

# Notes on Mathematics

David K. Zhang

Last modified January 16, 2022

# List of Definitions

Empty Set, $\emptyset$ . . . . .	1
Subset, $A \subseteq B$ . . . . .	1
Superset, $A \supseteq B$ . . . . .	1
Set Equality, $A = B$ , $A \neq B$ . . . . .	1
Proper Subset, $A \subsetneq B$ . . . . .	1
Proper Superset, $A \supsetneq B$ . . . . .	1
Power Set, $\mathcal{P}(A)$ , $2^A$ . . . . .	1
Cartesian Product, $A \times B$ . . . . .	2
Relation, Binary Relation, Relates, $a R b$ , $a \not R b$ . . . . .	2
Function, Maps, Domain, Codomain, $f : A \rightarrow B$ , $f(x)$ . . . . .	2
Injective Function, One-to-one Function, Injection, $f : A \hookrightarrow B$ . . . . .	2
Surjective Function, Onto Function, Surjection, $f : A \twoheadrightarrow B$ . . . . .	2
Bijjective Function, One-to-one Correspondence, Bijection, $f : A \xleftrightarrow{\sim} B$ . . . . .	3
Image, $f[S]$ . . . . .	3
Inverse Image, Preimage, $f^{-1}[S]$ . . . . .	3
Range . . . . .	3
Identity Function, $\text{id}_A$ . . . . .	3
Cartesian Product, $\prod_{i \in I} A_i$ . . . . .	3
Topology . . . . .	5
Metric, Distance Function . . . . .	5
Metric Space, Underlying Set, Point . . . . .	5
Continuity . . . . .	5
Neighborhood . . . . .	5
Group . . . . .	6
Abelian Group . . . . .	6
Rng . . . . .	7
Zero Rng, Trivial Rng . . . . .	8
Nonzero Rng, Nontrivial Rng . . . . .	8
Ring . . . . .	8
Commutative Ring . . . . .	8

# List of Theorems

Multiplying by Zero Yields Zero . . . . .	7
---	---

# Chapter 1

## Set Theory

### Definition: Empty Set, $\emptyset$

The *empty set*, denoted by  $\emptyset$ , is the set that contains no elements at all.

In other words,  $x \notin \emptyset$  for all  $x$ .

### Definition: Subset, $A \subseteq B$

Let  $A$  and  $B$  be sets. We say that  $A$  is a *subset* of  $B$ , denoted by  $A \subseteq B$ , if every element of  $A$  is also an element of  $B$ , i.e., for all  $x \in A$  we have  $x \in B$ .

### Definition: Superset, $A \supseteq B$

Let  $A$  and  $B$  be sets. We say that  $A$  is a *superset* of  $B$ , denoted by  $A \supseteq B$ , if  $B$  is a subset of  $A$ .

Note that the empty set is a subset of every set, and that every set is a superset of the empty set.

### Definition: Set Equality, $A = B$ , $A \neq B$

Let  $A$  and  $B$  be sets. We say that  $A$  and  $B$  are *equal*, denoted by  $A = B$ , if  $A \subseteq B$  and  $B \subseteq A$ . If this is not the case, then we write  $A \neq B$  to denote that  $A$  and  $B$  are not equal.

### Definition: Proper Subset, $A \subsetneq B$

Let  $A$  and  $B$  be sets. We say that  $A$  is a *proper subset* of  $B$ , denoted by  $\subsetneq$ , if  $A \subseteq B$  and  $A \neq B$ .

### Definition: Proper Superset, $A \supsetneq B$

Let  $A$  and  $B$  be sets. We say that  $A$  is a *proper superset* of  $B$ , denoted by  $\supsetneq$ , if  $A \supseteq B$  and  $A \neq B$ .

**Definition: Power Set,  $\mathcal{P}(A)$ ,  $2^A$** 

Let  $A$  be a set. The **power set** of  $A$ , denoted by  $\mathcal{P}(A)$  or  $2^A$ , is the set containing all subsets of  $A$ .

Note that  $\mathcal{P}(A)$  contains both the empty set  $\emptyset$  and the set  $A$  itself.

**Definition: Cartesian Product,  $A \times B$** 

Let  $A$  and  $B$  be sets. The **Cartesian product** of  $A$  and  $B$ , denoted by  $A \times B$ , is the set of all ordered pairs  $(a, b)$  consisting of an element  $a \in A$  followed by an element  $b \in B$ .

$$A \times B := \{(a, b) : a \in A \text{ and } b \in B\}$$

**Definition: Relation, Binary Relation, Relates,  $a R b$ ,  $a \not R b$** 

Let  $A$  and  $B$  be sets. A **relation** between  $A$  and  $B$ , also known as a **binary relation** between  $A$  and  $B$ , is a subset  $R \subseteq A \times B$  of their Cartesian product.

Given  $a \in A$  and  $b \in B$ , we write  $a R b$  to denote that  $(a, b) \in R$ . If this is the case, then we say that  $R$  **relates**  $a$  to  $b$ . Similarly, we write  $a \not R b$  to denote that  $(a, b) \notin R$ .

If  $A = B$ , then instead of saying that  $R$  is a relation *between*  $A$  and  $A$ , we simply say that  $R$  is a binary relation *on*  $A$ .

For example, the less-than relation  $<$  is a binary relation on the set  $\mathbb{N}$  of natural numbers. We write  $3 < 4$  to indicate that the ordered pair  $(3, 4) \in \mathbb{N} \times \mathbb{N}$  is an element of the relation  $<$ .

**Definition: Function, Maps, Domain, Codomain,  $f : A \rightarrow B$ ,  $f(x)$** 

Let  $A$  and  $B$  be sets. A **function** from  $A$  to  $B$  is a binary relation  $f \subseteq A \times B$  between  $A$  and  $B$  that has the following property: for each  $x \in A$ , there exists a unique  $y \in B$  such that  $x f y$ . Instead of the word “relates,” we say that the function  $f$  **maps**  $x$  to  $y$ . We call the set  $A$  the **domain** of  $f$ , and we call  $B$  the **codomain** of  $f$ .

We write  $f : A \rightarrow B$  to denote that  $f$  is a function from  $A$  to  $B$ , and given  $x \in A$ , we write  $f(x)$  to denote the unique element of  $B$  that is related to  $x$  by  $f$ .

**Definition: Injective Function, One-to-one Function, Injection,  $f : A \hookrightarrow B$** 

Let  $A$  and  $B$  be sets. A function  $f : A \rightarrow B$  is **injective**, or **one-to-one**, or an **injection**, if no two distinct elements of  $A$  are mapped to the same element of  $B$  by  $f$ .

$$\forall x, y \in A : x \neq y \implies f(x) \neq f(y)$$

We write  $f : A \hookrightarrow B$  to denote that  $f$  is an injective function from  $A$  to  $B$ .

**Definition: Surjective Function, Onto Function, Surjection,  $f : A \twoheadrightarrow B$** 

Let  $A$  and  $B$  be sets. A function  $f : A \rightarrow B$  is **surjective**, or **onto**, or a **surjection**, if every element of  $B$  is mapped to by  $f$ .

$$\forall y \in B \exists x \in A : f(x) = y$$

We write  $f : A \twoheadrightarrow B$  to denote that  $f$  is a surjective function from  $A$  to  $B$ .

**Definition: Bijective Function, One-to-one Correspondence, Bijection,  $f : A \xleftrightarrow{\sim} B$** 

Let  $A$  and  $B$  be sets. A function  $f : A \rightarrow B$  is **bijective**, or a **one-to-one correspondence**, or a **bijection**, if  $f$  is both injective and surjective. We write  $f : A \xleftrightarrow{\sim} B$  to denote that  $f$  is a bijective function from  $A$  to  $B$ .

**Definition: Image,  $f[S]$** 

Let  $A$  and  $B$  be sets. Given a function  $f : A \rightarrow B$ , the **image** of a subset  $S \subseteq A$  under  $f$ , denoted by  $f[S]$ , is the set defined by

$$f[S] := \{f(x) : x \in S\}.$$

In other words,  $f[S]$  is the subset of  $B$  containing all elements that  $f$  maps to from  $S$ . For example, consider the function  $f : \mathbb{R} \rightarrow \mathbb{R}$  defined by  $f(x) := x^2$ . The image of the interval  $(-1, 1)$  under  $f$  is the interval  $f[(-1, 1)] = [0, 1)$ .

**Definition: Inverse Image, Preimage,  $f^{-1}[S]$** 

Let  $A$  and  $B$  be sets. Given a function  $f : A \rightarrow B$ , the **inverse image** or **preimage** of a subset  $S \subseteq B$  under  $f$ , denoted by  $f^{-1}[S]$ , is the set defined by

$$f^{-1}[S] := \{x \in A : f(x) \in S\}.$$

In other words,  $f^{-1}[S]$  is the subset of  $A$  containing all elements that map into  $S$  under  $f$ . For example, consider the function  $f : \mathbb{R} \rightarrow \mathbb{R}$  defined by  $f(x) := x^2$ . The inverse image of the interval  $(1, 4)$  is the union of the two intervals  $f^{-1}[(1, 4)] = (-2, -1) \cup (1, 2)$ .

**Definition: Range**

Let  $A$  and  $B$  be sets. The **range** of a function  $f : A \rightarrow B$  is the image  $f[A]$  of  $A$  under  $f$ .

Note that a function is surjective if and only if its range equals its codomain.

**Definition: Identity Function,  $\text{id}_A$** 

Let  $A$  be a set. The **identity function** on  $A$  is the function  $\text{id}_A : A \rightarrow A$  defined by  $\text{id}_A(a) := a$  for all  $a \in A$ .

**Definition: Cartesian Product,  $\prod_{i \in I} A_i$** 

Let  $I$  be an index set, and let  $\{A_i\}_{i \in I}$  be an indexed family of sets. The ***Cartesian product*** of  $\{A_i\}_{i \in I}$ , denoted by  $\prod_{i \in I} A_i$ , is the set of all functions  $f : I \rightarrow \bigcup_{i \in I} A_i$  such that  $f(i) \in A_i$  for all  $i \in I$ .

$$\prod_{i \in I} A_i := \left\{ f : I \rightarrow \bigcup_{i \in I} A_i \mid \forall i \in I : f(i) \in A_i \right\}$$

# Chapter 2

## Topology

### Definition: Topology

Let  $X$  be a set. A **topology** on  $X$  is a collection  $T \subseteq \mathcal{P}(X)$  of subsets of  $X$

### Definition: Metric, Distance Function

Let  $X$  be a set. A **metric** on  $X$ , also known as a **distance function** on  $X$ , is a function  $d : X \times X \rightarrow \mathbb{R}$  that satisfies the following requirements:

- **Positive-definiteness:**  $d(x, y) \geq 0$  for all  $x, y \in X$ , and  $d(x, y) = 0$  if and only if  $x = y$ .
- **Symmetry:**  $d(x, y) = d(y, x)$  for all  $x, y \in X$ .
- **Triangle inequality:**  $d(x, z) \leq d(x, y) + d(y, z)$  for all  $x, y, z \in X$ .

### Definition: Metric Space, Underlying Set, Point

A **metric space** is an ordered pair  $(X, d)$  consisting of a set  $X$ , called the **underlying set** of the metric space, and a metric  $d$  on  $X$ . The elements of  $X$  are called the **points** of the metric space  $(X, d)$ .

### Definition: Continuity

Let  $(X, d_X)$  and  $(Y, d_Y)$  be metric spaces. A function  $f : X \rightarrow Y$  is **continuous** at a point  $x_0 \in X$  if, for every  $\epsilon > 0$ , there exists  $\delta > 0$ , such that for all  $x \in X$ , if  $d_X(x, x_0) < \delta$ , then  $d_Y(f(x), f(x_0)) < \epsilon$ .

### Definition: Neighborhood

Let  $(X, T)$  be a topological space, and let  $x \in X$ . A subset  $A \subseteq X$  is a **neighborhood** of  $x$  if there exists an open set  $U \in T$  such that  $x \in U$  and  $U \subseteq A$ .



# Chapter 3

## Group Theory

### Definition: Group

A **group** is an algebraic structure  $\langle G; 1, ^{-1}, \cdot \rangle$  consisting of:

- a set  $G$ , called the **underlying set**;
- a distinguished element  $1 \in G$ , called the **identity element**;
- a unary operation  $^{-1} : G \rightarrow G$ , written as  $x \mapsto x^{-1}$ , called **inversion**;
- a binary operation  $\cdot : G \times G \rightarrow G$ , written as  $(x, y) \mapsto x \cdot y$ , called the **group operation** or **group product**;

satisfying the following requirements:

- **Associative property**:  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$  for all  $x, y, z \in G$ .
- **Identity property**:  $1 \cdot x = x \cdot 1 = x$  for all  $x \in G$ .
- **Inverse property**:  $x \cdot x^{-1} = x^{-1} \cdot x = 1$  for all  $x \in G$ .

### Definition: Abelian Group

An **abelian group** is a group  $\langle G; 1, ^{-1}, \cdot \rangle$  that satisfies the following additional requirement:

- **Commutative property**:  $x \cdot y = y \cdot x$  for all  $x, y \in G$ .

# Chapter 4

## Ring Theory

In this chapter, we introduce a new class of algebraic structures, called rngs and rings, whose study is collectively called **ring theory**. Rngs and rings are more complicated than groups because their definition involves not one, but two binary operations.

### Definition: Rng

A **rng** (pronounced as “*rung*”) is an algebraic structure  $\langle R; 0, -, +, \cdot \rangle$  consisting of:

- a set  $R$ , called the **underlying set**;
- a distinguished element  $0 \in R$ , called the **zero element**;
- a unary operation  $- : R \rightarrow R$ , written as  $x \mapsto -x$ , called **negation**;
- a binary operation  $+ : R \times R \rightarrow R$ , written as  $(x, y) \mapsto x + y$ , called **addition**;
- a binary operation  $\cdot : R \times R \rightarrow R$ , written as  $(x, y) \mapsto x \cdot y$ , called **multiplication**;

satisfying the following requirements:

- **Additive structure**:  $\langle R; 0, -, + \rangle$  is an abelian group.
- **Associativity**:  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$  for all  $x, y, z \in R$ .
- **Left distributivity**:  $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$  for all  $x, y, z \in R$ .
- **Right distributivity**:  $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$  for all  $x, y, z \in R$ .

The key ingredient in the definition of a rng is **distributivity**, which establishes a link between two different binary operations. We begin our study of rngs by proving a simple (but important) result to demonstrate the utility of the distributive property.

### Multiplying by Zero Yields Zero

**Theorem:** Let  $\langle R; 0, -, +, \cdot \rangle$  be a rng. For any  $x \in R$ , we have  $0 \cdot x = x \cdot 0 = 0$ .

*Proof:* Let  $x \in R$  be given. Because  $0$  is the identity element of the abelian group  $\langle R; 0, -, + \rangle$ , we have  $0 = 0 + 0$ . Using left distributivity, it follows that  $0 \cdot x = (0 + 0) \cdot x = (0 \cdot x) + (0 \cdot x)$ , and by canceling one copy of  $0 \cdot x$  on both sides, we conclude that  $0 \cdot x = 0$ . We similarly apply

right distributivity to the expression  $x \cdot 0 = x \cdot (0 + 0) = (x \cdot 0) + (x \cdot 0)$  to conclude that  $x \cdot 0 = 0$ .

#### Definition: Zero Rng, Trivial Rng

The *zero rng* or *trivial rng* is the rng  $\langle \{0\}; 0, -, +, \cdot \rangle$  whose underlying set is a singleton containing the distinguished element 0, and whose operations are defined by  $-0 = 0 + 0 = 0 \cdot 0 = 0$ .

#### Definition: Nonzero Rng, Nontrivial Rng

A rng is *nonzero* or *nontrivial* if its underlying set contains more than one element.

#### Definition: Ring

A *ring* is an algebraic structure  $\langle R; 0, 1, -, +, \cdot \rangle$  consisting of:

- a set  $R$ , called the *underlying set*;
- a distinguished element  $0 \in R$ , called the *zero element*;
- a distinguished element  $1 \in R$ , called the *identity element*;
- a unary operation  $- : R \rightarrow R$ , written as  $x \mapsto -x$ , called *negation*;
- a binary operation  $+ : R \times R \rightarrow R$ , written as  $(x, y) \mapsto x + y$ , called *addition*;
- a binary operation  $\cdot : R \times R \rightarrow R$ , written as  $(x, y) \mapsto x \cdot y$ , called *multiplication*;

satisfying the following requirements:

- *Rng structure*:  $\langle R; 0, -, +, \cdot \rangle$  is a rng.
- *Identity*:  $1 \cdot x = x \cdot 1 = x$  for all  $x \in R$ .

#### Definition: Commutative Ring

A *commutative ring* is a ring  $R$  that satisfies the following additional requirement:

- *Commutativity*:  $x \cdot y = y \cdot x$  for all  $x, y \in R$ .