Appendix 1: The Construction of the Real Numbers

Fist-Order Set Theory

1.1 Definition: In the language of **first-order set theory** we allow ourselves to use only symbols from the following **symbol set**

$$\left\{ \neg, \wedge, \vee, \rightarrow, \leftrightarrow, =, \in, \forall, \exists, (,) \right\}$$

along with some variable symbols such as $x, y, z, u, v, w, \cdots$ or $x_1, x_2, x_3, \cdots$. The symbols in the symbol set are read as follows: $\neg$ is read as "not", $\wedge$ is read as "and", $\vee$ is read as "or", $\rightarrow$ is read as "implies", $\leftrightarrow$ is read as "if and only if", $\in$ is read as "is an element of", $\forall$" is read as "for all", $\exists$ is read as "there exists", and the symbols (and) are called parentheses.

1.2 Definition: 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 of the following three rules.

1. If x and y are variable symbols, then each of the following strings is a formula.

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

2. If F and G are formulas then each of the following strings is a formula.

$$\neg F \;, \quad (F \wedge G) \;, \quad (F \vee G) \;, \quad (F \rightarrow G) \;, \quad (F \leftrightarrow G)$$

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

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

1.3 Definition: 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 $\neg G$, $(G \wedge H)$, $(G \vee H)$, $(G \rightarrow H)$ or $(G \leftrightarrow H)$, 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 (respectivly, bound) in F, and similarly for each free (or bound) occurrence of x in H.

3. If F is a formula of one of the forms $\forall y\, G$ or $\exists y\, G$, where G is a formula and y is a variable symbol (possibly equal to x), then if y is different than x then each free (or bound) occurrence of x in G remains free (or bound) in the formula F, and if y is equal to x then every free occurrence of x in G becomes bound in the formula F, and every bound occurrence of x in G remains bound in the formula F.

1.4 Definition: 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 an application of part 3 of the above definition), and we shall say that that occurrence of x **is bound by** (that occurrence of) the quantifier symbol, or that (that occurrence of) the quantifier symbol **binds** that occurrence of x.

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

1.6 Example: In the following formula, determine which occurrences of the variable symbols are free and which are bound, and for each bound occurrence, indicate which quantifier binds it.

$$\forall x\, \exists y\big(\forall z(x \in y \to \exists y\ y = z) \wedge \forall x(\exists z\ z = u \vee z \in x)\big)$$

Solution: We indicate the free and bound occurrences and their binding quantifiers by placing integral labels under the relevant symbols: the free variables are given the label 0, each quantifier is given its own non-zero label, and each bound variable is given the same label as its binding quantifier:

$$\forall x\, \exists y\big(\forall z(x \in y \to \exists y\ y = z) \wedge \forall x(\exists z\ z = u \vee z \in x)\big)$$
$$\ \ 1\ \ 2\ \ \ \ 3\ \ \ 1\ \ \ \ \ 2\ \ \ \ \ \ 4\ \ 4\ \ \ \ \ 3\ \ \ \ \ 5\ \ \ 6\ \ 6\ \ \ \ 0\ \ \ 0\ \ \ 5$$

We remark that the free variables in this formula are z and u, so we say that it is a statement about z and u.

1.7 Example: Express the statement $x = \big\{y, \{z\}\big\}$ as a formal symbolic formula.

Solution: We can express the given statement in each of the following ways.

$$x = \big\{y, \{z\}\big\}$$
$$\forall u\,\big(u \in x \leftrightarrow u \in \big\{y, \{z\}\big\}\big)$$
$$\forall u\big(u \in x \leftrightarrow \big(u = y \vee u = \{z\}\big)\big)$$
$$\forall u\big(u \in x \leftrightarrow \big(u = y \vee \forall v(v \in u \leftrightarrow v = z)\big)\big)$$

The last expression is a formula.

1.8 Definition: Given a formula F and variable symbols x and y, we define $[F]_{x \mapsto y}$ as follows. When F is obtained using rule 1, the formula $[F]_{x \mapsto y}$ is obtained from F by replacing all occurrences of the symbol x by the symbol y. To deal with rule 2, we define $\big[\neg F\big]_{x \mapsto y} := \neg [F]_{x \mapsto y}$ and $\big[(F * G)\big]_{x \mapsto y} := \big([F]_{x \mapsto y} * [G]_{x \mapsto y}\big)$ for $* \in \{\wedge, \vee, \to, \leftrightarrow\}$. To deal with rule 3, we define $\big[\forall x\, F\big]_{x \mapsto y} := \forall x\, F$, and $\big[\forall y\, F\big]_{x \mapsto y} := \forall u\big[[F]_{y \mapsto u}\big]_{x \mapsto y}$ where u is the first variable which is not equal to x or y and which does not occur in F, and for a variable symbol z with $z \neq x$ and $z \neq y$ we define $\big[\forall z\, F\big]_{x \mapsto y} := \forall z [F]_{x \mapsto y}$.

The ZFC Axioms of Set Theory

1.9 Remark: Every mathematical **set** can be constructed using specific rules, which are known as the **ZFC axioms** of set theory, or the Zermelo-Fraenkel axioms of set theory, with the axiom of choice. We begin by listing the ZFC axioms, stating them informally.

Extension Axiom: Two sets are equal if and only if they have the same elements.

Empty Set Axiom: There exists a set $\emptyset$ with no 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 $\bigcup u = \bigcup_{v \in u} v$ 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 $\mathbf{N} = \{0, 1, 2, 3, \cdots\}$ 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.

We now proceed to state each of the ZFC axioms formally (as a formula in first-order set theory) and give some indication as to how these axioms can be used as a rigorous framework for essentially all of mathematics.

1.10 Definition: The **Extension Axiom** is the formula

$$\forall u \, \forall v \, \big(u = v \leftrightarrow \forall x (x \in u \leftrightarrow x \in v) \big) \,.$$

1.11 Definition: The **Empty Set Axiom** is the formula

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

1.12 Theorem: *The empty set is unique.*

Proof: Suppose that u and v are both empty. Let x be arbitrary. Since u is empty, we have $\neg x \in u$ and hence $x \in u \to x \in v$. Similarly, since v is empty, we have $\neg x \in v$ and hence $x \in v \to x \in u$. Since $x \in u \to x \in v$ and $x \in v \to x \in u$, we have $x \in u \leftrightarrow x \in v$. Since x was arbitrary, we have $\forall x \, (x \in u \leftrightarrow x \in v)$. By the Axiom of Extension, $u = v$.

1.13 Definition: We denote the unique empty set by $\emptyset$.

1.14 Remark: In a formal and rigorous treatment of the foundations of mathematics, we would need to decide at this point how to interpret the use of the symbol $\emptyset$. One approach is to add the symbol $\emptyset$ to our list of symbols, modify our definition of a formula to allow the use of the new symbol $\emptyset$, and add the axiom $\forall x \, \neg x \in \emptyset$ to our list of axioms. Another option is to interpret the use of the symbol as a shorthand notation for an expression which can be expressed formally using the existing symbols, so that for example the expression $u = \emptyset$ would be shorthand for the formula $\forall x \, \neg x \in u$.

1.15 Definition: Given sets u and v, we say that u is a **subset** of v, and we write $u \subseteq v$, when every element of u also lies in v, that is when $\forall x \, (x \in u \rightarrow x \in v)$.

1.16 Definition: For any formula F with free variable x, the following formula is an axiom.
$$\forall u \, \exists v \, \forall x \big(x \in v \leftrightarrow (x \in u \wedge F) \big)$$
More generally, for any formula F with free variables $x, u_1, u_2, \cdots, u_n$, the following formula is an axiom.
$$\forall u \forall u_1 \cdots \forall u_n \exists v \, \forall x \big(x \in v \leftrightarrow (x \in u \wedge F) \big)$$
Any axiom of this form is called an **Axiom of Separation**.

1.17 Notation: Given sets $u, u_1, \cdots, u_n$ and given a formula F with free variables $x, u_1, \cdots, u_n$, by the appropriate Axiom of Separation, there exists a set v with the property that $\forall x \big(x \in v \leftrightarrow (x \in u \wedge F) \big)$, and by the Extension Axiom, this set v is unique, and we denote it by
$$\big\{ x \in u \,\big|\, F \big\}.$$

1.18 Note: It is important to realize that a Separation Axiom only allows us to construct a subset of a given set u, so for example we cannot use a Separation Axiom to show that the collection $S = \{x \,|\, \neg \, x \in x\}$, which is used to formulate Russel's paradox, is a set.

1.19 Definition: The **Pair Axiom** is the formula
$$\forall u \, \forall v \, \exists w \, \forall x \big(x \in w \leftrightarrow (x = u \vee x = v) \big).$$

1.20 Notation: Given sets u and v, by the Pair Axiom there exists a set w with the property that $\forall x \big(x \in w \leftrightarrow (x = u \vee x = v) \big)$, and by the Extension Axiom, this set w is unique, and we denote it by
$$\{u, v\}$$

1.21 Example: With this axiom, we can construct some non-empty sets. For example, taking $u = v = \emptyset$ gives the set $\{\emptyset, \emptyset\} = \{\emptyset\}$ (note that $\{\emptyset\} \neq \emptyset$ by the Extension Axiom, since $\emptyset \in \{\emptyset\}$ but $\emptyset \notin \emptyset$). Then taking $u = \emptyset$ and $v = \{\emptyset\}$ gives the set $\big\{\emptyset, \{\emptyset\}\big\}$.

1.22 Definition: The **Union Axiom** is the formula
$$\forall u \, \exists w \, \forall x \big(x \in w \leftrightarrow \exists v \, (v \in u \wedge x \in v) \big).$$

1.23 Definition: Given a set u, by the Union Axiom there exists a set w with the property that $\forall x \big(x \in w \leftrightarrow \exists v \, (v \in u \wedge x \in v) \big)$, and by the Extension Axiom this set w is unique. We call the set w the **union** of the elements in u, and we denote it by
$$\bigcup u = \bigcup_{v \in u} v \, .$$
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 $u_1, u_2, \cdots, u_n$ are sets then $\{u_1, u_2, \cdots, u_n\}$ is a set and we define the **union** of the sets $u_1, \cdots, u_n$ to be
$$u_1 \cup u_2 \cup \cdots \cup u_n = \bigcup_{k=1}^{n} u_k = \bigcup \{u_1, u_2, \cdots, u_n\} \, .$$

1.24 Definition: Given a non-empty set u, we define the **intersection** of the elements in u to be the set

$$\bigcap u = \left\{ x \in \bigcup u \,\middle|\, \forall v (v \in u \to x \in v) \right\}$$

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 $u_1, u_2, \cdots, u_n$, we define the **intersection** of $u_1, u_2, \cdots, u_n$ to be the set

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

1.25 Definition: The **Power Set Axiom** is the formula

$$\forall u \,\exists w \,\forall v \,(v \in w \leftrightarrow v \subseteq u).$$

1.26 Definition: Given a set u, the set w with the property that $\forall v (v \in w \leftrightarrow v \subseteq u)$ (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

$$\mathcal{P}(u) = \{v \,|\, v \subseteq u\}.$$

1.27 Example: Find the power set of the set $\{\emptyset, \{\emptyset\}\}$.

Solution: We have

$$\mathcal{P}\Big(\{\emptyset, \{\emptyset\}\}\Big) = \Big\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\Big\}.$$

1.28 Definition: 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 $(x, y) = \{\{x\}, \{x, y\}\} \in \mathcal{P}\big(\mathcal{P}(u \cup v)\big)$. We define the **product** $u \times v$ to be the set

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

that is

$$u \times v = \big\{z \in \mathcal{P}\big(\mathcal{P}(u \cup v)\big) \,\big|\, \exists x \,\exists y \big((x \in u \wedge y \in v) \wedge z = (x, y)\big)\big\}.$$

1.29 Exercise: Find $\bigcup \Big(\{\emptyset\} \times \{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\Big).$

1.30 Definition: We define

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

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

$$\big(0 \in u \wedge \forall x \,(x \in u \to x + 1 \in u)\big).$$

1.31 Definition: The **Axiom of Infinity** is the formula

$$\exists u \big(0 \in u \wedge \forall x \,(x \in u \to x + 1 \in u)\big),$$

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

1.32 Theorem: *There exists a unique set w of the form*

$$w = \{ x \mid x \in v \text{ for every inductive set } v \}.$$

Moreover, this set w is an inductive set.

Proof: By the axiom of infinity, there exists an inductive set, say u. Let w be the set

$$w = \{ x \in u \mid x \in v \text{ for every inductive set } v \}$$
$$= \{ x \in u \mid \forall v \left(\left(0 \in v \wedge \forall y \left(y \in v \to y + 1 \in v \right) \right) \to x \in v \right) \}.$$

We claim that this set w does not depend on the choice of u. To prove this, let u_1 and u_2 be two inductive sets and let

$$w_1 = \{ x \in u_1 \mid x \in v \text{ for every inductive set } v \}$$
$$w_2 = \{ x \in u_2 \mid x \in v \text{ for every inductive set } v \}.$$

Then for any set x we have

$$x \in w_1 \iff x \in u_1 \text{ and } x \in v \text{ for every inductive set } v$$
$$\iff x \in v \text{ for every inductive set } v \text{ (since } u_1 \text{ is inductive)}$$
$$\iff x \in u_2 \text{ and } x \in v \text{ for every inductive set } v \text{ (since } u_2 \text{ is inductive)}$$
$$\iff x \in w_2.$$

Thus $w_1 = w_2$, showing that w is unique. We leave it as an exercise to show that w is inductive.

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

$$\mathbf{N} = \{ x \mid x \in v \text{ for every inductive set } v \}$$
$$= \{ 0, 1, 2, 3 \cdots \}.$$

For $x, y \in \mathbf{N}$, we write $x < y$ when $x \in y$ and we write $x \leq y$ when $x < y$ or $x = y$.

1.34 Notation: For a formula F, we write $\forall x \in u\, F$ as a shorthand notation for the formula $\forall x \left(x \in u \to F \right)$. Similarly, we write $\exists x \in u\, F$ as a shorthand notation for $\exists x \left(x \in u \wedge F \right)$.

1.35 Theorem: *(Principle of Induction) Let $F(x)$ be a formula with free variable x. Suppose that*

(1) $F(0)$, and
(2) $\forall x \in \mathbf{N} \left(F(x) \to F(x + 1) \right)$.
Then $\forall x \in \mathbf{N}\ F(x)$.

Proof: Let $u = \{ x \in \mathbf{N} \mid F(x) \}$. By (1) we have $0 \in u$. Let $x \in u$. Then $x \in \mathbf{N}$ and $F(x)$. Since $x \in \mathbf{N}$ we have $x + 1 \in \mathbf{N}$ (since $\mathbf{N}$ is inductive). Since $x \in \mathbf{N}$ and $F(x)$ we have $F(x + 1)$ by (2). Since $x + 1 \in \mathbf{N}$ and $F(x + 1)$, we have $x + 1 \in u$ (by the definition of u). We have shown that $0 \in u$ and that $\forall x \left(x \in u \to x + 1 \in u \right)$, so u is inductive. Since u is inductive, we have $\mathbf{N} \subseteq u$ (by the definition of $\mathbf{N}$). Thus $x \in \mathbf{N} \implies x \in u \implies F(x)$.

1.36 Remark: In the above theorem, the expression $F(0)$ is short for $\forall x \left(x = 0 \to F(x) \right)$ which in turn is short for $\forall x \left(\forall y \neg y \in x \to F(x) \right)$. Similarly, $F(x + 1)$ is short for the formula $\forall y \left(y = x + 1 \to F(y) \right)$, where $F(y) = \left[F(x) \right]_{x \mapsto y}$.

1.37 Definition: Given a formula $F(x, y)$ with free variables x and y, the following formula is an axiom:

$$\forall u \Big(\forall x \, \exists! y \; F(x, y) \to \exists w \, \forall y \, \big(y \in w \leftrightarrow \exists x \in u \; F(x, y) \big) \Big),$$

where $\exists! y F(x, y)$ is short for $\exists y \big(F(x, y) \wedge \forall z \, \big(F(x, z) \to z = y \big) \big)$ with $F(x, z)$ short for the formula $\forall y \, \big(y = z \to F(x, y) \big)$. More generally, given a formula $F(x, y, u_1, \cdots, u_n)$ with free variables $x, y, u_1, \cdots, u_n$, the following formula is an axiom:

$$\forall u \, \forall u_1 \cdots \forall u_n \Big(\forall x \, \exists! y \; F(x, y, u_1, \cdots, u_n) \to \exists w \, \forall y \, \big(y \in w \leftrightarrow \exists x \in u \; F(x, y, u_1, \cdots, u_n) \big) \Big).$$

An axiom of this form is called a **Replacement Axiom**.

1.38 Notation: Given sets $u, u_1, \cdots, u_n$ and given a formula $F(x, y, u_1, \cdots, u_n)$ with free variables $x, y, u_1, \cdots, u_n$ with the property that $\forall x \, \exists! y \; F(x, y, u_1, \cdots, u_n)$, for each set x we let $y = f(x)$ denote the unique set for which $F(x, y, u_1, \cdots, u_n)$ holds, and then we denote the unique set w, whose existence is stipulated by the above Replacement Axiom, by

$$\big\{ f(x) \big| x \in u \big\}.$$

1.39 Example: If u is a set then the collection

$$\big\{ \mathcal{P}(x) \big| x \in u \big\}$$

is also a set, by the Replacement Axiom taking $F(x, y)$ to be the formula $y = \mathcal{P}(x)$.

1.40 Definition: The **Axiom of Choice** is the formula given by

$$\forall u \Big(\big(\neg \phi \in u \wedge \forall x \in u \, \forall y \in u \, (\neg x = y \to x \cap y = \emptyset) \big) \to \exists w \, \forall v \in u \, \exists! \, x \in v \; x \in w \Big)$$

Relations, Equivalence Relations, Functions and Recursion

1.41 Remark: We have now stated each of the ZFC axioms formally. Up until now, we have used lower-case letters to denote all sets (and all elements of sets, which are also sets). From now on, we shall often use upper-case letters to denote sets, as is more customary.

1.42 Definition: 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 pais. For a binary relation R, we usually write xRy instead of $(x, y) \in R$.

1.43 Definition: Let R and S be binary relations. The **domain** of R is

$$\mathrm{Domain}(R) = \{x \,|\, \exists y \; xRy\}$$

and the **range** of R is

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

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 composite S **composed with** R is

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

1.44 Theorem: *Let A be a set and let R and S be binary relations. Then*

(1) $\mathrm{Domain}(R)$, $\mathrm{Range}(R)$, $R(A)$ and $R^{-1}(A)$ are sets, and
(2) R^{-1} and $S \circ R$ are binary relations.

Proof: The proof is left as an exercise.

1.45 Definition: An **equivalence relation** on a set X is a binary relation R on X such that

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

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

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

1.47 Definition: 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) for all $A \in S$ we have $A \neq \emptyset$,
(2) for all $A, B \in S$, if $A \neq B$ then $A \cap B = \emptyset$, and
(2) $\bigcup S = X$.

1.48 Theorem: *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

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

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

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

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

Proof: The proof is left as an exercise.

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

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

1.50 Definition: 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.

1.51 Remark: The Axiom of Choice is equivalent to the statement that every equivalence relation has a set of representatives.

1.52 Definition: Given 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

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

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

1.53 Definition: Let $f : X \to Y$. 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

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

1.54 Definition: Let $f : X \to Y$. Let I_X and I_Y denote the identity functions on X and Y respectively (that is $I_X(x) = x$ for all $x \in X$ and $I_Y(y) = y$ for all $y \in Y$). A **left inverse** of f is a function $g : Y \to X$ such that $g \circ f = I_X$. A **right inverse** of f is a function $h : Y \to X$ 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.

1.55 Theorem: *Let $f : X \to Y$. 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.

Proof: The proof is left as an exercise. We remark that the Axiom of Choice is needed.

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

1.57 Remark: The Axiom of Choice is equivalent to the statement that for every set S, there exists a function $f : S \to \bigcup S$ with the property that $\forall X \in S \left(X \neq \emptyset \to f(X) \in X \right)$. Such a function f is called a **choice function** for the set S.

1.58 Theorem: *(The Recursion Theorem)*

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

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

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

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

Proof: To prove part (1), note first that for each $n \in \mathbf{N}$ we can construct a (unique) function $f_n : \{0, 1, \cdots, n\} \to A$ such that $f(0) = a$ and $f_n(k+1) = g\big(f_n(k), k\big)$ for all k with $0 \leq k < n$ (that the functions f_n exist and are unique can be proven by induction). Notice that since $\{0, 1, \cdots, n\} = n+1$, we have $f_n : (n+1) \to A$, so $f_n \subseteq (n+1) \times A \subseteq \mathbf{N} \times A$, and so all of the functions f_n are subsets of $\mathbf{N} \times A$. We can combine all these functions into a single function $f : \mathbf{N} \to A$ as follows. First we let

$$F = \left\{ f \subseteq \mathbf{N} \times A \,\middle|\, \exists n \in \mathbf{N}\Big(f : (n+1) \to A \,,\ f(0) = a \,,\ \forall k \in (n+1)\ f(k+1) = g\big(f(k), k\big)\Big) \right\},$$

and then we let

$$f = \bigcup F.$$

We leave it as an exercise to prove that indeed f is a function which satisfies the conditions of the theorem.

We can prove part (2) in a similar manner. First we let

$$F = \Big\{ f \subseteq A \times \mathbf{N} \times B \,\Big|\, \exists n \in \mathbf{N}\Big(f : A \times (n+1) \to B \text{ and}$$

$$\forall a \in A\Big(f(a, 0) = g(a) \,\wedge\, \forall k \in (n+1)\ f(a, k+1) = h\big(a, f(a, k), k\big)\Big)\Big) \Big\},$$

then we let $f = \bigcup F$.

The Construction of the Integers, Rational, Real and Complex Numbers

1.59 Definition: By part (2) of the Recursion Theorem, there is a unique function $s : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ such that for all $a, b \in \mathbf{N}$ we have

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

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

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

Also, there is a unique function $p : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ such that for all $a, b \in \mathbf{N}$ 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 $\mathbf{N}$, and we write it as

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

1.60 Remark: It can be shown (using induction) that the sum and product satisfy all the usual properties in $\mathbf{N}$.

1.61 Definition: We define the set of **integers** to be the set

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

where R is the equivalence relation given by

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

For $a, b, c, d \in \mathbf{N}$, we define

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

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

1.62 Remark: It can be shown that the ordering and the sum and product defined above are well-defined and satisfy the usual properties in $\mathbf{Z}$.

1.63 Definition: We define the set of **rational numbers** to be the set

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

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

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

For $a, b, c, d \in \mathbf{Z}$ with $b, d > 0$, we define

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

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

1.64 Remark: It can be shown that the above ordering, sum and product are well-defined and satisfy the usual rules in $\mathbf{Q}$.

1.65 Definition: We define the set of **real numbers** to be the set

$$\mathbf{R} = \big\{ u \subseteq \mathbf{Q} \,\big|\, u \neq \emptyset \,,\; u \neq \mathbf{Q} \,,\; \forall a \in u \; \forall x \in \mathbf{Q} \; (x \leq a \rightarrow x \in u) \,,\; \forall a \in u \; \exists b \in u \; a < b \big\} \,.$$

For $u, v \in \mathbf{R}$, we define

$$u \leq v \Longleftrightarrow u \subseteq v$$
$$u + v = \big\{ a + b \,\big|\, a \in u \,,\; b \in v \big\} \,.$$

We define $0 \in \mathbf{R}$ to be the set $0 = \{ x \in \mathbf{Q} \,|\, x < 0 \text{ in } \mathbf{Q} \}$. Given $u \in \mathbf{R}$ we define $-u$ to be the interior of the complement of $\{ -a \,|\, a \in u \}$, that is

$$-u = \big\{ b \in \mathbf{Q} \,\big|\, \exists\, r \in \mathbf{Q} \text{ with } r > 0 \text{ such that } -(b + r) \notin u \big\}$$

and we define

$$|u| = \begin{cases} u & \text{if } 0 \leq u, \\ -u & \text{if } u \leq 0. \end{cases}$$

For $0 \leq u, v \in \mathbf{R}$ we define

$$u \cdot v = \big\{ a \cdot b \in \mathbf{Q} \,\big|\, 0 \leq a \in u \,,\; 0 \leq b \in v \big\} \cup \big\{ c \in \mathbf{Q} \,\big|\, c < 0 \big\} \,,$$

and for any $u, v \in \mathbf{R}$ we define $u \cdot v = |u| \cdot |v|$. For $a \in \mathbf{C}$ we write $a = \big\{ x \in \mathbf{Q} \,\big|\, x < a \big\} \in \mathbf{R}$ and we identify $\mathbf{Q}$ with a subset of $\mathbf{R}$.

1.66 Remark: It can be shown that the above ordering, sum and product are well-defined and satisfy the usual rules in $\mathbf{R}$.

1.67 Definition: We define the set of **complex** numbers to be the set

$$\mathbf{C} = \mathbf{R} \times \mathbf{R} \,.$$

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

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

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

1.68 Remark: It can be shown that the above sum and product are well-defined and satisfy the usual rules in $\mathbf{C}$.