Saurav Dwivedi

Constructive Mathematics

A handbook of definitions and theorems
Incepted. January 5, 2013

January 5, 2019

Preface

These notes originally aroused as an attempt to summarize definitions and theorems one often uses in everyday life as a practicing mathematician. Such a goal seemed vast, and I restricted the content to the definitions and theorems that I use quite often. These notes could be handy for a wide range of physicists and mathematicians.

About usage; I use distinct symbols for operations among objects, such as $\star, \oplus, \boxplus, \ldots$ for addition, $\#, \otimes, \boxtimes, \ldots$ for multiplication and $\odot, \boxdot, \circledast, \ldots$ for action of an object on other objects. The goal is to distinguish operations among objects. In practice, one just simplifies it by replacing $\star$ with $+$ and # with nothing. It should be clear from the context that an operation pertains to a distinct object.

Varanasi, Paris, January 5, 2019 *Saurav DWIVEDI*

Contents

Lists of Abbreviations

$\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$	Arbitrary sets.
$a, b, c, \ldots$	Elements of a set.
$\star, \#, \oplus, \otimes, \odot \ldots$	Binary operations on a set $\mathcal{A}$.
$e_\star, e_\#, \ldots$	Identity elements corresponding to binary operations $\star, \#, \ldots$.
$\mathbb{A}, \mathbb{B}, \mathbb{C}, \ldots$	Algebraic objects, such as group, ring, module.
$\mathbb{S}(\mathcal{A}; \star)$	A **Semigroup**, with underlying set $\mathcal{A}$, and binary operation $\star$ on it.
$\mathbb{M}(\mathcal{A}; \star; e_\star)$	A **Monoid**, with underlying set $\mathcal{A}$, binary operation $\star$ on it, and identity $e_\star$.
$\mathbb{G}(\mathcal{A}; \star; e_\star)$	A **Group**, with underlying set $\mathcal{A}$, binary operation $\star$ on it, and identity $e_\star$.
$\mathbb{R}(\mathcal{A}; \star, \#; e_\star, e_\#)$	A **Ring**, with underlying set $\mathcal{A}$, binary operations $\star, \#$ on it, and identities $e_\star, e_\#$.
$<$	Subsemigroup, submonoid, subgroup, subring, submodule, subalgebra, subcategory, ...
$\lhd$	Normal subgroup, ideal of a ring, ...
$x^i x_i = x^i x^i = x_i x_i = \sum_i x_i x_i$	Einstein's summation convention.

Part I
Algebra

Notes inspired by Basic Algebra (N. Jacobson).

Chapter 1
Sets

1.1 Set

Definition 1.1.1 (Cartesian product) ..

1.2 Map

Let $\mathcal{A}$ and $\mathcal{B}$ be sets. A map $f : \mathcal{A} \longrightarrow \mathcal{B}$ is a law that assigns to **each** element of $\mathcal{A}$ **exactly one** element of $\mathcal{B}$. For $a \in \mathcal{A}$, we write $a \mapsto f(a) \in \mathcal{B}$, and say $f(a)$ is **image** of a under map f. The **preimage** of $b \in \mathcal{B}$ is subset of those elements of $\mathcal{A}$, whose image is b, i.e., $f^{-1}(b) = \{a \in \mathcal{A} \mid b = f(a)\}$.

An **identity** map $id_{\mathcal{A}} : \mathcal{A} \longrightarrow \mathcal{A}$ identifies each element of $\mathcal{A}$ with itself: $id_{\mathcal{A}}(a) = a, \forall\, a \in \mathcal{A}$. Let $\mathcal{A} \subset \mathcal{B}$. An **inclusion** map $\iota : \mathcal{A} \hookrightarrow \mathcal{B}$ identifies every element of $\mathcal{A}$ as an element of $\mathcal{B} : \iota(a) = a \in \mathcal{B}, \forall\, a \in \mathcal{A}$.

Definition 1.2.1 (Injection) *A map $f : \mathcal{A} \longrightarrow \mathcal{B}$ is termed **injective** if $\forall\, f(a) = f(b) \Rightarrow a = b$ or equivalently $\forall\, a \neq b \Rightarrow f(a) \neq f(b)$. If $f : \mathcal{A} \longrightarrow \mathcal{B}$ is injection, every element of $\mathcal{B}$ is image of **at most** one element of $\mathcal{A}$.*

Definition 1.2.2 (Surjection) *A map $f : \mathcal{A} \longrightarrow \mathcal{B}$ is termed **surjective** if $\forall\, b \in \mathcal{B}, \exists\, a \in \mathcal{A}$ such that $b = f(a)$. Equivalently, a map $f : \mathcal{A} \longrightarrow \mathcal{B}$ is surjective if all elements of $\mathcal{B}$ have non empty preimage, i.e., $\forall\, b \in \mathcal{B}, f^{-1}(b) \neq \emptyset$. If $f : \mathcal{A} \longrightarrow \mathcal{B}$ is surjection, every element of $\mathcal{B}$ is image of **at least** one element of $\mathcal{A}$.*

Definition 1.2.3 (Bijection) *A map $f : \mathcal{A} \longrightarrow \mathcal{B}$ is **bijective** if it is both injective and surjective. A bijection is invertible, i.e., if $f : \mathcal{A} \longrightarrow \mathcal{B}$ is bijective, $\exists\, g : \mathcal{B} \longrightarrow \mathcal{A}$ such that $g \circ f = id_{\mathcal{A}}$ and $f \circ g = id_{\mathcal{B}}$. Such a map is **unique**, and called **inverse** map of f.*

Illustrations. The following law $f : \{a, b\} \longrightarrow \{x, y\}$, such that

$$f(a) = x \tag{1.1}$$
$$f(a) = y \tag{1.2}$$
$$f(b) = \emptyset \tag{1.3}$$

is **not** a mapping because b has no image and a has multiple images. The law $f : \{a, b\} \longrightarrow \{x, y\}$, defined as

$$f(a) = x \tag{1.4}$$
$$f(b) = x \tag{1.5}$$

is a map, but it is *neither* injective *nor* surjective.

If $f : \mathcal{A} \longrightarrow \mathcal{B}$ is surjective, then $Im(f) = \mathcal{B}$. Let $\{p\}$ be a singleton and $\mathcal{A}$ be a non empty set. A map $f : \{p\} \longrightarrow \mathcal{A}$ *is* injective but *not* surjective, and its image is singleton. A map $f : \mathcal{A} \longrightarrow \{p\}$ *is* surjective but *not* injective.

Identity map is *both* injective and surjective. Inclusion map *is* injective, but *not* surjective.

1.3 Relation

A relation $\mathcal{R}$ on a set $\mathcal{A}$ is a subset of $\mathcal{A} \times \mathcal{A}$. We say "$a, b \in \mathcal{A}$ have a relation if $(a, b) \in \mathcal{R}$, and write $a\mathcal{R}b$."

Definition 1.3.1 (Equivalence Relation) *An equivalence relation $\mathcal{E}$ on a set $\mathcal{A}$ is a relation such that:*

1. *$a\mathcal{E}a$ (Reflexivity),*
2. *$a\mathcal{E}b \implies b\mathcal{E}a$ (Symmetry),*
3. *$a\mathcal{E}b$ and $b\mathcal{E}c \implies a\mathcal{E}c$ (Transitivity),*

$\forall\, a, b, c \in \mathcal{A}$.

An **equivalence class** of an element $a \in \mathcal{A}$ is defined to be set of all elements of $\mathcal{A}$ equivalent to it: $[a] = \{b \in \mathcal{A} | b\mathcal{E}a\}$.

1.4 Quotient Set

Lemma 1.1 (Quotient Set). *An equivalence relation $\mathcal{E}$ on a set $\mathcal{A}$ makes a partition of $\mathcal{A}$ into equivalence classes, called **quotient set** of $\mathcal{A}$ by relation $\mathcal{E}$, denoted $\mathcal{A}/\mathcal{E}$.*

Proof. $\forall\, a \in \mathcal{A},\ [a] \subset \mathcal{A} \implies \bigcup_{a\in\mathcal{A}}[a] \subset \mathcal{A}$. Further, $\forall\, a \in \mathcal{A},\ a \in [a] \implies a \in \bigcup_{a\in\mathcal{A}}[a] \implies \mathcal{A} \subset \bigcup_{a\in\mathcal{A}}[a]$, which eventually implies $\mathcal{A} = \bigcup_{a\in\mathcal{A}}[a]$. It only remains to prove that equivalence classes are mutually **disjoint**. Now, let $a, b, c \in \mathcal{A},\ a \neq b$. Let $c \in [a] \cap [b]$. Thus $c\mathcal{E}a \implies a\mathcal{E}c \implies a \in [c] \implies [a] = [c]$. Also $c\mathcal{E}b \implies [b] = [c]$. Thus if $c \in [a] \cap [b]$, $[a] = [b] \implies a = b$, a contradiction. Therefore, $[a] \cap [b] = \varnothing$. Thus $\mathcal{E}$ partitions $\mathcal{A}$ into set of nonempty disjoint subsets of $\mathcal{A}$, called *blocks*, which are equivalence classes. □

We also use $\sim$ for $\mathcal{E}$, and $\mathcal{A}/\sim$ for $\mathcal{A}/\mathcal{E}$.

Chapter 2
Algebraic Structures on Sets

Abstract

2.1 Algebraic Objects with One Binary Operation

Definition 2.1.1 (Semigroup) *The construct* $\mathbb{S}(\mathcal{A};\star)$ *with underlying non-empty set* $\mathcal{A}$*, and associative binary operation* $\star$ *on* $\mathcal{A}$*,*

$$\star : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}, \tag{2.1}$$

forms a ***semigroup****.*

Definition 2.1.2 (Monoid) *A semigroup* $\mathbb{S}(\mathcal{A};\star)$ *with two-sided identity* $e_\star$*,*

$$a \star e_\star = e_\star \star a = a, \qquad \forall\, a \in \mathcal{A}, \tag{2.2}$$

forms a ***monoid*** $\mathbb{M}(\mathcal{A};\star;e_\star)$*.*

Chapter 3
Groups

Abstract Groups are categorical objects with one binary operation.

3.1 Group

Definition 3.1.1 (Group) *A monoid* $\mathbb{M}(\mathcal{A};\star;e_\star)$ *with two-sided inverse,*

$$a \star a^{-1} = a^{-1} \star a = e_\star\,, \qquad \forall\, a, a^{-1} \in \mathcal{A}\,, \tag{3.1}$$

*forms a **group*** $\mathbb{G}(\mathcal{A};\star;e_\star)$ *.*

One-sided identity, and one-sided inverse suffice to form a group. A group $\mathbb{G}(\mathcal{A};\star;e_\star)$ has unique identity $e_\star$.

Corollary 3.1. *A finite monoid forms a group.*

Lemma 3.1. *[Uniqueness] Let* a,b,c *be unique elements of a group* $\mathbb{G}(\mathcal{A};\star;e_\star)$ *. The binary operation of **any** two is unique,*

$$a \star b \neq a \star c\,, \qquad \forall\, a,b,c \in \mathcal{A}\,.$$

Proof. [Contradiction] Let $a,b,c,d \in \mathcal{A}$. $a \star b = c$ and $a \star d = c \implies b = d$. □

Corollary 3.2. *Let a group* $\mathbb{G}(\mathcal{A};\star;e_\star)$ *with order* $n = |\mathcal{A}|$ *, be represented by*

$$\mathcal{A} = \{e, a_2, a_3, \ldots, a_n\}\,.$$

$\mathbb{G}(\mathcal{A};\star;e_\star)$ *can alternatively be represented by*

$$\mathcal{A} = \{e \star a_i, a_2 \star a_i, a_3 \star a_i, \ldots, a_n \star a_i\}\,,\ or \tag{3.2}$$
$$\mathcal{A} = \{a_i \star e, a_i \star a_2, a_i \star a_3, \ldots, a_i \star a_n\}\,, \tag{3.3}$$

$\forall\, i \in \{1,2,3,\ldots,n\}$ *, except for order.*

Proof. Let $a_i \in \mathcal{A}$ in a group $\mathbb{G}(\mathcal{A};\star;e_\star)$. From Theorem 3.1, $a_i \star a_j$ is unique $\forall\, j \in \{1,2,3,\ldots,n\}$, and $|\mathcal{A}| = n$ is definite, implying $|\{a_i \star a_j|\ \forall\, j \in \{1,2,3,\ldots,n\}\}| = n$. $a_i \star a_j \in \mathcal{A}\ \forall\, j \in \{1,2,3,\ldots,n\} \implies \mathcal{A} = \{a_i \star a_j|\ \forall\, j \in \{1,2,3,\ldots,n\}\}$. □

3.1.1 Subgroup

Definition 3.1.2 (Subgroup) *For* $\mathcal{H} \subset \mathcal{A}$ *in* $\mathbb{G}(\mathcal{A};\star;e_\star)$ *, if* $\mathcal{H}$ *forms a group under (the same) binary operation* $\star$ *, then* $\mathbb{G}(\mathcal{H};\star;e_\star)$ *is termed **subgroup** of* $\mathbb{G}(\mathcal{A};\star;e_\star)$ *, abbreviated*

$$\mathbb{G}(\mathcal{H};\star;e_\star) < \mathbb{G}(\mathcal{A};\star;e_\star)\,.$$

3.1.2 Product Group

3.1.3 Cosets

Definition 3.1.3 (Coset) *A left [right] coset of a subgroup* $\mathbb{G}(\mathcal{H};\star;e_\star) < \mathbb{G}(\mathcal{A};\star;e_\star)$ *in* $\mathbb{G}(\mathcal{A};\star;e_\star)$ *is,*

$$\textsc{Coset}_L\left(\mathbb{G}(\mathcal{H};\star;e_\star)\right) = a \star \mathcal{H} = \{a \star h | h \in \mathcal{H}\}\,, \tag{3.4}$$

$$\textsc{Coset}_R\left(\mathbb{G}(\mathcal{H};\star;e_\star)\right) = \mathcal{H} \star a = \{h \star a | h \in \mathcal{H}\}\,. \tag{3.5}$$

Definition 3.1.4 (Conjugate) *The element* $b \star a \star b^{-1}$ *is termed* ***conjugate*** *of* $a \in \mathcal{A}$, $\forall\, b \in \mathcal{A}$ *in a group* $\mathbb{G}(\mathcal{A};\star;e_\star)$.

Definition 3.1.5 (Class) *Conjugates of* $a \in \mathcal{A}$ *form its* ***class*** *in the group* $\mathbb{G}(\mathcal{A};\star;e_\star)$.

$$\textsc{Class}\,(a) = \{b \star a \star b^{-1} |\, \forall\, b \in \mathcal{A}\}\,. \tag{3.6}$$

3.1.4 Normal (Invariant) Subgroup

Let $(\mathcal{H};\star;e_\star) < (\mathcal{G};\star;e_\star)$. We define a relation on $\mathcal{G}$ by

$$a \equiv b \ (mod\ \mathcal{H}) \tag{3.7}$$

if $a^{-1} \star b \in \mathcal{H}\ \forall\ a,b \in \mathcal{G}$. It turns out to be an equivalence relation if $(\mathcal{H};\star;e_\star)$ satisfies one of the following properties:

1. $g^{-1} \star h \star g \in \mathcal{H}, \forall\, g \in \mathcal{G}, h \in \mathcal{H}$.
2. $g \star \mathcal{H} = \mathcal{H} \star g, \forall\, g \in \mathcal{G}$.

A subgroup satisfying any of these properties is called a normal or invariant subgroup, designated as $(\mathcal{N};\star;e_\star) \lhd (\mathcal{G};\star;e_\star)$.

3.1.5 Quotient Group

Let $(\mathcal{N};\star;e_\star) \lhd (\mathcal{G};\star;e_\star)$. We define an equivalence relation on $\mathcal{G}$ by

$$a \equiv b \ (mod\ \mathcal{N}) \tag{3.8}$$

if $a^{-1} \star b \in \mathcal{N}\ \forall\ a,b \in \mathcal{G}$. The equivalence class of any element $g \in \mathcal{G}$ is give by

$$[g] = g \star \mathcal{N} = \{g \star n | n \in \mathcal{N}\}\,. \tag{3.9}$$

which is called *left* **coset** of $\mathcal{N}$ in $\mathcal{G}$. The set of all (left) cosets is the quotient set

$$\mathcal{G}/\mathcal{N} = \{g \star N | g \in \mathcal{G}\} = \{g \star n | g \in \mathcal{G}, n \in \mathcal{N}\}\,. \tag{3.10}$$

The quotient set $\mathcal{G}/\mathcal{N}$ forms a group under associative binary operation

$$\# : \mathcal{G}/\mathcal{N} \times \mathcal{G}/\mathcal{N} \longrightarrow \mathcal{G}/\mathcal{N} \tag{3.11}$$

defined by

$$(a \star \mathcal{N})\#(b \star \mathcal{N}) = (a \star b) \star \mathcal{N}\,, \tag{3.12}$$

or

$$[a]\#[b] = [a \star b]\,, \tag{3.13}$$

with identity $[e_\star]$. We observe $[e_\star] = \mathcal{N}$. Thus, $(\mathcal{G}/\mathcal{N};\#;[e_\star])$ is the **quotient** group of $(\mathcal{G};\star;e_\star)$ by $(\mathcal{N};\star;e_\star)$.

3.2 Homomorphism

Definition 3.2.1 (Homomorphism) *A map* $f : \mathcal{A} \longrightarrow \mathcal{B}$ *between groups* $\mathbb{G}(\mathcal{A};\star;e_\star)$ *and* $\mathbb{G}(\mathcal{B};\#;e_\#)$, *with binary operations*

$$\star : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}, \tag{3.14}$$

$$\# : \mathcal{B} \times \mathcal{B} \longrightarrow \mathcal{B}, \tag{3.15}$$

is ***homomorphism*** *of groups, with*

$$f(a \star b) = f(a) \# f(b) \qquad \forall\, a, b \in \mathcal{A}. \tag{3.16}$$

Chapter 4
Rings

Abstract Rings are categorical objects with two associative binary operations.

4.1 Ring

Definition 4.1.1 (Ring) *A construct $\mathbb{R}(\mathcal{A};\star,\#;e_\star,e_\#)$ with underlying non-empty set $\mathcal{A}$, associative binary operations $\star$ and $\#$ on $\mathcal{A}$,*

$$\star,\# : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}, \tag{4.1}$$

*forms a **ring**, when*

1. *$\mathbb{G}_{\mathbb{A}}(\mathcal{A};\star;e_\star)$ is a abelian group,*
2. *$\mathbb{M}(\mathcal{A};\#;e_\#)$ is a monoid, and*
3. *$\#$ is two-sided distributive over $\star$,*

$$a\#(b \star c) = (a\#b) \star (a\#c), \tag{4.2}$$
$$(a \star b)\#c = (a\#c) \star (b\#c), \tag{4.3}$$

$\forall\, a,b,c \in \mathcal{A}$.

$\mathbb{R}(\mathcal{A};\star,\#;e_\star,e_\#)$ is **abelian** ring when $\exists$ abelian monoid $\mathbb{M}_{\mathbb{A}}(\mathcal{A};\#;e_\#)$. $\mathbb{R}(\mathcal{A};\star,\#;e_\star)$ is ring without identity $e_\#$, when $\mathbb{S}(\mathcal{A}^\#;\#)$, $\mathcal{A}^\# = \{\mathcal{A}|e_\# \notin \mathcal{A}\}$, is a semigroup.

An observation in rings, of a prime relevance, is

$$\boxed{e_\star\#a = a\#e_\star = e_\star \qquad \forall\, a \in \mathcal{A}.} \tag{4.4}$$

4.1.1 Subring

Definition 4.1.2 (Subring) *Let $(\mathcal{R};\star,\#;e_\star,e_\#)$ be a ring and $\mathcal{H} \subset \mathcal{R}$. $(\mathcal{H};\star,\#;e_\star,e_\#)$ is a subring of $(\mathcal{R};\star,\#;e_\star,e_\#)$ if,*

$$(\mathcal{H};\star;e_\star) < (\mathcal{G};\star;e_\star), \tag{4.5}$$
$$(\mathcal{H};\#;e_\#) < (\mathcal{G};\#;e_\#). \tag{4.6}$$

4.1.2 Product Ring

4.1.3 Types of Rings

Definition 4.1.3 (Zero Divisor) *$a \in \mathcal{A}$ is termed left [right] zero divisor of the ring $\mathbb{R}(\mathcal{A};\star,\#;e_\star,e_\#)$, when $\exists\, b \in \mathcal{A}(b \neq e_\star)$ such that $a\#b = e_\star$ $[= b\#a]$. Both left and right zero divisor is termed* ***zero divisor*** *of the ring.*

$e_\star$ is a *trivial* zero divisor of all rings $\mathbb{R}(\mathcal{A};\star,\#;e_\star,e_\#)$ with $|\mathcal{A}| \geq 2$.

Definition 4.1.4 (Domain) *A ring with no non-trivial zero divisors is termed a* ***domain****. Let $\mathcal{A}^\star = \{\mathcal{A}|e_\star \notin \mathcal{A}\}$. The ring $\mathbb{R}(\mathcal{A};\star,\#;e_\star,e_\#)$ forms a domain, when $\mathbb{M}(\mathcal{A}^\star;\#;e_\#) < \mathbb{M}(\mathcal{A};\#;e_\#)$. This implies that, for $a,b \neq e_\star \implies a\#b \neq e_\star, \forall\, a,b \in \mathcal{A}$; there is no zero divisor in $\mathcal{A}^\star$.*

$e_\star$ is *one and only* zero divisor of a domain $\mathbb{R}_\mathbb{D}(\mathcal{A};\star,\#;e_\star,e_\#)$.

Definition 4.1.5 (Units) *The set $\mathcal{U}$ of #-invertible elements of monoid $\mathbb{M}(\mathcal{A};\#;e_\#)$ is called* ***units*** *of monoid, defined as $\mathcal{U} = \{u \in \mathcal{A}|\exists v \in \mathcal{A} : u\#v = e_\#\}$.*

A domain $\mathbb{R}_\mathbb{D}(\mathcal{A};\star,\#;e_\star,e_\#)$ with $\#-$invertible elements $u \in \mathcal{U} \subset \mathcal{A}$, is termed a domain of units $\mathbb{R}_\mathbb{D}(\mathcal{U};\star,\#;e_\star,e_\#)$ with $\mathbb{M}(\mathcal{U};\#;e_\#) < \mathbb{M}(\mathcal{A};\#;e_\#)$.

Definition 4.1.6 (Division Ring) *Let $(\mathcal{R};\star,\#;e_\star,e_\#)$ be a ring . It is a* ***division ring*** *if $\exists$ a group $(\mathcal{R}^\star;\#;e_\#)$ where $\mathcal{R}^\star = \mathcal{R} \setminus \{e_\star\}$. This implies that, for $a \in \mathcal{R}$, $e_\# \neq e_\star$, $\exists\, b \in \mathcal{R} : a\#b = e_\# = b\#a, \forall\, a,b \in \mathcal{R}$.*

All division rings are domain, but not conversely.

4.1.4 Field

Definition 4.1.7 (Field) *An* ***abelian*** *division ring is termed a* ***field****. The ring $(\mathcal{R};\star,\#;e_\star,e_\#)$ is a field, if $\exists$ a abelian group $(\mathcal{R}^\star;\#;e_\#)$, where $\mathcal{R}^\star = \mathcal{R} \setminus \{e_\star\}$. Note that $e_\star$ does not belong to a field since it has no inverse.*

4.1.5 Ideal

Definition 4.1.8 (Ideal) *Let $(\mathcal{I};\star;e_\star) < (\mathcal{R};\star;e_\star)$ be (additive) subgroup for the ring $(\mathcal{R};\star,\#;e_\star,e_\#)$. $\mathcal{I}$ is termed left [resp. right] ideal of the ring $(\mathcal{R};\star,\#;e_\star,e_\#)$, if $\forall\, a \in \mathcal{R}, i \in \mathcal{I} \implies a\#i$ $[i\#a] \in \mathcal{I}$. An ideal which is both left and right is termed* ***ideal*** *of the ring, and we write $\mathcal{I} \lhd \mathcal{R}$.*

$e_\star$ and $\mathcal{R}$ are **trivial** ideals of the ring $\mathbb{R}(\mathcal{R};\star,\#;e_\star,e_\#)$. $e_\#$ does not belong to any proper ideal.

Lemma 4.1. *If $\mathcal{I},\mathcal{J} \lhd \mathcal{R}$ then $\mathcal{I} \cup \mathcal{J}, \mathcal{I} \cap \mathcal{J}, \mathcal{I} + \mathcal{J}, \mathcal{I}\mathcal{J} \lhd \mathcal{R}$.*

Lemma 4.2. *An ideal is a subring.*

Lemma 4.3. *A* ***field*** *has* ***no*** *nontrivial ideal.*

4.1.6 Quotient Ring

Let $\mathcal{I} \subset \mathcal{R}$ be an ideal of the ring $(\mathcal{R};\star,\#;e_\star,e_\#)$. We have $(\mathcal{I};\star;e_\star) \lhd (\mathcal{R};\star;e_\star)$ (since $(\mathcal{R};\star;e_\star)$ is abelian). We define equivalence relation on $\mathcal{R}$ as

$$a \equiv b(mod\,\mathcal{I}) \tag{4.7}$$

$\forall\, a,b,c,d \in \mathcal{R}$, if

$$a \equiv b,\ c \equiv d \implies a \star c \equiv b \star d\,,\text{and } a\#c \equiv b\#d\,, \tag{4.8}$$

which is a consequence of $\mathcal{I}$ being an ideal of the ring $\mathcal{R}$. The equivalence class of $a \in \mathcal{R}$ is given by

$$[a] = a \star \mathcal{I} = \{a \star i | i \in \mathcal{I}\}\,. \tag{4.9}$$

The quotient set

$$\mathcal{R}/\mathcal{I} = \{a \star \mathcal{I} | a \in \mathcal{R}\} = \{a \star i | a \in \mathcal{R},\ i \in \mathcal{I}\}\,, \tag{4.10}$$

forms a ring under associative binary operations

$$\oplus : \mathcal{R}/\mathcal{I} \times \mathcal{R}/\mathcal{I} \longrightarrow \mathcal{R}/\mathcal{I}\,, \tag{4.11}$$
$$\otimes : \mathcal{R}/\mathcal{I} \times \mathcal{R}/\mathcal{I} \longrightarrow \mathcal{R}/\mathcal{I}\,, \tag{4.12}$$

defined by

$$[a] \oplus [b] = [a \star b]\,, \tag{4.13}$$

$$[a] \otimes [b] = [a\#b]\,, \tag{4.14}$$

or

$$(a \star \mathcal{I}) \oplus (b \star \mathcal{I}) = (a \star b) \star \mathcal{I}\,, \tag{4.15}$$

$$(a \star \mathcal{I}) \otimes (b \star \mathcal{I}) = (a\#b) \star \mathcal{I}\,, \tag{4.16}$$

with identities $[e_\star]$ and $[e_\#]$. We observe that $[e_\star] = \mathcal{I}$ and $[e_\#] = e_\# \star \mathcal{I}$. However, $(\mathcal{R}/\mathcal{I};\oplus;[e_\star])$ is quotient (abelian) group, and $(\mathcal{R}/\mathcal{I};\otimes;[e_\star])$ is monoid.

It is easily checked that $\otimes$ is (two sided) distributive over $\oplus$,

$$[a] \otimes ([b] \oplus [c]) = [a\#(b \star c)] = [(a\#b) \star (a\#c)] = [a\#b] \oplus [a\#c] = ([a] \otimes [b]) \oplus ([a] \otimes [c])\,, \tag{4.17}$$
$$([a] \oplus [b]) \otimes [c] = [(a \star b)\#c)] = [(a\#c) \star (b\#c)] = [a\#c] \oplus [b\#c] = ([a] \otimes [c]) \oplus ([b] \otimes [c])\,. \tag{4.18}$$

Thus $(\mathcal{R}/\mathcal{I};\oplus,\otimes;[e_\star],[e_\#])$ is a ring, called the quotient ring of $(\mathcal{R};\star,\#;e_\star,e_\#)$ by ideal $\mathcal{I}$.

4.1.7 Graded Ring

4.2 Homomorphism

Let $(\mathcal{A};\star,\#;e_\star,e_\#)$ and $(\mathcal{B};\oplus,\otimes;e_\oplus,e_\otimes)$ be two rings. $f : \mathcal{A} \longrightarrow \mathcal{B}$ is a homomorphism of rings if $\forall\, a,b \in \mathcal{A}$,

$$f(a \star b) = f(a) \oplus f(b)\,, \tag{4.19}$$
$$f(a\#b) = f(a) \otimes f(b)\,. \tag{4.20}$$

Lemma 4.4. *Let $f : \mathcal{A} \longrightarrow \mathcal{B}$ be a ring homomorphism. Then $ker(f)$ is an ideal in ring $\mathcal{A}$.*

Chapter 5
Modules

Abstract Modules over rings are generalization of Vector Spaces over fields.

5.1 Module

Definition 5.1.1 (Left Module) *Let* $(\mathcal{R};\star,\#;e_\star,e_\#)$ *be a ring. A* ***left*** *module over* $\mathcal{R}$ *is an abelian group* $(\mathcal{M},\oplus,e_\oplus)$ *with left ring action*

$$\odot : \mathcal{R} \times \mathcal{M} \longrightarrow \mathcal{M}\,, \tag{5.1}$$

such that $\forall\ r,s \in \mathcal{R},\ m,n \in \mathcal{M}$,

1. $r \odot (m \oplus n) = (r \odot m) \oplus (r \odot n)$,
2. $(r \star s) \odot m = (r \odot m) \oplus (s \odot m)$,
3. $(r\#s) \odot m = r \odot (s \odot m)$,
4. $e_\# \odot m = m$.

A left module is abbreviated as ${}_{\mathcal{R}}\mathcal{M}$.

Definition 5.1.2 (Right Module) *Let* $(\mathcal{R};\star,\#;e_\star,e_\#)$ *be a ring. A* ***right*** *module over* $\mathcal{R}$ *is an abelian group* $(\mathcal{M},\oplus,e_\oplus)$ *with right ring action*

$$\odot : \mathcal{M} \times \mathcal{R} \longrightarrow \mathcal{M}\,, \tag{5.2}$$

such that $\forall\ r,s \in \mathcal{R},\ m,n \in \mathcal{M}$,

1. $(m \oplus n) \odot r = (m \odot r) \oplus (n \odot r)$,
2. $m \odot (r \star s) = (m \odot r) \oplus (m \odot s)$,
3. $m \odot (r\#s) = (m \odot r) \odot s$,
4. $m \odot e_\# = m$.

A right module is abbreviated as $\mathcal{M}_{\mathcal{R}}$.

5.1.1 Submodule

Definition 5.1.3 (Submodule) *Let* $\mathcal{M}$ *be a left [resp. right] module over ring* $(\mathcal{R};\star,\#;e_\star,e_\#)$. *A subset* $\mathcal{N} \subset \mathcal{M}$ *is a left [resp. right] submodule of* $\mathcal{M}$ *if it is an abelian subgroup*

$$(\mathcal{N},\oplus,e_\oplus) < (\mathcal{M},\oplus,e_\oplus)\,, \tag{5.3}$$

and satisfies axioms of a left [resp. right] module over ring $\mathcal{R}$.

5.1.2 Product Module

Definition 5.1.4 (Product Module) *Let* $(\mathcal{M},\oplus,e_\oplus)$ *and* $(\mathcal{N},\boxplus,e_\boxplus)$ *be two left modules over ring* $\mathcal{R}$*, with left ring actions*

$$\odot : \mathcal{R}\times\mathcal{M} \longrightarrow \mathcal{M}\,, \tag{5.4}$$
$$\boxdot : \mathcal{R}\times\mathcal{N} \longrightarrow \mathcal{N}\,. \tag{5.5}$$

The product set $\mathcal{M}\times\mathcal{N}$ *is a left module* $(\mathcal{M}\times\mathcal{N},\otimes,e_\otimes)$ *over ring* $\mathcal{R}$ *with left action*

$$\circledast : \mathcal{R}\times(\mathcal{M}\times\mathcal{N}) \longrightarrow \mathcal{M}\times\mathcal{N}\,, \tag{5.6}$$

such that $\forall\, r\in\mathcal{R},\ m,m_1,m_2\in\mathcal{M},\ n,n_1,n_2\in\mathcal{N}$

$$(m_1,n_1)\otimes(m_2,n_2) = (m_1\oplus m_2, n_1\boxplus n_2)\,, \tag{5.7}$$
$$r\circledast(m,n) = (r\odot m, r\boxdot n)\,. \tag{5.8}$$

A product of right modules is seen to be a right module in similar setting.

By induction, a family of left [resp. right] modules $\{\mathcal{M}_i\}_{i\in\mathcal{I}}$ forms a left [resp. right] product module $\prod_{i\in\mathcal{I}}\mathcal{M}_i$.

5.1.3 Direct sum

Definition 5.1.5 (Direct sum of Modules) *...*

5.1.4 Finitely generated module

A $\mathcal{R}-$ module $(\mathcal{M},\oplus,e_\oplus)$ is finitely generated if there exist finitely many elements $m_1,m_2,m_3,\cdots\in\mathcal{M}$ such that $\mathcal{M}=\{(a_1\odot m_1)\oplus(a_2\odot m_2)\oplus\cdots \mid a_i\in\mathcal{R}, m_i\in\mathcal{M}\}$. We say $\mathcal{M}$ is generated by its subset $\mathcal{S}=\{m_1,m_2,m_3,\dots\}$.

5.1.5 Quotient Module

5.2 Homomorphism

Let $(\mathcal{M},\oplus,e_\oplus)$ and $(\mathcal{N},\boxplus,e_\boxplus)$ be two **left** modules over ring $\mathcal{R}$, with left ring actions

$$\odot : \mathcal{R}\times\mathcal{M} \longrightarrow \mathcal{M}\,, \tag{5.9}$$
$$\boxdot : \mathcal{R}\times\mathcal{N} \longrightarrow \mathcal{N}\,. \tag{5.10}$$

A module homomorphism $f:\mathcal{M}\longrightarrow\mathcal{N}$ is a $\mathcal{R}$-linear map such that $\forall\, m,n\in\mathcal{M}, r\in\mathcal{R}$,

$$f(m\oplus n) = f(m)\boxplus f(n)\,, \tag{5.11}$$
$$f(r\odot m) = r\boxdot f(m)\,. \tag{5.12}$$

Similarly, let $(\mathcal{M},\oplus,e_\oplus)$ and $(\mathcal{N},\boxplus,e_\boxplus)$ be two **right** modules over ring $\mathcal{R}$, with right ring actions

$$\odot : \mathcal{M}\times\mathcal{R} \longrightarrow \mathcal{M}\,, \tag{5.13}$$
$$\boxdot : \mathcal{N}\times\mathcal{R} \longrightarrow \mathcal{N}\,. \tag{5.14}$$

A module homomorphism $f:\mathcal{M}\longrightarrow\mathcal{N}$ is a $\mathcal{R}$-linear map such that $\forall\, m,n\in\mathcal{M}, r\in\mathcal{R}$,

$$f(m\oplus n) = f(m)\boxplus f(n)\,, \tag{5.15}$$
$$f(m\odot r) = f(m)\boxdot r\,. \tag{5.16}$$

5.3 Tensor product

Definition 5.3.1 (Tensor product of Modules) *...*

Chapter 6
Algebras

Abstract Algebras over rings are modules with a ring structure.

6.1 Algebra over a ring

Chapter 7
Categories

Abstract Categories are further generalization of Sets.

7.1 Category

Definition 7.1.1 (Category) *A category $\mathcal{C}$ is a quadruple $(Obj(\mathcal{C}), Hom_{\mathcal{C}}(\bullet,\bullet), \circ, Id_{\bullet})$, where*

1. $Obj(\mathcal{C}) := \{$*Class of objects* $X, Y, Z \ldots$ *such as sets, groups, rigs, modules, algebras etc.*$\}$,
2. $Hom_{\mathcal{C}}(\bullet,\bullet) := \{$*Class of sets* $Hom_{\mathcal{C}}(X,Y)$ *of morphisms of objects* $\forall\, X,Y \in Obj(\mathcal{C})\}$,
3. $\circ := \{Hom_{\mathcal{C}}(\bullet,\bullet) \times Hom_{\mathcal{C}}(\bullet,\bullet) \longrightarrow Hom_{\mathcal{C}}(\bullet,\bullet) \mid Hom_{\mathcal{C}}(X,Y) \times Hom_{\mathcal{C}}(Y,Z) = Hom_{\mathcal{C}}(X,Z), \forall\, X,Y,Z \in Obj(\mathcal{C})\}$,
4. $Id_{\bullet} := \{Id_X : X \longrightarrow X \mid Id_X$ *is identity morphism* $\forall\, X \in Obj(\mathcal{C})\}$,

such that the composition in ***associative***

$$h \circ (g \circ f) = (h \circ g) \circ f, \qquad \forall\, f \in Hom_{\mathcal{C}}(X,Y), g \in Hom_{\mathcal{C}}(Y,Z), h \in Hom_{\mathcal{C}}(Z,W), \tag{7.1}$$

and identity morphisms satisfy

$$Id_Y \circ f = f = f \circ Id_X, \qquad \forall\, f \in Hom_{\mathcal{C}}(X,Y), \qquad \forall\, X,Y \in Obj(\mathcal{C}). \tag{7.2}$$

7.1.1 Subcategory

7.1.2 Product Category

7.2 Functor

Definition 7.2.1 (Functor)

7.2.1 Natural Transformations

7.2.2 Functor Category

7.3 Coproduct and Product

7.4 Additive and Abelian Categories

Chapter 8
Homological Algebra

Chapter 9
Representation Theory

Abstract Based on Serre's classic.

9.1 Linear Representations of Finite Groups

Let $\mathcal{V} : \mathbb{M}^n \longrightarrow \mathbb{K}$ be $n-$dimensional vector space over a manifold $\mathbb{M}^n$, with basis $\{\vec{e}_i\}$. Linear

$$l : \mathcal{V} \longrightarrow \mathcal{V}\,, \tag{9.1}$$

maps vector to vector,

$$l(\vec{u}) = \vec{v}\,, \qquad l(u^i\vec{e}_i) = u^i l(\vec{e}_i) = v^j\vec{e}_j\,, \qquad i,j \in [1,n]\,, \tag{9.2}$$

Or

$$l(\vec{e}_i) = \frac{v^j}{u^i}\vec{e}_j = w_i^j\vec{e}_j\,, \qquad u^i, v^j, w_i^j \in \mathbb{K}\,. \tag{9.3}$$

Being a *bijection*, l entails *unique* $\{w^j\}$ for each $\vec{e}_i$. Thus, l generates square $n \times n$ matrix $\{w_i^j\}$ for the whole basis $\{\vec{e}_i\}$.

The bijections $l \in \mathcal{L}$ form a group $\mathbb{GL}(\mathcal{L};\otimes;\mathbb{I})$ of square (non singular) matrices under matrix multiplication, termed *general linear group*. The binary operation $\otimes : \mathcal{L} \times \mathcal{L} \rightarrow \mathcal{L}$ is defined as,

$$l(\vec{e}_i) \otimes l(\vec{e}_j) = w_i^k w_j^l \vec{e}_k \otimes \vec{e}_l = w_i^k w_j^l \delta_{kl} = w_i^k w_j^k = \lambda_{ij} \in \mathbb{K}\,. \tag{9.4}$$

Definition 9.1.1 (Linear Representation) *Let $\mathbb{G}(\mathcal{A};\star;e_\star)$ be an arbitrary group. The homomorphism*

$$\rho : \mathcal{A} \longrightarrow \mathcal{L}\,, \qquad \rho(a_1 \star a_2) = \rho(a_1) \otimes \rho(a_2) = l_1 \otimes l_2 \in \mathcal{L}\,, \tag{9.5}$$

turns elements of the group into square matrices. ρ is termed linear representation of $\mathbb{G}(\mathcal{A};\star;e_\star)$ in $\mathcal{V}$ of degree n, and vector space $\mathcal{V}$ is termed representation space of $\mathbb{G}(\mathcal{A};\star;e_\star)$.

Part II
Topology

Based on General Topology, Bourbaki, N.

Chapter 10
Homeomorphism

Part III
Geometry

Based on Nakahara's classic text.

Chapter 11
Differential Geometry

Abstract Vectors are multilinear objects over a manifold $\mathbb{M}^n$. Tensors are multilinear objects from product vector spaces and product one forms to an arbitrary field $\mathbb{K}$.

11.1 Vector Space

Definition 11.1.1 (Vector Space) *A vector $\vec{v} \in \vec{\mathcal{V}}$ over a manifold $\mathbb{M}^n$ is a multilinear from $\mathbb{M}^n$ to an arbitrary field $\mathbb{K}$,*

$$\vec{v} : \mathbb{M}^n \longrightarrow \mathbb{K} . \tag{11.1}$$

Any vector can be expanded into linear combination of basis vectors $\{\vec{e}_\mu\}$,

$$\vec{v} = v^\mu \vec{e}_\mu , \qquad (\textit{sum over } \mu) , \tag{11.2}$$

where $v^\mu \in \mathbb{K}$ are termed components of the vector $\vec{v}$ for the basis $\{\vec{e}_\mu\}$.

In the context of physics, each reference frame has its own basis.

11.2 One Form/Dual Vector Space

Theorem 11.1 (One Form). *The set of linears from $\vec{\mathcal{V}}$ to an arbitrary field $\mathbb{K}$,*

$$\widetilde{\mathcal{V}} : \vec{\mathcal{V}} \longrightarrow \mathbb{K} , \tag{11.3}$$

form a vector space with basis $\{\widetilde{\omega}^\nu\}$.

Proof. Let $\widetilde{\mathcal{V}} : \vec{\mathcal{V}} \longrightarrow \mathbb{K}$ be a vector space with basis $\{\widetilde{\omega}^\nu\}$. An arbitrary vector $\widetilde{v} \in \widetilde{\mathcal{V}}$ can be expanded to,

$$\widetilde{v}(\vec{u}) = v_\nu \widetilde{\omega}^\nu(\vec{u}) , \qquad \forall\, \vec{u} \in \vec{\mathcal{V}} ,\ v_\nu \in \mathbb{K} . \tag{11.4}$$

For a trivial case $\vec{u} = \vec{e}_\mu$, we have $\widetilde{v}(\vec{e}_\mu) = v_\nu \widetilde{\omega}^\nu(\vec{e}_\mu)$. Our choice

$$\widetilde{\omega}^\nu(\vec{e}_\mu) = \delta^\nu_\mu , \tag{11.5}$$

makes $\widetilde{v}(\vec{e}_\mu) = v_\nu \delta^\nu_\mu = v_\mu \in \mathbb{K}$. For vector space $\vec{\mathcal{V}}$ with basis $\{\vec{e}_\mu\}$, our *choice* $\widetilde{\omega}^\nu(\vec{e}_\mu) = \delta^\nu_\mu$ makes $\widetilde{\mathcal{V}} : \vec{\mathcal{V}} \longrightarrow \mathbb{K}$ to be a vector space with basis $\{\widetilde{\omega}^\nu\}$. □

The vector space $\widetilde{\mathcal{V}}$ is termed **one form**, and is *dual* to vector space $\vec{\mathcal{V}}$. It turns out that $\widetilde{\mathcal{V}} \cong \vec{\mathcal{V}}$ and $dim(\widetilde{\mathcal{V}}) = n = dim(\vec{\mathcal{V}})$.

11.3 Tensor

Definition 11.3.1 (Tensor of type $(0,q)$) *A tensor $t \in \mathcal{T}_q^0$ of type $(0,q)$ is a multilinear from product vector spaces to an arbitrary field $\mathbb{K}$,*

$$\mathcal{T}_q^0 : \overset{q}{\otimes} \vec{\mathcal{V}} \longrightarrow \mathbb{K}. \tag{11.6}$$

Definition 11.3.2 (Tensor of type $(p,0)$) *A tensor $t \in \mathcal{T}_0^p$ of type $(p,0)$ is a multilinear from product one forms to an arbitrary field $\mathbb{K}$,*

$$\mathcal{T}_0^p : \overset{p}{\otimes} \widetilde{\mathcal{V}} \longrightarrow \mathbb{K}. \tag{11.7}$$

Definition 11.3.3 (Tensor of type (p,q)) *A tensor $t \in \mathcal{T}_q^p$ of type (p,q) is a multilinear from product vector spaces and product one forms to an arbitrary field $\mathbb{K}$,*

$$\mathcal{T}_q^p : \overset{p}{\otimes} \widetilde{\mathcal{V}} \overset{q}{\otimes} \vec{\mathcal{V}} \longrightarrow \mathbb{K}. \tag{11.8}$$

11.3.1 Homomorphism

Let a $(0,2)$ type tensor

$$t_2^0 : \vec{\mathcal{V}} \otimes \vec{\mathcal{V}} \longrightarrow \mathbb{K} \tag{11.9}$$

be a homomorphism,

$$t(\vec{u},\vec{v}) = t(\vec{u}) \otimes t(\vec{v}), \qquad \forall\, \vec{u},\vec{v} \in \vec{\mathcal{V}}, \&\, t(\vec{u}),t(\vec{v}) \in \mathbb{K}. \tag{11.10}$$

The homomorphism allows a $(0,2)$ type tensor to decompose into two $(0,1)$ type tensors,

$$t_{(0,2)} \equiv t_{(0,1)} \otimes t_{(0,1)}. \tag{11.11}$$

Generalizing further, a $(0,q)$ type tensor decomposes into q $(0,1)$ type tensors,

$$t_{(0,q)} = \overset{q}{\otimes} t_{(0,1)}. \tag{11.12}$$

A tensor of type $(0,1)$ is a one form $t : \vec{\mathcal{V}} \longrightarrow \mathbb{K}$, expanded as

$$t_{(0,1)} = t_\mu \widetilde{\omega}^\mu, \tag{11.13}$$

for basis $\{\widetilde{\omega}^\mu\}$. A tensor of type $(0,2)$, $t : \vec{\mathcal{V}} \otimes \vec{\mathcal{V}} \longrightarrow \mathbb{K}$, decomposes as

$$t_{(0,2)} = t_{(0,1)} \otimes t_{(0,1)} = t_\mu \widetilde{\omega}^\mu \otimes t_\nu \widetilde{\omega}^\nu = t_{\mu\nu} \widetilde{\omega}^\mu \otimes \widetilde{\omega}^\nu, \tag{11.14}$$

where $t_{\mu\nu} = t_\mu t_\nu, \forall\, t_\mu, t_\nu \in \mathbb{K}$. Generalizing further, A tensor of type $(0,q)$ decomposes as

$$t_{(0,q)} = t_{\mu_1\mu_2\ldots\mu_q} \overset{q}{\underset{i=1}{\otimes}} \widetilde{\omega}^{\mu_i}. \tag{11.15}$$

where $t_{\mu_1\mu_2\ldots\mu_q} = t_{\mu_1} t_{\mu_2} \ldots t_{\mu_q}, \forall\, t_{\mu_1}, t_{\mu_2} \ldots t_{\mu_q} \in \mathbb{K}$.

11.3.2 Raising/Lowering

DO: `... Heuristic!`

DO: `... Heuristic!`

Chapter 12
Algebraic Geometry

12.1 Some Commutative Algebra

Definition 12.1.1 (Commutative Ring) *Let $(\mathcal{R};\star,\#;e_\star,e_\#)$ be a ring. It is called a **commutative** ring if $(\mathcal{R},\#,e_\#)$ is commutative monoid.*

Definition 12.1.2 (Integral Domain) *A commutative domain is termed **integral domain**.*

Definition 12.1.3 (Principal Ideal) *An ideal generated by one element of the ring is termed **principal** ideal. For $a \in \mathcal{R}$, principal ideal generated by a is $(a) = a\#\mathcal{R} = \{a\#r \mid \forall\ r \in \mathcal{R}\}$. Note that $a \in (a)$.*

Definition 12.1.4 (Ideal generated by a set) *Let $\mathcal{R}$ be a ring, and $\mathcal{S} \subset \mathcal{R}$ with $\mathcal{S} = \{a_1, a_2, a_3, \dots\}$. The ideal generated by set $\mathcal{S}$ is $(\mathcal{S}) = (a_1, a_2, \dots) = \sum_{i\in\mathcal{I}}(a_i) = \{\sum_{i\in\mathcal{I}} a_i\#r_i \mid a_i \in \mathcal{S}, r_i \in \mathcal{R}\}$. An ideal is termed finitely generated if it is generated by a finite set.*

Definition 12.1.5 (Prime Ideal) *Let $\mathcal{R}$ be a ring and $a,b,c \in \mathcal{R}$. a is a **prime** if $a|b\#c \implies a|b$ or $a|c$. We observe that if $b\#c \in (a)$ then $a|b\#c$. Since a is prime, $a|b$ or $a|c$ which implies that $b \in (a)$ or $c \in (a)$. An ideal $\mathcal{I} \lhd \mathcal{R}$ is termed **prime** if $\forall\ r,s \in \mathcal{R}$, $r\#s \in \mathcal{I} \Rightarrow r \in \mathcal{I}$ or $s \in \mathcal{I}$. Such an ideal is generated by a prime element.*

Lemma 12.1. *Every principal ideal is prime.*

Lemma 12.2. *Every maximal ideal is prime.*

Lemma 12.3. *$\mathcal{I} \lhd \mathcal{R}$ is a **prime** ideal iff $\mathcal{R}/\mathcal{I}$ is an **integral domain**.*

Lemma 12.4. *A field has no nontrivial ideal.*

Lemma 12.5. *$\mathcal{I} \lhd \mathcal{R}$ is a **maximal** ideal iff $\mathcal{R}/\mathcal{I}$ has no nontrivial ideal, and so is a **field**.*

Definition 12.1.6 (Principal Ideal Domain (PID)) *A domain is termed PID if every ideal in it is principal.*

Lemma 12.6. *The ring of polynomials $k[x_1, x_2, x_3, \dots]$ over a **field** k is a PID.*

Definition 12.1.7 (Unique Factorization Domain (UFD)) *A UFD/factorial/Gaußian domain is an integral domain such that every element can be factored into irreducible elements upto reordering or factors with units.*

Definition 12.1.8 (Ascending chain condition) *A ring $\mathcal{R}$ entails ascending chain condition on principal ideals if every sequence of principal ideals terminates somewhere: $(a_1) \subsetneqq (a_2) \subsetneqq (a_3) \subsetneqq \cdots \subsetneqq (a_n) = (a_{n+1})$ for some large $n \in \mathbb{Z}$, $\forall\ a_i \in \mathcal{R}$.*

Lemma 12.7. *Ascending chain condition on ring $\mathcal{R} \iff \mathcal{R}$ is factorial.*

Lemma 12.8. *Every PID is UFD.*

Definition 12.1.9 (Nötherian Ring) *A ring is termed **Nötherian** if it entails following equivalent conditions on its ideals,*

1. *Every ideal is finitely generated,*
2. *Every ascending chain of ideals terminates somewhere,*
3. *Every collection of ideals has a maximal ideal,*
4. *It is factorial.*

12.2 Local Rings

Definition 12.2.1 (Local Ring) *A ring $\mathcal{R}$ is termed **local** if it contains a **unique** maximal ideal $\mathcal{I}$, and we write $(\mathcal{R},\mathcal{I})$ for a local ring.*

Lemma 12.9. *If $(\mathcal{R},\mathcal{I})$ is a local ring, $\mathcal{R} \setminus \mathcal{I} = \mathcal{U}$ is set of units.*

Lemma 12.10 (Nakayama). *Let $(\mathcal{R},\mathcal{I})$ be a local ring. Let $\mathcal{M}$ be finitely generated $\mathcal{R}-$module. Then $\mathcal{M} = \mathcal{I}\mathcal{M} \Longrightarrow \mathcal{M} = e_{\oplus}$.*

Lemma 12.11. *If $(\mathcal{R},\mathcal{I})$ is Nötherian local ring, then $\mathcal{I}$ is finitely generated $\mathcal{R}-$module.*

Definition 12.2.2 (Integral dependence) *Let $\mathcal{S} < \mathcal{R}$ be a subring. $r \in \mathcal{R}$ is **integral** over $\mathcal{S}$ if it is root of a monic polynomial with coefficients in $\mathcal{S}$, i.e., if $r^n \star a_1 \# r^{n-1} \star \ldots \star a_n = e_*$,* $\quad \forall\, a_i \in \mathcal{S}$.

Definition 12.2.3 (Algebraic dependence) *Let k be a field and $\mathcal{A}$ be a $k-$algebra. Elements $a_1, a_2, \dots \in \mathcal{A}$ are **algebraically dependent** over k if $\exists\, f \in k[x_1, x_2, \dots]$ such that $f(a_1, a_2, \dots) = 0$.*

12.3 Algebraic Sets and Varieties

12.4 Schemes

Chapter 13
Complex Geometry

13.1 Complex Numbers

Define $\mathbb{I} := i\#\mathbb{R}$ with $i^2 = -1$, and call it set of *imaginary* numbers.

Lemma 13.1. *$\mathbb{I}$ is a $\mathbb{R}-$module.*

Definition 13.1.1 (Complex Number Field $\mathbb{C}$) *The $\mathbb{R}-$module defined as the direct sum $\mathbb{C} := \mathbb{R} \oplus \mathbb{I}$ is a **field**, called field of complex numbers. A complex number is explicitly written as $z = x + iy$, $\forall\ x, y \in \mathbb{R}$. x and y are termed **real** and **imaginary** parts of z .*

Definition 13.1.2 (Equality Principle) *Two complex numbers $z = x + iy$ and $z' = x' + iy'$ are equal iff $x = x'$ and $y = y'$.*

Chapter 14
Geometric Algebra

Geometric algebra is algebra constructed from geometric operations.

Thesis 1 (Euclid) *Magnitude (or measure) is a line segment.*

Thesis 2 (Descartes) *A line segment corresponds to a unique number.*

Thesis 3 (Graßmann) *A line segment possesses unique number and unique direction.*

Definition 14.0.1 (Scalar, Descartes) *A scalar is equivalence class of line segments that are congruent modulo translation and/or rotation.*

Definition 14.0.2 (Vector, Graßmann) *A vector is equivalence class of (directed) line segments that are congruent modulo translation.*

Definition 14.0.3 (Inner Product) *The dilatation of perpendicular projection of vector $\vec{a}$ onto vector $\vec{b}$ by the magnitude of $\vec{b}$ is termed inner product of $\vec{a}$ with $\vec{b}$, abbreviated $\vec{a} \bullet \vec{b}$.*

Definition 14.0.4 (Outer Product) *The oriented plane segment obtained by sweeping vector $\vec{a}$ along vector $\vec{b}$ is termed outer product of $\vec{a}$ with $\vec{b}$, abbreviated $\vec{a} \wedge \vec{b}$, and termed bivector.*

Definition 14.0.5 (k-Vector) *The outer product $\vec{a} \wedge \vec{b} \wedge \vec{c} \ldots$ of k-vectors corresponds to oriented space segment, termed k-vector or k-blade.*

A (generic) binary operation (or product) of two elements decomposes into *symmetric* and *anti-symmetric* parts,

$$A * B = \frac{1}{2}(A * B + B * A) + \frac{1}{2}(A * B - B * A) := \frac{1}{2}\{A, B\} + \frac{1}{2}[A, B] \tag{14.1}$$

However, the outer product has alternate symmetry: bivector is anti-symmetric, trivector is symmetric, 4-vector is anti-symmetric and so on. Thus, it is not a generic product. Adding a term with opposite symmetry, it becomes a generic product.

Definition 14.0.6 (Geometric Product) DO: … *Finish this section.*

14.1 Operational Geometry

Definition 14.1.1 (Spinor)

DO: `... Heuristic!`