

# UW W17 PMATH333 - Definitions and Theorems

Johnson Ng

April 11, 2017

# Contents

<b>A</b>	<b>ZF Set Theory and the Axiom of Choice</b>	<b>5</b>
A.1	Introduction . . . . .	5
A.2	ZFC Axioms of Set Theory . . . . .	6
A.3	Relations, Equivalence Relations, Functions and Recursion . . . . .	12
A.4	Construction of Integers, Rational, Real and Complex Numbers . . . . .	16

# List of Definitions

Definition A.2.1	Mathematical Symbols . . . . .	6
Definition A.2.2	Formula . . . . .	6
Definition A.2.3	Free or Bounded Variable . . . . .	7
Definition A.2.4	Is Bound By and Binds . . . . .	7
Definition A.2.5	Free Variable, Statement, Statement About . . . . .	7
Definition A.2.6	Unique Existence . . . . .	7
Definition A.2.7	Empty Set Axiom . . . . .	8
Definition A.2.8	Extension Axiom . . . . .	8
Definition A.2.9	$\emptyset$ . . . . .	8
Definition A.2.10	Subset . . . . .	9
Definition A.2.11	Separation Axiom . . . . .	9
Definition A.2.12	Pair Axiom . . . . .	9
Definition A.2.13	Union Axiom . . . . .	9
Definition A.2.14	Union . . . . .	9
Definition A.2.15	Intersection . . . . .	10
Definition A.2.16	Power Set Axiom . . . . .	10
Definition A.2.17	Power Set . . . . .	10
Definition A.2.18	Ordered Pair . . . . .	10
Definition A.2.19	Successor, Inductive . . . . .	11
Definition A.2.20	Axiom of Infinity . . . . .	11

Definition A.2.21	Natural Numbers . . . . .	11
Definition A.2.22	Replacement Axiom . . . . .	12
Definition A.2.23	Axiom of Choice . . . . .	12
Definition A.3.1	Binary Relation . . . . .	12
Definition A.3.2	Domain, Range, Image, Inverse Image, Inverse, Composition .	12
Definition A.3.3	Equivalence Relation . . . . .	13
Definition A.3.4	Equivalence Class . . . . .	13
Definition A.3.5	Partition . . . . .	13
Definition A.3.6	Set of Representatives . . . . .	14
Definition A.3.7	Function . . . . .	14
Definition A.3.8	One-to-one & Onto . . . . .	15
Definition A.3.9	Left and Right Inverses . . . . .	15
Definition A.3.10	Invertible . . . . .	15
Definition A.4.1	Sum and Product . . . . .	16
Definition A.4.2	Integers . . . . .	16
Definition A.4.3	Rational Numbers . . . . .	16
Definition A.4.4	Real Numbers . . . . .	17
Definition A.4.5	Complex Numbers . . . . .	17

# List of Theorems

Theorem A.2.1	Uniqueness of the Empty Set . . . . .	8
Theorem A.2.2	Existence & Uniqueness of an Inductive Set . . . . .	11
Theorem A.2.3	Principle of Induction . . . . .	11
Theorem A.3.1	Domain, Range, Image and Inverse Image as Sets . . . . .	13
Theorem A.3.2	Inverse and Composition as Binary Relations . . . . .	13
Theorem A.3.3	Correspondence of Equivalence Relations and Partitions . . . .	14
Theorem A.3.4	Surjective and Injective VS Inverses . . . . .	15
Theorem A.3.5	The Recursion Theorem . . . . .	15

# Appendix A

## ZF Set Theory and the Axiom of Choice

### A.1 Introduction

#### Example A.1.1 (Russel's Paradox)

Let  $X$  be the set of all sets, and let  $S = \{A \in X \mid A \notin A\}$ .

Note for example that  $Z \notin Z \implies Z \in S$ , and  $X \in X \implies X \notin S$ .

Thus we have  $S \in S \iff S \notin S$ .

To ensure that mathematical paradoxes (like the above) can no longer arise, mathematicians considered the following questions, and with these questions, rough answers are provided:

1. What exactly is an allowable mathematical object?

A: Every mathematical object is a mathematical set, and a mathematical set can be constructed using certain rules, for e.g. the now widely accepted Zermelo-Fraenkel Set Theory and the Axiom of Choice. While the Axiom of Choice is still highly criticized even today (e.g. the highly controversial **Banach-Tarski Paradox**), the Zermelo-Fraenkel Set Theory is widely welcomed, but not without critics. We shall call the Zermelo-Fraenkel Set Theory and the Axiom of Choice as the ZFC Axioms of Set Theory.

2. What exactly is an allowable mathematical statement?

A: Every mathematical statement can be expressed in a formal symbolic language, which uses symbols rather than words from any spoken language.

3. What exactly is allowable in a mathematical proof?

A: Every mathematical proof is a finite list of ordered pairs  $(\mathcal{S}_n, \mathcal{F}_n)$  (which we can think of as proven theorems), where each  $\mathcal{S}_n$  is a finite set of formulas (called the *premises*) and each  $\mathcal{F}_n$  is a single formula (called the *conclusion*), which that each pair  $(\mathcal{S}_n, \mathcal{F}_n)$  can be obtained from previous pairs  $(\mathcal{S}_i, \mathcal{F}_i)$  with  $i < n$ , using certain proof rules.

In the remainder of this appendix, we shall look more into the first 2 questions.

## A.2 ZFC Axioms of Set Theory

### Definition A.2.1 (Mathematical Symbols)

We allow ourselves to use only the following symbols from the following symbol set:

$\neg$	<i>not</i>
$\wedge$	<i>and</i>
$\vee$	<i>or</i>
$\implies$	<i>implies</i>
$\iff$	<i>if and only if</i>
$=$	<i>equals</i>
$\in$	<i>is an element of</i>
$\forall$	<i>for all</i>
$\exists$	<i>there exists</i>
$() \ \{ \} \ \square$	<i>parenthesis</i>

along with some variable symbols such as  $x, y, z, u, v, w, \dots$  or  $x_1, x_2, x_3, \dots$

### Definition A.2.2 (Formula)

A formula (in the formal symbolic language of first order set theory) is a non-empty finite string of symbols, from the above list, which can be obtained using finitely many applications following the three rules below:

1. If  $x$  and  $y$  are variable symbols, then each of the following strings are formulas.

$$x = y, \quad x \in y$$

2. If  $F$  and  $G$  are formulas then each of the following strings are formulas.

$$\neg F, \quad (F \wedge G), \quad (F \vee G), \quad (F \implies G), \quad (F \iff G)$$

3. If  $x$  is a variable symbol and  $F$  is a formula then each of the following is a formula.

$$\forall x \in F, \quad \exists x \in F$$

**Definition A.2.3 (Free or Bounded Variable)**

Let  $x$  be a variable symbol and let  $F$  be a formula. For each occurrence of the symbol  $x$ , which does not immediately follow a quantifier, in the formula  $F$ , we define whether the occurrence of  $x$  is free or bound inductively as follows:

1. If  $F$  is a formula of one of the forms  $y = z$  or  $y \in z$ , where  $y$  and  $z$  are variable symbols (possibly equal to  $x$ ), then every occurrence of  $x$  in  $F$  is free, and no occurrence is bound.
2. If  $F$  is a formula of one of the forms  $\neg H, (H \wedge G), (H \vee G), (H \implies G), (H \iff G)$ , where  $G$  and  $H$  are formulas, then each occurrence of the symbol  $x$  is either an occurrence in the formula  $G$  or an occurrence in the formula  $H$ , and each free (respectively, bound) occurrence of  $x$  in  $G$  remains free (respectively, bound) in  $F$ , and similarly for each free (or bound) occurrence of  $x$  in  $H$ . In other words, wlog, if  $x$  is bounded in  $G$ , then it is bounded in  $F$ , and vice versa.
3. If  $F$  is a formula of one of the forms  $\forall y \in G$  or  $\exists y \in G$ , where  $G$  is a formula and  $y$  is a variable symbol. If  $y$  is different from  $x$ , then each free (or bound) occurrence of  $x$  in  $G$  remains free (or bound) in the formula  $G$ , and if  $y = x$  then every free occurrence of  $x$  in  $G$  becomes bound in  $F$ , and every bound occurrence of  $x$  in  $G$  remains bound in  $F$ .

**Definition A.2.4 (Is Bound By and Binds)**

When a quantifier symbol occurs in a given formula  $F$ , and is followed by the variable symbol  $x$  and then by the formula  $G$ , any free occurrence of  $x$  in  $G$  will become bound in the given formula  $F$  (by the 3rd definition above). We shall say that the occurrence of  $x$  is bound by (that occurrence of) the quantifier symbol, or that (the occurrence of) the quantifier symbol binds the occurrence of  $x$ .

**Definition A.2.5 (Free Variable, Statement, Statement About)**

A **free variable** in a formula  $F$  is any variable symbol that has at least one free occurrence in  $F$ . A formula  $F$  with no free variables is called a **statement**. When the free variables in  $F$  all lie in the set  $\{x_1, x_2, \dots, x_n\}$ , we shall write  $F$  as  $F(x_1, x_2, \dots, x_n)$  and we shall say that  $F$  is a **statement about** the variables  $x_1, x_2, \dots, x_n$ .

**Definition A.2.6 (Unique Existence)**

When  $F(x)$  is a statement about  $x$ , we sometimes write  $F(y)$  as a short form for the formula  $\forall x(x = y \implies F(x))$ , and we sometimes write

$$\exists! y \quad F(y)$$

which we read as "there exists a unique  $y$  such that  $F(y)$ ", as a short form for the formula

$$(\exists y \quad F(y) \wedge \forall z \quad F(z)) \implies z = y$$



which is, in turn, for the formula

$$\exists y \left( \forall x (x = y \implies F(x)) \wedge \forall z (\forall x (x = z \implies F(x)) \implies z = y) \right)$$

**Remark (The ZFC Axioms of Set Theory (informal))**

Every mathematical set can be constructed using specific rules, which we shall use the ZFC Axioms of Set Theory. Below is a list of the ZFC Axioms, stated informally.

- *Empty Set Axiom:* There exists an empty set  $\emptyset$  with no elements.
- *Extension Axiom:* 2 sets are equal if and only if they have the same elements.
- *Separation Axiom:* If  $u$  is a set and  $F(x)$  is a statement about  $x$ ,  $\{x \in u : F(x)\}$  is a set.
- *Pair Axiom:* If  $u$  and  $v$  are sets then  $\{u, v\}$  is a set.
- *Union Axiom:* If  $u$  is a set then  $\bigcup_{v \in u} v$  is a set.
- *Power Set Axiom:* If  $u$  is a set then  $\mathcal{P}(u) = \{v : v \subseteq u\}$  is a set.
- *Axiom of Infinity:* If we define the natural numbers to be the sets  $0 = \emptyset, 1 = \{0\}, 2 = \{0, 1\}, 3 = \{0, 1, 2\}$  and so on, then  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$  is a set.
- *Replacement Axiom:* If  $u$  is a set and  $F(x, y)$  is a statement about  $x$  and  $y$  with the property that  $\forall x \exists! y F(x, y)$  then  $\{y : \exists x \in u F(x, y)\}$  is a set.
- *Axiom of Choice:* Given a set  $u$  of non-empty pairwise disjoint sets, there exists a set which contains exactly one element from each of the sets in  $u$ .

**Definition A.2.7 (Empty Set Axiom)**

The Empty Set Axiom is the formula

$$\exists u \forall x \neg x \in u$$

**Definition A.2.8 (Extension Axiom)**

The Extension Axiom is the formula

$$\forall u \forall v \left( u = v \iff \forall x (x \in u \iff x \in v) \right)$$

**Theorem A.2.1 (Uniqueness of the Empty Set)**

The empty set is unique.

**Definition A.2.9 ( $\emptyset$ )**

We denote the unique empty set by  $\emptyset$ .

**Definition A.2.10 (Subset)**

Given sets  $u$  and  $v$ , we say that  $u$  is a **subset** of  $v$ , and write  $u \subseteq v$ , when  $\forall x(x \in u \implies x \in v)$

**Definition A.2.11 (Separation Axiom)**

For any statement  $F(x)$  about  $x$ , the following formula is an axiom.

$$\forall u \exists v \forall x (x \in v \iff (x \in u \wedge F(x)))$$

More generally, for any statement  $F(x, u_1, u_2, \dots, u_n)$  about  $x, u_1, u_2, \dots, u_n$  where  $n \geq 0$ , the following formula is an axiom.

$$\forall u \forall u_1 \dots \forall u_n \exists v \forall x (x \in v \iff (x \in u \wedge F(x, u_1, \dots, u_n)))$$

Any axiom of this form is called the *Separation Axiom*.

**Note**

It is important to realize that a Separation Axiom only allows us to construct a subset of a given set  $u$ . So, e.g., we cannot use the Separation Axiom to show that the collection  $S = \{x : \neg x \in x\}$ , which is used to formulate *Russel's Paradox*, is a set.

**Definition A.2.12 (Pair Axiom)**

The Pair Axiom is the formula

$$\forall u \forall v \exists w \forall x (x \in w \iff (x = u \vee x = v))$$

**Definition A.2.13 (Union Axiom)**

The Union Axiom is the formula

$$\forall u \exists w \forall x (x \in w \iff \exists v (v \in u \wedge x \in v))$$

**Definition A.2.14 (Union)**

Given a set  $u$ , by the Union Axiom there exists a set  $w$  with the property that  $\forall x (x \in w \iff \exists v (v \in u \wedge x \in v))$ , and by the Extension Axiom, this set  $w$  is unique. We call the set  $w$  the **union** of the elements in  $u$ , and denote it by

$$\cup u = \bigcup_{v \in u} v.$$

Given two sets  $u$  and  $v$ , we define the union of  $u$  and  $v$  to be the set

$$u \cup v := \bigcup \{u, v\}.$$

Given three sets  $u$ ,  $v$ , and  $w$ , note that  $\{z\} = \{z, z\}$  is a set and so  $\{x, y, z\} = \{x, y\} \cup \{z\}$  is also a set. More generally, if  $u_1, u_2, \dots, u_n$  are sets then  $\{u_1, u_2, \dots, u_n\}$  is a set and we define the union of the sets  $u_1, u_2, \dots, u_n$  to be

$$u_1 \cup u_2 \cup \dots \cup u_n = \bigcup_{k=1}^n u_k = \bigcup \{u_1, u_2, \dots, u_n\}$$

**Definition A.2.15 (Intersection)**

Given a set  $u$ , we define the intersection of the elements in  $u$  to be the set

$$\bigcap u = \left\{ x \in \bigcup u \mid \forall v (v \in u \implies x \in v) \right\}$$

Given two sets  $u$  and  $v$ , we define the intersection of  $u$  and  $v$  to be the set

$$u \cap v = \bigcap \{u, v\}$$

and more generally, given sets  $u_1, u_2, \dots, u_n$ , we define the intersection of  $u_1, u_2, \dots, u_n$  to be the set

$$u_1 \cap u_2 \cap \dots \cap u_n = \bigcap_{k=1}^n u_k = \bigcap \{u_1, u_2, \dots, u_n\}$$

**Definition A.2.16 (Power Set Axiom)**

The Power Set Axiom is the formula

$$\forall u \exists w \forall v (v \in w \iff v \subseteq u)$$

**Definition A.2.17 (Power Set)**

Given a set  $u$ , the set  $w$  is with the property that  $\forall v (v \in w \iff v \subseteq u)$  (which exists by the Power Set Axiom and is unique by the Extension Axiom) is called the power set of  $u$  and is denoted by  $\mathcal{P}(u)$ , so we have

$$\mathcal{P}(u) = \{v \mid v \subseteq u\}$$

**Definition A.2.18 (Ordered Pair)**

Given two sets  $x$  and  $y$ , we define the ordered pair  $(x, y)$  to be the set

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Given two sets  $u$  and  $v$ , note that if  $x \in u$  and  $y \in v$  then we have  $\{x\} \in \mathcal{P}(u \cup v)$  and  $\{x, y\} \in \mathcal{P}(u \cup v)$  and so  $(x, y) = \{\{x\}, \{x, y\}\} \in \mathcal{P}(\mathcal{P}(u \cup v))$ . We define the product  $u \times v$  to be the set

$$u \times v = \{(x, y) \mid x \in u \wedge y \in v\},$$

i.e.

$$u \times v = \left\{ z \in \mathcal{P}(\mathcal{P}(u \cup v)) \mid \exists x \exists y ((x \in u \wedge y \in v) \wedge z = (x, y)) \right\}$$

**Definition A.2.19 (Successor, Inductive)**

We define

$$0 = \emptyset, \quad 1 = \{0\}, \quad 2 = \{0, 1\} = 1 \cup \{1\}, \quad 3 = \{0, 1, 2\} = 2 \cup \{2\},$$

and so on. For a set  $x$ , we define the successor of  $x$  to be the set

$$x + 1 = x \cup \{x\}.$$

A set  $u$  is called inductive when it has the property that

$$(0 \in u \wedge \forall x(x \in u \implies x + 1 \in u))$$

**Definition A.2.20 (Axiom of Infinity)**

The Axiom of Infinity is the formula

$$\exists u(0 \in u \wedge \forall x(x \in u \implies x + 1 \in u))$$

so the Axiom of Infinity states that there exists an inductive set.

**Theorem A.2.2 (Existence & Uniqueness of an Inductive Set)**

$\exists w := \{x | x \in v \text{ for every inductive set } v\}$

Moreover, this set  $w$  is an inductive set.

**Definition A.2.21 (Natural Numbers)**

The unique set  $w$  in the above theorem is called the set of natural numbers, and we denote it by  $\mathbb{N}$ . We write

$$\begin{aligned} \mathbb{N} &= \{x | x \in v \text{ for every inductive set } v\} \\ &= \{0, 1, 2, 3, \dots\} \end{aligned}$$

For  $x, y \in \mathbb{N}$ , we write  $x \dot{\prec} y$  when  $x \in y$  and write  $x \leq y$  when  $x < y \vee x = y$ .

**Remark**

For a formula  $F$ , we write  $\forall x \in u F$  as a shorthand notation for the formula  $\forall x(x \in u \implies F)$ . Similarly, we write  $\exists x \in u F$  as a shorthand notation for  $\exists x(x \in u \wedge F)$ .

**Theorem A.2.3 (Principle of Induction)**

Let  $F(x)$  be a statement about  $x$ . SPS that

1.  $F(0)$ , and
2.  $\forall x \in \mathbb{N}(F(x) \implies F(x + 1))$ .

Then  $\forall x \in \mathbb{N} F(x)$

**Remark**

The expression  $F(0)$  is short for  $\forall x(x = 0 \implies F(x))$ , which in turn is short for  $\forall x(\forall y \neg y \in x \implies F(x))$ . Similarly,  $F(x + 1)$  is short for the formula  $\forall y(y = x + 1 \implies F(y))$ , where  $F(y)$  is short for  $\forall x(x = y \implies F(x))$ .

**Definition A.2.22 (Replacement Axiom)**

Given a statement  $F(x, y)$  about  $x$  and  $y$ , the following formula is an axiom:

$$\forall u \left( \forall x \exists! y F(x, y) \implies \exists w \forall y (y \in w \iff \exists x \in u F(x, y)) \right)$$

where  $\exists! y F(x, y)$  is short for  $\exists y (F(x, y) \wedge \forall z (F(x, z) \implies z = y))$  with  $F(x, z)$  short for the formula  $\forall y (y = z \implies F(x, y))$ . More generally, given a statement  $F(x, y, u_1, \dots, u_n)$  about  $x, y, u_1, \dots, u_n$  with  $n \geq 0$ , the following formula is an axiom:

$$\forall u \forall u_1 \dots \forall u_n \left( \forall x \exists! y F(x, y, u_1, \dots, u_n) \implies \exists w \forall y (y \in w \iff \exists x \in u F(x, y, u_1, \dots, u_n)) \right)$$

An axiom of this form is called a Replacement Axiom.

**Definition A.2.23 (Axiom of Choice)**

The Axiom of Choice is the formula given by

$$\forall u \left( \left( \neg \phi \in u \wedge \forall x \in u \forall y \in u (\neg x = y \implies x \cap y = \emptyset) \right) \implies \exists w \forall v \in u \exists! x \in v x \in w \right)$$

From this point on, we will be using upper-case letters to denote sets, instead of lower-case as per the statements above.

### A.3 Relations, Equivalence Relations, Functions and Recursion

**Definition A.3.1 (Binary Relation)**

A binary relation  $R$  on a set  $X$  is a subset  $R \subseteq X \times X$ . More generally, a binary relation is any set  $R$  whose elements are ordered pairs. For a binary relation  $R$ , we usually write  $xRy$  instead of  $(x, y) \in R$ .

**Definition A.3.2 (Domain, Range, Image, Inverse Image, Inverse, Composition)**

Let  $R$  and  $S$  be binary relations.

The domain of  $R$  is

$$\text{Domain}(R) = \{x \mid \exists y xRy\}$$

and the range of  $R$  is

$$\text{Range}(R) = \{x | \exists y \, xRy\}.$$

For any set  $A$ , the image of  $A$  under  $R$  is

$$R(A) = \{y | \exists x \in A \, xRy\}$$

and the inverse image of  $A$  under  $R$  is

$$R^{-1}(A) = \{x | \exists y \in A \, xRy\}.$$

The inverse of  $R$  is

$$R^{-1} = \{(y, x) | (x, y) \in R\}$$

and the composition  $S$  composed with  $R$  is

$$S \circ R = \{(x, z) | \exists y \, xRy \wedge ySz\}$$

**Theorem A.3.1 (Domain, Range, Image and Inverse Image as Sets)**

Let  $A$  be a set and let  $R$  be a binary relation. Then  $\text{Domain}(R)$ ,  $\text{Range}(R)$ ,  $R(A)$  and  $R^{-1}(A)$  are sets.

**Theorem A.3.2 (Inverse and Composition as Binary Relations)**

Let  $A$  be a set and let  $R$  and  $S$  be binary relations. Then  $R^{-1}$  and  $S \circ R$  are binary relations.

**Definition A.3.3 (Equivalence Relation)**

An equivalence relation on a set  $X$  is a binary relation  $R$  on  $X$  such that

1.  $R$  is **reflexive**, i.e.  $\forall x \in X \, xRx$
2.  $R$  is **symmetric**, i.e.  $\forall x, y \in X \, (xRy \implies yRx)$ , and
3.  $R$  is **transitive**, i.e.  $\forall x, y, z \in X \, ((xRy \wedge yRz) \implies xRz)$ .

**Definition A.3.4 (Equivalence Class)**

Let  $R$  be an equivalence relation on the set  $X$ . For  $a \in X$ , the equivalence class of  $a$  modulo  $R$  is the set

$$[a]_R = \{x \in X | xRa\}$$

**Definition A.3.5 (Partition)**

A partition of a set  $X$  is a set  $S$  of non-empty pairwise disjoint sets whose union is  $X$ , that is a set  $S$  such that

1.  $\forall X, Y \in S \, (X \neq Y \implies X \cap Y = \emptyset)$
2.  $\bigcup S = X$ .

**Theorem A.3.3 (Correspondence of Equivalence Relations and Partitions)**

Given a set  $X$ , we have the following correspondence between equivalence relations on  $X$  and partitions of  $X$ .

1. Given an equivalence relation  $R$  on  $X$ , the set of all equivalence classes

$$S_R = \{[a]_R | a \in X\}$$

is a partition of  $X$ .

2. Given a partition  $S$  of  $X$ , the relation  $R_S$  on  $X$  is defined by

$$R_S = \{(x, y) \in X \times X | \exists A \in S (x \in A \wedge y \in A)\}$$

is an equivalence relation on  $X$ .

3. Given an equivalence relation  $R$  on  $X$  we have  $R_{S_R} = R$ , and a given partition  $S$  of  $X$ , we have  $S_{R_S} = S$ .

**Note (Set of All Equivalence Classes)**

Given an equivalence relation  $R$  on  $X$ , the set of all equivalence classes, which we denote by  $S_R$  in the above theorem, is usually denoted by  $X/R$ , so

$$X/R = \{[a]_R | a \in X\}$$

**Definition A.3.6 (Set of Representatives)**

Let  $R$  be an equivalence relation. A set of representatives for  $R$  is a subset of  $X$  which contains exactly one element from each equivalence class in  $X/R$ .

**Remark**

Notice that the AC is equivalent to the statement that every equivalence relation has a set of representatives.

**Definition A.3.7 (Function)**

Get sets  $X$  and  $Y$ , a function from  $X$  to  $Y$  is a binary relation  $f \subseteq X \times Y$  with the property that

$$\forall x \in X \exists! y \in Y (x, y) \in f$$

More generally, a function is a binary relation with the property that

$$\forall x \in \text{Domain}(f) \exists! y (x, y) \in f.$$

For a function  $f$ , we usually write  $y = f(x)$  instead of  $xy$ . It is customary to use the notation  $f : X \mapsto Y$  when  $X = \text{Domain}(f)$  and  $Y$  is any set with  $\text{Range}(f) \subseteq Y$ .

**Definition A.3.8 (One-to-one & Onto)**

Let  $f : X \mapsto Y$ . The function  $f$  is called *one-to-one* (or *injective*) when

$$\forall y \in Y \exists \text{ at most one } x \in X \ y = f(x)$$

and  $f$  is called *onto* (or *surjective*) when

$$\forall y \in Y \exists \text{ at least one } x \in X \ y = f(x)$$

**Definition A.3.9 (Left and Right Inverses)**

Let  $f : X \mapsto Y$ . Let  $I_X$  and  $I_Y$  denote the identity function on  $X$  and  $Y$  respectively. A left inverse of  $f$  is a function  $g : Y \mapsto X$  such that  $g \circ f = I_X$ . A right inverse of  $f$  is a function  $H : X \mapsto Y$  such that  $f \circ H = I_Y$ . Note that if  $f$  has a left inverse  $g$  and a right inverse  $H$ , then we have  $g = g \circ I_Y = g \circ f \circ H = I_X \circ H = H$ . In this case, we say that  $g$  is the (unique two-sided) inverse of  $f$ .

**Theorem A.3.4 (Surjective and Injective VS Inverses)**

Let  $f : X \mapsto Y$ . Then

1.  $f$  is one-to-one if and only if  $f$  has a left inverse.
2.  $f$  is onto if and only if  $f$  has a right inverse.
3.  $f$  is one-to-one and onto if and only if  $f$  has a (two-sided) inverse.

**Definition A.3.10 (Invertible)**

A function  $f : X \mapsto Y$  is called *invertible* (or *bijective*) when it is one-to-one and onto, or equivalently, when it has a (unique two-sided) inverse.

**Theorem A.3.5 (The Recursion Theorem)**

1. Let  $A$  be a set, let  $a \in A$ , and let  $g : A \times \mathbb{N} \mapsto A$ . Then there exists a unique function  $f : \mathbb{N} \mapsto A$  such that

$$f(0) = a \text{ and } f(n+1) = g(f(n), n) \text{ for all } n \in \mathbb{N}$$

2. Let  $A$  and  $B$  be sets, let  $g : A \mapsto B$ , and let  $h : A \times B \times \mathbb{N} \mapsto B$ . Then there exists a unique function  $f : A \times \mathbb{N} \mapsto B$  such that for all  $a \in A$  we have

$$f(a, 0) = g(a) \text{ and } f(a, n+1) = h(a, f(a, n), n) \text{ for all } n \in \mathbb{N}$$



## A.4 Construction of Integers, Rational, Real and Complex Numbers

### Definition A.4.1 (Sum and Product)

By Part(2) of the *Recursion Theorem*, there is a unique function  $s : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$  such that for all  $a, b \in \mathbb{N}$  we have

$$s(a, 0) = a, \quad s(1, b + 1) = s(a, b) + 1.$$

We call  $s(a, b)$  the sum of  $a$  and  $b \in \mathbb{N}$  and write it as

$$a + b = s(a, b).$$

Also, there is a unique function  $p : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$  such that for all  $a, b \in \mathbb{N}$  we have

$$p(a, 0) = 0, \quad p(a, b + 1) = p(a, b) + a$$

We call  $p(a, b)$  the product of  $a$  and  $b$  in  $\mathbb{N}$ , and we write it as

$$a \cdot b = p(a, b)$$

### Definition A.4.2 (Integers)

We define the set of integers to be the set

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/R$$

where  $R$  is the equivalence relation given by

$$(a, b)R(c, d) \iff a + d = b + c$$

For  $[(a, b)]$  and  $[(c, d)]$  in  $\mathbb{Z}$ , we define

$$[(a, b)] \leq [(c, d)] \iff b + c \leq a + d$$

$$[(a, b)] + [(c, d)] \iff [(a + c, b + d)]$$

$$[(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)]$$

For  $n \in \mathbb{N}$  we write  $n = [(n, 0)]$  and  $-n = [(0, n)]$ , so that every element of  $\mathbb{Z}$  can be written as  $\pm n$  for some  $n \in \mathbb{N}$ , and we can identify  $\mathbb{N}$  with a subset of  $\mathbb{Z}$

### Definition A.4.3 (Rational Numbers)

We define the set of rational numbers to be the set

$$\mathbb{Q} = (\mathbb{N} \times \mathbb{Z}^+)/R$$

where  $\mathbb{Z}^+ = \{x \in \mathbb{N} | x \neq 0\}$  and  $R$  is the equivalence relation given by

$$(a, b)R(c, d) \iff ad = bc$$

For  $[(a, b)]$  and  $[(c, d)]$  in  $\mathbb{Q}$  we define

$$\begin{aligned} [(a, b)] \leq [(c, d)] &\iff a \cdot d \leq b \cdot c \\ [(a, b)] + [(c, d)] &\iff [(a \cdot d + b \cdot c, b \cdot d)] \\ [(a, b)] \cdot [(c, d)] &= [(ac, bd)] \end{aligned}$$

For  $a \in \mathbb{N}$  and  $b \in \mathbb{Z}^+$ , it is customary to write  $\frac{a}{b} = [(a, b)]$ . Also for  $a \in \mathbb{Z}$  we write  $a = [(a, 1)]$ , and we identify  $\mathbb{Z}$  with a subset of  $\mathbb{Q}$

**Definition A.4.4 (Real Numbers)**

We define the set of real numbers to be the set

$$\mathbb{R} = \{x \subseteq \mathbb{Q} | x \neq \emptyset, x \neq \mathbb{Q}, \forall a \in x \forall b \in \mathbb{Q} (b \leq a \implies b \in x), \forall a \in x \exists b \in x a < b\}$$

For  $x, y \in \mathbb{R}$  we define

$$\begin{aligned} x \leq y &\iff x \subseteq y \\ x + y &= \{a + b | a, b \in \mathbb{Q}, a \in x, b \in y\} \end{aligned}$$

For  $0 \leq x, y \in \mathbb{R}$  we define

$$x \cdot y = \{a \cdot b | 0 \leq a, b \in \mathbb{Q}, a \in x, b \in y\} \cup \{c \in \mathbb{Q} | c < 0\},$$

and YOU can try to, similarly, define  $x \cdot y$  in the case that  $x \not\leq 0$  and  $y \not\leq 0$ .

**Definition A.4.5 (Complex Numbers)**

We define the set of complex numbers to be the set

$$\mathbb{C} = \mathbb{R} \times \mathbb{R}.$$

We define addition and multiplication in  $\mathbb{C}$  by

$$\begin{aligned} (a, b) + (c, d) &= (a + c, b + d) \\ (a, b) \cdot (c, d) &= (ac - bd, ad + bc). \end{aligned}$$

We write  $i = (0, 1)$ . For  $x \in \mathbb{R}$  we write  $x = (x, 0)$  and identify  $\mathbb{R}$  with a subset of  $\mathbb{C}$ .