Notes on Mathematics

David K. Zhang

Last modified January 16, 2022

List of Definitions

List of Theorems

Chapter 1

Set Theory

Definition: Empty Set, $\varnothing$

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

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

Definition: Non-empty Set

A set is ***non-empty*** if it contains at least one element.

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.

Using this notation, we write $A \neq \varnothing$ to denote that a set A is non-empty.

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 $\varnothing$ and the set A itself.

Definition: Union, $A \cup B$

Let A and B be sets. The ***union*** of A and B, denoted by $A \cup B$, is the set containing all elements of A together with all elements of B.

$$x \in (A \cup B) \iff x \in A \text{ or } x \in B$$

Definition: Intersection, Intersects, $A \cap B$

Let A and B be sets. The ***intersection*** of A and B, denoted by $A \cap B$, is the set containing all elements that are present in both A and B.

$$x \in (A \cap B) \iff x \in A \text{ and } x \in B$$

We say that A ***intersects*** B if the intersection $A \cap B$ is non-empty.

Definition: Difference, Relative Complement, $A \setminus B$

Let A and B be sets. The ***difference*** of A and B, also known as the ***relative complement*** of B in A, denoted by $A \setminus B$, is the set containing all the elements of A which are not elements of B.

$$A \setminus B \coloneqq \{x \in A : x \notin B\}$$

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 $b \in B$.

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

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, $f : A \to B$, $f(x)$

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 $f : A \to B$ 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 $f : A \to B$ 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 $f : A \to B$ 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, $f : A \hookrightarrow\!\!\!\!\!\rightarrow B$

Let A and B be sets. A function $f : A \to B$ is ***bijective***, or a ***one-to-one correspondence***, or a ***bijection***, if f is both injective and surjective. We write $f : A \hookrightarrow\!\!\!\!\!\rightarrow B$ 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 $f : A \to B$, the ***image*** of a subset $S \subseteq A$ under f, denoted by $f[S]$, is the set defined by

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

In other words, $f[S]$ is the subset of B containing all elements that f maps to from S. For example, consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) \coloneqq x^2$. 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 $f : A \to B$, the ***inverse image*** or ***preimage*** of a subset $S \subseteq B$ under f, denoted by $f^{-1}[S]$, is the set defined by

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

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 $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) \coloneqq x^2$. 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 $f : A \to B$ 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, id_A

Let A be a set. The ***identity function*** on A is the function $\mathrm{id}_A : A \to A$ defined by $\mathrm{id}_A(a) \coloneqq a$ 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 $f : I \to \bigcup_{i\in I} A_i$ such that $f(i) \in A_i$ for all $i \in I$.

$$\prod_{i\in I} A_i \coloneqq \left\{ f : I \to \bigcup_{i\in I} A_i \;\middle|\; \forall i \in I : f(i) \in A_i \right\}$$

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 that satisfies the following requirements:

- ***Empty set is open***: $\varnothing \in T$.
- ***Whole set is open***: $X \in T$.
- ***Closed under arbitrary unions***: If $S \subseteq T$, then $\bigcup S \in T$.
- ***Closed under finite intersections***: If $S \subseteq T$ and $|S|$ is finite, then $\bigcap S \in T$.

Definition: Topological Space, Point, Open Set

A ***topological space*** is an ordered pair (X, T) consisting of a set X, called the ***underlying set***, and a topology T on X. The elements of X are called the ***points*** of the topological space (T, X), and the elements of T are called ***open sets***.

Definition: Closed Set

Let (X, T) be a topological space. A subset $F \subseteq X$ is ***closed*** if $X \setminus F \in T$.

Definition: Clopen Set

Let (X, T) be a topological space. A subset of X is ***clopen*** if it is both open and closed.

Definition: Open Neighborhood

Let (X, T) be a topological space. An ***open neighborhood*** of a point $x \in X$ is an open set $U \in T$ that contains x.

Definition: Neighborhood

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

Definition: Limit Point, Cluster Point, Accumulation Point

Let (X, T) be a topological space, and let $A \subseteq X$. A point $x \in X$ is a ***limit point*** of A, also known as a ***cluster point*** or ***accumulation point***, if every open neighborhood of x contains a point in A other than x itself.

In other words, x is a limit point of A if every open neighborhood of x intersects $A \setminus \{x\}$.

Definition: Derived Set, A'

Let (X, T) be a topological space, and let $A \subseteq X$. The ***derived set*** of A, denoted by A', is the set of all limit points of A in X.

$$A' := \{x \in X : x \text{ is a limit point of } A\}$$

Closed $\iff$ Contains All Limit Points

Theorem: Let (X, T) be a topological space. A subset $A \subseteq X$ is closed if and only if A contains all of its limit points, i.e., $A' \subseteq A$.

Proof: Suppose $A \subseteq X$ is closed, and let $x \in A'$ be a limit point of A. We will prove that $x \in A$ by contradiction. If $x \notin A$, then $x \in X \setminus A$. By hypothesis, A is closed, so $X \setminus A$ is open. It follows that $X \setminus A$ is an open neighborhood of x that does not intersect A, contradicting the hypothesis that x is a limit point of A.

Conversely, suppose that $A' \subseteq A$. We must prove that A is closed, i.e., that $X \setminus A$ is open. For each point $x \in X \setminus A$, the hypothesis $A' \subseteq A$ implies that x is not a limit point of A. Hence, by definition, there exists an open neighborhood $U_x \in T$ of x that does not intersect A. The union of all such neighborhoods is precisely $X \setminus A = \bigcup_{x \in X \setminus A} U_x$, which, being a union of open sets, is consequently open.

Definition: Interior, A°

Let (X, T) be a topological space, and let $A \subseteq X$. The ***interior*** of A, denoted by A°, is the union of all open sets $U \in T$ that are subsets of A.

$$A^\circ := \bigcup \{U \in T : U \subseteq A\}$$

Definition: Closure, $\overline{A}$

Let (X, T) be a topological space, and let $A \subseteq X$. The ***closure*** of A, denoted by $\overline{A}$, is the intersection of all closed sets $F \subseteq X$ that are supersets of A.

$$\overline{A} := \bigcap \{F \subseteq X : X \setminus F \in T \text{ and } F \supseteq A\}$$

Definition: Continuous Function

Let (X, T_X) and (Y, T_Y) be topological spaces. A function $f : X \to Y$ is ***continuous*** with respect to the topologies T_X and T_Y if, for every $U \in T_Y$, we have $f^{-1}[U] \in T_X$.

Definition: Metric, Distance Function

Let X be a set. A ***metric*** on X, also known as a ***distance function*** on X, is a function $d : X \times X \to \mathbb{R}$ 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 $f : X \to Y$ 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 $d_Y(f(x), f(x_0)) < \epsilon$.

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 ${}^{-1} : G \to G$, written as $x \mapsto x^{-1}$, called ***inversion***;
- a binary operation $\cdot : G \times G \to G$, 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 $x \in G$.

Cancellation Laws

Theorem: Let $\langle G; 1, {}^{-1}, \cdot \rangle$ be a group, and let $x, y, z \in G$.

- ***Left cancellation law***: If $x \cdot y = x \cdot z$, then $y = z$.
- ***Right cancellation law***: If $x \cdot z = y \cdot z$, then $x = y$.

Proof: If $x \cdot y = x \cdot z$, then:

$$\begin{aligned}
y &= 1 \cdot y && \text{(identity property)} \\
&= (x^{-1} \cdot x) \cdot y && \text{(inverse property)} \\
&= x^{-1} \cdot (x \cdot y) && \text{(associative property)} \\
&= x^{-1} \cdot (x \cdot z) && \text{(by hypothesis)} \\
&= (x^{-1} \cdot x) \cdot z && \text{(associative property)} \\
&= 1 \cdot z && \text{(inverse property)} \\
&= z && \text{(identity property)}
\end{aligned}$$

Similarly, if $x \cdot z = y \cdot z$, then

$$x = x \cdot 1 = x \cdot (z \cdot z^{-1}) = (x \cdot z) \cdot z^{-1} = (y \cdot z) \cdot z^{-1} = y \cdot (z \cdot z^{-1}) = y \cdot 1 = y.$$

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 $- : R \to R$, written as $x \mapsto -x$, called ***negation***;
- a binary operation $+ : R \times R \to R$, written as $(x, y) \mapsto x + y$, called ***addition***;
- a binary operation $\cdot : R \times R \to R$, 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: Subrng, $S \leq R$

Let $\langle R; 0, -, +, \cdot \rangle$ be a rng. A ***subrng*** of $\langle R; 0, -, +, \cdot \rangle$ is a subgroup $S \leq \langle R; 0, -, + \rangle$ that satisfies the following additional requirement:

- ***Closed under products***: If $x, y \in S$, then $x \cdot y$ in S.

We write $S \leq R$ to indicate that S is a subrng of $\langle R; 0, -, +, \cdot \rangle$.

The zero rng is a subrng of every rng.

Definition: Rng Homomorphism

Let $\langle R; 0_R, -_R +_R, \cdot_R \rangle$ and $\langle S; 0_S, -_S +_S, \cdot_S \rangle$ be rngs. A ***rng homomorphism*** from R to S is a function $f : R \to S$ that satisfies the following requirements:

- ***Preserves additive structure***: f is a group homomorphism between the abelian groups $\langle R; 0_R, -_R +_R \rangle$ and $\langle S; 0_S, -_S +_S \rangle$.
- ***Preserves products***: $f(x \cdot_R y) = f(x) \cdot_S f(y)$ for all $x, y \in R$.

Every rng homomorphism is also a group homomorphism, so the theory and terminology of group homomorphisms is immediately applicable to rng homomorphisms. For example, the kernel of a rng homomorphism $f : R \to S$ is still defined to be the set

$$\ker f := \{x \in R : f(x) = 0_S\}.$$

As with groups, we will often refer to a rng $\langle R; 0, -, +, \cdot \rangle$ by the name of its underlying set R and denote the multiplication operation $\cdot$ by juxtaposition. We will never denote addition, subtraction, or negation by juxtaposition, so the symbols $+$ and $-$ will always be used.

Definition: Ideal, Left Ideal, Right Ideal, One-Sided Ideal, Two-Sided Ideal, $I \trianglelefteq R$

Let $\langle R; 0, 1, -, +, \cdot \rangle$ be a rng.

- A ***left ideal*** of R is a subrng $I \leq R$ that satisfies the following additional requirement:
  - ***Absorbs left multiplication***: $rx \in I$ for all $r \in R$ and $x \in I$.
- A ***right ideal*** of R is a subrng $I \leq R$ that satisfies the following additional requirement:

- ***Absorbs right multiplication***: $xr \in I$ for all $x \in I$ and $r \in R$.

- A ***one-sided ideal*** of R is a subrng $I \leq R$ that is a left ideal or a right ideal (possibly both).
- A ***two-sided ideal*** of R, or simply an ***ideal*** of R, is a subrng $I \leq R$ that is both a left ideal and a right ideal.

We write $I \trianglelefteq R$ to denote that I is a (two-sided) ideal of R.

Definition: Rng of Formal Power Series, $R[\![x]\!]$

Let $\langle R; 0, -, +, \cdot \rangle$ be a rng. The ***rng of formal power series*** over $\langle R; 0, -, +, \cdot \rangle$, denoted by $R[\![x]\!]$, TO DO: FINISH THIS DEFINITION

Definition: Rng of Polynomials, $R[x]$

Let $\langle R; 0, -, +, \cdot \rangle$ be a rng. The ***rng of polynomials*** over $\langle R; 0, -, +, \cdot \rangle$, denoted by $R[x]$, is the subrng of $R[\![x]\!]$ TO DO: FINISH THIS DEFINITION

Definition: Commutative Rng

A ***commutative rng*** is a rng $\langle R; 0, -, +, \cdot \rangle$ that satisfies the following additional requirement:

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

The word "commutative" in the term "commutative rng" emphasizes that the *multiplication* operation is commutative. By definition, the addition operation is always commutative in every rng.

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 $- : R \to R$, written as $x \mapsto -x$, called ***negation***;
- a binary operation $+ : R \times R \to R$, written as $(x, y) \mapsto x + y$, called ***addition***;
- a binary operation $\cdot : R \times R \to R$, 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: Subring

Let $\langle R; 0, 1, -, +, \cdot \rangle$ be a ring. A ***subring*** of $\langle R; 0, 1, -, +, \cdot \rangle$ is a subrng $S \leq \langle R; 0, -, +, \cdot \rangle$ that satisfies the following additional requirement:

- ***Contains the identity***: $1 \in S$.

In these notes, we will only use the notation $S \leq R$ for *subrngs*, not *subrings*. This ensures consistency with the notation $I \trianglelefteq R$ for ideals (i.e., $I \trianglelefteq R \implies I \leq R$), since an ideal is always a subrng, but not necessarily a subring.

Definition: Field

A ***field*** is a commutative ring $\langle K; 0, 1, -, +, \cdot\rangle$ that satisfies the following additional requirements:

- ***Nontriviality***: $0 \neq 1$.
- ***Invertibility***: Every element of $K \setminus \{0\}$ has a two-sided inverse, i.e., $K^\times = K \setminus \{0\}$.