\mathrm{Ob}\left(\mathsf{Bal}_R(M, N)\right) = \{b : M \times N \to G \mid G \in \mathrm{Ob}(\mathsf{Ab}),\, b \in \mathrm{Bal}_R(M, N; G)\}$$

- The morphisms from $b_1 : M \times N \to G_1$ to $b_2 : M \times N \to G_2$ are group homomorphisms $f : G_1 \to G_2$ such that $f \circ b_1 = b_2$.

$$\begin{array}{ccc} & & G_1 \\ & \overset{b_1}{\nearrow} & \\ M \times N & & \downarrow{\scriptstyle f} \\ & \underset{b_2}{\searrow} & \\ & & G_2 \end{array}$$

Definition 7.2.15 Tensor Product of R-modules

The **tensor product** of R-modules M and N, denoted by $\otimes : M \times N \to M \otimes_R N$, is the initial object in the category $\mathsf{Bal}_R(M, N)$. The tensor product satisfies the following universal property: for any R-module G and any R-balanced product $b : M \times N \to G$, there exists a unique group homomorphism $\widetilde{b} : M \otimes_R N \to G$ such that the following diagram commutes

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes_R N \\ & \searrow^{b} & \downarrow{\scriptstyle \exists! \, \widetilde{b}} \\ & & G \end{array}$$

The tensor product can be constructed as follows: let $F := \mathrm{Free}_{\mathsf{Ab}}(M \times N)$ be the free abelian group on $M \times N$, and let K be the subgroup of F generated by elements of the form

(i) $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$,

(ii) $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$,

(iii) $(mr, n) - (m, rn)$.

Then the tensor product $\otimes : M \times N \to M \otimes_R N$ can be constructed as the composition

$$\otimes : M \times N \xrightarrow{\iota} F \xrightarrow{\pi} F/K$$

and $M \otimes_R N := F/K$.

Proof. To prove the constructed tensor product F/K is the initial object in the category $\mathsf{Bal}_R(M, N)$, we need to check the universal property of tensor product. Let G be an R-module and $b : M \times N \to G$ be an R-balanced product.

$$\begin{array}{ccc} F & \xrightarrow{\pi} & F/K \\ {\scriptstyle \iota}\uparrow & \nearrow_{\hat{b}} & \downarrow{\scriptstyle \tilde{b}} \\ M \times N & \xrightarrow[b]{} & G \end{array}$$

First by the universal property of free abelian group, there exists a unique group homomorphism

$$\hat{b} : F \longrightarrow G$$
$$\sum_{i=1}^{k} r_i(m_i, n_i) \longmapsto \sum_{i=1}^{k} r_i b(m_i, n_i).$$

such that $\hat{b} \circ \iota = b$. Note that

$$\begin{aligned} \hat{b}\left((m_1 + m_2, n) - (m_1, n) - (m_2, n)\right) &= b(m_1 + m_2, n) - b(m_1, n) - b(m_2, n) = 0, \\ \hat{b}\left((m, n_1 + n_2) - (m, n_1) - (m, n_2)\right) &= b(m, n_1 + n_2) - b(m, n_1) - b(m, n_2) = 0, \\ \hat{b}\left((mr, n) - (m, rn)\right) &= b(mr, n) - b(m, rn) = 0. \end{aligned}$$

We see for any $k \in K$, $\hat{b}(k) = 0$. Thus by the universal property of quotient group, there exists a unique group homomorphism $\tilde{b} : F/K \to G$ such that $\tilde{b} \circ \pi = \hat{b}$. It is easy to check that $\tilde{b} \circ \pi \circ \iota = b$, which means the diagram commutes.

To show the uniqueness, assume there exists another group homomorphism $\tilde{b}' : F/K \to G$ such that $\tilde{b}' \circ \pi \circ \iota = b$. Since $\hat{b} \circ \iota = b$, by the uniqueness of $\tilde{b}$, we have $\tilde{b}' \circ \pi = \hat{b}$. Then by the uniqueness of $\tilde{b}$, we have $\tilde{b} = \tilde{b}'$. Thus the tensor product F/K is the initial object in the category $\mathsf{Bal}_R(M, N)$. □

Proposition 7.2.16 Pure Tensors Generate Tensor Product

Let R be a ring, M be a right R-module, and N be a left R-module. The elements of the image of the

tensor product map $\otimes : M \times N \to M \otimes_R N$

$$\mathrm{im}(\otimes) = \{m \otimes n \mid m \in M, n \in N\}.$$

are called **pure tensors**.

(i) $\mathrm{im}(\otimes)$ generates $M \otimes_R N$ as an abelian group:

$$M \otimes_R N = \langle \mathrm{im}(\otimes) \rangle_{\mathsf{Ab}} := \left\{ \sum_{i=1}^{k} m_i \otimes n_i \mid k \in \mathbb{Z}_{\geq 1}, m_i \in M, n_i \in N \right\}.$$

(ii) Let $F := \mathrm{Free}_{\mathsf{Ab}}(\mathrm{im}(\otimes))$. Then we have

$$M \otimes_R N \cong F/\langle X_M \cup X_N \rangle,$$

where

$$X_M = \{[(m+m') \otimes n] - [m \otimes n] - [m' \otimes n] \in F \mid m, m' \in M, n \in N\},$$
$$X_N = \{[m \otimes (n+n')] - [m \otimes n] - [m \otimes n'] \in F \mid m \in M, n, n' \in N\}.$$

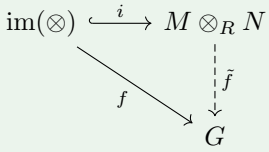
(iii) Let $f : \mathrm{im}(\otimes) \to G$ be a map. If and only if the map

$$\begin{aligned} M \times N &\longrightarrow G \\ (m, n) &\longmapsto f(m \otimes n) \end{aligned}$$

is $\mathbb{Z}$-bilinear, i.e.

$$f((m_1 + m_2) \otimes n) = f(m_1 \otimes n) + f(m_2 \otimes n),$$
$$f(m \otimes (n_1 + n_2)) = f(m \otimes n_1) + f(m \otimes n_2),$$

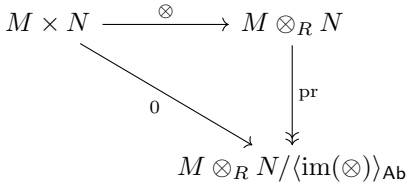
there exists a group homomorphism $\tilde{f} : M \otimes_R N \to G$ such that the following diagram commutes



If such $\tilde{f}$ exists, then it is unique and is totally determined by f as follows:

$$\begin{aligned} \tilde{f} : M \otimes_R N &\longrightarrow G \\ \sum_{i=1}^{k} m_i \otimes n_i &\longmapsto \sum_{i=1}^{k} f(m_i \otimes n_i). \end{aligned}$$

Proof. (i) Let $\mathrm{pr} : M \otimes_R N \to M \otimes_R N/\langle \mathrm{im}(\otimes) \rangle_{\mathsf{Ab}}$ be the canonical projection. Then we have the following commutative diagram

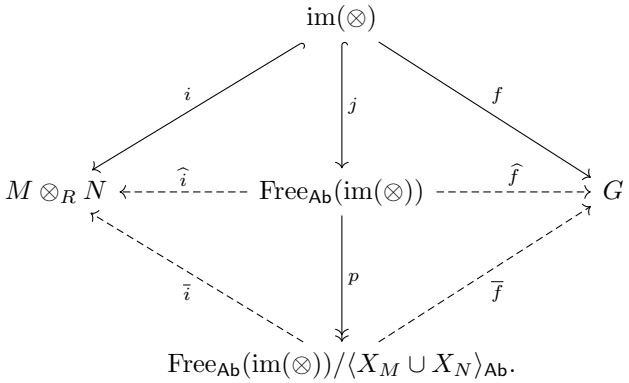


Note $0 = 0 \circ \otimes$. By the uniqueness in the universal property of tensor product, we have $\mathrm{pr} = 0$. Therefore, $M \otimes_R N = \langle \mathrm{im}(\otimes) \rangle_{\mathsf{Ab}}$.

(ii) Define

$$\begin{aligned} j : \mathrm{im}(\otimes) &\longrightarrow \mathrm{Free}_{\mathsf{Ab}}(\mathrm{im}(\otimes)) \\ m \otimes n &\longmapsto [m \otimes n] \end{aligned}$$

By the universal property of free abelian group, the inclusion $i : \mathrm{im}(\otimes) \hookrightarrow M \otimes_R N$ induces a group homomorphism $\widehat{i} : \mathrm{Free}_{\mathsf{Ab}}(\mathrm{im}(\otimes)) \to M \otimes_R N$.



Since

$$\widehat{i}\,(X_M) = \widehat{i}\,(X_N) = \{0\} \implies X_M \cup X_N \subseteq \ker \widehat{i} \implies \langle X_M \cup X_N \rangle_{\mathsf{Ab}} \subseteq \ker \widehat{i}$$

there exists a unique group homomorphism $\overline{i} : \mathrm{Free}_{\mathsf{Ab}}(\mathrm{im}(\otimes))/\langle X_M \cup X_N \rangle_{\mathsf{Ab}} \to M \otimes_R N$ such that $\overline{i} \circ p = \widehat{i}$. Since $\widehat{i}$ is surjective, $\overline{i}$ is also surjective. Define

$$\begin{aligned} \beta : M \times N &\longrightarrow \mathrm{Free}_{\mathsf{Ab}}\left(\mathrm{im}(\otimes)\right) / \langle X_M \cup X_N \rangle_{\mathsf{Ab}} \\ (m, n) &\longmapsto \overline{[m \otimes n]} \end{aligned}$$

We can check that β is a balanced product

$$\begin{aligned} \beta\left(m_1 + m_2, n\right) &= \overline{[(m_1 + m_2) \otimes n]} = \overline{[m_1 \otimes n]} + \overline{[m_2 \otimes n]} = \beta\left(m_1, n\right) + \beta\left(m_2, n\right), \\ \beta\left(m, n_1 + n_2\right) &= \overline{[m \otimes (n_1 + n_2)]} = \overline{[m \otimes n_1]} + \overline{[m \otimes n_2]} = \beta\left(m, n_1\right) + \beta\left(m, n_2\right), \\ \beta\left(mr, n\right) &= \overline{[(mr) \otimes n]} = \overline{[m \otimes (rn)]} = \beta\left(m, rn\right). \end{aligned}$$

By the universal property of tensor product $M \otimes_R N$, there exists a unique group homomorphism

$$\begin{aligned} \varphi : M \otimes_R N &\longrightarrow \mathrm{Free}_{\mathsf{Ab}}(\mathrm{im}(\otimes))/\langle X_M \cup X_N \rangle, \\ m \otimes n &\longmapsto \overline{[m \otimes n]}. \end{aligned}$$

such that $\varphi \circ \otimes = \beta$. Note

$$\begin{aligned} \varphi \circ \overline{i}\left(\overline{[m_1 \otimes n_1] + \cdots [m_k \otimes n_k]}\right) &= \varphi \circ \overline{i} \circ p\left([m_1 \otimes n_1] + \cdots [m_k \otimes n_k]\right) \\ &= \varphi \circ \widehat{i}\left([m_1 \otimes n_1] + \cdots [m_k \otimes n_k]\right) \\ &= \varphi\left(m_1 \otimes n_1\right) + \cdots + \varphi\left(m_k \otimes n_k\right) \\ &= \overline{[m_1 \otimes n_1]} + \cdots + \overline{[m_k \otimes n_k]} \\ &= \overline{[m_1 \otimes n_1] + \cdots + [m_k \otimes n_k]}. \end{aligned}$$

We have $\varphi \circ \overline{i} = \mathrm{id}$, which implies that $\overline{i}$ is injective. Therefore, $\overline{i}$ is an isomorphism.

(iii) If there exists a group homomorphism $\tilde{f} : M \otimes_R N \to G$ such that $f = \tilde{f} \circ i$, then we can check that the map $(m, n) \mapsto f(m \otimes n)$ is $\mathbb{Z}$-bilinear:

$$\begin{aligned} f\left((m_1 + m_2) \otimes n\right) &= \tilde{f}\left(i\left((m_1 + m_2) \otimes n\right)\right) = \tilde{f}\left(m_1 \otimes n + m_2 \otimes n\right) = f\left(m_1 \otimes n\right) + f\left(m_2 \otimes n\right), \\ f\left(m \otimes (n_1 + n_2)\right) &= \tilde{f}\left(i\left(m \otimes (n_1 + n_2)\right)\right) = \tilde{f}\left(m \otimes n_1 + m \otimes n_2\right) = f\left(m \otimes n_1\right) + f\left(m \otimes n_2\right). \end{aligned}$$

Conversely, if the map $(m,n) \mapsto f(m \otimes n)$ is $\mathbb{Z}$-bilinear, then we have

$$\begin{aligned}\widehat{f}\left([(m+m') \otimes n] - [m \otimes n] - [m' \otimes n]\right) &= \widehat{f}\left([(m+m') \otimes n]\right) - \widehat{f}\left([m \otimes n]\right) - \widehat{f}\left([m' \otimes n]\right) \\ &= f\left((m+m') \otimes n\right) - f\left(m \otimes n\right) - f\left(m' \otimes n\right) = 0, \\ \widehat{f}\left([m \otimes (n+n')] - [m \otimes n] - [m \otimes n']\right) &= \widehat{f}\left([m \otimes (n+n')]\right) - \widehat{f}\left([m \otimes n]\right) - \widehat{f}\left([m \otimes n']\right) \\ &= f\left(m \otimes (n+n')\right) - f\left(m \otimes n\right) - f\left(m \otimes n'\right) = 0,\end{aligned}$$

which implies

$$\widehat{f}\left(X_M\right) = \widehat{f}\left(X_N\right) = \{0\} \implies X_M \cup X_N \subseteq \ker \widehat{f} \implies \langle X_M \cup X_N \rangle_{\mathsf{Ab}} \subseteq \ker \widehat{f}.$$

Thus by the universal property of quotient group, there exists a unique group homomorphism

$$\begin{aligned}\overline{f} : \mathrm{Free}_{\mathsf{Ab}}(\mathrm{im}(\otimes))/\langle X_M \cup X_N \rangle_{\mathsf{Ab}} &\longrightarrow G \\ \overline{[m \otimes n]} &\longmapsto f(m \otimes n)\end{aligned}$$

such that $\overline{f} \circ p = \widehat{f}$. Composing $\overline{f}$ with the isomorphism $\varphi : M \otimes_R N \to \mathrm{Free}_{\mathsf{Ab}}(\mathrm{im}(\otimes))/\langle X_M \cup X_N \rangle$ in (ii), we obtain a group homomorphism

$$\begin{aligned}\tilde{f} : M \otimes_R N &\longrightarrow G \\ m \otimes n &\longmapsto f(m \otimes n).\end{aligned}$$

□

Proposition 7.2.17

Let Q, R, and S be commutative rings, M be a (Q,R)-bimodule, and N be a (R,S)-bimodule. Then $M \otimes_R N$ has a natural (Q,S)-bimodule structure given by

$$q \cdot (m \otimes n) := (q \cdot m) \otimes n, \quad (m \otimes n) \cdot s := m \otimes (n \cdot s)$$

for all $q \in Q$, $s \in S$, $m \in M$, and $n \in N$.

Example 7.2.3 Base Change Functor

Let $\varphi : R \to S$ be a ring homomorphism. The **base change functor** $- \otimes_R S : R\text{-}\mathsf{Mod} \to S\text{-}\mathsf{Mod}$ is defined as follows:

$$\begin{array}{ccc} R\text{-}\mathsf{Mod} & & S\text{-}\mathsf{Mod} \\ M & & M \otimes_R S \\ \Big\downarrow{\scriptstyle f} & \rightsquigarrow^{-\otimes_R S} & \Big\downarrow{\scriptstyle f \otimes_R \mathrm{id}_S} \\ N & & N \otimes_R S \end{array}$$

where the S-module structure on $M \otimes_R S$ is given by

$$s' \cdot (m \otimes s) := m \otimes (s's)$$

for all $s', s \in S$ and $m \in M$.

Proposition 7.2.18 Tensoring with the Base Ring

Let R be a ring and M be a left R-module. Then there is a natural isomorphism of R-modules

$$\begin{aligned}\lambda_M : R \otimes_R M &\xrightarrow{\sim} M \\ r \otimes m &\longmapsto r \cdot m\end{aligned}$$

Proof. Define the map

$$\begin{aligned}\rho_M : M &\longrightarrow R \otimes_R M \\ m &\longmapsto 1_R \otimes m.\end{aligned}$$

ρ_M is an R-linear map since for any $r \in R$ and $m, n \in M$,

$$\rho_M(rm) = 1_R \otimes (rm) = r \otimes m = r \cdot (1_R \otimes m) = r \cdot \rho_M(m).$$

□

7.2.3 Localization

Proposition 7.2.19

Let R be a commutative ring and $S \subseteq R$ be a multiplicative subset. The category of $S^{-1}R$ modules is equivalent to the category of R-modules M with the property that every $s \in S$ acts as an automorphism on M. The following functor F gives a equivalence of categories:

$$\begin{array}{ccc} S^{-1}R\text{-}\mathsf{Mod} & & R\text{-}\mathsf{Mod} \text{ where } S \text{ act as automorphisms} \\ M & & M \\ \downarrow{\scriptstyle f} & \overset{F}{\rightsquigarrow} & \downarrow{\scriptstyle f} \\ N & & N \end{array}$$

Proof. Assume S is a multiplicative subset of communitative ring R and the localization map is $\varphi : R \to S^{-1}R$. Then R can acts on $S^{-1}R$-module M through

$$R \xrightarrow{\varphi} S^{-1}R \xrightarrow{\sigma'_M} \mathrm{End}_{\mathsf{Ab}}(M),$$

which enables us to regard M as an R-module. Furthermore, since

$$\sigma'_M(\varphi(S)) \subseteq \sigma'_M\left(\left(S^{-1}R\right)^\times\right) \subseteq (\mathrm{End}_{\mathsf{Ab}}(M))^\times = \mathrm{Aut}_{\mathsf{Ab}}(M),$$

every $s \in S$ acts as an automorphism on M.
Conversely, if M is an R-module such that every $s \in S$ acts as an automorphism on M, i.e. $\sigma_M : R \to \mathrm{End}_{\mathsf{Ab}}(M)$ satisfies $\sigma_M(S) \subseteq \mathrm{Aut}_{\mathsf{Ab}}(M)$, then by unversal property

$$\begin{array}{ccc} S^{-1}R & \overset{\sigma'_M}{\dashrightarrow} & \mathrm{End}_{\mathsf{Ab}}(M) \\ & {\scriptstyle\varphi}\nwarrow \quad \nearrow{\scriptstyle\sigma_M} & \\ & R & \end{array}$$

we can define a $S^{-1}R$-module structure on M by lifting σ_M to σ'_M. It is easy to check that these two functors are quasi-inverse to each other. □

Definition 7.2.20 Localization of a Module

Let R be a commutative ring, S be a multiplicative set in R, and M be an R-module. The **localization of the module** M by S, denoted $S^{-1}M$, is an $S^{-1}R$-module that is constructed exactly as the localization of R, except that the numerators of the fractions belong to M. That is, as a set, it consists of equivalence classes, denoted $\frac{m}{s}$, of pairs (m, s), where $m \in M$ and $s \in S$, and two pairs (m, s) and (n, t) are equivalent if there is an element $u \in S$ such that

$$u(sn - tm) = 0.$$

Addition and scalar multiplication are defined as for usual fractions (in the following formula, $r \in R$, $s, t \in S$, and $m, n \in M$):

$$\frac{m}{s} + \frac{n}{t} = \frac{tm + sn}{st},$$
$$\frac{r}{s}\frac{m}{t} = \frac{rm}{st}.$$

Proposition 7.2.21 Universal Property of Localization

Let R be a commutative ring and $S \subseteq R$ be a multiplicative subset, an M be an R-module. The R-linear map

$$\begin{aligned} l_S : M &\longrightarrow S^{-1}M \\ m &\longmapsto \frac{m}{1} \end{aligned}$$

satisfies the any of following universal properties:

- for any R-linear map $\psi : M \to N$ such that S act as automorphisms on N (i.e. the induced ring homomorphism $\sigma_N : R \to \mathrm{End}_{\mathsf{Ab}}(N)$ satisfies $\sigma_N(S) \subseteq \mathrm{Aut}_{\mathsf{Ab}}(N)$), there exists a unique R-linear map

  $$\begin{aligned} \psi' : S^{-1}M &\longrightarrow N \\ \frac{m}{s} &\longmapsto \sigma_N(s)^{-1}(\psi(m)) \end{aligned}$$

  such that the following diagram commutes in R-Mod

  $$\begin{array}{ccc} S^{-1}M & \xrightarrow{\psi'} & N \\ & {\scriptstyle l_S}\nwarrow \quad \nearrow{\scriptstyle \psi} & \\ & M & \end{array}$$

- for any $S^{-1}R$-module N and R-linear map $\psi : M \to \mathrm{Res}(N)$, there exists a unique $S^{-1}R$-linear map $\psi' : S^{-1}M \to N$ such that the following diagram commutes in R-Mod

  $$\begin{array}{ccc} \mathrm{Res}(S^{-1}M) & \xrightarrow{\mathrm{Res}(\psi')} & \mathrm{Res}(N) \\ & {\scriptstyle l_S}\nwarrow \quad \nearrow{\scriptstyle \psi} & \\ & M & \end{array}$$

We have two equivalent universal properties because of the equivalence of categories in Proposition 7.2.19.

Proposition 7.2.22 Kernel of Localization Map

Let R be a commutative ring, S be a multiplicative set in R, and M be an R-module. Suppose

$$\begin{aligned} l_S : M &\longrightarrow S^{-1}M \\ m &\longmapsto \frac{m}{1} \end{aligned}$$

is the localization map. Then

$$\ker l_S = \{m \in M \mid \exists s \in S,\ sm = 0\}.$$

Proof. If $m \in \ker l_S$, then we have $\frac{m}{1} = \frac{0}{1}$ in $S^{-1}M$. By the definition of localization, there exists $s \in S$ such that

$$s(1 \cdot 0 - 1 \cdot m) = -sm = 0.$$

Thus we have

$$\ker l_S \subseteq \{m \in M \mid \exists s \in S,\ sm = 0\}.$$

Conversely, if $m \in M$ such that there exists $s \in S$ with $sm = 0$, then we have

$$l_S(m) = \frac{m}{1} = \frac{sm}{s} = \frac{0}{s} = \frac{0}{1},$$

which means $m \in \ker l_S$. Thus we have

$$\{m \in M \mid \exists s \in S,\ sm = 0\} \subseteq \ker l_S.$$

Therefore, we conclude that

$$\ker l_S = \{m \in M \mid \exists s \in S,\ sm = 0\}.$$

□

Proposition 7.2.23 Localization is a Left Adjoint Functor

Let R be a commutative ring, S be a multiplicative set in R, and M be an R-module. Define the localization functor as follows

$$\begin{array}{ccc} R\text{-Mod} & & S^{-1}R\text{-Mod} \\ M & & S^{-1}M \ni \frac{m}{s} \\ \downarrow{\scriptstyle f} & \overset{S^{-1}}{\rightsquigarrow} & \downarrow{\scriptstyle S^{-1}(f)} \quad \downarrow \\ N & & S^{-1}N \ni \frac{f(m)}{s} \end{array}$$

where $S^{-1}(f)$ is defiend as the composition $S^{-1}M \xrightarrow{f'} N \to S^{-1}N$.
Let $\mathrm{Res}_{R\to S^{-1}R} : S^{-1}R\text{-Mod} \to R\text{-Mod}$ be the functor that regards $S^{-1}R$-modules as R-modules. Then we have a pair of adjoint functors

$$R\text{-Mod} \underset{\mathrm{Res}}{\overset{S^{-1}}{\rightleftarrows}} S^{-1}R\text{-Mod} \quad (\perp)$$

and natural isomorphism

$$\mathrm{Hom}_{S^{-1}R\text{-Mod}}(S^{-1}M, N) \cong \mathrm{Hom}_{R\text{-Mod}}(M, \mathrm{Res}_{R\to S^{-1}R}(N)).$$

Proposition 7.2.24 Localization is an Exact Functor

Let R be a commutative ring, S be a multiplicative set in R. If

$$L \xrightarrow{u} M \xrightarrow{v} N$$

is an exact sequence of R-module, then

$$S^{-1}L \xrightarrow{S^{-1}(u)} S^{-1}M \xrightarrow{S^{-1}(v)} S^{-1}N$$

is an exact sequence of $S^{-1}R$-module.

Proof. Suppose $\frac{m}{s} \in \ker S^{-1}(v)$. Then we have

$$S^{-1}(v)\left(\frac{m}{s}\right) = \frac{v(m)}{s} = \frac{0}{1},$$

which imples that there exists $t \in S$ such that $tv(m) = v(tm) = 0$. Thus we have $tm \in \ker v$. By exactness, there exists $l \in L$ such that $u(l) = tm$. Since

$$S^{-1}(u)\left(\frac{l}{ts}\right) = \frac{u(l)}{ts} = \frac{tm}{ts} = \frac{m}{s},$$

we see that $\frac{m}{s} \in \mathrm{im}\, S^{-1}(u)$, which means $\mathrm{im}\, S^{-1}(u) = \ker S^{-1}(v)$. Hence S^{-1} is exact. □

Proposition 7.2.25 Localization of Module as Tensor Product

Let R be a ring, $S \subseteq R$ a multiplicative subset. The localization functor $S^{-1} : R\text{-Mod} \to S^{-1}R\text{-Mod}$ is

isomorphic to the tensor product functor $S^{-1}R \otimes_R -$. And we have isomorphisms

$$\begin{aligned} \theta_M : S^{-1}R \otimes_R M &\xrightarrow{\sim} S^{-1}M \\ \frac{a}{s} \otimes m &\longmapsto \frac{am}{s} \end{aligned}$$

naturally for all R-modules M.

Proof. **Step 1. Constructing the Isomorphism θ_M**
Define the map

$$\begin{aligned} b_M : S^{-1}R \times M &\longrightarrow S^{-1}M \\ \left(\frac{a}{s}, m\right) &\longmapsto \frac{am}{s}. \end{aligned}$$

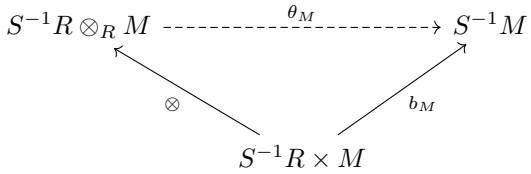
This map is well-defined because for any $\frac{a}{s} = \frac{a'}{s'}$, there exists $u \in S$ such that $u(s'a - sa') = 0$, so that

$$u(s'(am) - s(a'm)) = u(s'a - sa')m = 0 \implies \frac{am}{s} = \frac{a'm}{s'}.$$

It is straightforward to check that b_M is an R-balanced product. By the universal property of the tensor product, there exists a unique R-linear map

$$\begin{aligned} \theta_M : S^{-1}R \otimes_R M &\longrightarrow S^{-1}M \\ \frac{a}{s} \otimes m &\longmapsto \frac{am}{s} \qquad (a \in A, s \in S, m \in M). \end{aligned}$$

such that the following diagram commutes



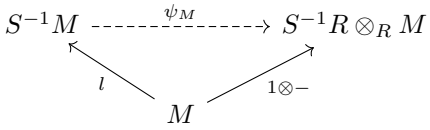
Step 2. Constructing the Inverse
Define the R-linear map

$$\begin{aligned} 1 \otimes - : M &\longrightarrow S^{-1}R \otimes_R M \\ m &\longmapsto 1_{S^{-1}R} \otimes m. \end{aligned}$$

Through the universal property of localization, we obtain a unique $S^{-1}R$-linear map

$$\begin{aligned} \psi_M : S^{-1}M &\longrightarrow S^{-1}R \otimes_R M \\ \frac{m}{s} &\longmapsto \frac{1}{s} \otimes m. \end{aligned}$$

such that the following diagram commutes



We can verify that θ_M and ψ_M are Inverses:

- Composition $\theta_M \circ \psi_M$: For any $\frac{m}{s} \in S^{-1}M$,

$$(\theta_M \circ \psi_M)\left(\frac{m}{s}\right) = \theta_M\left(\frac{1}{s} \otimes m\right) = \frac{1 \cdot m}{s} = \frac{m}{s}.$$

- Composition $\psi_M \circ \theta_M$: For any $\frac{a}{s} \otimes m \in S^{-1}R \otimes_R M$, by R-linearity of the tensor product, we have

$$(\psi_M \circ \theta_M)\Big(\frac{a}{s} \otimes m\Big) = \psi_M\left(\frac{am}{s}\right) = \frac{1}{s} \otimes am = \frac{a}{s} \otimes m.$$

Step 3. Naturality
Let $f : M \to N$ be a morphism of R-modules. We need to show that the following diagram commutes:

$$\begin{array}{ccc} S^{-1}R \otimes_R M & \xrightarrow{\mathrm{id}\otimes f} & S^{-1}R \otimes_R N \\ \downarrow{\scriptstyle \theta_M} & & \downarrow{\scriptstyle \theta_N} \\ S^{-1}M & \xrightarrow[S^{-1}f]{} & S^{-1}N \end{array}$$

For any $\frac{a}{s} \otimes m \in S^{-1}R \otimes_R M$, we have

$$\phi_N\Big((1 \otimes f)\Big(\frac{a}{s} \otimes m\Big)\Big) = \phi_N\Big(\frac{a}{s} \otimes f(m)\Big) = \frac{af(m)}{s},$$

and

$$(S^{-1}f)\Big(\theta_M\Big(\frac{a}{s} \otimes m\Big)\Big) = (S^{-1}f)\Big(\frac{am}{s}\Big) = \frac{af(m)}{s}.$$

Thus, the diagram commutes, and the isomorphism is natural.

Conclusion
We have constructed a natural isomorphism

$$\theta_M : S^{-1}R \otimes_R M \xrightarrow{\sim} S^{-1}M,$$

which establishes that the functors

$$S^{-1}(-) \quad \text{and} \quad S^{-1}A \otimes_A (-)$$

are isomorphic. □

Proposition 7.2.26 Localization Respects Quotients

Let M be an R-module and N be a submodule of M. Then we have an isomorphism

$$S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N)$$

and the following commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{\pi_M} & M/N \\ \downarrow{\scriptstyle S^{-1}} & & \downarrow{\scriptstyle S^{-1}} \\ S^{-1}M & \xrightarrow[\pi_{S^{-1}N}]{} & S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N) \end{array}$$

Proof. Since localization is exact, from the exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0,$$

we obtain the following exact sequence

$$0 \longrightarrow S^{-1}N \longrightarrow S^{-1}M \longrightarrow S^{-1}(M/N) \longrightarrow 0.$$

□

Proposition 7.2.27 Localization Commutes with Tensor Product

Let R be a commutative ring, S be a multiplicative set in R, and M, N be R-modules. Then we have an isomorphism

$$\begin{aligned} f : S^{-1}M \otimes_{S^{-1}R} S^{-1}N &\xrightarrow{\sim} S^{-1}(M \otimes_R N) \\ \frac{m}{s} \otimes \frac{n}{t} &\longmapsto \frac{m \otimes n}{st} \end{aligned}$$

Proof.

$$\begin{aligned} S^{-1}(M \otimes_R N) &\cong S^{-1}R \otimes_R (M \otimes_R N) && \text{(by Proposition 7.2.25)} \\ &\cong (S^{-1}R \otimes_R M) \otimes_R N && \text{(by associativity of tensor product)} \\ &\cong S^{-1}M \otimes_R N && \text{(by Proposition 7.2.25)} \\ &\cong (S^{-1}M \otimes_{S^{-1}R} S^{-1}R) \otimes_R N && \text{(by Proposition 7.2.18)} \\ &\cong S^{-1}M \otimes_{S^{-1}R} (S^{-1}R \otimes_R N) && \text{(by associativity of tensor product)} \\ &\cong S^{-1}M \otimes_{S^{-1}R} S^{-1}N && \text{(by Proposition 7.2.25)} \end{aligned}$$

□

Proposition 7.2.28 Localization as Colimit

Let R be a commutative ring, S be a multiplicative set in R, and M be an R-module. Then we have an isomorphism

$$S^{-1}M \cong \varinjlim_{f \in S} M_f,$$

where M_f is the localization of M by the multiplicative set $\langle f \rangle = \{f^n \mid n \in \mathbb{Z}_{\geq 0}\}$.
Formally, S can be endowed with a preorder relation: $f \mid g$ if and only if $fh = g$ for some $h \in S$, which makes S a thin category S. Then we can define a functor $M_- : \mathsf{S} \to R\text{-}\mathsf{Mod}$

$$\begin{array}{ccc} \mathsf{S} & & R\text{-}\mathsf{Mod} \\ f & & M_f \ni \frac{m}{f^n} \\ \downarrow & \overset{G}{\rightsquigarrow} & \downarrow l'_g \quad \downarrow \\ g = fh & & M_g \ni \frac{mh^n}{g^n} \end{array}$$

where l'_g is given by the following universal property

$$\begin{array}{ccc} M_f & \xrightarrow{l'_g} & M_g \\ & {\scriptstyle l_f} \nwarrow \quad \nearrow {\scriptstyle l_g} & \\ & M & \end{array}$$

And we have

$$S^{-1}M \cong \varinjlim M_-$$

Proof. First let's show that the l'_g induced by universal property can be writen as $l'_g : \frac{m}{f^n} \mapsto \frac{mh^n}{g^n}$. Suppose R acts on M_g through

$$\sigma_{M_g} : R \to S_g^{-1}R \xrightarrow{\sigma_{M'_g}} \mathrm{End}_{\mathsf{Ab}}(M_g),$$

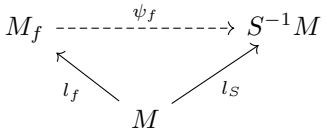
Then we can check for any $f^n \in S_f$,

$$\sigma_{M_g}(f^n)\sigma_{M'_g}\left(\frac{h^n}{g^n}\right) = \sigma_{M'_g}\left(\frac{f^n h^n}{g^n}\right) = \sigma_{M'_g}(1) = 1 \implies \sigma_{M_g}(f^n) \in \mathrm{Aut}_{\mathsf{Ab}}(M_g),$$

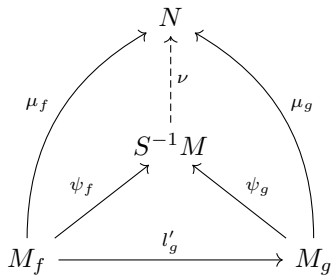
which means $\sigma_{M_g}(S_f) \subseteq \mathrm{Aut}_{\mathsf{Ab}}(M_g)$. Thus by universal property of M_f, we have

$$l'_g\left(\frac{m}{f^n}\right) = \sigma_{M_g}(f^n)^{-1}(m) = \sigma_{M'_g}\left(\frac{h^n}{g^n}\right)(m) = \frac{mh^n}{g^n}.$$

In a similar way, we can check that S_f can act on $S^{-1}M$ as automorphisms and induce ψ_f by the following universal property



And we are going to show that $\left(\psi_f : M_f \to S^{-1}M\right)_{f\in S}$ is the colimit of G.



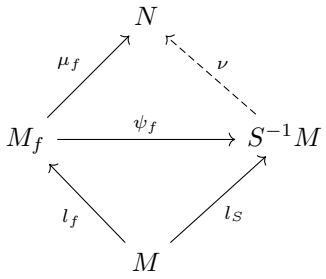
We can prove

$$\psi_f = \psi_g \circ l'_g$$

by checking

$$\left(\psi_g \circ l'_g\right) \circ l_f = \psi_g \circ l_g = l_S = \psi_f \circ l_f$$

and utilizing the uniqueness of the universal property.
Given any $\left(\mu_f : M_f \to S^{-1}M\right)_{f\in S}$ such that $\mu_f = \mu_g \circ l'_g$, note that $\mu_f \circ l_f = \mu_f \circ \mu_g \circ l'_g = \mu_g \circ l_g$. Thus we can define ν to be the unique map such that $\nu \circ l_S = \mu_f \circ l_f$.



Hence we have

$$(\nu \circ \psi_f) \circ l_f = \nu \circ l_S = \mu_f \circ l_f.$$

By the uniqueness of the universal property of M_f, we have $\mu_f = \nu \circ \psi_f$. If there exists another ν' such that $\mu_f = \nu' \circ \psi_f$, there must be $\nu' \circ l_S = \nu' \circ \psi_f \circ l_f = \mu_f \circ l_f = \nu \circ l_S$. The uniqueness of such ν forces $\nu = \nu'$.
Therefore we show that $S^{-1}M \cong \varinjlim_{f\in S} M_f$. □

Proposition 7.2.29

Suppose R is a commutative ring, S, S' are multiplicative sets in R, and M is an R-module. View $S'^{-1}M$ as an R-module, then $S^{-1}\left(S'^{-1}M\right)$ is isomorphic to $(SS')^{-1}M$ as R-modules.

Proof. Define

$$f : S^{-1}\left(S'^{-1}M\right) \longrightarrow (SS')^{-1}M$$
$$\frac{x/s'}{s} \longmapsto \frac{x}{ss'}$$

To show that f is well-defined, suppose that $\frac{x/s'}{s} = \frac{y/t'}{t}$, which means there exists $v \in S$ such that

$$v\left(t\frac{x}{s'} - s\frac{y}{t'}\right) = \frac{vtx}{s'} - \frac{vsy}{t'} = 0.$$

This further implies that there exists $w \in S'$ such that $w(vtt'x - vss'y) = 0$. Then we see there exists $vw \in SS'$ such that $vw(tt'x - ss'y) = 0$, which means $\frac{x}{ss'} = \frac{y}{tt'}$. Thus f is well-defined.

Define

$$\begin{aligned} g : (SS')^{-1} M &\longrightarrow S^{-1}\left(S'^{-1}M\right) \\ \frac{x}{ss'} &\longmapsto \frac{x/s'}{s} \text{ for some } s \in S, s' \in S' \end{aligned}$$

and we can check that g is well-defined in a similar way. It is clear that f and g are linear maps inverse to each other. □

Proposition 7.2.30

Let R be a commutative ring and M be an R-module. Suppose $x \in M$. Then the following are equivalent:

(i) $x = 0$.

(ii) x maps to 0 in $M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \operatorname{Spec} R$.

(iii) x maps to 0 in $M_{\mathfrak{m}}$ for all $\mathfrak{m} \in \operatorname{Max}(R)$.

As a consequence, $M \to \prod_{\mathfrak{p} \in \operatorname{Spec} R} M_{\mathfrak{p}}$ is an injective ring homomorphism.

Proof. (i) $\Longrightarrow$ (ii) and (ii) $\Longrightarrow$ (iii) are clear. It is left to show (iii) $\Longrightarrow$ (i). Let $x \in M$ and

$$\operatorname{Ann}_M(x) = \{r \in R \,|\, rx = 0\}$$

be the annihilator of x in R, which is an ideal of R. Note $\frac{x}{1} = \frac{0}{1}$ in $M_{\mathfrak{m}}$ if and only if

$$\operatorname{Ann}_M - \mathfrak{m} = \{r \in R - \mathfrak{m} \,|\, rx = 0\} \neq \varnothing \iff \operatorname{Ann}_M \subsetneq \mathfrak{m}.$$

If x maps to 0 in $M_{\mathfrak{m}}$ for all $\mathfrak{m} \in \operatorname{Max}(R)$, then Ann_M is not contained in any maximal ideal of R, which means $\operatorname{Ann}_M(x) = R$. Hence $x = 0$. □

Corollary 7.2.31

Given an R-module M, the following are equivalent:

(i) M is zero,

(ii) $M_{\mathfrak{p}}$ is zero for all $\mathfrak{p} \in \operatorname{Spec}(R)$,

(iii) $M_{\mathfrak{m}}$ is zero for all $\mathfrak{m} \in \operatorname{Max}(R)$.

Proof. (iii) $\Longrightarrow$ (i). Suppose $M_{\mathfrak{m}}$ is zero for all $\mathfrak{m} \in \operatorname{Max}(R)$. Given any $x \in M$, since x maps to 0 in $M_{\mathfrak{m}}$ for all $\mathfrak{m} \in \operatorname{Max}(R)$, there must be $x = 0$ by Proposition 7.2.30. Thus M is zero.

□

Corollary 7.2.32 Exactness is a Local Property

Given a sequence of R-modules $M \to M' \to M''$, the following are equivalent:

(i) $M \to M' \to M''$ is exact,

(ii) $M_{\mathfrak{p}} \to M'_{\mathfrak{p}} \to M''_{\mathfrak{p}}$ is exact for all $\mathfrak{p} \in \operatorname{Spec}(R)$,

(iii) $M_{\mathfrak{m}} \to M'_{\mathfrak{m}} \to M''_{\mathfrak{m}}$ is exact for all $\mathfrak{m} \in \operatorname{Max}(R)$.

Proof. (i) $\Longrightarrow$ (ii) because localization is an exact functor. (ii) $\Longrightarrow$ (iii) is clear. It is left to show (iii) $\Longrightarrow$ (i). Let $H = \ker(M' \to M'') / \operatorname{im}(M \to M')$. Since exact functor preserve cohomology, we have

$$H_{\mathfrak{m}} \cong \ker(M'_{\mathfrak{m}} \to M''_{\mathfrak{m}}) / \operatorname{im}(M_{\mathfrak{m}} \to M'_{\mathfrak{m}}) = 0$$

for all $\mathfrak{m} \in \operatorname{Max}(R)$. Thus by Corollary 7.2.31 we have $H = 0$, which implies $M \to M' \to M''$ is exact. □

Proposition 7.2.33 Glueing Functions

Let R be a ring. Let $f_1, \ldots, f_n$ be elements of R generating the unit ideal. Let M be an R-module. The sequence

$$0 \longrightarrow M \xrightarrow{\alpha} \bigoplus_{i=1}^{n} M_{f_i} \xrightarrow{\beta} \bigoplus_{i,j=1}^{n} M_{f_i f_j}$$

is exact, where $\alpha(m) = \left(\frac{m}{1}, \cdots, \frac{m}{1}\right)$ and $\beta\left(\frac{m_1}{f_1^{e_1}}, \cdots, \frac{m_n}{f_n^{e_n}}\right) = \left(\frac{m_i}{f_i^{e_i}} - \frac{m_j}{f_j^{e_j}}\right)_{(i,j)}$.

Proof. According to Corollary 7.2.32, it suffices to show that the localization of the sequence at any maximal ideal $\mathfrak{m}$ is exact. Given any maximal ideal $\mathfrak{m}$ of R, since $f_1, \ldots, f_n$ generate the unit ideal, there is an i such that $f_i \notin \mathfrak{m}$. Without loss of generality we may assume $f_1 \notin \mathfrak{m}$. Note that Proposition 7.2.29 guarantees $(M_{f_i})_{\mathfrak{m}} = (M_{\mathfrak{m}})_{f_i}$ and $(M_{f_i f_j})_{\mathfrak{m}} = (M_{\mathfrak{m}})_{f_i f_j}$. In particular we have $(M_{f_1})_{\mathfrak{m}} = M_{\mathfrak{m}}$ and $(M_{f_1 f_i})_{\mathfrak{m}} = (M_{\mathfrak{m}})_{f_i}$, because $f_1 \in M_{\mathfrak{m}}^{\times}$. Thus it is suffices to show that the sequence

$$0 \longrightarrow M_{\mathfrak{m}} \xrightarrow{\alpha_{\mathfrak{m}}} \bigoplus_{i=1}^{n} (M_{\mathfrak{m}})_{f_i} \xrightarrow{\beta_{\mathfrak{m}}} \bigoplus_{i,j=1}^{n} (M_{\mathfrak{m}})_{f_i f_j}$$

is exact for $f_1 = 1$.

Injectivity of $\alpha_{\mathfrak{m}}$ is trivial because the first component of $\alpha_{\mathfrak{m}}$ is the identity map on $M_{\mathfrak{m}}$.

For any $\mathbf{x} = \left(x_1, \frac{x_2}{f_2^{e_n}}, \cdots, \frac{x_n}{f_n^{e_n}}\right) \in \ker \beta_{\mathfrak{m}}$ we have $\beta_{\mathfrak{m}}(\mathbf{x}) = 0$. Consider the $(1,i)$-component of $\beta_{\mathfrak{m}}(\mathbf{x})$ for $i = 2, \cdots, n$. Then we get

$$x_1 - \frac{x_i}{f_i^{e_i}} = 0 \implies \mathbf{x} = (x_1, x_1, \cdots, x_1) = \alpha_{\mathfrak{m}}(x_1) \implies \ker \beta_{\mathfrak{m}} \subseteq \operatorname{im} \alpha_{\mathfrak{m}}.$$

For any $\mathbf{y} = (y, y, \cdots, y) \in \operatorname{im} \alpha_{\mathfrak{m}}$, we have $\beta_{\mathfrak{m}}(\mathbf{y}) = 0$, which means $\operatorname{im} \alpha_{\mathfrak{m}} \subseteq \ker \beta_{\mathfrak{m}}$. Thus the sequence is exact and we complete the proof. □

7.2.4 Graded Object

Definition 7.2.34 I-Graded Module (External Definition)

Let R be a ring and I be a set. An **I-graded R-module** is a family of R-modules $(M_i)_{i \in I}$. The category of I-graded R-modules, denoted by $R\text{-}\mathsf{Mod}^I$, is simply the functor category $[I, R\text{-}\mathsf{Mod}]$, where I is regarded as a discrete category.

Definition 7.2.35 I-Graded Module (Internal Definition)

Let R be a ring and I be a set. An **I-graded R-module** is an R-module M together with a family of submodules $(M_i)_{i \in I}$ such that

$$M = \bigoplus_{i \in I} M_i.$$

Proposition 7.2.36 $R\text{-}\mathsf{Mod}^I$ is a Monoidal Category

Let R be a ring and I be a commutative monoid. Then $\left(R\text{-}\mathsf{Mod}^I, \otimes\right)$ is a monoidal category with tensor

product defined as

$$(M \otimes N)_i = \bigoplus_{j+k=i} M_j \otimes N_k.$$

Definition 7.2.37 *I*-Graded Module over an Graded Ring (Internal Definition)

Let $(I, +)$ be a monoid and R be a I-graded ring with grading $(R_i)_{i\in I}$. An **I-graded module over graded ring** R is an R-module M together with a family of submodules $(M_i)_{i\in I}$ such that

(i) $M = \bigoplus_{i\in I} M_i$.

(ii) $R_i M_j \subseteq M_{i+j}$ for all $i, j \in I$.

When I is a monoid, Definition 7.2.35 is a special case of Definition 7.2.37 because any ring R can be regarded as a graded ring with trivial grading $R_0 = R$ and $R_i = 0$ for all $i \neq 0$.

7.3 Torsion-Free Modules

Definition 7.3.1 Torsion Element of a Module

Let R be a ring, and let M be a left R-module. An element $m \in M$ is called a **torsion element of** M if there exists a regular element $r \in R$ such that $rm = 0$.
If R is an integral domain, an element $m \in M$ is called a **torsion element of** M if one of the following equivalent conditions holds:

(i) There exists a element $r \in R - \{0\}$ such that $rm = 0$.

(ii) $\mathrm{Ann}_R(m) \neq \{0_R\}$.

Definition 7.3.2 Torsion Submodule

Let R be a ring, and let M be an R-module. The **torsion subset of** M is the subset of M consisting of all torsion elements of M, denoted by M_{tor}. If R is commutative, then M_{tor} is a submodule of M, called the **torsion submodule of** M. If R is an integral domain, then

$$M_{\mathrm{tor}} = \{m \in M \mid \exists r \in R - \{0\},\ rm = 0\}.$$

Proof. We can check that M_{tor} is a submodule of M when R is commutative. For any $m_1, m_2 \in M_{\mathrm{tor}}$, there exist regular elements $r_1, r_2 \in R$ such that $r_1 m_1 = 0$ and $r_2 m_2 = 0$. By Proposition 5.1.6, $r_1 r_2$ is also a regular element. Then we have

$$r_1 r_2 (m_1 + m_2) = r_1 r_2 m_1 + r_1 r_2 m_2 = 0 + 0 = 0 \implies m_1 + m_2 \in M_{\mathrm{tor}},$$

Let $m \in M_{\mathrm{tor}}$ and $r \in R$ be a regular element such that $rm = 0$. Then for any $s \in R$, we have

$$r(sm) = s(rm) = s \cdot 0 = 0 \implies sm \in M_{\mathrm{tor}}.$$

□

Definition 7.3.3 Torsion Module

Let R be a ring, and let M be an R-module. We say M is a **torsion module** if all elements of M are torsion elements, i.e. $M = M_{\mathrm{tor}}$.

Example 7.3.1

Let R be a commutative ring, and let M be an R-module. Then the torsion submodule M_{tor} is a torsion module.

Definition 7.3.4 Torsion-free Module

Let R be a ring, and let M be an R-module. We say M is a **torsion-free module** if 0 is the only torsion element of M, i.e. $M_{\text{tor}} = \{0_M\}$.

Proposition 7.3.5 Characterization of Torsion-Free Modules via Localization

Let R be an integral domain, M be an R-module and $S = R - \{0\}$ be the multiplicative set of R. Then the followings are equivalent:

(i) M is a torsion-free module.

(ii) $M \to S^{-1}M$ is injective.

(iii) We have the following exact sequence

$$0 \longrightarrow M \longrightarrow M \otimes_R \operatorname{Frac}(R).$$

Proof. (i) $\iff$ (ii). Suppose M is a torsion-free module. Suppose

$$\begin{aligned} l_S : M &\longrightarrow S^{-1}M \\ m &\longmapsto \frac{m}{1} \end{aligned}$$

is the localization map. Then according to Proposition 7.2.22, we have

$$\ker l_S = \{m \in M \mid \exists s \in S,\ sm = 0\} = M_{\text{tor}}.$$

Thus

$$M \text{ is torsion-free} \iff M_{\text{tor}} = \{0_M\} \iff \ker l_S = \{0_M\} \iff l_S \text{ is injective.}$$

□

Definition 7.3.6 Torsion-free Quotient

Let R be a commutative ring, and let M be an R-module. Then the quotient module $M_{\text{tf}} := M/M_{\text{tor}}$ is a torsion-free module, called the **torsion-free quotient of** M. This gives a functor $\text{tf} : R\text{-Mod} \to R\text{-Mod}$

$$\begin{array}{ccc} R\text{-Mod} & & R\text{-Mod}_{\text{tf}} \\ M & \overset{\text{tf}}{\rightsquigarrow} & M_{\text{tf}} \ni m + M_{\text{tor}} \\ \downarrow f & & \downarrow \overline{f} \quad\quad \downarrow \\ N & & N_{\text{tf}} \ni f(m) + N_{\text{tor}} \end{array}$$

$R\text{-Mod}_{\text{tf}}$ is a full subcategory of $R\text{-Mod}$ consisting of all torsion-free modules. And we have the adjunction

$$R\text{-Mod} \underset{U}{\overset{\text{tf}}{\rightleftarrows}} R\text{-Mod}_{\text{tf}} \quad (\perp)$$

where $U : R\text{-Mod}_{\text{tf}} \to R\text{-Mod}$ is the inclusion functor.

Proof. Let $m + M_{\text{tor}} \in M/M_{\text{tor}}$ be a torsion element of M/M_{tor}. Then there exists a regular element $r \in R$ such that

$$r\,(m + M_{\text{tor}}) = rm + M_{\text{tor}} = 0 + M_{\text{tor}},$$

which implies $rm \in M_{\text{tor}}$. Thus there exists a regular element $s \in R$ such that $srm = 0$. Since sr is a regular element, we get $m \in M_{\text{tor}}$, which implies $m + M_{\text{tor}} = 0 + M_{\text{tor}}$. Therefore, M/M_{tor} is a torsion-free module.

Next we are to show $f(M_{\text{tor}}) \subseteq N_{\text{tor}}$. For any $m \in M_{\text{tor}}$, there exists a regular element $r \in R$ such that $rm = 0_M$. Then we have

$$rf(m) = f(rm) = f(0_M) = 0_N,$$

which implies $f(m) \in N_{\text{tor}}$. Hence $f(M_{\text{tor}}) \subseteq N_{\text{tor}}$ and accordingly $\pi_N \circ f(M_{\text{tor}}) = \{0\}$, by the universal property of quotient module M/M_{tor}, we have the following commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \pi_M}\downarrow & & \downarrow{\scriptstyle \pi_N} \\ M/M_{\text{tor}} & \xrightarrow[\overline{f}]{} & N/N_{\text{tor}} \end{array}$$

Therefore, $\overline{f}$ is well-defined. □

Definition 7.3.7 $\mathfrak{a}$-Torsion

Let R be a ring, M be a left R-module and $\mathfrak{a}$ be a right ideal of R. The $\mathfrak{a}$-torsion of M is a submodule of M defined as

$$M[\mathfrak{a}] := \{m \in M \mid \forall a \in \mathfrak{a}, am = 0\}.$$

If $\mathfrak{a} = aR$ is a principal right ideal generated by $a \in R$, we simply write $M[a]$ instead of $M[\mathfrak{a}]$.

Proof. We can check that $M[\mathfrak{a}]$ is a submodule of M. For any $m_1, m_2 \in M[\mathfrak{a}]$, we have

$$a(m_1 + m_2) = am_1 + am_2 = 0 + 0 = 0, \quad \forall a \in \mathfrak{a},$$

which implies $m_1 + m_2 \in M[\mathfrak{a}]$. For any $m \in M[\mathfrak{a}]$ and $r \in R$, we have

$$a(rm) = (ar)m = 0, \quad \forall a \in \mathfrak{a},$$

which implies $rm \in M[\mathfrak{a}]$. Therefore, $M[\mathfrak{a}]$ is a submodule of M. □

Lemma 7.3.8

Let R be a ring, M be a left R-module and $\mathfrak{a}$ be a right ideal of R. Then for any $n \in \mathbb{Z}_+$, we have

$$M[\mathfrak{a}^n] \subseteq M[\mathfrak{a}^{n+1}].$$

Proof. For any $m \in M[\mathfrak{a}^n]$ and any $c \in \mathfrak{a}^n$, we have

$$cm = 0.$$

Hence for any $b \in \mathfrak{a}^{n+1}$, there exist $a \in \mathfrak{a}$ and $c' \in \mathfrak{a}^n$ such that $b = ac'$. Then we have

$$bm = ac'm = 0,$$

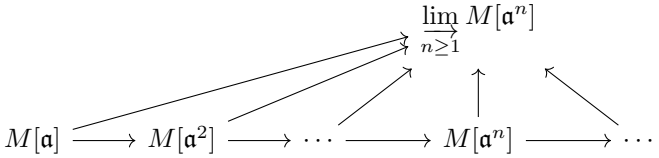
which implies $m \in M[\mathfrak{a}^{n+1}]$. Hence $M[\mathfrak{a}^n]$ is a submodule of $M[\mathfrak{a}^{n+1}]$. □

Definition 7.3.9 $\mathfrak{a}$-Power Torsion

Let R be a ring, M be a left R-module and $\mathfrak{a}$ be a right ideal of R. The $\mathfrak{a}$-power torsion of M is a submodule of M defined as

$$M[\mathfrak{a}^\infty] := \{m \in M \mid \exists n \in \mathbb{Z}_+, \forall a \in \mathfrak{a}^n, am = 0\} = \bigcup_{n \geq 1} M[\mathfrak{a}^n] = \varinjlim_{n \geq 1} M[\mathfrak{a}^n].$$

Proof. By Lemma 7.3.8 we see $M[\mathfrak{a}^n] \subseteq M[\mathfrak{a}^{n+1}]$ for all $n \in \mathbb{Z}_+$.



Therefore, the colimit $M[\mathfrak{a}^\infty] = \varinjlim_{n \geq 1} M[\mathfrak{a}^n]$ is a submodule of M □

Proposition 7.3.10

Let R be an integral domain and M be a finitely generated R-module. Then M is a torsion-free module if and only if M is a submodule of a finitely generated free R-module.

Proposition 7.3.11 Module Homomorphism Induced by Scalar Multiplication

Let R be a ring and M be a left R-module. Suppose N is an R-submodule of M, and $r \in R$. Then

$$\begin{aligned} \mu_r : N &\longrightarrow M, \\ n &\longmapsto rn. \end{aligned}$$

is an R-module homomorphism and we have

$$N/\ker \mu_r \cong \operatorname{im} \mu_r = rN = \{rn \mid n \in N\}.$$

And the following are equivalent:

(i) For any $n \in N$, if $rn = 0$, then $n = 0$.

(ii) μ_r is injective.

(iii) $N \cong rN$.

Corollary 7.3.12

Let R be a commutative ring and $r \in R$. Then the following are equivalent:

(i) r is a regular element.

(ii)
$$0 \longrightarrow R \xrightarrow{\mu_r} R \xrightarrow{\pi} R/rR \longrightarrow 0$$
is a short exact sequence of R-modules.

Proof. (i) $\Longrightarrow$ (ii). Suppose $r \in R$ is a regular element. Then $r \neq 0$. If there exists $n \in R$ such that $rn = 0$, there must be $n = 0$. Thus by Proposition 7.3.11 we have μ_r is injective. Since $\operatorname{im} \mu_r = rR = \ker \pi$, the sequence is exact.

(ii) $\Longrightarrow$ (i). Suppose the sequence is exact. Then μ_r is injective, which by Proposition 7.3.11 implies that for any $n \in R$, if $rn = 0$, then $n = 0$. Thus r is a regular element. □

Proposition 7.3.13

(i) If R is a commutative ring, then any flat R-module is torsion-free.

(ii) If R is a Dedekind domain. Then an R-module is flat if and only if it is torsion-free.

Proof. (i) If there exists $m \in M$ such that $rm = 0$ for some regular element $r \in R$, then by Corollary 7.3.12,

$$0 \longrightarrow R \xrightarrow{\mu_r} R \xrightarrow{\pi} R/rR \longrightarrow 0$$

is a short exact sequence of R-modules. Since M is flat, the functor $- \otimes_R M$ is exact. Thus we have the following exact sequence

$$0 \longrightarrow R \otimes_R M \xrightarrow{\mu_r \otimes 1} R \otimes_R M \xrightarrow{\pi \otimes 1} (R/rR) \otimes_R M \longrightarrow 0,$$

which is isomorphic to

$$0 \longrightarrow M \xrightarrow{\mu_r} M \xrightarrow{\pi} M/rM \longrightarrow 0.$$

According to Proposition 7.3.11, the injectivity of $\mu_r : M \to M$ implies $m = 0$. Therefore, M is torsion-free. □

7.4 Flat Modules

For any R-module M, the functor $- \otimes_R M$ is right exact.

Definition 7.4.1 Flat Module

Let R be a ring. An R-module M is called **flat** if the functor $- \otimes_R M$ is exact.

Proposition 7.4.2 Direct Sum of Flat Modules is Flat

Let R be a ring and $(M_i)_{i \in I}$ be a family of R-modules. If each M_i is flat, then $\bigoplus_{i \in I} M_i$ is flat.

Proof. For any exact sequence $0 \to A \to B \to C \to 0$, we have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

where the rows are exact. Since M_i is flat, we have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A \otimes M_i & \longrightarrow & B \otimes M_i & \longrightarrow & C \otimes M_i & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f \otimes 1} & & \downarrow{\scriptstyle g \otimes 1} & & \downarrow{\scriptstyle h \otimes 1} & & \\ 0 & \longrightarrow & A' \otimes M_i & \longrightarrow & B' \otimes M_i & \longrightarrow & C' \otimes M_i & \longrightarrow & 0 \end{array}$$

where the rows are exact. Then we have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \bigoplus_{i \in I} A \otimes M_i & \longrightarrow & \bigoplus_{i \in I} B \otimes M_i & \longrightarrow & \bigoplus_{i \in I} C \otimes M_i & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \bigoplus_{i \in I} f \otimes 1} & & \downarrow{\scriptstyle \bigoplus_{i \in I} g \otimes 1} & & \downarrow{\scriptstyle \bigoplus_{i \in I} h \otimes 1} & & \\ 0 & \longrightarrow & \bigoplus_{i \in I} A' \otimes M_i & \longrightarrow & \bigoplus_{i \in I} B' \otimes M_i & \longrightarrow & \bigoplus_{i \in I} C' \otimes M_i & \longrightarrow & 0 \end{array}$$

where the rows are exact. Thus $\bigoplus_{i \in I} M_i$ is flat.

□

7.5 Projective Modules

$\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(P, -)$ is a left exact functor.

Definition 7.5.1 Projective Module

Let R be a ring. An R-module P is called **projective** if $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(P, -)$ is an exact functor.

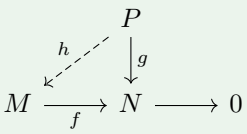
Proposition 7.5.2 Equivalent Definitions of Projective Module

Let R be a ring and P be an R-module. The following are equivalent:

(i) P is projective.

(ii) For any surjective R-module homomorphism $f : M \to N$, the induced map $f^* : \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(P, M) \to \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(P, N)$ is surjective.

(iii) For any surjective R-module homomorphism $f : M \to N$ and any R-module homomorphism $g : P \to N$, there exists an R-module homomorphism $h : P \to M$ such that the following diagram commutes



(iv) P is a direct summand of a free module.

7.6 Module over Commutative Ring

Proposition 7.6.1 R-Mod is a Symmetric Monoidal Category for Commutative Ring R

Let R be a commutative ring. Then the category R-Mod is a symmetric monoidal category with the following structure:

(i) Tensor product: the functor $\otimes_R : R\text{-Mod} \times R\text{-Mod} \to R\text{-Mod}$ defined by

$$\begin{array}{ccc} R\text{-Mod} \times R\text{-Mod} & & R\text{-Mod} \\ (X_1, Y_1) & & X_1 \otimes_R Y_1 \\ {\scriptstyle f\times g}\downarrow & \rightsquigarrow^{\otimes_R} & \downarrow{\scriptstyle f\otimes_R g} \\ (X_2, Y_2) & & X_2 \otimes_R Y_2 \end{array}$$

(ii) Associator: the natural isomorphism a

$$R\text{-Mod} \times R\text{-Mod} \times R\text{-Mod} \;\overset{(-\otimes-)\otimes-}{\underset{-\otimes(-\otimes-)}{\Downarrow a}}\; R\text{-Mod}$$

defined by

$$\begin{aligned} a_{(X,Y,Z)} : (X \otimes_R Y) \otimes_R Z &\longrightarrow X \otimes_R (Y \otimes_R Z) \\ (x \otimes_R y) \otimes_R z &\longmapsto x \otimes_R (y \otimes_R z) \end{aligned}$$

(iii) Unit object: $R \in \mathrm{Ob}(R\text{-Mod})$

(iv) The isomorphism in R-Mod:

$$\begin{aligned} \iota : R \otimes_R R &\longrightarrow R \\ r \otimes_R s &\longmapsto rs \end{aligned}$$

(v) Briad isomorphism: the natural isomorphism B

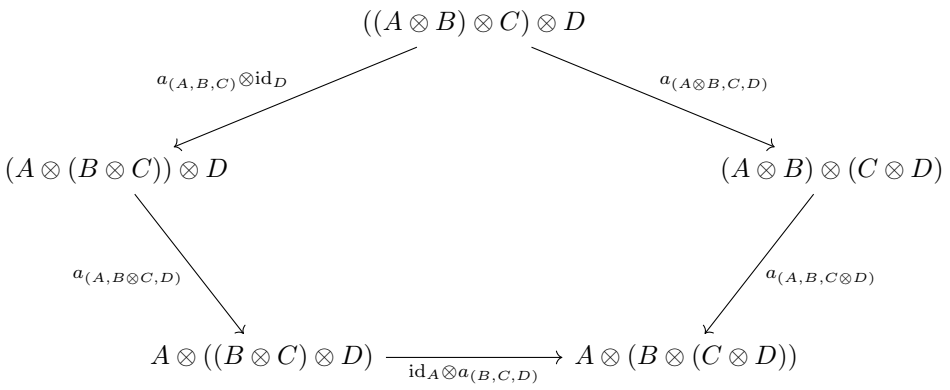
$$R\text{-Mod} \times R\text{-Mod} \;\overset{(-\otimes ?)}{\underset{(?\otimes -)}{\Downarrow B}}\; R\text{-Mod}$$

defined by

$$\begin{aligned} B_{X,Y} : X \otimes_R Y &\longrightarrow Y \otimes_R X \\ x \otimes_R y &\longmapsto y \otimes_R x \end{aligned}$$

Proof. We could check the following conditions holds

(i) The pentagon axiom: the following diagram commutes



(ii) Unit axiom: the functors $R \otimes_R - : R\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$ and $- \otimes_R R : R\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$ are category equivalences.

(iii) Hexagon axiom.

(iv)
$$B_{Y,X} \circ B_{X,Y} = \mathrm{id}_{X \otimes_R Y}.$$

□

R-Mod is an abelian category, so it is Ab-enriched. When R is a commutative ring, R-Mod is even self-enriched.

Proposition 7.6.2 *R-Mod is a Self-Enriched Category for Commutative Ring R*

If R is a commutative ring, then the category R-Mod is self-enriched. More explicitly, the category R-Mod is an R-Mod-enriched category with the following structure:

(i) Hom-object: for each pair of objects $A, B \in \mathrm{Ob}(R\text{-}\mathsf{Mod})$, the object $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(A, B) \in \mathrm{Ob}(R\text{-}\mathsf{Mod})$, where the R-module structure on $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(A, B)$ is defined pointwise as follows:

- addition:

$$\begin{aligned} + : \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(A, B) \times \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(A, B) &\longrightarrow \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(A, B) \\ (f, g) &\longmapsto (a \mapsto f(a) + g(a)) \end{aligned}$$

- scalar multiplication:

$$\begin{aligned} R \times \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(A, B) &\longrightarrow \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(A, B) \\ (r, f) &\longmapsto (a \mapsto r \cdot f(a)) \end{aligned}$$

(ii) Composition: for each triple of objects $A, B, C \in \mathrm{Ob}(R\text{-}\mathsf{Mod})$, the composition morphism in R-Mod defined by

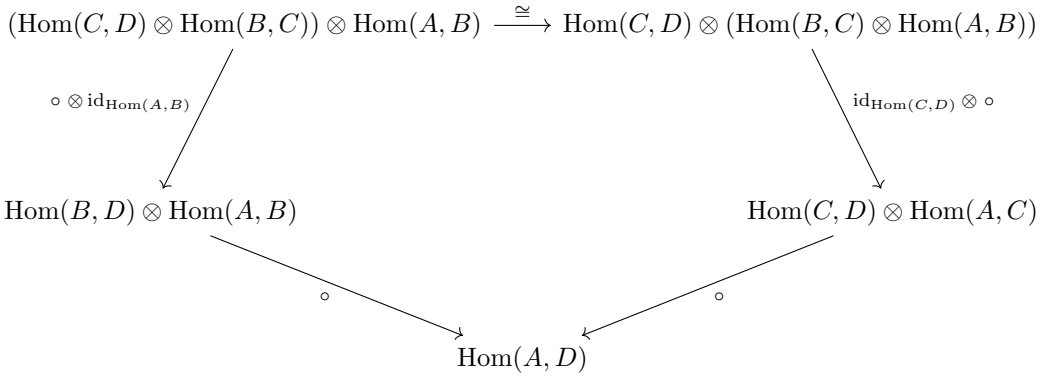
$$\begin{aligned} \circ : \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(B, C) \otimes_R \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(A, B) &\longrightarrow \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(A, C) \\ g \otimes_R f &\longmapsto g \circ f \end{aligned}$$

(iii) Identity: for each object $A \in \mathrm{Ob}(R\text{-}\mathsf{Mod})$, the morphism in R-Mod defined by

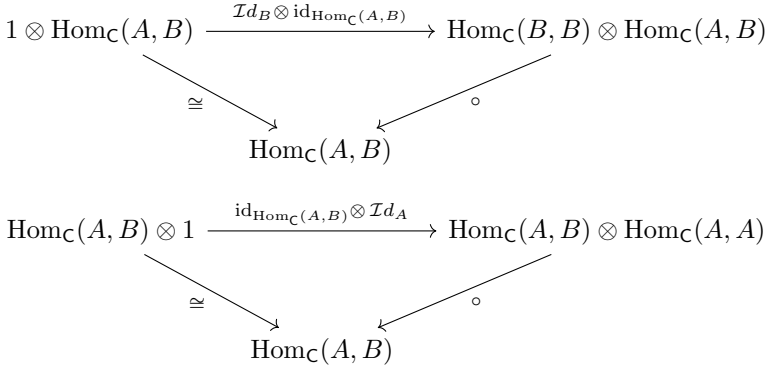
$$\begin{aligned} \mathcal{I}d_A : R &\longrightarrow \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(A, A) \\ r &\longmapsto (r \cdot \mathrm{id}_A : x \mapsto r \cdot x) \end{aligned}$$

Proof. the following conditions hold

(i) For each quadruple of objects $A, B, C, D \in \mathrm{Ob}(\mathsf{C})$, the following diagram in R-Mod commutes



(ii) For each pair of objects $A, B \in \mathrm{Ob}(\mathsf{C})$, the following diagrams in V commute



□

7.7 Free Module of Finite Rank over Commutative Ring

7.7.1 Determinant

Definition 7.7.1 Determinant of R-linear Transformation on Free Module of Finite Rank

Let R be a commutative ring and M be a free R-module of finite rank n. The **determinant** of an R-linear map $f : M \to M$ can be defined as one of the following equivalent ways:

(i) The functor $\wedge^n : R\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$ induces a map between hom-sets

$$\begin{aligned} \wedge^n : \mathrm{End}_{R\text{-}\mathsf{Mod}}(M) &\longrightarrow \mathrm{End}_{R\text{-}\mathsf{Mod}}(\wedge^n(M)) \\ f &\longmapsto f \wedge \cdots \wedge f. \end{aligned}$$

Note $\mathrm{End}_{R\text{-}\mathsf{Mod}}(\wedge^n(M))$ is a 1-dimensional R-module with basis $\mathrm{id}_{\wedge^n(M)}$. And R is a also a 1-dimensional R-module with basis 1_R. We have the following R-module isomorphism

$$\begin{aligned} \mathrm{coor}_{\mathrm{id}_{\wedge^n(M)}} : \mathrm{End}_{R\text{-}\mathsf{Mod}}(\wedge^n(M)) &\xrightarrow{\sim} R \\ \mathrm{id}_{\wedge^n(M)} &\longmapsto 1_R. \end{aligned}$$

The **determinant** map is defined as the composition

$$\begin{aligned} \det := \mathrm{coor}_{\mathrm{id}_{\wedge^n(M)}} \circ \wedge^n : \mathrm{End}_{R\text{-}\mathsf{Mod}}(M) &\longrightarrow R \\ f &\longmapsto \det(f) := \mathrm{coor}_{\mathrm{id}_{\wedge^n(M)}}(f \wedge \cdots \wedge f). \end{aligned}$$

$\det(f)$ is called the determinant of f.

(ii) Suppose $\{e_1, \cdots, e_n\}$ is a baisis of M, then for any $f \in \mathrm{End}_{R\text{-Mod}}(M)$, it can be uniquely represented by a matrix $A = (a_{ij})$ with respect to the basis $\{e_1, \cdots, e_n\}$

$$(f(e_1), \cdots, f(e_n)) = (e_1, \cdots, e_n)A.$$

Then the **determinant** of f is defined as follows

$$\begin{aligned} \det : \mathrm{End}_{R\text{-Mod}}(M) &\longrightarrow R \\ f &\longmapsto \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}. \end{aligned}$$

7.8 Finitely Generated Module over PID

Proposition 7.8.1 Torsion-free $\iff$ Free for Finitely Generated Modules over PID

Let R be a PID and M be a finitely generated R-module. Then M is torsion-free if and only if M is free.

Proposition 7.8.2

Let R be a PID and M be a free R-module. Then any submodule N of M is free. Moreover, we have $\mathrm{rk}_R(N) \leq \mathrm{rk}_R(M)$.

Proposition 7.8.3

Let R be a PID and M be an R-module. If $M_{\mathrm{tf}} = M/M_{\mathrm{tor}}$ is finitely generated, then

(i) M_{tf} is free.

(ii) $M = M_{\mathrm{tor}} \oplus E$, where E is a free submodule of M with $\mathrm{rk}_R(E) < \infty$.

Proof. Since M_{tf} is finitely generated, it is a finitely generated torsion-free module over PID, which is free. Then we have $M_{\mathrm{tf}} \cong R^{\oplus n}$ for some $n \in \mathbb{Z}_+$. Let $\{e_1, \ldots, e_n\}$ be a basis of M_{tf}. For any $m \in M$, we have $m = \sum_{i=1}^{n} r_i e_i$ for some $r_i \in R$. Define $E := \bigoplus_{i=1}^{n} Re_i$. Then we have $M = M_{\mathrm{tor}} \oplus E$. □

Proposition 7.8.4 Smith Normal Form

Let R be a PID and $M \in \mathrm{Mat}_{m\times n}(R)$ be an $m \times n$ matrix with entries in R. Then there exist invertible matrices $P \in \mathrm{GL}_m(R)$ and $Q \in \mathrm{GL}_n(R)$ such that

$$PMQ = \begin{bmatrix} d_1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & d_r & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}$$

where $d_i \in R$ are such that $d_i \mid d_{i+1}$ for all $1 \leq i < r$ and $r = \mathrm{rank}(M)$.

Chapter 8

Associative Algebra

8.1 Basic Properties

Definition 8.1.1 Associative Algebra over Commutative Ring

Let R be a commutative ring. An **associative R-algebra** is a ring A together with a ring homomorphism $\varphi : R \to Z(A)$, which makes A an R-module by defining the scalar multiplication as

$$\begin{aligned} R \times A &\longrightarrow A \\ (r, a) &\longmapsto r \cdot a := \varphi(r)a. \end{aligned}$$

$\varphi : R \to Z(A)$ is called the **structure homomorphism** of A.

Remark. We can check that

$$r \cdot (ab) = \sigma(r)ab = (r \cdot a)b = \sigma(r)ab = a\,(\sigma(r)b) = a(r \cdot b),$$

which justifies the naming "associative". □

We usually call associative R-algebra as R-algebra for short.

Proposition 8.1.2 Commutative Ring homomorphism $R \to S$ induces functor S-Alg $\to R$-Alg

Let R and S be commutative rings with a ring homomorphism $f : R \to S$. Then every S-algebra A is an R-algebra by defining $ra = f(r)a$, or equivalently through $R \to S \to Z(A)$. This defines a functor $F : S\text{-Alg} \to R\text{-Alg}$, which is identify map on objects and morphisms.

$$\begin{array}{ccc} S\text{-Alg} & & R\text{-Alg} \\ A & & A \\ {\scriptstyle g}\downarrow & \rightsquigarrow^{F} & \downarrow{\scriptstyle g} \\ B & & B \end{array}$$

In particular, commutative ring homomorphism $R \to S$ makes S an R-algebra.

8.2 Construction

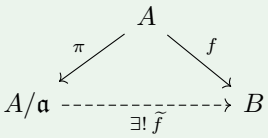
8.2.1 Quotient Object

Definition 8.2.1 Quotient Algebra

Let A be an R-algebra and $\mathfrak{a}$ be a two-sided ideal of A. Since $\mathfrak{a}$ is an R-submodule of A, the quotient ring $A/\mathfrak{a}$ can also be endowed with an R-module structure, which makes $A/\mathfrak{a}$ an R-algebra. We call $A/\mathfrak{a}$ the **quotient algebra** of A by $\mathfrak{a}$.

Proposition 8.2.2 Universal Property of Quotient Algebra

Let A be an R-algebra and $\mathfrak{a}$ be a two-sided ideal of A. Let $\pi : A \to A/\mathfrak{a}$ be the canonical projection. For any R-algebra homomorphism $f : A \to B$ such that $\mathfrak{a} \subseteq \ker(f)$ or equivalently $f(\mathfrak{a}) = \{0\}$, there exists a unique R-algebra homomorphism $\widetilde{f} : A/\mathfrak{a} \to B$ such that the following diagram commutes



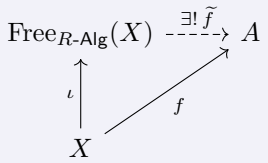
The unique R-algebra homomorphism $\widetilde{f} : A/\mathfrak{a} \to B$ is defined as

$$\begin{aligned} \widetilde{f} : A/\mathfrak{a} &\longrightarrow B \\ a + \mathfrak{a} &\longmapsto f(a). \end{aligned}$$

8.2.2 Free Object

Definition 8.2.3 Free R-Algebra

Let X be a set and R be a commutative ring. The **free R-algebra** on X, denoted by $\mathrm{Free}_{R\text{-}\mathsf{Alg}}(X)$, together with a function $\iota : X \to \mathrm{Free}_{R\text{-}\mathsf{Alg}}(X)$, is defined by the following universal property: for any R-algebra A and any function $f : X \to A$, there exists a unique R-algebra homomorphism $\widetilde{f} : \mathrm{Free}_{R\text{-}\mathsf{Alg}}(X) \to A$ such that the following diagram commutes



The free R-algebra $\mathrm{Free}_{R\text{-}\mathsf{Alg}}(X)$ can be contructed by direct sum of copies of R

$$\mathrm{Free}_{R\text{-}\mathsf{Alg}}(X) \cong \bigoplus_{w \in \mathrm{Free}_{\mathsf{Mon}}(X)} Rw.$$

8.2.3 Graded Object

Definition 8.2.4 I-Graded Algebra over an Graded Commutative Ring

Let $(I, +)$ be a monoid and R be a I-graded commutative ring with grading $(R_i)_{i \in I}$. An **I-graded algebra over graded ring** R is an R-algebra A together with a family of subalgebras $(A_i)_{i \in I}$ such that

(i) $A = \bigoplus_{i \in I} A_i$.

(ii) $A_i A_j \subseteq A_{i+j}$ for all $i, j \in I$.

(iii) $R_i A_j \subseteq A_{i+j}$ for all $i, j \in I$.

Elements in A_i are called **homogeneous elements of degree** i.

Definition 8.2.5 Degree-preserving R-algebra homomorphism

Let $(I, +)$ be a monoid and let $R = \bigoplus_{i \in I} R_i$ be an I-graded commutative ring. Let $A = \bigoplus_{i \in I} A_i$ and $B = \bigoplus_{i \in I} B_i$ be I-graded R-algebras. An R-algebra homomorphism $f : A \to B$ is called **degree-preserving** (or **graded**) if for every $i \in I$,

$$f(A_i) \subseteq B_i.$$

We write GrAlg_R^I for the category whose objects are I-graded R-algebras and whose morphisms are degree-preserving R-algebra homomorphisms.

Proposition 8.2.6 Graded Algebra Quotients out Graded Ideal

Let A be an I-graded algebra over graded ring R with grading $(A_i)_{i\in I}$ and $\mathfrak{a}$ be a I-graded two-sided ideal of A. Then we have an R-module isomorphism

$$\begin{aligned} A_i/\left(\mathfrak{a}\cap A_i\right) &\xrightarrow{\sim} \left(A_i+\mathfrak{a}\right)/\mathfrak{a} \\ a+\left(\mathfrak{a}\cap A_i\right) &\longmapsto a+\mathfrak{a}, \end{aligned}$$

and the quotient algebra $A/\mathfrak{a}$ has a decomposition

$$A/\mathfrak{a}=\bigoplus_{i\in I}\left(A_i+\mathfrak{a}\right)/\mathfrak{a}\cong\bigoplus_{i\in I}A_i/\left(\mathfrak{a}\cap A_i\right),$$

which makes $A/\mathfrak{a}$ an I-graded R-algebra.

Proof. By the definition of graded ideal, we have

$$\mathfrak{a}=\bigoplus_{i\in I}\mathfrak{a}_i,\quad \mathfrak{a}_i:=\mathfrak{a}\cap A_i.$$

Let $\pi: A\to A/\mathfrak{a}$ be the canonical projection. Restrict π to A_i, we have an R-module homomorphism

$$\pi|_{A_i}: A_i\longrightarrow \pi(A_i)$$

with kernel

$$\ker\left(\pi|_{A_i}\right)=\{x\in A_i\,|\,\pi(x)=0+\mathfrak{a}\}=\{x\in A_i\,|\,x\in\mathfrak{a}\}=A_i\cap\mathfrak{a}=\mathfrak{a}_i.$$

Thus we have an R-module isomorphism

$$\begin{aligned} A_i/\mathfrak{a}_i &\xrightarrow{\sim}\pi(A_i) \\ a+\mathfrak{a}_i &\longmapsto a+\mathfrak{a}. \end{aligned}$$

Take any $\pi(a)\in A/\mathfrak{a}$, where $a\in A$. Since $A=\bigoplus_{i\in I}A_i$, we can write $a=\sum_{i\in I}a_i$ with $a_i\in A_i$ and only finitely many a_i being nonzero. Thus

$$\pi(a)=\pi\left(\sum_{i\in I}a_i\right)=\sum_{i\in I}\pi(a_i)\in\sum_{i\in I}\pi(A_i),$$

which means $A/\mathfrak{a}\subseteq\sum_{i\in I}\pi(A_i)$. On the other hand, we have $\sum_{i\in I}\pi(A_i)\subseteq A/\mathfrak{a}$. Therefore, we have $A/\mathfrak{a}=\sum_{i\in I}\pi(A_i)$.

Moreover, if $\sum_{i\in I}\pi(a_i)=0$ with $a_i\in A_i$, then $\pi\left(\sum_{i\in I}a_i\right)=0$, which means $\sum_{i\in I}a_i\in\mathfrak{a}$. According to Proposition 5.2.17, this implies $a_i\in\mathfrak{a}\cap A_i$ for all $i\in I$. Thus we have $\pi(a_i)=0$ for all $i\in I$. Therefore, the sum $A/\mathfrak{a}=\sum_{i\in I}\pi(A_i)$ is direct, which means

$$A/\mathfrak{a}=\bigoplus_{i\in I}\pi(A_i).$$

Note

$$\pi(A_i)=\{x+\mathfrak{a}\,|\,x\in A_i\}=\{x+a+\mathfrak{a}\,|\,x\in A_i,a\in\mathfrak{a}\}=\left(A_i+\mathfrak{a}\right)/\mathfrak{a}.$$

Combining these results, we have the R-module isomorphism

$$A/\mathfrak{a}=\bigoplus_{i\in I}\pi(A_i)=\bigoplus_{i\in I}\left(A_i+\mathfrak{a}\right)/\mathfrak{a}\cong\bigoplus_{i\in I}A_i/\left(\mathfrak{a}\cap A_i\right).$$

Finally, we can check that the multiplication and scalar multiplication respect the grading:

$$\begin{aligned} \left(a_i+\mathfrak{a}\right)\left(a_j+\mathfrak{a}\right)&=a_ia_j+\mathfrak{a}\in\left(A_{i+j}+\mathfrak{a}\right)/\mathfrak{a},\quad \forall a_i\in A_i,a_j\in A_j, \\ r\cdot\left(a_i+\mathfrak{a}\right)&=ra_i+\mathfrak{a}\in\left(A_{i+j}+\mathfrak{a}\right)/\mathfrak{a},\quad \forall r\in R_j,a_i\in A_i. \end{aligned}$$

□

Example 8.2.1 Polynomial Algebra $R[X_1, \cdots, X_n]$

Let R be a commutative ring and $X_1, \cdots, X_n$ be indeterminates. Then $R[X_1, \cdots, X_n]$ is an $\mathbb{N}$-graded R-algebra with grading $R[X_1, \cdots, X_n]_i$ being the set of homogeneous polynomials of degree i.

8.2.4 Tensor Product

Definition 8.2.7 Tensor Product of Algebras

Let R be a commutative ring and A, B be R-algebras. The **tensor product of R-algebras A and B** is defined by the following universal property: for any triple (C, f_A, f_B), where C is an R-algebra and $f_A : A \to C$, $f_B : B \to C$ are R-algebra homomorphisms which satisfy

$$f_A(a)f_B(b) = f_B(b)f_A(a), \quad \forall a \in A, b \in B,$$

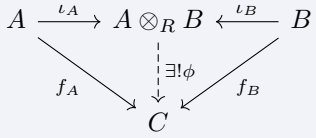
the tensor product

$$(A \otimes_R B, \iota_A : A \times B \to A \otimes_R B, \iota_B : A \times B \to A \otimes_R B)$$

is initial among such triples, i.e. there exists a unique R-algebra homomorphism

$$\phi : A \otimes_R B \longrightarrow C$$

such that the following diagram commutes



Concretely, $A \otimes_R B$ can be constructed as the tensor product of R-modules $A \otimes_R B$ together with multiplication defined as

$$(a_1 \otimes b_1)(a_2 \otimes b_2) := (a_1a_2) \otimes (b_1b_2), \quad \forall a_1, a_2 \in A, b_1, b_2 \in B$$

and unity

$$1_{A \otimes_R B} := 1_A \otimes 1_B.$$

And the R-algebra homomorphisms ι_A, ι_B are defined as

$$\begin{aligned} \iota_A : A &\longrightarrow A \otimes_R B \\ a &\longmapsto a \otimes 1_B, \end{aligned}$$

$$\begin{aligned} \iota_B : B &\longrightarrow A \otimes_R B \\ b &\longmapsto 1_A \otimes b. \end{aligned}$$

The unique R-algebra homomorphism $\phi : A \otimes_R B \to C$ is defined as

$$\begin{aligned} \phi : A \otimes_R B &\longrightarrow C \\ a \otimes b &\longmapsto f_A(a)f_B(b). \end{aligned}$$

Remark. It is straightforward to check that the multiplication defined above is well-defined and makes $A \otimes_R B$ an R-algebra. According to Proposition 7.2.16, since $(a, b) \mapsto f_A(a)f_B(b)$ is $\mathbb{Z}$-bilinear, ϕ is a well-defined abelian group homomorphism. We can further check that ϕ is an R-algebra homomorphism:

$$\phi(r(a \otimes b)) = \phi((ra) \otimes b) = f_A(ra)f_B(b) = rf_A(a)f_B(b) = r\phi(a \otimes b)$$

$$\phi\left((a_1 \otimes b_1)(a_2 \otimes b_2)\right) = \phi\left((a_1a_2) \otimes (b_1b_2)\right) = f_A(a_1a_2)f_B(b_1b_2) = f_A(a_1)f_A(a_2)f_B(b_1)f_B(b_2) = \phi(a_1 \otimes b_1)\phi(a_2 \otimes b_2)$$

$$\phi\left(1_{A \otimes_R B}\right) = \phi\left(1_A \otimes 1_B\right) = f_A(1_A)f_B(1_B) = 1_C$$

□

Definition 8.2.8 Tensor Product of R-algebra Homomorphisms

Let R be a commutative ring and A_1, A_2, B_1, B_2 be R-algebras. Given two R-algebra homomorphisms $f : A_1 \to A_2$ and $g : B_1 \to B_2$, the **tensor product of R-algebra homomorphisms** is defined as the R-algebra homomorphism

$$\begin{aligned} f \otimes_R g : A_1 \otimes_R B_1 &\longrightarrow A_2 \otimes_R B_2 \\ a \otimes b &\longmapsto f(a) \otimes g(b). \end{aligned}$$

which is induced by the universal property of tensor product $A_1 \otimes_R B_1$ through the following commutative diagram:

$$\begin{array}{ccccc} A_1 & \xrightarrow{\iota_{A_1}} & A_1 \otimes_R B_1 & \xleftarrow{\iota_{B_1}} & B_2 \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f \otimes_R g} & & \downarrow{\scriptstyle g} \\ A_2 & \xrightarrow[\iota_{A_2}]{} & A_2 \otimes_R B_2 & \xleftarrow[\iota_{B_2}]{} & B_2 \end{array}$$

Proposition 8.2.9 Symmetric Monoidal Structure on R-Alg

Let R be a commutative ring. The tensor product $\otimes_R$ defines a symmetric monoidal structure on the category R-Alg, with unit object R.

(i) Tensor product: the tensor product functor is

$$\begin{array}{ccc} R\text{-Alg} \times R\text{-Alg} & & R\text{-Alg} \\ (A_1, B_1) & & A_1 \otimes_R B_1 \\ {\scriptstyle f \times g}\downarrow & \overset{\otimes_R}{\rightsquigarrow} & \downarrow{\scriptstyle f \otimes_R g} \\ (A_2, B_2) & & A_2 \otimes_R B_2 \end{array}$$

(ii) Associator: for any R-algebras A, B, C, there is a natural isomorphism

$$\begin{aligned} \alpha_{A,B,C} : (A \otimes_R B) \otimes_R C &\xrightarrow{\sim} A \otimes_R (B \otimes_R C) \\ (a \otimes b) \otimes c &\longmapsto a \otimes (b \otimes c) \end{aligned}$$

(iii) Unit object: R.

(iv) An isomorphism in R-Alg:

$$\begin{aligned} \iota : R \otimes_R R &\xrightarrow{\sim} R \\ r \otimes r' &\longmapsto rr' \end{aligned}$$

(v) Symmetry: for any R-algebras A, B, there is a natural isomorphism

$$\begin{aligned} \gamma_{A,B} : A \otimes_R B &\xrightarrow{\sim} B \otimes_R A \\ a \otimes b &\longmapsto b \otimes a \end{aligned}$$

Proposition 8.2.10 Tensor Product of Quotient Algebras

Let R be a commutative ring and A_1, A_2 be R-algebras. Let $I_1 \subseteq A_1$, $I_2 \subseteq A_2$ be two-sided ideals of A_1, A_2 respectively. Then we have an R-algebra isomorphism

$$\begin{aligned} (A_1/I_1) \otimes_R (A_2/I_2) &\xrightarrow{\sim} (A_1 \otimes_R A_2)/(I_1 \otimes_R A_2 + A_1 \otimes_R I_2) \\ \overline{a_1} \otimes \overline{a_2} &\longmapsto \overline{a_1 \otimes a_2} \end{aligned}$$

Here, given inclusion $i_1 : I_1 \hookrightarrow A_1$, the R-module $I_1 \otimes_R A_2$ is identified as the image of $i_1 \otimes_R \mathrm{id}_{A_2} : I_1 \otimes_R A_2 \to A_1 \otimes_R A_2$

$$\mathrm{im}\,(i_1 \otimes_R \mathrm{id}_{A_2}) = \left\{ \sum_{n=1}^{m} x_n \otimes y_n \in A_1 \otimes_R A_2 \,\middle|\, m \in \mathbb{Z}_{\geq 1},\, x_n \in I_1,\, y_n \in A_2 \right\},$$

which is a two-sided ideal of $A_1 \otimes_R A_2$. The similar identification applies to $A_1 \otimes_R I_2$.

Proof. Let $J := I_1 \otimes_R A_2 + A_1 \otimes_R I_2$. Define

$$\begin{aligned} \iota_1 : A_1/I_1 &\longrightarrow (A_1 \otimes_R A_2)/J \\ a_1 + I_1 &\longmapsto (a_1 \otimes 1_{A_2}) + J, \end{aligned}$$

If $a_1, a_1' \in A_1$ satisfy $a_1 - a_1' \in I_1$, then

$$(a_1 \otimes 1_{A_2}) - (a_1' \otimes 1_{A_2}) = (a_1 - a_1') \otimes 1_{A_2} \in I_1 \otimes_R A_2 \subseteq J \implies (a_1 \otimes 1_{A_2}) + J = (a_1' \otimes 1_{A_2}) + J,$$

which shows that ι_1 is well-defined. And we can check that ι_1 is an R-algebra homomorphism. Similarly, we can define an R-algebra homomorphism

$$\begin{aligned} \iota_2 : A_2/I_2 &\longrightarrow (A_1 \otimes_R A_2)/J \\ a_2 + I_2 &\longmapsto (1_{A_1} \otimes a_2) + J. \end{aligned}$$

Moreover, the images of ι_1 and ι_2 commute in $(A_1 \otimes_R A_2)/J$: for any $a_1 \in A_1$, $a_2 \in A_2$,

$$\begin{aligned} \iota_1(a_1 + I_1)\iota_2(a_2 + I_2) &= ((a_1 \otimes 1_{A_2}) + J)\,((1_{A_1} \otimes a_2) + J) \\ &= (a_1 \otimes a_2) + J \\ &= ((1_{A_1} \otimes a_2) + J)\,((a_1 \otimes 1_{A_2}) + J) \\ &= \iota_2(a_2 + I_2)\iota_1(a_1 + I_1). \end{aligned}$$

Thus by the universal property of tensor product, there exists a unique R-algebra homomorphism

$$\begin{aligned} \varphi : (A_1/I_1) \otimes_R (A_2/I_2) &\longrightarrow (A_1 \otimes_R A_2)/J \\ (a_1 + I_1) \otimes (a_2 + I_2) &\longmapsto (a_1 \otimes a_2) + J. \end{aligned}$$

Next, we construct the inverse of φ. Given the quotient maps $\pi_1 : A_1 \to A_1/I_1$ and $\pi_2 : A_2 \to A_2/I_2$, we can define an R-algebra homomorphism $\psi := \pi_1 \otimes_R \pi_2$ as

$$\begin{aligned} \psi : A_1 \otimes_R A_2 &\longrightarrow (A_1/I_1) \otimes_R (A_2/I_2) \\ a_1 \otimes a_2 &\longmapsto (a_1 + I_1) \otimes (a_2 + I_2). \end{aligned}$$

Since for any $x \in I_1$, $y \in A_2$, we have

$$\psi(x \otimes y) = (0 + I_1) \otimes (y + I_2) = 0$$

and for any $x \in A_1$, $y \in I_2$, we have

$$\psi(x \otimes y) = (x + I_1) \otimes (0 + I_2) = 0,$$

we have $J \subseteq \ker(\psi)$. Thus, by the universal property of quotient algebra, there exists a unique R-algebra homomorphism

$$\begin{aligned} \widetilde{\psi} : (A_1 \otimes_R A_2)/J &\longrightarrow (A_1/I_1) \otimes_R (A_2/I_2) \\ (a_1 \otimes a_2) + J &\longmapsto (a_1 + I_1) \otimes (a_2 + I_2). \end{aligned}$$

We can check that $\widetilde{\psi}$ is the inverse of φ:

$$\begin{aligned} \widetilde{\psi} \circ \varphi\,((a_1 + I_1) \otimes (a_2 + I_2)) = \widetilde{\psi}\,((a_1 \otimes a_2) + J) = (a_1 + I_1) \otimes (a_2 + I_2), \\ \varphi \circ \widetilde{\psi}\,((a_1 \otimes a_2) + J) = \varphi\,((a_1 + I_1) \otimes (a_2 + I_2)) = (a_1 \otimes a_2) + J. \end{aligned}$$

Therefore, we show that φ is an R-algebra isomorphism. □

Corollary 8.2.11 *mod I* Reduction of R-Algebras

Let R be a commutative ring and $I \subseteq R$ be an ideal of R. For any R-algebra A, there is an isomorphism of R-algebras

$$\begin{aligned} A/IA &\xrightarrow{\sim} A \otimes_R (R/I) \\ \overline{a} &\longmapsto a \otimes \overline{1_R} \\ \overline{ra} &\longmapsto a \otimes \overline{r} \end{aligned}$$

where

$$IA := \{ra \in A \,|\, r \in I,\, a \in A\}$$

is the two-sided ideal of A generated by I.

Proof. Apply Proposition 8.2.10 with $A_1 = A$, $A_2 = R$, $I_1 = \{0\}$, $I_2 = I$. We obtain an R-algebra isomorphism

$$\begin{aligned} A \otimes_R (R/I) &\xrightarrow{\sim} (A \otimes_R R)/(0 \otimes_R R + A \otimes_R I) \\ a \otimes (r + I) &\longmapsto (a \otimes r) + (A \otimes_R I). \end{aligned}$$

Under the canonical isomorphism

$$\begin{aligned} \phi : A \otimes_R R &\xrightarrow{\sim} A \\ a \otimes r &\longmapsto ra, \end{aligned}$$

$A \otimes_R I$ is mapped to IA. Thus we have an R-algebra isomorphism

$$\begin{aligned} A \otimes_R (R/I) &\xrightarrow{\sim} A/IA \\ a \otimes (r + I) &\longmapsto ra + IA. \end{aligned}$$

□

Corollary 8.2.12

Let R be a commutative ring and $I \subseteq R$ be an ideal of R. We have a cononical isomorphism of R-algebras

$$\begin{aligned} (R/I) \otimes_R (R/I) &\xrightarrow{\sim} R/I \\ (r + I) \otimes (r' + I) &\longmapsto rr' + I. \end{aligned}$$

Proof. By Corollary 8.2.11, we have an R-algebra isomorphism

$$\begin{aligned} (R/I) \otimes_R (R/I) &\xrightarrow{\sim} (R/I)/(I(R/I)) \\ (r + I) \otimes (r' + I) &\longmapsto rr' + I(R/I). \end{aligned}$$

Since for any $r \in I$, $r' + I \in R/I$, we have

$$r(r' + I) = rr' + I = 0 + I,$$

which shows that $I(R/I) = \{0\}$. Thus we obtain the desired isomorphism. □

8.2.5 Tensor Algebra

Definition 8.2.13 Tensor Algebra $T^\bullet(M)$

Given a R-module M, the **k-th tensor power of** M is defined as

$$\begin{aligned} T^k(M) &:= M^{\otimes k} = \underbrace{M \otimes_R \cdots \otimes_R M}_{k \text{ times}}, \\ T^0(M) &:= R. \end{aligned}$$

The **tensor algebra** of M is defined as

$$T^\bullet(M) := \bigoplus_{k=0}^{\infty} T^k(M)$$

with multiplication $\otimes$ defined as

$$(m_1 \otimes \cdots \otimes m_k) \otimes (m_{k+1} \otimes \cdots \otimes m_{k+l}) = m_1 \otimes \cdots \otimes m_{k+l}$$

$T^\bullet(M)$ is an $\mathbb{N}$-graded R-algebra with grading $(T^k(M))_{k\geq 0}$.

Proposition 8.2.14 Tensor Algebra Functor $T^\bullet : R\text{-Mod} \to \mathsf{GrAlg}_R^{\mathbb{N}}$

Let R be a commutative ring. The tensor algebra construction $T^\bullet : R\text{-}\mathsf{Mod} \to \mathsf{GrAlg}_R^{\mathbb{N}}$ is a functor defined as follows

$$\begin{array}{ccc} R\text{-}\mathsf{Mod} & & \mathsf{GrAlg}_R^{\mathbb{N}} \\ M & & T^\bullet(M) \ni \quad m_1 \otimes \cdots \otimes m_k \\ \Big\downarrow{\scriptstyle g} & \overset{T^\bullet}{\rightsquigarrow} & \Big\downarrow{\scriptstyle T^\bullet(g)} \qquad\qquad \Big\downarrow{\scriptstyle g\otimes g\cdots\otimes g} \\ N & & T^\bullet(N) \ni g(m_1) \otimes \cdots \otimes g(m_k) \end{array}$$

Proof. According to Definition 8.2.8, for each $k \geq 0$, we can define an R-module homomorphism $T^k(g) := g^{\otimes k}$ on degree-k component:

$$\begin{aligned} &T^k(g) : T^k(M) \longrightarrow T^k(N) \\ &m_1 \otimes \cdots \otimes m_k \longmapsto g(m_1) \otimes \cdots \otimes g(m_k). \end{aligned}$$

Then we can define a degree-preserving R-algebra homomorphism $T^\bullet(g) := \bigoplus_{k=0}^{\infty} T^k(g)$ as follows:

$$\begin{aligned} &T^\bullet(g) : T^\bullet(M) \longrightarrow T^\bullet(N) \\ &(x_0, x_1, x_2, \cdots) \longmapsto \left(T^0(g)(x_0),\, T^1(g)(x_1),\, T^2(g)(x_2), \cdots\right). \end{aligned}$$

It is straightforward to check that $T^\bullet(\mathrm{id}_M) = \mathrm{id}_{T^\bullet(M)}$ and $T^\bullet(g_2 \circ g_1) = T^\bullet(g_2) \circ T^\bullet(g_1)$ for any R-module homomorphisms $g_1 : M \to N$, $g_2 : N \to P$. Thus, $T^\bullet$ is a functor. □

Proposition 8.2.15 Adjunction $T^\bullet \dashv U_{\mathsf{R\text{-}Mod}}$

Let R be a commutative ring. Suppose $U : R\text{-}\mathsf{Alg} \to R\text{-}\mathsf{Mod}$ is the forgetful functor. Then the tensor algebra functor $T^\bullet : R\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Alg}$ is left adjoint to U.

8.2.6 Exterior Algebra and Symmetric Algebra

Definition 8.2.16 Exterior Algebra $\wedge^\bullet(M)$

Given an R-module M,

$$I_\wedge(M) := \langle x \otimes x : x \in M \rangle = \left\{ \sum_{i=1}^{m} a_i (x_i \otimes x_i) b_i \,\middle|\, m \in \mathbb{Z}_{\geq 1},\, a_i, b_i \in T^\bullet(M),\, x_i \in M \right\}$$

is a graded two-sided ideal of $T^\bullet(M)$. The **exterior algebra** of M is defined as

$$\wedge^\bullet(M) = T^\bullet(M)/I_\wedge(M).$$

According to Proposition 8.2.6, $\wedge^\bullet(M)$ is a graded R-algebra with grading

$$\wedge^\bullet(M) \cong \bigoplus_{k=0}^{\infty} \wedge^k(M)$$

where

$$\bigwedge^k(M) := T^k(M)/\left(I_\wedge(M) \cap T^k(M)\right)$$

is an R-module and is called the **k-th exterior power of** M. Especially, we have $\bigwedge^0(M) \cong R$ and $\bigwedge^1(M) \cong M$ as R-modules, and we identify them directly.
The multiplication of $\bigwedge^\bullet(M)$ is denoted by

$$\begin{aligned} \wedge : \bigwedge^\bullet(M) \times \bigwedge^\bullet(M) &\longrightarrow \bigwedge^\bullet(M) \\ (a + I_\wedge(M), b + I_\wedge(M)) &\longmapsto (a \otimes b) + I_\wedge(M). \end{aligned}$$

and is called the **wedge product**. The graded version of the wedge product for degree-1 elements is given by

$$\begin{aligned} \wedge : \bigwedge^1(M) \times \bigwedge^1(M) &\longrightarrow \bigwedge^2(M) \\ (m_1, m_2) &\longmapsto m_1 \wedge m_2 := (m_1 \otimes m_2) + I_\wedge(M) \cap T^2(M) \end{aligned}$$

We can prove $\bigwedge^k(M)$ is an R-module generated by the elements of the form

$$m_1 \wedge m_2 \wedge \cdots \wedge m_k = (m_1 \otimes m_2 \otimes \cdots \otimes m_k) + I_\wedge(M) \cap T^k(M)$$

for $m_1, m_2, \cdots, m_k \in M$. The wedge product for degree-k and degree-l elements is given by

$$\begin{aligned} \wedge : \bigwedge^k(M) \times \bigwedge^l(M) &\longrightarrow \bigwedge^{k+l}(M) \\ (m_1 \wedge \cdots \wedge m_k,\ m_{k+1} \wedge \cdots \wedge m_{k+l}) &\longmapsto m_1 \wedge \cdots \wedge m_k \wedge m_{k+1} \wedge \cdots \wedge m_{k+l} \end{aligned}$$

where $m_i \in M$ for $1 \leq i \leq k + l$.

Remark. Since $T^k(M)$ is an R-module generated by the pure tensors of the form $m_1 \otimes m_2 \otimes \cdots \otimes m_k$ for $m_i \in M$, the quotient module $\bigwedge^k(M) = T^k(M)/\left(I_\wedge(M) \cap T^k(M)\right)$ is generated by the elements of the form $(m_1 \otimes m_2 \otimes \cdots \otimes m_k) + I_\wedge(M) \cap T^k(M)$. And by induction on k, we can show that

$$m_1 \wedge m_2 \wedge \cdots m_k = (m_1 \otimes m_2 \otimes \cdots \otimes m_k) + I_\wedge(M) \cap T^k(M).$$

□

Proposition 8.2.17

Given an R-module M and $m_1, m_2 \in M$, we have

$$m_1 \wedge m_2 = -m_2 \wedge m_1.$$

For any homogeneous elements $x, y \in \bigwedge^\bullet(M)$, we have

$$x \wedge y = (-1)^{\deg(x)\deg(y)} y \wedge x.$$

Definition 8.2.18 Exterior Algebra Functor: $\bigwedge^\bullet : R\text{-Mod} \to \mathsf{GrAlg}_R^{\mathbb{N}}$

The exterior algebra construction $\bigwedge^\bullet : R\text{-Mod} \to \mathsf{GrAlg}_R^{\mathbb{N}}$ is a functor defined as follows

$$\begin{array}{ccc} R\text{-Mod} & & \mathsf{GrAlg}_R^{\mathbb{N}} \\ M & & \bigwedge^\bullet(M) \ni \quad m_1 \wedge \cdots \wedge m_k \\ \Big\downarrow{\scriptstyle f} & \rightsquigarrow^{\bigwedge^\bullet} & \Big\downarrow{\scriptstyle \bigwedge^\bullet(f)} \qquad\quad \Big\downarrow{\scriptstyle f\wedge f\wedge\cdots\wedge f} \\ N & & \bigwedge^\bullet(N) \ni f(m_1) \wedge \cdots \wedge f(m_k) \end{array}$$

where $\bigwedge^\bullet(f)$ is induced by the universal property of the quotient algebra $T^\bullet(M)/I_\wedge(M)$ through the

following commutative diagram

$$\begin{array}{ccc} T^\bullet(M) & \xrightarrow{T^\bullet(f)} & T^\bullet(N) \\ \downarrow{\scriptstyle \pi_M} & & \downarrow{\scriptstyle \pi_N} \\ T^\bullet(M)/I_\wedge(M) & \xrightarrow[\wedge^\bullet(f)]{} & T^\bullet(N)/I_\wedge(N) \end{array}$$

Remark. Since for any $x \in M$,

$$\pi_N \circ T^\bullet(f)(x \otimes x) = \pi_N(f(x) \otimes f(x)) = f(x) \wedge f(x) + I_\wedge(N) = 0 + I_\wedge(N),$$

we see each generator of $I_\wedge(M)$ is mapped to 0 in $\pi_N \circ T^\bullet(f)$. Thus, we have $I_\wedge(M) \subseteq \ker(\pi_N \circ T^\bullet(f))$, which guarantees that there exists a unique R-algebra homomorphism

$$\begin{aligned} \textstyle\bigwedge^\bullet(f) : \bigwedge^\bullet(M) &\longrightarrow \bigwedge^\bullet(N) \\ m_1 \wedge \cdots \wedge m_k &\longmapsto f(m_1) \wedge \cdots \wedge f(m_k). \end{aligned}$$

such that $\bigwedge^\bullet(f) \circ \pi_M = \pi_N \circ T^\bullet(f)$. □

Proposition 8.2.19 Adjunction $\bigwedge^\bullet \dashv U_{\mathsf{R\text{-}Mod}}$

Let R be a commutative ring. Suppose $U_{\mathsf{R\text{-}Mod}} : \mathsf{GrAlg}_R^{\mathbb{N}} \to R\text{-}\mathsf{Mod}$ is the forgetful functor. Then the exterior algebra functor $\bigwedge^\bullet : R\text{-}\mathsf{Mod} \to \mathsf{GrAlg}_R^{\mathbb{N}}$ is left adjoint to U.

Example 8.2.2 Take Degree k Functor

Let R be a commutative ring and M be an R-module. The **take degree k functor** is defined as

$$\begin{array}{ccc} \mathsf{GrAlg}_R^{\mathbb{N}} & & R\text{-}\mathsf{Mod} \\ A = \bigoplus_{i=0}^{\infty} A_i & & A_k \\ \downarrow{\scriptstyle g} & \rightsquigarrow^{(-)_k} & \downarrow{\scriptstyle g|_{A_k}} \\ B = \bigoplus_{i=0}^{\infty} B_i & & B_k \end{array}$$

In particular, we have the composition functor $\bigwedge^k := (-)_k \circ \bigwedge^\bullet : R\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$ defined as follows

$$\begin{array}{ccccc} R\text{-}\mathsf{Mod} & & R\text{-}\mathsf{Mod} & & \\ M & & \bigwedge^k(M) \ni & m_1 \wedge \cdots \wedge m_k \\ \downarrow{\scriptstyle f} & \rightsquigarrow^{\bigwedge^k} & \downarrow{\scriptstyle \bigwedge^k(f)} & \downarrow{\scriptstyle f \wedge f \cdots \wedge f} \\ N & & \bigwedge^k(N) \ni & f(m_1) \wedge \cdots \wedge f(m_k) \end{array}$$

Proposition 8.2.20

Suppose R is a commutative ring and $M = \bigoplus_{x \in X} Rx$ is a free R-module. Then

(i) $\bigwedge^\bullet(M)$ has a basis $\{x_1 \wedge \cdots \wedge x_k : x_1, \cdots, x_k \in X, x_i \neq x_j \text{ for all } i \neq j\}$.

(ii) If M has a basis $\{x_1, \cdots, x_n\}$, then we have an R-linear isomorphism

$$\begin{aligned} \wedge^n(M) &\xrightarrow{\sim} R \\ x_1 \wedge \cdots \wedge x_n &\longmapsto 1_R. \end{aligned}$$

Moreover, we have $\wedge^m(M) = 0$ for all $m > n$.

8.3 Integral Element

Definition 8.3.1 Integral Element

Let R be a commutative ring and A be an R-algebra with structure homomorphism $\varphi : R \to Z(A)$. An element $x \in A$ is called **integral** over R if there exists a monic polynomial $f \in R[T]$ such that ${}^{\varphi}f(x) = 0$.

Definition 8.3.2 Generated Subalgebra

Let R be a commutative ring and A be an R-algebra. By the universal property of $R\langle T\rangle$, there exists a unique R-algebra homomorphism $\psi : R\langle T\rangle \to A$ such that $\psi(T) = x$.

$$\begin{array}{ccc} R\langle T\rangle & \overset{\exists!\,\psi}{\dashrightarrow} & A \\ {\scriptstyle\iota}\uparrow & \nearrow_{\mathrm{const}_x} & \\ \{T\} & & \end{array}$$

The **R-subalgebra of A generated by x** is defined as

$$R[x] := \psi\left(R\langle T\rangle\right) = \left\{ \sum_{k=0}^{n} r_k x^k \in A \;\middle|\; r_k \in R \right\}.$$

Proposition 8.3.3 Equivalent Definition of Integral Element

Let R be a commutative ring and A be an R-algebra. Let $R[x]$ be the R-subalgebra of A generated by x. Then A is an $R[x]$-module. And the following statements are equivalent:

(i) x is integral over R.

(ii) $R[x]$ is a finitely generated R-module.

(iii) There exists a faithful $R[x]$-submodule of A that is finitely generated as an R-module and contains x.

8.4 Trace and Norm

Lemma 8.4.1 Left Multiplication Endomorphism

Let R be a commutative ring and A be an R-algebra. For any $a \in A$, we can define the left multiplication endomorphism $l_a \in \mathrm{End}_{R\text{-}\mathsf{Mod}}(A)$ by

$$\begin{aligned} l_a : A &\longrightarrow A \\ x &\longmapsto ax. \end{aligned}$$

Moreover,

$$\begin{aligned} l_- : A &\longrightarrow \mathrm{End}_{R\text{-}\mathsf{Mod}}(A) \\ a &\longmapsto l_a \end{aligned}$$

is an R-algebra homomorphism.

Proof. For any $r \in R$, $a, b \in A$ and $x \in A$, we have

$$\begin{aligned} l_{ra+b}(x) &= (ra+b)x = r(ax) + bx = (ra)x + bx = l_{ra}(x) + l_b(x), \\ l_{ab}(x) &= (ab)x = a(bx) = l_a(l_b(x)), \\ l_{1_A}(x) &= 1_A x = x. \end{aligned}$$

Hence l_- is an R-algebra homomorphism. □

Definition 8.4.2 Trace, Norm and Characteristic Polynomial

Let R be a commutative ring and A be an R-algebra. Suppose A as an R-module is free of finite rank. For any $a \in A$, we can define the left multiplication endomorphism $l_a \in \mathrm{End}_{R\text{-}\mathsf{Mod}}(A)$ by

$$\begin{aligned} l_a : A &\longrightarrow A \\ x &\longmapsto ax. \end{aligned}$$

- The **trace** of $a \in A$ is defined as the trace of l_a, denoted by

  $$\mathrm{Tr}_{A|R}(a) := \mathrm{Tr}(l_a) \in R.$$

  That is, $\mathrm{Tr}_{A|R} : A \to R$ is an R-module homomorphism through the following composition

  $$\mathrm{Tr}_{A|R} : A \xrightarrow{l_-} \mathrm{End}_{R\text{-}\mathsf{Mod}}(A) \xrightarrow{\mathrm{Tr}} R.$$

- The **norm** of $a \in A$ is defined as the determinant of l_a, denoted by

  $$\mathrm{N}_{A|R}(a) := \det(l_a) \in R.$$

  That is, $\mathrm{N}_{A|R} : A \to R$ is a multiplicative monoid homomorphism through the following composition

  $$\mathrm{N}_{A|R} : A \xrightarrow{l_-} \mathrm{End}_{R\text{-}\mathsf{Mod}}(A) \xrightarrow{\det} R.$$

- The **characteristic polynomial** of $a \in A$ is defined as the characteristic polynomial of l_a, denoted by

  $$\mathrm{char}_{A|R}(a; X) := \mathrm{char}(l_a; X) = \det(X \cdot \mathrm{id}_A - l_a) = \mathrm{N}_{A[X]|R[X]}(X - a) \in R[X]$$

Proposition 8.4.3 Trace, Norm, and Characteristic Polynomial under Change of Base Ring

Let R be a commutative ring, A be an commutative R-algebra and M be a free R-module of finite rank. Suppose A as an R-module is free of finite rank. Given any A-linear transformation $\varphi \in \mathrm{End}_{A\text{-}\mathsf{Mod}}(M)$, by applying the functor of restriction of scalars to $R \to A$, we can regard φ as an R-linear transformation on M through $\mathrm{End}_{A\text{-}\mathsf{Mod}}(M) \hookrightarrow \mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$. And we have

(i) $\mathrm{Tr}_R(\varphi) = \mathrm{Tr}_{A|R}(\mathrm{Tr}_A(\varphi))$.

(ii) $\mathrm{N}_R(\varphi) = \mathrm{N}_{A|R}(\mathrm{N}_A(\varphi))$.

(iii) $\mathrm{char}_R(\varphi; X) = \mathrm{N}_{A[X]|R[X]}(\mathrm{char}_A(\varphi; X))$.

Corollary 8.4.4

Let R be a commutative ring, A be an commutative R-algebra and B be an A-algebra. Suppose A as an R-module is free of finite rank and B as an A-module is free of finite rank. Then for any $b \in B$, we have

(i) $\mathrm{Tr}_{B|R}(b) = \mathrm{Tr}_{A|R}(\mathrm{Tr}_{B|A}(b))$.

(ii) $\mathrm{N}_{B|R}(b) = \mathrm{N}_{A|R}(\mathrm{N}_{B|A}(b))$.

(iii) $\mathrm{char}_{B|R}(b;X) = \mathrm{N}_{A[X]|R[X]}(\mathrm{char}_{B|A}(b;X))$.

Proof. This is a direct consequence of Proposition 8.4.3 by taking $M = A$ and $\varphi = l_b$. □

Definition 8.4.5 Trace Pairing

Let R be a commutative ring and A be an R-algebra. Suppose A as an R-module is free of finite rank. The **trace pairing** is the symmetric R-bilinear form

$$\begin{aligned}\langle\cdot,\cdot\rangle_{A|R} : A \times A &\longrightarrow R\\ (x,y) &\longmapsto \mathrm{Tr}_{A|R}(xy).\end{aligned}$$

8.4.1 Discriminant

We first define the discriminant of a polynomial.

Definition 8.4.6 Resultant

Let R be a commutative ring and

$$\begin{aligned}f(X) &= a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in R[X],\\ g(X) &= b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0 \in R[X]\end{aligned}$$

be two polynomials of degree n and m respectively. The **resultant** of $f(X)$ and $g(X)$ is defined as

$$\mathrm{Res}(f,g) := \det \begin{bmatrix} \underbrace{\begin{matrix} a_n & 0 & \cdots & 0 \\ a_{n-1} & a_n & \cdots & 0 \\ a_{n-2} & a_{n-1} & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_n \\ a_0 & a_1 & \cdots & a_{n-1} \\ 0 & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_0 \end{matrix}}_{m \text{ columns}} & \underbrace{\begin{matrix} b_m & 0 & \cdots & 0 \\ b_{m-1} & b_m & \cdots & 0 \\ b_{m-2} & b_{m-1} & \ddots & \vdots \\ \vdots & \vdots & \ddots & b_m \\ b_0 & b_1 & \cdots & b_{m-1} \\ 0 & b_0 & \cdots & b_{m-2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_0 \end{matrix}}_{n \text{ columns}} \end{bmatrix}_{(m+n)\times(m+n)}.$$

If R is an integral domain with field of fractions K and $f(X), g(X)$ have roots $\alpha_1, \alpha_2, \cdots, \alpha_n$ and $\beta_1, \beta_2, \cdots, \beta_m$ in some algebraic closure $\overline{K}$ of K respectively, then

$$\mathrm{Res}(f,g) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) = a_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_m^n \prod_{j=1}^{m} f(\beta_j).$$

Remark. Suppose R is an integral domain with field of fractions K and $f(X), g(X)$ have roots $\alpha_1, \alpha_2, \cdots, \alpha_n$ and $\beta_1, \beta_2, \cdots, \beta_m$ in some algebraic closure $\overline{K}$ of K respectively. Then we have

$$\begin{aligned}\frac{1}{a_n} f(X) &= (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n),\\ \frac{1}{b_m} g(X) &= (X - \beta_1)(X - \beta_2)\cdots(X - \beta_m).\end{aligned}$$

Let

$$V = \begin{bmatrix} \alpha_1^{m+n-1} & \alpha_1^{m+n-2} & \cdots & \alpha_1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_n^{m+n-1} & \alpha_n^{m+n-2} & \cdots & \alpha_n & 1 \\ \beta_1^{m+n-1} & \beta_1^{m+n-2} & \cdots & \beta_1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \beta_m^{m+n-1} & \beta_m^{m+n-2} & \cdots & \beta_m & 1 \end{bmatrix}, \quad S = \begin{bmatrix} a_n & 0 & \cdots & 0 & b_m & 0 & \cdots & 0 \\ a_{n-1} & a_n & \cdots & 0 & b_{m-1} & b_m & \cdots & 0 \\ a_{n-2} & a_{n-1} & \ddots & \vdots & b_{m-2} & b_{m-1} & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_n & \vdots & \vdots & \ddots & b_m \\ a_0 & a_1 & \cdots & a_{n-1} & b_0 & b_1 & \cdots & b_{m-1} \\ 0 & a_0 & \cdots & a_{n-2} & 0 & b_0 & \cdots & b_{m-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0 \end{bmatrix}.$$

Then

$$VS = \begin{bmatrix} \alpha_1^{m-1}f(\alpha_1) & \alpha_1^{m-2}f(\alpha_1) & \cdots & f(\alpha_1) & \alpha_1^{n-1}g(\alpha_1) & \alpha_1^{n-2}g(\alpha_1) & \cdots & g(\alpha_1) \\ \alpha_2^{m-1}f(\alpha_2) & \alpha_2^{m-2}f(\alpha_2) & \cdots & f(\alpha_2) & \alpha_2^{n-1}g(\alpha_2) & \alpha_2^{n-2}g(\alpha_2) & \cdots & g(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_n^{m-1}f(\alpha_n) & \alpha_n^{m-2}f(\alpha_n) & \cdots & f(\alpha_n) & \alpha_n^{n-1}g(\alpha_n) & \alpha_n^{n-2}g(\alpha_n) & \cdots & g(\alpha_n) \\ \beta_1^{m-1}f(\beta_1) & \beta_1^{m-2}f(\beta_1) & \cdots & f(\beta_1) & \beta_1^{n-1}g(\beta_1) & \beta_1^{n-2}g(\beta_1) & \cdots & g(\beta_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_m^{m-1}f(\beta_m) & \beta_m^{m-2}f(\beta_m) & \cdots & f(\beta_m) & \beta_m^{n-1}g(\beta_m) & \beta_m^{n-2}g(\beta_m) & \cdots & g(\beta_m) \end{bmatrix} = \begin{bmatrix} \mathbf{0}_{n\times m} & D_g \\ D_f & \mathbf{0}_{m\times n}. \end{bmatrix}$$

This implies that

$$\begin{aligned} \det(V)\det(S) &= \det(VS) \\ &= (-1)^{mn}\det(D_g)\det(D_f) \\ &= (-1)^{mn}\left(\prod_{i=1}^{n} g(\alpha_i) \prod_{1\le i<j\le n}(\alpha_i-\alpha_j)\right)\left(\prod_{j=1}^{m} f(\beta_j) \prod_{1\le i<j\le m}(\beta_i-\beta_j)\right). \end{aligned}$$

Since $\det(V)$ is a Vandermonde determinant, we have

$$\det(V) = \prod_{1\le i<j\le n}(\alpha_i-\alpha_j) \prod_{1\le i<j\le m}(\beta_i-\beta_j) \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j)$$

Thus

$$\det(S) = \frac{(-1)^{mn}\prod_{i=1}^{n} g(\alpha_i)\prod_{j=1}^{m} f(\beta_j)}{\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j)}.$$

Note

$$\begin{aligned} \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j) &= \prod_{i=1}^{n}\frac{g(\alpha_i)}{b_m} = \frac{1}{b_m^n}\prod_{i=1}^{n} g(\alpha_i) \\ = (-1)^{mn}\prod_{j=1}^{m}\prod_{i=1}^{n}(\beta_j-\alpha_i) &= (-1)^{mn}\prod_{j=1}^{m}\frac{f(\beta_j)}{a_n} = \frac{(-1)^{mn}}{a_n^m}\prod_{j=1}^{m} f(\beta_j). \end{aligned}$$

We can conclude that

$$\det(S) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j) = a_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_m^n \prod_{j=1}^{m} f(\beta_j).$$

□

Definition 8.4.7 Discriminant of Polynomial

Let R be an integral domain and $f(X) \in R[X]$ be a polynomial. The **discriminant** of $f(X)$ is defined as

$$\mathrm{Disc}(f) := (-1)^{\frac{n(n-1)}{2}} \frac{\mathrm{Res}(f, f')}{a_n}.$$

Proposition 8.4.8

Let K be a field and $f(X) \in K[X]$ be a polynomial of degree n with roots $\alpha_1, \alpha_2, \cdots, \alpha_n$ in some algebraic closure $\overline{K}$ of K. Then

$$\mathrm{Disc}(f) = (-1)^{\frac{n(n-1)}{2}} a_n^{n-2} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-2} \prod_{\substack{i,j \\ i \neq j}} (\alpha_i - \alpha_j) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Proof. By definition of resultant, we have

$$\mathrm{Disc}(f) = (-1)^{\frac{n(n-1)}{2}} \frac{\mathrm{Res}(f, f')}{a_n} = (-1)^{\frac{n(n-1)}{2}} \frac{a_n^{n-1} \prod_{i=1}^{n} f'(\alpha_i)}{a_n} = (-1)^{\frac{n(n-1)}{2}} a_n^{n-2} \prod_{i=1}^{n} f'(\alpha_i).$$

Since

$$f'(X) = \frac{\mathrm{d}}{\mathrm{d}X} \left(a_n \prod_{i=1}^{n} (X - \alpha_i) \right) = a_n \sum_{i=1}^{n} \prod_{j \neq i} (X - \alpha_j) \implies f'(\alpha_i) = a_n \prod_{j \neq i} (\alpha_i - \alpha_j),$$

we have

$$\prod_{i=1}^{n} f'(\alpha_i) = \prod_{i=1}^{n} \left(a_n \prod_{j \neq i} (\alpha_i - \alpha_j) \right) = a_n^n \prod_{\substack{i,j \\ i \neq j}} (\alpha_i - \alpha_j).$$

Thus

$$\mathrm{Disc}(f) = (-1)^{\frac{n(n-1)}{2}} a_n^{n-2} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-2} \prod_{\substack{i,j \\ i \neq j}} (\alpha_i - \alpha_j).$$

Note

$$\begin{aligned} \prod_{\substack{i,j \\ i \neq j}} (\alpha_i - \alpha_j) &= \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)(\alpha_j - \alpha_i) \\ &= \prod_{1 \leq i < j \leq n} -(\alpha_i - \alpha_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2. \end{aligned}$$

We get

$$\mathrm{Disc}(f) = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-2} \prod_{\substack{i,j \\ i \neq j}} (\alpha_i - \alpha_j) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

□

Definition 8.4.9 Discriminant of Bilinear Form $M \times M \to R$

Let R be a commutative ring and M be an free R-module of rank n. Let $Q : M \times M \to R$ be a R-bilinear form. Then

$$\begin{aligned} \varphi_Q : M &\longrightarrow M^* \\ x &\longmapsto Q(x, -) \end{aligned}$$

is an R-module homomorphism. Taking top exterior powers gives an R-module homomorphism

$$\begin{aligned} \bigwedge^n(\varphi_Q) : \bigwedge^n(M) &\longrightarrow \bigwedge^n(M^*) \\ x_1 \wedge \cdots \wedge x_n &\longmapsto \varphi_Q(x_1) \wedge \cdots \wedge \varphi_Q(x_n). \end{aligned}$$

Note we have natural isomorphisms

$$\begin{aligned} \psi_M : \bigwedge^n(M^*) &\xrightarrow{\sim} (\bigwedge^n(M))^* \\ f_1 \wedge \cdots \wedge f_n &\longmapsto (x_1 \wedge \cdots \wedge x_n \mapsto \det\left([f_i(x_j)]_{1\le i,j\le n}\right)), \end{aligned}$$

By composing $\bigwedge^n(\varphi_Q)$ with ψ_M, we get an R-module endomorphism of the rank-1 free R-module $\bigwedge^n(M)$

$$\begin{aligned} \theta := \psi_M \circ \bigwedge^n(\varphi_Q) : \bigwedge^n(M) &\longrightarrow (\bigwedge^n(M))^* \\ x_1 \wedge \cdots \wedge x_n &\longmapsto (x_1 \wedge \cdots \wedge x_n \mapsto \det\left([Q(x_i, x_j)]_{1\le i,j\le n}\right)). \end{aligned}$$

Let ε be a basis of $\bigwedge^n(M)$ and

$$\begin{aligned} \varepsilon^* : \bigwedge^n(M) &\longrightarrow R \\ \varepsilon &\longmapsto 1_R. \end{aligned}$$

be the dual basis of ε. Then there exists a unique $\lambda \in R$ such that

$$\theta(\varepsilon) = \lambda \cdot \varepsilon^*.$$

Then the **discriminantof** Q is defined as the image of λ under the canonical projection $R \to R/(R^\times)^2$

$$\mathrm{Disc}(Q) := \lambda \mod (R^\times)^2 \in R/(R^\times)^2,$$

where $R/(R^\times)^2$ is the quotient monoid of the multiplicative monoid R by modulo the congruence relation

$$a \sim b \iff \exists u \in R^\times, a = u^2 b.$$

We can check that this definition is independent of the choice of basis ε. If we choose another basis $\tilde{\varepsilon} = c\varepsilon$ for some $c \in R^\times$, then $\tilde{\varepsilon}^* = c^{-1}\varepsilon^*$ and

$$\theta(\tilde{\varepsilon}) = \theta(c\varepsilon) = c\theta(\varepsilon) = c\lambda\varepsilon^* = c\lambda(c\tilde{\varepsilon}^*) = (c^2\lambda) \cdot \tilde{\varepsilon}^*.$$

If $E = \{e_1, e_2, \cdots, e_n\}$ is a basis of M, then the **discriminant of Q with respect to the basis** $\{e_1, e_2, \cdots, e_n\}$ is defined as

$$\mathrm{Disc}(Q; e_1, e_2, \cdots, e_n) := \det\left([Q(e_i, e_j)]_{1\le i,j\le n}\right) \in R.$$

The relation between $\mathrm{Disc}(Q)$ and $\mathrm{Disc}(Q; e_1, e_2, \cdots, e_n)$ is given by

$$\mathrm{Disc}(Q) = \mathrm{Disc}(Q; e_1, e_2, \cdots, e_n) \mod (R^\times)^2 \in R/(R^\times)^2.$$

The ideal of R generated by $\mathrm{Disc}(Q; e_1, e_2, \cdots, e_n)$ is called the **discriminant ideal of** Q, which is independent of the choice of basis $\{e_1, e_2, \cdots, e_n\}$.

Remark. Here we check the relation between $\mathrm{Disc}(Q)$ and $\mathrm{Disc}(Q; e_1, e_2, \cdots, e_n)$. Let $\langle \cdot, \cdot \rangle : M^* \times M \to R$ be the

dual pairing defined by $\langle f, x\rangle := f(x)$. Note $\varepsilon := e_1 \wedge e_2 \wedge \cdots \wedge e_n$ is a basis of $\wedge^n(M)$. Then we have

$$\langle \theta(\varepsilon), \varepsilon\rangle = \langle \lambda\varepsilon^*, \varepsilon\rangle = \lambda\langle \varepsilon^*, \varepsilon\rangle = \lambda.$$

Denote

$$f_i := \varphi_Q(e_i) \in M^*.$$

We have

$$\begin{aligned}\langle \theta(\varepsilon), \varepsilon\rangle &= \langle \psi_M(f_1 \wedge f_2 \wedge \cdots \wedge f_n), e_1 \wedge e_2 \wedge \cdots \wedge e_n\rangle \\ &= \det\left([f_i(e_j)]_{1\le i,j\le n}\right) \\ &= \det\left([\varphi_Q(e_i)(e_j)]_{1\le i,j\le n}\right) \\ &= \det\left([Q(e_i, e_j)]_{1\le i,j\le n}\right).\end{aligned}$$

□

Definition 8.4.10 Discriminant of Algebra

Let R be a commutative ring and A be an R-algebra. Suppose A is a free R-module of rank n. Then the **discriminant** of A over R is defined as

$$d_A = \mathrm{Disc}\left(\langle\cdot,\cdot\rangle_{A|R}\right)$$

where $\langle\cdot,\cdot\rangle_{A|R}$ is the trace pairing of A over R.
Assume $\{e_1, e_2, \cdots, e_n\}$ is a basis of A over R. The **discriminant** of A with respect to the basis $\{e_1, e_2, \cdots, e_n\}$ is defined as

$$\begin{aligned}d_A(e_1, e_2, \cdots, e_n) :&= \det\left(\left[\langle e_i, e_j\rangle_{A|R}\right]_{1\le i,j\le n}\right) \\ &= \det\begin{bmatrix}\mathrm{Tr}_{A|R}(e_1e_1) & \mathrm{Tr}_{A|R}(e_1e_2) & \cdots & \mathrm{Tr}_{A|R}(e_1e_n) \\ \mathrm{Tr}_{A|R}(e_2e_1) & \mathrm{Tr}_{A|R}(e_2e_2) & \cdots & \mathrm{Tr}_{A|R}(e_2e_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}_{A|R}(e_ne_1) & \mathrm{Tr}_{A|R}(e_ne_2) & \cdots & \mathrm{Tr}_{A|R}(e_ne_n)\end{bmatrix} \in R.\end{aligned}$$

The relation between d_A and $d_A(e_1, e_2, \cdots, e_n)$ is given by

$$d_A = d_A(e_1, e_2, \cdots, e_n) \mod (R^\times)^2.$$

The ideal of R generated by $d_A(e_1, e_2, \cdots, e_n)$ is called the **discriminant ideal of A over R** and is denoted by $\mathfrak{d}_A$.

Definition 8.4.11 Order

Let R be an integral domain with field of fractions K and A be a finite-dimensional K-algebra. An R-**order** in A is a unital R-subalgebra $\mathcal{O} \subseteq A$ which is finitely generated as an R-module and satisfies $\mathcal{O} \otimes_R K \cong A$.

Remark. Since the K-algebra A can be regarded as an R-algebra through the restriction of scalars along $R \hookrightarrow K$, it makes sense to talk about R-subalgebras of A. □

Lemma 8.4.12

Let R be a commutative ring, M be a free R-module of rank n and $N \subseteq M$ be a submodule which is also a free R-module of rank n. Let $Q : M \times M \to R$ be a R-bilinear form.

(i) Given any basis $\{e_1, e_2, \cdots, e_n\}$ of M over R and any basis $\{f_1, f_2, \cdots, f_n\}$ of N over R, there exists a matrix $P \in M_n(R)$ such that

$$\begin{bmatrix}f_1 & f_2 & \cdots & f_n\end{bmatrix} = \begin{bmatrix}e_1 & e_2 & \cdots & e_n\end{bmatrix} P.$$

The discriminants with respect to the bases $\{e_1, e_2, \cdots, e_n\}$ and $\{f_1, f_2, \cdots, f_n\}$ satisfy

$$\mathrm{Disc}\left(Q|_{N\times N}; f_1, f_2, \cdots, f_n\right) = \det(P)^2\, \mathrm{Disc}\left(Q; e_1, e_2, \cdots, e_n\right).$$

(ii) Let $\mathrm{Fitt}_0(M/N)$ be the 0-th Fitting ideal of the R-module M/N. Then we have equality of ideals

$$(\mathrm{Disc}(Q|_{N\times N})) = \mathrm{Fitt}_0(M/N)^2\,(\mathrm{Disc}(Q))\,.$$

Proof. (i) Let $\{e_1, e_2, \cdots, e_n\}$ be a basis of M over R. Since N is a unital R-submodule of M which is also a free R-module of rank n, we can assume that $\{f_1, f_2, \cdots, f_n\}$ is a basis of N over R. Note each f_i can be expressed as a linear combination of $e_1, e_2, \cdots, e_n$. Thus there exists a matrix $M \in M_n(R)$ such that

$$\begin{bmatrix} f_1 & f_2 & \cdots & f_n \end{bmatrix} = \begin{bmatrix} e_1 & e_2 & \cdots & e_n \end{bmatrix} P.$$

Thus we have

$$\begin{aligned}
\mathrm{Disc}\,(Q|_{N\times N}; f_1, f_2, \cdots, f_n) &= \det\left(\left[\langle f_i, f_j\rangle_{Q|_{N\times N}}\right]_{1\le i,j\le n}\right) \\
&= \det\left(P^\top \left[\langle e_i, e_j\rangle_Q\right]_{1\le i,j\le n} P\right) \\
&= \det(P)^2 \det\left(\left[\langle e_i, e_j\rangle_Q\right]_{1\le i,j\le n}\right) \\
&= \det(P)^2\,\mathrm{Disc}\,(Q; e_1, e_2, \cdots, e_n)\,.
\end{aligned}$$

(ii) By identifying matrix P and its corresponding linear map $P : R^n \to R^n$, the R-module M/N has a presentation

$$R^n \xrightarrow{P} R^n \xrightarrow{\pi} M/N \longrightarrow 0$$

where π is defined by

$$\pi(0, \cdots, \underbrace{1_R}_{\text{i-th component}}, \cdots, 0) = e_i + N$$

for $1 \le i \le n$. By definition, the 0-th Fitting ideal of M/N is generated by $\det(P)$

$$\mathrm{Fitt}_0(M/N) = (\det(P)).$$

□

Corollary 8.4.13 Discriminant Relation

Let R be a commutative ring and A an R-algebra which is a free R-module of rank n. Let $B \subseteq A$ be a unital R-subalgebra of A which is also a free R-module of rank n. Then for any basis $\{e_1, e_2, \cdots, e_n\}$ of A over R and any basis $\{b_1, b_2, \cdots, b_n\}$ of B over R, there exists a matrix $M \in M_n(R)$ such that

$$\begin{bmatrix} b_1 & b_2 & \cdots & b_n \end{bmatrix} = \begin{bmatrix} e_1 & e_2 & \cdots & e_n \end{bmatrix} M.$$

The discriminants with respect to the bases $\{e_1, e_2, \cdots, e_n\}$ and $\{b_1, b_2, \cdots, b_n\}$ satisfy

$$d_B(b_1, b_2, \cdots, b_n) = \det(M)^2\, d_A(e_1, e_2, \cdots, e_n).$$

In particular, if $R = \mathbb{Z}$, then $\mathbb{Z}/(\mathbb{Z}^\times)^2 \cong \mathbb{Z}$ and we have

$$d_B = [A : B]^2 d_A,$$

where $[A : B]$ is the index of B in A as abelian groups.

Proof. Note

$$\left(\langle\cdot,\cdot\rangle_{A|R}\right)|_{B\times B} = \langle\cdot,\cdot\rangle_{B|R}.$$

$d_B(b_1, b_2, \cdots, b_n) = \det(M)^2\, d_A(e_1, e_2, \cdots, e_n)$ is a direct consequence of Lemma 8.4.12. If $R = \mathbb{Z}$, then $\det(M) = \pm[A : B]$ and $\mathbb{Z}/(\mathbb{Z}^\times)^2 \cong \mathbb{Z}$. Thus □

8.5 Algebra over Field

Lemma 8.5.1 Nonzero Ring Homomorphism from Field is Injective

If K is a field, R is a ring, a ring homomorphism $f : K \to R$ is either injective or the zero map. Furthermore, If R is not a zero ring, then f is injective.

Proof. Since the only ideals of K are $\{0\}$ and K, the kernel of f is either $\{0\}$ or K. If $\ker f = \{0\}$, then f is injective. If $\ker f = K$, then f is the zero map. By Proposition 5.1.11, if R is not a zero ring, then $\ker f$ is not K, so f is injective. □

Corollary 8.5.2

If K is a field and A is a nonzero K-algebra, then the ring homomorphism $K \to Z(A)$ is injective.

Proof. This is a direct consequence of Lemma 8.5.1. □

Proposition 8.5.3 Structure of $K[a]$

Let K be a field, A be a K-algebra and $a \in A$. Consider the evaluation ring homomorphism

$$\begin{aligned} \mathrm{ev}_a : K[X] &\longrightarrow A \\ f &\longmapsto f(a). \end{aligned}$$

Since $K[X]$ is a PID, we can suppose $\ker \mathrm{ev}_a = (P_a)$ for some $P_a \in K[X]$. Since $\mathrm{im}\, \mathrm{ev}_a = K[a]$, we have the following isomorphism in K-Alg

$$K[a] \cong K[X]/(P_a(X)).$$

And it can be divided into two cases:

(i) If $P_a = 0$, then ev_a is injective and $K[a] \cong K[X]$.

(ii) If $P_a \neq 0$, then ev_a is not injective. If we further assume A is a domain, then $P_a(X)$ is irreducible, $K[a]$ is a field and

$$[K[a] : K] = \deg P_a(X).$$

Moreover,

$$\deg P_a(X) = 0 \iff A \text{ is a zero ring.}$$

Proof. (i) If $P_a = 0$, then $\ker \mathrm{ev}_a = \{0\}$, so ev_a is injective. And $K[a] \cong K[X]$.

(ii) If A is a domain, then $K[a]$ as a subring of A is an integral domain. This implies $(P_a(X))$ is a nonzero prime ideal of $K[X]$. By Proposition 6.4.4, $P_a(X)$ is irreducible. Since $K[X]/(P_a(X))$ as K-vector space has a basis $\{1, X, X^2, \cdots, X^{\deg P_a(X)-1}\}$, we have $[K[a] : K] = \deg P_a(X)$.

And we have

$$\deg P_a(X) = 0 \iff P_a \in K^\times \iff \ker \mathrm{ev}_a = (P_a) = K[X] \iff \mathrm{ev}_a \text{ is the zero map} \iff A \text{ is a zero ring.}$$

□

Definition 8.5.4 Algebraic Element and Transcendental Element

Let K be a field, A be a K-algebra, and $a \in A$. Consider the evaluation ring homomorphism

$$\begin{aligned} \mathrm{ev}_a : K[X] &\longrightarrow A \\ f &\longmapsto f(a). \end{aligned}$$

and $\ker \mathrm{ev}_a = (P_a)$ for some $P_a \in K[X]$. Polynomials in $\ker \mathrm{ev}_a$ are called **annihilating polynomials** of a over K.

- If $P_a = 0$, then a is called a **transcendental element** over K. a is not the root of any nonzero polynomial in $K[X]$.

- If $P_a \neq 0$, then a is called an **algebraic element** over K. Suppose $P_a(X) = \sum_{i=0}^{n} a_i X^i$ with $a_n \in K^\times$. Then the monic polynomial $m_a(X) = P_a(X)/a_n$ is called the **minimal polynomial** of a over K. According to Proposition 8.5.3, if we further assume A is a domain, then $m_a(X)$ is irreducible.

If K is a field and $A = \{0_A\}$ is a zero K-algebra, then $0_A \in A$ is algebraic over K with minimal polynomial $m_{0_A}(X) = 1_K$.

Proposition 8.5.5 Algebraic Element is Integral

Let K be a field and A be a K-algebra. Then $a \in A$ is algebraic over K if and only if a is integral over K.

Proof. Suppose a is algebraic over K. Then the minimal polynomial $m_a(X) \in K[X]$ is a monic polynomial such that $m_a(a) = 0$. Thus a is integral over K. □

Proposition 8.5.6 Monic Irreducible Annihilating Polynomial is Minimal Polynomial

Let K be a field, A be a nonzero K-algebra and $a \in A$ be an algebraic element over K. If $f_a(X) \in K[X]$ is a monic irreducible annihilating polynomial of a over K, then $f_a(X)$ is the minimal polynomial of a over K.

Proof. Let $m_a(X)$ be the minimal polynomial of a over K. Since f_a is irreducible and $f_a \in \ker \mathrm{ev}_a = (m_a)$, by Proposition 6.2.6, either $m_a \in K[X]^\times = K^\times$ or f_a and m_a are associates. If $m_a \in K^\times$, then $\deg m_a = 0$, which implies that A is a zero ring by Proposition 8.5.3, contradicting the assumption. Thus f_a and m_a are associates. Since both f_a and m_a are monic, we have $f_a = m_a$. □

Chapter 9

Commutative Unital Algebra

9.1 Basic Properties

Definition 9.1.1 Commutative Algebra

Let R be a commutative ring. A **commutative R-algebra** is an R-algebra where the multiplication is commutative. Or equivalently, a commutative R-algebra is a commutative ring A together with a ring homomorphism $R \to A$.

Remark. There is a category isomorphism $R\text{-}\mathsf{CAlg} \cong (R/\mathsf{CRing})$. □

9.2 Polynomial Algebra

Definition 9.2.1 Polynomial Ring

Let R be a commutative ring. The **polynomial ring** in n variables over R is the ring $R[x_1, \cdots, x_n]$ defined as the set of all formal sums

$$\sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha$$

where $a_\alpha \in R$ satisfies $a_\alpha = 0$ for all but finitely many $\alpha \in \mathbb{N}^n$ and $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$. The addition and multiplication are defined as follows:

$$\sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha + \sum_{\alpha \in \mathbb{N}^n} b_\alpha x^\alpha = \sum_{\alpha \in \mathbb{N}^n} (a_\alpha + b_\alpha) x^\alpha$$

and

$$\left(\sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha \right) \left(\sum_{\beta \in \mathbb{N}^n} b_\beta x^\beta \right) = \sum_{\gamma \in \mathbb{N}^n} \left(\sum_{\alpha + \beta = \gamma} a_\alpha b_\beta \right) x^\gamma.$$

Proposition 9.2.2 Properties of Polynomial Ring

Let R be a commutative ring.

(i) If R is a UFD, then $R[x_1, \cdots .x_n]$ is a UFD.

(ii) R is a field $\iff$ $R[x]$ is a PID $\iff$ $R[x]$ is an Euclidean domain.

(iii) R is an integral domain $\iff$ $R[x]$ is an integral domain.

(iv) R is Noetherian $\implies$ $R[x]$ is Noetherian.

(v) R is reduced $\implies$ $R[x]$ is reduced.

Proposition 9.2.3 Division Algorithm in Polynomial Ring

Let R be a commutative ring and $f, g \in R[x]$ be nonzero polynomials. If the leading coefficient of g is in $R^\times$, then there exist unique polynomials $q, r \in R[x]$ such that $f = qg + r$ and $\deg r < \deg g$.

Proof. We can prove this by induction on $\deg f$. The base case is $\deg f = 0$. If $g = a_0 \in R^\times$, then we can take $q = f/a_0$ and $r = 0$. If $\deg g \geq 1$, then we can take $q = 0$ and $r = f$.

Suppose the statement holds for any $h \in R[x]$ with $\deg h < n$. Let $f \in R[x]$ be a polynomial of degree n. If $\deg f < \deg g$, then we can take $q = 0$ and $r = f$. If $\deg f \geq \deg g$. Suppose

$$f = \sum_{i=0}^{n} a_i x^i \quad \text{and} \quad g = \sum_{i=0}^{m} b_i x^i$$

where $a_n, b_m \neq 0$. Let $h = f - \frac{a_n}{b_m} x^{n-m} g$. Then $\deg h < \deg f$. By induction hypothesis, there exist $\tilde{q}, \tilde{r} \in R[x]$ such that $h = \tilde{q}g + \tilde{r}$ and $\deg \tilde{r} < \deg g$. Thus there exist

$$q = \tilde{q} + \frac{a_n}{b_m} x^{n-m} \quad \text{and} \quad r = \tilde{r}$$

such that $f = qg + r$ and $\deg r < \deg g$. If there are Q and R such that $f = Qg + R$ and $\deg R < \deg g$, then we have

$$h = f - \frac{a_n}{b_m} x^{n-m} g = \left(Q - \frac{a_n}{b_m} x^{n-m} \right) g + R = \tilde{q}g + \tilde{r}.$$

By uniqueness, we have $Q - \frac{a_n}{b_m} x^{n-m} = \tilde{q}$ and $R = \tilde{r}$, which implies $Q = q$ and $R = r$. □

Corollary 9.2.4 Polynomial Remainder Theorem

Let R be a commutative ring and $f(x) \in R[x]$ be a polynomial. If $a \in R$, then there exist a unique polynomial $q(x) \in R[x]$ such that $f(x) = q(x)(x - a) + f(a)$.

Proof. This is a direct application of Proposition 9.2.3. □

Corollary 9.2.5

Let R be a commutative ring.

(i) Let $a \in R$ and $f_1(x), \cdots, f_r(x) \in R[x]$ be polynomials. Then we have

$$(f_1(x), \cdots, f_r(x), x - a) = (f_1(a), \cdots, f_r(a), x - a).$$

(ii) Let $a \in R$ and $f_1(x), \cdots, f_r(x) \in R[x]$ be polynomials. Then we have

$$\frac{R[x]}{(f_1(x), \cdots, f_r(x), x - a)} \cong \frac{R}{(f_1(a), \cdots, f_r(a))}.$$

(iii) Suppose $a_1, \cdots, a_n \in R$. Then we can define a **evaluation homomorphism**

$$\begin{aligned} \mathrm{ev}_{a_1, \cdots, a_n} : R[x_1, \cdots, x_n] &\longrightarrow R \\ \sum_{\alpha \in \mathbb{N}^n} r_\alpha x^\alpha &\longmapsto \sum_{\alpha \in \mathbb{N}^n} r_\alpha a_1^{\alpha_1} \cdots a_n^{\alpha_n}. \end{aligned}$$

The kernel of $\mathrm{ev}_{a_1, \cdots, a_n}$ is

$$\ker \mathrm{ev}_{a_1, \cdots, a_n} = (x_1 - a_1, \cdots, x_n - a_n)$$

and we have

$$\frac{R[x_1, \cdots, x_n]}{(x_1 - a_1, \cdots, x_n - a_n)} \cong R.$$

Proof. (i) By the polynomial remainder theorem, we have

$$f_i(x) = q_i(x)(x-a) + f_i(a), \quad i = 1, 2, \cdots, r,$$

which implies

$$(f_1(x), \cdots, f_r(x), x-a) = (f_1(a), \cdots, f_r(a), x-a).$$

(ii) First we show the kernel of

$$\begin{aligned} \mathrm{ev}_a : R[x] &\longrightarrow R \\ f(x) &\longmapsto f(a) \end{aligned}$$

is $\ker \mathrm{ev}_a = (x-a)$. By the polynomial remainder theorem, we have

$$f(x) = q(x)(x-a) + f(a)$$

Note

$$f(x) \in \ker \mathrm{ev}_a \iff f(a) = 0 \iff f(x) \in (x-a).$$

We have $\ker \mathrm{ev}_a = (x-a)$ and $R[x]/(x-a) \cong R$.

From Example 5.2.1, we have the following equality of ideals in $R[x]/(x-a)$

$$(f_1(x), \cdots, f_r(x), x-a)/(x-a) = (f_1(x) + (x-a), \cdots, f_r(x) + (x-a)).$$

By the third isomorphism theorem, we have

$$\frac{R[x]}{(f_1(x), \cdots, f_r(x), x-a)} \cong \frac{R[x]/(x-a)}{(f_1(x) + (x-a), \cdots, f_r(x) + (x-a))}.$$

Apply the isomorphism

$$\begin{aligned} \overline{\mathrm{ev}_a} : R[x]/(x-a) &\longrightarrow R \\ f(x) + (x-a) &\longmapsto f(a) \end{aligned}$$

we get

$$\frac{R[x]/(x-a)}{(f_1(x) + (x-a), \cdots, f_r(x) + (x-a))} \cong \frac{R}{(f_1(a), \cdots, f_r(a))}.$$

(iii) We can prove

$$\ker \mathrm{ev}_{a_1, \cdots, a_n} = (x_1 - a_1, \cdots, x_n - a_n)$$

by induction on n. The base case is $n = 1$, which has been proved in (ii). Suppose the statement holds for $n-1$. Let $f(x_1, \cdots, x_n) \in R[x_1, \cdots, x_n]$.

$$\ker \mathrm{ev}_{a_1, \cdots, a_n} = \ker \left(\mathrm{ev}_{a_n} \circ \mathrm{ev}_{a_1, \cdots, a_{n-1}} \right) = \mathrm{ev}_{a_n}^{-1}((x_1 - a_1, \cdots, x_n - a_n)).$$

By the polynomial remainder theorem, we have and we have

$$\frac{R[x_1, \cdots, x_n]}{(x_1 - a_1, \cdots, x_n - a_n)} \cong R.$$

□

Example 9.2.1 *R-algebra Endomorphisms of $R[x]$*

Let R be a commutative ring. By the universal property of free commutative R-algebra, we have the following isomorphism

$$\mathrm{End}_{R\text{-}\mathsf{CAlg}}(R[x]) \cong \mathrm{Hom}_{\mathsf{Set}}(x, R[x]) \cong R[x].$$

For $f \in R[x]$, or for any function $\mathbf{1}_f : \{x\} \to R[x]$, there exists a unique R-algebra homomorphism

$$\begin{aligned} \widetilde{f} : R[x] &\longrightarrow R[x] \\ \sum_{k=0}^{n} a_k x^k &\longmapsto \sum_{k=0}^{n} a_k f(x)^k \end{aligned}$$

If $\deg f \leq 0$

9.3 Construction

9.3.1 Free Object

Definition 9.3.1 Free Commutative Algebra

Let X be a set and R be a commutative ring. The **free commutative R-algebra** on X, denoted by $\mathrm{Free}_{R\text{-}\mathsf{CAlg}}(X)$, together with a map $\iota : X \to \mathrm{Free}_{R\text{-}\mathsf{CAlg}}(X)$, is defined by the following universal property: for any commutative R-algebra A and any map $f : X \to A$, there exists a unique homomorphism $\widetilde{f} : \mathrm{Free}_{R\text{-}\mathsf{CAlg}}(X) \to A$ such that the following diagram commutes

$$\begin{array}{ccc} \mathrm{Free}_{R\text{-}\mathsf{CAlg}}(X) & \overset{\exists!\,\widetilde{f}}{\dashrightarrow} & A \\ {\scriptstyle\iota}\uparrow & \nearrow_{f} & \\ X & & \end{array}$$

The free commutative R-algebra $\mathrm{Free}_{R\text{-}\mathsf{CAlg}}(X)$ can be contructed as the polynomial algebra $R[X]$.
And we can define a functor

$$\begin{array}{ccccc} \mathsf{CRing} & & \mathsf{CRing} & & \\ R & & R[X] \ni & f(X) = \sum_{\beta} a_\beta x^\beta & \\ {\scriptstyle\varphi}\downarrow & \overset{\mathrm{Free}_{\bullet\text{-}\mathsf{CAlg}}(X)}{\rightsquigarrow} & {\scriptstyle\varphi(-)}\downarrow & \downarrow & \\ S & & S[X] \ni & {}^{\varphi}f(X) = \sum_{\beta} \varphi(a_\beta) x^\beta & \end{array}$$

Proof. We can check that $\mathrm{Free}_{\bullet\text{-}\mathsf{CAlg}}(X)$ is a functor

$${}^{\psi\circ\varphi}f(X) = \sum_{\beta} (\psi \circ \varphi)(a_\beta) x^\beta = \sum_{\beta} \psi(\varphi(a_\beta)) x^\beta = {}^{\psi}({}^{\varphi}f)(X).$$

□

9.3.2 Coproduct

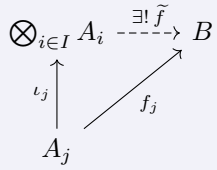
Definition 9.3.2 Coproduct of Commutative Algebras

Let R be a commutative ring and $(A_i)_{i\in I}$ be a family of commutative R-algebras. The **coproduct** of $(A_i)_{i\in I}$ in R-CAlg, denoted by $\bigotimes_{i\in I} A_i$, together with a family of R-algebra homomorphisms

$$\left(\iota_j : A_j \to \bigotimes_{i\in I} A_i \right)_{j\in I},$$

is the tensor product of $(A_i)_{i\in I}$ over R.
It is defined by the following universal property: for any commutative R-algebra B and any family of R-algebra homomorphisms $\{f_j : A_j \to B\}_{j\in I}$, there exists a unique R-algebra homomorphism $\widetilde{f} : \bigotimes_{i\in I} A_i \to$

B such that the following diagram commutes for all $j \in I$



Proposition 9.3.3 Diagonal Base Change for Commutative Algebras

If $\varphi : R \to S$, $f : S \to A$, $g : S \to B$ are ring homomorphisms of commutative rings. Denote $T := S \otimes_R S$. Then we have the following isomorphism in S-CAlg

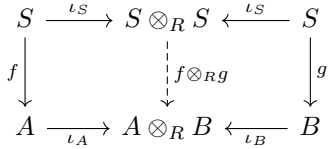
$$\begin{aligned} \theta : A \otimes_S B &\xrightarrow{\sim} (A \otimes_R B) \otimes_{S\otimes_R S} S \\ a \otimes_S b &\longmapsto (a \otimes_R b) \otimes_T 1_S \\ (a \cdot s) \otimes_S b = a \otimes_S (s \cdot b) &\longmapsfrom (a \otimes_R b) \otimes_T s. \end{aligned}$$

Proof. This is a direct consequence of Proposition 2.4.47. Here we give another proof by explicit construction.

First, there exists a unique R-algebra homomorphism

$$\begin{aligned} f \otimes_R g : S \otimes_R S &\longrightarrow A \otimes_R B \\ s \otimes_R s' &\longmapsto f(s) \otimes_R g(s'). \end{aligned}$$

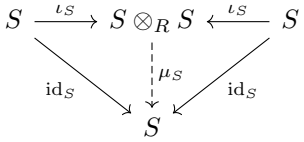
such that the following diagram commutes



This makes $A \otimes_R B$ an $S \otimes_R S$-algebra. Similarly, there exists a unique R-algebra homomorphism

$$\begin{aligned} \mu_S : S \otimes_R S &\longrightarrow S \\ s \otimes_R s' &\longmapsto ss'. \end{aligned}$$

such that the following diagram commutes



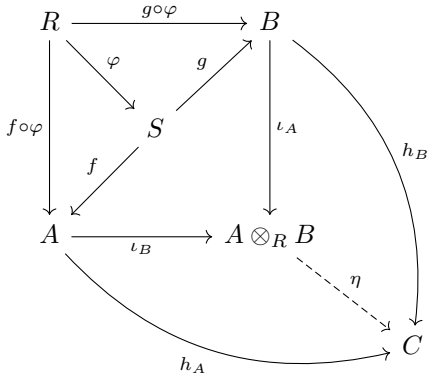
This makes S an $S \otimes_R S$-algebra.

Given any S-algebra C and any S-algebra homomorphisms $h_A : A \to C$, $h_B : B \to C$ such that $h_A \circ f = h_B \circ g$, by the universal property of tensor product $A \otimes_R B$, there exists a unique R-algebra homomorphism

$$\begin{aligned} \eta : A \otimes_R B &\longrightarrow C \\ a \otimes_R b &\longmapsto h_A(a) h_B(b) \end{aligned}$$

such that

$$h_A = \eta \circ \iota_A, \quad h_B = \eta \circ \iota_B.$$



Take $C := A \otimes_S B$ and we get an R-algebra homomorphism

$$\begin{aligned} \eta : A \otimes_R B &\longrightarrow A \otimes_S B \\ a \otimes_R b &\longmapsto a \otimes_S b. \end{aligned}$$

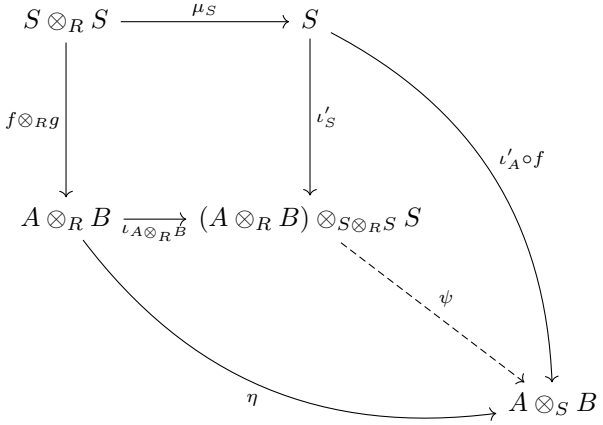
Since for any $s \otimes_R s' \in S \otimes_R S$, we have

$$\begin{aligned} \mu \circ (f \otimes_R g)(s \otimes_R s') &= \mu(f(s) \otimes_R g(s')) \\ &= f(s) \otimes_S g(s') \\ &= (f(s) \otimes_S 1_B)\,(1_A \otimes_S g(s')) \\ &= (f(s) \otimes_S 1_B)\,(f(s') \otimes_S 1_B) \\ &= (f(s)f(s')) \otimes_S 1_B \\ &= f(ss') \otimes_S 1_B \\ &= \iota'_A \circ f \circ \mu_S(s \otimes_R s'), \end{aligned}$$

by the universal property of the tensor product $(A \otimes_R B) \otimes_{S \otimes_R S} S$, there exists a unique $S \otimes_R S$-algebra homomorphism

$$\begin{aligned} \psi : (A \otimes_R B) \otimes_{S \otimes_R S} S &\longrightarrow A \otimes_S B \\ (a \otimes_R b) \otimes s &\longmapsto (a \otimes_S b)\,(f(s) \otimes_S 1_B) = (a \cdot s) \otimes_S b. \end{aligned}$$

such that the following diagram commutes



Define

$$\begin{aligned} j_A : A &\longrightarrow (A \otimes_R B) \otimes_{S \otimes_R S} S \\ a &\longmapsto (a \otimes_R 1_B) \otimes_T 1_S, \end{aligned}$$

and

$$\begin{aligned} j_B : B &\longrightarrow (A \otimes_R B) \otimes_{S \otimes_R S} S \\ b &\longmapsto (1_A \otimes_R b) \otimes_T 1_S. \end{aligned}$$

Note that for any $s \otimes s' \in S$, we have

$$\begin{aligned}(f(s) \otimes_R g(s')) \otimes_T 1_S &= \iota_{A\otimes_R B} \circ (f \otimes_R g)(s \otimes_R s') \\ &= \iota'_S \circ \mu_S(s \otimes_R s') \\ &= (1_A \otimes_R 1_B) \otimes_T ss'.\end{aligned}$$

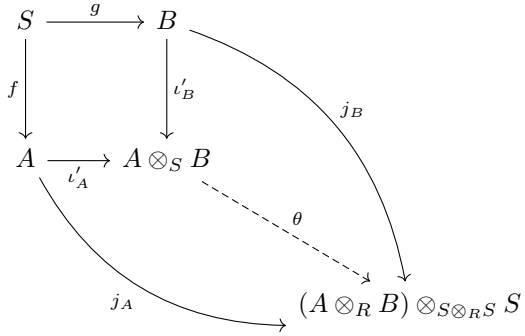
Then for any $s \in S$, we have

$$\begin{aligned}j_A \circ f(s) &= (f(s) \otimes_R 1_B) \otimes_T 1_S \\ &= (f(s) \otimes_R g(1_S)) \otimes_T 1_S \\ &= (1_A \otimes_R 1_B) \otimes_T (s1_S) \\ &= (1_A \otimes_R 1_B) \otimes_T (1_S s) \\ &= (f(1_S) \otimes_R g(s)) \otimes_T 1_S \\ &= (1_A \otimes_R g(s)) \otimes_T 1_S \\ &= j_B \circ g(s).\end{aligned}$$

By the universal property of the coproduct $A \otimes_S B$, there exists a unique S-algebra homomorphism

$$\begin{aligned}\theta : A \otimes_S B &\longrightarrow (A \otimes_R B) \otimes_{S\otimes_R S} S \\ a \otimes_S b &\longmapsto (a \otimes_R b) \otimes_T 1_S\end{aligned}$$

such that the following diagram commutes



Then it is straightforward to check that ψ and θ are inverse to each other:

$$\psi \circ \theta(a \otimes_S b) = \psi((a \otimes_R b) \otimes_T 1_S) = (a \cdot 1_S) \otimes_S b = a \otimes_S b,$$

and

$$\begin{aligned}\theta \circ \psi((a \otimes_R b) \otimes_T s) &= \theta((a \cdot s) \otimes_S b) \\ &= ((a \cdot s) \otimes_S b) \otimes_T 1_S \\ &= ((a \otimes_S b) \cdot (s \otimes_R 1_S)) \otimes_T 1_S \\ &= (a \otimes_S b) \otimes_T ((s \otimes_R 1_S) \cdot 1_S) \\ &= (a \otimes_R b) \otimes_T s.\end{aligned}$$

□

Chapter 10

Vector Space

10.1 Basic Definitions and Properties

Definition 10.1.1 Vector Space

Let K be a field. A **K-vector space** is an abelian group $(V, +)$ equipped with a map (called **scalar multiplication**)

$$\begin{aligned} K \times V &\longrightarrow V \\ (\lambda, v) &\longmapsto \lambda v \end{aligned}$$

such that the following conditions hold for all $u, v, w \in V$ and $\lambda, \mu \in K$:

(i) (Distributivity over vector addition) $\lambda(v + w) = \lambda v + \lambda w$.

(ii) (Distributivity over field addition) $(\lambda + \mu)v = \lambda v + \mu v$.

(iii) (Compatibility of scalar multiplication) $(\lambda\mu)v = \lambda(\mu v)$.

(iv) (Identity element of scalar multiplication) $1_K v = v$, where 1_K is the multiplicative identity in K.

Lemma 10.1.2

Let V be a K-vector space and S, T be subsets of V.

(i) Suppose $\lambda \in K^\times$. Then we have

$$\lambda S \subseteq T \implies S \subseteq \lambda^{-1} T.$$

(ii) For all $c_1, c_2 \in K$ we have

$$c_1(c_2 S) = (c_1 c_2) S$$

(iii) Suppose $\lambda \in K^\times$. Then we have

$$S = T \iff \lambda S = \lambda T.$$

(iv) $1_K S = S$.

Proof. (i) Suppose $\lambda S \subseteq T$. Then we have

$$\begin{aligned} s \in S &\implies \lambda s \in \lambda S \\ &\implies \lambda s \in T \\ &\implies \exists t \in T,\ \lambda s = t \\ &\implies s = \lambda^{-1} t \in \lambda^{-1} T \\ &\implies s \in \lambda^{-1} T, \end{aligned}$$

which implies $S \subseteq \lambda^{-1} T$.

(ii) For all $s \in S$, we have

$$\begin{aligned} x \in c_1(c_2 S) &\iff \exists s \in S,\ x = c_1(c_2 s) \\ &\iff \exists s \in S,\ x = (c_1 c_2)s \\ &\iff x \in (c_1 c_2)S. \end{aligned}$$

(iii)

$$\begin{aligned} \lambda S = \lambda T &\implies \lambda S \subseteq \lambda T \text{ and } \lambda T \subseteq \lambda S \\ &\implies S \subseteq \lambda^{-1}(\lambda T) \text{ and } T \subseteq \lambda^{-1}(\lambda S) \\ &\implies S \subseteq T \text{ and } T \subseteq S \\ &\implies S = T. \end{aligned}$$

□

10.2 Tensor Product of Vector Spaces

Proposition 10.2.1

Let V, W be vector spaces over a field K. If either V or W is finite-dimensional, then we have natural isomorphisms

$$\mathsf{Hom}_{\mathsf{Vect}_K}(V, W) \cong V^\vee \otimes W.$$

If V is a vector space over a field K, then the dual space of V is defined to be the vector space

$$V^\vee = \mathsf{Hom}_{\mathsf{Vect}_K}(V, K).$$

Proposition 10.2.2

Let V be vector spaces over a field K and A is a basis of V. Then we have isomorphism

$$V \cong \bigoplus_{a \in A} K.$$

And we have isomorphism for the dual space

$$V^\vee \cong \left(\bigoplus_{a \in A} K \right)^\vee \cong \prod_{a \in A} K \cong K^A.$$

If $|A|$ is finite, then we have

$$\dim V^\vee = |A|.$$

If $|A|$ is infinite, then we have

$$\dim V^\vee = |K^A| > |A|.$$

Definition 10.2.3 Transpose of a Linear Map

Let V, W be vector spaces over a field K and $f \in \mathsf{Hom}_{\mathsf{Vect}_K}(V, W)$. The transpose of f is the linear map

$$\begin{aligned} f^* : W^\vee &\longrightarrow V^\vee \\ \phi &\longmapsto \phi \circ f. \end{aligned}$$

The following identity holds for all $\phi \in W^\vee$ and $v \in V$

$$\langle f^*(\phi), v \rangle = \langle \phi, f(v) \rangle.$$

The map

$$\begin{aligned} {}^* : \mathsf{Hom}_{\mathsf{Vect}_K}(V, W) &\longrightarrow \mathsf{Hom}_{\mathsf{Vect}_K}(W^\vee, V^\vee) \\ f &\longmapsto f^* \end{aligned}$$

is an injective linear map. * is an isomorphism, if and only if W is finite-dimensional.
From the viewpoint of category theory, taking the dual of vector spaces and the transpose of linear maps is the contravariant functor $\mathrm{Hom}_{\mathsf{Vect}_K}(-, K)$

$$\begin{array}{ccc} K\text{-}\mathsf{Vect}^{\mathrm{op}} & & K\text{-}\mathsf{Vect} \\ V & & V^\vee \ni \phi \\ \downarrow{\scriptstyle f} & \overset{\mathrm{Hom}_{\mathsf{Vect}_K}(-,K)}{\rightsquigarrow} & \downarrow{\scriptstyle f^*} \quad \downarrow{\scriptstyle f^*} \\ W & & W^\vee \ni \phi \circ f \end{array}$$

10.3 Bilinear Forms

Definition 10.3.1 Bilinear Map

Let V and W be vector spaces over a field K. A map $B : V \times W \to K$ is said to be **bilinear** if

(i) For all $w \in W$, the map

$$\begin{aligned} B(\cdot, w) : V &\longrightarrow K \\ v &\longmapsto B(v, w) \end{aligned}$$

is linear.

(ii) For all $v \in V$, the map

$$\begin{aligned} B(v, \cdot) : W &\longrightarrow K \\ w &\longmapsto B(v, w) \end{aligned}$$

is linear.

Definition 10.3.2 Bilinear Form

A bilinear map $B : V \times V \to K$ is called a **bilinear form** on V.

Definition 10.3.3 Nondegenerate Bilinear Form

A bilinear form $B : V \times V \to K$ is said to be **nondegenerate** if the linear map

$$\begin{aligned} V &\longrightarrow V^\vee \\ v &\longmapsto B(\cdot, v) \end{aligned}$$

is an injection.

Proposition 10.3.4 Equivalent Characterizations of Nondegenerate Bilinear Forms

Let V be a finite-dimensional vector space over a field K and $B : V \times V \to K$ be a bilinear form. The following conditions are equivalent:

(i) B is nondegenerate.

(ii) The linear map

$$\begin{aligned} V &\longrightarrow V^\vee \\ v &\longmapsto B(\cdot, v) \end{aligned}$$

is an isomorphism.

(iii)
$$(\forall y \in V,\ B(x,y) = 0) \implies x = 0.$$

10.4 Inner Product Space

10.4.1 Sesquilinear Forms

Definition 10.4.1 Antilinear Map

Let V and W be vector spaces over $\mathbb{C}$. A map $f : V \to W$ is said to be **antilinear** or **conjugate linear** if for all $v_1, v_2 \in V$ and $\lambda \in \mathbb{C}$, we have
$$f(v_1 + v_2) = f(v_1) + f(v_2), \quad f(\lambda v) = \overline{\lambda} f(v).$$

Definition 10.4.2 Sesquilinear Map

Let V and W be vector spaces over $\mathbb{C}$. A map $B : V \times V \to W$ is said to be **sesquilinear** if

(i) For each $v \in V$, $B(\cdot, v)$ is linear.

(ii) For each $u \in V$, $B(u, \cdot)$ is antilinear.

Definition 10.4.3 Sesquilinear Form

A map $B : V \times V \to \mathbb{C}$ is called a **sesquilinear form** on V if it is a sesquilinear map.

Sesquilinear maps are completely determined by their values on the diagonal, as follows.

Proposition 10.4.4 Polarization Identity

Suppose V and W be vector spaces over $\mathbb{C}$ and $B : V \times V \to W$ is a sesquilinear form. Let $Q(v) := B(v, v)$. The **polarization identity** is given by
$$B(v_1, v_2) = \frac{1}{4}\left(Q(v_1 + v_2) - Q(v_1 - v_2) + iQ(iv_1 + v_2) - iQ(iv_1 - v_2)\right).$$

Definition 10.4.5 Hermitian Form

A sesquilinear form $B : V \times V \to \mathbb{C}$ is called a **Hermitian form** if it satisfies the condition
$$B(v_1, v_2) = \overline{B(v_2, v_1)}.$$

Proposition 10.4.6 Equivalent Characterizations of Hermitian Forms

Let $B : V \times V \to \mathbb{C}$ be a sesquilinear form on a complex vector space V. The following conditions are equivalent:

(i) B is a Hermitian form.

(ii) For all $v \in V$, we have $B(v, v) \in \mathbb{R}$.

Proof. Let $Q(v) := B(v, v)$.

- If B is a Hermitian form, then for all $v \in V$, we have
$$B(v, v) = \overline{B(v, v)}.$$
Since $B(v, v)$ is a complex number equal to its own conjugate, it must be real.

- Conversely, if $Q(v) = B(v,v) \in \mathbb{R}$ for all $v \in V$, then for any $v_1, v_2 \in V$, we have

$$\begin{aligned}\overline{B(v_2,v_1)} &= \frac{1}{4}\left(Q(v_2+v_1) - Q(v_2-v_1) + \bar{i}Q(iv_2+v_1) - \bar{i}Q(iv_2-v_1)\right)\\ &= \frac{1}{4}\left(Q(v_2+v_1) - Q(-(v_1-v_2)) - iQ(-i(iv_1-v_2)) + iQ(i(iv_1+v_2))\right)\\ &= \frac{1}{4}\left(Q(v_1+v_2) - Q(v_1-v_2) + iQ(iv_1+v_2) - iQ(iv_1-v_2)\right)\\ &= B(v_1,v_2),\end{aligned}$$

  which shows that B is a Hermitian form.

□

Definition 10.4.7 Positivity

A sesquilinear form $B : V \times V \to \mathbb{C}$ is said to be **positive** if for all $v \in V$, we have

$$B(v,v) \geq 0.$$

Proposition 10.4.8 Properties of Positive Sesquilinear Forms

Let $B : V \times V \to \mathbb{C}$ be a positive sesquilinear form and let $Q(v) := B(v,v)$. The following properties hold:

(i) Every positive sesquilinear form is Hermitian.

(ii) (Cauchy-Schwarz Inequality) For all $v_1, v_2 \in V$, we have

$$|B(v_1,v_2)|^2 \leq Q(v_1)Q(v_2).$$

(iii) (Minkowski Inequality) For all $v_1, v_2 \in V$, we have

$$Q(v_1+v_2)^{\frac{1}{2}} \leq Q(v_1)^{\frac{1}{2}} + Q(v_2)^{\frac{1}{2}}.$$

10.4.2 Inner Product Space

Definition 10.4.9 Positive Definiteness

Let $B : V \times V \to \mathbb{C}$ be a sesquilinear form on a $\mathbb{C}$-linear space V. The form B is said to be **positive-definite** if for all $v \in V - \{0\}$, we have

$$B(v,v) > 0.$$

Definition 10.4.10 Inner Product Space

Let $\Bbbk = \mathbb{R}$ or $\mathbb{C}$. A **inner product space** is a $\Bbbk$-linear space V equipped with a map $\langle \cdot, \cdot \rangle : V \times V \to \Bbbk$ such that the following conditions hold:

(i) (Linearity in the first argument): For all $v_1, v_2 \in V$ and $\lambda \in \Bbbk$, we have

$$\langle v_1+v_2, v_3\rangle = \langle v_1, v_3\rangle + \langle v_2, v_3\rangle, \quad \langle \lambda v_1, v_2\rangle = \lambda\langle v_1, v_2\rangle.$$

(ii) (Conjugate symmetry): For all $v_1, v_2 \in V$, we have

$$\langle v_1, v_2\rangle = \overline{\langle v_2, v_1\rangle}.$$

(iii) (Positive-definiteness): For all $v \in V - \{0\}$, we have

$$\langle v, v\rangle > 0.$$

The map $\langle \cdot, \cdot \rangle : V \times V \to \Bbbk$ is called the **inner product** on V.

Definition 10.4.11 Complex Inner Product Space

A **complex inner product space** is a complex vector space V equipped with a positive-definite Hermitian form $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$, which is called the **inner product** on V.

Proposition 10.4.12 Parallelogram Law

Let V be an inner product space over $\Bbbk$. Then for all $v_1, v_2 \in V$, we have

$$\|v_1 + v_2\|^2 + \|v_1 - v_2\|^2 = 2\|v_1\|^2 + 2\|v_2\|^2.$$

10.4.3 Orthogonality

Definition 10.4.13 Orthogonality

Let V be an inner product space.

- Two vectors $v_1, v_2 \in V$ are said to be **orthogonal** if
$$\langle v_1, v_2 \rangle = 0,$$
which is denoted by $v_1 \perp v_2$.
- A vector $v \in V$ is said to be **orthogonal to a subspace** $W \subseteq V$ if
$$\langle v, w \rangle = 0 \text{ for all } w \in W,$$
which is denoted by $v \perp W$.
- Let $W_1, W_2 \subseteq V$ be subspaces of V. We say that W_1 and W_2 are **orthogonal** if
$$\langle w_1, w_2 \rangle = 0 \text{ for all } w_1 \in W_1 \text{ and } w_2 \in W_2,$$
which is denoted by $W_1 \perp W_2$.

Proposition 10.4.14

Let V be an inner product space over $\Bbbk$. Then we have

(i) Let $x, y, z \in V$. If $x \perp z$ and $y \perp z$, then $(ax + by) \perp z$ for all $a, b \in \Bbbk$.

(ii) Let $x \in V$. We have
$$x \perp x \iff x = 0.$$

(iii) Let $W_1, W_2 \subseteq V$ be subspaces. If $W_1 \perp W_2$, Then
$$W_1 \cap W_2 = \{0\}.$$

Proof. (i) Let $x, y, z \in V$ and $a, b \in \Bbbk$. Then we have

$$\begin{aligned} \langle ax + by, z \rangle &= a\langle x, z \rangle + b\langle y, z \rangle \\ &= a \cdot 0 + b \cdot 0 = 0. \end{aligned}$$

Thus, $ax + by \perp z$.

(ii) Let $x \in V$ and assume $x \perp x$. Then we have

$$\langle x, x \rangle = 0.$$

Since the inner product is positive-definite, we have $\langle x, x \rangle > 0$ for all $x \in V - \{0\}$. Therefore, x must be the zero vector, i.e., $x = 0$. Conversely, if $x = 0$, then we have $\langle 0, 0 \rangle = 0$, which implies $0 \perp 0$.

(iii) Let $W_1, W_2 \subseteq V$ be subspaces and assume $W_1 \perp W_2$. Let $x \in W_1 \cap W_2$. Then we have $x \in W_1$ and $x \in W_2$. By the definition of orthogonality, we have $x \perp x$. By the previous part, we have $x = 0$. Thus, $W_1 \cap W_2 = \{0\}$.

□

Definition 10.4.15 Orthogonal Complement

Let V be an inner product space and $W \subseteq V$ be a subspace. The **orthogonal complement** of W, denoted by $W^\perp$, is defined as

$$W^\perp = \{v \in V \mid v \perp W\}.$$

The orthogonal complement is a closed subspace of V.

Proposition 10.4.16 Properties of Orthogonal Complements

Let V be an inner product space and $W \subseteq V$ be a subspace. The following properties hold:

(i) $W \perp W^\perp$.

(ii) $W \cap W^\perp = \{0\}$.

(iii) If $W_1 \subseteq W_2 \subseteq V$ are subspaces, then

$$W_2^\perp \subseteq W_1^\perp.$$

(iv)

$$W^\perp = \left(\overline{W}\right)^\perp = \left(\overline{\operatorname{span}(W)}\right)^\perp.$$

(v) If W is finite-dimensional, then $\dim W + \dim W^\perp = \dim V$.

Chapter 11

Field

11.1 Field Extension

Definition 11.1.1 Field

A **field** is a commutative ring K such that $K^\times = K - \{0\}$.

Proposition 11.1.2 Ideals of Field

The only ideals of a field K are $\{0\}$ and K.

Definition 11.1.3 Field Homomorphism

A **field homomorphism** is a ring homomorphism between fields.

Proposition 11.1.4

Let Field denote the category of fields. We have

(i) Monomorphisms in Field are exactly injective ring homomorphisms of fields.

(ii) Isomorphisms in Field are exactly bijective ring homomorphisms of fields, i.e. ring isomorphisms of fields.

(iii) Every morphism in Field is a monomorphism.

Proof. This follows from Lemma 8.5.1. □

Definition 11.1.5 Subfield

Let L be a field and $K \subseteq L$ is a subset of L. If K is a field under the operations inherited from L, we say K is a **subfield** of L

Definition 11.1.6 Field Extension

Let $u : L \hookrightarrow K$ be a field monomorphism. We say K is a **field extension** of L. We write K/L to denote the field extension.

Remark. Though in the notation of field extension K/L, the function $u : L \hookrightarrow K$ is not given explicitly, K/L is just a simple way to denote $u : L \hookrightarrow K$ and includes totally the same information as u.

Note that $u(L)$ is a subfield of K. This allows us to think of L as a subfield of K. □

Definition 11.1.7 K-embedding and K-isomorphism

A K**-embedding** is a morphism in the coslice category (Field/K). A K**-isomorphism** is an isomorphism in

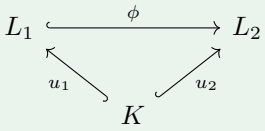
(Field/K). We say two field extensions L_1/K and L_2/K are **K-isomorphic** if there exists a K-isomorphism between them.

Proposition 11.1.8 Equivalent Characterizations of K-embedding

Let $u_1 : F \hookrightarrow K_1$, $u_2 : F \hookrightarrow K_2$, $\phi : K_1 \hookrightarrow K_2$ be field extensions. Then the following are equivalent:

(i) $\phi : K_1 \hookrightarrow K_2$ is a K-embedding between u_1 and u_2.

(ii) We have the following commutative diagram:



(iii) $\phi : K_1 \to K_2$ is an K-algebra homomorphism.

Proof. Note (Field/K) is a full subcategory of $(K/\mathsf{CRing}) \cong K\text{-}\mathsf{CAlg}$. □

Corollary 11.1.9 K-endomorphism Fixes Base Field

Let $u : K \hookrightarrow L$ be a field extension and $\phi : L \hookrightarrow L$ be a K-embedding. Then $\phi|_{u(K)} = \mathrm{id}_{u(K)}$.

Proof. Proposition 11.1.8 implies that $u = \phi \circ u$. So for any $x \in K$, we have $\phi(u(x)) = u(x)$. This implies $\phi|_{u(K)} = \mathrm{id}_{u(K)}$. □

Proposition 11.1.10 K-automorphism Acts on Set of Roots

Let $u : K \hookrightarrow L$ be a field extension and $\phi : L \hookrightarrow L$ be a K-embedding. Suppose $f(X) \in K[X]$ is a polynomial and

$$S_f = \{x \in L \mid f(x) = 0\}$$

be the set of roots of f in L. Then $\phi|_{S_f} : S_f \to S_f$ is a bijection and we can define a monoid homomorphism

$$\begin{aligned} \mathrm{End}_{(\mathsf{Field}/K)}(L/K) &\longrightarrow \mathrm{Aut}_{\mathsf{Set}}(S_f) \\ \phi &\longmapsto \phi|_{S_f} \end{aligned}$$

Moreover, $\mathrm{Aut}_{(\mathsf{Field}/K)}(L/K)$ acts on S_f through this map.

Proof. Let $x \in S_f$. Since

$$f(\phi(x)) = \phi(f(x)) = \phi(0) = 0,$$

we have $\phi(x) \in S_f$. Hence $\phi(S_f) \subseteq S_f$. Since S_f is finite set and ϕ is injective, we see $\phi|_{S_f} : S_f \to S_f$ is a bijection. It is easy to check

$$\begin{aligned} \mathrm{Aut}_{(\mathsf{Field}/K)}(L/K) &\longrightarrow \mathrm{Aut}_{\mathsf{Set}}(S_f) \\ \phi &\longmapsto \phi|_{S_f} \end{aligned}$$

is a group homomorphism.

□

Definition 11.1.11 Subextension

Let $u : K \hookrightarrow L$ be a field extension and $M \subseteq L$ be a subfield of L. If one of the following equivalent conditions hold:

(i) $u(K) \subseteq M$,

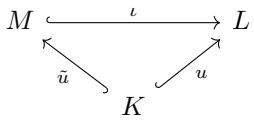
(ii) M is a K-subalgebra of L,

then we can define a map

$$\begin{aligned} \tilde{u} : K &\longrightarrow M : \\ x &\longmapsto u(x) \end{aligned}$$

which shrink the codomain of u to M. We say $\tilde{u} : K \to M$ is a **subextension** of $u : K \hookrightarrow L$.

Remark. If $u(K) \subseteq M$, we can also say M is a subextension of L/K, because $\tilde{u} : K \to M$ is totally determined by M. And we have the following commutative diagram:



where $\iota : M \hookrightarrow K$ is the inclusion map. □

Proposition 11.1.12 Characteristic of a Field

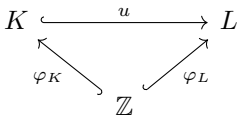
The characteristic of a field is either 0 or a prime number.

Proof. Let K be a field and $\varphi : \mathbb{Z} \to K$ be the unique ring homomorphism. Since (0) is a maximal ideal of K, $\ker \varphi$ is a maximal ideal of $\mathbb{Z}$. Therefore, $\ker \varphi$is either (0) or $p\mathbb{Z}$ for some prime number p, which implies $\operatorname{char}(K)$ is either 0 or p. □

Proposition 11.1.13 Field Extension Preserves Characteristic

Leet L/K be a field extension. Then $\operatorname{char}(L) = \operatorname{char}(K)$.

Proof. Since $\mathbb{Z}$ is an initial object in CRing, there exists unique ring homomorphisms $\varphi_K : \mathbb{Z} \to K$ and $\varphi_L : \mathbb{Z} \to L$ such that the following diagram commutes in CRing



Thus we have

$$\ker \varphi_L = \ker (u \circ \varphi_K) = \varphi_K^{-1}(0) = \ker \varphi_K,$$

which implies $\operatorname{char}(L) = \operatorname{char}(K)$. □

In field category Field, Let Field_0 denote the full subcategory of fields of characteristic 0 and Field_p denote the full subcategory of fields of characteristic p. Field_0 and all Field_p are connected components of Field. Though Field has no initial objects, Field_0 and Field_p have initial objects.

Proposition 11.1.14 Initial Objects in Field_0 and Field_p

(i) $\mathbb{Q}$ is an initial object in Field_0.

(ii) $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is an initial object in Field_p.

Proof. (i) Omitted.

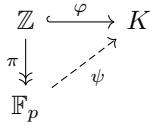
(ii) For any field K of characteristic p, there exists a uniqueness ring homomorphism

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow K \\ n &\longmapsto n \cdot 1_K \end{aligned}$$

and we have $\ker \varphi = \mathbb{F}_p$. Therefore, by ring homomorphism theorem, there exists a unique field homomorphism

$$\begin{aligned} \psi : \mathbb{F}_p &\longrightarrow K \\ n + p\mathbb{Z} &\longmapsto n \cdot 1_K \end{aligned}$$

such that the following diagram commutes



If $\eta : \mathbb{F}_p \to K$ is field homomorphism, then $\eta(1 + p\mathbb{Z}) = 1_K$ implies

$$\eta(n + p\mathbb{Z}) = n \cdot \eta(1 + p\mathbb{Z}) = n \cdot 1_K,$$

which implies $\eta = \psi$.

□

Corollary 11.1.15

There is natural bijection between isomorphisms in Field_p and isomorphisms in $(\mathbb{F}_p/\mathsf{Field})$. There is natural bijection between isomorphisms in Field_0 and isomorphisms in $(\mathbb{Q}/\mathsf{Field})$.

Proof. This follows from Proposition 11.1.14. □

Definition 11.1.16 Prime Subfield

If K is a field, the **prime subfield** of K is the smallest subfield of K containing 1_K.

Proposition 11.1.17 Equivalent Characterizations of Prime Subfield

Let K be a field and P be a subfield of K. The following are equivalent:

(i) P is the prime subfield of K.

(ii)
- If $\mathrm{char}(K) = 0$, P is the image of the unique field extension $\mathbb{Q} \hookrightarrow K$.
- If $\mathrm{char}(K) = p$, P is the image of the unique field extension $\mathbb{F}_p \hookrightarrow K$.

Proof. We prove the proposition by discussing the two cases: $\mathrm{char}(K) = 0$ and $\mathrm{char}(K) = p$.

- Let K be a field with a positive characteristic p. From Proposition 11.1.14 we see $\mathbb{F}_p$ is initial in Field_p and there exists a unique field extension from $\mathbb{F}_p$ to K

$$\begin{aligned} \psi : \mathbb{F}_p &\longhookrightarrow K \\ n + p\mathbb{Z} &\longmapsto n \cdot 1_K \end{aligned}$$

If F is any subfield of K containing 1_K, then F must contains $n \cdot 1_K$ for all $n \in \mathbb{Z}$, which implies $\psi(\mathbb{F}_p) \subseteq F$. Therefore, $\psi(\mathbb{F}_p)$ is the smallest subfield of K containing 1_K. So we proved $\psi(\mathbb{F}_p)$ is the prime subfield of K.

- Let K be a field with characteristic 0. From Proposition 11.1.14 we see $\mathbb{Q}$ is initial in Field_0 and there exists a unique field extension from $\mathbb{Q}$ to K

$$\begin{aligned} \psi : \mathbb{Q} &\longhookrightarrow K \\ n &\longmapsto n \cdot 1_K \end{aligned}$$

If F is any subfield of K containing 1_K, then F must contains $n \cdot 1_K$ for all $n \in \mathbb{Z}$, which implies $\psi(\mathbb{Q}) \subseteq F$. Therefore, $\psi(\mathbb{Q})$ is the smallest subfield of K containing 1_K. So we proved $\psi(\mathbb{Q})$ is the prime subfield of K.

□

Proposition 11.1.18 Subfield Contains Prime Subfield

Let K be a field with prime subfield P. If $F \subseteq K$ is a subfield of K, then

(i) $P \subseteq F$.

(ii)
- If $\mathrm{char}(K) = 0$, $F/\mathbb{Q}$ is a subextension of $K/\mathbb{Q}$.
- If $\mathrm{char}(K) = p$, $F/\mathbb{F}_p$ is a subextension of $K/\mathbb{F}_p$.

Proof. Let F be a subfield of K. Since F is a field, $1_K \in F$. Therefore, P is a subfield of F. □

Theorem 11.1.19 Hilbert's Weak Nullstellensatz

If $\overline{\Bbbk}$ is an algebraically closed field, then the maximal ideals of $\overline{\Bbbk}[x_1, \cdots, x_n]$ are precisely those ideals of the form $(x_1 - a_1, \cdots, x_n - a_n)$, where $a_i \in \overline{\Bbbk}$.

Theorem 11.1.20 Hilbert's Nullstellensatz

If $\Bbbk$ is any field and $\mathfrak{m}$ is a maximal ideal of $\Bbbk[x_1, \ldots, x_n]$, then $\Bbbk[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite extension of $\Bbbk$.

Proposition 11.1.21

If K is a field, then any finite subgroup of $K^\times$ is cyclic.

Proof. Let G be any subgroup of $K^\times$. By the structure theorem for finite abelian groups, we can write

$$G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$$

with $n_1 \mid n_2 \mid \cdots \mid n_r$. Let $n = G = n_1 n_2 \cdots n_r$. It is sufficient to show that $r = 1$. Since for any $g = (g_1, \cdots, g_r) \in C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$, we have

$$g^{n_r} - 1 = (g_1^{n_r}, g_2^{n_r}, \cdots, g_r^{n_r}) - (1, 1, \cdots, 1) = 0,$$

we know the polynomial $f(X) = X^{n_r} - 1$ has n distinct roots in K. Since

$$n \leq \deg f = n_r,$$

there must be $n = n_r$ and $r = 1$. □

11.1.1 Algebraic Extension

Definition 11.1.22 Algebraic Element and Transcendental Element

Let L/K be a field extension and $\alpha \in L$. Consider the evaluation ring homomorphism

$$\begin{aligned} \mathrm{ev}_\alpha : K[X] &\longrightarrow L \\ f &\longmapsto f(\alpha). \end{aligned}$$

and $\ker \mathrm{ev}_\alpha = (P_\alpha)$ for some $P_\alpha \in K[X]$. Polynomials in $\ker \mathrm{ev}_\alpha$ are called **annihilating polynomials** of α over K.

- If $P_\alpha = 0$, then α is called a **transcendental element** over K. In this case, zero polynomial is the only annihilating polynomial of α over K.
- If $P_\alpha \neq 0$, then α is called an **algebraic element** over K. Suppose $P_\alpha(X) = \sum_{i=0}^n a_i X^i$ with $a_n \in K^\times$. Then the monic polynomial $m_\alpha(X) = P_\alpha(X)/a_n$ is called the **minimal polynomial** of α over K, which is irreducible in $K[X]$.

Remark. This definition is a special case of Definition 8.5.4. □

Definition 11.1.23 Algebraic Extension

A field extension L/K is **algebraic** if every element of L is algebraic over K. That is, for any $\alpha \in L$, there exists a nonzero polynomial $f \in K[X]$ such that $f(\alpha) = 0$.

Proposition 11.1.24 Simple Algebraic Extension as a Quotient Ring

Let L/K be a field extension and $\alpha \in L$ be an algebraic element over K. Suppose $P(X) \in K[X]$ is an irreducible annihilating polynomial of α, or equivalently $P(X) \in K[X] - \{0\}$ is a constant multiple of the minimal polynomial $m_\alpha(X)$ of α over K. Then

$$K(\alpha) \cong K[X]/(P(X))$$

and $[K(\alpha) : K] = \deg P(X)$.

Proof. The equivalence between irreducible annihilating polynomial and constant multiple of minimal polynomial follows from Proposition 8.5.6. According to Proposition 8.5.3, we see

$$K[X]/(P(X)) \cong K[\alpha] = \{f(\alpha) \in L \mid f \in K[X]\},$$

$K[\alpha]$ is a field and $[K[\alpha] : K] = \deg P(X)$. It is sufficient to show $K(\alpha) = K[\alpha]$. It is clear that $K[\alpha] \subseteq K(\alpha)$. Since $K(\alpha)$ is the smallest subfield of L containing K and α, we have $K(\alpha) \subseteq K[\alpha]$. Therefore, $K(\alpha) = K[\alpha]$. □

Corollary 11.1.25 Power Basis of Simple Algebraic Extension $K(\alpha)$

Let L/K be a field extension and $\alpha \in L$ be an algebraic element over K. Then $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ is a K-basis of $K(\alpha)$, where $n = [K(\alpha) : K]$.

Proof. Let $n = [K(\alpha) : K]$. By Proposition 11.1.24, the minimal polynomial of α over K has degree n. Thus we can assume

$$m_\alpha(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$$

is the minimal polynomial of α over K. Note

$$m_\alpha(\alpha) = 0 \implies \alpha^n = -\left(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0\right).$$

We see $K(\alpha)$ is spanned by $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ over K, i.e.

$$K(\alpha) = \operatorname{span}_K\{1, \alpha, \ldots, \alpha^{n-1}\}.$$

If there exists $b_0, b_1, \cdots, b_{n-1} \in K$ such that

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0,$$

then the polynomial

$$f(X) = b_0 + b_1 X + \cdots + b_{n-1}X^{n-1} \in K[X]$$

satisfies $f(\alpha) = 0$. Since $\deg f < \deg m_\alpha$, we must have $f(X) = 0$ and $b_0 = b_1 = \cdots = b_{n-1} = 0$. This implies $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ is linearly independent over K. Therefore, $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ is a K-basis of $K(\alpha)$. □

Proposition 11.1.26

Let L/K be an algebraic extension. Then any K-embedding $L \hookrightarrow L$ is an K-isomorphism, namely

$$\operatorname{End}_{(\mathsf{Field}/K)}(L/K) = \operatorname{Aut}_{(\mathsf{Field}/K)}(L/K).$$

Proof. Let $u : L \hookrightarrow L$ be a K-embedding. It is sufficient to show u is surjective. Given $\alpha \in L$, suppose $m_\alpha(X) \in K[X]$ is the minimal polynomial of α over K. Let

$$S_{m_\alpha} = \{x \in L \mid m_\alpha(x) = 0\} = \{\alpha_1, \cdots, \alpha_m\}$$

be the set of roots of $m_\alpha(X)$ in L. Let $L_0 = K(\alpha_1, \cdots, \alpha_m)$. By Proposition 11.1.10, $u|_{S_{m_\alpha}} : S_{m_\alpha} \to S_{m_\alpha}$ is a bijection. Therefore, $u(L_0) \subseteq L_0$ and $u|_{L_0} : L_0 \to L_0$ is a K-embedding. Since L_0/K is a finite extension, $u|_{L_0}$ is an K-isomorphism. Therefore, $u|_{L_0}$ is surjective and there exists $\beta \in L_0$ such that $u(\beta) = \alpha$. This implies u is surjective. □

If L/K is not algebraic, we have the following counterexample.

Example 11.1.1

$\mathbb{Q}(\pi)/\mathbb{Q}$ is a transcendental extension. We can check that

$$\begin{aligned} u : \mathbb{Q}(\pi) &\longrightarrow \mathbb{Q}(\pi) \\ \pi &\longmapsto \pi^2 \end{aligned}$$

is a $\mathbb{Q}$-embedding but not a $\mathbb{Q}$-isomorphism.

11.1.2 Finitely Generated Extension

Definition 11.1.27 Generated Subextension

Let L/K be a field extension and $S \subseteq L$. The **subextension generated by** S is the smallest subextension of L/K containing S, denoted by $K(S)/K$. If $S = \{\alpha_1, \cdots, \alpha_n\}$ is a finite set, we write $K(S) = K(\alpha_1, \cdots, \alpha_n)$.

Proof. Here the smallest means if M/K is another subextension of L/K containing S, then $K(S)/K$ is a subextension of M/K. □

Proposition 11.1.28 Equivalent Characterizations of Generated Subextension

Let L/K be a field extension and $S \subseteq L$. Suppose M/L is a subextension of L/K. The following are equivalent:

(i) $M/K = K(S)/K$.

(ii) M/K is the intersection of all subextensions of L/K containing S.

(iii)
$$M = \{Q(\alpha_1, \cdots, \alpha_n) \in L \,|\, n \in \mathbb{Z}_{\geq 1},\ Q \in K(X_1, \cdots, X_n),\ \alpha_i \in S\}.$$

Definition 11.1.29 Compositum of Field Extensions

Let Ω/K be a field extension and $(L_i/K)_{i\in I}$ be a collection of subextensions of Ω/K. The **compositum** of $(L_i/K)_{i\in I}$ is the subextension of Ω/K generated by $\cup_{i\in I} L_i$, which is denoted by

$$\left(\bigvee_{i\in I} L_i\right)/K := K\left(\bigcup_{i\in I} L_i\right)/K.$$

We also denote the compositum by $L_1L_2\cdots L_n/K$ if I is finite.

Definition 11.1.30 Finitely Generated Extension

A field extension L/K is **finitely generated** if there exists a finite set $S \subseteq L$ such that $L = K(S)$.

Definition 11.1.31 Simple Extension

A field extension L/K is **simple** if $L = K(\alpha)$ for some $\alpha \in L$.

11.1.3 Finite Extension

Definition 11.1.32 Degree of Field Extension

Let L/K be a field extension. The **degree** of L/K is the dimension of L as a K-vector space, denoted by $[L:K] = \dim_K L$.

Definition 11.1.33 Finite Extension

A field extension L/K is **finite** if $[L:K] < \infty$.

Proposition 11.1.34

Let L/K be a finite generated extension and $L = K(\alpha_1, \cdots, \alpha_n)$. If $\alpha_1, \cdots, \alpha_n$ are algebraic elements over K, then L/K is a finite extension and $L = K[\alpha_1, \cdots, \alpha_n]$, where $K[\alpha_1, \cdots, \alpha_n]$ denotes the K-subalgebra of L generated by $\alpha_1, \cdots, \alpha_n$.

Proposition 11.1.35 Equivalent Characterization of Finite Extension

Let L/K be a field extension. The following are equivalent:

(i) L/K is a finite extension.

(ii) L/K is a finitely generated algebraic extension.

Proposition 11.1.36

If L/K is a finite extension and M/L be a subextension of L/K, then the following are equivalent:

(i) $M/K = L/K$

(ii) M/K and L/M are K-isomorphic.

(iii) $[M:L] = [L:K]$.

Lemma 11.1.37 Zariski's Lemma

If a field L is a finite-type K-algebra, then L is a finite extension of K (that is, L is also finitely generated as a K-linear space).

Example 11.1.2 Quadratic Extension

Suppose L/K is a quadratic extension and $\mathrm{char}(K) \neq 2$. Then there exists $\sqrt{a} \in L$ such that $L = K(\sqrt{a})$ and the minimal polynomial of $\sqrt{a}$ is $X^2 - a \in K[X]$.

Proof. Since L/K is a quadratic extension. For any $\alpha \in L - K$, suppose the minimal polynomial of α over K is $m_\alpha(X) \in K[X]$ with $\deg m_\alpha \leq 2$. If $\deg m_\alpha = 1$, then $m_\alpha(X) = X - \alpha$. This forces $\alpha \in K$, which contradicts the assumption. Thus $\deg m_\alpha = 2$. Since $\mathrm{char}(K) \neq 2$, we can write

$$m_\alpha(X) = X^2 + bX + c = \left(X + \frac{b}{2}\right)^2 - \frac{b^2}{4} + c.$$

for some $b, c \in K$ and we have

$$m_\alpha(\alpha) = \left(\alpha + \frac{b}{2}\right)^2 - \frac{b^2}{4} + c = 0.$$

Take $\sqrt{a} := \alpha + \frac{b}{2}$ and $f(X) := X^2 - b^2/4 + c \in K[X]$. We have

$$f\left(\sqrt{a}\right) = \left(\alpha + \frac{b}{2}\right)^2 - \frac{b^2}{4} + c = 0.$$

Note that $\sqrt{a} \notin K$. Otherwise, we have $\alpha = \sqrt{a} - \frac{b}{2} \in K$, which leads to a contradiction. Then the minimal polynomial of $\sqrt{a}$ has degree 2. Therefore, f is the minimal polynomial of $\sqrt{a}$ over K. This means $K(\sqrt{a})$ is a quadratic extension of K. Therefore, $K(\sqrt{a})$ is a 2-dimensional K-subspace of L and accordingly $K(\sqrt{a}) = L$. □

11.2 Algebraic Closure

Proposition 11.2.1 Simple Extension by Adjoining a Root of an Irreducible Polynomial

Let K be a field and $f \in K[X]$ be a irreducible polynomial. Denote $L := K[X]/(f)$ and $\alpha := X + (f(X)) \in L$. Then

(i) $u : K \hookrightarrow K[X] \twoheadrightarrow L$ is a field extension of degree $\deg f$.

$$[L : K] = \deg f.$$

(ii) $L = K(\alpha)$.

(iii) α is algebraic over K with minimal polynomial $f \in K[X]$.

Proof. It is easy to check

$$\left\{\alpha^k = X^k + (f(X)) \,\middle|\, k = 0, 1, \cdots, \deg f - 1\right\}$$

is a K-basis of L. Therefore, $[L : K] = \deg f$. Since

$$f(\alpha) = f(X + (f(X))) = f(X) + (f(X)) = 0 + (f(X)).$$

α is algebraic over K with minimal polynomial f. □

Proposition 11.2.2

Let L_1/K_1 and L_2/K_2 be field extensions and $\varphi : K_1 \xrightarrow{\sim} K_2$ is a field isomorphism. Let $\widetilde{\varphi} : K_1[X] \to K_2[X]$ be the ring homomorphism induced by $\varphi : K_1 \to K_2$ and denote ${}^{\varphi}f := \widetilde{\varphi}(f) \in K_2[X]$ for any $f \in K_1[X]$.

(i) Suppose $\eta : L_1 \hookrightarrow L_2$ is field extension such that the following diagram commutes

$$\begin{array}{ccc} L_1 & \xrightarrow{\eta} & L_2 \\ {\scriptstyle u_1}\uparrow & & \uparrow{\scriptstyle u_2} \\ K_1 & \xrightarrow[\varphi]{\sim} & K_2 \end{array}$$

If $\alpha \in L_1$ is algebraic over K_1 with minimal polynomial $f \in K_1[X]$, then $\eta(\alpha) \in L_2$ is algebraic over K_2 with minimal polynomial ${}^{\varphi}f \in K_2[X]$.

(ii) If $\alpha \in L_1$ is algebraic over K_1 with minimal polynomial $f_1 \in K_1[X]$, and $\beta \in L_2$ is algebraic over K_2 with minimal polynomial $f_2 := \varphi(f_1) \in K_2[X]$, then there exists a field isomorphism $\psi : K_1(\alpha_1) \xrightarrow{\sim} K_2(\alpha_2)$ such that $\psi(\alpha_1) = \alpha_2$ and the following diagram commutes the following diagram commutes

$$\begin{array}{ccc} K_1(\alpha_1) & \overset{\psi}{\dashrightarrow} & K_2(\alpha_2) \\ {\scriptstyle u_1}\uparrow & & \uparrow{\scriptstyle u_2} \\ K_1 & \xrightarrow[\varphi]{\sim} & K_2 \end{array}$$

Proof. (i) Since f is the minimal polynomial of α over K_1, f is monic and irreducible in $K_1[X]$ and we have

$$f(\alpha) = \sum_{k=0}^{n} c_k \alpha^k = 0.$$

Since $\varphi : K_1 \to K_2$ is a field isomorphism, we have ${}^{\varphi}f$ is monic and irreducible in $K_2[X]$. Note that

$$ {}^{\varphi}f(\eta(\alpha)) = \sum_{k=0}^{n} \varphi(c_k)\eta(\alpha)^k = \sum_{k=0}^{n} \eta(c_k)\eta(\alpha)^k = \eta\left(\sum_{k=0}^{n} c_k\alpha^k\right) = \eta(0) = 0. $$

By Proposition 8.5.6 we show ${}^{\varphi}f$ is the minimal polynomial of $\eta(\alpha)$ over K_2.

(ii) Suppose $\pi_1 : K_1[X] \to K_1[X]/(f_1)$ and $\pi_2 : K_2[X] \to K_2[X]/(f_2)$ are the canonical projections. Since for any $g \in K_1[X]$,

$$ \pi_2(\widetilde{\varphi}(gf_1)) = \pi_2(\widetilde{\varphi}(g)\widetilde{\varphi}(f_1)) = \pi_2(\widetilde{\varphi}(g)\varphi(f_1)) = \pi_2(\widetilde{\varphi}(g)f_2) = \pi_2(\widetilde{\varphi}(g))\pi_2(f_2) = 0, $$

we see $(f_1) \subseteq \ker(\pi_2 \circ \widetilde{\varphi})$. By the universal property of $\pi_1 : K_1[X] \to K_1[X]/(f_1)$, there exists a unique ring homomorphism

$$ \begin{aligned} \widehat{\varphi} : K_1[X]/(f_1) &\longrightarrow K_2[X]/(f_2) \\ g + (f_1) &\longmapsto \widetilde{\varphi}(g) + (f_2) \end{aligned} $$

such that the following diagram commutes

$$ \begin{array}{ccc} K_1(\alpha_1) & \xrightarrow{\psi} & K_2(\alpha_2) \\ \sim\uparrow & & \uparrow\sim \\ K_1[X]/(f_1) & \xrightarrow{\widehat{\varphi}} & K_2[X]/(f_2) \\ {\scriptstyle \pi_1}\uparrow\!\!\uparrow & & \uparrow\!\!\uparrow{\scriptstyle \pi_2} \\ K_1[X] & \xrightarrow{\widetilde{\varphi}} & K_2[X] \\ \uparrow & & \uparrow \\ K_1 & \xrightarrow[\varphi]{} & K_2 \end{array} $$

Let $\psi : K(\alpha) \hookrightarrow L_2$ be the composition of the following maps

$$ \begin{array}{ccccccc} K_1(\alpha_1) & \xrightarrow{\sim} & K_1[X]/(f_1) & \xrightarrow{\widehat{\varphi}} & K_2[X]/(f_2) & \xrightarrow{\sim} & K_2(\alpha_2) \\ \alpha_1 & \longmapsto & X & \longmapsto & X & \longmapsto & \alpha_2 \end{array} $$

Then ψ is a K-embedding such that $\psi(\alpha_1) = \alpha_2$.

□

Corollary 11.2.3 *K-embedding Preserves Algebraic Element and Minimal Polynomial*

Let L_1/K and L_2/K be field extensions.

(i) Suppose $u : L_1 \hookrightarrow L_2$ is a K-embedding. If $\alpha \in L_1$ is algebraic over K with minimal polynomial $f \in K[X]$, then $u(\alpha) \in L_2$ is also algebraic over K with minimal polynomial $f \in K[X]$.

(ii) If $\alpha \in L_1$ and $\beta \in L_2$ are algebraic over K with the same minimal polynomial $f \in K[X]$, then there exists a unique K-embedding $\psi : K(\alpha) \hookrightarrow L_2$ such that $\psi(\alpha) = \beta$. Furthermore, $\psi(K(\alpha)) = K(\beta)$.

Proof. This a direct consequence of Proposition 11.2.2 by setting $K_1 = K_2 = K$.

(i) Since $f(\alpha) = 0$, we have $f(u(\alpha)) = u(f(\alpha)) = 0$. Since f is irreducible over K, f is also the minimal polynomial of $u(\alpha)$ over K.

(ii) Let $\psi : K(\alpha) \hookrightarrow L_2$ be the composition of the following maps

$$ \begin{array}{ccccccc} K(\alpha) & \xrightarrow{\sim} & K[X]/(f) & \xrightarrow{\sim} & K(\beta) & \hookrightarrow & L_2 \\ \alpha & \longmapsto & X & \longmapsto & \beta & \longmapsto & \beta \end{array} $$

Then ψ is a K-embedding such that $\psi(K(\alpha)) = K(\beta)$.

Suppose $\eta : K(\alpha) \hookrightarrow L_2$ is K-embedding such that $\eta(\alpha) = \beta$. Since $K(\alpha)$ is generated by α over K, η is totally determined by $\eta(\alpha)$. Therefore, $\eta(\alpha) = \psi(\alpha) \implies \eta = \psi$.

□

Corollary 11.2.4

Let L/K be a simple extension and $L = K(\alpha)$ for some $\alpha \in L$. Suppose $m_\alpha(X) \in K[X]$ is the minimal polynomial of α over K. Then

$$\begin{aligned} \mathrm{ev}_\alpha : \mathrm{Aut}_{(\mathsf{Field}/K)}(K(\alpha)/K) &\longrightarrow \{x \in K(\alpha) \,|\, m_\alpha(x) = 0\} \\ \sigma &\longmapsto \sigma(\alpha) \end{aligned}$$

is a bijection and we have

$$|\mathrm{Aut}_{(\mathsf{Field}/K)}(K(\alpha)/K)| = |\{x \in K(\alpha) \,|\, m_\alpha(x) = 0\}| \leq \deg m_\alpha(X),$$

with equality if and only if $m_\alpha(X)$ splits over $K(\alpha)$ into $\deg m_\alpha(X)$ distinct linear factors.

Proof. Suppose $\sigma : K(\alpha) \hookrightarrow K(\alpha)$ is a K-automorphism. By Corollary 11.2.3, $u(\alpha)$ is algebraic over K with minimal polynomial $m(X)$. Thus we can define a map

$$\begin{aligned} \mathrm{ev}_\alpha : \mathrm{Aut}_{(\mathsf{Field}/K)}(K(\alpha)/K) &\longrightarrow \{x \in L \,|\, m(x) = 0\} \\ \sigma &\longmapsto \sigma(\alpha) \end{aligned}$$

Since σ is totally determined by $\sigma(\alpha)$, for any $\sigma_1, \sigma_2 \in \mathrm{Aut}_{(\mathsf{Field}/K)}(K(\alpha)/K)$, we have

$$\sigma_1(\alpha) = \sigma_2(\alpha) \implies \sigma_1 = \sigma_2.$$

Therefore, ev_α is injective. Conversely, for any $\beta \in L$ such that $m(\beta) = 0$, $m(X)$ is the minimal polynomial of β over K because $m(X)$ is irreducible over K. By Corollary 11.2.3, there exists a unique K-embedding $\sigma : K(\alpha) \hookrightarrow K(\alpha)$ such that $\sigma(\alpha) = \beta$. By Proposition 11.1.26, σ is a K-automorphism. Therefore, ev_α is surjective. Thus ev_α is a bijection. □

Definition 11.2.5 Algebraic Closed Field

A field K is **algebraically closed** if every nonconstant polynomial $f \in K[X]$ has a root in K.

Proposition 11.2.6 Equivalent Characterization of Algebraic Closed Field

Let K be a field. The following are equivalent:

(i) K is algebraically closed.

(ii) If $u : K \hookrightarrow L$ is an algebraic extension, then u is an isomorphism.

(iii) Every nonconstant polynomial $f \in K[X]$ splits into linear factors.

Proof. (i) $\implies$ (ii). For any $x \in L$, suppose $f \in K[X]$ is the minimal polynomial of x over K. Since K is algebraically closed, f splits into linear factors in $K[X]$. Since f is irreducible over K, there must be $f(X) = c(X - a)$ for some $c \in K^\times$ and $a \in K$.

$$u(f)(x) = u(c)(x - u(a)) = 0 \implies x = u(a).$$

Therefore, u is surjective, which implies u is an isomorphism. □

Definition 11.2.7 Algebraic Closure

An **algebraic closure** of a field K is an algebraic extension $\overline{K}/K$ such that $\overline{K}$ is algebraically closed.

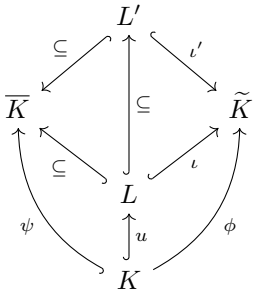
Proposition 11.2.8 Existence and Uniqueness of Algebraic Closure

Let K be a field. There exists an algebraic closure $\overline{K}/K$ and it is unique up to K-isomorphism.

Proof. **Uniqueness**. Let

$$\mathcal{T} = \left\{ (L, \iota) \,\middle|\, L/K \text{ is a subextension of } \overline{K}/K \text{ and } \iota : L \hookrightarrow \widetilde{K} \text{ is a } K\text{-embedding} \right\}.$$

We can define a partial order on $\mathcal{T}$ by $(L, \iota) \leq (L', \iota')$ if and only if $L \subseteq L'$ and $\iota'|_L = \iota$, or equivalently, the following diagram commutes



For each chain $\mathcal{C} = \{(L_i, \iota_i)\}_{i \in I}$ in $\mathcal{T}$, we can define $L_{\mathcal{C}} := \bigcup_{i \in I} L_i$ and $\iota_{\mathcal{C}} : L_{\mathcal{C}} \hookrightarrow \widetilde{K}$ by $\iota_{\mathcal{C}}(x) = \iota_i(x)$ whenever $x \in L_i$ for some $i \in I$. $\iota_{\mathcal{C}}$ is well-defined because for any $x \in L_i \cap L_j$ for some $i, j \in I$, we can assume $i \leq j$ without loss of generality and we have $\iota_i(x) = \iota_j(s(x))$ where $s : L_i \hookrightarrow L_j$ is the inclusion map. Then $(L_{\mathcal{C}}, \iota_{\mathcal{C}})$ is an upper bound of $\mathcal{C}$ in $\mathcal{T}$. By Zorn's lemma, there exists a maximal element $(L_{\max}, \iota_{\max})$ in $\mathcal{T}$.

We claim $L_{\max} = \overline{K}$ and prove by contradiction. Suppose $L_{\max} \neq \overline{K}$, then there exists $\alpha \in \overline{K} - L_{\max}$. Since α is algebraic over $L_{\max}$, there exists a minimal polynomial $m_\alpha \in L_{\max}[X]$ such that $m_\alpha(\alpha) = 0$. Let $\widetilde{m_\alpha} := \iota_{\max}(m_\alpha) \in \widetilde{K}[X]$ be the image of m_α under $\iota_{\max}$. Since $\widetilde{K}$ is algebraically closed, $\widetilde{m_\alpha}$ has a root $\beta \in \widetilde{K}$. Since $m_\alpha \in L_{\max}[X]$ is the minimal polynomial of both $\alpha \in \overline{K}$ and $\beta \in \widetilde{K}$, by Corollary 11.2.3, there exists a $L_{\max}$-embedding $\eta : L_{\max}(\alpha) \hookrightarrow \widetilde{K}$ such that $\eta(\alpha) = \beta$. Then $(L_{\max}(\alpha), \eta) \in \mathcal{T}$ and $(L_{\max}(\alpha), \eta) \leq (L_{\max}, \iota_{\max})$ does not hold. This contradicts the maximality of $(L_{\max}, \iota_{\max})$. Therefore, $L_{\max} = \overline{K}$.

To show $\eta : \overline{K} \hookrightarrow \widetilde{K}$ is a K-isomorphism, it is sufficient to show $\eta(\overline{K}) = \widetilde{K}$ is surjective. Since $\widetilde{K}$ is algebraically closed, $\eta(\overline{K})$ is algebraically closed. Since $\widetilde{K}/K$ is an algebraic extension, $K/\eta(\overline{K})$ is also an algebraic extension. According to Proposition 11.2.6, the inclusion $\eta(\overline{K}) \hookrightarrow \widetilde{K}$ is an isomorphism, which implies $\eta(\overline{K}) = \widetilde{K}$. Therefore, $\overline{K}$ is unique up to K-isomorphism. □

Proposition 11.2.9 Embed Algebraic Extension into Algebraic Closure

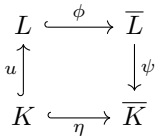
Let L/K be an algebraic extension and $\overline{K}/K$ be an algebraic closure of K. Then there exists a K-embedding $\gamma : L \hookrightarrow \overline{K}$, namely

$$\mathrm{Hom}_{(\mathsf{Field}/K)}(L, \overline{K}) \neq \varnothing.$$

If L/K is a finite extension, then

$$|\mathrm{Hom}_{(\mathsf{Field}/K)}(L, \overline{K})| \leq [L : K].$$

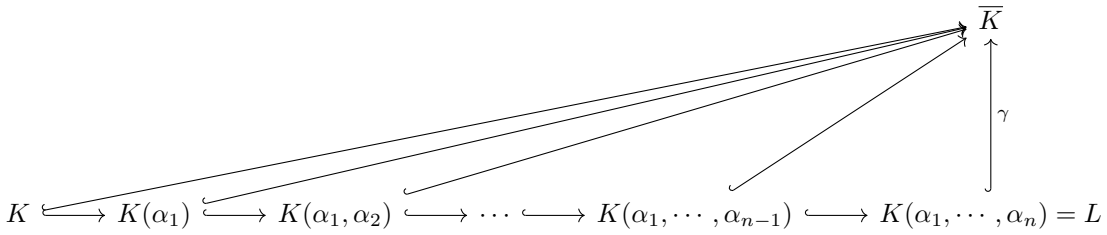
Proof. Suppose $\phi : L \hookrightarrow \overline{L}$ is an algebraic closure of L. Then $\phi \circ u : K \hookrightarrow \overline{L}$ is an algebraic closure of K. By the uniqueness of algebraic closure, there exists a K-embedding $\psi : L \hookrightarrow \overline{K}$. Let $\gamma := \psi \circ \phi$. Since the following diagram commutes



we see $\gamma : L \hookrightarrow \overline{K}$ is a K-embedding.

If L/K is a finite extension, then $L = K(\alpha_1, \cdots, \alpha_n)$ for some $\alpha_1, \cdots, \alpha_n \in L$ and we have the following tower

of field extensions



Thus we get a chain of restrictions of γ:

$$\begin{array}{ccc}
\mathrm{Hom}_{(\mathsf{Field}/K)}\left(K(\alpha_1,\cdots,\alpha_n)/K, \overline{K}/K\right) & & \gamma \\
\downarrow{\scriptstyle \mathrm{res}_n} & & \downarrow \\
\mathrm{Hom}_{(\mathsf{Field}/K)}\left(K(\alpha_1,\cdots,\alpha_{n-1})/K, \overline{K}/K\right) & & \gamma|_{K(\alpha_1,\cdots,\alpha_{n-1})} \\
\downarrow{\scriptstyle \mathrm{res}_{n-1}} & & \downarrow \\
\vdots & & \vdots \\
\downarrow{\scriptstyle \mathrm{res}_2} & & \downarrow \\
\mathrm{Hom}_{(\mathsf{Field}/K)}\left(K(\alpha_1)/K, \overline{K}/K\right) & & \gamma|_{K(\alpha_1)} \\
\downarrow{\scriptstyle \mathrm{res}_1} & & \downarrow \\
\mathrm{Hom}_{(\mathsf{Field}/K)}\left(K/K, \overline{K}/K\right) & & \gamma|_K
\end{array}$$

□

Proposition 11.2.10 Algebraic Closure of an Algebraic Extension

Let $\iota : K \hookrightarrow L$ be an algebraic extension.

(i) If $\tau : K \hookrightarrow \overline{K}$ is an algebraic closure of K, then there exists a K-embedding $\sigma : L \hookrightarrow \overline{K}$ such that σ is an algebraic closure of L.

(ii) If $\eta : L \hookrightarrow \overline{L}$ is an algebraic closure of L, then $\eta \circ \iota : K \hookrightarrow \overline{L}$ is an algebraic closure of K.

Specially, if $\overline{K}/K$ is an algebraic closure of K, and $\overline{L}/L$ is an algebraic closure of L, then we have field isomorphism

$$\overline{K} \cong \overline{L}.$$

11.3 Normal Extension

Definition 11.3.1 Splitting of Polynomial over a Field

Let L/K be a field extension and $f \in K[X]$ be a polynomial such that $\deg f \geq 1$. We say f **splits** over L if f can be written as

$$f(X) = a(X-\alpha_1)\cdots(X-\alpha_n)$$

for some $a \in K^\times$, $\alpha_1, \ldots, \alpha_n \in L$.

Proposition 11.3.2

Let L/K be a field extension and $f, g \in K[X]$ be polynomials. If g splits over L and $f \mid g$, then f also splits over L.

Proof. Suppose field embedding is $\iota : K \hookrightarrow L$ and $\tilde{f}$, $\tilde{g} \in L[X]$ are the images of f, g under ι. Since g splits over L, we can write

$$g(X) = c(X-\alpha_1)\cdots(X-\alpha_m) \in L[X]$$

for some $c \in L^\times$, $\alpha_1, \ldots, \alpha_m \in L$. Since $f \mid g$, we must have

$$f(X) = d(X - \alpha_{i_1}) \cdots (X - \alpha_{i_n}) \in L[X]$$

for some $d \in L^\times$ and $1 \leq i_1 < \cdots < i_n \leq m$. This shows f splits over L. □

Definition 11.3.3 Splitting Field

Let K be a field. Suppose $\mathcal{P}$ is a family of polynomials in $K[X]$. If L/K is a field extension such that

(i) Each $f \in \mathcal{P}$ splits over L,

(ii) The set of roots of polynomials in $\mathcal{P}$

$$S = \{\alpha \in L \mid f(\alpha) = 0 \text{ for some } f \in \mathcal{P}\}$$

is the generating set of L/K, that is, $L = K(S)$,

then we say L/K is a **splitting field of $\mathcal{P}$ over K**. If $\mathcal{P} = \{f\}$ is a singleton, then we say L/K is a **splitting field of f over K**.

Remark. Splitting field is a field extension instead of a field. So this terminology is a little bit misleading. But for historical reasons, we still use it.

If we explicitly state that $\mathcal{P} \subseteq K[X]$, then we can say L/K is a splitting field of $\mathcal{P}$ and the phrase "over K" becomes redundant information that can be omitted.

We say L/K is "a" splitting field of $\mathcal{P}$ instead of "the" splitting field of $\mathcal{P}$ because the splitting field of $\mathcal{P}$ is only unique up to isomorphism in (Field/K), not unique up to unique isomorphism in (Field/K). □

Proposition 11.3.4 Existance and Uniqueness of Splitting Field

Let K be a field and $\mathcal{P}$ be a family of polynomials in $K[X]$. Then the splitting field of $\mathcal{P}$ over K exists and is unique up to K-isomorphism.

Proof. Suppose $\overline{K}/K$ is an algebraic closure of K. Suppose for each $f \in \mathcal{P}$, f has degree n_f and splits into

$$f(X) = c_f(X - \alpha_{f,1}) \cdots (X - \alpha_{f,n_f})$$

in $\overline{K}$. Let $L_{\mathcal{P}} = K(\alpha_{f,k} : f \in \mathcal{P}, 1 \leq k \leq n_f)$. Then $L_{\mathcal{P}}/K$ is a splitting field of $\mathcal{P}$ over K.

Suppose L/K is another splitting field of $\mathcal{P}$ over K. Since L is generated by the roots of polynomials in $\mathcal{P}$, we have $L \subseteq L_{\mathcal{P}}$. Since $L_{\mathcal{P}}$ is generated by the roots of polynomials in $\mathcal{P}$, we have $L_{\mathcal{P}} \subseteq L$. Therefore, $L = L_{\mathcal{P}}$. □

Proposition 11.3.5 Properties of Splitting Field

Let K be a field. Suppose $\mathcal{P}$ is a family of polynomials in $K[X]$ and $L_{\mathcal{P}}$ is a splitting field of $\mathcal{P}$ over K. Then

(i) $L_{\mathcal{P}}/K$ is an algebraic extension.

(ii) If $\mathcal{P}$ is finite, then $L_{\mathcal{P}}/K$ is a finite extension.

(iii) If $\mathcal{P} = \{f\}$ is a singleton, then

$$[L_f : K] \leq (\deg f)!\,,$$

where $L_f := L_{\{f\}}$.

Definition 11.3.6 Normal Extension

Let L/K be a field extension. We say L/K is a **normal extension** if for any $\alpha \in L$, the minimal polynomial $m_\alpha \in K[X]$ of α splits completely into linear factors over L, i.e.,

$$m_\alpha(X) = (X - \alpha_1) \cdots (X - \alpha_n), \quad \alpha_1, \ldots, \alpha_n \in L.$$

Proposition 11.3.7 Equivalent Characterization of Normal Extension

Let L/K be a field extension. The following are equivalent:

(i) L/K is a normal extension.

(ii) L is a splitting field of a family of nonconstant polynomials in $K[X]$.

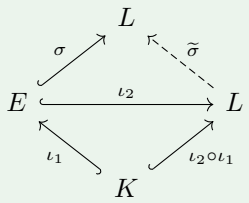
(iii) Let $\overline{K}/K$ be an algebraic closure of K. For any K-embedding $\iota_1, \iota_2 \in \mathrm{Hom}_{(\mathsf{Field}/K)}(L/K, \overline{K}/K)$, we have $\iota_1(L) = \iota_2(L)$.

Proposition 11.3.8

Let $L/E/K$ be a tower of field extensions given by $\iota_1 : K \hookrightarrow E$ and $\iota_2 : E \hookrightarrow L$. If L/K is normal, then given any K-embedding $\sigma : E \hookrightarrow L$, there exists a K-automorphism $\widetilde{\sigma} : L \hookrightarrow L$ such that

$$\widetilde{\sigma} \circ \iota_2 = \sigma,$$

that is, the following diagram commutes



Proof. Let $j : L \hookrightarrow \overline{L}$ be an algebraic closure of L. By Proposition 11.2.10, $j \circ \iota_1 : K \hookrightarrow \overline{L}$ is an algebraic closure of K.

Consider the K-embedding $j \circ \sigma : E \hookrightarrow \overline{L}$. □

11.4 Separable Extension

Definition 11.4.1 Separable Polynomial

et K be a field and $f \in K[X]$ be a nonzero polynomial. We say f is **separable** if f has no multiple roots in an algebraic closure of K. We say f is **inseparable** if f is not separable.

Definition 11.4.2 Separable Degree of Irreducible Polynomial

Let K be a field and $f \in K[x]$ be an irreducible polynomial. The **separable degree** of f is the cardinality of the set of roots of f in any algebraic closure $\overline{K}$ of K, which is denoted by

$$\deg_s(f) := \left|\left\{\alpha \in \overline{K} : f(\alpha) = 0\right\}\right|$$

Proposition 11.4.3 Equivalent Characterization of Separable Polynomial

Let K be a field and $f \in K[X]$ be a nonzero polynomial. The following are equivalent:

(i) f is separable.

(ii) f has no multiple roots in a splitting field of K.

(iii) $\gcd(f, f') = 1$

Proposition 11.4.4 Equivalent Characterization of Inseparability for Irreducible Polynomial

Let K be a field and $f \in K[X]$ be an irreducible polynomial. The following are equivalent:

(i) f is inseparable.

(ii) f has multiple roots in a splitting field of K.

(iii) $f' = 0$.

(iv) $\mathrm{char}(K) = p > 0$ and $f(X) = g(X^p)$ for some $g \in K[X]$.

Proof. (i) $\implies$ (ii). Suppose f is inseparable. If f splits into

$$f(X) = c(X - \alpha_1)^{n_1} \cdots (X - \alpha_k)^{n_k} \in \overline{K}[X],$$

over $\overline{K}$, then $K(\alpha_1, \ldots, \alpha_k)$ is a splitting field of f over K. Hence f has multiple roots in a splitting field of K.

(ii) $\implies$ (iii). Suppose f has multiple roots in a splitting field of K and α is a multiple root of f. Then $\gcd(f, f') \neq 1$, which implies there exists a common factor of f and f'. Note f is irreducible. The only factors of f are f and 1, up to a unit. Hence $f | f'$. Since $\deg f' < \deg f$, there must be $f' = 0$.

(iii) $\implies$ (iv). Suppose

$$f(X) = \sum_{n=0}^{N} a_n X^n \in K[X]$$

is an irreducible polynomial and

$$f'(X) = \sum_{n=1}^{N} n a_n X^{n-1} = 0,$$

Thus for any $n \in \mathbb{Z}_{\geq 1}$, we have

$$\begin{aligned} n a_n = 0 &\implies (n \cdot 1_K)\, a_n = 0 \\ &\implies n \cdot 1_K = 0 \text{ or } a_n = 0 \end{aligned}$$

Note $a_N \neq 0$. There must be $N \cdot 1_K = 0$, which implies $\mathrm{char}(K) = p > 0$. Furthermore, since $n \cdot 1_K = 0 \iff p \mid n$, we have

$$p \nmid n \iff n \cdot 1_K \neq 0 \implies a_n = 0.$$

So we can write

$$f(X) = \sum_{k=0}^{M} a_{kp} X^{kp} = g(X^p),$$

where

$$g(X) = \sum_{k=0}^{M} a_{kp} X^k \in K[X].$$

(iv) $\implies$ (i). Suppose $\mathrm{char}(K) = p > 0$ and $f(X) = g(X^p)$ for some

$$g(X) = \sum_{k=0}^{M} b_k X^k \in K[X].$$

Suppose $y_1, \cdots, y_M$ are the roots of g in an algebraic closure $\overline{K}$ of K. For each y_i, we can find $x_i \in \overline{K}$ such that $x_i^p = y_i$. Thus we have

$$f(X) = c \prod_{i=1}^{M} (X^p - y_i) = c \prod_{i=1}^{M} (X^p - x_i^p) = c \prod_{i=1}^{M} (X - x_i)^p \in \overline{K}[X],$$

which implies f has multiple roots in an algebraic closure of K. □

Definition 11.4.5 Separable Element

Let L/K be a field extension and $\alpha \in L$ be an algebraic element over K. We say α is a **separable element** over K if the minimal polynomial of α over K is separable.

Definition 11.4.6 Separable Extension

A algebraic extension L/K is **separable** if every element of L is separable over K.

Lemma 11.4.7

Let L/K be a finite extension such that $L = K(\alpha_1, \cdots, \alpha_n)$ for some $\alpha_1, \cdots, \alpha_n \in L$. Suppose $\overline{K}/K$ is an algebraic closure of K. Define $K_0 := K$ and $K_i := K_{i-1}(\alpha_i)$ for $1 \leq i \leq n$. Denote the minimal polynomial of α_i over K_{i-1} by $m_{\alpha_i} \in K_{i-1}[X]$.

(i) If m_{α_i} is separable for any $1 \leq i \leq n$, then

$$\left|\mathrm{Hom}_{(\mathsf{Field}/K)}(L, \overline{K})\right| = [L : K]$$

and L/K is separable.

(ii) If there exists $1 \leq j \leq n$ such that m_{α_j} is inseparable, then

$$\left|\mathrm{Hom}_{(\mathsf{Field}/K)}(L, \overline{K})\right| < [L : K].$$

Proof. If α_i is separable over K_{i-1}, then the minimal polynomial m_{α_i} is separable, which implies

$$\deg_s(m_{\alpha_i}) = \deg(m_{\alpha_i}) = [K_i : K_{i-1}]$$

(last equality by Lemma 9.9.2). By multiplicativity (Lemma 9.7.7) we have

$$[K : F] = \prod [K_i : K_{i-1}] = \prod \deg(m_{\alpha_i}) = \prod \deg_s(m_{\alpha_i}) = \left|\mathrm{Mor}_F(K, \bar{F})\right|$$

where the last equality is Lemma 9.12.9. By the exact same argument we get the strict inequality $\left|\mathrm{Mor}_F(K, \bar{F})\right| < [K : F]$ if one of the α_i is not separable over K_{i-1}.

Finally, assume again that each α_i is separable over K_{i-1}. We will show K/F is separable. Let $\gamma = \gamma_1 \in K$ be arbitrary. Then we can find additional elements $\gamma_2, \ldots, \gamma_m$ such that $K = F(\gamma_1, \ldots, \gamma_m)$ (for example we could take $\gamma_2 = \alpha_1, \ldots, \gamma_{n+1} = \alpha_n$). Then we see by the last part of the lemma (already proven above) that if γ is not separable over F we would have the strict inequality $\left|\mathrm{Mor}_F(K, \bar{F})\right| < [K : F]$ contradicting the very first part of the lemma (already prove above as well). □

Proposition 11.4.8 Equivalent Characterization of Finite Separable Extension

Let L/K be a finite field extension. The following are equivalent:

(i) L/K is a separable extension.

(ii) $L = K(\alpha_1, \cdots, \alpha_n)$ for some separable elements $\alpha_1, \cdots, \alpha_n \in L$ over K.

(iii) Let $\overline{K}/K$ be an algebraic closure of K.

$$\left|\mathrm{Hom}_{(\mathsf{Field}/K)}(L, \overline{K})\right| = [L : K]$$

(iv) The trace pairing is nondegenerate.

(v) $L \otimes_K \overline{K} \cong \overline{K} \times \cdots \times \overline{K}$

Definition 11.4.9 Perfect Field

A field K is **perfect** if every finite extension of K is separable.

Definition 11.4.10 Equivalent Characterization of Perfect Field

Let K be a field. The following are equivalent:

(i) K is perfect.

(ii) Every irreducible polynomial in $K[X]$ is separable.

(iii) Every algebraic extension of K is separable.

(iv) Either $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p$ and the Frobenius endomorphism

$$\begin{aligned} \sigma : K &\longrightarrow K \\ x &\longmapsto x^p \end{aligned}$$

is a automorphism of K.

Example 11.4.1 Examples of Perfect Fields

Examples of perfect fields include

- Field of characteristic 0.
- Finite field.
- Algebraically closed field.
- Field which is algebraic over a perfect field.

11.5 Trace and Norm of Field Extension

Definition 11.5.1 Trace and Norm of Finite Extension

Let L/K be a finite field extension and $\alpha \in L$ be an algebraic element over K. We can define a K-linear map

$$\begin{aligned} l_\alpha : L &\longrightarrow L \\ x &\longmapsto \alpha x \end{aligned}$$

called the **left multiplication by** α.

(i) The **trace** of $\alpha \in L$ over K is defined as

$$\mathrm{Tr}_{L/K}(\alpha) := \mathrm{Tr}\left(l_\alpha\right).$$

(ii) The **norm** of $\alpha \in L$ over K is defined as

$$\mathrm{N}_{L/K}(\alpha) := \det\left(l_\alpha\right).$$

Remark. This definition is a special case of Definition 8.4.2. □

Definition 11.5.2 Trace Pairing

Let L/K be a finite extension. The **trace pairing** is the symmetric K-bilinear form

$$\begin{aligned} \langle \cdot, \cdot \rangle_{L/K} : L \times L &\longrightarrow K \\ (x, y) &\longmapsto \mathrm{Tr}_{L/K}(xy). \end{aligned}$$

Remark. This definition is a special case of Definition 8.4.5. □

11.6 Finite Field

Definition 11.6.1 Finite Field

A **finite field** is a field with a finite number of elements.

It is clear that the characteristic of a finite field is a prime number, otherwise the embedding from $\mathbb{Q}$ would force the field to be infinite.

Lemma 11.6.2 Existance of Finite Field

Assume p be a prime number and $m \in \mathbb{Z}_{\geq 1}$. Define $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Let K be the splitting field of the polynomial $f(X) = X^{p^m} - X \in \mathbb{F}_p[X]$. Then

(i) $f(\alpha) = 0$ for all $\alpha \in K$.

(ii) $|K| = p^m$.

(iii) $K/\mathbb{F}_p$ is an extension of degree m.

Proof. (i) Let $f(X) = X^{p^m} - X$ and $K/\mathbb{F}_p$ be a splitting field of f. For any $x, y \in K$, we have $(x+y)^{p^m} = x^{p^m} + y^{p^m}$, which implies the set of roots of f in K

$$M := \{\alpha \in K \mid f(x) = 0\} = \left\{\alpha \in K \mid \alpha^{p^m} = \alpha\right\}$$

is a subfield of K. By Proposition 11.1.18, $M/\mathbb{F}_p$ is a subextension of $K/\mathbb{F}_p$. Note that $f(X) = X^{p^m} - X \in \mathbb{F}_p[X]$ splits over M and $M = \mathbb{F}_p(M)$. We see $M/\mathbb{F}_p$ is a splitting field of f by definition. By the uniqueness of splitting field, $M/\mathbb{F}_p$ and $K/\mathbb{F}_p$ are $\mathbb{F}_p$-isomorphic. Since K as a splitting field is finite, we get $M = K$. Therefore, for all $\alpha \in K$, there must be $f(\alpha) = 0$.

(ii) Since

$$f'(X) = p^m X^{p^m - 1} - 1 = -1,$$

we have $\gcd(f, f') = 1$. From Proposition 11.4.3 we see f has p^m distinct roots in K, which implies $|M| \geq p^m$. On the other hand, $|M| \leq \deg f = p^m$. Thus we have $|K| = |M| = p^m$.

(iii) From $|K| = |\mathbb{F}_p|^{[K:\mathbb{F}_p]} = p^{[K:\mathbb{F}_p]} = p^m$, we see $[K : \mathbb{F}_p] = m$.

□

Corollary 11.6.3 Uniqueness of Finite Field

For any prime number p and $m \in \mathbb{Z}_{\geq 1}$, there exists a unique finite field of order $q := p^m$ up to isomorphism, denoted by $\mathbb{F}_q$. Any finite field must be isomorphic to $\mathbb{F}_q$ for some prime number p and $m \in \mathbb{Z}_{\geq 1}$.

Proof. The existence of $\mathbb{F}_q$ follows from Lemma 11.6.2. The uniqueness of $\mathbb{F}_q$ follows the uniqueness of splitting field. Finite field must have positive characteristic, which is a prime number p. Then the finite field is an extension of $\mathbb{F}_p$ of degree m. Any Characteristic zero field is infinite since it contains an isomorphic copy of $\mathbb{Q}$. Thus finite field F must have positive characteristic, say p. Thus $F/\mathbb{F}_p$ is a finite extension and $|F| = p^{[F:\mathbb{F}_p]}$. □

Due to the uniqueness of finite fields, whenever we use the notation $\mathbb{F}_q$, it is understood that the proposition holds for any finite field of order q we choose.

Definition 11.6.4 Frobenius Endomorphism of Commutative $\mathbb{F}_q$-algebra

Let p be a prime number and $m \in \mathbb{Z}_{\geq 1}$. Let $q = p^m$. The **Frobenius endomorphism** of $\mathbb{F}_q$-algebra is defined as the following $\mathbb{F}_q$-algebra homomorphism

$$\begin{aligned} \mathrm{Fr}_{q,A} : A &\longrightarrow A \\ x &\longmapsto x^q \end{aligned}$$

Remark. In the definition of Frobenius endomorphism of a commutative ring, we see $\mathrm{Fr}_{q,A}$ is a ring homomorphism. To check $\mathrm{Fr}_{q,A}$ is a $\mathbb{F}_q$-algebra homomorphism, we only need to check $\mathrm{Fr}_{q,A}$ is $\mathbb{F}_q$-linear. This is clear because for any $a \in \mathbb{F}_q$ and $x \in A$, we have

$$\mathrm{Fr}_{q,A}(ax) = (ax)^q = a^q x^q = a\mathrm{Fr}_{q,A}(x).$$

□

Proposition 11.6.5 Additivity of the Frobenius Powers

Let p be a prime number and $m \in \mathbb{Z}_{\geq 1}$. Let $q = p^m$. Then for any $a, b \in \mathbb{F}_q$ and any $k \in \mathbb{Z}_{\geq 0}$, we have

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}.$$

Proof. Consider the Frobenius automorphism

$$\begin{aligned} \mathrm{Fr}_{p,\mathbb{F}_q} : \mathbb{F}_q &\longrightarrow \mathbb{F}_q \\ x &\longmapsto x^p. \end{aligned}$$

For any $a, b \in \mathbb{F}_q$ and any $k \in \mathbb{Z}_{\geq 0}$, we have

$$(a+b)^{p^k} = \left(\mathrm{Fr}_{p,\mathbb{F}_q}\right)^k (a+b) = \left(\mathrm{Fr}_{p,\mathbb{F}_q}\right)^k (a) + \left(\mathrm{Fr}_{p,\mathbb{F}_q}\right)^k (b) = a^{p^k} + b^{p^k}.$$

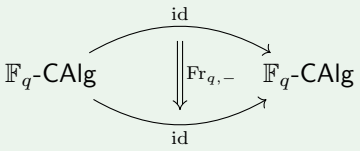
□

Proposition 11.6.6 Functoriality of Frobenius Endomorphism

Let p be a prime number and $m \in \mathbb{Z}_{\geq 1}$. Let $q = p^m$. Let A, B be commutative $\mathbb{F}_q$-algebras and $f : A \to B$ be a $\mathbb{F}_q$-algebra homomorphism. Then the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \mathrm{Fr}_{q,A}}\downarrow & & \downarrow{\scriptstyle \mathrm{Fr}_{q,B}} \\ A & \xrightarrow[f]{} & B \end{array}$$

This implies Frobenius endomorphism gives a natural transformation $\mathrm{Fr}_{q,-} : \mathrm{id}_{\mathbb{F}_q\text{-}\mathsf{CAlg}} \Rightarrow \mathrm{id}_{\mathbb{F}_q\text{-}\mathsf{CAlg}}$.



Proof. For any $x \in A$, we have

$$\mathrm{Fr}_{q,B} \circ f(x) = f(x)^p = f(x^p) = f \circ \mathrm{Fr}_{q,A}(x).$$

□

Proposition 11.6.7 Properties of Finite Field

Let p be a prime number and $m \in \mathbb{Z}_{\geq 1}$. Let $q = p^m$. Then

(i) Let $k \in \mathbb{Z}_{\geq 1}$. Then there exists a field extension $\mathbb{F}_{q^k}/\mathbb{F}_q$ such that it is a splitting field of the polynomial $f(X) = X^{q^k} - X \in \mathbb{F}_q[X]$.

(ii) $\mathbb{F}_q$ is a splitting field of the polynomial $f(X) = X^q - X \in \mathbb{F}_p[X]$. So for any $x \in \mathbb{F}_q$ and any $r \in \mathbb{Z}_{\geq 0}$, we have

$$x^{q^r} = x.$$

(iii) $\mathbb{F}_{q^k}/\mathbb{F}_q$ is a Galois extension of degree k.

(iv) The characteristic of $\mathbb{F}_q$ is p.

(v) Let $a, b \in \mathbb{Z}_{\geq 1}$ and $\mathbb{F}_{q^a}/\mathbb{F}_q$, $\mathbb{F}_{q^b}/\mathbb{F}_q$ be field extensions. Then

$$\mathrm{Hom}_{(\mathsf{Field}_p/\mathbb{F}_q)}(\mathbb{F}_{q^a}/\mathbb{F}_q, \mathbb{F}_{q^b}/\mathbb{F}_q) \neq \varnothing \iff a \mid b.$$

If $a \mid b$, then $\left[\mathbb{F}_{q^b} : \mathbb{F}_{q^a}\right] = \frac{b}{a}$.

Proof. (i) Suppose $\iota : \mathbb{F}_q \hookrightarrow K$ is a splitting field of $f(X) = X^{q^k} - X \in \mathbb{F}_q[X]$. For any $x, y \in K$, we have

$$(x+y)^{q^k} = x^{q^k} + y^{q^k}, \quad (xy)^{q^k} = x^{q^k} y^{q^k},$$

which implies the set of roots of f in K

$$M := \{\alpha \in K \mid f(x) = 0\} = \left\{\alpha \in K \mid \alpha^{q^k} = \alpha\right\}$$

is a subfield of K. By Lemma 11.6.2, since $\mathbb{F}_q$ is a splitting field of $X^{p^m} - X \in \mathbb{F}_p[X]$, for any $a \in \mathbb{F}_q$, we have $a^q = a$, which implies $a^{q^k} = a$ for all $k \in \mathbb{Z}_{\geq 1}$. Thus we have $\iota(\mathbb{F}_q) \subseteq M$ and we can shrink the codomain of ι to get the field extension $\iota' : \mathbb{F}_q \hookrightarrow M$ such that $i \circ \iota' = \iota$, where $i : M \hookrightarrow K$ is the inclusion map. This means $M/\mathbb{F}_q$ is a subextension of $K/\mathbb{F}_q$.

Note that $f(X) = X^{q^k} - X \in \mathbb{F}_q[X]$ splits over M and $M = \mathbb{F}_q(M)$. We see $M/\mathbb{F}_q$ is a splitting field of f by definition. By the uniqueness of splitting field, $M/\mathbb{F}_q$ and $K/\mathbb{F}_q$ are $\mathbb{F}_q$-isomorphic. Since K as a splitting field is finite, we see $M = K$.

Since

$$f'(X) = q^k X^{q^k - 1} - 1 = -1,$$

we have $\gcd(f, f') = 1$. From Proposition 11.4.3 we see f has q^k distinct roots in K, which implies $|M| \geq q^k$. On the other hand, $|M| \leq \deg f = q^k$. Thus we have $|K| = |M| = q^k$. Thus $\iota : \mathbb{F}_q \hookrightarrow K$ is the desired field extension.

(ii) Take $q = p$ and $k = m$. This is a direct consequence of (i).

(iii) From (ii) we see $\mathbb{F}_{q^k}/\mathbb{F}_q$ is a Galois extension. Since

$$q^{[\mathbb{F}_{q^k} : \mathbb{F}_q]} = |\mathbb{F}_q|^{[\mathbb{F}_{q^k} : \mathbb{F}_q]} = |\mathbb{F}_{q^k}| = q^k,$$

we obtain $[\mathbb{F}_{q^k} : \mathbb{F}_q] = k$.

(iv) By (i), there exists a field extension $\mathbb{F}_{p^m}/\mathbb{F}_p$. Since field extension preserves characteristic, we have $\mathrm{char}(\mathbb{F}_{p^m}) = \mathrm{char}(\mathbb{F}_p) = p$.

(v) Let $a, b \in \mathbb{Z}_{\geq 1}$ and $\mathbb{F}_{q^a}/\mathbb{F}_q$, $\mathbb{F}_{q^b}/\mathbb{F}_q$ be field extensions.

- $\mathrm{Hom}_{(\mathsf{Field}_p/\mathbb{F}_q)}(\mathbb{F}_{q^a}/\mathbb{F}_q, \mathbb{F}_{q^b}/\mathbb{F}_q) \neq \varnothing \implies a \mid b$. If there exists an $\mathbb{F}_q$-embedding $\mathbb{F}_{q^a} \hookrightarrow \mathbb{F}_{q^b}$, then

$$b = [\mathbb{F}_{q^b} : \mathbb{F}_q] = [\mathbb{F}_{q^b} : \mathbb{F}_{q^a}][\mathbb{F}_{q^a} : \mathbb{F}_q] = [\mathbb{F}_{q^b} : \mathbb{F}_{q^a}]\, a,$$

  Thus we have $a \mid b$.
- $a \mid b \implies \mathrm{Hom}_{(\mathsf{Field}_p/\mathbb{F}_q)}(\mathbb{F}_{q^a}/\mathbb{F}_q, \mathbb{F}_{q^b}/\mathbb{F}_q) \neq \varnothing$. Suppose $a \mid b$. Then we have $q^a - 1 \mid q^b - 1$. So we can asssume there exists $c \in \mathbb{Z}_{\geq 1}$ such that $q^b - 1 = c(q^a - 1)$. Note

$$\begin{aligned} X^{q^b} - X &= X\left(X^{q^b - 1} - 1\right) \\ &= X\left(\left(X^{q^a - 1}\right)^c - 1\right) \\ &= X\left(X^{q^a - 1} - 1\right)\left(\sum_{j=0}^{c-1}\left(X^{q^a-1}\right)^j\right) \\ &= \left(X^{q^a} - X\right)\left(\sum_{j=0}^{c-1}\left(X^{q^a-1}\right)^j\right). \end{aligned}$$

We have

$$\left(X^{q^a}-X\right) \mid \left(X^{q^b}-X\right).$$

According to Proposition 11.3.2, since $X^{q^b}-X \in \mathbb{F}_q[X]$ splits over $\mathbb{F}_{q^b}$, we see $X^{q^a}-X \in \mathbb{F}_q[X]$ also splits over $\mathbb{F}_{q^b}$. Recall that $\mathbb{F}_{q^a}$ is a splitting field of $X^{q^a}-X \in \mathbb{F}_q[X]$. By the minimality of splitting field, there exists an $\mathbb{F}_q$-embedding $\mathbb{F}_{q^a} \hookrightarrow \mathbb{F}_{q^b}$.

□

Proposition 11.6.8 Galois Group of Finite Field

Let p be a prime number and $m \in \mathbb{Z}_{\geq 1}$. Let $q = p^m$. Suppose $L/\mathbb{F}_q$ is a finite extension of degree $n := [L : \mathbb{F}_q]$. Then

(i) $L/\mathbb{F}_q$ is a Galois extension.

(ii) $\mathrm{Gal}(L/\mathbb{F}_q)$ is a cyclic group of order n. The Frobenius automorphism $\mathrm{Fr}_{q,L}$ generates $\mathrm{Gal}(L/\mathbb{F}_q)$, that is,

$$\mathrm{Gal}(L/\mathbb{F}_q) = \left\{ \left(\mathrm{Fr}_{q,L}\right)^k \,\middle|\, k = 0, 1, \cdots, n-1 \right\}.$$

Proof. (i) Since $\mathbb{F}_p$ is initial in Field_p, we have a tower of field extensions $L/\mathbb{F}_q/\mathbb{F}_p$. From Proposition 11.6.7 (iii), we see $L/\mathbb{F}_p$ is a Galois extension. According to Proposition 12.1.2, $L/\mathbb{F}_q$ is also a Galois extension.

(ii) It is clear that $\mathrm{Fr}_{q,L} \in \mathrm{Gal}(L/\mathbb{F}_q)$. Note $|\mathrm{Gal}(L/\mathbb{F}_q)| = [L : \mathbb{F}_q] = n$. We only need to show that the order of $\mathrm{Fr}_{q,L}$ is n. For any $x \in L$, we have

$$\left(\mathrm{Fr}_{q,L}\right)^n (x) = x^{q^n} = x,$$

which means $\left(\mathrm{Fr}_{q,L}\right)^n = \mathrm{id}_L$. Hence, the order of $\mathrm{Fr}_{q,L}$ divides n.

Now we prove $\left(\mathrm{Fr}_{q,L}\right)^k \neq \mathrm{id}_L$ for any $1 \leq k < n$. Suppose there exists $k \in \mathbb{Z}_{\geq 1}$ such that $\left(\mathrm{Fr}_{q,L}\right)^k = \mathrm{id}_L$. Then for any $x \in L$, we have

$$x^{q^k} = x.$$

So every element of L is a root of the polynomial

$$f(T) = T^{q^k} - T \in \mathbb{F}_q[T],$$

which means f has at least $|L| = q^n$ distinct roots in L. Thus we have

$$q^n = |L| \leq \deg f = q^k,$$

which implies $k \geq n$. Therefore, we see the order of $\mathrm{Fr}_{q,L}$ is n.

□

By Galois correspondence, we can classify all intermediate fields of finite field extension of $\mathbb{F}_q$.

Proposition 11.6.9

Suppose p is a prime number and $m \in \mathbb{Z}_{\geq 1}$. Let $q = p^m$. Suppose $L \supseteq \mathbb{F}_q$ is a finite extension of degree $n := [L : \mathbb{F}_q]$. Then there is a one-to-one correspondence between the set of intermediate fields of $L/\mathbb{F}_q$ and the set of divisors of n:

$$\begin{aligned} \{d \in \mathbb{Z}_{\geq 1} \mid d \mid n\} &\xrightarrow{\sim} E_d := \{E \mid \mathbb{F}_q \subseteq E \subseteq L\}, \\ d &\longmapsto \left\{ x \in L \,\middle|\, x^{q^{\frac{n}{d}}} = x \right\}, \\ [L : E] &\longmapsfrom E. \end{aligned}$$

Moreover, we have $E_d \cong \mathbb{F}_{q^{\frac{n}{d}}}$. For any factors d_1, d_2 of n,

$$d_1 \mid d_2 \iff E_{d_1} \supseteq E_{d_2}.$$

Proof. By Galois correspondence, there is a one-to-one correspondence

$$\begin{aligned} f : \{H \leq \mathrm{Gal}(L/\mathbb{F}_q)\} &\xrightarrow{\sim} \{E \mid \mathbb{F}_q \subseteq E \subseteq L\}, \\ H &\longmapsto L^H := \{x \in L \mid \sigma(x) = x, \forall \sigma \in H\}, \\ \mathrm{Gal}(L/E) &\longmapsfrom E. \end{aligned}$$

And there is a one-to-one correspondence

$$\begin{aligned} g : \{d \in \mathbb{Z}_{\geq 1} \mid d \mid n\} &\xrightarrow{\sim} \{H \leq \mathrm{Gal}(L/\mathbb{F}_q)\}, \\ d &\longmapsto \left\langle (\mathrm{Fr}_{q,L})^{\frac{n}{d}} \right\rangle, \\ |H| &\longmapsfrom H. \end{aligned}$$

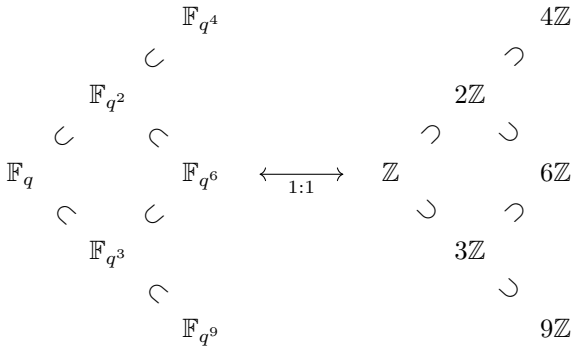
Note

$$\begin{aligned} f \circ g(d) &= L^{\left\langle (\mathrm{Fr}_{q,L})^{\frac{n}{d}} \right\rangle} \\ &= \left\{ x \in L \,\middle|\, (\mathrm{Fr}_{q,L})^{\frac{n}{d}}(x) = x \right\} \\ &= \left\{ x \in L \,\middle|\, x^{q^{\frac{n}{d}}} = x \right\}, \end{aligned}$$

and

$$g \circ f(E) = |\mathrm{Gal}(L/E)| = [L : E].$$

Thus the desired one-to-one correspondence is given by $f \circ g$. □



Chapter 12

Galois Theory

12.1 Basic Definitions

Definition 12.1.1 Galois Extension

Let K be a field and L/K be a field extension. The extension L/K is called a **Galois extension** if it is normal and separable.

Proposition 12.1.2 Properties of Galois Extension

(i) Suppose $L/E/F$ is a tower of field extensions. If L/F is Galois, then L/E is Galois.

(ii) Suppose L_1/F and L_2/F are subextension of a extension Ω/F. If L_1/F is Galois, then L_1L_2/L_2 is Galois.

(iii) Suppose $(L_i/F)_{i\in I}$ is a family of subextensions of a extension Ω/F. If each L_i/F is Galois, then the compositum

$$\left(\bigvee_{i\in I} L_i\right)/F$$

is Galois.

Definition 12.1.3 Fixed Field

Let L/K be a field extension and $H \leq \mathrm{Aut}(L/K)$ be a subgroup of the automorphism group of L/K. The **fixed field** of H is defined as

$$L^H := \{x \in L \,|\, \sigma(x) = x, \forall \sigma \in H\}\,.$$

Proposition 12.1.4

Let L/K be a field extension. Define

$$\begin{aligned}\mathsf{Subextension}(L/K) &:= \{E/K \,|\, E/K \text{ is a subextension of } L/K\}\\ \mathsf{Subgroup}\,(\mathrm{Aut}(L/K)) &:= \{H \,|\, H \leq \mathrm{Aut}(L/K)\}\end{aligned}$$

the following maps

$$\begin{aligned}\Phi : \mathsf{Subextension}(L/K) &\longrightarrow \mathsf{Subgroup}\,(\mathrm{Aut}(L/K))\\ E/K &\longmapsto \mathrm{Aut}(L/E)\end{aligned}$$

$$\begin{aligned}\Psi : \mathsf{Subgroup}\,(\mathrm{Aut}(L/K)) &\longrightarrow \mathsf{Subextension}(L/K)\\ H &\longmapsto L^H := \{x \in L \,|\, \sigma(x) = x, \forall \sigma \in H\}\end{aligned}$$

(i) Both the $(\mathsf{Subgroup}\,(\mathrm{Aut}(L/K)), \leq)$ and $(\mathsf{Subextension}(L/K), \subseteq)$ are partially ordered sets. The maps Φ and Ψ are inclusion-reversing, i.e.

$$H_1 \leq H_2 \implies \Psi(H_2) \subseteq \Psi(H_1) \iff L^{H_2} \subseteq L^{H_1}$$
$$E_1 \subseteq E_2 \implies \Phi(E_2) \leq \Phi(E_1) \iff \mathrm{Aut}(L/E_2) \leq \mathrm{Aut}(L/E_1)$$

(ii) For any subextension E/K of L/K and any subgroup $H \leq \mathrm{Aut}(L/K)$, we have

$$E \subseteq \Psi \circ \Phi(E) = L^{\mathrm{Aut}(L/E)}$$
$$H \leq \Phi \circ \Psi(H) = \mathrm{Aut}(L/L^H)$$

(iii) The group $\mathrm{Aut}(L/K)$ acts on the set of subextensions $\mathsf{Subextension}(L/K)$ by

$$\begin{aligned}\mathrm{Aut}(L/K) \times \mathsf{Subextension}(L/K) &\longrightarrow \mathsf{Subextension}(L/K)\\ (\sigma, E/K) &\longmapsto \sigma \cdot E := \sigma(E) = \{\sigma(x) \,|\, x \in E\}\end{aligned}$$

The group $\mathrm{Aut}(L/K)$ also acts on the set of subgroups $\mathsf{Subgroup}\,(\mathrm{Aut}(L/K))$ by

$$\begin{aligned}\mathrm{Aut}(L/K) \times \mathsf{Subgroup}\,(\mathrm{Aut}(L/K)) &\longrightarrow \mathsf{Subgroup}\,(\mathrm{Aut}(L/K))\\ (\sigma, H) &\longmapsto \sigma \cdot H = \sigma H \sigma^{-1} = \left\{\sigma\tau\sigma^{-1} \,\middle|\, \tau \in H\right\}\end{aligned}$$

The maps Φ and Ψ are equivariant with respect to this action. That is, for any $\sigma \in \mathrm{Aut}(L/K)$, $E/K \in \mathsf{Subextension}(L/K)$ and $H \leq \mathrm{Aut}(L/K)$, we have

$$\Phi(\sigma \cdot E) = \sigma \cdot \Phi(E)$$
$$\Psi(\sigma \cdot H) = \sigma \cdot \Psi(H)$$

namely,

$$\mathrm{Aut}(L/\sigma(E)) = \sigma\,\mathrm{Aut}(L/E)\sigma^{-1}$$
$$L^{\sigma H \sigma^{-1}} = \sigma(L^H)$$

(iv) If $L \supseteq K$ is a Galois extension, then

$$\Psi \circ \Phi(K/K) = L^{\mathrm{Gal}(L/K)} = K,$$

and

$$\begin{aligned}\Phi : \mathsf{Subextension}(L/K) &\longrightarrow \mathsf{Subgroup}\,(\mathrm{Aut}(L/K))\\ E/K &\longmapsto \mathrm{Gal}(L/E)\end{aligned}$$

is injective.

Proof. (iv) Suppose L/K is Galois. In (ii), we already have $K \subseteq L^{\mathrm{Gal}(L/K)}$. To show $L^{\mathrm{Gal}(L/K)} = K$, it suffices to show that $L^{\mathrm{Gal}(L/K)} \subseteq K$. Take any $x \in L^{\mathrm{Gal}(L/K)}$. Then we have

$$\sigma(\alpha) = \alpha \quad \text{for all } \sigma \in \mathrm{Gal}(L/K).$$

Let $P_x \in K[T]$ be the minimal polynomial of x over K. Suppose $\deg P_x = n$. Since L/K is normal and separable, P_x has n distinct roots in L. Let these roots be $x_1, x_2, \ldots, x_n \in L$. From Proposition 8.5.6, we know P_x is also the minimal polynomial of each x_i over K for $i = 1, 2, \ldots, n$. By Corollary 11.2.3, for each $i = 1, 2, \ldots, n$, there exists an automorphism $\sigma_i \in \mathrm{Gal}(L/K)$ such that $\sigma_i(x) = x_i$. However, since $x \in L^{\mathrm{Gal}(L/K)}$, we have $\sigma_i(x) = x$ for all i. This implies that all roots of P_x are equal to x, which forces $\deg P_x = 1$ and accordingly $x \in K$. Therefore, we conclude that $L^{\mathrm{Gal}(L/K)} = K$.

□

12.2 Infinite Galois Correspondence

Definition 12.2.1 Krull Topology

Let K be a field and $L \supseteq K$ a Galois extension. The **Krull topology** on $\mathrm{Gal}(L/K)$ is given by the neighborhood basis of the identity id_L, which consists of the sets

$$\mathrm{Gal}(L/E)$$

where E runs over all intermediate extensions $L \supseteq E \supseteq K$ with E/K being finite Galois. Equipping $\mathrm{Gal}(L/K)$ with this topology makes it a topological group.

Remark. First we check the collection of sets defined above indeed forms a neighborhood basis of identity. First we have $\mathrm{id}_L \in \mathrm{Gal}(L/E)$ for any intermediate extension E/K. Next, there exists at least one such intermediate extension, namely $E = K$. Finally, given two such intermediate extensions $E_1 \subseteq K$, $E_2 \subseteq K$, we can take $E_3 := E_1E_2$ to be the compositum of E_1 and E_2. Then E_3/K is an also finite Galois extension. □

Intuitively, the Krull topology says that two automorphisms σ and τ in $\mathrm{Gal}(L/K)$ are close if they agree on a sufficiently large finite Galois subextension E/K of L/K, i.e.

$$\sigma|_E = \tau|_E.$$

Chapter 13

Valuation Theory

13.1 Valuation of Ring

Definition 13.1.1 Totally Ordered Abelian Group

Suppose $(\Gamma, +)$ is an abelian group and $\leq$ is a total order on Γ. Totally ordered abelian group is a tuple $(\Gamma, +, \leq)$ such that for any $a, b, c \in \Gamma$,

$$a \leq b \implies a + c \leq b + c.$$

The total order $\leq$ can induce a strict total order $<$ on Γ by defining $a < b \iff a \leq b$ and $a \neq b$.

Proposition 13.1.2 Properties of Totally Ordered Abelian Group

Let $(\Gamma, +, \leq)$ be a totally ordered abelian group. Then

(i) $a \leq a', b \leq b' \implies a + b \leq a' + b'$.

(ii) $x \leq y \iff -y \leq -x$.

(iii) Γ is torsion-free. That is, for all $n \in \mathbb{Z}_{\geq 1}$ and $a \in \Gamma$,

$$na = 0 \implies a = 0.$$

Proof. (i) If $a \leq a', b \leq b'$, then $a + b \leq a' + b \leq a' + b'$.

(ii) $x \leq y \implies x - x - y \leq y - x - y \implies -y \leq -x$. The other direction is similar.

(iii) If $a > 0$, then $na > 0$ for all $n \in \mathbb{Z}_{\geq 1}$. If $a < 0$, then $na < 0$ for all $n \in \mathbb{Z}_{\geq 1}$. Therefore, if $a \neq 0$, then $na \neq 0$ for all $n \in \mathbb{Z}_{\geq 1}$.

□

Proposition 13.1.3 Extended Totally Ordered Abelian Group

Let $(\Gamma, +, \leq)$ be a totally ordered abelian group. The total order and group addition on Γ are extended to the set $\Gamma \cup \{\infty\}$ by the rules:

- $\alpha \leq \infty$ for all $\alpha \in \Gamma \cup \{\infty\}$,
- $\infty + \alpha = \alpha + \infty = \infty$ for all $\alpha \in \Gamma \cup \{\infty\}$.

Definition 13.1.4 Valuation of Ring

Let R be a commutative ring, and $(\Gamma, +, \leq)$ be a totally ordered abelian group. A valuation on R with value group Γ refers to a mapping $v : R \to \Gamma \sqcup \{\infty\}$ satisfying the following properties:

- $v(1) = 0$, $v(0) = \infty$,

- $v(xy) = v(x) + v(y), \quad \forall x, y \in R,$
- $v(x+y) \geq \min\{v(x), v(y)\}, \quad \forall x, y \in R.$

Furthermore, we require that $v(R) - \{\infty\}$ generates the group Γ. If there exists an embedding of the totally ordered abelian group $\Gamma \hookrightarrow \mathbb{R}$, then v is referred to as a rank 1 valuation.

Proposition 13.1.5 Properties of Valuation of Ring

Let $v : R \to \Gamma \cup \{\infty\}$ be a valuation of a commutative ring R. Then

(i) If $x \in R^\times$, then $v(x^{-1}) = -v(x)$.

(ii) $v(R^\times)$ is a subgroup of Γ.

(iii) If $a^n = 1$ for some $n \in \mathbb{Z}_{\geq 1}$, then $v(a) = 0$. Specially, $v(-1) = 0$.

(iv) $v(-a) = v(a)$ for all $a \in R$.

(v) $v^{-1}(\infty)$ is a prime ideal of R.

(vi) By the universal property quotient set, v induces a map

$$\begin{aligned} \tilde{v} : R/v^{-1}(\infty) &\longrightarrow \Gamma \cup \{\infty\} \\ x + v^{-1}(\infty) &\longmapsto v(x) \end{aligned}$$

Moreover, $\tilde{v}$ is a valuation of $R/v^{-1}(\infty)$.

(vii) For any $x_1, \cdots, x_n \in R$, we have

$$v(x_1 + \cdots + x_n) \geq \min\{v(x_1), \cdots, v(x_n)\}$$

If there exists j such that for all $i \neq j$ we have $v(x_j) < v(x_i)$, then the equality

$$v(x_1 + \cdots + x_n) = v(x_j)$$

holds.

Proof. (i) $v(x^{-1}) = v(x^{-1}x) - v(x) = v(1) - v(x) = -v(x)$.

(ii) If $x \in R^\times$, then $v(x) + v(x^{-1}) = 0 \implies v(x) \neq \infty$.

(iii) $v(a^n) = nv(a) = 0 \implies v(a) = 0$.

(iv) $v(-a) = v(-1) + v(a) = 0 + v(a) = v(a)$.

(v) For any $x, y \in v^{-1}(\infty)$, we have $v(x+y) \geq \min(v(x), v(y)) = \infty$, which means $x + y \in v^{-1}(\infty)$. For any $r \in R$ and $x \in v^{-1}(\infty)$, we have $v(rx) = v(r) + v(x) = \infty$, which means $rx \in v^{-1}(\infty)$. Thus $v^{-1}(\infty)$ is a ideal of R. If $x, y \in R$ and $xy \in v^{-1}(\infty)$, then $v(xy) = v(x) + v(y) = \infty$, which means $x \in v^{-1}(\infty)$ or $y \in v^{-1}(\infty)$. Thus $v^{-1}(\infty)$ is a prime ideal of R.

(vi) We first check $\tilde{v}$ is well-defined. If $x - y = a \in v^{-1}(\infty)$, then we have

$$v(x) = v(y + a) \geq \min\{v(y), v(a)\} = \min\{v(y), \infty\} = v(y).$$

Similarly, we have $v(y) = v(x - a) \geq v(x)$, which means $v(x) = v(y)$. Thus $\tilde{v}$ is well-defined. It is easy to check that $\tilde{v}$ is a valuation.

□

13.2 Valuation of Field

Definition 13.2.1 Valuation of Field

Suppose K is a field and $(\Gamma, +, \geq)$ is an totally ordered abelian group. Then a **valuation of** K is any map

$$v : K \to \Gamma \cup \{\infty\}$$

which satisfies the following properties for all a, b in K :

- $v(a) = \infty$ if and only if $a = 0$,
- $v(ab) = v(a) + v(b)$, i.e. v is a abelian group homomorphism from $K^\times$ to Γ,
- $v(a + b) \geq \min(v(a), v(b))$, with equality if $v(a) \neq v(b)$.

Definition 13.2.2 Value Group

The **value group** of a valuation v is the subgroup of Γ defined as $v(K^\times)$.

Definition 13.2.3 Discrete Valuation

A **discrete valuation** on a field K is a valuation $v : K \to \mathbb{Z} \cup \{\infty\}$.

Definition 13.2.4 Valuation Ring

The **valuation ring** of a valuation v is the subring of K defined as

$$\mathcal{O}_v := \{a \in K : v(a) \geq 0\}.$$

Proposition 13.2.5

Suppose v is a valuation of a field K. Then the unit group of $\mathcal{O}_v$ has the form

$$\mathcal{O}_v^\times = \{a \in K : v(a) = 0\}.$$

Proof. For any $a \in \mathcal{O}_v^\times$, we have $a^{-1} \in \mathcal{O}_v$ and $v(a) = -v(a^{-1}) \leq 0$. This forces $v(a) = 0$. Conversely, for any $a \in K$ such that $v(a) = 0$, we have $v(a^{-1}) = -v(a) = 0$, which means $a^{-1} \in \mathcal{O}_v$. Thus $a \in \mathcal{O}_v^\times$. □

Definition 13.2.6 Residue Field of a Valuation

Suppose v is a valuation of a field K. Then

$$\mathfrak{m}_v := \{a \in K : v(a) > 0\}$$

is a maximal ideal of $\mathcal{O}_v$. The **residue field** of v is defined as $\kappa_v = \mathcal{O}_v/\mathfrak{m}_v$.

Definition 13.2.7 Equivalent Valuation

Suppose a filed K has two valuations $v : K \to \Gamma \cup \{\infty\}$ and $v' : K \to \Gamma' \cup \{\infty\}$. we say v and v' are **equivalent** if there is an order-preserving group isomorphism $\varphi : v(K^\times) \to v'(K^\times)$ such that $v' = v \circ \varphi$.

Proposition 13.2.8

Two valuations are equivalent if and only if their valuation rings are equal.

Proposition 13.2.9

Suppose v is a valuation of a field K and ϖ is an element in $\mathcal{O}_v - \{0\}$ such that

$$\sup\{nv(\varpi) \in \Gamma \mid n \in \mathbb{N}\} = \infty.$$

Then there is a natural isomorphism $K \cong \mathcal{O}_v\left[\frac{1}{\varpi}\right]$.

Proof. Since $K = \mathrm{Frac}(\mathcal{O}_v)$, we have an embedding $\mathcal{O}_v\left[\frac{1}{\varpi}\right] \hookrightarrow K$. For any $x \in K$, there exists $n \in \mathbb{N}$ such that $nv(\varpi) \geq -v(x)$. Thus

$$v(x\varpi^n) = v(x) + nv(\varpi) \geq 0 \implies x\varpi^n \in \mathcal{O}_v \implies x \in \mathcal{O}_v\left[\frac{1}{\varpi}\right].$$

□

13.3 Absolute Value of Field

Definition 13.3.1 Absolute Value

An **absolute value** on a field K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ satisfying the following conditions:

(i) For any $x \in K$, $|x| = 0 \iff x = 0$.

(ii) For any $x, y \in K$, $|xy| = |x| \cdot |y|$.

(iii) For any $x, y \in K$, $|x + y| \leq |x| + |y|$.

A field equipped with an absolute value is called a **normed field**, denoted by $(K, |\cdot|)$.

A normed field $(K, |\cdot|)$ induces a metric $d(x, y) = |x - y|$ on K, making it a Hausdorff topological field.

Definition 13.3.2 Trivial Absolute Value

An absolute value $|\cdot|$ on a field K is called **trivial** if

$$|x| = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x \neq 0. \end{cases}$$

Proposition 13.3.3 Properties of Absolute Value

Let $(K, |\cdot|)$ be a normed field. Then we have the following properties:

(i) $|1| = |-1| = 1$.

(ii) $|x| = |-x|$ for all $x \in K$.

(iii) $|n \cdot 1| \leq n$ for all $n \in \mathbb{Z}$.

Definition 13.3.4 Equivalent Absolute Value

Two absolute values on a field are said to be **equivalent** if as topological spaces they are homeomorphic.

Proposition 13.3.5 Equivalent Characterization of Equivalent Absolute Values

Let K be a field and $|\cdot|$ and $|\cdot|_\star$ are two nontrivial absolute values on K. Then the following are equivalent:

(i) $|\cdot|$ and $|\cdot|_\star$ are equivalent absolute values.

(ii) For any $x \in K$, $|x| < 1 \implies |x|_\star < 1$.

(iii) There exists $s > 0$ such that $|\cdot| = |\cdot|_\star^s$.

Proof. (i) $\implies$ (ii): For any $x \in K$ such that $|x| < 1$, we have

$$\lim_{n\to\infty} |x^n| = \lim_{n\to\infty} |x|^n = 0,$$

which implies the sequence $(x^n)_{n=1}^{\infty}$ converges to 0 in $(K, |\cdot|)$. Since $(K, |\cdot|)$ and $(K, |\cdot|_\star)$ as topological spaces are homeomorphic, the sequence $(x^n)_{n=1}^{\infty}$ also converges to 0 in $(K, |\cdot|_\star)$, which means

$$\lim_{n\to\infty} |x|_\star^n = \lim_{n\to\infty} |x^n|_\star = 0.$$

Therefore, $|x|_\star < 1$.

(ii) $\implies$ (iii): Assume condition (ii): $|x| < 1 \implies |x|_\star < 1$ for all $x \in K$. By considering the inverse x^{-1}, we also conclude that $|x| > 1 \implies |x|_\star > 1$.

Let $y \in K$ such that $|y| > 1$. For any $x \in K^\times - \{1\}$, there exists a real number $r(x)$ such that

$$|x| = |y|^{r(x)},$$

with $r(x) \neq 0$.

Consider a sequence of rational numbers $\left(\frac{m_i}{n_i}\right)_{i=1}^{\infty}$ such that $\frac{m_i}{n_i} > r(x)$, $n_i > 0$, and

$$\lim_{i\to\infty} \frac{m_i}{n_i} = r(x).$$

Then by assumption (ii), we have

$$|x| < |y|^{m_i/n_i} \implies \left|\frac{x^{n_i}}{y^{m_i}}\right| < 1 \implies \left|\frac{x^{n_i}}{y^{m_i}}\right|_\star < 1 \implies |x|_\star < |y|_\star^{m_i/n_i}.$$

Taking the limit as $i \to \infty$, we obtain

$$|x|_\star \leq |y|_\star^{r(x)}.$$

Similarly, by considering a sequence of rational numbers $\left(\frac{m_i}{n_i}\right)_{i=1}^{\infty}$ such that $\frac{m_i}{n_i} < r(x)$ and $\lim_{i\to\infty} \frac{m_i}{n_i} = r(x)$, we can show that

$$|x|_\star \geq |y|_\star^{r(x)}.$$

Thus, we conclude that

$$|x|_\star = |y|_\star^{r(x)}.$$

Taking the logarithm of both sides, we find

$$\log|x| = r(x)\log|y| \quad \text{and} \quad \log|x|_\star = r(x)\log|y|_\star.$$

Dividing these equations yields

$$\frac{\log|x|}{\log|x|_\star} = \frac{\log|y|}{\log|y|_\star}.$$

Take $t = \frac{\log|y|}{\log|y|_\star} > 0$. We conclude that for all $x \in K$, $|x| = |x|_\star^t$. This completes the proof.

(iii) $\implies$ (i): Since $|\cdot| = |\cdot|_\star^s$, we can prove that the identity map $f : (K, |\cdot|) \to (K, |\cdot|_\star)$ is a homeomorphism by checking that both f and f^{-1} are continuous. For any ϵ-ball $B_{|\cdot|_\star}(x, \epsilon)$, we have

$$f^{-1}(B_{|\cdot|_\star}(x, \epsilon)) = B_{|\cdot|}(x, \epsilon^{1/s}),$$

which is open in $(K, |\cdot|)$. Thus f is continuous. Similarly, f^{-1} is continuous. □

Definition 13.3.6 Places of a Field

Let K be a field. A **place** on K is an equivalence classes of non-trivial absolute values on K. The set of all places on a field K is denoted by $\mathtt{pl}_K$.

Definition 13.3.7 Archimedean Absolute Value

An absolute value is called **Archimedean** if the set

$$\{|n| : n \in \mathbb{Z}\}$$

is unbounded in $\mathbb{R}$ equipped with the Euclidean topology. Otherwise, it is called **non-Archimedean**.

Example 13.3.1 Absolute Value Induced by Harr Measure on Locally Compact Hausdorff Topological Field

Let K be a locally compact Hausdorff topological field. Since the additive group $(K, +)$ is a locally compact Hausdorff group, a Haar measure μ can be defined on it. Using the Haar measure, an absolute value

$$|\cdot| : a \longmapsto |a| = \frac{\mu(aX)}{\mu(X)}$$

can be defined on the field K. The topology induced by this absolute value coincides with the original topology of K.

Proposition 13.3.8 Classification of Non-discrete, Locally Compact Hausdorff Topological Fields

Let K be a non-discrete, locally compact Hausdorff topological field. There are exactly three possibilities for K:

(i) Archimedean fields: $\mathbb{R}$ and $\mathbb{C}$.

(ii) p-adic number fields: finite extensions of $\mathbb{Q}_p$. These are non-Archimedean fields of characteristic 0.

(iii) Function fields over a finite field $\mathbb{F}_q$: finite extensions of the field of formal Laurent series $\mathbb{F}_q((x))$, where $q = p^n$ is a power of a prime. These are non-Archimedean fields of characteristic p.

Definition 13.3.9 Local Field

A **local field** is a non-discrete, locally compact Hausdorff topological field.

Definition 13.3.10 Completion of a Normed Field

Let $(K, |\cdot|)$ be a normed field. The **completion** of K with respect to the absolute value $|\cdot|$ is the Cauchy completion of the metric space (K, d), where $d(x, y) = |x - y|$.

The completion of a normed field is functorial, i.e. it is a functor from the category of normed fields to the category of complete normed fields.

Definition 13.3.11 Global Field

Let K be a field. K is called a **global field** if it satisfies the following properties:

(i) the completion of K with respect to every place on K is a local field

(ii) product formula:

$$\prod_{v \in \mathtt{pl}_K} |x|_v = 1.$$

It can be proven that there are exactly two types of global fields:

(i) Number fields: finite extensions of $\mathbb{Q}$.

(ii) Function fields: finite extensions of $\mathbb{F}_q(t)$.

Definition 13.3.12 Finite Places of a Global Field

Let K be a global field. A place v on K is called **finite** if either

(i) v restricts to a p-adic place on $\mathbb{Q}$ for some prime p, or

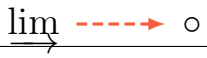
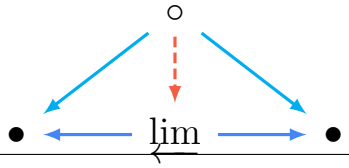
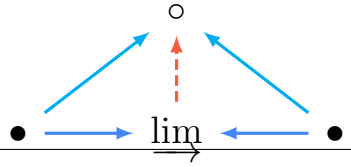
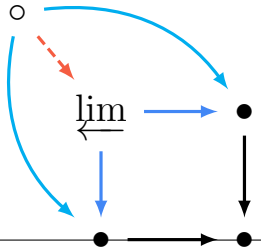
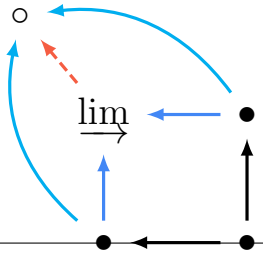
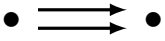
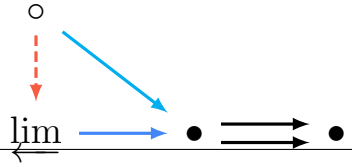
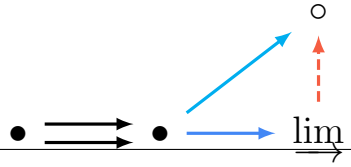
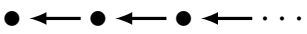
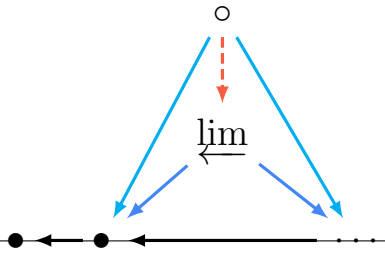
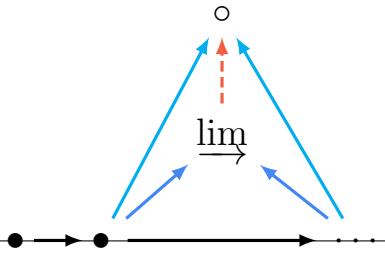
(ii) v restricts to a $p(t)$-adic place on $\mathbb{F}_q(t)$ for some prime element $p(t) \in \mathbb{F}_q[t]$.

Appendices

Appendix A

Category Theory Facts

Category	Initial Object	Terminal Object
Cat	$\mathbb{0}$	$\mathbb{1}$
Set	$\varnothing$	$\{*\}$
Top	$\varnothing$	$\{*\}$
Grp	$\{0\}$	
R-Mod	$\{0\}$	
Ring	$\mathbb{Z}$	$\{0\}$
R-Alg	R	$\{0\}$
Sch	$\operatorname{Spec}\mathbb{Z}$	$\operatorname{Spec}\{0\} = \varnothing$
Field_p	$\mathbb{Q}$ if $p = 0$ $\mathbb{F}_p$ if $p > 0$	

Diagram	Limit	Colimit
Empty Category $\varnothing$	Terminal Object 	Initial Object 
Discrete Category 	Product	Coproduct
	Finite Product 	Finite Coproduct 
	Pullback 	Pushout 
	Equalizer 	Coequalizer 
	Inverse Limit 	Direct Limit 

Index