Foundations of Mathematics I
Set Theory
(only a draft)

Ali Nesin
Mathematics Department
Istanbul Bilgi University
Kuştepe Şişli
Istanbul Turkey
anesin@bilgi.edu.tr

February 12, 2004

Contents

Part I

Naive Set Theory

This part is about naive set theory, as opposed to axiomatic set theory that will be the subject of the next part. Naive set theory does not care so much about the definition or the existence of a set; on the contrary, in the axiomatic set theory our primary concern will be the existence of a set.

Here, in this part, we will accept the concept of a "set" without defining it; further we will assume that any collection of mathematical objects is a set, whatever this means. Going even further, we will assume that the natural numbers such as 0, 1, 2, integers such as -2, -4, rational numbers such as $3/5$, $-6/5$ and the real numbers such as $\sqrt{2}$, π, π^π exist and that the reader is familiar with the basic operations of $+$ and $\times$ performed with them. In other words we assume all that has been taught in elementary school, mid-school and high school.

In the next part we will define all mathematical objects carefully (this means mathematically). We will prove that all the mathematical objects that are defined are in fact sets. To prove that these objects are sets, we will use axioms of set theory, that we will define. But for the moment we are away from this realm and we work intuitively, without asking the question of existence.

Chapter 1

Basic Concepts and Examples

1.1 Sets, Subsets and Emptyset

A **set** is just a collection of objects[1]. The objects of the collection that form the set are called the **elements** of the set.

One should be aware of the fact that there is nothing that prevents a set from being an element of another set. Indeed, as we will see in the next part, not only every element is a set, but that everything is a set!

An element of a set is sometimes called a **member** of the set.

If X is a set, to express the fact that x is an element of X, we write $x \in X$. If x is not an element of the set X, we write $x \notin X$.

For example, there is a set whose elements are just 0, 1 and 2; we denote this set by $\{0, 1, 2\}$. Clearly $2 \in \{0, 1, 2\}$, but[2] $3 \notin \{0, 1, 2\}$. In general, a set that has finitely many elements $x_1, \ldots, x_n$ is denoted by $\{x_1, \ldots, x_n\}$.

Conversely, given a finite number of n sets $x_1, \ldots, x_n$, we can form the set $\{x_1, \ldots, x_n\}$. The sets $x_1, \ldots, x_n$ are elements of the set $\{x_1, \ldots, x_n\}$.

In particular, if x is a set, we can form the set $\{x\}$ whose only element is x. We have $x \in \{x\}$. A set with only one element is called a **singleton**.

Two sets are called **equal** if they contain the same elements (and not if they have the same number of elements as some would say). For example $\{0\} \neq \{2\}$ because these two sets have different elements.

A set is called **finite** if it has finitely many elements. Otherwise we say that the set is **infinite**. A finite set cannot be equal to an infinite set. Also two finite sets that have different number of elements cannot be equal.

[1] Notice how loose and unprecise we are.

[2] To prove that $3 \notin \{0, 1, 2\}$, we need to show that $3 \neq 0$, $3 \neq 1$ and $3 \neq 2$. But to prove these inequalities we need to know the mathematical definitions of 0, 1, 2 and 3. Since these numbers are not mathematically defined yet, we cannot prove for the moment that $3 \notin \{0, 1, 2\}$. We will do this in the next part. For the moment we **assume** that every natural number is different from the rest.

The set $\{0, 1, 2, 3, \ldots\}$ is infinite.

In general, we have $x \neq \{x\}$ because the set $\{x\}$ has only one element, whereas the set x could have more than one element. Note that if $x = \{x\}$, then $x \in x$, i.e. x is an element of itself, a quite strange and unexpected phenomena, which will be forbidden by an axiom that will be introduced in the next part, in other words such an object will not be a set (it may be something else!)

The sets $\{x, x, y\}$, $\{x, y\}$ and $\{y, x\}$ are equal because they contain the same elements, namely x and y. This set has either one or two elements: It has one element if $x = y$, otherwise it has two elements. On the other hand the set $\{3, 5\}$ has exactly two elements because $3 \neq 5$ (as we will prove in the second part of our book once we know what these objects are).

It would be interesting to know what the reader things about the equality $2 = \{0, 1\}$. Does it hold or not? It all depends on the definition of 2. As we will see in the next part, the integer 2 will be defined as the set $\{0, 1\}$, so that the equality $2 = \{0, 1\}$ does indeed hold. But we will not go into these fine points of set theory in this part.

The number of elements of a set X is denoted by $|X|$. Thus $|\{0, 1, 2\}| = 3$, $|\{0, 1, 2, 3, \ldots\}| = \infty$ and $1 \leq |\{x, y\}| \leq 2$. The set $\{x, y\}$ has always at least one element.

Here is another set: $\{\{0, 1, 2\}, \{2, 3, 6\}\}$. This set has just two elements, namely $\{0, 1, 2\}$ and $\{2, 3, 6\}$. The two elements $\{0, 1, 2\}$ and $\{2, 3, 6\}$ of this set are sets themselves and each have three elements.

A set x is called a **subset** of another set y if every element of x is also an element of y. We then write $x \subseteq y$. In this case, one sometimes says that y is a **superset** of x.

For example, the set $\{0, 2, 3\}$ is a subset of the set $\{0, 1, 2, 3, 4\}$ because each one of the elements of the first one appears in the second one. But the set $\{0, 2, 3\}$ is not an element of the set $\{0, 1, 2, 3, 4\}$ unless $\{0, 2, 3\}$ is equal to one of 0, 1, 2, 3, 4 (which is not the case as we will see in the next part).

Another example: The set of even integers is a subset of the set of integers divisible by 6.

We will refrain from giving non mathematical examples such as "the set of pupils in your class is a subset of the set of pupils of your school".

Another (mathematical) example: The set $\{0, 1\}$ is a subset of $\{0, 1, 2\}$. This is clear. Is it an element? No if the set $\{0, 1\}$ is not equal to one of 0, 1 and 2. Unfortunately, the way we will define numbers in the second part of the book, 2 is equal to the set $\{0, 1\}$; therefore $\{0, 1\}$ is also an element of $\{0, 1, 2\}$. But the reader is not supposed to know these fine points at this stage and may as well suppose that $\{0, 1\}$ is not an element of $\{0, 1, 2\}$. Anyway, we will try to convince the reader in the second part that the definition of 2 as the set $\{0, 1\}$ is in some sense arbitrary.

Clearly every set is a subset of itself. Thus for all sets x, we have $x \subseteq x$.

We also note the following fact which is used very often in mathematics: Two sets x and y are equal[3] if and only if $x \subseteq y$ and $y \subseteq x$. This means that

[3]Here we act as if we know what the equality means, because we are doing intuitive set

two sets are equal if they have the same elements, i.e. if an element of one of them is an element of the other and vice versa.

If $x \subseteq y$ and $x \neq y$, then we write $x \subset y$. For example, $\{0, 3\} \subset \{0, 2, 3, \pi\}$.

If the set x is not a subset of the set y, we write $x \not\subseteq y$. For example, $\{\pi\} \not\subseteq \{3.14, 3.14159, 22/7\}$.

The statement of our first theorem must be well known by the reader, but its proof may not be so well known. In fact the proof is very interesting and we urge the reader to digest it well.

Theorem 1.1.1 *A set with no elements is a subset of every set.*

Proof: Let $\emptyset$ be a set with no elements[4]. Let x be any set. Assume $\emptyset$ is not a subset of x. We will obtain a contradiction, proving that $\emptyset$ is a subset of x. Since $\emptyset$ is not a subset of x, by the very definition of the concept of "subset", there is an element in $\emptyset$ which is not in x. But $\emptyset$ has no elements. Thus $\emptyset$ cannot have an element which is not in x. Hence $\emptyset \subseteq x$. □

Corollary 1.1.2 *There is at most one set without elements.*

Proof: Let $\emptyset_1$ and $\emptyset_2$ be two sets with no elements. By the theorem above, $\emptyset_1 \subseteq \emptyset_2$ and $\emptyset_2 \subseteq \emptyset_1$. Hence $\emptyset_1 = \emptyset_2$. □

A set that has no elements at all is called **emptyset** and is denoted by $\emptyset$. As we have seen in the Corollary above there is only one set with no elements[5].

Here we list all the subsets of the set $\{0, 1, 2\}$:

$$\emptyset$$
$$\{0\}$$
$$\{1\}$$
$$\{2\}$$
$$\{0,\ 1\}$$
$$\{0,\ 2\}$$
$$\{1,\ 2\}$$
$$\{0,\ 1,\ 2\}$$

The **set of subsets** of a set X is denoted by $\wp(X)$. Thus the set $\wp(\{0, 1, 2\})$ has the eight elements listed above.

Theorem 1.1.3 *If $|X| = n$ is finite then $|\wp(X)| = 2^n$.*

---

theory. In the second part, in some sense, the equality will be defined so as to satisfy this property.

[4]We do not know yet that there is only one set with no elements. We will prove it right after this theorem.

[5]In fact, all we have shown in the Corollary is that a set with no elements is unique **in case there is such a set**. In the next part one of our axioms will state that there is a set with no elements. This fact cannot be proven, so either the existence of such a set or a statement implying its existence must be accepted as an axiom.

Proof: Assume $|X| = n$. To form a subset of X, we must decide which elements are in the subset, i.e. for each element of X we must give a decision "yes" or "no". Since there are n elements in X and since for each element there are two possible decisions "yes" or "no", there are 2^n possible subsets of X. □

Exercises.

i. Let $X = \{0, 1\}$. List the elements of $\{\wp(A) : A \in \wp(X)\}$.

ii. Let $X = \emptyset$. List the elements of $\{\wp(A) : A \in \wp(X)\}$.

iii. Show that $\emptyset \neq \{\emptyset\}$.

iv. Write the 16 elements of $\wp(\wp(\{0, 1\}))$.

v. Show that $\wp(\emptyset) = \{\emptyset\}$.

vi. Show that $\wp(\wp(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.

vii. Find $\wp(\wp(\wp(\emptyset)))$.

viii. Find a set X with an element x such that $x \in X$ and $x \subseteq X$.

ix. Can we have $x \subseteq \{x\}$? **Answer:** According to the definition, $x \subseteq \{x\}$ if and only if any element of x is an element of $\{x\}$, and this means that any element of x (if any) is x. This implies that either $x = \emptyset$ or $x = \{x\}$. This last possibility is quite curious, and, mush later in the book will be forbidden with the help of an axiom. We do not want a set to have itself as an element, because we feel that to define and to know a set we need to know its elements, so that if $x \in x$ then to know x we need to know its element x!

x. Suppose $x = \{x\}$. Find $\wp(x)$. Is $x \subseteq \wp(x)$? Find $\wp(\wp(x))$. Is $x \subseteq \wp(\wp(x))$?

xi. Show that $X = \emptyset$ satisfies the following formula: "for every $x \in X$, x is a subset of X".

xii. Can you find a set $X \neq \emptyset$ such that for every $x \in X$, x is a subset of X?

xiii. Show that $X \subseteq Y$ if and only if $\wp(X) \subseteq \wp(Y)$.

xiv. Show that if $X \subseteq Y$ then $\wp(X) \in \wp(\wp(Y))$.

xv. Show that for any set X, $\{\emptyset\} \in \wp(X)$ if and only if $\emptyset \in X$.

xvi. Show that for any set X, $\{\emptyset\} \in \wp(\wp(X))$.

xvii. Show that for any set X, $\{\emptyset\} \in \wp(\wp(\wp(\wp(\wp(X)))))$.

xviii. Show that for any set X, $\{X\} \in \wp(\wp(X))$.

xix. Show that for any set X, $\{\{\emptyset\}, \{\{X\}\}\} \in \wp(\wp(\wp(\wp(X))))$.

xx. Show that $\{\wp(A) : A \subseteq X\} \in \wp(\wp(\wp(X)))$.

xxi. Show that $\{\{x\}, \{x, y\}\} = \{\{z\}, \{z, t\}\}$ if and only if $x = z$ and $y = t$.

xxii. * Show that any element of $\emptyset$ is $\emptyset$. (Hint: See Theorem 1.1.1 and its proof).

xxiii. * Have a philosophical discussion among your friends about whether we should allow the existence of a set x such that $x = \{x\}$.

xxiv. * Have a philosophical discussion among your friends about whether we should allow the existence of two sets x and y such that $x \in y$ and $y \in x$.

1.2 Notes on Formalism

Let us look at the definition of "subset" once again: $x \subseteq y$ *if and only if* every element of x is an element of y. Here, "if and only if" means that

if $x \subseteq y$ *then* every element of x is an element of y,

and

if every element of x is an element of y *then* $x \subseteq y$.

Some abbreviate the phrase "if and only if" by the symbol $\Leftrightarrow$ and write the sentence above in the following abbreviated form:

$x \subseteq y \Leftrightarrow$ every element of x is an element of y,

although it is a bad taste to use such symbols in print, or even in classroom or exams. Let us continue to abbreviate sentences in this way. Now consider the phrase

every element of x is an element of y.

We can rephrase this as

for all z, if z is an element of x then z is an element of y

and then as follows:

for all z, if $z \in x$ then $z \in y$.

Very often, mathematicians use the symbol
Rightarrow for "if ... then ...", i.e. instead of "if p then q" they write $p \Rightarrow q$. With this formalism, we can write the above phrase as

for all z, $z \in x \Rightarrow z \in y$.

That is not enough: "for all z" is abbreviated as $\forall z$. Now the phrase

every element of x is an element of y

becomes

$$\forall z\ (z \in x \Rightarrow z \in y).$$

Finally, the definition of "subset" can be written as

$$x \subseteq y \Leftrightarrow \forall z\ (z \in x \Rightarrow z \in y).$$

What we have above is really a short cut for the English sentence "x is a subset of y if and only if every element of x is an element of y", it is some kind of steno, a shorthand, as useful as "TGIF". Although it is convenient, we will refrain from using such abbreviations without any apparent reason, and we advice the young reader not to use such symbolism in their papers, unless they are asked to do so.

Since the above definition is for all sets x and y, we can write,

$$\forall x\, \forall y\ (x \subseteq y \Leftrightarrow \forall z\ (z \in x \Rightarrow z \in y)).$$

The fact that every set is a subset of itself is formalized by $\forall x\, x \subseteq x$.

Let us formalize the equality of two sets. As we know, two sets x and y are equal if and only if $x \subseteq y$ and $y \subseteq x$. Thus

$$x = y \Leftrightarrow (x \subseteq y \text{ and } y \subseteq x).$$

(The reader should note the need of parentheses). Instead of the word "and" we will write $\wedge$, thus we now have

$$x = y \Leftrightarrow (x \subseteq y \wedge y \subseteq x).$$

We can continue and replace $x \subseteq y$ with $\forall z\ (z \in x \Rightarrow z \in y)$ and $y \subseteq x$ with $\forall z\ (z \in y \Rightarrow z \in x)$. Thus

$$x = y \Leftrightarrow ((\forall z\ (z \in x \Rightarrow z \in y) \wedge (\forall z\ (z \in y \Rightarrow z \in x))).$$

A moment of thought will convince the reader that

$$(\forall z\ (z \in x \Rightarrow z \in y) \wedge (\forall z\ (z \in y \Rightarrow z \in x))$$

is equivalent to

$$\forall z\ ((z \in x \Rightarrow z \in y) \wedge (z \in y \Rightarrow z \in x)),$$

and that this one is equivalent to

$$\forall z\ (z \in x \Leftrightarrow z \in y).$$

Thus

$$x = y \Leftrightarrow \forall z\ (z \in x \Leftrightarrow z \in y).$$

Since this is true for all sets x and y, we have

$$\forall x\, \forall y\ (x = y \Leftrightarrow \forall z\ (z \in x \Leftrightarrow z \in y)).$$

Let us look at the meaning of $x \neq y$. By definition, $x \neq y$ if it is not true that $x = y$, i.e. if there is an element in one of the sets which is not in the other. Thus, $x \neq y$ if and only if

either there is an element in x which is not in y

or

there is an element in y which is not in z.

The first one, namely "there is an element in x which is not in y" means

there is a $z \in x$ such that $z \notin y$,

i.e.,

there is a z such that $z \in x \wedge z \notin y$.

We abbreviate "there is a z" by the symbols $\exists z$. Thus the phrase "there is an element in x which is not in y" is formalized by

$$\exists z(z \in x \wedge z \notin y).$$

Now $x \neq y$ is formalized by

$$\text{either } \exists z(z \in x \wedge z \notin y) \text{ or } \exists z(z \in y \wedge z \notin x).$$

Finally, the "either ... or ..." part is shortened by $\ldots \vee \ldots$, so that $x \neq y$ becomes equivalent to

$$(\exists z(z \in x \wedge z \notin y)) \vee (\exists z(z \in y \wedge z \notin x)).$$

A moment of reflection will show that this is equivalent to

$$\exists z((z \in x \wedge z \notin y) \vee (\exists z(z \in y \wedge z \notin x)).$$

What about the proposition that $x \subset y$, how is it formalized? By definition, $x \subset y$ if and only if $x \subseteq y$ and $x \neq y$. We know how to formalize $x \subset y$. What about $x \neq y$? By definition, $x \neq y$ if there is an element in one of them

To be completed... This subsection may have to go somewhere else.

1.3 Number Sets

Whole numbers such as 0, 1, 2, 3, 4, 5 are called **natural numbers**. The set

$$\{0, 1, 2, 3, 4, 5, \ldots\}$$

whose elements are natural numbers is denoted by the symbol $\mathbb{N}$. Thus

$$\mathbb{N} = \{0,\ 1,\ 2,\ 3,\ \ldots\}.$$

For example $5 \in \mathbb{N}$, but $-3 \notin \mathbb{N}$, $2/3 \notin \mathbb{N}$.

In the next part we will prove using our axioms that $\mathbb{N}$ is indeed a set, here in this part, we do not worry about such questions. Deep questions such as "what is 0?", "what is 1?", "is $\mathbb{N}$ a set?" will be asked and answered in the next part, not in this one.

We can add and multiply two natural numbers to obtain a third natural number, i.e. "$\mathbb{N}$ is closed under addition and multiplication". On the other hand substraction is not well-defined in $\mathbb{N}$, because for example $2-5$ is not a natural number. To subtract one natural number from another we need the negative of natural numbers as well.

Any natural number is an **integer**, as well as -3, -2, -1, which are not natural numbers. The set of integers is denoted by $\mathbb{Z}$. Thus

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

We have $-3, 5 \in \mathbb{Z}$, but $3/5 \notin \mathbb{Z}$. Clearly $\mathbb{N} \subset \mathbb{Z}$. We can add and multiply two integers, or subtract one integer from another to obtain a third integer. In other words, the set $\mathbb{Z}$ is closed under addition, multiplication and substraction. On the other hand division is not well-defined in $\mathbb{Z}$, because for example $2/5$ is not an integer. To divide one integer to another (nonzero) integer, we need to extend the number system to the set of rational numbers, where one can divide a number by a nonzero number.

Numbers such as $3/5$, $-10/7$ are called **rational numbers**. Thus every rational number is of the form a/b for some a and $b \in \mathbb{Z}$. But we have to assume that $b \neq 0$, because we cannot divide by 0, it is forbidden. The set of rational numbers is denoted by $\mathbb{Q}$. Thus

$$\mathbb{Q} = \{a/b : a, b \in \mathbb{Z} \text{ and } b \neq 0\}.$$

Now in the set $\mathbb{Q}$ we can add, multiply, subtract any two numbers. We can also divide one rational number to another nonzero rational number. Thus $\mathbb{Q}$ is closed under addition, multiplication, substraction, and division by nonzero elements.

By taking $b = 1$, we see that $\mathbb{Z} \subset \mathbb{Q}$.

Although the set of rational numbers looks like a perfect set to work with, it is not, because, there are "holes" in $\mathbb{Q}$, for example, one cannot solve the equation $x^2 = 2$ in $\mathbb{Q}$ as the next lemma shows:

Lemma 1.3.1 *There is no $q \in \mathbb{Q}$ such that $q^2 = 2$.*

Proof: Assume not. Let $q \in \mathbb{Q}$ be such that $q^2 = 2$. Let a, $b \in \mathbb{Z}$ be such that $q = a/b$. Simplifying if necessary, we may choose a and b so that they are not both divisible by 2. From $a^2/b^2 = (a/b)^2 = q^2 = 2$ we get $a^2 = 2b^2$. Thus a^2 is even. It follows that a is even (because the square of an odd number is always odd). Let $a_1 \in \mathbb{Z}$ be such that $a = 2a_1$. Now $4a_1^2 = (2a_1)^2 = a^2 = 2b^2$ and $2a_1^2 = b^2$. Hence b is even as well, a contradiction. □

Thus $2^{1/2} \notin \mathbb{Q}$ and $\mathbb{Q}$ is not closed under taking (rational) powers. To overcome this difficulty with the rational numbers, we have to extend the set $\mathbb{Q}$ of rational numbers to a larger set called the set of **real numbers** and denoted by $\mathbb{R}$. All rational numbers are real numbers. But also $\sqrt{2}$, π, $-\pi^\pi$, $(\pi^2+\pi)^{2/3}$ are real numbers. The intuitive feeling of the concept of real numbers is much less obvious and much weaker than that of the other numbers defined previously,

in fact ancient Greeks had some considerable difficulty before they became aware and recognized irrational numbers. In fact even after the Greeks became aware of the irrational numbers, they had a hard time to admit their existence, for example the Pythogarian school forbid its members from revealing it. Later on in this book, we will define each one of these concepts mathematically. Loosely speaking, we will obtain the set of real numbers by filling the "gaps" in $\mathbb{Q}$. But for the moment only an intuitive feeling is enough. The following may help the reader to gain further intuition: A positive real number can be regarded (or defined) as a distance on a straight line.

Although we know it is not and cannot be the case for most of our readers, in this part we assume that the reader is familiar with the set $\mathbb{R}$ of real numbers and the four operations performed with these numbers.

In $\mathbb{R}$ we can take any power of a nonnegative number. Unlike in $\mathbb{Q}$, there is a number, called $\sqrt{2}$, in $\mathbb{R}$ such that $\sqrt{2} > 0$ and $(\sqrt{2})^2 = 2$. We also have real numbers of the form $\sqrt{2}^{\sqrt{2}}$ and π^π. These operations will be defined mathematically in the next part.

We of course have, $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

In between $\mathbb{Z}$ and $\mathbb{R}$ there are other number sets closed under addition, substraction and multiplication. For example, the set

$$\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$$

is closed under addition, substraction and multiplication. On the other hand $\mathbb{Z}[\sqrt{2}]$ is not closed under division (by a nonzero element). But the set

$$\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

is closed under division (by a nonzero element). We leave this as an exercise to the reader.

Exercises and Examples.

i. Show that between any two rational numbers there is a rational number.

ii. Show that there is no smallest rational number > 0.

iii. Show that there are positive irrational numbers α and β such that α^β is rational. (Hint: If $\sqrt{2}^{\sqrt{2}}$ is rational, we are done. Otherwise consider $[\sqrt{2}^{\sqrt{2}}]^{\sqrt{2}}$.)

iv. Let $\epsilon > 0$ and $\alpha > 0$ be rational numbers. Show that there is an $n \in \mathbb{N}$ such that $n\epsilon > \alpha$.

v. Show that any nonempty subset of $\mathbb{Z}$ closed under substraction is the set of multiples of a given natural number n.

1.4 Subsets Defined By a Property

Given a set X, we may want to consider the collection of elements of X with a certain property. For example, we may take take X to be $\mathbb{N}$ and consider the collection of elements of $\mathbb{N}$ with the property of "being even". This new collection is "of course" a subset of $\mathbb{N}$. It is the set of all even natural numbers.

If we symbolize the property by P and abbreviate the fact that x has property P by $P(x)$, then we denote this set by

$$\{x \in X : P(x)\}.$$

For example, in the example above, the set of even natural numbers we obtained is written by

$$\{x \in \mathbb{N} : \ x \text{ is even}\}.$$

We may denote the same set as

$$\{2x : x \in \mathbb{N}\}.$$

We will abbreviate this set as $2\mathbb{N}$. Similarly, $2\mathbb{Z}$ will denote the set of even integers. For $r \in \mathbb{R}$, the definitions of the sets $r\mathbb{N}$, $r\mathbb{Z}$, $r\mathbb{Q}$ should be clear. For example,

$$r\mathbb{Q} := \{rq : q \in \mathbb{Q}\} = \{s \in \mathbb{R} : s = rq \text{ for some } q \in \mathbb{Q}\}.$$

Intervals. For a real number a, consider the set

$$\{s \in \mathbb{R} : s > a\}.$$

This set is denoted by (a, ∞). Similarly for two real numbers a and b we define the following sets:

$$\begin{array}{lcl}
(a,b) & = & \{x \in \mathbb{R} : a < x < b\} \\
(a,b] & = & \{x \in \mathbb{R} : a < x \leq b\} \\
[a,b) & = & \{x \in \mathbb{R} : a \leq x < b\} \\
[a,b] & = & \{x \in \mathbb{R} : a \leq x \leq b\} \\
(a,\infty) & = & \{x \in \mathbb{R} : a < x\} \\
[a,\infty) & = & \{x \in \mathbb{R} : a \leq x\} \\
(-\infty,a) & = & \{x \in \mathbb{R} : x < a\} \\
(-\infty,a] & = & \{x \in \mathbb{R} : x \leq a\} \\
(-\infty,\infty) & = & \mathbb{R}
\end{array}$$

These sets are called **intervals**[6]. We also denote the intervals $(0, \infty)$ and $[0, \infty)$ by $\mathbb{R}^{>0}$ and $\mathbb{R}^{\geq 0}$ respectively.

[6]The reader should be aware that we did not define an object called "infinity" or ∞ here. We just denoted some subsets with the help of the symbol ∞. We did not use the symbol ∞ in the definition of these subsets, we just used it in the names of the subsets as a meaningless symbol.

Exercises.

i. Show that if $b \leq a$ then $(a, b) = \emptyset$.

ii. Find the elements of the set $\{x \in \mathbb{R} : x > n \text{ for all } n \in \mathbb{N}\}$.

iii. Find the set $\{x \in \mathbb{R} : x^2 \in (0, 1)\}$.

1.5 Sets of Sets

We recall that the set of all subsets of a set X is denoted by $\wp(X)$. Here, in this section, we will see some other examples of sets whose elements are sets. There will be no theorems or results, just a few examples to make the reader more comfortable with large sets of sets. All our examples will be subsets of $\wp(X)$ for some set X defined by a certain property as in the last section.

Examples.

i. The collection of all sets of the form (r, ∞) for $r \in \mathbb{R}$ is a set. We denote it as $\{(r, \infty) : r \in \mathbb{R}\}$. Naming X this set, we have

$$\begin{array}{l} (5, \infty) \in X \\ 7 \notin X \\ 7 \in (5, \infty) \in X \\ \emptyset \notin X \\ \mathbb{R} \notin X \\ [5, \infty) \notin X \end{array}$$

ii. For a natural number n, define $A_n := \{n, n + 1, \ldots, 2n\}$. Thus

$$\begin{array}{l} A_0 = \{0\} \\ A_1 = \{1, 2\} \\ A_2 = \{2, 3, 4\} \\ A_3 = \{3, 4, 5, 6\} \end{array}$$

Consider the set whose elements are all these sets A_0, A_1, A_2, A_3, ... This set is denoted as

$$\{A_n : n \in \mathbb{N}\}.$$

iii. We may consider the set of subsets X of $\mathbb{R}$ such that $(-\epsilon, \epsilon) \subseteq X$ for some $\epsilon \in \mathbb{R}^{>0}$. This set will be written as

$$\{X \subseteq \mathbb{R} : \text{ for some } \epsilon \in \mathbb{R}^{>0}, (-\epsilon, \epsilon) \subseteq X\}.$$

Exercises.

i. Let X be a finite set with n elements. Find the number of elements of the set $\{A \in \wp(X) : |A| = n - 1\}$.

ii. Let X be a finite set with n elements. Find the number of elements of the set $\{A \in \wp(X) : |A| \text{ is even}\}$.

iii. Let X be a finite set with n elements. Find the number of elements of the set $\{A \in \wp(X) : |A| \text{ is divisible by } 3\}$.

iv. Let U be the set of subsets X of $\mathbb{R}$ such that for some $\epsilon \in \mathbb{R}^{>0}$, $(-\epsilon, \epsilon) \subseteq X$.

Let V be the set of subsets X of $\mathbb{R}$ such that for some $\epsilon \in \mathbb{R}^{>0}$, $[-\epsilon, \epsilon] \subseteq X$.

Let W be the set of subsets X of $\mathbb{R}$ such that for some $\epsilon \in \mathbb{Q}^{>0}$, $(-\epsilon, \epsilon) \subseteq X$.

Show that $U = V = W$.

v. A subset U of $\mathbb{R}$ is called **open** if for any $x \in U$ there is an $\epsilon \in \mathbb{R}^{>0}$ such that $(x - \epsilon, x + \epsilon) \subseteq U$.

Show that a subset U of $\mathbb{R}$ is open if for any $x \in U$ there is an $\epsilon \in \mathbb{R}^{>0}$ such that $[x - \epsilon, x + \epsilon] \subseteq U$.

Show that $\emptyset$ is open.

Show that the intersection[7] of two open subsets is open.

Show that if $U \neq \emptyset$, $\mathbb{R}$ is open, then $\{x \in \mathbb{R} : x \notin U$ is not open.

vi. A subset U of $\mathbb{Q}$ is called **open** if it is the intersection with $\mathbb{Q}$ of an open subset of $\mathbb{R}$. Show that $\mathbb{Q}$ can be written as the union of two disjoint nonempty open subsets. Try to convince yourself that $\mathbb{R}$ does not have this property.

1.6 Parametrized Sets

The two sets defined in Examples i, page 21 and ii, page 21 are parametrized. For example the set (in fact the elements of the set) $\{A_n : n \in \mathbb{N}\}$ is (are) parametrized by natural numbers $n \in \mathbb{N}$.

Let us consider another example: Let X be any set. Consider the set Y whose elements are the set of all subsets of subsets of X. Thus each element of Y is of the form $\wp(A)$ for some subset A of X, i.e.

$$Y = \{\wp(A) : A \subseteq X\} = \{\wp(A) : A \in \wp(X)\}.$$

Here we parametrized the elements of Y by the elements of $\wp(X)$.

If X is any set, then setting $B_x = x$, we see that $X = \{B_x : x \in X\}$ and so every set is parametrized by itself!

[7] Term to be defined.

It is also possible to parametrize a singleton set $\{a\}$ by natural numbers. Indeed, for all $n \in \mathbb{N}$, define $C_n = a$. Then $\{a\} = \{C_n : n \in \mathbb{N}\}$ and the singleton set is parametrized by the infinite set $\mathbb{N}$.

Another mathematical jargon for "parametrized" is "indexed". If X is a set indexed by I, we say that I is the **index set** of X although the set I is far from being unique.

Sometimes, we may need two or more parameters. For example consider the set

$$\{(r, s) : r < 1 \text{ and } s > 2\}$$

of intervals. Here, each element of the set is parametrized by two real numbers r and s.

Sometimes, a set $\{x_i : i \in I\}$ indexed by I is denoted by $(x_i)_{i \in I}$ or by $(x_i)_i$ when the context is clear enough. Sometimes the indexed set $(x_i)_i$ is called a **family**.

Chapter 2

Operations with Sets

2.1 Difference

Let X and Y be two sets. We want to consider the set of elements of X which are not in Y, i.e. we want to consider the set $\{x \in X : x \notin Y\}$. This is the set of elements x of X with the property that $x \notin Y$. We denote this set by $X \setminus Y$.

For example $\{0, 2, 3, 5\} \setminus \{2, 5, 7, 8\} = \{0, 3\}$ and $\mathbb{N} \setminus 2\mathbb{N}$ is the set of odd natural numbers.

Clearly, for all sets x and y,

i. $x \setminus x = \emptyset$
ii. $x \setminus y \subseteq x$
iii. $x \setminus \emptyset = x$
iv. $x \setminus y = \emptyset$ if and only if $x \subseteq y$

If a set X is fixed once for all, for a subset Y of X, we write Y^c for $X \setminus Y$. Whenever we use the notation Y^c, we assume that the superset X is clear from the context. The set Y^c is called the **complement** of Y (in X).

Given a superset X, it is again clear that

i. $(Y^c)^c = Y$
ii. $X^c = \emptyset$
iii. $\emptyset^c = X$

2.2 Intersection

Given two sets X and Y we may want to consider the set of common elements of X and Y. This new set is called the **intersection** of X and Y and is denoted $X \cap Y$. For example if $X = \{0, 1, 2, 5, 8\}$ and $Y = \{1, 3, 5, 6\}$ then $X \cap Y = \{1, 5\}$.

Two sets that intersect in emptyset are called **disjoint**.

The following properties are well-known and we leave the proofs to the reader:

i. $x \cap x = x$
ii. $x \cap y \subseteq x$
iii. $x \cap y = y \cap x$
iv. $x \cap y = x$ if and only if $x \subseteq y$
v. $(x \cap y) \cap z = x \cap (y \cap z)$
vi. $x \cap \emptyset = \emptyset$
vii. $(x \setminus y) \cap (y \setminus x) = \emptyset$

Property (v) says that there is no need of parentheses when intersecting several sets. For example the sets $x \cap (y \cap (z \cap t))$ and $(x \cap y) \cap (y \cap t)$ are equal and they may be denoted by $x \cap y \cap y \cap t$.

We can also intersect infinitely many subsets. For example, we may want to consider all the common elements of the intervals $(-1/n, 1/n)$ for $n = 1, 2, 3, \ldots$ We denote this set as $\bigcap_{n=1,2,\ldots}(-1/n, 1/n)$ or as $\bigcap_{n=1}^{\infty}(-1/n, 1/n)$; it is the **intersection** of all the sets of the form $(-1/n, 1/n)$ for some nonzero natural number n. Incidentally, the reader should note that $\bigcap_{n=1}^{\infty}(-1/n, 1/n) = \{0\}$. Similarly

$$\bigcap_{n=1}^{\infty} [\,-1/n, 1/n) = \{0\}$$
$$\bigcap_{n=1}^{\infty} [\,-1/n, 1/n] = \{0\}$$
$$\bigcap_{n=1}^{\infty} [\,-1/n, \infty) = [0, \infty)$$
$$\bigcap_{n=1}^{\infty} (-1/n, \infty) = [0, \infty)$$
$$\bigcap_{n=1}^{\infty} (0, 1/n) = \emptyset$$
$$\bigcap_{n=1}^{\infty} (0, 1/n] = \emptyset$$
$$\bigcap_{n=1}^{\infty} [0, 1/n] = \{0\}$$

Another example: We may want to intersect all the sets of form (r, ∞) for $r \in \mathbb{R}$. We denote this set as $\bigcap_{r\in\mathbb{R}}(r, \infty)$. It should be clear that $\bigcap_{r\in\mathbb{R}}(r, \infty) = \emptyset$. Also, $\bigcap_{n\in\mathbb{N}}(n, \infty) = \emptyset$.

In general if $X = \{A_i : i \in I\}$ is a set indexed by the index set I and if each A_i is a set, then the intersection of all the sets in X is denoted by $\bigcap_{i\in I} A_i$.

If the set X is not given by an index set as above, we denote the intersection of all the elements of X by $\bigcap_{x\in X} x$ or sometimes by $\cap X$. Thus we have

$$y \in \cap X \text{ if and only if } y \in x \text{ for all } x \in X.$$

For reasons that will be clear in the next part, $\cap\emptyset$ is left undefined for the moment. The reader should only note for the moment that if in the definition

$$y \in \cap X \text{ if and only if } y \in x \text{ for all } x \in X$$

we take $X = \emptyset$, then we get

$$y \in \cap\emptyset \text{ if and only if } y \in x \text{ for all } x \in \emptyset$$

and, since the statement on the right hand side holds for all y, every y is in $\cap\emptyset$. (See also Exercise viii, page 28).

Exercises.

i. Show that for any set X, $\cap_{\wp}(X) = \emptyset$.

ii. Show that $x \setminus y = x$ if and only if $x \cap y = \emptyset$ and that $x \setminus y = \emptyset$ if and only if $x \subseteq y$.

iii. Show that $\bigcap_{n=1}^{\infty}(-1/n, 1 + 1/n) = [0, 1]$.

iv. Show that $\bigcap_{r<1}$ and $_{2<s}(r, s) = [1, 2]$.

v. Show that $\bigcap_{\epsilon>0}(-\epsilon, \epsilon) = \bigcap_{\epsilon>0}[-\epsilon, \epsilon] = \{0\}$.

2.3 Union

Given two sets x and y we may want to consider the set of elements which are either in x or in y. This new set is called the **union** of x and y and is denoted $x \cup y$. For example if $x = \{0, 1, 2, 5, 8\}$ and $y = \{1, 3, 5, 6\}$ then $x \cup y = \{0, 1, 2, 3, 5, 6, 8\}$.

We leave the proof of the following well-known properties to the reader:

$$\begin{array}{ll} i. & x \cup x = x \\ ii. & x \subseteq x \cup y \\ iii. & x \cup y = y \cup x \\ iv. & x \cup y = x \Leftrightarrow y \subseteq x \\ v. & (x \cup y) \cup z = x \cup (y \cup z) \\ vi. & x \cup \emptyset = x \end{array}$$

Property (v) says that the parentheses are not needed when intersecting several sets. For example the sets $x \cup (y \cup (z \cup t))$ and $(x \cup y) \cup (y \cup t)$ are equal and they may be denoted by $x \cup y \cup y \cup t$.

There are two famous relationships between $\cap$ and $\cup$ called De Morgan laws:

$$\begin{array}{ll} vii. & x \cap (y \cup z) = (x \cap y) \cup (x \cap z) \\ viii. & x \cup (y \cap z) = (x \cup y) \cap (x \cup z) \end{array}$$

We can also take the union of infinitely many subsets. For example, we may want to consider all the common elements of the intervals $(1/n, 1-1/n)$ for $n = 1, 2, 3, \ldots$ We denote this set as $\bigcup_{n=1,2,\ldots}(1/n, 1-1/n)$ or as $\bigcup_{n=1}^{\infty}(1/n, 1-1/n)$; it is the **union** of all the sets of the form $(1/n, 1-1/n)$ for some nonzero natural number n. The reader should prove that

$$\bigcup_{n=1}^{\infty}(1/n, 1 - 1/n) = (0, 1).$$

Similarly

$$\begin{array}{l} \bigcup_{n=1}^{\infty}[1/n, 1 - 1/n) = (0, 1) \\ \bigcup_{n=1}^{\infty}[1/n, 1 - 1/n] = (0, 1) \\ \bigcup_{n=1}^{\infty}[1/n, \infty) = (0, \infty) \\ \bigcup_{n=1}^{\infty}(1/n, \infty) = (0, \infty) \end{array}$$

Similarly, we may want to take the union of all the sets of form (r, ∞) for $r \in \mathbb{R}^{>0}$. We denote this set as $\bigcup_{r\in\mathbb{R}^{>0}}(r, \infty)$ or by $\bigcup_{r>0}(r, \infty)$ if there is no room for confusion. It is clear that $\bigcup_{r>0}(r, \infty) = (0, \infty)$.

In general if $X = \{A_i : i \in I\}$ is a set indexed by the index set I and if each A_i is a set, then the union of all the sets in X is denoted by $\bigcup_{i\in I} A_i$.

If the set X is not given by an index set as above, we denote the union of all the elements of X by $\bigcup_{x\in X} x$ or sometimes by $\cup X$. Thus we have

$$y \in \cup X \text{ if and only if there is an } x \in X \text{ such that } y \in x.$$

Lemma 2.3.1 $\cup\emptyset = \emptyset$.

Proof: Since the proposition "$y \in \cup X$ if and only if $y \in x$ for some $x \in X$" holds for all sets X, applying this to the particular case $X = \emptyset$, we get "$y \in \cup\emptyset$ if and only if $y \in x$ for some $x \in \emptyset$". Since there is no element x in $\emptyset$, there is no such y. Hence $\cup\emptyset = \emptyset$. □

Exercises.

i. For subsets A and B of a superset X, show that $(A \setminus B)^c = A^c \cup B$.

ii. Show that for any sets x, y, z,

$$\begin{aligned} &y \cap (x \setminus y) = \emptyset \\ &(x \cap y) \setminus z = (x \setminus z) \cap (y \setminus z) \\ &(x \setminus y) \setminus z = x \setminus (y \cup z) \end{aligned}$$

iii. Let $X \neq \emptyset$ be a set. Show that $\cap X \subseteq \cup X$.

iv. Find $\bigcup_{n\in\mathbb{N}}[n, n^2]$.

v. Find $\bigcup_{n\in\mathbb{N}}(n, n^2)$.

vi. Let X be any set and for $i \in I$ let $Y_i \subseteq X$. Show that $(\bigcup_i Y_i)^c = \bigcap_i Y_i^c$ and $(\bigcap_i Y_i)^c = \bigcup_i Y_i^c$.

vii. Show that for any set X, $\cup\wp(X) = X$.

viii. For a set X, suppose we define $\cap X$ (changing the previous definition) as follows:

$$y \in \cap X \text{ if and only if } y \in \cup X \text{ and } y \in x \text{ for all } x \in X.$$

Show that this coincides with the earlier definition if $X \neq \emptyset$ and that with the new definition, $\cap\emptyset = \emptyset$.

ix. Show that $\bigcup_{r>0}[r, \infty) = (0, \infty)$.

x. Show that for any set A and for any set X of sets, $(\bigcup_{x\in X} x)\setminus A = \bigcup_{x\in X}(x\setminus A)$.

xi. Let X and Y be two nonempty sets of subsets. Show that

$$\left(\bigcup_{x\in X} x\right) \cap \left(\bigcup_{y\in Y} y\right) = \bigcup_{x\in X,\, y\in Y} (x \cap y)$$
$$\left(\bigcap_{x\in X} x\right) \cup \left(\bigcap_{y\in Y} y\right) = \bigcap_{x\in X,\, y\in Y} (x \cup y)$$

xii. **Symmetric Difference.** For two sets X and Y define the symmetric difference of X and Y as follows: $X\Delta Y = (X \setminus Y) \cup (Y \setminus X)$. Show that for all sets X, Y, Z,

a) $X\Delta(Y\Delta Z) = (X\Delta Y)\Delta Z$.

b) $X\Delta Y = Y\Delta X$.

c) $X\Delta\emptyset = \emptyset\Delta X = X$.

d) $X\Delta X = \emptyset$.

2.4 Cartesian Product of Two Sets

We expect the reader knows from high school the parametrization of the plane $\mathbb{R} \times \mathbb{R}$ as pairs of real numbers (x, y): Any point P of the plane $\mathbb{R} \times \mathbb{R}$ is represented by two coordinates x and y and one writes $P = (x, y)$.

What is the pair (x, y)? What do we really mean by this notation? What is the mathematical object (x, y)? This is the subject of this subsection.

What counts in pure mathematics is not so much how the pair (x, y) is defined, but its properties that we need. From the pair (x, y) the only property we need is the following:

$$(x, y) = (z, t) \text{ if and only if } x = z \text{ and } y = t.$$

Accordingly, we would like to define the **pair** (x, y) in such a way that the above property holds.

The set $\{\{x\}, \{x, y\}\}$ has this property, i.e.,

$$\{\{x\}, \{x, y\}\} = \{\{z\}, \{z, t\}\} \text{ if and only if } x = z \text{ and } y = t.$$

(See Exercise xxi, page 15).

Accordingly, we define the pair (x, y) as the set $\{\{x\}, \{x, y\}\}$.

The "first" element x of the pair (x, y) is called its **first coordinate**, the "second" element y of the pair (x, y) is called its **second coordinate**.

For two sets X and Y, we define $X \times Y$ as the set of all pairs (x, y) for $x \in X$ and $y \in Y$. Thus

$$X \times Y = \{(x, y) : x \in X,\, y \in Y\}.$$

The set $X \times Y$ is called the **Cartesian product** of X and Y (in that order).

Lemma 2.4.1 *If X and Y are sets, then $X \times Y \subseteq \wp(\wp(X \cup Y))$.*

Proof: Let $x \in X$ and $y \in Y$ be any two elements. Clearly $x, y \in X \cup Y$. Therefore $\{x\}$ and $\{x, y\}$ are subsets of $X \cup Y$, and so $\{x\}$ and $\{x, y\}$ are elements of $\wp(X \cup Y)$. It follows that $\{\{x\}, \{x, y\}\}$ is a subset of $\wp(X \cup Y)$, and hence an element of $\wp(\wp(X \cup Y))$. Therefore $X \times Y \subseteq \wp(\wp(X \cup Y))$. □

Corollary 2.4.2 *If X and Y are sets, then $X \times Y$ is the set of elements $\alpha \in \wp(\wp(X \cup Y))$ such that there are $x \in X$ and $y \in Y$ for which $\alpha = \{\{x\}, \{x, y\}\}$. In other words, the set $X \times Y$ is a definable subset of $\wp(\wp(X \cup Y))$.*

Given three sets x, y and z, we can form (x, y) and (y, z) and then $((x, y), z)$ and $(x, (y, z))$. Unfortunately these two sets are not necessarily equal. We let (x, y, z) denote the first one of these. Later we will give a better definition of (x, y) and (x, y, z).

Exercises.

i. Write the elements of $((x, y), z)$.

ii. Can we ever have $((x, y), z) = (x, (y, z))$?

iii. If $|X| = n$ and $|Y| = m$, how many elements does $X \times Y$ have?

iv. Find $\cap(x, y)$, $\cup(x, y)$, $\cap \cap (x, y)$, $\cap \cup (x, y)$, $\cup \cap (x, y)$, $\cup \cup (x, y)$.

v. Find $((\cup \cup (x, y)) \setminus (\cup \cap (x, y))) \cup (\cap \cup (x, y))$.

vi. What is $X \times \emptyset$?

vii. Show that $\cup \cup (X \times Y) = X \cup Y$ if $X \neq \emptyset$ and $Y \neq \emptyset$.

viii. Suppose $A \subseteq A \times A$. What can you say about A?

ix. Show that $X \times Y = \emptyset$ if and only if one of X or Y is empty.

x. Show that $(X \cup Y) \times Z = (X \times Z) \cup (Y \times Z)$, $(X \cap Y) \times Z = (X \times Z) \cap (Y \times Z)$ and $(X \setminus Y) \times Z = (X \setminus Z) \cap (Y \setminus Z)$.

xi. Find similar equalities for $(\cup_i X_i) \times Z$ and $(\cap_i X_i) \times Z$.

Chapter 3

Functions

3.1 Functions

Loosely and naively speaking, a **function** or a **map** f from a set X into a set Y is a "rule" that assigns to **each** element x of X a **unique** element $f(x)$ of Y. Note that we highlighted the words "each" and "unique".

For example, the rule that assigns to a real number its square root is not a function because a negative number does not have a square root. The rule that assigns the elements x and $-x$ to an element $x \in \mathbb{R}$ is not a function either because a function must assign a unique element to each element.

On the other hand, a function may assign the same element of the set of arrival to two different elements of the domain. For example, to a real number x we can assign its square x^2 and get a function from $\mathbb{R}$ into $\mathbb{R}$. Although the element 1 is assigned to the elements 1 and -1, this does not prevent the squaring from being a function. As this example also shows, an element of the set of arrival is not necessarily assigned to an element of the domain, e.g. in this example, the element -1 is not assigned, since it is not a square.

The set X is called the **domain** of the function f, and the set Y is called the **arrival set** of f.

If f is a function from X into Y, very often we denote this fact as $f : X \longrightarrow Y$. The "rule" f may be made explicit by the notation $x \mapsto f(x)$.

If $A \subseteq X$ and $f : X \longrightarrow Y$ is a function, we let

$$f(A) = \{f(x) : x \in A\}$$

and we call this set the **image** or the **range** of A under f. The set $f(X)$ is called the **image** or the **range** of f

Given a function $f : X \longrightarrow Y$ and a set Y_1 that contains $f(X)$ as a subset, we can define **another** function $f_1 : X \longrightarrow Y_1$ by the rule used to define f. For each $x \in X$ we then have $f(x) = f_1(x)$ by the very definition of f_1. Although the two functions take the same values with the same input, i.e. although they are defined by the same rule, their arrival sets are distinct. (But their images

are the same set $f(X)$). We will differentiate f and f_1 and consider them as two different functions (but we may denote them by the same letter f). In other words, a function is more than a rule; the domain X and the arrival set Y are also parts of the definition of a function.

Two functions are equal if they have the same domain, the same arrival set and if they take the same value on any element of the domain. Thus two functions $f : X \longrightarrow Y$ and $g : X_1 \longrightarrow Y_1$ are equal if and only if $X = X_1$, $Y = Y_1$ and $f(x) = g(x)$ for all $x \in X$. In particular, two functions $f, g : X \longrightarrow Y$ are equal if and only if $f(x) = g(x)$ for all $x \in X$. For example the functions f and g from $\mathbb{R}$ into $\mathbb{R}$ defined by $f(x) = \sqrt{x^2}$ and $g(x) = |x|$ are equal.

The set of functions from X into Y will be denoted by $\mathrm{Func}(X, Y)$.

Examples and Definitions.

i. Let X be a set. Then there is a function $\mathrm{Id}_X : X \longrightarrow X$ that satisfies $\mathrm{Id}_X(x) = x$. The function $\mathrm{Id}_X : X \longrightarrow X$ is called the **identity function**.

ii. Let X and Y be two sets. For a fixed element $b \in Y$, the function that sends each element x of X to the element b of Y is called the **constant b function**.

iii. Let X, Y, Z be three sets. Let $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ be two functions. The function

$$g \circ f : X \longrightarrow Z$$

is defined by the rule

$$(g \circ f)(x) = g(f(x)).$$

Note that $f \circ g$ is not necessarily defined (unless $Z = X$) and even when it is, the equality $f \circ g = g \circ f$ may not hold.

We could define $f \circ g$ if $g(Y)$ were a subset of X, but we will not do it.

The function $g \circ f : X \longrightarrow Z$ is called the **composite** of f and g. The operation $\circ$ is called **composition**.

If $X = Y$ we may compose f with itself as many times as we wish. We denote $f \circ \ldots \circ f$ (n times) by f^n. Note that $f^{(n)} \circ f^{(m)} = f^{(n+m)} = f^{(m)} \circ f^{(n)}$.

iv. Let $f : X \longrightarrow Y$ be a function. Let $A \subseteq X$. Then there is a function $f_{|A} : A \longrightarrow Y$ such that $f(a) = f_{|A}(a)$ for all $a \in A$.

The function $f_{|A}$ is called the **restriction** of f to A.

v. Let X and Y be two sets. The functions $\pi_1 : X \times Y \longrightarrow X$ and $\pi_2 : X \times Y \longrightarrow Y$ given by $\pi_1(x, y) = x$ and $\pi_2(x, y) = y$ are called the first and second **projections** respectively.

Lemma 3.1.1 *Let X, Y, Z, T be sets and $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$ and $h : Z \longrightarrow T$ be three functions. Then,*

i. $h \circ (g \circ f) = (h \circ g) \circ f$. *(***Associativity***)*

ii. $f \circ \mathrm{Id}_X = f$ *and* $\mathrm{Id}_Y \circ f = f$.

Proof: i. Let $x \in X$. On the one hand $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$. On the other hand $((h \circ g) \circ f)(x) = ((h \circ g)(f(x)) = h(g(f(x)))$. Thus $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$ for all $x \in X$ and this means exactly that $h \circ (g \circ f) = (h \circ g) \circ f$.

ii. Left as an exercise. □

If f is a function from X into Y and $A \subseteq X$, we denote by $f(A)$ the set values of f at the elements of A. More formally,

$$f(A) := \{y \in Y : y = f(a) \text{ for some } a \in A\}.$$

We call $f(A)$ the **image** of A under f. If $B \subseteq Y$, $f^{-1}(B)$ is defined to be the set $f^{-1}(B) := \{x \in X : f(x) \in B\}$. It is called the **inverse image** of B under f

It is possible that both $A \in X$ and $A \subseteq X$ hold, e.g. X may be the set $\{0, 1, \{0, 1\}\}$ and $A = \{0, 1\}$, in which case the meaning of $f(A)$ is controversial depending whether we consider A as an element or as a subset of X. For example let X be as before, $Y = \{5, 6, 7\}$ and $f : X \longrightarrow Y$ be defined by

$$\begin{array}{lcl} f(0) & = & 5 \\ f(1) & = & 6 \\ f(\{0,1\}) & = & 7 \end{array}$$

In this case $f(A) = 7$ if we consider A as an element of X and $f(A) = \{f(0), f(1)\} = \{5, 6\}$ in case we consider A as a subset of X. Such situations occur rarely and when they occur we must just be careful.

Given a function $f : X \longrightarrow Y$, we define its **graph** to be the set of pairs $(x, f(x))$ for $x \in X$. More precisely the graph of the function f is

$$\mathrm{Gph}(f) = \{(x, y) \in X \times Y : y = f(x)\}.$$

The set $\mathrm{Gph}(f)$ has the following properties:

1. $\mathrm{Gph}(f) \subseteq X \times Y$,
2. For any $x \in X$ there is a unique $y \in Y$ such that $(x, y) \in \mathrm{Gph}(f)$.

Conversely let F be a set that satisfies the two properties above,

1. $F \subseteq X \times Y$,
2. For any $x \in X$ there is a unique $y \in Y$ such that $(x, y) \in F$.

Then we can define a function $f : X \longrightarrow Y$ such that $F = \mathrm{Gph}(f)$. Indeed, we can define $f : X \longrightarrow Y$ by the rule

$$f(x) = y \text{ if and only if } (x, y) \in F.$$

In the next section we will use this fact to give a more mathematical definition of a function.

Exercises. Below, f denotes a function.

i. How many functions are there from a set of n elements into a set of m elements?

ii. What can you say about the relationship between $f(A \setminus B)$ and $f(A) \setminus f(B)$?

iii. Show that $f(\emptyset) = \emptyset$. (Here $\emptyset$ is considered as a subset of the domain).

iv. Let $X = Y = \mathbb{N}$, and let us associate to a natural number x, the natural number $2x + 1$. If we denote by f this function, we have $f(x) = 2x + 1$. For example, $f(3) = 7$, $f(f(3)) = f(7) = 15$.

a. Find $f(\mathbb{N})$, $f(f(\mathbb{N}))$, $f(f(f(\mathbb{N})))$.

b. Find $f(f \ldots (f(\mathbb{N})) \ldots)$. (Here there are n f's. We denote this set by $f^n(\mathbb{N})$).

v. Let $f : X \longrightarrow Y$ be a function.

i. Show that if $(B_i)_i$ is a family of subsets of Y, then

$$f^{-1}(\bigcup_i B_i) = \bigcup_i f^{-1}(B_i),$$

and

$$f^{-1}(\bigcap_i B_i) = \bigcap_i f^{-1}(B_i)$$

and if $B \subseteq Y$ then $f^{-1}(B^c) = f^{-1}(B)^c$.

ii. Show that if $(A_i)_i$ is a family of subsets of X, then $f(\bigcup_i A_i) = \bigcup_i f(A_i)$, $f(\bigcap_i A_i) \subseteq \bigcap_i f(A_i)$.

iii. Find an example where the last inclusion fails to be an equality.

iv. If $A \subseteq X$ what is the relationship between $f(A^c)$ and $f(A)^c$?

vi. a) Find a function $f : \wp(\mathbb{N}) \longrightarrow \mathbb{N}$ such that if $x \in \wp(\mathbb{N}) \setminus \{\emptyset\}$ then $f(x) \in x$.

b) Find a function $f : \wp(\mathbb{Z}) \longrightarrow \mathbb{Z}$ such that if $x \in \wp(\mathbb{Z}) \setminus \{\emptyset\}$ then $f(x) \in x$.

c) Find a function $f : \wp(\mathbb{Q}) \longrightarrow \mathbb{Q}$ such that if $x \in \wp(\mathbb{Q}) \setminus \{\emptyset\}$ then $f(x) \in x$.

d) Find a function $f : \wp(\mathbb{R}) \longrightarrow \mathbb{R}$ such that if $x \in \wp(\mathbb{R}) \setminus \{\emptyset\}$ then $f(x) \in x$. (Don't even try!)

vii. Let X and Y be two sets. Find a set Z such that the map $f : \wp(X) \times \wp(Y) \longrightarrow Z$ defined by $f(A, B) = A \times B$ is a function. (One may just take $Z := \{A \times B : A \in \wp(X), B \in \wp(Y)\}$. But we want something better. Try to define Z in terms of X and Y using only the set theoretic operations like $\cup$, $\cap$, $\wp$).

3.2 More On Functions

To define a function $f : X \longrightarrow Y$, we said that we need the two sets X and Y and a "rule" that assigns to each element of X a unique element of Y. This is a very loose definition, not acceptable by mathematical standards, because we did not define what we mean by a "rule". In fact, a function is not defined the way we defined it in the previous section. Mathematically, a function is a set of the form (X, Y, F) such that[1] X and Y are two sets and F is a subset of $X \times Y$ that satisfies the following property:

$$\text{For any } x \in X \text{ there is a unique } y \in Y \text{ such that } (x, y) \in F.$$

Then our "rule" $f(x) = y$ is defined by

$$f(x) = y \text{ if and only if } (x, y) \in F.$$

Exercises.

i. With the new definition of a function given above, given two functions (X, Y, F) and (Y, Z, G) define their composite $(X, Y, F) \circ (Y, Z, G)$.

ii. Let (X, Y, F) be a function. Show that the set X is uniquely determined by Y and F. In other words if (X, Y, F) and (X_1, Y, F) are functions, then $X = X_1$. This exercise shows that a function may be defined only as a pair (Y, F) such that for every x there is a unique $y \in Y$ such that $(x, y) \in F$.

3.3 Binary Operations

Let X be a set. A function $f : X \times X \longrightarrow X$ is sometimes called a **binary operation**. For x, $y \in X$, instead of $f(x, y)$ it is customary to write $x \star y$, $x \cdot y$, $x + y$, $x \bigodot y$, $x \otimes y$ etc. or even as xy. If it does not have a specific name, the outcome $x \star y$ may be called the **product** of the two elements x and y. A set X with a binary operation $\star$ on it is denoted by $(X, \star)$ most of the time.

Examples.

i. Let $X = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ or $\mathbb{R}$. The addition and multiplication are binary operations on X. If $X = \mathbb{Z}, \mathbb{Q}$ or $\mathbb{R}$ then substraction $-$ is a binary operation on X. If $X = \mathbb{Q} \setminus \{0\}$ or $\mathbb{R} \setminus \{0\}$ then division is a binary operation on X.

ii. Let X be a set. Then $\cap$, $\cup$, $\setminus$, Δ are binary operations on $\wp(X)$.

[1] Recall that (X, Y, F) stands for $((X, Y), F)$.

Potential Properties of Binary Operations. Let $\star$ be a binary relation defined on a set X.

i. **Associativity.** If $(x \star y) \star z = x \star (y \star z)$ for all x, y, $z \in X$, then we say that $\star$ is associative. Associativity means that the parentheses are useless when taking the product of several elements. If associativity does not hold, even the products $(x \star x) \star x$ and $x \star (x \star x)$ may be different, in which case we may have difficulties defining x^3.

When a binary operation is associative, the product of three (or even more) elements x, y and z (in that order) may be denoted as $x \star y \star z$ without parentheses.

Almost all the interesting mathematical binary operations are associative and if they are not, most of the time there is a close relationship between $(x \star y) \star z$ and $x \star (y \star z)$.

ii. **Commutativity.** If $x \star y = y \star x$ for all x, $y \in X$, then we say that $\star$ is commutative.

iii. **Identity Element.** If $e \in X$ is such that $x \star e = x$ for all $x \in X$, then we say that e is a right identity element for $\star$. Left identity is defined similarly. An element which is both left and right identity element is called an identity element of the binary operation $\star$.

If e is a left identity and f is the right identity, then $e = f$, because $f = e \star f = e$. It follows that if X has a left and right identity element, then it has an identity element and this identity element is unique.

iv. **Inverse Element.** Assume X has an identity element, say e. Let $x \in X$. If there is a $y \in X$ such that $x \star y = e$, then y is called a right inverse of x. Left inverse is defined similarly. If $\star$ is associative and if $x \in X$ has both a left inverse y and a right inverse z, then $x = z$, because, $y = y \star e = y \star (x \star z) = (y \star x) \star z = e \star z = z$.

Exercises. For each of the following binary operations determine whether associativity and commutativity hold and determine the existence of a right or left identity element, and in which case the existence of right or left inverse.

i. $X = \wp(A)$ for the intersection $\cap$.

ii. $X = \wp(A)$ for the union $\cup$.

iii. $X = \wp(A)$ for the difference $\setminus$.

iv. $X = \wp(A)$ for the symmetric difference Δ.

v. $X = \mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ for $+$ and $\times$.

vi. $X = \mathbb{N} \setminus \{0\}$, $\mathbb{Z} \setminus \{0\}$, $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ for the division.

vii. $X = 2\mathbb{Z}$ for $+$.

viii. $X = \mathbb{R}$, $a \in \mathbb{R}$ a fixed element and $x \star y = x + y - a$.

ix. X any set, $e \in X$ a fixed element. Define $\star$ as $x \star y = e$ for all x, $y \in X$.

x. X any set. Define $\star$ as $x \star y = x$ for all x, $y \in X$.

xi. $X = \mathbb{R}$ and $x \star y = \max\{x, y\}$.

xii. $X = \mathbb{R}$ and $x \star y = x - y$.

xiii. $X = \mathbb{R}$ and $x \star y = |x - y|$.

3.4 Operations with Functions

In section 3.1 we have seen how to compose two functions when appropriate. At page 31, we have seen that a function $f : X \longrightarrow Y$ gives rise to a function from $\wp(X)$ into $\wp(Y)$, that we still denote by f. Here we will see some other operations on functions, i.e. from one or more functions we will obtain new ones.

Examples and Exercises.

i. Let f and g be two functions from a set X into $\mathbb{R}$. We can define $f + g : X \longrightarrow \mathbb{R}$ by the rule $(f + g)(x) = f(x) + g(x)$ for all $x \in \mathbb{R}$. We can also define the function $fg : X \longrightarrow \mathbb{R}$ by the rule $(fg)(x) = f(x)g(x)$. More generally if $\star$ is a binary operation on a set Y and f and g are two functions from X into Y, then we can define $f \star g : X \longrightarrow Y$ by $(f \star g)(x) = f(x) \star g(x)$. Thus the binary operation $\star$ on Y gives rise to a binary operation on $\mathrm{Func}(X, Y)$, still denoted by $\star$. Properties of $(Y, \star)$ reflect to $(\mathrm{Func}(X, Y), \star)$:

   a. Show that if $(Y, \star)$ is associative (resp. commutative) then so is $(\mathrm{Func}(X, Y), \star)$.

   b. Show that if $(Y, \star)$ has a left (resp. right) identity element then so does $(\mathrm{Func}(X, Y), \star)$.

   c. Show that if $(Y, \star)$ has an identity element and if every element of Y is invertible, then the same properties hold for $(\mathrm{Func}(X, Y), \star)$.

ii. If $f : X \longrightarrow X_1$ and $g : Y \longrightarrow Y_1$ are two functions, we can define the function $f \times g : X \times Y \longrightarrow X_1 \times Y_1$ by the rule $(f \times g)(x, y) = (f(x), g(y))$.

iii. Any function $f : X \longrightarrow Y$ gives rise to a function $\tilde{f} : \wp(X) \longrightarrow \wp(Y)$ by the rule $\tilde{f}(A) = f(A) := \{f(a) : a \in A\}$ for all $A \in \wp(X)$.

iv. Any function $f : X \longrightarrow Y$ gives rise to a function $\tilde{f}^{-1} : \wp(Y) \longrightarrow \wp(X)$ by the rule $\tilde{f}^{-1}(B) = f^{-1}(B) := \{x \in X : f(x) \in B\}$ for all $B \in \wp(Y)$.

v. Let $f : X \longrightarrow X_1$ and $g : Y \longrightarrow Y_1$ be two functions. Assume that $X \cap Y = \emptyset$. Then we can define the function $f \cup g : X \cup Y \longrightarrow X_1 \cup Y_1$, the **union** of f and g, by the rule

$$(f \cup g)(z) = \begin{cases} f(z) & \text{if } z \in X \\ g(z) & \text{if } z \in Y \end{cases}$$

vi. We can generalize the above example. Let $f : X \longrightarrow X_1$ and $g : Y \longrightarrow Y_1$ be two functions. Assume that for all $z \in X \cap Y$, $f(x) = g(x)$. Then we can define the function $f \cup g : X \cup Y \longrightarrow X_1 \cup Y_1$, the **union** of f and g, by the rule

$$(f \cup g)(z) = \begin{cases} f(z) & \text{if } z \in X \\ g(z) & \text{if } z \in Y \end{cases}$$

vii. We can generalize even further the above example. Let I be an index set. Let $(f_i : X_i \longrightarrow Y_i)_{i \in I}$ be a family of functions indexed by I. Assume that for all $i, j \in I$ and all $x \in X_i \cap X_j$, $f_i(x) = f_j(x)$. Then we can define the function $\cup_{i \in I} f_i : \cup_{i \in I} X_i \longrightarrow \cup_{i \in I} Y_i$ by the following rule: For all $x \in \cup_{i \in I} X_i$,

$$(\cup_{i \in I} f_i)(x) = f_i(x)$$

if $x \in X_i$.

Exercises.

i. Let f and g be two functions from a set X into $\mathbb{R}$. Show that if $s : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ is given by $s(x, y) = x + y$, then $f + g = s \circ (f \times g)$ and that if $p : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ is given by $p(x, y) = xy$, then $fg = p \circ (f \times g)$.

3.5 Injections, Surjections, Bijections

3.5.1 Injections

A function $f : X \longrightarrow Y$ is called **one-to-one** or an **injection** if for all $x_1, x_2 \in X$, $f(x_1) = f(x_2)$ implies $x_1 = x_2$. That means that if $f : X \longrightarrow Y$ is an injective function, then no two different elements of X can go to the same element of Y under f. For example the function $f : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = x^2$ is not injective. But the function $f : \mathbb{R}^{\leq 0} \longrightarrow \mathbb{R}$ defined by the same rule $f(x) = x^2$ is injective. These examples show that "to be injective" is a property that has to do more with the domain than with the arrival set.

Further Examples.

i. If X and Y are nonempty sets and $x_0 \in X$ is fixed, then the map $f : Y \longrightarrow X \times Y$ defined by $f(y) = (x_0, y)$ is one-to-one.

ii. The map $f : \mathbb{N} \longrightarrow \mathbb{N}$ defined by $f(n) = n + 1$ is one to one.

iii. If $f_1 : X_1 \longrightarrow Y_1$ and $f_2 : X_2 \longrightarrow Y_2$ are one-to-one then the function $f_1 \times f_2 : X_1 \times X_2 \longrightarrow Y_1 \times Y_2$ defined by $(f_1 \times f_2)(x_1, x_2) = (f_1(x_1), f_2(x_2))$ is also one- to-one.

Lemma 3.5.1 *i. The composition of two injections is an injection.*
ii. If $f \circ g$ is an injection then g is an injection.

Proof: i. Let f and g be two injections. Assume $(f \circ g)(x_1) = (f \circ g)(x_2)$, i.e. assume $f(g(x_1)) = f(g(x_2))$. Since f is an injection, $g(x_1) = g(x_2)$. Since g is an injection, $x_1 = x_2$.
ii. Assume $g(x_1) = g(x_2)$. Applying f we get $f(g(x_1)) = f(g(x_2))$, i.e. $(f \circ g)(x_1) = (f \circ g)(x_2)$. Since $f \circ g$ is an injection, this implies $x_1 = x_2$. □

3.5.2 Surjections

A function $f : X \longrightarrow Y$ is called **onto** or a **surjection** if for all $y \in Y$ there is an $x \in X$ such that $f(x) = y$, i.e. if $f(X) = Y$. That means that if $f : X \longrightarrow Y$ is an surjection, then every elements of Y is "attained" by an element of X under f. For example the function $f : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = x^2$ is not onto because -1 is not attained. But the function $f : \mathbb{R} \longrightarrow \mathbb{R}^{\geq 0}$ defined by the same rule $f(x) = x^2$ is onto. These examples show that "to be surjective" is a property that has to do more with the arrival set than with the domain.

Further Examples.

i. If X and Y are nonempty sets, then the projection maps $\pi_1 : X \times Y \longrightarrow X$ and $\pi_2 : X \times Y \longrightarrow Y$ are surjections. The map π_1 is not one to one unless $|Y| = 1$.

ii. The map $f : \mathbb{N} \longrightarrow \mathbb{N}$ defined by $f(n) = [n/2]$ where $[x]$ stands for the integer part of x is onto (but not one to one).

iii. The map $f : \mathbb{N} \longrightarrow \mathbb{N}$ defined by

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

is onto.

iv. If $f_1 : X_1 \longrightarrow Y_1$ and $f_2 : X_2 \longrightarrow Y_2$ are onto then the function $f_1 \times f_2 : X_1 \times X_2 \longrightarrow Y_1 \times Y_2$ defined by $(f_1 \times f_2)(x_1, x_2) = (f_1(x_1), f_2(x_2))$ is also onto.

Lemma 3.5.2 *i. The composition of two surjections is an surjection.*
ii. If $g \circ f$ is a surjection then g is a surjection.
iii. If $f : X \longrightarrow Y$ is any function, then the function $f : X \longrightarrow f(X)$ is a surjection.
iv. The projection map $\pi_1 : X \times Y \longrightarrow X$ (resp. $\pi_2 : X \times Y \longrightarrow Y$) is a surjection if $Y \neq \emptyset$ (resp. $X \neq \emptyset$).

Proof: i. Let $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ be two surjections. Clearly $(g \circ f)(X) = g(f(X)) = g(Y) = Z$. So $g \circ f$ is a surjection.

ii. Assume $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ are functions. Assume $g \circ f$ is a surjection. Then $Z = g(f(X)) \subseteq g(Y)$.

iii and iv are clear and are left as exercise. □

3.5.3 Bijections

A function $f : X \longrightarrow Y$ is called **bijection** if it is one-to-one and onto. Two sets X and Y for which there is such a bijection are said to be in **one-to-one correspondence** or **in bijection**.

Lemma 3.5.3 *i. The composition of two bijections is a bijection.*

ii. If $f \circ g$ is a bijection then g is an injection and f is a surjection.

iii. If $f : X \longrightarrow Y$ is an injection, then $f : X \longrightarrow f(X)$ is a bijection.

Proof: Follows from lemmas 3.5.1 and 3.5.2. □

Lemma 3.5.4 (Inverse) *Let $f : X \longrightarrow Y$ be a bijection. Then there is a unique bijection $f^{-1} : Y \longrightarrow X$ such that for all $x \in X$ and $y \in Y$,*

$$f^{-1}(y) = x \iff f(x) = y.$$

We have

$$f \circ f^{-1} = \mathrm{Id}_Y \text{ and } f^{-1} \circ f = \mathrm{Id}_X .$$

Furthermore if $g : Y \longrightarrow X$ satisfies

$$f \circ g = \mathrm{Id}_Y \text{ or } g \circ f = \mathrm{Id}_X$$

then $g = f^{-1}$. It follows that $(f^{-1})^{-1} = f$.

Proof: Left as an exercise. □

Given a bijection $f : X \longrightarrow Y$, the bijection $f^{-1} : X \longrightarrow Y$ of the lemma above is called the **inverse** of f.

Lemma 3.5.5 *i. Let $f : X \longrightarrow Y$ be a bijection. Then $(f^{-1})^{-1} = f$.*

ii. Let $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ be bijections. Then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof: Left as an exercise. □

Exercises.

i. Find all bijections from $\{0, 1, 2\}$ into $\{0, 1, 2\}$. Find all bijections from $\{0, 1, 2, 3\}$ into $\{0, 1, 2, 3\}$. Find all injections from the set $\{0, 1, 2\}$ into the set $\{0, 1, 2, 3\}$. Find all surjections from $\{0, 1, 2, 3\}$ into $\{0, 1, 2\}$.

ii. Let $f : X \longrightarrow Y$ be a bijection. Show that for all A, $B \subseteq X$,

a. $f(A \cap B) = f(A) \cap f(B)$

b. $f(A \cup B) = f(A) \cup f(B)$

c. $f(A \setminus B) = f(A) \setminus f(B)$

d. Show that the induced map $f : \wp(X) \longrightarrow \wp(Y)$ is also a bijection.

iii. Let X be a set. The set of functions from X into $\{0, 1\}$ is denoted by ${}^X2$. The purpose of this exercise is to show that there is a bijection between the sets $\wp(X)$ and ${}^X2$.

a) For a subset A of X, define $f_A : X \longrightarrow \{0, 1\}$ by the rule

$$f_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

Thus $f_A \in {}^X2$. (The function f_A is called the **characteristic function** of A).

b) Show that the rule $A \mapsto \phi(A) := f_A$ defines a function ϕ from $\wp(X)$ into ${}^X2$.

c) Let $f \in {}^X2$ be a function. Let $X_f := \{x \in X : f(x) = 1\}$. Show that the rule $f \mapsto \psi(f) = X_f$ defines a function ψ from ${}^X2$ into $\wp(X)$.

e) For $A \in \wp(X)$, show that $\psi(\phi(A)) = A$.

f) For $f \in {}^A2$, show that $\psi(\phi(f)) = f$.

g) Conclude that the functions $A \mapsto \phi(A)$ and $f \mapsto \psi(f)$ are bijections and that they are inverses of each other.

iv. Let X be a set. The set of functions from $\{0, 1\}$ into X is denoted by ${}^2X$. Show that there is a bijection between the sets $X \times X$ and ${}^2X$.

3.6 Sym(X)

Let X be any set and $G = \mathrm{Sym}(X)$, the set of all bijections from X into X. Consider the composition operation $\circ$ on $\mathrm{Sym}(X)$. The triple $(\mathrm{Sym}(X), \circ, \mathrm{Id}_X)$ has the following properties:

0. For all f, $g \in \mathrm{Sym}(X)$, $f \circ g$, $f^{-1}, \mathrm{Id}_X \in \mathrm{Sym}(X)$
1. Associativity. For all f, g, $h \in \mathrm{Sym}(X)$, $(f \circ g) \circ h = f \circ (g \circ h)$.
2. Identity Element. For all $f \in \mathrm{Sym}(X)$, $f \circ \mathrm{Id}_X = \mathrm{Id}_X \circ f = f$.
3. Inverse Element. For all $f \in \mathrm{Sym}(X)$, $f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}_X$.

We call $\mathrm{Sym}(X)$ the **symmetric group on** X. If $X = \{1, \ldots, n\}$, the set $\mathrm{Sym}(X)$ is simply denoted by $\mathrm{Sym}(n)$ and is called the **symmetric group on** n **letters**. The group $\mathrm{Sym}(n)$ has $n!$ many elements. Sometimes, composition will also be called multiplication.

Let us first get acquainted with the groups of the form $\mathrm{Sym}(n)$ for $n \in \mathbb{N}$. We consider the following element g of $\mathrm{Sym}(7)$:

$$\begin{aligned} g(1) &= 2 \\ g(2) &= 5 \\ g(3) &= 3 \\ g(4) &= 7 \\ g(5) &= 1 \\ g(6) &= 6 \\ g(7) &= 4 \end{aligned}$$

We can represent this element as

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 3 & 7 & 1 & 6 & 4 \end{pmatrix},$$

where we put the domain on the first line, and the image of the elements of the domain just below it. We can represent this element also as $(1,2,5)(3)(4,7)(6)$ or as $(1,2,5)(4,7)$. We will prefer the last representation. The last representation can be read as follows: "1 goes to 2, 2 goes to 5, 5 goes back to 1; 4 goes to 7, 7 goes back to 4; the rest of the numbers (3 and 6) are fixed".

Written this way, the element $g = (1,2,5)(4,7)$ may be seen as an element of $\mathrm{Sym}(7)$ as well as an element of $\mathrm{Sym}(8)$. If one is careful enough when needed, this never causes a problem.

It is impossible to represent $\mathrm{Id}_{\mathrm{Sym}(6)}$ with the representation we adopted, so we will write simply $\mathrm{Id}_{\mathrm{Sym}(6)}$ or just 1 (by abuse of language).

Such a representation is called the **cyclic representation** of the bijection. The elements such as $(1,2,5)$, (3) and $(4,7)$ of a cyclic representation are called **cycles**. The cycle $(1,2,3)$ is a 3-cycle. The cycle $(4,7)$ is a 2-cycle. The element $(1,2,5)(4,7)$ of $\mathrm{Sym}(7)$ has four cycles, namely $(1,2,5)$, (3), $(4,7)$ and (6). On the other hand, the element $(1,2,5)(4,7)$ of $\mathrm{Sym}(8)$ has five cycles, namely $(1,2,5)$, (3), $(4,7)$, (6) and (8). The element $\mathrm{Id}_{\mathrm{Sym}(6)}$ or 1 of $\mathrm{Sym}(6)$ has six cycles. But the element 1 of $\mathrm{Sym}(8)$ has eight cycles.

Clearly $(1,2,3) = (2,3,1) = (3,1,2) \neq (1,3,2)$.

The multiplication (more precisely, the composition) of disjoint cycles is very simple: One just juxtaposes them, e.g. the multiplication of $(1,2,5)$ and $(4,7)$ is just $(1,2,5)(4,7)$, or $(4,7)(1,2,5)$. Similarly, the product of the two elements $(1,5,7)(3,4)$ and $(2,6)(8,9)$ is just $(1,5,7)(2,6)(3,4)(8,9)$.

If the cycles are not disjoint, then the multiplication (i.e. the product or the composition) of elements is slightly more complicated. For example to compute $(1,2,3)(1,2,4,3,5)$ we start from the right and see where 1 goes to: 1 first goes to 2 (the right cycle) and the left cycle takes 2 to 3. Thus the product starts as $(1,3,\ldots$. Now we restart the same procedure with 3. As a result we obtain $(1,2,3)(1,2,4,3,5) = (1,3,5,2,4)$. As an exercise the reader should check that

$$\begin{aligned} (1,2,3,4)(3,5,4) &= (1,2,3,5) \\ (1,3,2,4)(1,4)(3,5,4) &= (2,4)(3,5) \end{aligned}$$

The inverse of an element is easy to find. For example $(1,2,3,4,5)^{-1} = (1,5,4,3,2)$ and $((1,2,3,4)(5,6,7))^{-1} = (1,4,3,2)(5,7,6)$.

We can use the same notation for Sym($\mathbb{N}$). For example the element $g := (0,1)(2,3)(4,5)(6,7)\ldots$ is in Sym($\mathbb{N}$) and $g^2 = \mathrm{Id}_{\mathbb{N}}$. On the other hand the function represented by $(0,1,2,3,4,5,\ldots)$ is not in Sym($\mathbb{N}$) because the number 0 is not in the range and this function is not onto, hence not a bijection. An infinite cycle in Sym($\mathbb{N}$) cannot have a beginning, nor an end.

On the other hand the element $(\ldots,7,5,3,1,2,4,6,8,\ldots)$ is in Sym($\mathbb{N}$).

The reader should not that, we do not see the element $(0,1)(2,3)(4,5)(6,7)\ldots$ as the product of infinitely many elements $(0,1)$, $(2,3)$, $(4,5)$ etc. We can only multiply finitely many elements of Sym(X).

The **type** of the element g of Sym(n) is a sequence of n natural numbers $a_1 - a_2 - \ldots - a_n$ where a_i is the number of i-cycles in the cyclic representation of g. For example the type of $(1,2,5)(4,7) \in \mathrm{Sym}(8)$ is $3-1-1$, the type $(1,2,5)(4,7) \in \mathrm{Sym}(9)$ is $4-1-1$, the type of $(1,2,3)(4,5,6) \in \mathrm{Sym}(6)$ is $0-0-2$. The following formalism is more convenient and expressive: We will say that $(1,2,5)(4,7) \in \mathrm{Sym}(8)$ is of type $(1)(2)(3,4)(5,6,7)(8)$, or even of type $(1,2)(3,4,5)$ if there is no possible confusion. For example the elements of Sym(5) of type $(1,2,3)(4,5)$ are:

$$(1,2,3)(4,5), (1,3,2)(4,5), (1,2,4)(3,5), (1,4,2)(3,5), (1,2,5)(3,4),$$

$$(1,5,2)(3,4), (1,3,4)(2,5), (1,4,3)(2,5), (1,3,5)(2,4), (1,5,3)(2,4),$$

$$(1,4,5)(2,3), (1,5,4)(2,3), (2,3,4)(1,5), (2,4,3)(1,5), (2,3,5)(1,4),$$

$$(2,5,3)(1,4), (2,4,5)(1,3), (2,5,4)(1,3), (3,4,5)(1,2), (3,5,4)(1,2).$$

Exercises.

i. Show that Sym(n) has $n!$ elements.

ii. Write the elements of Sym(n) for $n = 1$, 2, 3, 4. Draw the multiplication table of these groups.

iii. Find elements of each type of Sym(n) for $n = 2,3,4,5,6$.

iv. How many types of elements are there in Sym(9) whose square is 1?

v. Show that if $g := (\ldots,7,5,3,1,2,4,6,8,\ldots) \in \mathrm{Sym}(\mathbb{N})$, then $g^n \neq 1$ for any $n \in \mathbb{Z} \setminus \{0\}$.

vi. Let $a := (0,1) \in \mathrm{Sym}(\mathbb{N})$. Show that $C_{\mathrm{Sym}(\mathbb{N})}(a) := \{g \in \mathrm{Sym}(\mathbb{N}) : ga = ag\} = \{g \in \mathrm{Sym}(\mathbb{N}) : g(\{0,1\}) = \{0,1\}\}$.

vii. Multiply the elements

$$(0,1)(1,2)(3,4)\ldots \text{ and } (1,2)(3,4)(5,6)\ldots$$

of Sym(n) both ways. Are they equal? How many cycles do the products have?

viii. Show that it is not true that for every $g \in \mathrm{Sym}(\mathbb{N})$ there is an $h \in \mathrm{Sym}(\mathbb{N})$ such that $h^2 = g$.

ix. ** Is it true that every element of Sym($\mathbb{N}$) is a product of finitely many squares?

x. ** Let p be an integer. Is it true that every element of Sym($\mathbb{N}$) is a product of finitely many p-th powers?

xi. For an element $g \in \mathrm{Sym}(X)$, define $o(g)$ to be the least positive natural number m such that $g^m = Id_X$ if there is such an m, otherwise define $o(g) = \infty$. Thus $o(g) = Id_X$ if and only if $g = Id_X$.

Let $G = \mathrm{Sym}(\mathbb{N})$. Show that

$$o(1,2,3) = 3$$
$$o(1,2,3,4) = 4$$
$$o((1,2,3)(4,5)) = 6$$
$$o(\ldots,7,5,3,1,2,4,6,8,\ldots) = \infty$$

For each $n = 1, 2, \ldots, 12$ find $\max\{o(g) : g \in \mathrm{Sym}(n)\}$.

3.7 Families, Sequences and Cartesian Products

In Section 1.6, we have defined a family $(X_i)_{i\in I}$ as set indexed by the "index set" I. We are now in a position to redefine the same concept in a more precise (mathematical) way. Let X and I be two sets. Let $x : I \longrightarrow X$ be a surjection. Thus

$$X = \{x(i) : i \in I\}$$

so that X now becomes a family indexed by I. Sometimes we will write x_i instead of $x(i)$ and $(x_i)_{i\in I}$ instead of X.

A **sequence** from a set X is a subset of X indexed by $\mathbb{N}$, thus a sequence is just a function $x : \mathbb{N} \longrightarrow X$. A sequence usually is written as $(x_i)_{i\in\mathbb{N}}$ or as $(x_i)_i$ for short where x_i stands for $x(i)$ for all $i \in \mathbb{N}$. We may also write a sequence as

$$x_0, x_1, x_2, \ldots$$

which more visual and more convenient.

Let $(X_i)_{i\in I}$ be a family of sets. The set of all sequences x from the set $\cup_i X_i$ such that $x_i \in X_i$ for all $i \in I$ is called the **Cartesian product** of the family $(X_i)_{i\in I}$. We denote the Cartesian product by $\prod_{i\in I} X_i$. If all the sets X_i are equal to a set X, then instead of $\prod_{i\in I} X_i$ we write $\prod_{i\in I} X$.

We have already defined the Cartesian product of two sets X_1 and X_2 in chapter 2.4. We should check that the concept we have defined then coincides

with the concept we have defined here when I has just two elements. But this is not true. The set $X_1 \times X_2$ defined in chapter 2.4 is not equal to the set $\prod_{i\in\{1,2\}} X_i$ that we have defined above. Nevertheless there is a bijection between them.

Lemma 3.7.1 *There is a bijection between $X_1 \times X_2$ and $\prod_{i\in\{1,2\}} X_i$.*

Proof: Let $\alpha \in X_1 \times X_2$. Define $\phi_\alpha : \{1,2\} \longrightarrow X_1 \cup X_2$ by the rule $\phi_\alpha(i) = \pi_i(\alpha)$ where π_1 and π_2 are the two projections of $X_1 \times X_2$ onto X_1 and X_2. Then $\phi_a \in \prod_{i\in\{1,2\}} X_i$. We leave to the reader the easy fact that the map $\phi : X_1 \times X_2 \longrightarrow \prod_{i\in\{1,2\}} X_i$ defined by $\phi(a) = \phi_a$ is a bijection between the two sets. □

Let I be an index set and $(X_i)_{i\in I}$ and $(Y_i)_{i\in I}$ be two families. For each $i \in I$, let $f_i : X_i \longrightarrow Y_i$ be a function. Then the function $\prod_{i\in I} f_i : \prod_{i\in I} X_i \longrightarrow \prod_{i\in I} Y_i$ given by $(\prod_{i\in I} f_i)((x_i)_{i\in I}) = (f(x_i))_{i\in I}$ is called the **product** of the functions $(f_i)_{i\in I}$. The product $f_1 \times f_2$ of two functions $f_1 : X_1 \longrightarrow Y_1$ and $f_2 : X_2 \longrightarrow Y_2$ is of course defined by $(f_1 \times f_2)(x_1, x_2) = (f_1(x_1), f_2(x_2))$.

Chapter 4

Relations

4.1 Definitions

Let X be a set. A **binary relation** R of X is just a subset of $X \times X$. For $x, y \in X$, rather than writing $(x, y) \in R$, one often writes xRy. The usual symbols for relations are $<, \leq, \prec, \preceq, \ll, \subset, \subseteq, \sqsubseteq, \sim, \simeq, \approx, \equiv, \perp, \parallel, \lhd, \trianglelefteq$ etc.

Examples.

i. Let $X = \{0, 1, 2, 3\}$. Define

$$< = \{(0,1),\ (0,2),\ (1,2),\ (0,3),\ (1,3),\ (2,3)\}.$$

Then $<$ is a relation. It is the order relation that we are familiar with.

ii. Let X be any set. Then $\emptyset$ and $X \times X$ are binary relations on X. In the first one no two elements of X are related, in the second one any two elements of X are related.

iii. Let X be any set. Then $\delta(X \times X) := \{(x, y) \in X \times X : x = y\}$ is a binary relation on X (called equality!).

iv. Let $X = \mathbb{N}$. Then $\{(x, y) \in \mathbb{N} \times \mathbb{N} : x \text{ divides } y \text{ in } \mathbb{N}\}$ is a binary relation on $\mathbb{N}$.

v. Let U be any set. Let X be the set of finite subsets of U. Then $\{(A, B) \in X \times X : |A| = |B|\}$ is a relation on X.

vi. Let U be any set. Let $X = \wp(U)$. Then

$$\{(A, B) \in X \times X :\ \text{there is a bijection } f : A \longrightarrow B\}$$

is a relation on X.

vii. Let U be any set. Let $X = \wp(U)$. Then

$$\{(A, B) \in X \times X : \text{ there is an injection } f : A \longrightarrow B\}$$

is a relation on X.

viii. Let U be any set. Let $X = \wp(U)$. Then $\{(A, B) \in X \times X : A \subseteq B\}$ is a relation on X.

ix. Let U be any set. Let $X = \wp(U)$. Then $\{(A, B) \in X \times X : A \cap B \neq \emptyset\}$ is a relation on X.

x. Let U be any set. Let $X = \wp(U)$. Then $\{(A, B) \in X \times X : A \cap B = \emptyset\}$ is a relation on X.

xi. If $f : X \longrightarrow X$ is a function, the graph of f is a relation on X.

Potential Properties of Relations. **i.** A binary relation R is called **reflexive** if xRx for all $x \in X$.

ii. A binary relation R is called **irreflexive** if $\neg xRx$ for all $x \in X$.

iii. A binary relation R is called **symmetric** if xRy implies yRx for all x, $y \in X$.

iv. A binary relation R is called **antisymmetric** if xRy implies $\neg yRx$ for all x, $y \in X$.

v. A binary relation R is called **transitive** if xRy and yRz implies xRz for all x, y, $z \in X$.

Exercises.

i. Determine whether or not the binary relations defined in the examples above are reflexive, irreflexive, symmetric, antisymmetric or transitive.

ii. Let R be a binary relation on a set X. Show that there is a smallest reflexive relation S that contains R.

iii. Let R be a binary relation on a set X. Show that there is a smallest symmetric relation S that contains R.

iv. Let R be a binary relation on a set X. Show that there is a smallest transitive relation S that contains R.

4.2 Equivalence Relations

An **equivalence relation** is a reflexive, symmetric and transitive binary relation.

An equivalence relation is very often denoted by one of the following symbols: $\equiv$, $\sim$, $\simeq$, $\approx$, $\cong$.

According to the definition, for a binary relation $\equiv$ on a set X to be an equivalence relation, the following should hold:

EqR1. Reflexivity. For all $x \in X$, $x \equiv x$.

EqR2. Symmetry. For all $x, y \in X$, if $x \equiv y$ then $y \equiv x$.

EqR3. Transitivity. For all $x, y, z \in X$, if $x \equiv y$ and $y \equiv z$ then $x \equiv y$.

Examples and Exercises.

i. The equality is an equivalence relation on any set.

ii. The relation R defined by xRy for all x, y on any set is an equivalence relation.

iii. On any subset of $\mathbb{R}$ the relation defined by $xRy \iff x^2 = y^2$ is an equivalence relation.

iv. Let $n > 0$ be any natural number. On $\mathbb{Z}$, the relation $\equiv_n$ defined by

$$x \equiv_n y \iff n \text{ divides } x - y$$

is an equivalence relation.

v. On the set $\mathbb{R}$ or $\mathbb{Q}$ the relation $\equiv$ defined by $x \equiv y$ if and only if $x - y \in \mathbb{Z}$ is an equivalence relation.

vi. On the set $\mathbb{R}$ the relation $\equiv$ defined by $x \equiv y$ if and only if $x - y \in \mathbb{Q}$ is an equivalence relation.

vii. Let X and Y be two sets. Let $A \subseteq X$. The relation $\equiv_A$ defined on $\text{Func}(X, Y)$ by

$$f \equiv g \iff f_{|A} = g_{|A}$$

is an equivalence relation.

viii. On $X := \mathbb{R} \times \mathbb{R} \times \mathbb{R}$, the relation $\equiv$ defined by $(x, y, z) \equiv (x_1, y_1, z_1)$ by $2(x - x_1) + 3(y - y_1) - (z - z_1) = 0$ is an equivalence relation.

ix. On $\mathbb{C}$, the relation defined by

$$x \equiv y \iff |x| = |y|$$

is an equivalence relation.

x. More generally, if X and Y are sets and F is a set of functions from X into Y, then the relation $\equiv$ defined on X by

$$x \equiv y \text{ if and only if } f(x) = f(y) \text{ for all } f \in F$$

is an equivalence relation on X.

Given an equivalence relation $\equiv$ on a set X and an element $a \in X$, we define the **equivalence class** $\overline{a}$ of a as follows:

$$\overline{a} = \{x \in X : a \equiv x\}.$$

The equivalence class of a may also be denoted as $[a]$, $\tilde{a}$ or some other similar way.

A **partition** P of a set X is a set of subsets of X (i.e. P is an element of $\wp\wp(X)$) such that

i. $\cup P = X$, and

ii. For any $A, B \in P$, if $A \neq B$ then $A \cap B = \emptyset$.

Examples.

i. The set $\{\{0,3\},\{1,2,4\}\}$ is a partition of $\{0,1,2,3,4\}$.

ii. The sets $(n, n+1]$ for $n \in \mathbb{Z}$ partition $\mathbb{R}$, meaning that $\{(n, n+1] : n \in \mathbb{Z}\}$ is a partition of $\mathbb{R}$.

Lemma 4.2.1 *Let $\equiv$ be an equivalence relation on a set X. Then the set $\{\overline{x} : x \in X\}$ is a partition of X. Conversely, any partition P of X gives rise to an equivalence relation on X via*

$$x \equiv y \text{ if and only if there exists } A \in P \text{ such that } x \in A \text{ and } y \in A.$$

Thus there is a one-to-one correspondence between the set of partitions on X and the set of equivalence relations on X.

Proof: Let $\equiv$ be an equivalence relation on X. Since $x \equiv x$ for all $x \in X$, we have $x \in \overline{x}$. It follows that $\cup\{\overline{x} : x \in X\} = X$. Now we prove that for any x, $y \in X$, either $\overline{x} = \overline{y}$ or $\overline{x} \cap \overline{y} = \emptyset$. We proceed to show that if $\overline{x} \cap \overline{y} \neq \emptyset$, then $\overline{x} = \overline{y}$. Let $z \in \overline{x} \cap \overline{y}$. Thus $z \equiv x$ and $z \equiv y$. Let $t \in \overline{x}$. Thus $t \equiv x$. Since $\equiv$ is symmetric we have

$$t \equiv x$$
$$x \equiv z$$
$$z \equiv y$$

By transitivity we get $t \equiv y$, i.e. $t \in \overline{y}$. We proved that any element t of $\overline{x}$ is an element of $\overline{y}$. The other direction holds as well. Thus $\overline{x} = \overline{y}$. Thus $\{\overline{x} : x \in X\}$ is a partition of X.

Conversely, let P be a partition of X and define the relation $\equiv$ as follows:

$$x \equiv y \text{ if and only if there exists } A \in P \text{ such that } x \in A \text{ and } y \in A.$$

It is a matter of triviality to check that this is an equivalence relation. □

Quotient Set. Let $\equiv$ be an equivalence on a set X. The set

$$\{\overline{x} : x \in X\}$$

is called the **quotient set** and it is denoted by $X/\equiv$. It is important to note that each element of $X/\equiv$ is a subset of X and any two distinct elements of $X/\equiv$ are disjoint subsets of X.

Examples

i. Consider the equality as an equivalence relation on the set X. Then the quotient set is $\{\{x\} : x \in X\}$ and it is in one to one correspondence with X.

ii. On any set X consider the equivalence relation defined by $x \equiv y$ for all $x, y \in X$. Then $|X/\equiv| = 1$.

iii. On $\mathbb{R}$ consider the equivalence relation defined by $xRy \iff x^2 = y^2$. Then, for each $x \in \mathbb{R}$, $\overline{x} = \{x, -x\}$. Thus there is a natural one to one correspondence between $\mathbb{R}/\equiv$ and $\mathbb{R}^{\geq 0}$ given by $\overline{r} \mapsto |r|$.

iv. Let $n > 0$ be any natural number. On $\mathbb{Z}$, consider the equivalence relation $\equiv_n$ defined by

$$x \equiv_n y \iff n \text{ divides } x - y.$$

Then for each $i \in \mathbb{Z}$, $\overline{i} = n\mathbb{Z} + i = \mathbb{Z} + j$ where $j = 0, 1, \ldots, n-1$ is the remainder when we divide i by n. Therefore we have $\mathbb{Z}/\equiv_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ and $|\mathbb{Z}/\equiv_n| = n$.

v. On the set $\mathbb{R}$, consider the equivalence relation $\equiv$ defined by $x \equiv y$ if and only if $x - y \in \mathbb{Z}$. Then for each $r \in \mathbb{R}$, $\overline{r} = r + \mathbb{Z} = s + \mathbb{Z}$ for some unique $s \in [0, 1)$. Therefore $\mathbb{R}/\equiv$ is in a natural one to one correspondence with the interval $[0, 1)$.

vi. On the set $\mathbb{R}$, consider the relation $\equiv$ defined by $x \equiv y$ if and only if $x - y \in \mathbb{Q}$. Then for each $r \in \mathbb{R}$, $\overline{r} = r + \mathbb{Q}$. In this case, we cannot find a well-known set with which $\mathbb{R}/\equiv$ is in a one-to-one correspondence[1].

vii. Let X and Y be two sets. Let $a \in X$. Consider the equivalence relation $\equiv_a$ defined on $\text{Func}(X, Y)$ by

$$f \equiv g \iff f_{|A} = g_{|A}.$$

Given $f \in \text{Func}(X, Y)$, $\overline{f} = \{g \in \text{Func}(X, Y) : f(a) = g(a)\}$. There is a one to one correspondence between $\text{Func}(X, Y)\equiv$ and Y given by $\overline{f} \mapsto f(a)$. There is also a correspondence between $\text{Func}(X, Y)\equiv$ and the set of constant functions from X into Y.

viii. On $X := \mathbb{R} \times \mathbb{R} \times \mathbb{R}$, consider the equivalence relation $\equiv$ defined by $(x, y, z) \equiv (x_1, y_1, z_1)$ by $2(x - x_1) + 3(y - y_1) - (z - z_1) = 0$. Then

$$\overline{(x, y, z)} = \{(x_1, y_1, z_1) : 2x + 3y - z = 2x_1 + 3y_1 - z_1\}.$$

There is a (not so natural) correspondence between $\mathbb{R}^3/\equiv$ and $\mathbb{R}^2$ given by $(x, y, z) \mapsto (x, y)$.

ix. On $\mathbb{C}$, consider the equivalence relation defined by $x \equiv y \iff |x| = |y|$. Then $\overline{x} = \{y \in \mathbb{C} : |x| = |y|\}$ and there is a natural one to one correspondence between $\mathbb{C}/\equiv$ and $\mathbb{R}^{\geq 0}$ given by $x \mapsto |x|$. Each equivalence class $\overline{x}$ is the circle of center 0 and radius $|x|$.

[1] But there is such a set as we will see later in the second part of the book.

Canonical Surjection. If $\equiv$ is an equivalence relation on the set X, then the map from X onto the quotient set $X/\equiv$ given by $x \mapsto \overline{x}$ is called the **canonical surjection** from X into $X/\equiv$. Most often we will denote the canonical surjection with symbol π. Thus, for all $x \in X$, $\pi(x) = \overline{x} = \{y \in X : x \equiv y\} \in X/\equiv$.

Induced Map. Let X be a set and $\equiv$ be an equivalence relation on X. Let Y be a set and let $f : X \longrightarrow Y$ be a function such that for all $x, y \in X$, if $x \equiv y$ then $f(x) = f(y)$. Then the map $f : X \longrightarrow Y$ induces a map $\tilde{f} : X \equiv\!\!\longrightarrow Y$ by the rule $\tilde{f}(\overline{x}) = f(x)$.

Exercises.

i. Let X be a set.

a) For $i \in I$ (index set), let R_i be an equivalence relation on X. Thus $R_i \subseteq X \times X$ for each $i \in I$. Show that $\cap_{i\in I} R_i$ is an equivalence relation.

b) Conclude that for any relation R on X there is a smallest equivalence relation containing R. This equivalence relation is called the equivalence relation **generated** by R.

c) Let $X = \cup_{n\in\mathbb{N}}\{(x, y) \in \mathbb{R} : 2n + 1 \leq x^2 + y^2 \leq 2n + 2\}$. Define R on X as follows: For A, $B \in X$, $A\,R\,B$ if and only the line segment AB is in X. Show that this is not an equivalence relation. Find the equivalence relation generated by this relation. Find its set of equivalence classes.

ii. Let X be the set of functions from $\mathbb{R}$ into $\mathbb{R}$. Let $a \in \mathbb{R}$. Define the following relation on X: $f \equiv g$ if and only if there is an $\epsilon > 0$ such that $f(x) = g(x)$ for all $x \in (a - \epsilon, a + \epsilon)$. Show that this is an equivalence relation. Show that the functions induced by two distinct polynomials are not equivalent.

iii. Let X be a set. For two subsets A and B of X define

$$X \equiv Y \iff \text{There is a bijection } f : X \longrightarrow Y.$$

Show that this is an equivalence relation on $\wp(X)$.

iv. Let X be a set. For two subsets A and B of X define

$$X \equiv Y \iff X \Delta Y \text{ is finite.}$$

Show that this is an equivalence relation on $\wp(X)$.

v. Let $a \in \mathbb{R}$ be fixed. We will say that two functions f and g from $\mathbb{R}$ into $\mathbb{R}$ have the same **germ** around a, and we write $f \simeq_a g$, if there is an $\epsilon \in \mathbb{R}^{>0}$ such that $f(x) = g(x)$ for all $x \in (a - \epsilon, a + \epsilon)$.

a. Show that $\simeq_a$ is an equivalence relation on the set $X := {}^{\mathbb{R}}\mathbb{R}$ of all functions from $\mathbb{R}$ into $\mathbb{R}$. For $f \in X$, let $[f]$ denote the equivalence class of f with respect to this equivalence relation.

b. For f and g in X, we have already defined $f+g$ and fg at page 37. Show that if $f_1 \simeq_a g_1$ and $f_2 \simeq_a g_2$ then $f_1+f_2 \simeq_a g_1+g_2$ and $f_1f_2 \simeq_a g_1g_2$. It follows that one can define addition and multiplication on $X/\simeq_a$.

c. For $r \in \mathbb{R}$, define $c_r : \mathbb{R} \longrightarrow \mathbb{R}$ by $c_r(x) = r$ for all $x \in \mathbb{R}$, i.e. c_r is the constant function that takes always the value r. Show that the function $c : \mathbb{R} \longrightarrow X/\simeq_a$ defined by $c(r) = [c_r]$ is one-to-one and that it satisfies the equalities $c(r+s) = c(r)+c(s)$ and $c(rs) = c(r)c(s)$ for all $r, s\mathbb{R}$.

vi. Let X be a set. For two subsets A and B of X, define the relation $A \equiv B$ by the condition "$A\Delta B$ is finite".

a) Show that this is an equivalence relation on $\wp(X)$.

b) Show that $\wp(X)/\equiv$ has only one element if X is finite.

c) Conversely show that if $\wp(X)/\equiv$ has only one element then X is finite.

d) Show that $\wp(\mathbb{N})/\equiv$ is infinite.

Now let $A, B, A_1, B_1 \subseteq X$ be such that $A \equiv A_1$ and $B \equiv B_1$, then

e) $A \cap B \equiv A_1 \cap B_1$.

f) $A \cup B \equiv A_1 \cup B_1$.

g) $A^c \equiv A_1^c$.

h) $A \setminus B \equiv A_1 \setminus B_1$.

i) $A\Delta B \equiv A_1\Delta B_1$.

4.3 Partial Orders

A **partial order** on a set is a irreflexive and transitive binary relation on this set. A set together with a partial order is called a **partially ordered set** or a **poset** for short.

Partial orders are denoted by such symbols as $<$, $\prec$, $\subset$, $\lhd$ in general.

Examples.

i. Let $<$ be a partial order on a set X and let $A \subseteq X$. Then the partial order restricted to A, i.e. the binary relation $< \cap (A \times A)$, is a partial order on A.

ii. Let X be a set. On $\wp(X)$ define the relation

$$A < B \iff A \subseteq B \text{ and } A \neq B.$$

This is a partial order on $\wp(X)$.

iii. The natural order on (any subset of) $\mathbb{R}$ is a partial order.

iv. On $\mathbb{Z}$ define

$$x \prec y \iff y < x.$$

This is a partial order. In general, the inverse of a partial order is a partial order.

v. On $\mathbb{R}$ define

$$x < y \iff |x| < |y|.$$

This is a partial order.

vi. On $\mathbb{Z}$ define

$$x \prec y \iff y \text{ divides } x \iff \text{ there is a } z \in \mathbb{Z} \text{ such that } x = yz.$$

If $<$ is a partial order on a set X, we define the relation $\leq$ on X by

$$x \leq y \iff x < y \text{ or } x = y.$$

The binary relation $\leq$ is reflexive and transitive. Conversely, if $\leq$ is a reflexive and transitive binary relation on a set X, then the relation $<$ on X defined by

$$x < y \iff x \leq y \text{ and } x \neq y$$

is irreflexive and transitive, i.e. is a partial order. Thus there is no much difference between irreflexive and transitive binary relation (i.e. partial orders) and reflexive and transitive binary relations. For this reason, sometimes we will define a partial order as a reflexive and transitive binary relation, in which case, we use a notation of the form $\leq$, $\preceq$, $\subseteq$, $\sqsubseteq$, $\trianglelefteq$.

If $<$ is a binary relation on a set X, we define $x \geq y$ by $y \leq x$ and "$x > y$ or $x = y$" and "$y < x$ or $y = x$" respectively. Given a binary relation $\leq$, we could also define $<$ by "$x \leq y$ and $x \neq y$". It is easy to show that given a partial order $<$ on X, the relation $\leq$ defined on X is reflexive, transitive and satisfies

$$\forall x \, \forall y \, ((x \leq y \wedge y \leq x) \to x = y).$$

Conversely if a relation $\leq$ on X satisfies these three properties then $<$ is a partial order. Therefore, we may switch from $<$ to $\leq$ as it suits us.

Define upper bound, lower bound, least upper bound = supremum and greatest lower bound = infimum, maximum and minimum

Exercises.

i. Let $<$ and $\prec$ be two partial orders on two sets X and Y respectively. Define the partial order on $X \times Y$ via

$$(x, y) < (z, t) \iff x < z \text{ or } (x = z \text{ and } y \prec t).$$

Is this a partial order?

ii. Let $(Y, <)$ be a poset. Let $f : X \longrightarrow Y$ be any function. Show that the relation $<$ on X defined by

$$x_1 < x_2 \iff f(x_1) < f(x_2)$$

is a partial order on X.

iii. Let $(Y, <)$ be a poset, X a set and $A \subseteq X$. For two functions f and g from X into Y define

$$f < g \iff f(a) < g(a) \text{ for all } a \in A.$$

Show that this is a partial order on ${}^X Y$.

iv. Let $(Y, \leq)$ be a poset (reflexive and transitive), X a set and $A \subseteq X$. For two functions f and g from X into Y define

$$f \leq g \iff f(a) \leq g(a) \text{ for all } a \in A.$$

Show that this is a (reflexive) partial order.

v. Find supremum and infimum (if they exist) of the following sets:

(a) $\{x \in \mathbb{R} : x^2 + x - 1 < 0\}$,
(b) $\{x \in \mathbb{R} : x^2 + x - 1 > 0\}$,
(c) $\{\frac{1}{n} + (-1)^n : n \in \mathbb{N},\, n > 0\}$,
(d) $\{\frac{1}{1-x} : x \in \mathbb{R},\, x > 1\}$,
(e) $\{\frac{1}{1-x} : x \in \mathbb{R},\, x < 1\}$.

4.4 Total Orders

A partial order $<$ on a set X is called a **total order** if for all $x, y \in X$ one of

$$x < y,\ x = y,\ y < x$$

holds.

Lemma 4.4.1 *Let $<$ be a total order on a set X. For $x, y \in X$ only one of*

$$x < y,\ x = y,\ y < x$$

holds.

Proof: Assume $x < y$ and $x = y$ hold. Then $x < x$ contradicting irreflexivity. Similarly $x = y$ and $y < x$ cannot hold simultaneously. Assume finally that $x < y$ and $y < x$ hold. Then by transitivity $x < x$, contradicting irreflexivity again. □

Chapter 5

Induction

"Induction" is a method of proving statements about natural numbers. Suppose $\phi(x)$ is a statement about the natural number x, and that we want to prove the statement "$\phi(x)$ for all $x \in \mathbb{N}$". We can proceed as follows:

1) We first show that the statement $\phi(x)$ holds for $n = 0$, i.e. we prove $\phi(0)$.

2) Next, we show that whenever $\phi(n)$ holds for some natural number n, then $\phi(n+1)$ holds; in other words, we show that if $\phi(n)$ holds then $\phi(n+1)$ holds.

If we can successfully do these two steps, then $\phi(x)$ will hold for all $x \in \mathbb{N}$. Because, by the first step, we will know that $\phi(0)$ holds. Since $\phi(0)$ holds, by the second step (take $n = 0$) $\phi(1)$ will hold. Now that we know $\phi(1)$ holds, by the second step (take $n = 1$) $\phi(2)$ will hold. Now that we know $\phi(2)$ holds, by the second step (take $n = 2$) $\phi(3)$ will hold, etc. So $\phi(x)$ will hold for all $x \in \mathbb{N}$, as we can check one by one all numbers[1].

Example. As an exercise, let us prove that for all $x \in \mathbb{N}$, $0+1+2+\ldots+x = x(x+1)/2$. We let $\phi(x)$ denote "$0+1+2+\ldots+x = x(x+1)/2$".

Step 1. $\phi(0)$ holds. Indeed, $\phi(0)$ says that the sum of natural numbers from 0 to 0 is $0(0+1)/2$, i.e. is 0. This is of course true.

Step 2. If $\phi(n)$ holds then $\phi(n+1)$ holds. Assume $\phi(n)$ holds, i.e. assume that $0+1+2+\ldots+n = n(n+1)/2$. Under this assumption, we will show that $0+1+2+\ldots+n+(n+1) = (n+1)(n+2)/2$ (just replace x by $n+1$ in $\phi(x)$): $0+1+2+\ldots+n+(n+1) = (0+1+2+\ldots+n)+(n+1) = n(n+1)/2+(n+1) = (n+1)(n+2)/2$. (Here the second equality follows from the assumption that $\phi(n)$ holds. The rest are purely algebraic).

Therefore $\phi(x)$ holds for all $x \in \mathbb{N}$.

Definition by Induction. We can also define functions or sets by induction. For example, let us consider the function $f : \mathbb{N} \longrightarrow \mathbb{N}$ by the rule $f(0) = 1$ and

[1] If this last statement sounds strange to you, then you are a pretty good mathematician. What we have here is not a precise mathematical proof, but only a heuristic argument why $\phi(x)$ should hold for all $x \in \mathbb{N}$. In the next part, we will prove that steps (1) and (2), do indeed proof "$\phi(x)$ for all $x \in \mathbb{N}$".

$f(n+1) = 2f(n)$ for all $n \in \mathbb{N}$. Then,

$$\begin{array}{rcl} f(0) & = & 1 \\ f(1) & = & 2f(0) = 2 \\ f(2) & = & 2f(1) = 2 \times 2 = 4 \\ f(3) & = & 2f(2) = 2 \times 4 = 8 \end{array}$$

More generally, one sees that $f(n) = 2^n$.

Let us consider the following function defined by induction: $g(0) = 3$, $g(1) = 2$, $g(2) = 1$ and $g(n+1) = g(g(n))$ for all $n \geq 2$. Then

$$\begin{array}{rcl} g(0) & = & 3 \\ g(1) & = & 2 \\ g(2) & = & 1 \\ g(3) & = & g(g(2)) = g(1) = 2 \\ g(4) & = & g(g(3)) = g(2) = 1 \\ g(5) & = & g(g(4)) = g(1) = 2 \\ g(6) & = & g(g(5)) = g(2) = 1 \end{array}$$

On the other hand the following attempt of definition by induction fails: $h(0) = 0$, $h(1) = 2$, $h(2) = 3$ and $h(n+1) = h(h(n))$ for all $n \geq 2$, because

$$h(3) = h(h(2)) = h(3) = h(h(2)) = h(3) = \ldots$$

We can use induction to define addition from the successor function $S : \mathbb{N} \longrightarrow \mathbb{N}$ given by $S(n) = n + 1$ as follows: $n + 0 = n$ for all $n \in \mathbb{N}$ and

$$n + (m + 1) = (n + m) + 1$$

for all n, $m \in \mathbb{N}$.

We can use $+$ to define multiplication: $n \times 0 = n$ for all $n \in \mathbb{N}$ and

$$n \times (m + 1) = n \times m + n$$

for all n, $m \in \mathbb{N}$.

We can use $\times$ to define **exponentiation**: $n^0 = 1$ if $n \neq 0$, $0^m = 0$ for all $m \neq 0$ and

$$n^{m+1} = n^m \times n$$

for all n, $m \in \mathbb{N}$.

We also define **factorial** as follows: $0! = 1$ and

$$(n + 1)! = n! \times (n + 1)$$

for all $n \in \mathbb{N}$.

n Choose k. For n, $k \in \mathbb{N}$ and $k \leq n$, define

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!}.$$

A priory $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!} \in \mathbb{Q}$. We will see in fact that it is in $\mathbb{N}$.

Exercises.

i. Show that for any natural number n and for any real number $x \in [0,1]$,

$$(1-x)^n \leq 1 - nx + \frac{n(n-1)}{2}x^2.$$

ii. Show that $n! > 2^n$ for all n large enough.

iii. Show that $(x-1)^n \geq x^n - nx^{n-1}$ for all $x > 1$.

iv. Show that if $0 < x < 1$ and $n > 0$ is a natural number, then $(1-x)^n \leq 1 - nx + \frac{n(n-1)}{2}x^2$.

v. Show that for any $n \in \mathbb{N} \setminus \{0\}$, $1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$.

vi. Show that for any $n \in \mathbb{N} \setminus \{0\}$, $1^4 + 2^4 + \ldots + n^4 = \frac{n(n+1)(6n^3+9n^2+n-1)}{30}$.

vii. Given a set X, define $\wp^n(X)$ as follows by induction on n: $\wp^0(X) = X$ and $\wp^{n+1}(X) = \wp(\wp^n(X))$. Show that $\wp(\wp^n(X)) = \wp^n(\wp(X))$ for all sets X and all natural numbers n.

viii. Given a set X and a natural number n, define $\wp^n(X)$ as follows by induction on n: $\wp^0(X) = X$ and $\wp^{n+1}(X) = \wp(\wp^n(X))$. Find all n such that for any set X, $\{\{\emptyset\}, \{\{X\}\}\} \in \wp^n(X)$.

ix. Show that $\left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n \\ n-k \end{array} \right)$.

x. Show that $\left(\begin{array}{c} n \\ 0 \end{array} \right) = \left(\begin{array}{c} n \\ n \end{array} \right) = 1$.

xi. Show that $\left(\begin{array}{c} n \\ 1 \end{array} \right) = n$.

xii. Show that $\left(\begin{array}{c} n+1 \\ k+1 \end{array} \right) = \left(\begin{array}{c} n \\ k \end{array} \right) + \left(\begin{array}{c} n \\ k+1 \end{array} \right)$.

xiii. Deduce that $\left(\begin{array}{c} n \\ k \end{array} \right) \in \mathbb{N}$. (Hint: By induction on n).

xiv. Show that for $n \in \mathbb{N}$ and $0 \leq k \leq n$, a set with n elements has $\left(\begin{array}{c} n \\ k \end{array} \right)$ subsets with k elements.

xv. Show that for $n \in \mathbb{N}$ and $k \in \mathbb{N}$ with $k \leq n$, a set with n elements has $\left(\begin{array}{c} n \\ k \end{array} \right)$ subsets with k elements.

xvi. Show that for x, $y \in \mathbb{R}$ and $n \in \mathbb{N}$,

$$(x+y)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) x^k y^{n-k}.$$

(Hint: By induction on n).

xvii. Show that $\sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) = 2^n$.

xviii. Show that $\sum_{k=0}^{n} (-1)^k \left(\begin{array}{c} n \\ k \end{array} \right) = 0$.

xix. Compute $(x+y+z)^3$ in terms of x, y and z.

xx. Compute $(x+y+z)^4$ in terms of x, y and z.

xxi. Show that for $x > 1$ and $n \in \mathbb{N}$, $(x-1)^n \geq x^n - nx^{n-1}$.

xxii. Show that for $x < 1$, $(1-x)^n \geq 1 - nx$.

xxiii. Show that for $n \in \mathbb{N} \setminus \{0\}$, $(1+\frac{1}{n})^n \leq (1+\frac{1}{n+1})^{n+1}$.

xxiv. Find and prove (by induction) formulas for the sums

$$\frac{3}{1^2 \cdot 2^2} + \frac{5}{2^2 \cdot 3^2} + \cdots + \frac{2n+1}{n^2 \cdot (n+1)^2}$$

and

$$1 + 9 + 25 + \cdots + (2n+1)^2.$$

xxv. Prove by induction that for all real numbers a and b and natural number n,

$$(a^n + a^{n-1}b + a^{n-2}b^2 + \cdots ab^{n-1} + b^n)(a-b) = a^{n+1} - b^{n+1}.$$

Chapter 6

Bijections, revisited

6.1 Schröder-Bernstein's Theorem

The next result is probably the first nontrivial result of the book.

Theorem 6.1.1 (Schröder-Bernstein) *Let A and B be two sets. If there are injections from A into B and from B into A, then there is a bijection between A and B.*

Proof: Let $f : A \longrightarrow B$ and $g : B \longrightarrow A$ be two injections. Given $a \in A$, consider the finite or infinite sequence $(a, f(a), g(f(a)), f(g(f(a))), \ldots)$. If this sequence ends at B, call the point a a B-point.

6.2 Examples of Sets in Bijection

Two sets are said to be in bijection if there is a bijection between them. It is clear that two finite sets are in bijection if and only if they have the same number of elements. It is also clear that a finite set cannot be in bijection with an infinite set.

Although a finite set cannot be in bijection with one of its proper subsets, an infinite set can be in bijection with one of its subsets. For example the map $x \mapsto x + 1$ is a bijection between $\mathbb{N}$ and $\mathbb{N} \setminus \{0\}$. The map $x \mapsto 2x$ is a bijection between $\mathbb{Z}$ and $2\mathbb{Z}$.

We do not have enough tools for the moment to prove the following theorems:

Theorem 6.2.1 *If X is an infinite set and $x \in X$, then there is a bijection between X and $X \setminus \{x\}$.*

We will prove this theorem in the next part. But we can prove the following results – although naively.

Theorem 6.2.2 *If X is an infinite set then there is an injection from $\mathbb{N}$ into X.*

Proof: We will define an injection $f : \mathbb{N} \longrightarrow X$. Let $x_0 \in X$, $x_1 \in X \setminus \{x_0\}$ and for each $n \in \mathbb{N}$, let $x_{n+1} \in X \setminus \{x_0, \ldots, x_n\}$. Since X is infinite we can continue this procedure of choosing an element x_{n+1} not equal to any of the previously chosen elements $x_0, \ldots, x_n$. Set $f(n) = x_n$. Then clearly f is an injection from $\mathbb{N}$ into $\mathbb{N}$. □

Theorem 6.2.3 *If A is an infinite subset of $\mathbb{N}$, then there is a bijection between $\mathbb{N}$ and A.*

We will give a naive proof of this result later on in this part. Now we will find some bijections between unexpected sets. If there is a bijection between two sets X and Y, we will represent this fact as $X \sim Y$. Note that

$X \sim X$
If $X \sim Y$ then $Y \sim X$
If $X \sim Y$ and$Y \sim Z$ then $Y \sim X$

Chapter 7

Some Automorphism Groups

7.1 Binary Unirelational Structures

A **binary unirelational structure** Γ is a set X together with a binary relation R. Thus a binary unirelational structure Γ is a pair (X, R) where X is a set and R is a binary relation Γ.

An **isomorphism** of a binary unirelational structure (X, R) onto another binary unirelational structure (Y, S) is a bijection $f : X \longrightarrow Y$ such that for any $x_1\, x_2 \in X$, $x_1 R x_2$ if and only if $f(x_1) R f(x_2)$. Two binary relational structures among which there is an isomorphism are called **isomorphic**. An isomorphism from a graph onto itself is called an **automorphism** of the binary unirelational structure. The set of all automorphisms of a binary unirelational structure Γ is called the **automorphism group** of Γ and is denoted by $\mathrm{Aut}(\Gamma)$.

The **dual** of a binary unirelational structure (X, R) is the binary unirelational structure (X, S) defined as follows:

$$xSy \iff x \not R y,$$

i.e. xSy if and only if xRy does not hold.

Exercises.

i. Show that the set $\mathrm{Aut}(\Gamma)$ of all automorphisms of a binary unirelational structure Γ is is closed under composition and inversion.

ii. Show that the automorphism groups of a binary unirelational structure and of its dual are equal.

iii. Let (X, R) and (Y, S) be two binary unirelational structures. Let ϕ be an isomorphism from (X, R) onto (Y, S). Show that

$$\mathrm{Aut}(Y, S) = \phi\, \mathrm{Aut}(X, R) \phi^{-1}.$$

7.2 Automorphism Groups of Graphs

A **graph** Γ is a set X together with a symmetric and irreflexive binary relation X. Thus a graph Γ is a pair (X, R) where X is a set and R is a symmetric and irreflexive binary relation X.

If (X, R) is a graph and x, $y \in X$ are such that xRy then we say that x and y are **connected**. We often write $x - y$ instead of xRy. We also say that x and y are **related**.

The **complete graph** on a set X is the graph where any two distinct x, $y \in X$ are related.

Exercises.

i. Show that the automorphism group of a complete graph on a set X is $\mathrm{Sym}(X)$.

ii. Let us find all graph structures on the set $X = \{1, 2, 3\}$. For any two distinct points x and y we know that if $x - y$ then $y - x$, so to shorten our writing, we will write only one of the two relations.

$\Gamma_\emptyset$: no relations at all
Γ_3 : only $1 - 2$ (and $2 - 1$ of course)
Γ_2 : only $1 - 3$
Γ_1 : only $2 - 3$
Γ_{13} : only $1 - 2$ and $2 - 3$
Γ_{12} : only $1 - 3$ and $2 - 3$
Γ_{23} : only $1 - 2$ and $1 - 3$
Γ_{123} : all possible relations $1 - 2$, $2 - 3$ and $1 - 3$

iii. ¶ Show that Γ_1, Γ_2 and Γ_3 are isomorphic. Show that Γ_{13}, Γ_{12} and Γ_3 are isomorphic. Show that G_1 and G_{23} are duals of each other.

Thus on X there are only fundamentally different (i.e. nonisomorphic) graph structures, $\Gamma_\emptyset$, Γ_1, Γ_{23} and Γ_{123}.

iv. Let X be a set. Let Γ be the set of subsets of X with two elements. On Γ define the relation $\alpha R \beta$ if and only if $|\alpha \cap \beta| = 1$. Then Γ becomes a graph with this relation.

a) Calculate $\mathrm{Aut}(\Gamma)$ when $|X| = 4$.

b) Draw the dual of Γ when $|X| = 5$.

c) Show that for any α, $\beta \in \Gamma$ there is an automorphism $\phi \in \mathrm{Aut}(\Gamma)$ such that $\phi(\alpha) = \beta$.

d) Calculate $\mathrm{Aut}(\Gamma)$ when $|X| = 5$.

v. Show that $\mathrm{Aut}(\Gamma_\emptyset) = \mathrm{Aut}(\Gamma_{123}) = \mathrm{Sym}(3)$ and $\mathrm{Aut}(\Gamma_1) = \mathrm{Aut}(\Gamma_{23}) = \{1, (2, 3)\}$.

vi. Show that the automorphism group of a graph Γ on $X = \{1, 2, 3, 4\}$ is the automorphism group of one of the following graphs:

$\Gamma_\emptyset$: no relations at all
Γ_{12} : only $1-2$ (and $2-1$ of course)
Γ_{123} : only $1-2$ and $2-3$
Γ_{12-34} : only $1-2$ and $3-4$
Γ_{1234} : only $1-2$, $2-3$ and $3-4$
Γ_* : only $1-2$, $1-3$ and $1-4$

Show that

$\mathrm{Aut}(\Gamma_\emptyset) = Sym(4)$
$\mathrm{Aut}(\Gamma_{12}) = \mathrm{Aut}(\Gamma_{12-34}) = \{1, (1,2), (3,4), (1,2)(3,4)\}$
$\mathrm{Aut}(\Gamma_{123}) = \{1, (1,3)\}$
$\mathrm{Aut}(\Gamma_{12-34}) = \{1, (12), (34), (12)(34), (13)(24), (23)(14), (1324), (1223)\}$
$\mathrm{Aut}(\Gamma_{1234}) = \{1, (14)(23)\}$
$\mathrm{Aut}(\Gamma_*) = \{1, (12), (13), (23), (123), (132)\}$

Draw the multiplication table of $\mathrm{Aut}(\Gamma_{12-34})$

vii. Let Γ be a graph such that for any α, α_1, β, β_1, if $\alpha \neq \alpha_1$ and $\beta \neq \beta_1$, then there is a $\phi \in \mathrm{Aut}(G)$ such that $\phi(\alpha) = \beta$ and $\phi(a_1) = \beta_1$. What can you say about Γ?

viii. Find a graph Γ on six points such that $\mathrm{Aut}(\Gamma) = \{Id\}$.

ix. Find a finite graph Γ such that $|\mathrm{Aut}(\Gamma)| = 3$.

x. Let $n \geq 3$ and let Γ be the cyclic graph on $\{1, 2, \ldots, n\}$, i.e. the only relations are $1-2-3-\ldots-(n-1)-n-1$. Show that $\rho := (1, 2, \ldots, n) \in \mathrm{Aut}(\Gamma)$. Show that $\tau = (2, n)(3, n-1)\ldots \in \mathrm{Aut}(\Gamma)$. (For example if $n = 6$ then $\tau = (2, 6)(3, 5)$, if $n = 7$ then $\tau = (2, 7)(3, 6)(4, 5)$). Show that

$$\mathrm{Aut}(\Gamma) = \{\rho^i \tau^j : i = 0, 1, \ldots, n-1 \text{ and } j = 0, 1\}$$

and that $|\mathrm{Aut}(\Gamma)| = 2n$.

7.3 Geometric Automorphism Groups

Problem 7.3.1 (Isometries of $\mathbb{R}$) *Let $G := \{g : \mathbb{R} \longrightarrow \mathbb{R} : |x - y| = |g(x) - g(y)|\}$. We will show that G is a group under composition and we will find all the elements of G. Note that G is clearly closed under composition and $Id_\mathbb{R} \in G$. Also if $g \in G$ is a bijection, then $g^{-1} \in G$ as well. To show that G is a group, we just need to show that the elements of G are bijections.*

i. *Show that any element of G is one-to-one.*

ii. *For $a \in \mathbb{R}$, let $\tau_a : \mathbb{R} \longrightarrow \mathbb{R}$ be given by $\tau_a(x) = x + a$ (translation). Show that $\tau_a \in G$. Show that the set $T = \{\tau_a : a \in \mathbb{R}\}$ is a group under composition.*

iii. *For $\epsilon = \pm 1$, let $\rho_\epsilon : \mathbb{R} \longrightarrow \mathbb{R}$ be given by $\rho_\epsilon(x) = \epsilon x$. Show that $\rho_\epsilon \in G$. Show that the set $R = \{\rho_1, \rho_{-1}\}$ is a group under composition.*

iv. *Show that for any $g \in G$ there are unique $\epsilon \in \{1, -1\}$ and $a \in \mathbb{R}$ such that $g = \tau_a \circ \rho_\epsilon$. Conclude that the elements of G are bijections.*

v. *Conclude that G is a group under composition.*

The group G is called the **group of isometries** *of $\mathbb{R}$.*

Problem 7.3.2 (Isometries of $\mathbb{R}^2$) *Let $G := \{g : \mathbb{R}^2 \longrightarrow \mathbb{R}^2 : |x - y| = |g(x) - g(y)|\}$. We will show that G is a group under composition and we will find all the elements of G explicitly. Note that G is clearly closed under composition and $Id_{\mathbb{R}} \in G$. Also if $g \in G$ is a bijection, then $g^{-1} \in G$ as well. To show that G is a group, we just need to show that the elements of G are bijections.*

Note that G is the set of functions from $\mathbb{R}^2$ into $\mathbb{R}^2$ that send any circle into a circle of the same radius.

i. *Show that any element of G is one-to-one.*

ii. *For $(a, b) \in \mathbb{R}^2$, let $\tau_{(a,b)} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ be given by $\tau_{(a,b)}(x, y) = (x+a, y+b)$ (translation). Show that $\tau_{(a,b)} \in G$. Show that the set $T := \{\tau_{(a,b)} : (a, b) \in \mathbb{R}\}$ is a group under composition.*

iii. *For $\theta \in [0, 2\pi)$, let $\rho_\theta : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ be the clockwise rotation of angle θ around the center $(0, 0)$, i.e. $\rho_\theta(x, y) = (x\cos(\theta) - y\sin(\theta), x\sin(\theta) + y\cos(\theta))$. Show that $\rho_\theta \in G$. Show that the set $R := \{\rho_\theta : \theta \in [0, 2\pi)\}$ is a group under composition.*

iv. *For $\epsilon = \pm 1$, let $\sigma_\epsilon : \mathbb{R} \longrightarrow \mathbb{R}$ be given by $\sigma_\epsilon(x, y) = (x, \epsilon y)$. Show that $\sigma_\epsilon \in G$. Show that the set $S = \{\sigma_1, \sigma_{-1}\}$ is a group under composition.*

v. *Show that for any $g \in G$ there is a unique $(a, b) \in \mathbb{R}^2$ such that such that $(\tau_{a,b} \circ g)(0, 0) = (0, 0)$.*

vi. *Show that for any $g \in G$ such that $g(0, 0) = (0, 0)$ there is there is a unique $\theta \in [0, 2\pi)$ such that $(\rho_\theta \circ g)(0, 0) = (0, 0)$ and $(\rho_\theta \circ g)(1, 0) = (1, 0)$*

vii. *Show that for any $g \in G$ such that $g(0, 0) = (0, 0)$ and $g(1, 0) = (1, 0)$ we have $g(0, 1) = (0, \epsilon)$ for some $\epsilon = \pm 1$. Conclude that for such g there is a unique $\epsilon = \pm 1$ such that $(s_\epsilon \circ g)(0, 0) = (0, 0)$, $(s_\epsilon \circ g)(1, 0) = (1, 0)$ and $(s_\epsilon \circ g)(0, 1) = (0, 1)$.*

vii. *Show that if $g \in G$ is such that $g(0, 0) = (0, 0)$, $g(1, 0) = (1, 0)$ and $g(1, 0) = (1, 0)$, then $g = \mathrm{Id}_{\mathbb{R}^2}$.*

viii. *Conclude that for any $g \in G$ there are unique $(a, b) \in \mathbb{R}^2$, $\theta \in [0, 2\pi)$ and $\epsilon = \pm 1$ such that $g = \tau_{(a,b)} \circ \rho_\theta \circ \sigma_\epsilon$. Conclude that g is a bijection.*

ix. *Conclude that G is a group under composition.*

The group G is called the **group of isometries** *of $\mathbb{R}$.*

x. *Conclude that an element of G sends a line onto a line.*

Problem 7.3.3 (Affine Transformations of $\mathbb{R}^2$) *Let $G := \{g : \mathbb{R}^2 \longrightarrow \mathbb{R}^2 :$ g is a bijection and sends a line into a line$\}$. It is clear that G is a group under composition. We will find all the elements of G explicitly. As we have noticed in the end of Problem 7.3.2, the elements of the group defined there are in G. Thus the groups T and R are subsets of G. We adopt the same terminology.*

i. *Show that an element of G respect the parallelism, i.e. sends two parallel lines onto two parallel lines.*

ii. *For $c \in \mathbb{R}^{>0}$, let $h_c : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ be defined by $h_c(x, y) = (cx, y)$. Show that $h_c \in G$ and that the set $H := \{h_c : c \in \mathbb{R}^{>0}\}$ is a group under composition.*

iii. *For $d \in \mathbb{R}$ define $u_d : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ by $u_d(x, y) = (x + dy, y)$. Show that $u_d \in G$ and that the set $U := \{t_d : d \in \mathbb{R}\}$ is a group under composition.*

iv. *For a bijection phi $: \mathbb{R} \longrightarrow \mathbb{R}$ satisfying the properties $\phi(x + y) = \phi(x) + \phi(y)$, $\phi(xy) = \phi(x)\phi(y)$ and $\phi(1) = 1$, define the map $\alpha_\phi : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ by $\alpha_\phi(x, y) = (\phi(x), \phi(y))$. Show that $\alpha_\phi \in G$ and that the set $A := \{\alpha_\phi :$ ϕ as above$\}$ is a group under composition.*

v. *Show that for any $g \in G$ there is a unique $(a, b) \in \mathbb{R}^2$ such that such that $(\tau_{a,b} \circ g)(0, 0) = (0, 0)$.*

vi. *Show that for any $g \in G$ such that $g(0, 0) = (0, 0)$ there is there is a unique $\theta \in [0, 2\pi)$ such that $(\rho_\theta \circ g)(0, 0) = (0, 0)$ and $(\rho_\theta \circ g)(1, 0)$ is on the positive side of the x-axis.*

vii. *Show that for any $g \in G$ such that $g(0, 0) = (0, 0)$ and $g(1, 0)$ is on the positive side of the x-axis, there is a unique $c \in \mathbb{R}^{>0}$ such that $(h_c \circ g)(0, 0) = (0, 0)$ and $(h_c \circ g)(1, 0) = (1, 0)$.*

viii. *Show that for any $g \in G$ such that $g(0, 0) = (0, 0)$ and $g(1, 0) = (1, 0)$ there is a unique $d \in \mathbb{R}$ such that $(u_d \circ g)(0, 0) = (0, 0)$, $(u_d \circ g)(1, 0) = (1, 0)$ and $(u_d \circ g)(0, 1) = (0, 1)$.*

ix. *Show that if $g \in G$ satisfies $g(0, 0) = (0, 0)$, $g(1, 0) = (1, 0)$ and $g(0, 1) = (0, 1)$, then $g \in A$. (Hint: Express the addition and multiplication of real numbers geometrically and use part (i)).*

x. *Show that for any $g \in G$ there are unique $(a, b) \in \mathbb{R}^2$, $\theta \in [0, 2\pi)$, $c \in \mathbb{R}^{>0}$, $d \in \mathbb{R}$ and bijection phi $: \mathbb{R} \longrightarrow \mathbb{R}$ satisfying the properties $\phi(x + y) = \phi(x)+\phi(y)$, $\phi(xy) = \phi(x)\phi(y)$ and $\phi(1) = 1$, such that $g = \tau_{(a,b)} \circ \rho_\theta \circ h_c \circ u_d \circ \alpha_\phi$.*

The group G is called the **affine transformations** *of $\mathbb{R}^2$.*

Problem 7.3.4 *On $\mathbb{R}^2$ define the metric $d((x, y), (z, t)) := |z - x| + |t - y|$. Let G be the group of isometries of this metric. Find the elements of G.*

Problem 7.3.5 *On $\mathbb{R}^2$ define the metric $d((x, y), (z, t)) := \max(|z - x|, |t - y|)$. Let G be the group of isometries of this metric. Find the elements of G.*

7.4 Back and Forth Argument

In this subsection we will prove two theorems using an interesting method called **back and forth**.

7.4.1 Dense Total Orderings

Theorem 7.4.1 *Any two countable dense total orderings without end points are isomorphic.*

Corollary 7.4.2 *A countable dense total ordering is ω-homogeneous.*

7.4.2 Random Graphs

Theorem 7.4.3 *Any two countable random graphs are isomorphic.*

Corollary 7.4.4 *A countable random graph is ω-homogeneous.*

Chapter 8

Formulae

In this chapter, we will see the formulae of set theory.

Formulae are like sentences of a language. Like any language, mathematical languages have alphabets. All mathematical languages include the following symbols:

Logical Connectives. There are two of those: $\wedge$ called **conjunction** and $\neg$ called **negation**.

Existential Quantifier. There is only one: *exists*.

Parentheses. There are two kinds of parentheses, left parenthesis (and right parenthesis).

Equality Symbol. The equality is symbolized by $=$, or by $\equiv$ sometimes.

Variables. There are an infinity of them: v_0, v_1, v_2, $v_3, \ldots$

Instead of the infinitely many variables, we could have adapted only two symbols v and $|$ and use

v for v_0
$v|$ for v_1
$v||$ for v_2
$v|||$ for v_3 etc.

Apart from these symbols, each mathematical theory has its own specific symbols. Set theory has only one specific symbol: $\in$, called the **membership relation**.

Thus the symbols we will use to write the formulae in set theory are the following:

$$\wedge, \neg, \exists, (,), =, \in, v_0, v_1, v_2, v_3, \ldots$$

These symbols – although do have an intended meaning – do not have a meaning. They are only symbols and nothing more.

The formulae will be certain "words" in this alphabet, i.e. a finite string of symbols written only using these symbols.

Chapter 9

Miscellaneous Exercises

i. Let $\phi : \mathbb{R} \longrightarrow \mathbb{R}$ be such that $\phi(x+y) = \phi(x) + \phi(y)$ for all $x, y \in \mathbb{R}$.

a) Assume $\phi(x^2) = \phi(x)^2$. Show that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in \mathbb{R}$ and $\phi(q) = q$ for all $q \in \mathbb{Q}$.

b) Assume $\phi(x^{-1}) = \phi(x)^{-1}$. Show that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in \mathbb{R}$.

Part II

Axiomatic Set Theory

Chapter 10

Basics

10.1 Russell's Paradox

A century ago, mathematicians, as common people do, believed that any set of objects could be a set in the mathematical sense. For example, they could speak about the set of all sets without much questioning the use of the term "set".

After reading the first volume of a work of Frege, Bertrand Russell found the following mathematical paradox:

Russell's Paradox. Let X be the set of all sets. Let

$$Y := \{x \in X : x \notin x\}.$$

Thus a set x is in Y if and only if $x \notin x$. In symbols:

$$\forall x \ (x \in Y \iff x \notin x).$$

Since Y is a set, the formula above – that holds for all sets x – should also hold for Y. Replacing x by Y we get:

$$Y \in Y \iff Y \notin Y.$$

In English this translates as follows: Y is an element of itself if and only if it is not an element of itself. This is certainly a contradiction, and a contradiction in set theory, the basis of all mathematics, therefore of all sciences... This is very serious, and one cannot just ignore it.

Russell's Paradox changed the way mathematicians looked at mathematics; from naive mathematicians – that believed naively that any collection could be a set – they turned into more careful creatures.

A careful analysis of the above paradox (like the one a careful creature would carry out) reveals that the acceptance of the collection of all sets as a set is the source of the problem. The collection of all sets is certainly something, a

"collection" for example, but is not allowed to be a set itself. Something that contains all sets cannot – or should not be – a set, because otherwise we arrive at a contradiction...

What to do?

The solution is the following: be much more careful before naming something a set. Set the rules for something to be a set and insure that each naive set is really a set, i.e. that it passes the test of being a set.

The experience shows that collections which are too large cause problems. Therefore our test should exclude too large collections from being sets. The easiest way to avoid big collections from being sets is to start from the smallest of all sets, the emptyset, and to construct the other sets step by step from the emptyset, by taking the unions, the intersections, the products, the "set" of subsets of the previously constructed sets to construct new sets. By doing so, one should never have enough time to arrive at large collections for them to be sets. For example, if the steps never end, if after each step we can take the next step to invent new sets, during this procedure, we will never meet the collection of all sets. This is the idea behind Russell's theory of types as well as the Zermelo-Fraenkel set theory that we will expose in this book.

10.2 Easy Axioms

We accept the two undefined terms "set" and "being an element of". If x and y are sets and x is an element of y, we write $x \in y$, otherwise we write $x \notin y$. In this case, we also say that "x is in y" or "x is not in y" respectively. The elements of a set will be sets themselves. Every object we will define will be a set, including objects like "function" and "equivalence relation".

We do not know whether any set exists yet. They may or may not exist. We create our first set:

A1. Emptyset. *There exists a set with no elements.*

This is an axiom and we accept it without any discussions.

Formally this axiom is written as

$$\exists x \forall y \, y \notin x.$$

Now the following question arises: How many sets without elements are there? We would like to say that there is only one set without elements. This would be saying that the set of humans with five heads on their shoulders is equal to the set of apple trees of 3000 meters long, since both sets are - presumably - empty.

To prove that there is only one set with no elements, we assume that x and y are two sets with no elements and we proceed to show that $x = y$. But since we do not know the meaning of the equality of two sets, we cannot proceed! The second axiom will tell us exactly when two sets are equal.

A2. Equality. *Two sets which have the same elements are equal.*

Formally this axiom is written as

$$\forall x \forall y \, (\forall z \, (z \in x \iff z \in y) \to x = y).$$

Now we can prove our first theorem:

Theorem 10.2.1 *There is only one set without elements.*

Proof: By A1 we know that there is at least one set without elements. Let x and y be "two" sets without elements. Assume that $x \neq y$. Then by A2, there is an element in one of them which is not in the other. But this is absurd because none of the sets can have elements. Thus it is not true that $x \neq y$. Hence $x = y$. □

The statement of the theorem can be written as follows:

$$\exists x (\forall y \, y \notin x \wedge \forall z ((\forall t \, t \notin z) \to z = x)).$$

The unique set without elements is called **emptyset** and is denoted by the symbol $\emptyset$.

We will use the symbol $\emptyset$ in our formal formulas as an abbreviation.

We prove a statement which is not supposed to make any sense at this point (because $\sqrt{2}$ is not defined yet):

Theorem 10.2.2 *For any $x \in \emptyset$, $x = \sqrt{2}$.*

Proof: Assume not. Then $\emptyset$ contains an element which is not equal to $\sqrt{2}$. But this is absurd because $\emptyset$ does not contain any elements at all! □

What saves us from a contradiction in the statement above is that emptyset has no elements. But if it had one, this element would have to be equal to $\sqrt{2}$, and as you must have guessed to π as well. Fortunately $\emptyset$ has no elements and we do not get a contradiction of the form "$\sqrt{2} = \pi$".

A set x is called a **subset** of another set y if any element of x is an element of y. We then write $x \subseteq y$.

Formally we write this as

$$x \subseteq y \iff \forall z (z \in x \to z \in y).$$

We use the symbol $\iff$ as an abbreviation for the English phrase "if and only if", while the symbol $\leftrightarrow$ is used as a mathematical symbol.

To prove that x is a subset of y we need to prove that x and y are sets and that every element of x is an element of y.

Clearly every set is a subset of itself. Formally $\forall x \, x \subseteq x$.

Theorem 10.2.3 *$\emptyset$ is a subset of every set.*

Proof: Let x be a set. Assume $\emptyset$ is not a subset of x. Then by definition, there is an element in $\emptyset$ which is not in x. But $\emptyset$ has no elements. Thus $\emptyset$ cannot have an element which is not in x. Hence $\emptyset \subseteq x$. □

Formally, the above statement can be written as follows: $\forall x \ \emptyset \subseteq x$, where $\emptyset \subseteq x$ is in fact an abbreviation of a longer sentence.

Theorem 10.2.4 *$\emptyset$ is the only subset of $\emptyset$.*

Proof: Let x be a subset of $\emptyset$. If $x \neq \emptyset$, then there is an element y in x. Since $x \subseteq \emptyset$, y is also an element of $\emptyset$. Contradiction. Thus $x = \emptyset$. □

A3. Definable Subsets. *Let x be a set and $\phi(y)$ a "property". Then there is a set whose elements are exactly the elements of x that satisfy the property ϕ.*

We will be unprecise about the meaning of the word "property". The reader should only be aware that "properties" are given by finite formulas that involve only the mathematical symbols

$$\forall, \exists, \wedge, \vee, \rightarrow, \iff, (,), =, \neg,$$

the abbreviations like $\emptyset$ and $\subseteq$, variables like x, y and z and constants (parameters, the existing sets).

By A2, given x and ϕ, the set as in A3 is unique. We denote this set as

$$\{y \in x : \phi(y)\}.$$

Using this axiom we can prove that the intersection of two sets is a set.

Theorem 10.2.5 *If x and y are sets then there is a set whose elements are exactly the common elements of x and y.*

Proof: Let $\phi(z)$ be $z \in y$. Use A3 to see that $\{z \in x : \phi(z)\}$ is a set. This set is exactly the set of common elements of x and y. □

By A2, given x and y, the set given in Theorem 10.2.5 is unique. We call this set the **intersection** of x and y and we denote it by $x \cap y$.

Thus $z \in x \cap y \iff (z \in x) \wedge (z \in y)$.

Axiom A3 allows us to prove that the difference of two sets is a set:

Theorem 10.2.6 *If x and y are sets then there is a set whose elements are exactly the elements of x which are not in y.*

Proof: Let $\phi(z)$ be $z \notin y$. Use A3 to see that $\{z \in x : \phi(z)\}$ is a set. This set is exactly the set of elements of x which are not in y. □

By A2, given x and y, the set given in Theorem 10.2.6 is unique. We denote this set by $x \setminus y$. It can be called "x minus y".

Now we prove that a certain collection cannot be a set:

Theorem 10.2.7 (Bertrand Russell) *There is no set that contains all sets as elements.*

Proof: Assume not. Let x be a set that contains all sets as elements. Let $\phi(y)$ be "$y \notin y$" Consider the set

$$z := \{y \in x : \phi(y)\} = \{y \in x : y \notin y\}.$$

z is a set by A3. For any set y, we have

$$y \in z \iff y \notin y.$$

Since the above statement holds for any set y and since z is a set, we may replace y of the formula above by z:

$$z \in z \iff z \notin z.$$

This is a clear contradiction. Thus x is not a set, or the set of all sets does not exist. □

At this point we cannot prove that the union of two sets is a set. We need the following axiom for this.

A4. Union of Two Sets. *If x and y are two sets, then there is a set whose elements are exactly the elements that are in either x or y. By A2 such a set is unique. It is called the* **union** *of x and y and is denoted by $x \cup y$.*

Thus we have $z \in x \cup y \iff (z \in x) \vee (z \in y)$.

Later on we will adopt a more general axiom than A4.

There are some relationships between $\cup$ and $\setminus$:

$$(x \setminus y) \setminus z = x \setminus (y \cup z)$$
$$y \cup (x \setminus y) = x \cup y$$

With the first four axioms in hand, we can only be sure of the existence of $\emptyset$, indeed:

1) The first axiom tells us that emptyset exists.

2) The second axiom cannot be used to create new sets.

3) The new sets obtained by A3 are subsets of the old sets. Thus, starting from $\emptyset$, we cannot obtain new sets using A3.

4) If x and y are emptysets, the new set obtained using A4 is also emptyset, hence not new.

Another way of seeing this is by noticing that the universe that contains only emptyset as a set satisfies all four axioms.

Now we will adopt a new axiom that will allow us to define new sets.

A5. Sets with One Elements. *If x is a set, then there is a set which has only x as an element.*

We write this set as $\{x\}$.

Now, starting from $\emptyset$, we can obtain new sets:

$$\begin{gathered}\emptyset\\ \{\emptyset\}\\ \{\{\emptyset\}\}\\ \{\{\{\emptyset\}\}\}\\ \dots\end{gathered}$$

These sets have only one element. Such sets are called **singleton** sets. A set whose elements are x and y is denoted by $\{x, y\}$. If we can name all the elements of a set one by one and enumerate them as $a_1, \dots, a_n$, then we will denote this set by $\{a_1, \dots, a_n\}$.

Using A4, we can obtain sets with more than one element:

$$\begin{gathered}\{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}\\ \{\emptyset, \{\emptyset\}\} \cup \{\{\{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}\end{gathered}$$

Now we define "zero" as the emptyset:

$$0 := \emptyset.$$

Given a set x, we define its successor $S(x)$ as

$$S(x) = x \cup \{x\}.$$

By axioms A4 and A5, $S(x)$ is a set. Next we define 1, 2, 3 etc. as follows:

$$\begin{array}{lllllll}
1 & := & S(0) & = & 0 \cup \{0\} & = & \{0\}\\
2 & := & S(1) & = & 1 \cup \{1\} & = & \{0\} \cup \{1\} = \{0, 1\}\\
3 & := & S(2) & = & 2 \cup \{2\} & = & \{0, 1\} \cup \{2\} = \{0, 1, 2\}\\
4 & := & S(3) & = & 3 \cup \{3\} & = & \{0, 1, 2\} \cup \{3\} = \{0, 1, 2, 3\}\\
\dots & & & & & &
\end{array}$$

By using our axioms and results we can form sets that contain any finite number of these sets. For example, $\{0, 3\}$ is a set because

$$\{0, 3\} = 1 \cup (4 \setminus 3).$$

To prove that $\{0, 3\}$ is a set we can also use A3 with $x = 4$ and $\phi(y)$ as "$y = 0 \vee y = 3$".

Although we now have sets with as many elements as we wish, we are still not sure that there are sets with infinitely many elements. For example, we do not know that yet that there is a set that contains 0, 1, 2, 3, 4,... In fact, we cannot prove yet that there is such a set. We need a new axiom for this. Before creating sets with infinitely many elements, we will state a few more axioms and we will define some basic notions of set theory.

10.3 Slightly More Complicated Axioms

A4′. Union. *If x is a set, then there is a set whose elements are exactly the elements of the elements of x.*

This axiom tells us that the union of the elements (remember that the elements of a set are sets as well) of a set is a set.

Although we do not know whether there are sets with infinitely many elements, the set x in A4′ could have - hypothetically - infinitely many elements.

If $x = \{a, b\}$, then the set obtained by A4′ is just $a \cup b$. Similarly, if $x = \{a, b, c\}$, then the set obtained by A4′ is just $a \cup b \cup c$.

We denote the set given by A4′ by $\cup x$ or $\cup_{y \in x} y$. Note that

$$z \in \cup x \Leftrightarrow \exists y (y \in x \wedge z \in y).$$

For the moment, A4′ is not stronger than A4, because, given two sets x and y, we do not know yet that $\{x, y\}$ is a set. We now adopt an axiom that will solve this problem:

A5′. Sets with Two Elements. *If x and y are sets then there is a set whose elements are only x and y.*

We denote this set as $\{x, y\}$ of course. By taking $x = y$ in A5′, we see that A5 is a consequence of A5′, therefore we can erase A5 from the list of our axioms. Also, as we have noticed A4 is a consequence of A4′ and A5′, and we can also erase A4 from our list.

Lemma 10.3.1 $\cup \emptyset = \emptyset$.

Proof: By definition, for any set x, $z \in \cup x$ if and only if there exists a $y \in x$ such that $z \in y$. Apply this to $x = \emptyset$: $z \in \cup \emptyset$ if and only if there exists a $y \in \emptyset$ such that $z \in y$. Thus $\cup \emptyset$ cannot have an element. □

We can also form the intersection of all sets which are the elements of a given set:

Theorem 10.3.2 *Let x be a set. Then there is a set whose elements are exactly the elements of $\cup x$ which are elements of all the elements of x.*

Proof: Let $\phi(z)$ be "$\forall y (y \in x \rightarrow z \in y)$". Now use A3: $\{z \in \cup x : \phi(z)\}$ is the set we are looking for. □

This set is denoted by $\cap x$ or $\cap_{y \in x} y$. Thus

$$z \in \cap x \Leftrightarrow \forall y \ (y \in x \rightarrow z \in x).$$

The following statement cannot be proven: "Let x be a set. Then there is a set whose elements are exactly the common elements of all the elements of x." Because to prove that this is a set we need x to be nonempty. Indeed, if we adopted this definition, $\cap \emptyset$ would be the set of all sets, creating Russell's Paradox.

A6. Power Set. *If x is a set then there is a set whose elements are exactly the subsets of x.*

We denote this set with the symbol $\wp(x)$ and call it the **power set** of x. Thus

$$y \in \wp(x) \iff y \subseteq x.$$

For example if $x = 2 = \{0, 1\}$, then

$$\wp(x) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}.$$

Note that $\emptyset$ and x are always elements of $\wp(x)$.

Even after these more complicated axioms, we still cannot prove that infinite sets exist, because given a finite set whose elements are finite sets all our axioms create only finite sets. In the next section we will adopt an axiom that will allow us "to be sure" of the existence of infinite sets. We should also say that we do not really know what "finite" or "infinite" means at this point since we did not define these concepts yet. Finiteness is not such an easy concept as we will later see.

10.4 Cartesian Product of Two Sets

If X and Y are two sets, one can form their Cartesian product $X \times Y$. In this section we will define $X \times Y$ mathematically. The elements of $X \times Y$ will be entities denoted as (x, y) for $x \in X$ and $y \in Y$. We will first define these pairs (x, y). The only property of the pairs (x, y) which will interest us will be the following:

$$(x, y) = (z, t) \iff x = z \text{ and } y = t.$$

So we will define the pair (x, y) as a set satisfying the above property.

For two sets x and y, we let $(x, y) = \{\{x\}, \{x, y\}$. We call (x, y) the **(ordered) pair** of x and y.

Lemma 10.4.1 *i. (x, y) is a set.*
ii. $(x, y) = (z, t)$ if and only if $x = z$ and $y = t$.

Proof: See Exercise xxi, page 15. The second part follows also from Exercise vi, page 83. □

Lemma 10.4.2 *Let X and Y be two sets. Then there is a set $X \times Y$ whose elements are exactly the ordered pairs (x, y) for $x \in X$ and $y \in Y$.*

Proof: Since $x \in X$, we have $x \in X \cup Y$. Similarly $y \in X \cap Y$. It follows that the sets $\{x\}$ and $\{x, y\}$ are subsets of $X \cup Y$ and hence elements of $\wp(X \cup Y)$. Therefore $\{\{x\}, \{x, y\}\}$ is a subset of $\wp(X \cup Y)$. Hence $(x, y) = \{\{x\}, \{x, y\}\} \in \wp(\wp(X \cup Y))$. Thus all the elements of $X \times Y$ are elements of $\wp(\wp(X \cup Y))$. Now among the elements of $\wp(\wp(X \cup Y))$ we will distinguish the ones of the

form (x, y) by a formula $\phi(z)$, i.e. by a property. In other words, we will find a formula $\phi(z)$ such that for all z, the following will hold:

$$\phi(z) \iff \exists x \exists y \, (x \in X \wedge y \in Y \wedge z = \{\{x\}, \{x, y\}\}).$$

If we can do this, then we will have

$$X \times Y = \{z \in \wp(\wp(X \cup Y)) : \phi(z)\},$$

and so by A3, $X \times Y$ will be a set.

Now we find the formula $\phi(z)$ logically equivalent to

$$\exists x \exists y \, (x \in X \wedge y \in Y \wedge z = \{\{x\}, \{x, y\}\}).$$

In this "pseudo-formula" we can replace $z = \{\{x\}, \{x, y\}\}$ by

$$\exists t \exists u \, (t \in z \wedge u \in z \wedge t = \{x\} \wedge u = \{x, y\} \wedge \forall w \, (w \in z \to (w = t \vee w = u))).$$

In this "formula", the strings $t = \{x\}$ and $u = \{x, y\}$ are still nonacceptable. We replace $t = \{x\}$ by $x \in t \wedge \forall s \, (s \in t \to s = x)$. And we replace $u = \{x, y\}$ by $x \in u \wedge y \in u \wedge \forall s \, (s \in u \to (s = x \vee s = y))$. After doing all these replacements, we get $\phi(z)$, a legitimate formula. □

Exercises.

i. Find $X \times \emptyset$.

ii. Let x and y be two sets.

a) Show that $\{\{x\}, \{x, y\}\}$ is a set. Call this set (x, y).

b) Show that $(x, y) = (z, t)$ if and only if $x = z$ and $y = t$.

iii. Find $\cup 1$, $\cup 2$, $\cup 3$, $\cup 4$.

iv. Find $\cup \cup 4$.

v. Show that $\cup \wp(x) = x$.

vi. Show that $\cap \cap (x, y) = x$. Show that $y = (\cup \cup (x, y) \setminus \cap \cap (x, y)) \cup (\cap \cup (x, y))$.

vii. Let X be a set. Show that the diagonal $\{(x, x) : x \in X\}$ is a set.

viii. Let $A \subseteq X \times Y$ be a subset of $X \times Y$. Show that the object A^{-1} defined by

$$A^{-1} = \{(y, x) : (x, y) \in A\}$$

is a set.

ix. Find a formula $\phi(Z, T)$ such that $\phi(X \times Y, T)$ holds if and only if $T = X$. Find a formula $\psi(Z, T)$ such that $\phi(X \times Y, T)$ holds if and only if $T = Y$.

10.5 Functions

In naive set theory, a function f from a set X into a set Y is a rule that assigns to each element x of X a unique element $f(x)$ of Y. The graph of a function is the set of pairs (x, y) such that $x \in X$, $y \in Y$ and $y = f(x)$.

Since everything should be a set in set theory, we may attempt to define a function as its graph, hence as a subset F of $X \times Y$ with the property that for every $x \in X$ there is a unique $y \in Y$ such that $(x, y) \in F$. This attempt is not too far from the accepted definition of a function. We also need the sets X and Y in the definition.

Given a function $f : X \longrightarrow Y$, we can extend the set Y to a larger set Y_1 to get **another** function $f_1 : X \longrightarrow Y_1$: For each $x \in X$, just let $f_1(x) = f(x)$. Although the two functions f and f_1 take the same values with the same input, we would like to differentiate them, they should be two different functions. But this is impossible if we define a function only as its graph. So, rather than defining a function as its graph, we will define a function as a triple (F, X, Y) where $F \subseteq X \times Y$ will be the graph of the function. Here is the formal definition:

Let X and Y be two sets. A **function** or a **map** is a triple (F, X, Y) with the following properties:

i. F is a subset of $X \times Y$.

ii. For each $x \in X$ there is a unique $y \in Y$ such that $(x, y) \in F$.

The set X is called the **domain** and the set Y is called the **set of arrival** of the function. The set F is called the **graph** of the function.

In fact we do not need the domain X in the definition of a function, because given a graph $F \subset X \times Y$, the set X can be found back as follows: First of all note that $\cup\cup F = X \cup Y$. Now $X = \{x \in \cup\cup F : (x, y) \in G \text{ for some } y\}$. Given a a set F, we define $\pi_1(F)$ as the set $\{x \in \cup\cup F : (x, y) \in F \text{ for some } y\}$. Clearly $\pi_1(G)$ is a set. With this notation in hand, a reformed definition of a graph may be read as follows:

A **function** or a **map** is a pair (F, Y) such that

i. $F \subseteq \mathrm{pr}_1(F) \times Y$,

ii. For each $x \in \mathrm{pr}_1(F)$ there is a unique $y \in Y$ such that $(x, y) \in F$.

If $f = (F, Y)$ is a function, given $x \in \mathrm{pr}_1(F)$ the unique element y of Y for which $(x, y) \in F$ is denoted by $f(x)$

It may happen that we are not so much interested in Y, in which case we drop Y from the notation and we only say that f is a function (from X into Y).

If (f, Y) is a function and $(x, y) \in f$, we write $y = f(x)$.

If (f, Y) is a function from X into Y, we very often denote this fact as $f : X \longrightarrow Y$. The "rule" f may be made explicit by the notation $x \mapsto f(x)$.

When we say that $f : X \longrightarrow Y$ is a function, we assume implicitly that X and Y are sets and that $X \neq \emptyset$.

Very often the condition (ii) is easily checked. Condition (i) may be more tedious to check. One should not forget to prove (at this beginning stage of our mathematical education) that f is a set. The fact that f is a subset of $X \times Y$ will then be clear most of the time.

Lemma 10.5.1 (Identity Function) *Let X be a set. Then there is a function $\mathrm{Id}_X : X \longrightarrow X$ that satisfies $\mathrm{Id}_X(x) = x$.*

Proof: We need to check condition (i) of the definition. For this we just need to show that the diagonal

$$\delta(X) := \{(x, x) : x \in X\}$$

is a set. This is given in Exercise vii, page 83. □

The function $\mathrm{Id}_X : X \longrightarrow X$ is called the **identity function**.

Lemma 10.5.2 (Composition) *Let X, Y, Z be three sets. Let $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ be two functions. Define*

$$g \circ f := \{(x, z) : \exists y(y \in Y \wedge (x, y) \in f \wedge (y, z) \in g\}.$$

Then $g \circ f$ is a function from X into Z. We have

$$(g \circ f)(x) = g(f(x)).$$

Proof: It is clear that $g \circ f$ is a set and that it is a subset of $X \times Z$. We need to show condition (ii) of the definition of a function.

Given $x \in X$, there is a $y \in Y$ such that $(x, y) \in f$. Since $y \in Y$, there is a $z \in Z$ such that $(y, z) \in g$. Thus $(x, z) \in g \circ f$.

Assume now that (x, z) and (x, z_1) are two elements of $g \circ f$. We need to show that $z = z_1$. By definition of $g \circ f$ there are y, $y_1 n Y$ such that

$$(x, y) \in f \text{ and } (x, y_1) \in f \text{ and } (y, z) \in g \text{ and } (y_1, z_1) \in g.$$

The first two conditions imply $y = y_1$, and now, the last two conditions imply $z = z_1$. □

The function $g \circ f : X \longrightarrow Z$ is called the **composition** of f and g.

Lemma 10.5.3 (Restriction) *Let $f : X \longrightarrow Y$ be a function. Let $A \subseteq X$. Then there is a function $f_{|A} : A \longrightarrow Y$ such that $f(a) = f_{|A}(a)$ for all $a \in A$.*

Proof: Define $f_{|A} = f \cap (A \times Y)$. □

The function $f_{|A}$ is called the **restriction** of f to A.

Lemma 10.5.4 (Image Restriction) *Let $f : X \longrightarrow Y$ be a function. Let $Y_1 \subseteq Y$ be such that $f(X) \subseteq Y_1$. Then there is a function $g : X \longrightarrow Y_1$ such that $g(x) = f(x)$ for all $x \in X$.*

Proof: Clearly (f, Y_1) is a function. □

We denote this function as $f : X \longrightarrow Y_1$.

Exercises.

i. Let X and Y be two sets. Show that there is a set whose elements are exactly the functions from X into Y. We denote this set by ${}^{X}Y$.

ii. Find ${}^{X}\emptyset$.

iii. Show that if we allowed X to be emptyset in the definition of a function from X into Y, then ${}^{\emptyset}Y$ would be the set of all sets.

iv. Let X be a set. Let $\pi_1(X) := \{x : \text{ fo some } y,\ (x,y) \in X\}$. Show that $\pi_1(X)$ is a set.

v. Let X and Y be sets. Show that $\mathrm{pr}_1 : X \times Y \longrightarrow X$ given by $\mathrm{pr}_1(x,y) = x$ and $\mathrm{pr}_2 : X \times Y \longrightarrow Y$ given by $\mathrm{pr}_1(x,y) = y$ are functions. These are called **first** and **second projections**.

vi. Let $f : X \longrightarrow Y$ be a function.

For $A \subseteq X$, show that $f(A) := \{f(a) : a \in A\}$ is a set. It is called the **image** of A under f. The set $f(X)$ is called the **image** of f.

For two subsets A and B of X show that $f(A \cup B) = f(A) \cup f(B)$ and that $f(A \cap B) \subseteq f(A) \cap f(B)$. Show that the equality in the second formula does not always hold.

vii. Let X and Y be two sets.

a) Show that there is a set whose elements are bijections from X into Y.

b) Show that there is a set whose elements are injections from X into Y.

c) Show that there is a set whose elements are surjections from X into Y.

viii. Let X and Y be two sets. Show that there is a function $f : X \times Y \longrightarrow Y \times X$ such that $f(x,y) = (y,x)$. Show that f is a bijection.

ix. Let X, Y and Z be three sets. Show that there is a function $f : (X \times Y) \times Z \longrightarrow X \times (Y \times Z)$ such that $f((x,y),z) = (x,(y,z))$. Show that f is a bijection.

x. Let $f : X \longrightarrow Y$ be a function.

For $A \subseteq Y$, show that $f^{-1}(A) := \{x \in X : f(x) \in A\}$ is a set. It is called the **inverse image** of A under f.

Show that $f^{-1}(Y) = X$.

For two subsets A and B of Y show that $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$ and that $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

Chapter 11

Natural Numbers

11.1 Definition and Basic Properties

Recall that if x is a set, $S(x)$ is defined to be the set $x \cup \{x\}$.

A set x is called **inductive** if $0 \in x$ and for all $y \in x$, $S(y) \in x$.

Lemma 11.1.1 *If x is a set of inductive sets then $\cap_{y \in x} y$ is an inductive set.*

Proof: By Theorem 10.3.2, $\cap_{y \in x} y$ is a set. It remains to prove that it is an inductive set. Since every element of x is inductive, 0 is in every element of x. Hence $0 \in \cap_{y \in x} y$. Assume now $z \in \cap_{y \in x} y$. Then z is in every element of x. Since every element of x is inductive. $S(z)$ is in every element of x as well. Thus $S(z) \in \cap_{y \in x} y$. □

Until now, there was no axiom to ensure the existence of an infinite set. Our next axiom will give rise to an infinite set (the term "infinite" is to be defined mathematically later on).

A6. Inductive Sets. *There is an inductive set.*

Theorem 11.1.2 *There is a smallest inductive set. In other words, there is an inductive set which is a subset of all inductive sets. This smallest inductive set is (of course!) the intersection of all inductive sets.*

Proof: The intersection of all inductive sets is inductive (as in the proof of the lemma above), but *a priori* it is not a set. We will prove that it is in fact a set. Let x be an inductive set (whose existence is insured by A6). The collection c of inductive subsets of x is a set by Axioms A6 and A3. Then by Theorem 10.3.2, $\omega := \cap_{z \in c} z$ is a set, and by Lemma 11.1.1 ω is an inductive set. We claim that ω is a subset of all inductive sets. Indeed, let t be any inductive set. By A5′, $\{x, t\}$ is a set. By lemmas 10.3.2 and 11.1.1, $x \cap t$ is an inductive subset of x. Thus $x \cap t \in c$ and ω is a subset of $x \cap t$. It follows that ω is a subset of t. □

From now on we let ω or $\mathbb{N}$ denote the smallest inductive set.

11.2 Well-ordering on ω

A **well-ordered set** is a linear order with the property that every nonempty subset has a least element. In this subsection, we will show that ω is a well-ordered set with respect to the relation $\in$.

Lemma 11.2.1 *For all $x, y \in \omega$, if $x \in y$ then $x \subseteq y$.*

Proof: We proceed by induction on y. The statement holds trivially if $y = 0 = \emptyset$, since there is no such x. Assume the statement holds for y. We proceed to show that the statement holds for $S(y)$. Let $x \in S(y)$. Since $S(y) = y \cup \{y\}$, either $x \in y$ or $x \in \{y\}$. In the first case $x \subseteq y$ by our assumption. In the second case $x = y$. Thus in both cases $x \subseteq y$, proving our lemma. □

Lemma 11.2.2 *For all $x \in \omega$, either $\emptyset \in x$ or $x = \emptyset$.*

Proof: We proceed by induction on x. The statement holds trivially if $x = 0 = \emptyset$. Assume the statement holds for x. Since $x \subseteq S(x)$, if $\emptyset \in x$, then $\emptyset \in S(x)$. If $\emptyset = x$, then $S(x) = S(\emptyset) = \{\emptyset\}$ and it contains $\emptyset$ as an element. □

Lemma 11.2.3 *For all $x \in \omega$, $x \notin x$.*

Proof: We proceed by induction on x. The statement is clear if $x = 0$. Assume the statement holds for x, i.e. that $x \notin x$. We prove that $S(x) \notin S(x)$. Assume otherwise, i.e. that $S(x) \in S(x)$. Thus $S(x) \in x \cup \{x\}$. If $S(x) \in \{x\}$, then $S(x) = x$ and $x \in S(x) = x$, contradicting our assumption that $x \notin x$. Hence $S(x) \in x$. By Lemma 11.2.1, $S(x) \subseteq x$. Since $x \in S(x)$, we again get $x \in x$. □

Lemma 11.2.4 *For all $x, y \in \omega$, if $y \in x$ then either $S(y) \in x$ or $S(y) = x$.*

Proof: We proceed by induction on x. The statement is clear if $x = 0$. Assume the statement holds for x. We prove that the statement holds for $S(x)$. Let $y \in S(x) = x \cup \{x\}$. If $y \in \{x\}$, then $y = x$ and so $S(y) = S(x)$. If $y \in x$, then by induction either $S(y) \in x$ or $S(y) = x$. In either case $S(y) \in S(x)$. □

Theorem 11.2.5 *The relation $\in$ is a linear order on ω.*

Proof: We first show that $(\omega, \in)$ is a linear order.

i. By Lemma 11.2.3, for all $x \in \omega$, $x \notin x$.

ii. Let $x, y, z \in \omega$ be such that $x \in y$ and $y \in z$. By Lemma 11.2.1, $y \subseteq z$. Thus $x \in z$.

iii. Let $x, y \in \omega$. We want to show that either $x \in y$ or $x = y$ or $y \in x$. We do this by induction on x. In other words we show by induction on x that "for all $y \in \omega$, either $x \in y$ or $x = y$ or $y \in x$". If $x = 0$, then this is given by Lemma 11.2.2. Assume the statement holds for x. We show it for $S(x)$. Let $y \in \omega$.

Case 1. If $y \in x$, then $y \in x \subseteq S(x)$, so $y \in S(x)$.

Case 2. If $y = x$, then $y \in S(x)$.

Case 3. If $x \in y$, then by Lemma 11.2.4, either $S(x) \in y$ or $S(x) = y$. This proves the lemma. □

We now show that any nonempty subset of ω has a least element (for ϵ). Let X be a subset of ω without a least element. We will prove by induction on x the following statement: "For all $y \in \omega$, if $y \in x$ then $y \notin X$". Let $\phi(x)$ be this statement.

Clearly $\phi(x)$ holds for $x = 0$. Assuming $\phi(x)$ holds, we show that $\phi(S(x))$. Assume not. Let $y \in S(x) = x \cup \{x\}$ be an element of X. If $y \in x$ then by induction $y \notin X$, a contradiction. Thus $y = x$. But then, x is the least element of X, a contradiction again. This proves the statement $\forall x\ \phi(x)$.

Now we show that $X = \emptyset$. Assume otherwise. Let $x \in X$. Then $\phi(S(x))$ does not hold. A contradiction. □

Exercises.

i. Show that if $x \in \omega$ then $x \subseteq \omega$.

Proof: If $x = 0 = \emptyset$, that is clear. Assuming it holds for x, we show that it holds for $S(x)$. Since $S(x) = x \cup \{x\}$ and since $x \subseteq \omega$ by induction, this is clear. □

11.3 Peano's Axioms

In this subsection, we will prove the so-called "Peano's Axioms" (Theorem 11.3.1). After the proof of the Peano's Axioms, we will not need for a long time what has been done until now in the preceding sections and subsections. To develop arithmetic and to construct other number sets, we will only use the Peano's Axioms.

As it is customary, we will let $\mathbb{N} = \omega$.

Theorem 11.3.1 (Peano's Axioms) *PA1. S is a one to one function from $\mathbb{N}$ into $\mathbb{N}$.*

PA2. If X is a subset of $\mathbb{N}$ with the property that

a) $0 \in X$,

b) For all $x \in X$, $S(x) \in X$,

then $X = \mathbb{N}$.

Proof: PA2. By hypothesis X is an inductive set. By Theorem 11.1.2, $X = \mathbb{N}$.

PA1. We first prove that S is a function. We only need to prove that $\{(x, S(x)) : x \in \mathbb{N}\}$ is a set. This is easy and we leave it to the reader.

We now show that S is one to one. Assume $S(x) = S(y)$ and $x = y$. Then $x \cup \{x\} = y \cup \{y\}$. Then x, which is an element of the left hand side is an element of the right hand side. Thus $x \in y \cup \{y\}$. If $x \in \{y\}$ then $x = y$. Thus $x \notin \{y\}$ and $x \in y$. By Lemma 11.2.1, $x \subseteq y$. Similarly $y \subseteq x$.

Lemma 11.3.2 $S(\mathbb{N}) = \mathbb{N} \setminus \{0\}$.

Proof: Let $X = \{0\} \cup \{x \in \mathbb{N} : \text{ there exists } y \in \mathbb{N} \text{ such that } S(y) = x\}$. We will show that $X = \mathbb{N}$ by using PA2. By definition $0 \in X$. Assume $x \in X$. Then $x \in \mathbb{N}$. So $S(x) \in X$ by definition of X. By PA2, $X = \mathbb{N}$.

Thus $\mathbb{N} \setminus \{0\} \subseteq S(\mathbb{N})$. Since $S(\mathbb{N}) \subseteq \mathbb{N}$, for the reverse inclusion, we just need to show that $0 \notin S(\mathbb{N})$. But $x \in S(x)$ for any $x \in \mathbb{N}$, so that $S(x) \neq \emptyset = 0$. □

From now on we will forget about the construction of ω and we will only use the properties expressed in Theorem 11.3.1.

11.4 Addition of Natural Numbers

A subset A of $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ will be called **additive** (only for this subsection) if

i. $(x, 0, x) \in A$ for all $x \in \mathbb{N}$.

ii. If $(x, y, z) \in A$ then $(x, S(y), S(z)) \in A$.

Theorem 11.4.1 (Addition) *There is a smallest additive set and it is the graph of a function from* $\mathbb{N} \times \mathbb{N}$ *into* $\mathbb{N}$.

Proof: Let A be the intersection of all additive subsets of $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$. (Note that $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ is an additive set). Clearly A is a set and is an additive set. Therefore it is the smallest additive set. We will show that for all $(x, y) \in \mathbb{N} \times \mathbb{N}$ there exists a unique $z \in \mathbb{N}$ such that $(x, y, z) \in A$. We proceed by induction on y.

Suppose first $y = 0$. Then $(x, 0, x) \in A$. Assume $(x, 0, z) \in A$ with $z \neq x$. Consider the set $A_1 := A \setminus \{(x, 0, z)\}$. We now show that A_1 is an additive set. Clearly $(x_1, 0, x_1) \in A$ for all $x_1 \in \mathbb{N}$ because none of the elements of this kind was taken away from A and they are all in A_1. This proves (i) for A_1. Assume $(x, y, z) \in A_1$. Then $(x, y, z) \in A$. Thus $(x, S(y), S(z)) \in A$. Since $S(y) \neq 0$, $(x, S(y), S(z)) \in A_1$ as well. This proves (ii). Therefore A_1 is an additive set. Since A is the smallest additive set, $A_1 = A$ and $(x, 0, z) \notin A$ for $z \neq x$.

Suppose now we know the result for y and we proceed to prove it $S(y)$. Let $x \in \mathbb{N}$. By induction, there is a $z \in \mathbb{N}$ such that $(x, y, z) \in A$. Thus $(x, S(y), S(z)) \in A$. Assume there exists a $z_1 \in \mathbb{N}$ such that $z_1 \neq S(z)$ and $(x, S(y), z_1) \in A$. Consider the set $A_1 = A \setminus \{(x, S(y), z_1)\}$. We will show that A_1 is an additive set. Let $x_2 \in \mathbb{N}$. Then $(x_2, 0, x_2) \in A$. Since the element $(x, S(y), z_1)$ missing in A_1 cannot have the second coordinate equal to 0, $(x_2, 0, x_2) \in A$. This proves (i). To prove (ii), let $(x_2, y_2, z_2) \in A_1$. Then $(x_2, y_2, z_2) \in A$, so that $(x_2, S(y_2), S(z_2)) \in A$. Assume $(x_2, S(y_2), S(z_2)) \notin A$. Then $(x_2, S(y_2), S(z_2)) = (x, S(y), z_1)$. Thus $x_2 = x$ and $S(y_2) = S(y)$ and $S(z_2) = z_1$. Since S is one to one, $x_2 = x$ and $y_2 = y$ and $S(z_2) = z_1$. So $(x, y, z_2) = (x_2, y_2, z_2) \in A$. Since $(x, y, z) \in A$, by induction, we get $z_2 = z$. Thus $S(z) = S(z_2) = z_1$, a contradiction to the fact that $S(z) \neq z_1$. This proves (ii). Hence A_1 is an additive set. But this contradicts the fact that A is the smallest additive set. □

We call this function **addition** and let $x + y = z$ if $(x, y, z) \in A$. We have

A1. $x + 0 = x$ for all $x \in \mathbb{N}$.

A2. $x + S(y) = S(x + y)$ for all x, $y \in \mathbb{N}$.

Lemma 11.4.2 *For all $x \in \mathbb{N}$, if $S(x) = x + 1$.*

Proof: $x + 1 = x + S(0) = S(x + 0) = S(x)$. □

Theorem 11.4.3 *2 + 2 = 4.*

Proof: $2 + 2 = 2 + S(1) = S(2 + 1) = S(2 + S(0)) = S(S(2 + 0)) = S(S(2)) = S(3) = 4$. □

Lemma 11.4.4 (Associativity of Addition) *For all x, y, $z \in \mathbb{N}$, $x + (y + z) = (x + y) + z$.*

Proof: By induction on z. Assume first $z = 0$. Then $x+(y+z) = x+(y+0) = x + y = (x + y) + 0 = (x + y) + z$. Now we assume the statement holds for z and we prove it for $S(z)$: $x + (y + S(z)) = x + S(y + z) = S(x + (y + z)) = S((x + y) + z) = (x + y) + S(z)$. □

Lemma 11.4.5 *For all $x \in \mathbb{N}$, $0 + x = x$.*

Proof: This is clear if $x = 0$. Assume the result for x. Then $0 + S(x) = S(0 + x) = S(x)$. □

Lemma 11.4.6 (Right Simplification for Addition) *For all x, y, $z \in \mathbb{N}$, if $x + z = y + z$ then $x = y$.*

Proof: This is clear if $z = 0$. Assume the result for z. Assume also that $x + S(z) = y + S(z)$. Then $S(x + z) = S(y + z)$. Since S is one to one, this implies that $x + z = y + z$. By induction $x = y$. □

Lemma 11.4.7 *For all x, $y \in \mathbb{N}$, if $y + S(x) = S(y) + x$.*

Proof: If $x = 0$, then the statement says that $y + 1 = S(y)$. But $y + 1 = y + S(0) = S(y + 0) = S(y) = S(y) + x$. Assume the result for x. Then $y + S(S(x)) = S(y + S(x)) = S(S(x) + y) = S(x) + S(y) =$ ... Do it together with next lemma... □

Lemma 11.4.8 (Commutativity of Addition) *For all x, $y \in \mathbb{N}$, if $x + y = y + x$.*

Proof: If $x = 0$, then this is just Lemma 11.4.5. Assume the result for x. Then by Lemma 11.4.7 and induction, $S(x) + y = x + S(y) = S(x + y) = S(y + x) = y + S(x)$. □

Corollary 11.4.9 (Left Simplification for Addition) *For all x, y, $z \in \mathbb{N}$, if $x + y = x + z$ then $y = z$.*

Proof: By Lemmas 11.4.8 and 11.4.6. □

Lemma 11.4.10 *For all x, $y \in \mathbb{N}$, if $x + y = 0$ then $x = y = 0$.*

Proof: If $y = 0$, the result is clear. Otherwise, $y = S(z)$ for some z and $x + y = x + S(z) = S(x + z) \neq 0$. □

Exercises.

i. Suppose your computer knows how to add 1 to a natural number, knows how to subtract 1 from a positive natural number and recognizes 0. Teach how to add two natural numbers to your computer.

11.5 Multiplication of Natural Numbers

A subset M of $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ will be called **multiplicative** (only for this subsection) if

i. $(x, 0, 0) \in M$ for all $x \in \mathbb{N}$.
ii. If $(x, y, z) \in M$ then $(x, S(y), z + x) \in M$.

Theorem 11.5.1 (Multiplication) *There is a smallest multiplicative set and it is a function*

Proof: Let M be the intersection of all the multiplicative subsets of $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$. (Note that $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ is a multiplicative set). Clearly M is a set and is a multiplicative set. Therefore it is the smallest multiplicative set. We will show that for all $(x, y) \in \mathbb{N} \times \mathbb{N}$ there exists a unique $z \in \mathbb{N}$ such that $(x, y, z) \in M$. We proceed by induction on y.

Suppose first $y = 0$. We know that $(x, 0, 0) \in A$. Assume $(x, 0, z) \in M$ with $z \neq 0$. Consider the set $M_1 := M \setminus \{(x, 0, z)\}$. We will show that M_1 is an inductive set. Clearly $(x_1, 0, 0) \in M$ for all $x_1 \in \mathbb{N}$ because none of the elements of this kind was taken away from M and they are all in M_1. This proves (i) for M_1. Assume $(x, y, z) \in M_1$. Then $(x, y, z) \in M$. Thus $(x, S(y), z + x) \in M$. Since $S(y) \neq 0$, $(x, S(y), z + x) \in M_1$ as well. This proves (ii). Therefore M_1 is a multiplicative set. Since M is the smallest multiplicative set, $M_1 = M$ and $(x, 0, z) \notin M$ for $z \neq 0$.

Suppose now we know the result for y. We prove it $S(y)$. Let $x \in \mathbb{N}$. By induction, there is a $z \in \mathbb{N}$ such that $(x, y, z) \in M$. Thus $(x, S(y), z + x) \in M$. Assume there exists a $z_1 \in \mathbb{N}$ such that $z_1 \neq z + x$ and $(x, S(y), z_1) \in M$. Consider the set $M_1 := M \setminus \{(x, S(y), z_1)\}$. We will show that M_1 is a multiplicative set. Let $x_2 \in \mathbb{N}$. Then $(x_2, 0, 0) \in M$. Since the element $(x, S(y), z_1)$ missing in M_1 cannot have the second coordinate equal to 0, $(x_2, 0, 0) \in M_1$. This proves (i). To prove (ii), let $(x_2, y_2, z_2) \in M_1$. Then $(x_2, y_2, z_2) \in M$,

so that $(x_2, S(y_2), z_2 + x_2) \in M$. Assume $(x_2, S(y_2), z_2 + x_2) \notin M_1$. Then $(x_2, S(y_2), z_2 + x_2) = (x, S(y), z_1)$. Thus $x_2 = x$ and $S(y_2) = S(y)$ and $z_2 + x_2 = z_1$. Since S is one to one, $x_2 = x$ and $y_2 = y$ and $z_2 + x = z_1$. So $(x, y, z_2) = (x_2, y_2, z_2) \in M$. Since $(x, y, z) \in M$, by induction, we get $z = z_2$ and $z_1 = z_2 + x = z + x$, a contradiction to the fact that $z + x \neq z_1$. This proves (ii). Hence M_1 is a multiplicative set. But this contradicts the fact that M is the smallest multiplicative set. □

We call this function **multiplication** and let $x \times y = z$ if $(x, y, z) \in M$. As it is customary, instead of $x \times y$, we may just write xy. We have,

M1. $x0 = 0$ for all $x \in \mathbb{N}$.

M2. $xS(y) = xy + x$ for all x, $y \in \mathbb{N}$.

Theorem 11.5.2 $2 \times 2 = 4$.

Proof: We directly compute using definitions and the previous results about addition: $2 \times 2 = 2 \times S(1) = 2 \times 1 + 2 = 2 \times S(0) + 2 = (2 \times 0 + 2) + 2 = (0 + 2) + 2 = 2 + 2 = 4$. □

Lemma 11.5.3 (Right Identity Element for Multiplication) *For all* $x \in \mathbb{N}$, *if* $x1 = x$.

Proof: This follows from the definition of the multiplication and Lemma 11.4.5: $x1 = xS(0) = x0 + x = 0 + x = x$. □

Lemma 11.5.4 *For all* $x \in \mathbb{N}$, $0x = 0$.

Proof: If $x = 0$ this is just the definition. We assume $0x = 0$ and prove that $0S(x) = 0$: $0S(x) = 0x + 0 = 0 + 0 = 0$. □

Lemma 11.5.5 (Left Identity Element for Multiplication) *For all* $x \in \mathbb{N}$, $1x = x$.

Proof: If $x = 0$ this is just the definition. We assume $1x = x$ and prove that $1S(x) = S(x)$: $1S(x) = 1x + 1 = x + 1 = S(x)$. □

Lemma 11.5.6 (Left Distributivity) *For all* x, y, $z \in \mathbb{N}$, $x(y+z) = xy+xz$.

Proof: Assume first $z = 0$. Then $x(y + 0) = xy = xy + 0 = xy + x0 = xy + xz$. Now assume the statement holds for z. We show it holds for $S(z)$: $x(y+S(z)) = xS(y + z) = x(y + z) + x = (xy + xz) + x = xy + (xz + x) = xy + xS(z)$. □

Lemma 11.5.7 (Associativity of Multiplication) *For all* x, y, $z \in \mathbb{N}$, $x(yz) = (xy)z$.

Proof: If $z = 0$, then $x(yz) = x(y0) = x0 = 0 = (xy)0 = (xy)z$. Assume now the statement holds for z. We show it holds for $S(z)$ by using Lemma 11.5.6: $x(yS(z)) = x(yz + y) = x(yz) + xy = (xy)z + xy = (xy)S(z)$. □

Lemma 11.5.8 (Right Distributivity) *For all x, y, $z \in \mathbb{N}$, $(y+z)x = yx + zx$.*

Proof: If $z = 0$, then $(y+z)x = (y+z)0 = 0 = 0+0 = y0 + z0 = yx + zx$. Assume now the statement holds for x. We show it holds for $S(x)$ by using Lemma 11.5.5 and the commutativity and the associativity of addition: $(y+z)S(x) = (y+z)(x+1) = (y+z)x + (y+z)1 = (yx+zx) + (y+z) = (yx+y) + (zx+z) = yS(x) + zS(x)$. □

Lemma 11.5.9 (Commutativity of Multiplication) *For all x, $y \in \mathbb{N}$, if $xy = yx$.*

Lemma 11.5.10 (Simplification for Multiplication) *For all x, y, $z \in \mathbb{N}$, if $xy = xz$ and $x \neq 0$, then $y = z$.*

Lemma 11.5.11 *For all x, $y \in \mathbb{N}$, if $xy = 0$, then either $x = 0$ or $y = 0$.*

Proof: Assume $x \neq 0$. Since $xy = 0 = x0$, by Lemma 11.5.10, $y = 0$. □

Exercises.

i. Suppose your computer knows how to add 1 to a natural number, knows how to subtract 1 from a positive natural number and recognizes 0. Teach how to multiply two natural numbers to your computer. (Hint: use Exercise i, page 92).

11.6 Well-Ordering of Natural Numbers

In Theorem 11.2.5, we showed that $\in$ is a well-ordering of $\omega = \mathbb{N}$. Here in this section, we will give another definition of the same ordering and reprove that this is a well-ordering using only the Peano's Axioms and its consequences.

For x, $y \in \mathbb{N}$, define $x < y$ if there exists an $a \in \mathbb{N} \setminus \{0\}$ such that $x + a = y$.

Lemma 11.6.1 *For all $x \in \mathbb{N}$, $x < S(x) = x + 1$.*

Proof: By Lemma 11.4.2, $S(x) = x + 1$. Since $1 = \{0\}$, $1 \neq \emptyset = 0$. Thus $x < x + 1$. □

Theorem 11.6.2 (Well-ordering of $\mathbb{N}$) *$<$ is a well-ordering on $\mathbb{N}$.*

Proof: i. Assume $x \in \mathbb{N}$ and $x < x$. Then $x + a = x$ for some $a \in \mathbb{N} \setminus \{0\}$. Then, since $x + a = x = x + 0$, by Lemma 11.4.9, $a = 0$, a contradiction.

ii. Assume now x, y, $z \in \mathbb{N}$, $x < y$ and $y < z$. Then there are nonzero natural numbers a and b such that $x + a = y$ and $y + b = z$. Then $x + (a + b) = (x + a) + b = y + b = z$ and $a + b \neq 0$ by Lemma 11.4.10. Thus $x < z$.

It follows that $(\mathbb{N}, <)$ is a poset.

iii. Let x, $y \in \mathbb{N}$. We want to show that either $x < y$ or $x = y$ or $y < x$.

Suppose first $x = 0$. If $y \neq 0$, then, since $x + y = 0 + y = y$, we have $x < y$.

Assume now that we know the result for x. We will prove it for $S(x)$. Let $y \in \mathbb{N}$. Either $y < x$ or $y = x$ or $x < y$.

Case 1. If $y < x$, then by Lemma 11.6.1 and part (ii), $y < S(x)$.

Case 2. If $y = x$, then by Lemma 11.6.1 and part (ii), $y < S(x)$.

Case 3. If $x < y$, then there exists an $a \in \mathbb{N} \setminus \{0\}$ such that $x + a = y$.

Subcase 3.1. If $a = 1$, then by Lemma 11.6.1, $y = x + 1 = S(x)$.

Subcase 3.2. If $a \neq 1$, then by Lemma 11.3.2, $a = S(b)$ for some $b \neq 0$. Then $y = x + a = x + S(b) = S(x) + b$ by Lemma 11.4.7. Thus $y > S(x)$.

It follows that $(\mathbb{N}, <)$ is a total order.

iv. We now show that given $x, y \in \mathbb{N}$, $y \in \mathbb{N}$, if $y < S(x)$ then $y \leq S(x)$.

Since $y < S(x)$, there is an $a \in \mathbb{N} \setminus \{0\}$ such that $y + a = S(x)$. By hypothesis $a \neq 0$. Thus $a = S(b)$ for some b. Thus $S(y + b) = y + S(b) = y + a = S(x)$ and so $y + b = x$. If $b = 0$ then $y = x$. If $b \neq 0$ then $y < x$. This proves the claim.

v. Let $X \subseteq \mathbb{N}$ be a subset that does not have a least element. We will show that $X = \emptyset$. We will show by induction on x that "for all $y \in \mathbb{N}$ if $y < x$ then $y \notin X$". This statement clearly holds for $x = 0$. Assume it holds for x. Let $y < S(x)$ be an element of X. then, by induction $y \not< x$. By part (iv), $y = x$. But then x is the least element of X, a contradiction. This proves the statement "for all $y \in \mathbb{N}$ if $y < x$ then $y \notin X$".

Now if $a \in X$, then this statement would be false for $S(a)$. Thus $X = \emptyset$. □

Lemma 11.6.3 *For all x, y, $z \in \mathbb{N}$, $x < y$ if and only if $x + z < y + z$.*

Proof: ($\Rightarrow$) Suppose $x < y$. Let $a \neq 0$ be such that $x + a = y$. Then $(x + z) + a = (x + a) + z = y + z$. So $x + z < y + z$.

($\Leftarrow$) Suppose $x + z < y + z$. Let $a \neq 0$ be such that $x + z + a = y + z$. Then $(x + a) + z = y + z$. By simplifying, we get $x + a = y$. So $x + z < y + z$.

Lemma 11.6.4 *For all x, y, $z \in \mathbb{N}$, if $y < z$ and $x \neq 0$ then $xy > xz$.*

Proof: Let $a \neq 0$ be such that $y + a = z$. Now $xz = x(y + a) = xy + xa$ and $xa \neq 0$ by Lemma 11.5.11. So $xy < xz$. □

Exercises.

i. Let $x \in \mathbb{N}$. Show that there is no $y \in \mathbb{N}$ such that $x < y < S(x)$.

ii. Show that $x + x = 2 \times x$ for all $x \in \mathbb{N}$.

iii. Show that $2\mathbb{N} \cap (2\mathbb{N} + 1) = \emptyset$.

iv. Show that if the structure $(\mathbb{N}_1, S_1, 0_1)$ satisfies the Peano Axioms, then $(\mathbb{N}_1, S_1, 0_1) \simeq (\mathbb{N}, S, 0)$ and the isomorphism is unique.

v. Show that given $x, y \in \mathbb{N}$, $y \in \mathbb{N}$, if $x < y$ then $S(x) \leq y$.

Proof: Since $x < y$, there is an $a \in \mathbb{N} \setminus \{0\}$ such that $x + a = y$. By hypothesis $a \neq 0$. Thus $a = S(b)$ for some b. Thus $y = x + a = x + S(b) = S(x) + b$ by Lemma 11.4.7 and so $S(x) \leq y$. □

vi. Show that if $x < y < x + 2$, then $y = x + 1$.

vii. Show that the ordering $<$ defined in this section is the same as the relation $\in$. I.e. show that for x, $y \in \mathbb{N}$, $x > y$ if and only if $x \in y$.

11.7 Finite and Infinite Sets

A set is called **finite** if it is in bijection with a natural number. A set which is not finite is called an **infinite** set. If A is a finite set and if $f : A \longrightarrow n$ is a bijection between A and the natural number n, then letting $a_i = f^{-1}(i)$ for $i \in n$, we will write

$$A = \{a_0, a_1, \ldots, a_{n-1}\}.$$

Given a finite set A, the natural number n as in the definition is unique as the next lemma shows:

Lemma 11.7.1 *Let n, $m \in \omega$. If there is a bijection between n and m then $n = m$.*

Proof: Assume first $n = 0$. Let $f : n \longrightarrow m$ be a bijection. If $m \neq 0$, then $0 \in m$ and $f(x) = 0$ for some $x \in n = 0 = \emptyset$, a contradiction.

Suppose we know the result for n. Let us prove the result for $n + 1$. Let $f : n + 1 \longrightarrow m$ be a bijection. Let $f(n) = x \in m$. In particular $m \neq 0$ and $m = S(k)$ for some k. Define $g : n \setminus \{x\} \longrightarrow k$ by

$$g(y) = \begin{cases} y & \text{if } y < x \\ y - 1 & \text{if } y > x \end{cases}$$

It is easy to check that g is a bijection. Now the map $g \circ f_{|n}$ is a bijection from n onto k. By induction $n = k$, and so $n + 1 = S(n) = S(k) = m$. □

Thus if A is a finite set, then there is a unique natural number n such that A and n are in bijection. We set $|A| = n$ and call n the **cardinality** of A.

Exercises.

i. Show that if A and B are finite sets with $|A| = n$ and $|B| = m$, then $|A \cup B| \leq n + m$.

ii. Show that ω is an infinite set.

11.8 Functions Defined by Induction

Theorem 11.8.1 *To be announced.*

11.9 Powers

Corollary 11.9.1 *There is a unique map* $f : \mathbb{N}\times\mathbb{N}\setminus\{(0,0)\}$ *such that* $f(n,0) = 1$ *for all* $n \neq 0$, $f(0,1) = 0$ *and* $f(n,m+1) = f(n,m)n$ *for all* n, $m \in \mathbb{N}$.

We let $f(n,m) = n^m$.

Lemma 11.9.2 *For all* a, b, $c \in \mathbb{N}$ *for which the operations below are defined,* $a^{b+c} = a^b a^c$, $(a^b)^c = a^{bc}$.

Lemma 11.9.3 *Let* X *be the set of finite subsets of* $\mathbb{N} \times \mathbb{N}$. *Then there is a unique function* $f : X \longrightarrow \mathbb{N}$ *such that*

$$f(\emptyset) = 1$$

and

$$f(\{(n_1,m_1),\ldots,(n_k,m_k)\}) = f(\{(n_1,m_1),\ldots,(n_{k-1},m_{k-1})\})n_k^{m_k}.$$

We let

$$f(\{(n_1,m_1),\ldots,(n_k,m_k)\}) = n_k^{m_k}\ldots n_k^{m_k}.$$

Exercises.

i. Let X be the set of finite subsets of $\mathbb{N}$. Show that there is a unique function $f : X \longrightarrow \mathbb{N}$ such that

$$f(\emptyset) = 0$$

and

$$f(\{n_1,\ldots,n_k\}) = f(\{n_1,\ldots,n_{k-1}\}) + n_k.$$

11.10 Divisibility

Theorem 11.10.1 (Division) *Let* a, $b \in \mathbb{N}$. *Assume* $b \neq 0$. *Then there are unique* q, $r \in \mathbb{N}$ *such that* $a = bq + r$ *and* $r < b$.

Proof: We proceed by induction on a to show the existence. If $a < b$, we can let $q = 0$ and $r = a$. Assume $a \geq b$. Let c be such that $a = b + c$. Since $c < a$, by induction there are q_1 and r such that $c = bq_1 + r$ and $r < b$. Now, we have, $a = b + c = b + bq_1 + r = b(1 + q_1) + r$. We let $q = 1 + q_1$. This proves the existence.

Now we prove the uniqueness. Assume $bq + r = bq_1 + r_1$ and $r < b$, $r_1 < b$. If $q = q_1$, then, by simplifying we get $r = r_1$. Assume $q \neq q_1$. We may assume without loss of generality that $q < q_1$. Let $p > 0$ be such that $q + p = q_1$. Then $bq + r = bq_1 + r_1 = b(q + p) + r_1 = bq + bp + r_1$, so $r = bp + r_1 \geq bp \geq b$, a contradiction. □

We say that a natural number a divides another natural number b if $ac = b$ for some $c \in \mathbb{N}$. We then write $a|b$. Note that all natural numbers divide 0, but that only 1 divides 1. Note also that 1 divides all natural numbers.

Lemma 11.10.2 *The relation "divisibility" is a partial order on $\mathbb{N}$ with 1 as the least element and 0 as the largest element.*

This partial order has elements which are immediate successors of 1, as we will show soon. These numbers are called **irreducible numbers**. Thus a natural number p is irreducible if $p > 1$ and if the only natural numbers that divide p are 1 and p. In other words, p is irreducible if $p > 1$ and if $p = xy$ implies either x or y is p (equivalently 1).

Proposition 11.10.3 *Every natural number > 1 is divisible by an irreducible number.*

Proof: Let $a > 1$ be a natural number. If a is not divisible by a natural number $\neq 1, a$, then a is irreducible and so a is divisible by an irreducible number, namely a. Otherwise, a is divisible by a natural number $b \neq 1, a$. By induction b is divisible by an irreducible number. This irreducible number divides a as well. □

Lemma 11.10.4 *If a divides x and $x + y$, then a divides y.*

This is clear if $a = 0$, because then $x = x + y = 0$. Assume $a > 0$. Let $b, c \in \mathbb{N}$ be such that $ab = x$ and $ac = x + y$. Since $ab = x \leq x + y = ac$, we have $b \leq c$. Thus $c = b + z$ for some z. Now $ab + az = a(b + z) = ac = x + y = ab + y$, so $az = y$ and a divides y. □

The reader may be used to the term **prime** instead of irreducible. The term prime, in general, has another meaning, which happens to coincide with "irreducible" in the context of natural numbers. We say that a natural number $p > 1$ is prime if, for all $x, y \in \mathbb{N}$, if $p|xy$ then either $p|x$ or $p|y$. We will now show that a natural number is a prime number if and only if it is irreducible.

Theorem 11.10.5 *A number is prime if and only if it is an irreducible number.*

Proof: Let p be prime. Assume that $a|p$. Then $p = ab$ for some b. It follows that p divides ab. Thus p divides either a or b. Assume – without loss of generality – that p divides a. Then $px = a$ some x. Hence $p = ab = pxb$. Since $p \neq 0$, it follows that $xb = 1$. Thus $b = 1$, and so $a = p$.

Let now p be an irreducible. We will prove that p is a prime. Let p divide xy. We will show that p divides either x or y. We proceed by induction on $p + x + y$. By Theorem 11.10.1, $x = pq_1 + x_1$ and $y = pq_2 + y_1$ where $x_1, y_1 < p$. Since $xy = (pq_1 + x_1)(pq_2 + y_1) = p(pq_1q_2 + q_1y_1 + q_2x_1) + x_1y_1$, by Lemma 11.10.4, p divides x_1y_1. Assume $x_1y_1 \neq 0$. Thus $p \leq x_1y_1 < p^2$. It follows that $x_1y_1 = rp$ for some $r = 1, \ldots, p - 1$. If $r = 1$, then either $p = x_1$ or $p = y_1$, a contradiction. Let q be an irreducible dividing r. Thus $q \leq r < p$. By induction q divides either x_1 or y_1, say q divides x_1. Write $x_1 = qx_2$ and $r = qr'$. We have $qx_2y_1 = x_1y_1 = rp = qr'p$ and $x_2y_1 = r'p$. By induction p divides either x_2 or y_1, in which case it divides x or y (respectively). Thus we may assume that $x_1y_1 = 0$. Hence one of x_1 or y_1 is 0, say $x_1 = 0$. Then $x = pq_1 + x_1 = pq_1$ and p divides x. □

Theorem 11.10.6 (Euclid) *The set of prime numbers is infinite (i.e. there are infinitely many prime numbers).*

Proof: Suppose that there are only n prime numbers. Call them $p_1, \ldots, p_n$. Consider the number $k = p_1 \ldots p_n + 1$. By Proposition 11.10.3, some prime number p_i for $i = 1, \ldots, k$ divides k. Since p_i divides the product $p_1 \ldots p_n + 1$, by Lemma 11.10.4, p_i divides 1, a contradiction. □

Theorem 11.10.7 *Every natural number $\neq 0$ is a product of finitely many prime numbers. In other words, for every $n \in \mathbb{N} \setminus \{0\}$, there are finitely many distinct prime numbers $p_1, \ldots, p_k$ and nonzero natural numbers $n_1, \ldots, n_k$ such that $n = p_1^{n_1} \cdots p_k^{n_k}$. Furthermore the decomposition is unique if we convene that $p_1 < p_2 < \ldots < p_k$.*

We first show that the decomposition is unique if it exists:

Lemma 11.10.8 *Let $p_1 < \ldots < p_r$ and $q_1 < \ldots < q_s$ be two finite sets of prime numbers. Let $n_1, \ldots, n_r$ and $m_1, \ldots, m_s$ be natural numbers. Assume that $p_1^{n_1} \ldots p_r^{n_r} = q_1^{m_1} \ldots q_s^{m_s}$. Then $r = s$, $p_i = q_i$ and $n_i = m_i$ for all $i = 1, \ldots, r$.*

Proof: Assume the hypotheses. We proceed by induction on $n_1 + \ldots + n_r$. We may assume that all n_i and m_j are positive. If $n_1 + \ldots + n_r = 0$ (or 1), then the lemma is obvious. Let $N = p_1^{n_1} \ldots p_r^{n_r} = q_1^{m_1} \ldots q_s^{m_s}$. Let p be the smallest prime dividing N. Then p divides one of the $p_1, \ldots, p_r$ (this can be proven by induction on $m_1 + \cdots + m_s$). Thus $p = p_i$ some $i = 1, \ldots, r$. But p is the smallest prime dividing N. So $p = p_1$. Similarly $p = q_1$. Simplifying, we get $p_1^{n_1 - 1} \ldots p_r^{n_r} = q_1^{m_1 - 1} \ldots q_s^{m_s}$. By induction we get the result. □

Now we prove the existence part of Theorem 11.10.7. If $n = 1$, then take $k = 0$. If n is an prime number then take $k = 1$, $p_1 = n$, $n_1 = 1$. Otherwise there is a prime $p < n$ that divides n. Let $n = pm$. By induction there are finitely many distinct prime numbers $p_1, \ldots, p_k$ and nonzero natural numbers $n_1, \ldots, n_k$ such that $m = p_1^{n_1} \cdots p_k^{n_k}$. If $p = p_i$ for some $i = 1, \ldots, k$, then $n = p_1^{n_1} \cdots p_i^{n_i + 1} \ldots p_k^{n_k}$. If $p \neq p_i$ for any $i = 1, \ldots, k$, then $n = p_1^{n_1} \ldots p_k^{n_k} p$. This proves Theorem 11.10.7. □

Exercises.

i. Suppose $n|m$ and $m \neq 0$. Show that $n \leq m$.

ii. Suppose $n|m$ and $m|n$. Show that $n = m$.

iii. Show that if $a|b$ then $a^c|b^c$.

iv. Analyzing carefully the inductive nature of Theorem 11.10.1, write a computer program that knows how to divide a natural number into another (nonzero) natural number. Hint: See Exercise i, 92 and Exercise i, 94.

11.11 Uniqueness of $\mathbb{N}$

In this subsection, we show that if $(\mathbb{N}_1, S_1, O_1)$ is a structure satisfying the Peano's Axioms (defined below), then there is a (unique) bijection $f : \mathbb{N} \longrightarrow \mathbb{N}_1$ such that $f(S(x)) = S(f(x))$ and $f(0) = 0_1$ for all $x \in \mathbb{N}$. This will show that a structure satisfying Peano's Axioms is unique "up to isomorphism". We make this more precise:

Let $\mathbb{N}'$ be a set, $S' : \mathbb{N}' \longrightarrow \mathbb{N}'$ a function and $0' \in \mathbb{N}'$ an element. Suppose that the triple $(\mathbb{N}', S', 0')$ satisfies the following:

PA1. S' is a one to one function from $\mathbb{N}'$ into $\mathbb{N}'$.

PA2. If X is a subset of $\mathbb{N}'$ with the property that

a) $0' \in X$,

b) For all $x \in X$, $S'(x) \in X$,

then $X = \mathbb{N}'$.

Then we say that the triple $(\mathbb{N}', S', 0')$ satisfies the Peano axioms. Of course, for a triple that satisfies the Peano axioms, all the results of the previous sections xxx hold.

Theorem 11.11.1 *Any two triples $(\mathbb{N}', S', 0')$ and $(\mathbb{N}'', S'', 0'')$ satisfying the Peano Axioms are "isomorphic", i.e. there is a bijection $f : \mathbb{N}'' \longrightarrow \mathbb{N}'$ such that $f(0'') = 0'$ and $f(S''(x)) = S'(f(x))$ for all $x \in \mathbb{N}''$.*

Proof: Since the composition and the inverse of isomorphisms is clearly an isomorphism, we may suppose that $(\mathbb{N}'', S'', 0'') = (\mathbb{N}, S, 0)$. Define $f : \mathbb{N} \longrightarrow \mathbb{N}'$ by the rule,

$$f(0) = 0'$$

and

$$f(S(x)) = S'(f(x)).$$

By Theorem 11.8.1 f is a function. We just need to prove that it is one to one and that it is unique.

We first show that f is one to one. Assume $f(x) = f(y)$. We will show that $x = y$. We proceed by induction on x.

Assume $x = 0$. Then $f(y) = 0'$. If $y \neq 0$, then $y = S(x_1)$ and so $0' = f(y) = f(S(x_1)) = S'(f(x_1))$, contradicting the fact that $0'$ is not in the range of S'. Thus $y = 0 = x$.

Assume now $x \neq 0$. Then $x = S(x_1)$. So $S'(f(x_1)) = f(S(x_1)) = f(x) = f(y)$. In particular $f(x)$ and $f(y)$ are nonzero. Therefore $y \neq 0$ as well. Let $y = S(y_1)$. Then $S'(f(x_1)) = f(y) = f(S(y_1)) = S'(f(y_1))$. Since S' is one to one, it follows that $f(x_1) = f(y_1)$. By the inductive hypothesis $x_1 = y_1$. Hence $x = S(x_1) = S(y_1) = y$. This proves that f is one to one.

We now show that if f' is another such function then $f = f'$. By assumption $f(0) = 0' = f'(0)$. Assume $f(x) = f'(x)$. Then $f(S(x)) = S'(f(x)) = S'(f'(x)) = f'(S(x))$. This proves that $f = f'$. □

Chapter 12

Integers

12.1 Definition of The Set $\mathbb{Z}$ of Integers

Prologue. We can add and multiply two elements of $\mathbb{N}$, but in general we cannot subtract one element from another, for example, although we could subtract 5 from 6, we cannot subtract 6 from 5. In order to do subtraction, we need to introduce another number system, namely the ring (term to be defined) $\mathbb{Z}$ of integers. In other words, we want to invent (or create) the number system

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, 3, ...\}$$

that we are all familiar since our elementary school years.

We want to be able to speak about $5 - 6$ and we cannot. Instead of $5 - 6$, let us try to write $(5, 6)$; we want $(5, 6)$ to stand for $5 - 6$. There is one problem though: $5 - 6 = 8 - 9$, but $(5, 6) \neq (8, 9)$.

We can try to solve this problem as follows: We may define a relation $\equiv$ on $\mathbb{N} \times \mathbb{N}$ by

$$(x, y) \equiv (z, t) \iff x - y = z - t,$$

show that this is an equivalence relation and define -1 as the equivalence class of $(5, 6)$ (which is the same as the equivalence class of $(8, 9)$). But there is a problem: The operation $-$ appears in the definition of $\equiv$, and we did not define it yet. Here is the clever solution to this problem: Instead of defining the relation $\equiv$ as above, we define it as follows:

$$(x, y) \equiv (z, t) \iff x + t = z + y.$$

We first show that this is an equivalence relation.

Lemma 12.1.1 *The relation $\equiv$ on $\mathbb{N} \times \mathbb{N}$ defined by*

$$(x, y) \equiv (z, t) \iff x + t = z + y$$

is an equivalence relation.

Proof: It is clear that $(x, y) \equiv (x, y)$. It is also clear that if $(x, y) \equiv (z, t)$ then $(z, t) \equiv (x, y)$. It remains to prove the transitivity. Assume $(x, y) \equiv (z, t)$ and $(z, t) \equiv (u, v)$. Thus $x+t = z+y$ and $z+v = u+t$. Adding these two equalities term by term, we get,

$$(x + t) + (z + v) = (z + y) + (u + t).$$

Using the associativity and the commutativity of the addition, we get,

$$x + v + t + z = u + y + z + t.$$

Simplifying, we find $x + v = u + y$, i.e. $(x, y) \equiv (u, v)$. □

Now we are ready to define the set $\mathbb{Z}$ of integers:

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N}/\equiv .$$

Note that

$$\begin{array}{c}(0, 0) \equiv (1, 1) \equiv (2, 2) \dots \\ (1, 0) \equiv (2, 1) \equiv (3, 2) \dots \\ (0, 3) \equiv (1, 4) \equiv (2, 5) \dots\end{array}$$

The class of $(0, 0)$ will stand for 0, the class of $(1, 0)$ will stand for 1 and the class of $(0, 3)$ will stand for -3, but not now, in due time.

12.2 Operations $+$, $-$ and $\times$ on $\mathbb{Z}$

In this subsection, we will define three operations on the set $\mathbb{Z}$ that we will call "addition", "subtraction" and "multiplication". Recall that the element $\overline{(x, y)}$ of $\mathbb{Z}$ is supposed to stand for the element "$x - y$". Let us, in a moment of weakness, write

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

Assuming we know the properties of the three operations $+$, $-$ and $\times$ on $\mathbb{Z}$, we then have,

$$\begin{array}{c}\overline{(x, y)} + \overline{(z, t)} = (x - y) + (z - t) = (x + z) - (y + t) = \overline{(x + z, y + t)}, \\ \overline{(x, y)} - \overline{(z, t)} = (x - y) - (z - t) = (x + t) - (y + z) = \overline{(x + t, y + z)}, \\ \overline{(x, y)} \times \overline{(z, t)} = (x - y)(z - t) = (xz + yt) - (xt + yz) = \overline{(xz + yt, xt + yz)}.\end{array}$$

So, getting the hint from above, let us (attempt to) define the three operations $+$, $-$ and $\times$ as

$$\begin{array}{rcl}\overline{(x, y)} + \overline{(z, t)} & = & \overline{(x + z, y + t)}, \\ \overline{(x, y)} - \overline{(z, t)} & = & \overline{(x + t, y + z)}, \\ \overline{(x, y)} \times \overline{(z, t)} & = & \overline{(xz + yt, xt + yz)}.\end{array}$$

But in order to be allowed to give such definitions, we should first prove that we are allowed to do so. Let us explain what we mean on the first example $+$. It is very possible that

$$\overline{(x, y)} = \overline{(x_1, y_1)}$$

and

$$\overline{(z,t)} = \overline{(z_1,t_1)},$$

but that

$$\overline{(x+z,y+t)} \neq \overline{(x_1+z_1,y_1+t_1)},$$

in which case we are not allowed to define the addition of $\overline{(x,y)}$ and $\overline{(z,t)}$ as $\overline{(x+z,y+t)}$, because this definition depends not on the equivalence classes $\overline{(x,y)}$ and $\overline{(z,t)}$, but on the choice of the elements (x,y) and (z,t). Fortunately, this problem does not occur, all that should work does work:

Lemma 12.2.1 *Assume* $\overline{(x,y)} = \overline{(x_1,y_1)}$ *and* $\overline{(z,t)} = \overline{(z_1,t_1)}$. *Then,*
i. $\overline{(x+z,y+t)} = \overline{(x_1+z_1,y_1+t_1)}$.
ii. $\overline{(x+t,y+z)} = \overline{(x_1+t_1,y_1+z_1)}$.
iii. $\overline{(xz+yt,xt+yz)} = \overline{(x_1z_1+y_1t_1,x_1t_1+y_1z_1)}$.

Proof: Assume $\overline{(x,y)} = \overline{(x_1,y_1)}$ and $\overline{(z,t)} = \overline{(z_1,t_1)}$. Thus $(x,y) \equiv (x_1,y_1)$ and $(z,t) \equiv (z_1,t_1)$, i.e.

$$x + y_1 = x_1 + y \text{ and } z + t_1 = z_1 + t.$$

i. Adding term by term, and using associativity and commutativity, we get

$$x + z + y_1 + t_1 = x_1 + z_1 + y + t,$$

which means exactly that $(x+z,y+t) \equiv (x_1+z_1,y_1+t_1)$ i.e. that $\overline{(x+z,y+t)} = \overline{(x_1+z_1,y_1+t_1)}$.

ii. Take the first equality as it is and reverse the second one:

$$(*) \qquad x + y_1 = x_1 + y \text{ and } z_1 + t = z + t_1.$$

Now add them:

$$x + y_1 + z_1 + t = x_1 + y + z + t_1,$$

which means

$$x + t + y_1 + z_1 = x_1 + t_1 + y + z,$$

which means $\overline{(x+t,y+z)} = \overline{(x_1+t_1,y_1+z_1)}$.

iii. This is slightly more difficult. We want to show that

$$xz + yt + x_1t_1 + y_1z_1 = x_1z_1 + y_1t_1 + xt + yz.$$

We will eliminate y_1 and t_1 from the above equality and arrive at a known equality. Then, going backwards, the equality will be proven.

The quantities y_1 and t_1 occur four times, twice on the left, twice on the right. It is easy to deal with the ones on the left where they appear linearly. It is slightly harder to get rid of the ones at the right hand side where they appear as a product. We first deal with the right hand side. We add $xz + xt_1 + zy_1$ to both sides: $(xz + yt + x_1t_1 + y_1z_1) + (xz + xt_1 + zy_1) = (x_1z_1 + y_1t_1 + xt + yz) + (xz + xt_1 + zy_1) = (x_1z_1 + xt + yz) + (xz + xt_1 + zy_1 + y_1t_1) =$

$(x_1z_1 + xt + yz) + (x + y_1)(z + t_1) = (x_1z_1 + xt + yz) + (x_1 + y)(z_1 + t)$. Multiplying out and simplifying, we get

$$2xz + x_1t_1 + y_1z_1 + xt_1 + zy_1 = 2x_1z_1 + xt + yz + x_1t + yz_1.$$

Now there is no more y_1 nd t_1 left on the right hand side. Now we deal with the left hand side. We add x_1z, xz_1 and $2zx$ to both sides, factor out x_1 and z_1 from the left hand side and use the known equalities (*): $(2x_1z_1 + xt + yz + x_1t + yz_1) + x_1z + xz_1 + 2zx = (2xz + x_1t_1 + y_1z_1 + xt_1 + zy_1) + x_1z + xz_1 + 2zx = 2xz + x_1(t_1 + z) + (y_1 + x)z_1 + x(t_1 + z) + z(x + y_1) = 2xz + x_1(t + z_1) + (y + x_1)z_1 + x(t + z_1) + z(x_1 + y) = 2xz + x_1t + x_1z_1 + yz_1 + x_1z_1 + xt + xz_1 + zx_1 + zy$, i.e. $2x_1z_1 + xt + yz + x_1t + yz_1 + x_1z + xz_1 + 2zx = 2xz + x_1t + x_1z_1 + yz_1 + x_1z_1 + xt + xz_1 + zx_1 + zy$. Simplifying, we see that this last equality holds. Now, we can go backwards. □

At this point, we can define the three operations $+$, $-$ and $\times$ on $\mathbb{Z}$ as above, i.e.

$$\begin{array}{rcl} \overline{(x,y)} + \overline{(z,t)} & = & \overline{(x+z, y+t)}, \\ \overline{(x,y)} - \overline{(z,t)} & = & \overline{(x+t, y+z)}, \\ \overline{(x,y)} \times \overline{(z,t)} & = & \overline{(xz+yt, xt+yz)}. \end{array}$$

For $\overline{(x,y)} \in \mathbb{Z}$, we also let

$$-\overline{(x,y)} = \overline{(0,0)} - \overline{(x,y)} = \overline{(y,x)}.$$

Very often, for α, $\beta \in \mathbb{Z}$, we will write $\alpha\beta$ instead of $\alpha \times \beta$.

Before investigating the properties of these operations, we will define an ordering on $\mathbb{Z}$.

Exercises.

i. Show that for all α, $\beta \in \mathbb{Z}$,

$$\begin{array}{rcl} \alpha - \beta & = & \alpha + (-\beta) \\ -(\alpha - \beta) & = & -\alpha + \beta \\ -(-\alpha + \beta) & = & \alpha - \beta \\ -(-\alpha - \beta) & = & \alpha + \beta. \end{array}$$

ii. Show that the equation $\alpha + \alpha = \overline{(1,0)}$ has no solution in $\mathbb{Z}$.

iii. Show that the equation $\alpha + \alpha = \overline{(0,1)}$ has no solution in $\mathbb{Z}$.

iv. Show that the equation $\alpha + \alpha + \alpha = \overline{(2,0)}$ has no solution in $\mathbb{Z}$.

v. Find all solutions of $\alpha\beta = \overline{(1,0)}$ in $\mathbb{Z}$.

12.3 Ordering on $\mathbb{Z}$

We would like to define the ordering on $\mathbb{Z}$ as follows: For $\overline{(x,y)}, \overline{(z,t)} \in \mathbb{Z}$,

$$\overline{(x,y)} < \overline{(z,t)} \iff x + t < z + y.$$

But for this definition to make sense, we need to prove the following result:

Lemma 12.3.1 *Assume $(x,y) \equiv (x_1,y_1)$ and $(z,t) \equiv (z_1,t_1)$. Assume that $x + t < z + y$. Then $x_1 + t_1 < z_1 + y_1$.*

Proof: The hypotheses say that

$$\begin{array}{ll} (1) & x + y_1 = x_1 + y \\ (2) & z + t_1 = z_1 + t \\ (3) & x + t < z + y \end{array}$$

We have to prove that $x_1 + t_1 < z_1 + y_1$. We compute using (1), (2) and (3):

$$x_1 + y + t_1 + z = x + y_1 + z_1 + t = z + y + y_1 + z_1,$$

so, simplifying, we get $x_1 + t_1 < y_1 + z_1$. □

According to the lemma, we have the right to define the relation $<$ on $\mathbb{Z}$ as above:

$$\overline{(x,y)} < \overline{(z,t)} \iff x + t < y + z.$$

Now we show that this is a total order on $\mathbb{Z}$.

Lemma 12.3.2 *$<$ is a total order on $\mathbb{Z}$. Furthermore, any element of $\mathbb{Z}$ has an immediate successor and an immediate predecessor.*

Proof: Irreflexivity. Easy.

Transitivity. Assume $\overline{(x,y)} < \overline{(z,t)}$ and $\overline{(z,t)} < \overline{(u,v)}$. Thus $x + t < z + y$ and $z + v < v + t$. Hence $x + t < v + t$ and so $\overline{(x,y)} < \overline{(u,v)}$.

Comparability. We will use the fact that $<$ is a total order on $\mathbb{N}$. Let $\overline{(x,y)}$ and $\overline{(z,t)}$ be two elements of $\mathbb{Z}$. If $x + t < z + y$ then $\overline{(x,y)} < \overline{(z,t)}$. If $z + y < x + t$ then $\overline{(z,t)} < \overline{(x,y)}$. If $x + t = z + y$ then $\overline{(x,y)} = \overline{(z,t)}$.

Immediate Successor. Let $\overline{(x,y)}$ be an element of $\mathbb{Z}$. It is easy to show that $\overline{(x,y)} < \overline{(x+1,y)}$ and that there are no elements of $\mathbb{Z}$ in between.

Immediate Predecessor. Let $\overline{(x,y)}$ be an element of $\mathbb{Z}$. It is easy to show that $\overline{(x,y+1)} < \overline{(x,y)}$ and that there are no elements of $\mathbb{Z}$ in between. □

Exercises. α, β, γ stand for the elements of $\mathbb{Z}$.

i. Show that if $\alpha < \beta$ then $\alpha + \gamma < \beta + \gamma$.

ii. Show that if $\alpha < \beta$ then $-\beta < -\alpha$.

iii. Show that $\alpha < \beta$ if and only if $\beta - \alpha > 0$.

iv. Assume $\alpha < \beta$ and $0 < \gamma$. Show that $\alpha\gamma < \beta\gamma$.

v. Assume $\alpha < \beta$ and $\gamma < 0$. Show that $\beta\gamma < \alpha\gamma$.

vi. Assume $\alpha < \beta$ and $\gamma < 0$. Show that $\beta\gamma < \alpha\gamma$.

vii. Assume $\alpha > 0$ and $\beta > 0$. Show that $\alpha\beta > 0$.

viii. Assume $\alpha < 0$ and $\beta < 0$. Show that $\alpha\beta > 0$.

12.4 Embedding of $(\mathbb{N}, +, \times, <)$ in $(\mathbb{Z}, +, \times, <)$

In "real life", $\mathbb{N}$ is a subset of $\mathbb{Z}$, but as we defined it here, $\mathbb{N} \cap \mathbb{Z} = $. In this subsection we will remedy this this by transporting $\mathbb{N}$ into $\mathbb{Z}$.

Consider the function $i : \mathbb{N} \longrightarrow \mathbb{Z}$ defined by the rule $i(x) = \overline{(x, 0)}$. Then, i is an injection and for all $x, y \in \mathbb{N}$,

i. $i(x + y) = i(x) + i(y)$.

ii. $i(xy) = i(x)i(y)$.

iii. $x < y \iff i(x) < i(y)$.

These properties are easy to check and we leave them to the reader.

This shows that a copy of the structure $(\mathbb{N}, +, \times, <)$ exists in $\mathbb{Z}$, namely the subset $i(\mathbb{N})$ of $\mathbb{Z}$ together with the operations $+$ and $\times$ and the relation $<$ restricted to to the subset $i(\mathbb{N})$ of $\mathbb{Z}$.

Lemma 12.4.1 *$\mathbb{Z} = i(\mathbb{N}) \cup -i(\mathbb{N})$ and $i(\mathbb{N}) \cap -i(\mathbb{N}) = \{0\}$.*

Proof: Let $\overline{(x, y)} \in \mathbb{Z}$. Assume $x \geq y$. Then there is an $a \in \mathbb{N}$ such that $y + a = x$. Thus $\overline{(x, y)} = \overline{(y + a, y)} = \overline{(a, 0)} = i(a)$. Assume $x < y$. Then there is an $a \in \mathbb{N}$ such that $x + a = y$. Thus $\overline{(x, y)} = \overline{(x, x + a)} = \overline{(0, a)} = -\overline{(a, 0)} = -i(a)$. This proves that $\mathbb{Z} = i(\mathbb{N}) \cup -i(\mathbb{N})$. The last part is easy as well. □

From now on we identify the elements of $\mathbb{N}$ with the elements of $i(\mathbb{N})$ via the injection i, in other words, we rename the elements of $i(\mathbb{N})$ by the elements of $\mathbb{N}$: For $x \in \mathbb{N}$, the element $\overline{(x, 0)}$ will be denoted by x from now on. With this convention, we get $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$ and for all $x \in \mathbb{N}$,

$$\begin{array}{rll} 0 & \text{stands for} & \overline{(0, 0)} \\ x & \text{stands for} & \overline{(x, 0)} \\ -x & \text{stands for} & \overline{(0, x)}. \end{array}$$

Now we can write the multiplication and the order on $\mathbb{Z}$ in terms of the elements of $\mathbb{N}$. For all x, $y \in \mathbb{N}$,

$$\begin{array}{l} x(-y) = -(xy) = (-x)y \\ -x \leq y \\ -x \leq -y \iff y \leq x. \end{array}$$

These properties are also easy to check and we leave them to the reader.

Exercises.

i. Show that $0 \times \alpha = 0$ for all $\alpha \in \mathbb{Z}$. (Here 0 stands for the element $i(0) = (0,0)$ of $\mathbb{Z}$).

ii. Show that $1 \times \alpha = \alpha$ for all $\alpha \in \mathbb{Z}$. (Here 1 stands for the element $i(1) = (1,0)$ of $\mathbb{Z}$).

iii. Show that $-1 \times \alpha = -\alpha$ for all $\alpha \in \mathbb{Z}$. (Here -1 stands for the element $-i(1) = (0,1)$ of $\mathbb{Z}$).

iv. Show that $2 \times \alpha = \alpha + \alpha$ for all $\alpha \in \mathbb{Z}$. (Here 2 stands for the element $i(2) = (2,0)$ of $\mathbb{Z}$).

v. Show that $\mathbb{Z}$ is the smallest subset of $\mathbb{Z}$ containing 1 and closed under subtraction.

12.5 Additive Structure of $\mathbb{Z}$

In this subsection, we will investigate the properties of $+$ and $-$ on $\mathbb{Z}$. From the above subsection, we will only retain the convention that the element $\overline{(0,0)}$ is denoted by 0.

Theorem 12.5.1 *i. For all $\alpha, \beta, \gamma \in \mathbb{Z}$, $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$,*
ii. For all $\alpha \in \mathbb{Z}$, $\alpha + 0 = 0 + \alpha = \alpha$
iii. For all $\alpha \in \mathbb{Z}$ there is a $\beta \in \mathbb{Z}$ (namely $-\alpha$) such that $\alpha + \beta = \beta + \alpha = 0$.
iv. For all α, $\beta \in \mathbb{Z}$, $\alpha + \beta = \beta + \alpha$.

Proof: i. Let $\alpha = \overline{(x,y)}$, $\beta = \overline{(x_1,y_1)}$ and $\gamma = \overline{(x_2,y_2)}$. Then

$$(\alpha + \beta) + \gamma = \overline{((x + x_1) + x_2, (y + y_1) + y_2)}$$

and

$$\alpha + (\beta + \gamma) = \overline{(x + (x_1 + x_2), y + (y_1 + y_2))}.$$

The equality is now clear.
ii, iii, iv. Easy. □

We now define the following terms:

$$\begin{array}{rcl} -x + y & := & (-x) + y \\ -x - y & := & (-x) + (-y) \quad = \quad (-x) - y \end{array}$$

Lemma 12.5.2 *For all x, $y \in \mathbb{Z}$,*

$$\begin{array}{rcl} -(x - y) & = & -x + y \\ -(-x + y) & = & x - y \\ -(-x - y) & = & x + y \end{array}$$

Proof: Left as an exercise. □

Exercises. We compute in $\mathbb{Z}$. The elements α, β, γ stand for the elements of $\mathbb{Z}$.

i. Show that if $\alpha + \gamma = \beta + \gamma$ then $\alpha = \beta$.

ii. Show that if $\alpha + \beta = \alpha$ for some $\alpha \in \mathbb{Z}$ then $\beta = 0$.

12.6 Multiplicative Structure of $\mathbb{Z}$

As we let 0 stand for $\overline{(0,0)}$ above, in this subsection, we will also let 1 stand for $\overline{(1,0)}$

Theorem 12.6.1 *For all α, $\beta, \gamma \in \mathbb{Z}$ we have i. $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.*
ii. $\alpha \times 1 = 1 \times \alpha = \alpha$.
iii. $\alpha\beta = \beta\alpha$.

Proof: Left as an exercise. □

The theorem above gives the multiplicative properties of $\mathbb{Z}$. The next theorem is about the relationship between addition and multiplication.

Theorem 12.6.2 *For all α, $\beta, \gamma \in \mathbb{Z}$, $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.*

Proof: Left as an exercise. □

Exercises. α, β, γ stand for the elements of $\mathbb{Z}$.

i. Assume $\alpha\beta = 1$. Show that $\alpha = \beta = \pm 1$.

ii. Assume $\alpha\beta = 0$. Show that either $\alpha = 0$ or $\beta = \pm 1$.

iii. Show that $2x = 3$ has no solution in $\mathbb{Z}$.

12.7 Ordering on $\mathbb{Z}$, Revisited

In the two last subsections above we investigated the additive and the multiplicative properties of $\mathbb{Z}$. In this subsection, we investigate the relationship of these two operations to the order relation .

Theorem 12.7.1 *Let $\alpha, \beta, \gamma \in \mathbb{Z}$. Assume that $\alpha < \beta$. Then*
i. $\alpha + \gamma < \beta + \gamma$.
ii. If $\gamma > 0$, then $\alpha\gamma < \beta\gamma$.

Proof: Left as an exercise. □

Absolute Value. For $\alpha \in \mathbb{Z}$, we define $|\alpha| = \max\{\alpha, -\alpha\}$. We call $|\alpha|$, the absolute value of α.

Sign Function. For $\alpha \in \mathbb{Z}$, we define

$$\operatorname{sgn}(\alpha) = \begin{cases} 1 & \text{if } \alpha > 0 \\ 0 & \text{if } \alpha = 0 \\ -1 & \text{if } \alpha < 0 \end{cases}$$

sgn is called the **sign function**.

Exercises. α, β, γ stand for the elements of $\mathbb{Z}$.

i. Show that $|\alpha| > 0$, i.e. is in $\mathbb{N}$.

ii. Show that $|\alpha| = 0$ if and only if $\alpha = 0$.

iii. Show that $|\alpha| = |\beta|$ if and only if $\alpha = \pm\beta$.

iv. Show that $|\alpha + \beta| \leq |\alpha| + |\beta|$.

v. Show that $|\alpha\beta| \leq |\alpha||\beta|$.

vi. Show that $\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$.

vii. Show that any $\alpha \in \mathbb{Z}$ can be written as $\alpha = \operatorname{sgn}(a)\prod_p p^{\operatorname{ord}_p(\alpha)}$ where the product ranges over all primes $p > 1$ and $\operatorname{ord}_p(a)$ is the largest natural number such $p^{\operatorname{ord}_p(\alpha)}$ divides $|a|$.

12.8 Divisibility and Subgroups

We should start by nothing that, in terms of divisibility, an integer n and its additive inverse $-n$ have no distinction what so ever: an integer divides n if and only if it divides $-n$ and n divides an integer if and only if $-m$ divides this integer. Oh! By divisibility we mean the following: An integer n divides an integer m if there is an integer q such that $m = nq$.

We first extend Theorem 11.10.1 from $\mathbb{N}$ to $\mathbb{Z}$:

Theorem 12.8.1 (Division) *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there are unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.*

Proof: If $a \in \mathbb{N}$, then this is just Theorem 11.10.1. Assume $a < 0$. Then applying Theorem 11.10.1 to $-a$ we have $-a = qb + r$ where $0 \leq r < b$. If $r = 0$, then $a = (-q)b$ and we are done for the existence. Assume $0 < r < b$. We have $a = -qb - r = (-q-1)b + (b-r)$. Since $0 < b - r < b$, this proves the existence.

Now we prove the uniqueness. Assume $bq + r = bq_1 + r_1$ where $0 \leq r,\ r_1 < b$. If $q = q_1$, then clearly $r = r_1$. Assume $q \neq q_1$. Without loss of generality $q > q_1$. Then $b < b(q - q_1) = r_1 - r \leq b$, a contradiction. □

A nonempty subset of $\mathbb{Z}$ closed under substraction is called a **subgroup** of $\mathbb{Z}$. Note that if $n \in \mathbb{Z}$, then the set

$$n\mathbb{Z} := \{nz : z \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z}$. We show that these are all the subgroups of $\mathbb{Z}$:

Theorem 12.8.2 (Subgroups of $\mathbb{Z}$) *A subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some unique $n \in \mathbb{N}$.*

Proof: Let H be a subgroup of $\mathbb{Z}$. We first prove three easy properties of H.

1) Since $H \neq \emptyset$, there is an element $h \in H$. Hence $0 = h - h \in H$.

2) Let $h \in H$. Then $-h = 0 - h \in H$ because $0 \in H$ by above. Hence $-H = H$.

3) Let $h, k \in H$. Then $h + k = h - (-k) \in H$. Thus H is also closed under addition.

Now we classify all subgroups of $\mathbb{Z}$.

If $H = \{0\}$, then $H = 0\mathbb{Z}$. So we assume $H \neq \{0\}$. Since $H = -H$, then H has positive elements. Let n be the smallest positive integer in H. Since $n \in H$, $-n$ is also in H. Since H is closed under addition, it follows that $n\mathbb{Z} \subseteq H$. We will show the reverse inclusion. Let $h \in H$. Using Theorem 12.8.1, $h = nq + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < n$. But now, $r = h - nq$ and since $nq \in n\mathbb{Z} \subseteq H$, we get $r \in H$. But, unless $r = 0$, this contradicts the fact that n was chosen to be the least positive integer in H. Thus $r = 0$ and $h = nq + r = nq \in n\mathbb{Z}$. □

We note that for $n, m \in \mathbb{Z}$, $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if $m|n$, in other words the inclusion order on the set of subgroups of $\mathbb{Z}$ is the divisibility order reversed. Thus a maximal (and proper, i.e. $\neq \mathbb{Z}$) subgroup of $\mathbb{Z}$ is of the form $p\mathbb{Z}$ for some prime $p \in \mathbb{N}$. It also follows that any ascending chain of subgroups of $\mathbb{Z}$ is stationary, i.e. if $H_0 \subseteq H_1 \subseteq H_2 \subseteq \ldots$ is an ascending chain of subgroups, then there is an n_0 such that for all $n > n_0$, $H_n = H_{n_0}$.

Greatest Common Divisor, Least Common Multiple. Let a and b be two integers which are not both 0. We say that d is the **greatest common divisor** of a and b if d is the largest natural number that divides both a and b.

Lemma 12.8.3 *For any $a, b \in \mathbb{Z}$, $\gcd(a, b)$ exists and there are $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.*

Proof: Replacing a and b by $|a|$ and $|b|$, we may assume that $a \geq 0$ and $b \geq 0$.

Existence. Since 1 divides both a and b and since any number that divides both a and b can be at most $\max(a, b) > 0$, the set of natural numbers that divide both a and b is a finite nonempty set bounded by $\max(a, b)$. Therefore there is a largest such number. This proves the existence of $\gcd(a, b)$. We let $d = \gcd(a, b)$.

Second Part. We proceed by induction on $\max(a, b)$. If $a = 1$, then take $x = 1$, $y = 0$. If $b = 1$, then take $x = 0$, $y = 1$. This takes care of the initial step $\max(a, b)$. Assume $\max(a, b) > 1$. If $a = b$, then $d = a$ and we may take $x = 1$, $y = 0$. Assume $a \neq b$. Without loss of generality, we may assume that $a > b$. Note that the divisors of a and b are the same as the divisors of $a - b$ and b. Hence $\gcd(a - b, b) = \gcd(a, b) = d$. Since $\max(a - b, b) < a = \max(a, b)$, by induction there are two integers x and y' such that $x(a - b) + y'b = d$, i.e. $xa + (y' - x)b = d$. Take $y = y' - x$. □

Let a and b be two nonzero integers. We say that m is the **least common multiple** of a and b if m is the least natural number that is divisible by both a and b.

Lemma 12.8.4 *For any a, $b \in \mathbb{Z}\backslash\{0\}$, $\operatorname{lcm}(a,b)$ exists and $ab = \pm \gcd(a,b)\operatorname{lcm}(a,b)$.*

Proof: Replacing a and b by $|a|$ and $|b|$ again, we may assume that $a > 0$ and $b > 0$. Since a and b both divide ab, $\operatorname{lcm}(a,b)$ exists.

Let $d = \gcd(a,b)$ and $m = \operatorname{lcm}(a,b)$. Let a' and b be such that $a = da'$ and $b = db'$. Then $ab = d^2a'b'$. We need to prove that $m = da'b'$.

Since $da'b' = ab' = a'b$, a and b both divide $da'b'$.

Let x be divisible by both a and b. Then $x = au = bv$ for some u, v. We have $a'du = au = x = bv = b'dv$ and so $a'u = b'v$. Since a' and b' cannot have a common divisor (otherwise d would be larger), b' must divide u. **(This last fact needs a serious proof, that we have not undertaken yet. I should put this somewhere else)**. Write $u = cb'$. Now $x = au = acb' = a'dcb'$ and so $a'b'd$ divides x, in particular $a'b'd \leq x$. This shows that $a'b'd$ is the least multiple of a and b, i.e. $a'b'd = m$.

There is another way to define gcd and lcm, which is more modern and better in several ways. If $(H_i)_i$ is any family of subgroups of $\mathbb{Z}$, then it is clear that $\cap_i H_i$ is also a subgroup of $\mathbb{Z}$. In particular, for any n, $m \in \mathbb{Z}$, $n\mathbb{Z} \cap m\mathbb{Z} = k\mathbb{Z}$ for some unique $k \in \mathbb{N}$. Since $n\mathbb{Z} \cap m\mathbb{Z}$ is the largest subgroup contained in $n\mathbb{Z}$ and in $m\mathbb{Z}$, it is clear that k is the smallest natural numbers that is a multiple of both n and m. We call k the **least common multiple** of n and m and we let $\operatorname{lcm}(n,m) = k$.

If $(H_i)_i$ is any family of subgroups of $\mathbb{Z}$, then it is clear that

$$\sum_i H_i = \{h_{i_1} + \ldots + h_{i_k} : k \in \mathbb{N} \text{ and } h_{i_j} \in H_{i_j} \text{ for all } j = 1, \ldots, k\}$$

is also a subgroup of $\mathbb{Z}$. In particular, for any n, $m \in \mathbb{Z}$, $n\mathbb{Z} + m\mathbb{Z} = k\mathbb{Z}$ for some unique $k \in \mathbb{N}$. Since $n\mathbb{Z} + m\mathbb{Z}$ is the smallest subgroup containing both $n\mathbb{Z}$ and $m\mathbb{Z}$, it is clear that k is the smallest natural numbers that is divisible by both n and m. We call k the **greatest common divisor** of n and m and we let $\gcd(n,m) = k$. One also writes $(n,m) = k$ sometimes.

Writing $n = \operatorname{sgn}(n)\prod_p p^{\operatorname{ord}_p(n)}$ and $m = \operatorname{sgn}(m)\prod_p p^{\operatorname{ord}_p(m)}$, where p ranges over all the primes in $\mathbb{N}$, we see that

$$\operatorname{lcm}(n,m) = \prod_p p^{\max\{\operatorname{ord}_p(n),\operatorname{ord}_p(m)\}}$$

and

$$\gcd(n,m) = \prod_p p^{\min\{\operatorname{ord}_p(n),\operatorname{ord}_p(m)\}}.$$

In particular,

$$\begin{aligned} \operatorname{lcm}(n,m)\gcd(n,m) &= \textstyle\prod_p p^{\min\{\operatorname{ord}_p(n),\operatorname{ord}_p(m)\}+\min\{\operatorname{ord}_p(n),\operatorname{ord}_p(m)\}} \\ &= \textstyle\prod_p p^{\operatorname{ord}_p(n)+\operatorname{ord}_p(m)} = \prod_p p^{\operatorname{ord}_p(n)}\prod_p p^{\operatorname{ord}_p(m)} = |nm|. \end{aligned}$$

Thus we have:

Proposition 12.8.5 $\operatorname{lcm}(n,m)\gcd(n,m) = |nm|$.

Two integers are said to be **prime to each other** if they are both divisible only by 1 and -1. In other words n and m are prime to each other if and only if $\gcd(n,m) = 1$.

Theorem 12.8.6 *Two integers a and b are prime to each other if and only if there are integers x and y such that $ax + by = 1$.*

Proof: Suppose there are integers x and y such that $ax + by = 1$. Then if an integer divides both a and b, then this integer must divide $ax + by = 1$, so it must be ± 1.

Conversely, suppose that $\gcd(a,b) = 1$. Then $1 \in \mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. It follows that there are integers x and y such that $ax + by = 1$. □

Exercises.

i. Show that $\gcd(\gcd(a,b),b) = \gcd(a,\gcd(b,c))$.

ii. Show that $\operatorname{lcm}(\operatorname{lcm}(a,b),b) = \operatorname{lcm}(a,\operatorname{lcm}(b,c))$.

12.9 Euclidean Algorithm

There is a famous algorithm to find the greatest common divisor of two integers, called **Euclidean Algorithm**.

Let n and m be two given nonzero integers. We want to find their greatest common divisor. Set $r_0 = n$ and $r_1 = m$. Divide r_0 by r_1 to get $r_0 = qr_1 + r_2$ where $q \in \mathbb{Z}$ and $0 \le r_2 < r_1$. Inductively, suppose we have found r_k and r_{k+1} where $0 \le r_{k+1} < r_k$. Divide r_k by r_{k+1} to get $r_k = qr_{k+1} + r_{k+2}$ where $q \in \mathbb{Z}$ and $0 \le r_{k+2} < r_{k+1}$. In this way we get a strictly decreasing sequence $(r_k)_k$. At a finite stage $n > 1$, we must have $r_n = 0$. We claim that $r_{n-1} = \gcd(n,m)$.

Since $r_k = qr_{k+1} + r_{k+2}$, it is clear that $\gcd(r_k, r_{k+1}) = \gcd(r_{k+1}, r_{k+2})$, therefore

$$\begin{aligned} \gcd(n,m) &= \gcd(r_0,r_1) = \gcd(r_1,r_2) = \ldots = \gcd(r_{n-1},r_n) \\ &= \gcd(r_{n-1},0) = r_{n-1}. \end{aligned}$$

12.10 Quotients

The reader must have seen how to work "modulo n". Here we set the foundations.

For $x \in \mathbb{Z}$ and $A \subseteq \mathbb{Z}$, we let

$$n + A = \{n + a : a \in A\}$$

and

$$nA = \{na : a \in A\}.$$

Let H be a subgroup of $\mathbb{Z}$. Thus $H = n\mathbb{Z}$ for some $n \in \mathbb{N}$. Define the following relation on $\mathbb{Z}$:

$$x \equiv_n y \iff x - y \in n\mathbb{Z} \iff n \text{ divides } x - y.$$

It is easy to check that this is an equivalence relation. Let $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\equiv_n$. For $x \in \mathbb{Z}$, we denote the equivalence class of x by $\overline{x}$. Thus

$$\begin{aligned} \overline{x} &= \{y \in \mathbb{Z} : n \text{ divides } x - y\} = \{y \in \mathbb{Z} : x - y \in n\mathbb{Z}\} \\ &= \{y \in \mathbb{Z} : y - x \in n\mathbb{Z}\} = \{y \in \mathbb{Z} : y \in x + n\mathbb{Z}\} = x + n\mathbb{Z}. \end{aligned}$$

Unfortunately, in the notation $\overline{x}$, as an element of $\mathbb{Z}/n\mathbb{Z}$, i.e. as $x + n\mathbb{Z}$, the number n does not exist. Therefore the reader should know at any point of our discussion what the integer n is.

Lemma 12.10.1 *Given n, for every $x \in \mathbb{Z}$ there is a unique $r = 0, 1, \ldots, n-1$ such that the element $\overline{x}$ of $\mathbb{Z}/n\mathbb{Z}$ is equal to $\overline{r}$.*

Proof: Follows immediately from Theorem 12.8.1. □

12.11 Chinese Remainder Theorem

12.12 Subgroups of $\mathbb{Z} \oplus \mathbb{Z}$

Chapter 13

Rational Numbers

13.1 Rational Numbers

Prologue. In $\mathbb{Z}$ we can do addition, substraction and multiplication, but not division. For example we cannot divide 2 by 3 (i.e. the equation $3x = 2$ has no solution in $\mathbb{Z}$), because $2/3$ is not in $\mathbb{Z}$. To remedy this situation, we will extend the structure $\mathbb{Z}$ to a larger set where not only we can do addition, substraction and multiplication compatible with the similar operations in $\mathbb{Z}$, but also division.

We would like to invent numbers that will stand for $2/3$ e.g. If we attempt to denote $2/3$ by the pair $(2, 3)$, then we should have $(2, 3) = (4, 6)$ and as we know this is not the case. We overcome this difficulty by noting that $a/b = c/d$ if and only if $ad = bc$. Accordingly, on the set $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, we define the following relation:

$$(x, y) \equiv (z, t) \iff xt = yz.$$

We will show that this is an equivalence relation. Then we will let $\mathbb{Q}$ to denote the set $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\equiv$. Finally we will define the four operations as follows:

$$\begin{array}{rcl} \overline{(x,y)} + \overline{(z,t)} & = & \overline{(xt + yz, yt)} \\ \overline{(x,y)} - \overline{(z,t)} & = & \overline{(xt - yz, yt)} \\ \overline{(x,y)} \times \overline{(z,t)} & = & \overline{(xz, yt)} \\ \overline{(x,y)}/\overline{(z,t)} & = & \overline{(xt, yz)} \end{array}$$

(For the last operation we need $z \neq 0$). After that, we will define an ordering on $\mathbb{Q}$. To finish, we will embed $\mathbb{Z}$ inside $\mathbb{Q}$.

Lemma 13.1.1 *The relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\equiv$ defined by $(x, y) \equiv (z, t) \iff xt = yz$ is an equivalence relation.*

Proof: a. i. Reflexivity. Let $(x, y) \in X$. Then since $xy = yx$, we have $(x, y) \equiv (x, y)$.

ii. Symmetry. Let $(x, y), (z, t) \in X$ be such that $(x, y) \equiv (z, t)$. Hence $xt = yz$. Therefore $zy = tx$, implying $(z, t) \equiv (x, y)$.

iii. Transitivity. Let (x,y), (z,t), $(u,v) \in X$ be such that $(x,y) \equiv (z,t)$ and $(z,t) \equiv (u,v)$. Hence $xt = yz$ and $zv = tu$. Multiplying these equalities side by side, we get $xtzv = yztu$. Since $t \neq 0$, by simplifying we get $xzv = yzu$. If $z \neq 0$, then we can simplify further to get $xv = yu$, hence $(x,y) \equiv (u,v)$.

Assume $z = 0$. Then $xt = yz = 0$ and $tu = zv = 0$. Since $t \neq 0$, we get $x = u = 0$, so that $xv = 0 = yu$ and $(x,y) \equiv (u,v)$ again. □

We let $\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\equiv$. Now we show that the attempt to define the four operations as above is successful:

Lemma 13.1.2 *Let (x,y), (z,t), (x',y'), $(z',y') \in \mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$. Assume $(x,y) \equiv (x',y')$ and $(z,t) \equiv (z',t')$. Then*
i. $(xt+yz, yt) \equiv (x't' + y'z', y't')$.
ii. $(xt-yz, yt) \equiv (x't' - y'z', y't')$.
iii. $(xz, yt) \equiv (x'z', y't')$.
iv. If $z \neq 0$, then $z' \neq 0$ and $(xt, yz) \equiv (x't', y'z')$.

Proof: i. Assume $(x,y) \equiv (x',y')$ and $(z,t) \equiv (z',t')$. Then $xy' = yx'$ and $zt' = tz'$. Multiplying the first one by tt' and the second one by yy' we get $xy'tt' = yx'tt'$ and $zt'yy' = tz'yy'$. Adding these two side by side we get $xy'tt'+zt'yy' = yx'tt'+tz'yy'$, and factoring, we get $(xt+yz)y't' = yt(x't'+y'z')$, meaning $(xt+yz, yt) \equiv (x't' + y'z', y't')$.

ii. Similar.

iii. Assume $(x,y) \equiv (x',y')$ and $(z,t) \equiv (z',t')$. Then $xy' = yx'$ and $zt' = tz'$. Multiplying these two side by side, we get $xy'zt' = yx'tz'$, i.e. $xzy't' = ytx'z'$, meaning $(xz, yt) \equiv (x'z', y't')$.

iv. If $z' = 0$, then $zt' = z't = 0$. But $t' \neq 0$, so $z = 0$. For the second part, we need to show that $xty'z' = yzx't'$. Left as an exercise. □

It follows that we can define the four operations $+$, $-$, $\times$ and division on the set $\mathbb{Q}$. As usual, we let $\alpha\beta$ denote $\alpha \times \beta$.

Next we attempt define the order on $\mathbb{Q}$ as follows: Let $\overline{(a,b)}$, $\overline{(c,d)} \in \mathbb{Q}$. Clearly, $\overline{(a,b)} = \overline{(-a,-b)}$, so that we may assume that $b > 0$ and $d > 0$. Now we want to let

$$\overline{(a,b)} < \overline{(c,d)} \iff ad < bc.$$

But for this definition to be valid, we need to prove the following:

Lemma 13.1.3 *Let (x,y), (z,t), (x_1,y_1), $(z_1,y_1) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$. Assume $(x,y) \equiv (x_1,y_1)$, $(z,t) \equiv (z_1,t_1)$ and $xt < yz$. Then $x_1t_1 < y_1z_1$.*

Proof: By assumptions $xy_1 = x_1y$, $zt_1 = z_1t$, y, y_1, t, $t_1 > 0$ and $xt < yz$. From the inequalities we get $xtt_1y_1 < yzt_1y_1$. This and the first two equalities yield $x_1ytt_1 < yy_1z_1t$. Since $y > 0$ and $t > 0$, we can simplify to get $x_1t_1 < y_1z_1$. □

This shows that the relation $<$ is well defined.

By abuse of language, we will let $0 = \overline{(0,1)} \in \mathbb{Q}$ and $1 = \overline{(1,1)} \in \mathbb{Q}$.

Theorem 13.1.4 *The following hold:*

A1. Associativity. *For all* α, β, $\gamma \in \mathbb{Q}$, $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$.

A2 Identity Element. *For all* $\alpha \in \mathbb{Q}$, $\alpha + 0 = 0 + \alpha = \alpha$.

A3 Inverse Element. *For all* $\alpha \in \mathbb{Q}$, *there is a unique* $\beta \in \mathbb{Q}$ *such that* $\alpha+\beta = \beta+\alpha = 0$, *namely, if* $\alpha = \overline{(a,b)}$, *then* $\beta = \overline{(-a,b)}$.

A4. Commutativity. *For all* α, $\beta \in \mathbb{Q}$, $\alpha+\beta = \beta+\alpha$.

If $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, *then we also have:*

M1. Associativity. *For all* α, β, $\gamma \in \mathbb{Q}^*$, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

M2. Identity Element. *For all* $\alpha \in \mathbb{Q}^*$, $\alpha \times 1 = 1 \times \alpha = \alpha$.

M3. Inverse Element. *For all* $\alpha \in \mathbb{Q}^*$, *there is a unique* $\beta \in \mathbb{Q}^*$ *such that* $\alpha\beta = \beta\alpha = 1$, *namely, if* $\alpha = \overline{(a,b)}$, *then* $\beta = 1/\alpha = \overline{(b,a)}$.

M4. Commutativity. *For all* α, $\beta \in \mathbb{Q}^*$, $\alpha\beta = \beta\alpha$.

D. Distributivity. *For all* α, β, $\gamma \in \mathbb{Q}$, $\alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma$ *and* $(\alpha+\beta)\gamma = \alpha\gamma+\beta\gamma$.

O. Total Order. $<$ *is a total order on* $\mathbb{Q}$.

OA. *For all* α, β, $\gamma \in \mathbb{Q}$, *if* $\alpha < \beta$ *then* $\alpha+\gamma < \beta+\gamma$.

OM. *For all* α, β, $\gamma \in \mathbb{Q}$, *if* $\alpha < \beta$ *and* $0 < \gamma$, *then* $\alpha\gamma < \beta\gamma$.

Proof: Left to the reader. □

We let $\alpha/\beta = \frac{\alpha}{\beta} = \alpha \times 1/\beta$ and $\alpha^{-1} = 1/\alpha$ if $\alpha \neq 0$.

Lemma 13.1.5 (Density.) *For all* α, $\beta \in \mathbb{Q}$, *if* $a < b$ *then* $\alpha < \frac{\alpha+\beta}{2} < \beta$.

Finally we embed $\mathbb{Z}$ in $\mathbb{Q}$.

Proposition 13.1.6 *Let* $i : \mathbb{Z} \longrightarrow \mathbb{Q}$ *be the map defined by* $i(x) = \overline{(x,1)}$. *Then* i *is a one to one map and for all* $x, y \in \mathbb{Z}$,

i. $i(x+y) = i(x)+i(y)$.

ii. $i(xy) = i(x)i(y)$.

iii. $x < y$ *if and only if* $i(x) < i(y)$.

Furthermore, with our earlier convention, we have $i(0) = 0$ *and* $i(1) = 1$.

Also, for any $\alpha \in \mathbb{Q}$, *there are* $x \in \mathbb{Z}$, $y \in \mathbb{N} \setminus \{0\}$ *such that* $\alpha = i(x)/i(y)$. *If we make the assumption that* $(x,y) = 1$, *then* x *and* y *are unique.*

Proof: Easy. □

Now we identify $\mathbb{Z}$ with the subset $i(\mathbb{Z})$ of $\mathbb{Q}$. With this identification

Exercises.

i. Show that $\mathbb{Q}$ has no last or first element (for the order).

ii. Show that there is no $x \in \mathbb{Q}$ such that $x \times x = 2$.

iii. Show that if $\alpha\beta = 0$ for α, $\beta \in \mathbb{Q}$ then either α or β is zero.

13.2 Some Combinatorics

n choose m

Fermat's little Theorem

Problem. Quotient Fields.

Problem. Subgroups of $\mathbb{Q}$. A **subgroup** of $\mathbb{Q}$ is a nonempty subset of $\mathbb{Q}$ closed under substraction.

Theorem 13.2.1 (Finitely Generated Subgroups of $\mathbb{Q}$) *For a/b, $c/d \in \mathbb{Q}$, $\langle a/b, c/d\rangle = \langle \gcd(ad, bc)/bd\rangle$. Thus a finitely generated subgroup of $\mathbb{Q}$ is in fact generated by one element.*

Theorem 13.2.2 (Classification of Subgroups of $\mathbb{Q}$) *Let G be a nontrivial subgroup of $\mathbb{Q}^+$. Then there are unique $a \in \mathbb{N} \setminus \{0\}$ and $f : \{\text{primes of } \mathbb{N}\} \longrightarrow \mathbb{N} \cup \{\infty\}$ such that*

$$G = \mathbb{Q}(a, f) = a\{x/p_1^{n_1} \dots p_k^{n_k} : k \in \mathbb{N}, \, p_i \text{ prime and } n_i \leq f(p_i) \text{ forall } i\}.$$

Chapter 14

Real Numbers

Chapter 15

Well-Ordered Sets

15.1 Definitions and Examples

A totally ordered structure $(X, <)$ is called a **well-ordered set** if any nonempty subset of X has a least element.

Examples.

i. **Easy Examples.** By definition $\emptyset$ is a well-ordered set. We have seen that ω is a well-ordered set with its "natural" order. Any subset of a well-ordered set is a well-ordered set with the restricted order. In particular each natural number n is a well ordered set. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}^{\geq 0}$ (together with the natural order on them) are not well-ordered structures.

ii. **Translation.** Let $(X, <)$ be a well-ordered structure. Let $f : X \longrightarrow Y$ be a bijection from X onto Y. Then we can translate the well-order structure of X onto Y via f as follows: Declare that, for $y, y' \in Y$, $y < y'$ if $f^{-1}(y) < f^{-1}(y')$. This gives a well-order structure on Y, which essentially the one of X. We will see that the two well-ordered sets are "isomorphic".

iii. **Union – Addition.** Let $(X, <_1)$ and $(Y, <_2)$ be two well-ordered sets. Replacing X by $X \times \{0\}$ and Y by $Y \times \{1\}$, and translating the orders of X and Y onto these sets via the obvious maps, we may assume that $X \cap Y = \emptyset$. Now consider the set $Z = X \cup Y$. Define the relation $<$ on Z as follows:

$$z < z' \iff \begin{cases} z, z' \in X \text{ and } z <_1 z' \\ z, z' \in Y \text{ and } z <_2 z' \\ z \in X \text{ and } z' \in Y \end{cases}$$

This relation well-orders Z. We will say that the ordered set is the **disjoint union** of the ordered sets $(X, <_1)$ and $(Y, <_2)$ (in this order!) We will also say for a while that Z is the **sum** of X and Y and we will write $Z = X + Y$.

iv. **Lexicographic Ordering.** Let $(X, <_1)$ and $(Y, <_2)$ be two well-ordered sets. Consider the following relation on the set $X \times Y$

$$(x, y) < (x', y') \iff \begin{cases} y <_2 y' \\ y = y' \text{ and } x <_1 x' \end{cases}$$

This defines a well-ordering called **lexicographic ordering** on the Cartesian product $X \times Y$.

Note that the lexicographic ordering on $X \times 2$ is exactly the order defined in the previous item when $X = Y$, i.e. $X \times 2 = X + X$.

A nonempty well-ordered set X has a minimal element, say x_0. If $X \neq \{x_0\}$, then $X \setminus \{x_0\}$ has also a minimal element, say x_1. Thus x_1 is the element "right after" x_0. In other words $x_0 < x_1$ and if $x_0 < x$ then $x_1 \leq x$.

Let X be a well-ordered set, and let $x \in X$. Suppose x is the last element of X, i.e. suppose that $\{y \in X : x < y\}$ is not empty. Then this set has a (unique) least element. We will call this element the **successor** of x and we will denote it $S(x)$.

An **initial segment** of a well-ordered set X is a subset I such that for all $a \in I$ and $x \in X$, if $x < a$ then $x \in I$.

Exercises. Throughout X and Y stand for well-ordered sets.

i. Show that Y has a last element if and only if $X + Y$ has a last element.

ii. Show that X and Y have a last element if and only if $X \times Y$ has a last element.

iii. Show that $2 \times X$ is not $X + X$ always.

iv. Let I be an initial segment of X. Show that either $I = X$ or $I = (-\infty, a)$ for some $a \in X$. Conclude that for any two initial segments of X, one is a subset (hence an initial segment) of the other.

v. Find all initial segments of $\mathbb{N}$.

vi. Find all initial segments of $\mathbb{N} + \mathbb{N}$.

vii. Let $\Im$ be a set of initial segments of X. Show that $\cup_{I \in \Im} I$ is an initial segment of X.

15.2 Transfinite Induction

The following theorem, whose proof is trivial (and shorter than its statement), is the essence of well-ordered sets:

Theorem 15.2.1 *Let X be a well-ordered set. Let A be a subset of X. Assume that for any $x \in X$, if $(-\infty, x) \subseteq A$ then $x \in A$. Then $A = X$.*

Proof: Assume $X \neq A$. Let x be the least element of $X \setminus A$. Then $(-\infty, x) \subseteq A$. So, by hypothesis, $x \in A$, a contradiction. □

15.3 Morphisms

A **morphism** from a well-ordered structure $(X, <_1)$ into a well-ordered structure $(Y, <_2)$ is a map $f : X \longrightarrow Y$ such that for all x, $x' \in X$, $x <_1 x'$ if and only if $f(x) <_2 f(x')$. Note that any morphism from a well-ordered set into another must be a one to one map, because if $f(x) = f(x')$ we can neither have $x < x'$ nor $x' < x$. A morphism which is also onto is called an **isomorphism** of well-ordered sets. An isomorphism from a well-ordered set into itself is called an **automorphism**, but as we will soon see in this subsection a well-ordered set has a unique automorphism, only the identity. It follows that there is at most one isomorphism from a well-ordered set onto another, because if ϕ and ψ are two such isomorphisms then $\psi^{-1} \circ \phi$ is an automorphism, therefore by the result that we have stated $\psi^{-1} \circ \phi = \mathrm{Id}$, i.e. $\phi = \psi$.

If two well-ordered sets X and Y are isomorphic, then we write $X \simeq Y$. This is an equivalence relation on the **class** of all well-ordered sets.

Theorem 15.3.1 *A well-ordered set has a unique automorphism, namely the identity.*

Proof: Let $(X, <)$ be a well-ordered structure. Let $\phi : X \longrightarrow X$ be an automorphism. Let $A = \{a \in X : \phi(a) = a\}$. We will use Theorem 15.2.1. Let $x \in X$ and assume that $(-\infty, x) \subseteq A$. We proceed to show that $x \in A$. This will prove the theorem. By assumption, if $a \in X$ and $a < x$, then $\phi(a) = a$. It follows that (since ϕ is one to one), $\phi(x) \geq x$. Assume $\phi(x) > x$. Let $y \in X$ be such that $\phi(y) = x$. Then, since $\phi(y) = x < \phi(x)$, $y < x$. Hence $x = \phi(y) = y$, a contradiction. □

Now we show that given any two well-ordered sets, there is an embedding of one into another. We will show more, we will show that given any two well-ordered sets, there is a unique isomorphism of one of the two onto an initial segment of the other. For example, the set $2\mathbb{N}$ of even natural numbers, as a subset of $\mathbb{N}$, is a well-ordered set and the map $2n \mapsto n$ is an embedding of $2\mathbb{N}$ onto an initial segment of $\mathbb{N}$ (onto $\mathbb{N}$ in fact).

We first need the following result which is a generalization of Theorem 15.3.1, whose proof is in fact very similar.

Lemma 15.3.2 *Let X be a well-ordered set and A an initial segment of X. Then the only embedding of A onto an initial segment of X is the identity map on A.*

Proof: Let B be an initial segment of X. It is easy to show that either $A \subseteq B$ or $B \subseteq A$. Assume that there is an embedding f of A onto B. We will show that $A = B$ and that $f = \mathrm{Id}_A$. If $B \subseteq A$, we may switch the roles of A and B and replace f by f^{-1} if necessary to assume that $A \subseteq B = X$. Thus we assume that there is an isomorphism from A onto X. We proceed to show that $A = X$. Let $A_1 = \{a \in A.f(a) = a\}$. If $A_1 = A$ then we are done. Otherwise, let x be the least element of $A \setminus A_1$. If $f(x) < x$, then $f(x) \in A_1$, so $f(f(x)) = f(x)$ and

$f(x) = x$, a contradiction. Thus $f(x) > x$. Let $y \in A$ be such that $f(y) = x$. Then $f(y) = x < f(x)$ and so $y < x$, implying $y \in A_1$. But then $x = f(y) = y$, a contradiction again. □

Theorem 15.3.3 *Given any two well-ordered sets, there is a unique embedding of one into an initial segment of the other.*

Proof: Uniqueness follows from Lemma 15.3.2. We will show the existence.

Let $(X, <)$ and $(Y, <)$ be two well-ordered sets. Consider the set $\Im$ of all initial segments of X that embed into an initial segment of Y. If $A \in \Im$, let f_A be the unique embedding of A into Y. Note that if A, $B \in \Im$, then one of A or B is a subset of the other and if $A \subseteq B$, then f_B is an extension of f_A. By Example vii, page 38, $f := \cup_{A \in \Im} f_A$ is a function from $Z := \cup_{A \in \Im} A$ into Y. It is easy to show that Z is an initial segment of X and that f is an embedding of Z onto an initial segment of Y. Thus Z is a maximal element of $\Im$. If $Z = X$ then there is nothing more to do. If $f(Z) = Y$ then f^{-1} is an embedding of Y onto the initial segment Z of X. Assume $Z \neq X$ and $f(Z) \neq Y$. Let x and y be the least elements of $X \setminus Z$ and $Y \setminus f(Z)$ respectively. We can extend f to $Z \cup \{x\}$ by sending x to y, we then obtain an embedding of the initial segment $Z \cup \{x\}$ onto the initial segment $f(Z) \cup \{y\}$. Thus $Z \cup \{x\} \in \Im$. But this contradicts the fact that Z is a maximal element of $\Im$. □

Exercises.

i. Show that $n + \mathbb{N} \simeq \mathbb{N}$ for all $n \in \mathbb{N}$.

ii. Show that $n \times \mathbb{N} \simeq \mathbb{N}$ for all $n \in \mathbb{N}$.

iii. Show that $\mathbb{N} \times n \not\simeq \mathbb{N}$ for all $0 \neq n \in \mathbb{N}$.

iv. Let n, $m \in \mathbb{N}$. Show that $\mathbb{N} + n \simeq \mathbb{N} + m$ if and only if $n = m$.

v. Let n, $m \in \mathbb{N}$. Show that $\mathbb{N} \times n \simeq \mathbb{N} \times m$ if and only if $n = m$.

vi. Show that for n, $m \in \mathbb{N}$, the meaning of $n + m$ as a well-ordered set coincides with the old notion $n + m$ that we have defined.

vii. Show that $\mathbb{N} \times \mathbb{N} \not\simeq \mathbb{N}$.

viii. Show that $A + (B + C) \simeq (A + B) + C$ for all well-ordered sets A, B, C.

ix. Show that $A \times (B \times C) \simeq (A \times B) \times C$ for all well-ordered sets A, B, C.

Chapter 16

Ordinals

16.1 Definition

An **ordinal** is a well-ordered set X such that for all $x \in X$, $(-\infty, x) = x$. Thus, if α is an ordinal and x, $y \in \alpha$, $y < x$ if and only if $y \in x$. Therefore an ordinal is well-ordered by the membership relation $\in$. But this condition is not enough to make a set an ordinal. (See examples below).

Note that in an ordinal α, if $x \in \alpha$, then $x = (-\infty, x) \subseteq \alpha$, i.e. any element of an ordinal is a subset of the ordinal.

Examples.

i. The set $\mathbb{N}$ is an ordinal. When considered as an ordinal, it is customary to denote $\mathbb{N}$ by ω.

ii. An initial segment of an ordinal is an ordinal. Thus each natural number is an ordinal. On the other hand $\{0, 1, 3\}$ is not an ordinal, although it is well ordered by the membership relation.

iii. If α is an ordinal, then $\alpha^+ := \alpha \cup \{\alpha\}$ is also an ordinal.

Let $\alpha \neq \emptyset = 0$ be an ordinal and x its least element. We then have: $x = (-\infty, x) = \emptyset = 0$. Thus 0 is the least element of any ordinal $\neq 0$.

Assume $\alpha \neq \{0\} = 1$. Let x be the least element of $\alpha \setminus \{0\}$. Then $x = (-\infty, x) = \{0\} = 1$. Thus any ordinal that has at least two elements contain 0 and 1 as elements.

Theorem 16.1.1 *If $\alpha\, \beta$ are ordinals then either $\alpha < \beta$ or $\alpha = \beta$ or $\beta < \alpha$.*

Proof: Assume not. Consider $\alpha \cap \beta$. This is an initial segment of both α and β. Let a and b be the least elements of $\alpha \setminus (\alpha \cap \beta)$ and $\beta \setminus (\alpha \cap \beta)$ respectively. Then $a = (-infty, a) = \alpha \cap \beta$ and similarly $b = (-infty, b) = \alpha \cap \beta$. Thus $a = b \in \alpha \cap \beta$, a contradiction. □

Corollary 16.1.2 *A subset of an ordinal is an ordinal if and only if it is an initial segment of that ordinal.*

Corollary 16.1.3 *A proper subset of an ordinal is an ordinal if and only if it is an element of that ordinal.*

Corollary 16.1.4 *Two isomorphic ordinals are equal.*

Proof: Let α and β be two isomorphic ordinals. By Theorem 16.1.1, we may assume that $\alpha < \beta$. Let $f : \alpha \longrightarrow \beta$ be the isomorphism. By Theorem 15.3.3, $f = \mathrm{Id}_\alpha$. So $\alpha = \beta$. □

Exercises.

i. Show that every element of an ordinal is an ordinal.

ii. Let α be an ordinal and $\beta \in \alpha$. Show that either $\beta^+ \in \alpha$ or $\beta^+ = \alpha$.

iii. Show that the union of a set of ordinals is an ordinal.

iv. An ordinal that has no last element is called a **limit ordinal**. Find the set of limit ordinals of ω, $\omega + \omega$ and $\omega \times \omega$.

16.2 Axiom of Replacement

We will prove in the next subsection that any well-ordered set is isomorphic to an ordinal. For this we need the following axiom (which is considered to be dangerous by some prominent set theorists).

Axiom of Replacement. *If X is set and $\phi(x, y)$ is a formula such that for all $x \in X$ there is a unique set y such that $\phi(x, y)$, then there is a set Y whose elements are exactly those sets y such that $\phi(x, y)$ for some $x \in X$.*

It is aesthetically best not to use the Axiom of Replacement if one can do otherwise.

16.3 Classification of Well-Ordered Sets

Theorem 16.3.1 *Every well-ordered set is isomorphic to a unique ordinal.*

Proof: Uniqueness follows from Corollary 16.1.4. We will show the existence of an isomorphism. Let X be a well-ordered set. Consider the set $\Im$ of initial segments of X which are isomorphic to an ordinal. Thus for each $A \in \Im$, there is an ordinal α_A and an isomorphism $f_A : A \longrightarrow \alpha_A$. By Theorem 16.1.4, the ordinal α is unique. By Theorem 15.3.3, the isomorphism f_A is unique.

Let $A, B \in \Im$. Either $A \subseteq B$ or $B \subseteq A$. Assume $A \subseteq B$. Also either $\alpha_A \subseteq \alpha_B$ or $\alpha_B \subseteq \alpha_A$. Assume $\alpha_B \subseteq \alpha_A$. Then $f_A^{-1} \circ f_B$ is an isomorphism

from B into an initial segment A. Thus $A = B$. Therefore we may assume that $\alpha_A \subseteq \alpha_B$.

Suppose for a moment that $\{\alpha_A : A \in \Im\}$ is a set. Then $\cup_{A\in\Im}\alpha_A$ is an ordinal and we may consider the map $f := \cup_{A\in\Im} f_A$ from the initial segment $Y := \cup_{A\in\Im} A$ of X onto the ordinal $\alpha := \cup_{A\in\Im}\alpha_A$. It is easy to check that this is an isomorphism. Thus $Y \in \Im$ and is the unique maximal element of $\Im$. If $Y = X$ then we are done. Otherwise, consider the least element y of $X \setminus Y$ and extend f to an isomorphism from $Y \cup \{y\}$ onto the ordinal α^+, contradicting the maximality of Y.

Thus, it remains to show that $\{\alpha_A : A \in \Im\}$ is a set. This is a direct consequence of the Axiom of Replacement. □

16.4 Addition of Ordinals

If α and β are ordinals, then the well-ordered set $\alpha + \beta$ is a well-ordered set, and by Theorem 16.3.1 $\alpha + \beta$ is isomorphic to a unique ordinal. Changing our previous notation, we will denote this unique ordinal by $\alpha + \beta$.

16.5 Multiplication of Ordinals

If α and β are ordinals, then the well-ordered set $\alpha \times \beta$ is a well-ordered set, and by Theorem 16.3.1 $\alpha \times \beta$ is isomorphic to a unique ordinal. Changing our previous notation, we will denote this unique ordinal by $\alpha \times \beta$.

Paradox of Burali-Forti

Chapter 17

Cardinals

A **cardinal** is an ordinal that is not in bijection with one of its elements. For example ω and each natural number is a cardinal.

17.1 Addition of Cardinals

17.2 Multiplication of Cardinals

17.3 Problems

i. Let X be a set. A set Σ of subsets of X is called a **σ-algebra** if Σ is closed under finite or countable unions and intersections and complementation. Show that a σ-algebra Σ is either finite or countable. (**Solution:** Assume not. For $x \in \cup\Sigma$, let $A(x) = \cap\{U \in \Sigma : x \in U\}$. Then $A(x) \cap A(y) \neq \emptyset$ if and only if $A(x) = A(y)$. Every element of Σ is a countable union of these disjoint $A(x)$'s).

17.4 Final Exam of Math 112, May 2003

You should do at least one of Ic, IId and III.

I. Automorphisms of $(\mathbb{Q}, <)$.

Ia) Let $a, b \in \mathbb{Q}$, $a > 0$. Let $f_{a,b} : \mathbb{Q} \longrightarrow \mathbb{Q}$ be defined by $f_{a,b}(x) = ax + b$. Show that $f_{a,b}$ is an order preserving bijection.

Ib) Let $a, b \in \mathbb{Q}$ with $a < b$ and $k \in \mathbb{Z}$. Show that there is an order preserving bijection between the rational intervals $[k, k+1] \cap \mathbb{Q}$ and $[a, b] \cap \mathbb{Q}$.

Ic) Show that there are uncountably many order preserving bijections of $\mathbb{Q}$.

II. Automorphisms of $(R, +, \times)$.

IIa) Show that any additive map f from $\mathbb{Z}$ into $\mathbb{R}$ is given by $f(x) = rx$ for some $r \in \mathbb{R}$.

IIb) Show that any additive map f from $\mathbb{Q}$ into $\mathbb{R}$ is given by $f(x) = rx$ for some $r \in \mathbb{R}$.

IIc) Show that the only additive and multiplicative map f from $\mathbb{Q}$ into $\mathbb{Q}$ is $\mathrm{Id}_{\mathbb{Q}}$.

IId) Show that the only additive and multiplicative map f from $\mathbb{R}$ into $\mathbb{R}$ is Id_R.

III. Uniqueness of the Real Number System. For $i = 1, 2$, let $(R_i, +_i, \times_i, 0_i, 1_i)$ be two structures satisfying the axioms of real numbers (ordered complete field). Show that there is a unique bijection $f : R_1 \longrightarrow R_2$ such that

i. $f(x +_1 y) = f(x) +_2 f(y)$

ii. $f(x \times_1 y) = f(x) \times_2 f(y)$.

Chapter 18

Axiom of Choice and Zorn's Lemma

Axiom of Choice. *Any set that does not contain $\emptyset$ has a choice function.*

18.1 Zorn's Lemma

Theorem 18.1.1 *Any nonempty inductive set has a maximal element.*

Proof: Let A be a nonempty inductive set. Let X be the set of chains of A ordered with inclusion. It is easy to show that a maximal element of X gives rise to a maximal element of A.

We note the following:

i. X is a set of subsets of A.

ii. Any subset of an element of X is also in X.

iii. The union of a chain of elements from X is also in X.

Let f be a choice function for $\Im(A) \setminus \{\emptyset\}$.

For $x \in X$, let $\hat{x} = \{a \in A : x \cup \{a\} \in X\}$. Clearly $x \subseteq \hat{x}$.

Define $g : X \longrightarrow X$ by $g(x) = x$ if $x = \hat{x}$ and $g(x) = x \cup \{f(\hat{x} \setminus x)\}$.

We will show that g has a fixed point.

We will say that a subset T of X is a tower, if

T1. $\emptyset \in T$.

T2. If $x \in T$ then $g(x) \in T$.

T3. If $S \subseteq T$ and if S is a chain, then $\cup S \in T$.

Clearly X is a tower and the intersection of towers is a tower. Thus there is a smallest tower, say $T_\circ$.

We will show that $T_\circ$ is a chain. From this it follows easily that $g(x_\circ) = x_\circ$ if $x_\circ = \cup T_\circ$.

So let us show that $T_\circ$ is a chain.

We say that $x \in T_\circ$ is comparable if x is comparable with any element of T. Clearly $\emptyset$ is comparable. Clearly the set of comparable elements of $T_\circ$

form a chain. We will show that the set of comparable elements form a tower. We already have noticed T1. T3 is easy as well. Let us show T2. Let x be comparable. If $y \subseteq x$, since x and $g(y)$ are comparable, $g(y) \subseteq x$. Let $U := \{y \in T_\circ :$ either $y \subseteq x$ or $g(x) \subseteq y$. Then U is a tower. So $U = T_\circ$. It follows that $g(x)$ is also is comparable. This proves the theorem. □

18.2 Some Consequences of Zorn's Lemma

18.2.1 Finite and Infinite Sets

18.2.2 König's Lemma

A **tree** is a poset T such that for every $t \in T$, $\{s : s < t\}$ is a well-ordered set. An element of a tree is called a **node** or a **vertex**. Thus in a tree there are least elements and every vertex of a tree is either an end point or it has at least one immediate successor. A **branch** is a linearly ordered subset of a tree. A tree is called **finitely branching** if every node has finitely many immediate successors.

Lemma 18.2.1 (König's Lemma) *Every infinite finitely branching tree with a unique least element has an infinite branch.*

Proof: Let T be such a tree. For $n \in \omega$, consider the set $T(n)$ of elements t of T such that $\{s \in T : s < t\}$ has cardinality $n-1$. Since T is finitely branching, $T(n)$ is finite for all n. An **initial subtree** of a tree T is subset S of T such that for $s \in S$, $\{t \in T : t < s\} \subseteq S$. Consider the set Z of all infinite initial subtrees of T. Since $T \in Z$, $Z \neq \emptyset$. Order Z by reversing the inclusion order, i.e. for S_1, $S_2 \in Z$, define $S_1 < S_2$ if $S_2 \subset S_1$. We claim that Z is an inductive set. More precisely, we claim that if $(S_i)_{i\in I}$ is a chain from Z, then $\cap_{i\in I} S_i \in Z$.

We first show that $\cap_{i\in I} S_i$ is an initial subtree. Let $s \in \cap_{i\in I} S_i$ and let $t \in T$ be such that $t < s$. Then $t \in S_i$ for all $i \in I$. Hence $t \in \cap_{i\in I} S_i$.

We next show that $\cap_{i\in I} S_i$ is infinite. Assume otherwise. Then $\cap_{i\in I} S_i \subseteq T(n)$ for some $n \in \omega$. For each $t \in T(n+1)$, since $t \notin \cap_{i\in I} S_i$ there is an $i(t) \in I$ such that $t \notin S_{i(t)}$. Let $i = \max\{i(t) : t \in T(n+1)\}$. Then $T(n+1) \cap S(i) = \emptyset$. But then $S(i) \subseteq T(n)$ and $S(i)$ is finite, a contradiction.

By Zorn's Lemma Z has a maximal element, say S. Thus S is a minimal infinite initial tree. We claim that S is a branch. Assume otherwise. Then S has two incomparable elements t_1 and t_2. Deleting one of the t_i and elements above it, we get an infinite proper initial subtree of S, a contradiction. □

18.2.3 Some Unexpected Consequences of Zorn's Lemma

Chapter 19

Axioms of Set Theory – ZFC

Chapter 20

$V = L$

Chapter 21

Continuum Hypothesis

Chapter 22

Banach-Tarski Paradox

Let S^2 be the unit ball in $\mathbb{R}^3$. By partitioning S^2 and applying translations and rotations, we will duplicate S^2.

Let G be a group acting on a set X. A subset E of X is called **G-paradoxical** if there are pairwise disjoint subsets $A_1, \ldots, A_n$, $B_1, \ldots, B_m$ of E and $g_1, \ldots, g_n$, $h_1, \ldots, h_m \in G$ such that $E = \cup_i g_i(A_i) = \cup_i h_j(B_j)$.

Proposition 22.0.2 *S^1 is countably $\mathrm{SO}_2(\mathbb{R})$-paradoxical.*

Proof: Let G be the subgroup formed by the rational multiples of 2π. Let $G = \{\rho_i : i \in \mathbb{N}\}$. Let H be a set of representatives of $SO_2(\mathbb{R})/G$. Let $A = H(1,0)$ and $A_i = \rho_i(A)$. The family $(A_i)_i$ is a countable partition of S^1. Then $(A_{2i})_i$ and (A_{2i+1}) are such that $S^1 = \cup_i g_{2i}(A_{2i}) = \cup_i g_{2i+1}(A_{2i+1})$ where g_{2i} takes A_{2i} onto A_i and g_{2i+1} takes A_{2i+1} onto A_i. □

Let G act on a set X. Let $A, B \subseteq X$. We say that A and B are **G-equidecomposable** if there are finite partitions of $A = \sqcup_{i=1}^n A_i$ and $B = \sqcup_{i=1}^n B_n$ and $g_1, \ldots, g_n \in G$ such that $g_i(A_i) = B_i$. This is an equivalence relation.

Lemma 22.0.3 *If $A \sim_G B$ and if A is G-paradoxical, then B is G-paradoxical.*

Proof: Easy. □

Lemma 22.0.4 *S^1 is $\mathrm{SO}_2(\mathbb{R})$-equidecomposable with $S^1 \setminus \{$one point$\}$.*

Proof: Let $A = \{e^{in} : n \in \mathbb{N} \setminus \{0\}\}$. We have $S^1 \setminus \{1\} = (S^1 \setminus (A \cup \{1\})) \sqcup A \sim (S^1 \setminus A) \sqcup (A \cup \{1\}) = S^1$. □

A group G is called **paradoxical** if G acting on itself by left multiplication is G-paradoxical.

Lemma 22.0.5 *The free group F on two generators is paradoxical.*

Proof: Let a be b be the generators of F. Let

$$B(\sigma) = \{\text{words starting with } \sigma\},$$

where $\sigma = a,\ b,\ a^{-1},\ b^{-1}$. So

$$F = \{1\} \sqcup B(a) \sqcup B(b) \sqcup B(a^{-1}) \sqcup B(b^{-1}).$$

But also $F = a^{-1}B(a) = a^{-1}B(a) \sqcap B(a)$ and $F = b^{-1}B(b) = b^{-1}B(b) \sqcap B(b)$. □

Lemma 22.0.6 *Let G be a paradoxical group acting freely on X. Then X is G-paradoxical.*

Proof: Let $A_1, \ldots, A_n,\ B_1, \ldots, B_m \subseteq G$ be disjoint and $g_1, \ldots, g_n,\ h_1, \ldots, h_m \in G$ such that $G = \cup_i g_i A_i = \cup_i h_j B_j$. Let M be a choice set in the set of G-orbits. Now $(gM)_{g\in G}$ partitions X because the action is free. Let $A_i' = \cup_{g\in A_i} g(M)$ and $B_j' = \cup_{g\in B_j} g(M)$. These are all pairwise disjoint. We have $X = \cup_i g_i(A_i') = \cup_j h_j(B_j')$ because $G = \cup_i g_i A_i = \cup_i h_j B_j$. □

Corollary 22.0.7 *If a group G contains a paradoxical subgroup H then G is paradoxical.*

Proof: Note that the action of H on G is free. So G is H-paradoxical by the previous lemma. So G is G-paradoxical. □

Corollary 22.0.8 *Any group containing a free subgroup of rank 2 is paradoxical.*

Fact 22.0.9 $\mathrm{SO}_3(\mathbb{R})$ *contains a free subgroup of rank 2. Thus* $\mathrm{SO}_3(\mathbb{R})$ *is paradoxical.*

Let $G \leq \mathrm{SO}_3(\mathbb{R})$ be free on two generators. Let D be the set of points on S^2 which are fixed by some $g \in G \setminus \{g\}$. Then D is countable. Let G act on $S^2 \setminus D$. Thus $S^2 \setminus D$ is paradoxical. We will show that $S^2 \setminus D$ is $\mathrm{SO}_3(\mathbb{R})$-equidecomposable with S^2. Choose an axis of rotation not passing through an element of D. Consider the set of all rotations around this axis for which some integer power of it sends an element of D to another point of D. This set is countable. Pick a rotation ρ not in this set. Then $\rho^n(D) \cap \rho^m(D) = \emptyset$ for $n \neq m$. Let $A = \cup_{n=1}^{\infty} \rho^n(D)$ and $B = S^2 \setminus (A \cup D)$. We have $S^2 \setminus D = A \sqcup B \sim B \cup \rho^{-1}(A) = S^2$.

Thus S^2 is $SO_3(\mathbb{R})$-paradoxical.

Chapter 23

First Order Structures

Chapter 24

Ultraproducts and Ultrafilters

24.1 Nonstandard Models of $\mathbb{N}$

24.2 Nonstandard Models of $\mathbb{R}$

Chapter 25

Dimension Theory

Chapter 26

Exams

26.1 First Semester Midterm, November 2002

i. a) *Given a set X, define $\cup X$ as follows:*

$$y \in \cup X \text{ if and only if there is an } x \in X \text{ such that } y \in x.$$

Show that $\cup\emptyset = \emptyset$. (3 pts.)

Proof: Set $X = \emptyset$ in the definition. Thus

$$y \in \cup\emptyset \text{ if and only if there is an } x \in \emptyset \text{ such that } y \in x.$$

Since there is no $x \in \emptyset$, we see that $\cup\emptyset = \emptyset$.

b) *Given a set X, define $\cap_1 X$ and $\cap_2 X$ as follows:*

$$\begin{array}{lll} y \in \cap_1 X & \text{if and only if} & y \in x \text{ for all } x \in X \\ y \in \cap_2 X & \text{if and only if} & y \in \cup X \text{ and } y \in x \text{ for all } x \in X \end{array}$$

Is $\cap_1 X = \cap_2 X$ for all X? Which definition do you prefer for $\cap X$ and why? (5 pts.)

Answer: Certainly $\cap_2 X \subseteq \cap_1 X$ because $\cap_2 X = (\cap_1 X) \cap (\cup X)$ by definition.

The reverse inclusion holds only if $X \neq \emptyset$. Indeed, assume $X \neq \emptyset$ and let $y \in \cap_1 X$. To show that $y \in \cap_2 X$, we need to show that $y \in \cup X$, i.e. that $y \in x$ for some $x \in X$. Since $X \neq \emptyset$ and $y \in \cap_1 X$, this holds trivially, i.e. $y \in x$ for some $x \in X$.

The reverse inclusion does not hold if $X = \emptyset$. Indeed, $\cap_2\emptyset = (\cap_1\emptyset)\cap(\cup\emptyset) = (\cap_1\emptyset) \cap \emptyset = \emptyset$. On the other hand,

$$y \in \cap_1\emptyset \text{ if and only if } y \in x \text{ for all } x \in \emptyset$$

and this condition holds for all y. Hence $\cap_1\emptyset$ is the whole universe and is not even a set.

Thus we should prefer $\cap_2 X$ for the definition of $\cap X$ since the outcome would then be a set for any set X, even for $X = \emptyset$!

ii. *Find a set X such that $X \cap \wp(X) \neq \emptyset$.* (3 pts.)

Answer. Since $\emptyset \in \wp(X)$ for any X, any set X that contains $\emptyset$ as element would do, e.g. we may take $X = \{\emptyset\}$.

iii. *Let $(A_i)_{i\in I}$ be a family of sets.*

a) *Show that $\bigcap_{i\in I} \wp(A_i) = \wp(\bigcap_{i\in I} A_i)$.* (3 pts.)

Proof:

$$\begin{array}{lll} X \in \bigcap_{i\in I} \wp(A_i) & \text{if and only if} & X \in \wp(A_i) \text{ for all } i \in I \\ & \text{if and only if} & X \subseteq A_i \text{ for all } i \in I \\ & \text{if and only if} & X \subseteq \bigcap_{i\in I} A_i \\ & \text{if and only if} & X \in \wp(\bigcap_{i\in I} A_i) \end{array}$$

b) *What is the relationship between $\bigcup_{i\in I} \wp(A_i)$ and $\wp(\bigcup_{i\in I} A_i)$?* (4 pts.)

Answer: We have $\bigcup_{i\in I} \wp(A_i) \subseteq \wp(\bigcup_{i\in I} A_i)$. Indeed,

$$\begin{array}{lll} X \in \bigcup_{i\in I} \wp(A_i) & \text{if and only if} & X \in \wp(A_i) \text{ for some } i \in I \\ & \text{if and only if} & X \subseteq A_i \text{ for some } i \in I \\ & \text{implies} & X \subseteq \cup_{i\in I} A_i \\ & \text{if and only if} & X \in \wp(\cup_{i\in I} A_i) \end{array}$$

The reverse inclusion is false, in fact if one of the sets A_i does not contain all the others, then $\cup_{i\in I} A_i \in \wp(\cup_{i\in I} A_i) \setminus \bigcup_{i\in I} \wp(A_i)$.

iv. *What is the set $(X \times Y) \cap (Y \times X)$?* (3 pts.)

Answer: Let $(u, v) \in (X \times Y) \cap (Y \times X)$. Since $(u, v) \in X \times Y$, u is an element of X and v is an element of Y. Similarly, since $(u, v) \in Y \times X$, u is an element of Y and v is an element of X. Thus both u and v are elements of $X \cap Y$, i.e. $(u, v) \in (X \cap Y) \times (X \cap Y)$.

The reverse inclusion $(X \cap Y) \times (X \cap Y) \subseteq (X \times Y) \cap (Y \times X)$ is trivial.

v. *Let α be a set such that $x \subseteq \alpha$ for all $x \in \alpha$. Show that $\alpha \cup \{\alpha\}$ has the same property. Give four examples of such sets.* (4 pts.)

Proof: Let $x \in \alpha \cup \{\alpha\}$. Then either $x \in \alpha$ or $x \in \{\alpha\}$.

If $x \in \alpha$, then by assumption $x \subseteq \alpha$. Since $\alpha \subseteq \alpha \cup \{\alpha\}$, in this case we get $x \subseteq \alpha \cup \{\alpha\}$.

If $x \in \{\alpha\}$, then $x = \alpha$, and so $x = \alpha \subseteq \alpha \cup \{\alpha\}$.

Since $\emptyset$ has the property stated, starting from $\emptyset$, we can get as many examples as we wish to, here are the first four:

$$\begin{aligned}\emptyset &= 0\\ 0 \cup \{0\} &= 1\\ 1 \cup \{1\} &= 2\\ 2 \cup \{2\} &= 3\end{aligned}$$

vi. *Let Γ be a graph such that for any vertices α, α_1, β, β_1, if $\alpha \neq \alpha_1$ and $\beta \neq \beta_1$, then there is a $\phi \in \mathrm{Aut}(\Gamma)$ such that $\phi(\alpha) = \beta$ and $\phi(\alpha_1) = \beta_1$. What can you say about Γ?* (5 pts.)

Answer: Then either the graph is the complete graph (all possible edges exist) or the graph without edges at all. Indeed, otherwise we may find α, α_1 and $\beta \neq \beta_1$ such that α and α_1 are connected (hence $\alpha \neq \alpha_1$) and β and β_1 are not connected, but then it is impossible to send the connected pair (α, α_1) to the nonconnected pair (β, β_1).

vii. *Let $\phi : \mathbb{R} \longrightarrow \mathbb{R}$ be a* **one to one** *map such that $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(x^2) = \phi(x)^2$ for all x, $y \in \mathbb{R}$. Show that $\phi(xy) = \phi(x)\phi(y)$ for all x, $y \in \mathbb{R}$ and $\phi(q) = q$ for all $q \in \mathbb{Q}$.* (10 pts.)

Proof: For any $x, y \in \mathbb{R}$, we have $\phi(x)^2 + 2\phi(x)\phi(y) + \phi(y)^2 = (\phi(x) + \phi(y))^2 = \phi(x + y)^2 = \phi((x + y)^2) = \phi(x^2 + 2xy + y^2) = \phi(x^2) + 2\phi(xy) + \phi(y^2) = \phi(x)^2 + 2\phi(xy) + \phi(y)^2$ and so $2\phi(x)\phi(y) = 2\phi(xy)$ and simplifying, we get $\phi(x)\phi(y) = \phi(xy)$. This proves the first part.

Since $\phi(0) = \phi(0 + 0) = \phi(0) + \phi(0)$, we must have $\phi(0) = 0$.

Since $\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$, we must have $\phi(1) = 0$ or $\phi(1) = 1$. But the first case is forbidden because ϕ is one to one and $\phi(0) = 0$ already. Hence $\phi(1) = 1$.

Now, it follows easily by induction that $\phi(n) = n$ for all $n \in \mathbb{N}$ because $\phi(n+1) = \phi(n) + \phi(1) = \phi(n) + 1 = n + 1$ (the last equality is the inductive hypothesis).

Also, for $n \in \mathbb{N}$, we have $0 = \phi(0) = \phi(n + (-n)) = \phi(n) + \phi(-n)$ and so $\phi(-n) = -\phi(n) = -n$. Thus $\phi(n) = n$ for all $n \in \mathbb{Z}$.

Now if $q \in \mathbb{Q}$, then $q = n/m$ some n, $m \in \mathbb{Z}$ and $m \neq 0$. Then we have $n = \phi(n) = \phi(mn/m) = \phi(m)\phi(n/m) = m\phi(n/m)$ and so $\phi(n/m) = n/m$, i.e. $\phi(q) = q$.

viii. *Given a set X, define $\wp^n(X)$ as follows by induction on n: $\wp^0(X) = X$ and $\wp^{n+1}(X) = \wp(\wp^n(X))$.*

a) *Is there a natural number n such that for any set X, $\{\{\emptyset\}, \{\{X\}\}\} \in \wp^n(X)$?* (8 pts.)

Answer: For $n \geq 4$ note the equivalence of the following propositions:

$$\{\{\emptyset\}, \{\{X\}\}\} \in \wp^n(X)$$
$$\{\{\emptyset\}, \{\{X\}\}\} \subseteq \wp^{n-1}(X)$$
$$\{\emptyset\}, \{\{X\}\} \in \wp^{n-1}(X)$$
$$\{\emptyset\}, \{\{X\}\} \subseteq \wp^{n-2}(X)$$
$$\emptyset, \{X\} \in \wp^{n-2}(X)$$
$$\emptyset \in \wp^{n-2}(X) \text{ and } \{X\} \subseteq \wp^{n-3}(X)$$
$$\{X\} \subseteq \wp^{n-3}(X)$$
$$\{X\} \subseteq \wp^{n-3}(X)$$
$$X \in \wp^{n-3}(X)$$
$$X \subseteq \wp^{n-4}(X)$$

If $n = 4$, the last condition holds for all X.

Does it hold for $n = 5$, i.e. do we have $X \subseteq \wp(X)$ for all X? For this condition to hold, we need any element of X to be a subset of X, and this does not always hold. For any $i \geq 1$, one can find a set X such that $X \not\subseteq \wp^i(X)$. Thus the condition does not hold for any $n \geq 5$ (details are left as an exercise).

For $n = 0, 1, 2, 3$, find examples of X such that $\{\{\emptyset\}, \{\{X\}\}\} \notin \wp^n(X)$.

b) *Show that* $\wp(\wp^n(X)) = \wp^n(\wp(X))$ *for all sets* X *and all natural numbers* n. (8 pts.)

Proof: We proceed by induction on n. The condition certainly holds for $n = 0$. Assume it holds for n. We have $\wp(\wp^{n+1}(X)) = \wp(\wp^n(\wp(X))) = \wp^{n+1}(\wp(X))$.

c) Show that $\wp^n(\wp^m(X)) = \wp^m(\wp^n(X))$ for all sets X and all natural numbers n and m. (8 pts.)

Proof: We proceed by induction on m. The condition certainly holds for $m = 0$. By part (b) it also holds for $m = 1$. Assume it holds for m. We have $\wp^n(\wp^{m+1}(X)) = \wp^n(\wp(\wp^m(X))) = \wp(\wp^n(\wp(X)) = \wp^{n+1}(\wp^m(X))$.

ix. *Define a partial order* $\prec$ *on* $\mathbb{N}\backslash\{0, 1\}$ *by* $x \prec y$ *if and only if* $x^2|y$. *Describe all the automorphisms of this poset.* (5 pts.)

Answer: The minimal elements of this ordered set (call it Γ) are the square free numbers. Thus any automorphism of Γ should send the square free numbers onto the square free numbers. But the prime numbers have a privilege. Indeed if p is a prime number, then p has an immediate successor (namely p^2) that has only one predecessor, namely p. Thus any automorphism should be multiplicative and be given by a permutation of primes.

x. *Let* X *be a set. Let* Γ *be the set of subsets of* X *with two elements. On* Γ *define the relation* $\alpha R \beta$ *if and only if* $\alpha \cap \beta = \emptyset$. *Then* Γ *becomes a graph with this relation.*

a) *Calculate* $\mathrm{Aut}(\Gamma)$ *when* $|X| = 4$. (3 pts.)

Answer: The graph Γ is just six vertices joined two by two. A group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$ preserves the edges. And Sym(3) permutes the edges. Thus the group has $8 \times 3! = 48$ elements.

More formally, one can prove this as follows. Let the vertices be 1, 2, 3, 4, 5, 6 and the edges be $v_1 = (1,4)$, $v_2 = (2,5)$ and $v_3 = (3,6)$. We can embed Sym(3) in $\mathrm{Aut}(\Gamma) \leq \mathrm{Sym}(6)$ via

$$\begin{array}{lcl} \mathrm{Id}_3 & \mapsto & \mathrm{Id}_6 \\ (12) & \mapsto & (12)(45) \\ (13) & \mapsto & (13)(46) \\ (23) & \mapsto & (23)(56) \\ (123) & \mapsto & (123)(456) \\ (132) & \mapsto & (132)(465) \end{array}$$

For any $\phi \in \mathrm{Aut}(\Gamma)$ there is an element α in the image of Sym(3) such that $\alpha^{-1}\phi$ preserves the three edges $v_1 = (1,4)$, $v_2 = (2,5)$ and $v_3 = (3,6)$. Thus $\alpha^{-1}\phi \in \mathrm{Sym}\{1,4\} \times \mathrm{Sym}\{2,5\} \times \mathrm{Sym}\{3,6\} \simeq (\mathbb{Z}/2\mathbb{Z})^3$. It follows that $\mathrm{Aut}(\Gamma) \simeq (\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathrm{Sym}(3)$ (to be explained next year).

b) *Draw the graph* Γ *when* $X = \{1,2,3,4,5\}$. (3 pts.)

There are ten points. Draw two pentagons one inside the other. Label the outside points as $\{1,2\}$, $\{3,4\}$, $\{5,1\}$, $\{2,3\}$, $\{4,5\}$. Complete the graph.

c) *Show that* Sym(5) *imbeds in* $\mathrm{Aut}(\Gamma)$ *naturally. (You have to show that each element* σ *of* Sym(5) *gives rise to an automorphism* $\tilde{\sigma}$ *of* Γ *in such a way that the map* $\sigma \mapsto \tilde{\sigma}$ *is an injection from* Sym(5) *into* $\mathrm{Aut}(\Gamma)$ *and that* $\widetilde{\sigma_1 \circ \sigma_2} = \widetilde{\sigma_1} \circ \widetilde{\sigma_2}$*).* (8 pts.)

d) *Show that* $\mathrm{Aut}(\Gamma) \simeq \mathrm{Sym}(5)$. (12 pts.)

Proof of (c) and (d): Clearly any element of $\sigma \in \mathrm{Sym}(5)$ gives rise to an automorphism $\tilde{\sigma}$ of Γ via $\tilde{\sigma}\{a,b\} = \{\sigma(a), \sigma(b)\}$. The fact that this map preserves the incidence relation is clear. This map is one to one because if $\tilde{\sigma} = \tilde{\tau}$, then for all distinct a, b, c, we have

$$\begin{array}{rcl} \{\sigma(b)\} & = & \{\sigma(a),\sigma(b)\} \cap \{\sigma(b),\sigma(c)\} = \tilde{\sigma}\{a,b\} \cap \tilde{\sigma}\{b,c\} \\ & = & \tilde{\tau}\{a,b\} \cap \tilde{\tau}\{b,c\} = \{\tau(a),\tau(b)\} \cap \{\tau(b),\tau(c)\} = \{\tau(b)\}, \end{array}$$

and hence $\sigma(b) = \tau(b)$.

Let $\phi \in \mathrm{Aut}(\Gamma)$. We will compose ϕ by elements of Sym(5) to obtain the identity map. There is an $\sigma \in \mathrm{Sym}(5)$ such that $\phi\{1,2\} = \tilde{\sigma}\{1,2\}$ and $\phi\{3,4\} = \tilde{\sigma}\{3,4\}$. Thus, replacing ϕ by $\sigma^{-1}\phi$, we may assume that ϕ fixes the vertices $\{1,2\}$ and $\{3,4\}$. Now ϕ must preserve or exchange the vertices $\{3,5\}$ and $\{4,5\}$. By applying the element (34) of Sym(5) we may assume that these two vertices are fixed as well. Now ϕ must preserve or exchange the vertices $\{1,3\}$ and $\{2,3\}$. By applying the element (12) of Sym(5) we may assume that these two vertices are fixed as well. Now all the vertices must be fixed.

26.2 First Semester Final, January 2003

Axiom of Regularity (AR) states that every nonempty set A has an element x such that $A \cap x = \emptyset$. Throughout, we will accept the axiom of regularity. Let X be a set and $<$ be a total order on X. We say that $(X, <)$ is a **well-ordered set** (or that $<$ well-orders X) if every nonempty subset of X contains a minimal element for that order, i.e. if for every nonempty subset A of X, there is an $m \in A$ such that $m \leq a$ for all a in A. Clearly, given a well-ordered set A, such an m is unique. In particular every nonempty well-ordered set has a unique minimal element.

Note that $\emptyset$ is a well-ordered set.

Of course, subsets of a well-ordered set X inherit the well-order of X. If $(X, <)$ is an ordered set and $x \in X$, we define $i(x) = \{y \in X : y < x\}$ (the **initial segment** of x). If X is a set, we set $X^+ = X \cup \{X\}$. An **ordinal** is a well-ordered set such that $\beta = i(\beta)$ for all $\beta \in \alpha$.

i. Show that no set x is a member of itself. (3 pts.)

ii. Show that there are no sets x and y such that $x \in y$ and $y \in x$. (3 pts.)

iii. Show that $X \subset X^+$. (2 pts.)

iv. Assume X is a well-ordered set. Order X^+ by extending the order of X and stating that X is larger than its elements (i.e. put the element X to the very end of X). Show that X^+ is also a well-ordered set. (3 pts.)

v. (**Transfinite Induction**) Let $(X, <)$ be a well-ordered set and let $A \subseteq X$ be such that for all $x \in X$, if $i(x) \subseteq A$, then $x \in A$. Show that $A = X$. (5 pts.)

vi. Let X and Y be two well-ordered sets. Let $A = (X \times \{0\}) \cup (Y \times \{1\})$. Order A as follows:

$$\begin{array}{ll} (x_1, 0) < (x_2, 0) & \text{for all } x_1 \text{ and } x_2 \text{ in } X \text{ and } x_1 < x_2. \\ (y_1, 1) < (y_2, 1) & \text{for all } y_1 \text{ and } y_2 in Y \text{ and } y_1 < y_2. \\ (x, 0) < (y, 1) & \text{for all } x \in X \text{ and } y \in Y. \end{array}$$

Show that the above relation well-orders A. (4 pts.)

vii. Show that $\emptyset$ is an ordinal. (2 pts.)

viii. Show that an ordinal α is a set well-ordered by the relation $\in$, i.e. by the relation $<$ defined as follows: For all β, $\gamma \in \alpha$, $\beta < \gamma$ if and only if $\beta \in \gamma$.

Show that the converse of this statement is false. (3 pts.)

ix. Show that if $\alpha \neq \emptyset$ is an ordinal, then $\emptyset \in \alpha$ and $\emptyset$ is the least element of α. (7 pts.)

x. Show that if α is an ordinal and $\beta \in \alpha$, then $\beta \subset \alpha$. (2 pts.)

xi. Show that every element of an ordinal is an ordinal. (2 pts.)

xii. Show that if α is an ordinal, then α^+ is also an ordinal. (2 pts.)

xiii. Let α be an ordinal and $\beta \in \alpha$. Show that either $\beta^+ \in \alpha$ or $\beta^+ = \alpha$. (8 pts.)

xiv. In Question vi, take $X = \omega$ and $Y = 1 = \{0\}$. Show that the well-ordered set A obtained there is isomorphic to the ordinal ω^+, i.e. there is an order-preserving bijection from A onto ω^+. (4 pts.)

xv. In Exercise vi, take $X = 1 = \{0\}$ and $Y = \omega$. Show that the well-ordered set A obtained there is isomorphic to ω, i.e. there is an order-preserving bijection from A onto ω. (4 pts.)

xvi. Let $\alpha\,\beta$ be ordinals. Show that either $\alpha < \beta$ or $\alpha = \beta$ or $\beta < \alpha$. (20 pts.)

xvii. Show that the union of a set of ordinals is an ordinal. (3 pts.)

xviii. Let α and β be two ordinals. Let $f : \alpha \longrightarrow \beta$ be a strictly increasing function. Show that if f is onto, then $\alpha = \beta$ and f is the identity map. (20 pts.)

Axiom of Replacement says the following: If X is set and $\phi(x, y)$ is a formula such that for all $x \in X$ there is a unique set y such that $\phi(x, y)$, then there is a set Y whose elements are exactly those sets y such that $\phi(x, y)$ for some $x \in X$. You need this axiom for the next exercise.

xix. Show that every well-ordered set is isomorphic to an ordinal. (20 pts.)

26.3 First Semester, Resit, January 2004

Important Note. Write either in English or in Turkish, but in any event make full sentences. Use proper punctuation. Do not use symbols such as $\Leftrightarrow$, $\Rightarrow$, $\exists$, $\forall$. For each use of these symbols I will take away 1 pt. Explain all your answers, but grades will be taken away for unnecessary text. Any unexplained answer will get 0 point, whether the answer is correct or not.

I. Transitive Relations. Let X be a set. A **binary relation** on X is just a subset of $X \times X$.

A binary relation R on X is called **transitive** if, for all x, y, $z \in X$, $(x, y) \in R$ and $(y, z) \in R$ implies $(x, z) \in R$.

i. Which of the following a transitive binary relation on any set X? Explain. (0 or 4 pts.)

i. $X \times X$.

ii. $\emptyset$.

iii. $\{(x, x) : x \in X\}$.

iv. $\{(x, y) \in X^2 : x \neq y\}$.

Solution. The first three of them are always transitive. In the first one any two elements are related, so it is clearly transitive. The second one is transitive because no two elements are related. The third one is just the equality relation. Last one is not transitive because if $x \neq y$ are two distinct elements of X, then x and y are related and y and x are related, but x and x are not related.

ii. Which of the following a transitive binary relation on $\mathbb{N}$? Explain. (0 or 4 pts.)

i. $\{(x, y) \in \mathbb{N}^2 : 5 \text{ divides } x - y\}$.

ii. $\{(x, y) \in \mathbb{N}^2 : 5 \text{ divides } x + y\}$.

iii. $\{(x, y) \in \mathbb{N}^2 : 5 > x - y\}$.

iv. $\{(x, y) \in \mathbb{N}^2 : 12 < x - y\}$.

Solution. Only the first one is transitive.

iii. Show that the intersection of a set of transitive relations on X is a transitive relation on X. (4 pts.)

Solution. Let $(R_i)_i$ be a family of transitive relations. Let (x, y), $(y, z) \in \cap_i R_i$. Then (x, y), $(y, z) \in R_i$ for all i. Since each R_i is transitive, this implies that $(x, z) \in R_i$ for all i. Hence $(x, z) \in \cap_i R_i$. This shows that $\cap_i R_i$ is a transitive relation.

iv. Show that for any binary relation R on X the intersection R^t of all the transitive relations that contain R is the unique smallest transitive relation on X that contains R. (10 pts.)

R^t is called the **transitive closure** of R

Solution. By above, the intersection R^t of all the transitive relations that contain R is the a transitive relation on X that contains R. Since it is the intersection of **all** the transitive relations on X that contains R, it can only be the smallest one.

v. Show that if R and S are two binary relations then $(R \cap S)^t \subseteq R^t \cap S^t$. (8 pts.)

Solution. Since $R \subseteq R^t$ and $S \subseteq S^t$, $R \cap S \subseteq R^t \cap S^t$. Since $R^t \cap S^t$ is transitive by the above question, this implies that $(R \cap S)^t \subseteq R^t \cap S^t$ (because $(R \cap S)^t$ is the **smallest** transitive relation that contains $R \cap S$).

vi. Let R be a binary relation. Show that the subset

$$\{S := (x, y) \in X^2 : \exists x = y_1, y_2, \ldots, y_n = y \in X \text{ such that}$$

$$(y_i, y_{i+1}) \in R \text{ for all } i = 1, \ldots, n-1\}$$ is a transitive relation that contains R. Conclude that $R^t = S$. (10 pts.)

Solution. Let (x, y) and (y, z) be in S. By the very definition of S, there are $x = y_1, y_2, \ldots, y_n = y \in X$ and $y = z_1, z_2, \ldots, z_m = z \in X$ such that $(z_j, z_{j+1}) \in R$ and $(z_j, z_{j+1}) \in R$ for all $i = 1, \ldots, n-1\}$ and $j = 1, \ldots, m-1$. Setting $t_i = y_i$ and $t_{n+j} = z_j$ for all $i = 1, \ldots, n-1\}$ and $j = 1, \ldots, m-1\}$, we see that $x = t_1$, $(t_k, t_{k+1}) \in R$ and $t_{n+m} = z$. Thus $(x, z) \in S$. This shows that S is transitive.

vii. Show that in general $(R \cap S)^t \neq R^t \cap S^t$. (5 pts.)

Solution. Let $X = \{a, b, c, d\}$. Let $R = \{(a, b), (b, d)\}$ and $R = \{(a, c), (c, d)\}$. Then $R^t = \{(a, b), (b, d), (a, d)\}$ and $R = \{(a, c), (c, d), (a, d)\}$. So $R^t \cap S^t = \{(a, d)\}$ and $R \cap S = \emptyset$.

II. Partial Orders. A binary relation $<$ on a set X is called a **partial order** on X if (writing $x < y$ instead of $(x, y) \in <$),

PO1. Irreflexivity. For every $x \in X$, $x \not< x$.

and

PO2. Transitivity. For every x, y, $z \in X$, if $x < y$ and $y < z$ then $x < z$.

We write $x \leq y$ if either $x < y$ or $x = y$.

Let $(X, <)$ be a partially ordered set and $A \subseteq X$. An element $u \in X$ is called an **upper bound** of A if $a \leq u$ for all $a \in A$. An element $v \in X$ is called a **least upper bound** of A if i) v is an upper bound for A and ii) for any upper bound u of A, if $u \leq v$ then $u = v$.

viii. Give an example of a partially ordered set $(X, <)$ and a subset A of X which

i. has a least upper bound which is not in A.

ii. has exactly two least upper bounds.

iii. does not have a least upper bound.

iv. has a least upper bound which is in A. (4 pts.)

Solution: i. Take $X = \mathbb{R}$ with the usual order and let $A = (0, 1)$. Then $\text{lub}(A) = 1 \notin A$.

ii. Let $X = \{a, b, c\}$ and set $a < b$ and $a < c$. Take also $A = X$. Then both b and c are least upper bounds of A.

iii. Let $X = \mathbb{R}$ or $\mathbb{N}$ with the usual order and take $A = \mathbb{N}$.

iv. Take $X = \mathbb{R}$ with the usual order and let $A = (0, 1]$. Then $\text{lub}(A) = 1 \in A$.

ix. Let $(X, <)$ be a partially ordered set and A a subset of X. Suppose that A has a least upper bound which is in A. Show that this is the only upper bound of A. (2 pts.)

Proof: Let $a \in A$ be a least upper bound of A. Let b be another upper bound of A. Then, since $a \in A$, $a \leq b$. Therefore, a being an upper bound and b a least upper bound, $a = b$.

x. Let $(X, <)$ be a partially ordered set. Show that any element of X is an upper bound of $\emptyset$. (2 pts.)

Proof: Certainly any element of X is greater than or equal to any element of $\emptyset$. □

xi. Let $(X, <)$ be a partially ordered set. What can you say about $(X, <)$ if $\emptyset$ has a least upper bound? (2 pts.)

Solution: Then the partially ordered set X must have a unique least element.

xii. Let U be a set and let $X = \wp(U)$. Order X by strict inclusion. Show that this is a partial order on X. (2 pts.) Show that any subset of X has a unique least upper bound. (5 pts.)

Proof: Let a, b, $c \in X$ be such that $a \subset b \subset c$. Then $a \subset c$. Since $a \not\subset a$, this shows that X is a partial order. Let $A \subset X$. Then I claim that $\cup A$, i.e. $\cup_{a \in A} a$ is the unique least upper bound of A. Since $a \subseteq \cup_{a \in A} a$ for all $a \in A$, it is clear that $\cup_{a \in A} a$ is an upper bound of A. Assume b is another upper bound of A. Then $a \subseteq b$ for all $a \in A$; hence $\cup_{a \in A} a \subseteq b$. This shows that $\cup_{a \in A} a$ is the least upper bound of A. □

xiii. Let $(X, <)$ be a partial order. Suppose that for any $a, b \in X$, the set $\{a, b\}$ has a unique least upper bound. Let $a \vee b$ denote this least upper bound.

i. Give an infinite example of such a partially ordered set. (2 pts.)

ii. Prove or disprove: $(a \vee b) \vee c = a \vee (b \vee c)$ for all a, b, $c \in X$. (10 pts.)

Solution: i. $\mathbb{N}$ with the natural order is such an example. Here $\text{lub}(x, y) = \max(x, y)$.

ii. Proof: Clearly $a \leq a \vee (b \vee c)$. Also $b \leq b \vee c \leq a \vee (b \vee c)$, thus $b \leq a \vee (b \vee c)$ as well. These show that $a \vee b \leq a \vee (b \vee c)$.

On the other hand $c \leq b \vee c \leq a \vee (b \vee c)$. With the result of the previous paragraph we get $(a \vee b) \vee c \leq a \vee (b \vee c)$.

Similarly one can also show that $a \vee (b \vee c) \leq (a \vee b) \vee c$. Therefore $(a \vee b) \vee c = a \vee (b \vee c)$.

III. Total Orders. If in addition to PO1 and PO2 stated above,

O3 For every x, $y \in X$, either $x < y$ or $x = y$ or $y < x$,

then the partial order is called a **total order**.

xiv. Show that in a totally ordered set $(X, <)$ if a subset A of X has a least upper bound then this least upper bound is the only upper bound of A. (4 pts.)

Proof: Let $A \subseteq X$ have a least upper bound, say b. Let c be another least upper bound. Then either $b \leq c$ or $c \leq b$, and any of these imply $b = c$.

IV. Well-Ordered Sets. We say that a totally ordered set $(X, <)$ is a **well-ordered set** (or that $<$ well-orders X) if every nonempty subset of X contains a minimal element for that order, i.e. if for every nonempty subset A of X, there is an $m \in A$ such that $m \leq a$ for all a in A. (Note that the element m must be in A).

xv. Give an example of a finite and an infinite well-ordered set. (2 pts.)

Solution. $\mathbb{N}$ is an infinite well ordered set. Any finite subset of $\mathbb{N}$ is a well-ordered set with the restricted (and natural) order.

xvi. Let $X = \mathbb{N} \times \{0\} \cup \mathbb{N} \times \{1\}$. On X define the relation $<$ as follows: For all x, $y \in \mathbb{N}$,

$$\begin{array}{lll} (x,0) < (y,0) & \text{if and only if} & x < y \\ (x,1) < (y,1) & \text{if and only if} & x < y \\ (x,0) < (y,1) & \text{always} & \end{array}$$

i. Is $(X, <)$ a totally ordered set? (2 pts.)

ii. Is $(X, <)$ a well-ordered set? (2 pts.)

Proof: i. Yes. This is the order obtained by putting a copy of $\mathbb{N}$ (namely $\mathbb{N} \times \{1\}$) to the "very end" of a copy of $\mathbb{N}$ (namely $\mathbb{N} \times \{0\}$).

ii. Yes. Let $\emptyset \neq A \subseteq X$.

If $A \cap (\mathbb{N} \times \{0\} \neq \emptyset$, let $n = \text{lub}\{n \in \mathbb{N} : (n, 0) \in A\}$. Then $(n, 0) = \text{lub}(A)$.

If $A \cap (\mathbb{N} \times \{0\} = \emptyset$, let $n = \text{lub}\{n \in \mathbb{N} : (n, 1) \in A\}$. Then $(n, 1) = \text{lub}(A)$.

xvii. Is the set $\{1/n : n \in \mathbb{N} \backslash \{0\}\}$ together with the natural order a well-ordered set? (2 pts.)

Answer: No, because the set itself does not have a least element.

xviii. Is the set $\{1/n : n \in \mathbb{N} \setminus \{0\}\} \cup \{0\}$ together with the natural order a well-ordered set? (2 pts.)

Answer: No. Let $A = \{1/n : n \in \mathbb{N} \setminus \{0\}\}$. Then A does not have a least element: $\text{glb}(A) = 0 \notin A$.

xix. Find an infinite well-ordered set with a maximal element. (4 pts.)

Solution: Let $X = \mathbb{N} \cup \{a\}$ where a is a new element. Define an order on X as follows: Take the natural order on $\mathbb{N}$ and declare that a is greater than any element of $\mathbb{N}$. Then this is a well-order and a is its maximal element.

xx. Show that in a well-ordered set the minimal element of any nonempty subset is unique. (2 pts.)

Proof: Let A be a nonempty subset of a well-ordered set X. Let a and b be two least elements of A. Either $a < b$ or $b < a$ or $a = b$, The first case contradicts the fact that b is a minimal element of A because $a \in A$. The second case gives a contradiction in a similar way.

xxi. Show that every nonempty well-ordered set has a unique minimal element. (2 pts.)

Proof: Follows from above taking A to be the well-ordered set itself.

xxii. Let $(X, <)$ be a well-ordered set. Show that all the elements of X except possibly one of them satisfies the following property: "There exists a y such that $x < y$ and for all z if $x < z$ then $y < z$". (5 pts.) Show that such a y, when exists, is unique (3 pts.)

Proof: Let $x \in X$. Assume x is not the last element of X. Then $\{y \in X : x < y\}$ is a nonempty subset of X and as such has a minimal element, say y, and by one of the questions above this minimal element y is unique.

26.4 First Semester, February 2003

Let X be a set. A set of subsets of X - whose elements are called **open subsets** of X - is called a **topology** on X, if

T1. $\emptyset$ and X are open subsets of X.

T2. The intersection of two open subsets of X is an open subset of X.

T3. The union of any collection of open subsets of X is an open subset of X.

More formally, a subset τ of $\wp(X)$ is called a topology on X, if

T1. $\emptyset \in \tau$ and $X \in \tau$.
T2. If $U, V \in \tau$, then $U \cap V \in \tau$.
T2. If $\sigma \subseteq \tau$, then $\cup \sigma \in \tau$.

i. Show that $\{\emptyset, X\}$ is a topology on X. (2 pts.)

ii. Show that $\wp(X)$ is a topology on X. (2 pts.)

iii. Let A be a subset of X. Show that $\{\emptyset, A, X\}$ is a topology on X. (2 pts.)

iv. Let A and B be two subsets of X. Find a finite topology on X that contains A and B. (3 pts.)

v. Let A, B and C be three subsets of X. Find a finite topology on X that contains A and B. What is the maximum size of the smallest such topology? (4 pts.)

vi. Let τ be a topology on X. Let $A \subseteq X$. Show that there is a unique largest open subset of A. We denote this subset by A°. (6 pts.)

Show that for all subsets A and B of X,

a) If $A \subseteq B$ then $A^\circ \subseteq B^\circ$. (4 pts.)

b) $(A \cap B)^\circ \subseteq A^\circ \cap B^\circ$. (5 pts.)

c) $(A \cup B)^\circ = A^\circ \cup B^\circ$. (7 pts.)

vii. Show that if σ and τ are topologies on X, then $\sigma \cap \tau$ is also a topology on X. (5 pts.)

viii. Show that if T is any set of topologies on X, then $\cap T$ is also a topology on X. (3 pts.)

ix. Show that if $\sigma \subseteq \wp(X)$ is a set of subsets of X, then the intersection $\langle\sigma\rangle$ of all the topologies that contain σ is the smallest topology on X that contains σ. In other words, if $A \in \sigma$ then A is open in the topology $\langle\sigma\rangle$, and $\langle\sigma\rangle$ is the smallest topology on X with this property. This topology is called the **topology generated** by σ. (10 pts.)

x. Let σ be the set of singleton subsets of X. Find $\langle\sigma\rangle$. (3 pts.)

xi. Let $n \in \mathbb{N}$. Let σ be the set of subsets of X of cardinality n. Find $\langle\sigma\rangle$. (5 pts.)

xii. Assume σ is the set of cofinite subsets of X. Find $\langle\sigma\rangle$. (4 pts.)

xiii. Let $\sigma \subseteq \wp(X)$. Consider the set $[\sigma]$ of subsets A of X with the following property:

$$\text{For any } x \in A \text{ there are finitely many } S_1, \ldots, S_n \in \sigma \text{ such that } x \in S_1 \cap \ldots \cap S_n \subseteq U.$$

a) Show that $[\sigma]$ is a topology on X. (5 pts.)

b) Show that $\langle\sigma\rangle \subseteq [\sigma]$. (5 pts.)

c) Show that $\langle\sigma\rangle = [\sigma]$. (5 pts.)

Thus $U \in \langle\sigma\rangle$ if and only if for all $x \in \langle\sigma\rangle$ there are finitely many $S_1, \ldots, S_n \in \sigma$ such that $x \in S_1 \cap \ldots \cap S_n \subseteq U$. (15 pts.)

xiv. Let σ be the set of all open intervals of $\mathbb{R}$. Consider the set $\mathbb{R}$ with the topology $\langle\sigma\rangle$.

a) Show that a subset A of $\mathbb{R}$ is open (in this topology) if and only if for all $a \in A$ there is an $\epsilon \in \mathbb{R}^{>0}$ such that $(a-\epsilon, a+\epsilon) \subseteq A$. (7 pts.)

b) Show that no finite and nonempty subset of $\mathbb{R}$ is open (in this topology). (2 pts.)

c) Show that $[0,1)$ is not open. (3 pts.)

d) Show that a cofinite subset is open. (3 pts.)

d) Is $\mathbb{Q}$ open? (3 pts.)

xv. Let σ_1 be the set of all intervals of $\mathbb{R}$ of the form $[a,b)$ of $\mathbb{R}$ for $a \leq b \in \mathbb{R}$.

a. Show that $\langle\sigma\rangle \subset \langle\sigma_1\rangle$. (5 pts.)

b. Can a singleton set be open in this topology? (3 pts.)

c. Show that $[0,1]$ is not open in this topology. (3 pts.)

xvi. Let σ_2 be the set of all closed and bounded intervals of $\mathbb{R}$. Show that $\langle\sigma_1\rangle \subset \langle\sigma_2\rangle$ where σ_1 is as in number xv. (5 pts.)

26.5 First Semester Final and Its Correction, January 2004

You may assume that you know all the basic arithmetic properties of $(\mathbb{Z}, +, \times, 0, 1)$ and $(\mathbb{N}, +, \times, 0, 1)$.

i. *Let $X = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Define the relation $\equiv$ on X by*

$$(x,y) \equiv (z,t) \Leftrightarrow xt = yz$$

for every (x,y), $(z,t) \in X$.

a) Show that this is an equivalence relation on X.

b) Find the equivalence classes of $(0,1)$ and of $(3,3)$.

c) Show that if $(x,y) \equiv (x',y')$ and $(z,t) \equiv (z',t')$ then $(xt+yz, yt) \equiv (x't'+y'z', y't')$.

d) Show that if $(x,y) \equiv (x',y')$ and $(z,t) \equiv (z',t')$ then $(xz, yt) \equiv (x'z', y't')$.

Proof: a. i. Reflexivity. Let $(x,y) \in X$. Then since $xy = yx$, we have $(x,y) \equiv (x,y)$.

ii. Symmetry. Let (x,y), $(z,t) \in X$ be such that $(x,y) \equiv (z,t)$. Hence $xt = yz$. Therefore $zy = tx$, implying $(z,t) \equiv (x,y)$.

iii. Transitivity. Let (x,y), (z,t), $(u,v) \in X$ be such that $(x,y) \equiv (z,t)$ and $(z,t) \equiv (u,v)$. Hence $xt = yz$ and $zv = tu$. Multiplying these

equalities side by side, we get $xtzv = yztu$. Since $t \neq 0$, by simplifying we get $xzv = yzu$. If $z \neq 0$, then we can simplify further to get $xv = yu$, hence $(x, y) \equiv (u, v)$.

Assume $z = 0$. Then $xt = yz = 0$ and $tu = zv = 0$. Since $t \neq 0$, we get $x = u = 0$, so that $xv = 0 = yu$ and $(x, y) \equiv (u, v)$ again.

b. $\overline{(0,1)} := \{(x, y) \in X : (x, y) \equiv (0, 1)\} = \{(x, y) \in X : x = 0\} = \{(0, y) : y \in \mathbb{Z} \setminus \{0\}\}$.
$\overline{(3,3)} := \{(x, y) \in X : (x, y) \equiv (3, 3)\} = \{(x, y) \in X : 3x = 3y\} = \{(x, x) : x \in \mathbb{Z} \setminus \{0\}\}$.

c) Assume $(x, y) \equiv (x', y')$ and $(z, t) \equiv (z', t')$. Then $xy' = yx'$ and $zt' = tz'$. Multiplying the first one by tt' and the second one by yy' we get $xy'tt' = yx'tt'$ and $zt'yy' = tz'yy'$. Adding these two side by side we get $xy'tt' + zt'yy' = yx'tt' + tz'yy'$, and factoring, we get $(xt + yz)y't' = yt(x't' + y'z')$, meaning $(xt + yz, yt) \equiv (x't' + y'z', y't')$.

d) Assume $(x, y) \equiv (x', y')$ and $(z, t) \equiv (z', t')$. Then $xy' = yx'$ and $zt' = tz'$. Multiplying these two side by side, we get $xy'zt' = yx'tz'$, i.e. $xzy't' = ytx'z'$, meaning $(xz, yt) \equiv (x'z', y't')$.

ii. *Find a graph which has only three automorphisms.*

Solution. Consider the graph whose points are

$$\{a,\ a',\ a'',\ a''',\ b,\ b',\ b'',\ b''',\ c,\ c',\ c'',\ c'''\}$$

and whose vertices are

$$aa',\ aa'',\ a''a''',\ bb',\ bb'',\ b''b''',\ cc',\ cc'',\ c''c''',\ ab,\ bc,\ ca,\ a'b'',\ b'c'',\ c'a''.$$

It works!

iii. *Let a and b be two integers which are not both 0. We say that d is the* **greatest common divisor** *of a and b if d is the largest natural number that divides both a and b. Show that for any $a,\ b \in \mathbb{Z}$, $\gcd(a, b)$ exists and that there are $x,\ y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.*

Proof: Replacing a and b by $|a|$ and $|b|$, we may assume that $a \geq 0$ and $b \geq 0$.

Existence. Since 1 divides both a and b and since any number that divides both a and b can be at most $\max(a, b) > 0$, the set of natural numbers that divide both a and b is a finite nonempty set bounded by $\max(a, b)$. Therefore there is a largest such number. This proves the existence of $\gcd(a, b)$. We let $d = \gcd(a, b)$.

Second Part. We proceed by induction on $\max(a, b)$. If $a = 1$, then take $x = 1,\ y = 0$. If $b = 1$, then take $x = 0,\ y = 1$. This takes care of the

initial step $\max(a,b)$. Assume $\max(a,b) > 1$. If $a = b$, then $d = a$ and we may take $x = 1$, $y = 0$. Assume $a \neq b$. Without loss of generality, we may assume that $a > b$. Note that the divisors of a and b are the same as the divisors of $a - b$ and b. Hence $\gcd(a-b,b) = \gcd(a,b) = d$. Since $\max(a-b,b) < a = \max(a,b)$, by induction there are two integers x and y' such that $x(a-b) + y'b = d$, i.e. $xa + (y'-x)b = d$. Take $y = y' - x$.

iv. *Let a and b be two nonzero integers. We say that m is the* **least common multiple** *of a and b if m is the least natural number that is divisible by both a and b. We let $m = \operatorname{lcm}(a,b)$. Show that for any $a, b \in \mathbb{Z} \setminus \{0\}$, $\operatorname{lcm}(a,b)$ exists and that $ab = \pm \gcd(a,b)\operatorname{lcm}(a,b)$.*

Proof: Replacing a and b by $|a|$ and $|b|$ again, we may assume that $a > 0$ and $b > 0$. Since a and b both divide ab, $\operatorname{lcm}(a,b)$ exists.

Let $d = \gcd(a,b)$ and $m = \operatorname{lcm}(a,b)$. Let a' and b be such that $a = da'$ and $b = db'$. Then $ab = d^2a'b'$. We need to prove that $m = da'b'$.

Since $da'b' = ab' = a'b$, a and b both divide $da'b'$.

Let x be divisible by both a and b. Then $x = au = bv$ for some u, v. We have $a'du = au = x = bv = b'dv$ and so $a'u = b'v$. Since a' and b' cannot have a common divisor (otherwise d would be larger), b' must divide u. (This last fact needs a serious proof, that we have not undertaken yet. I shouldn't have asked this question at this stage). Write $u = cb'$. Now $x = au = acb' = a'dcb'$ and so $a'b'd$ divides x, in particular $a'b'd \leq x$. This shows that $a'b'd$ is the least multiple of a and b, i.e. $a'b'd = m$.

v. *Find formulas for the sums*

$$1^2 + 2^2 + \ldots + n^2$$

and

$$1^3 + 2^3 + \ldots + n^3,$$

and prove your result.

Proof: We claim that

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

We proceed by induction on n. For $n = 1$, it is easy to check the validity of the formula. Assume the statement holds for n. To prove it for $n+1$, we compute:

$$\begin{aligned} 1^2 + 2^2 + \ldots + n^2 + (n+1)^2 &= \tfrac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \tfrac{(n+1)(n(2n+1)+6(n+1))}{6} \\ &= \tfrac{(n+1)(2n^2+7n+6))}{6} \\ &= \tfrac{(n+1)(n+2)(2n+3)}{6} \\ &= \tfrac{n'(n'+1)(2n'+1)}{6} \end{aligned}$$

where $n' = n + 1$. This proves the equality by induction.

We claim that

$$1^3 + 2^3 + \ldots + n^3 = \frac{n^2(n+1)^2}{4}.$$

We proceed by induction on n. For $n = 1$, it is easy to check the validity of the formula. Assume the statement holds for n. To prove it for $n + 1$, we compute:

$$\begin{aligned} 1^3 + 2^3 + \ldots + n^3 + (n+1)^3 &= \tfrac{n^2(n+1)^2}{4} + (n+1)^3 \\ &= \tfrac{(n+1)^2(n^2+4n+4)}{4} \\ &= \tfrac{(n+1)^2(n+2)^2}{4} \\ &= \tfrac{m^2(m+1)^2}{4} \end{aligned}$$

where $m = n + 1$. This proves the equality by induction.

vi. *Recall that a natural number $p \neq 0, 1$ is called* **prime** *if whenever p divides a product xy of two natural numbers x and y then p divides either x or y. A natural number $p \neq 0, 1$ is called* **irreducible** *if whenever $p = xy$ for two natural numbers x and y then either x or y is 1. Show that a natural number is prime if and only if it is irreducible.*

Proof: Let p be prime. Assume that $a|p$. Then $p = ab$ for some b. It follows that p divides ab. Thus p divides either a or b. Assume – without loss of generality – that p divides a. Then $px = a$ some x. Hence $p = ab = pxb$. Since $p \neq 0$, it follows that $xb = 1$. Thus $b = 1$, and so $a = p$.

Let now p be an irreducible. We will prove that p is a prime. Let p divide xy. We will show that p divides either x or y. We proceed by induction on $p+x+y$. Dividing x and y by p we get $x = pq_1+x_1$ and $y = pq_2+y_1$ where $x_1, y_1 < p$. Since $xy = (pq_1+x_1)(pq_2+y_1) = p(pq_1q_2+q_1y_1+q_2x_1)+x_1y_1$, thus p divides x_1y_1. Assume $x_1y_1 \neq 0$. Thus $p \leq x_1y_1 < p^2$. It follows that $x_1y_1 = rp$ for some $r = 1, \ldots, p-1$. If $r = 1$, then either $p = x_1$ or $p = y_1$, a contradiction. Let q be an irreducible dividing r. Thus $q \leq r < p$. By induction q divides either x_1 or y_1, say q divides x_1. Write $x_1 = qx_2$ and $r = qr'$. We have $qx_2y_1 = x_1y_1 = rp = qr'p$ and $x_2y_1 = r'p$. By induction p divides either x_2 or y_1, in which case it divides x or y (respectively). Thus we may assume that $x_1y_1 = 0$. Hence one of x_1 or y_1 is 0, say $x_1 = 0$. Then $x = pq_1 + x_1 = pq_1$ and p divides x. □

26.6 Second Semester, Midterm, May 2003

Let X be a set. A **filter** on X is a set $\Im$ of subsets of X that satisfies the following properties:

i) If $A \in \Im$ and $A \subseteq B \subseteq X$, then $B \in \Im$.

ii) If A and B are in $\Im$, then so is $A \cap B$.

iii) $\emptyset \notin \Im$ and $X \in \Im$.

If $A \subseteq X$ is a fixed nonempty subset of X, then the set of subsets $\Im(A)$ of X that contain A is a filter on X. Such a filter is called **principal filter**. If X is infinite, then the set of cofinite subsets of X is a filter, called **Fréchet filter**. A filter is called **ultrafilter** if it is a maximal filter.

We fix a set X.

i. Show that a principle filter $\Im(A)$ on X is an ultrafilter if and only if A is a singleton set.

Proof: It is clear that if $\emptyset \neq B \subset A$, then $\Im(A) \subset \Im(B)$. Thus $\Im(A)$ cannot be an ultrafilter unless A is a singleton set. Conversely let $A = \{a\}$ is a singleton set. Let $\Im$ be a filter properly containing $\Im(A)$. Let $Y \in \Im \setminus \Im(A)$. Then $a \notin Y$ and so $a \in Y^c$. Therefore $Y^c \in \Im(A) \subset \Im$. It follows that $\emptyset = Y \cap Y^c \in \Im$, a contradiction.

ii. Show that the Fréchet filter (on an infinite set) is not contained in a principal filter.

Proof: Let $\Im$ be the Fréchet filter. Assume $\Im \subseteq Im(A)$ for some $A \subseteq X$. Let $a \in A$. Then $X \setminus \{a\}$, being a cofinite set, is in $\Im$, but is not in $\Im$.

iii. Show that the intersection of a set of filters is a filter.

Proof: All three conditions of the definition are trivially met.

iv. Show that if $\Im$ is a set of subsets of X such that $A_1 \cap A_2 \cap \ldots \cap A_n \neq \emptyset$ for any $A_1, A_2, \ldots, A_n \in \Im$, then there is a filter that contains $\Im$. Describe this filter in terms of $\Im$.

Proof: Let

$$\langle \Im \rangle = \{A \subseteq X : \text{ there are } A_1, \ldots, A_n \in \Im \text{ such that } A_1, \cap \ldots \cap A_n \subseteq A\}.$$

It is easy to show that $\Im \subseteq \langle \Im \rangle$ and that $\langle \Im \rangle$ is a filter. You should also note that $\langle \Im \rangle$ is the smallest filter that contains $\Im$.

v. Show that a filter $\Im$ is an ultrafilter if and only if for any $A \subseteq X$, either A or A^c is in $\Im$. Conclude that in an ultrafilter $\Im$, if $A \sqcup B \in \Im$, then one of A or B in $\Im$.

Proof: Suppose first that $\Im$ is a filter such that for any $A \subseteq X$, either A or A^c is in $\Im$. Let $\Im'$ be a filter properly containing $\Im$. Let $A \in \Im' \setminus \Im$. Then $A^c \in \Im \subset \Im'$. Thus $\emptyset = A \cap A^c \in \Im'$, a contradiction.

Conversely, let $\Im$ be an ultrafilter. Let $A \subseteq X$. Assume that neither A nor A^c is in $\Im$. By question number iv, there are B and C in $\Im$ such that $A \cap B = \emptyset$ and $A^c \cap C = \emptyset$. Then $A \cap B \cap C = \emptyset$ and $A^c \cap B \cap C = \emptyset$, implying that $\emptyset B \cap C \in \Im$, a contradiction.

Assume now $A \sqcup B$ is in the ultrafilter $\Im$. Then either A or A^c is in $\Im$. In the second case $B = A^c \cap (A \sqcup B) \in \Im$.

vi. Conclude that any ultrafilter on X that contains a finite subset of X is a principal filter. Deduce that every nonprincipal ultrafilter contains the Fréchet filter.

Proof: If $\Im$ is an ultrafilter that contains a finite subset, let A be a subset of $\Im$ of smallest size. Let $a \in A\}$. By the second part of the previous question, either $\{a\} \in \Im$ or $A \setminus \{a\} \in \Im$. Hence $A = \{a\}$.

Now let $\Im$ be a nonprincipal ultrafilter. Then it does not contain any finite subset. By the previous question, it contains all cofinite subsets, hence the Fréchet filter is a subset of $\Im$.

vii. (AC) Show that for any filter $\Im$ on X, there is an ultrafilter on X that contains $\Im$.

Proof: Let Z be the set of filters on X that contains $\Im$. Order Z by inclusion. Since $\Im \in Z$, $Z \neq \emptyset$. It is clear that Z is an inductive set, because if $(\Im_i)_{i\in I}$ is a chain from Z, then one can show easily that $\cup_{i\in I}\Im_i$ is a filter that contains $\Im$. Hence by Zorn's Lemma Z has a maximal element. Clearly this maximal element of Z is an ultrafilter.

viii. (AC) Show that if X is infinite then there are nonprincipal ultrafilters on X.

Proof: Apply the previous question to the Fréchet Filter to get an ultrafilter $\Im$ that contains the Fréchet filter. By ii, $\Im$ is not principal.

ix. Let $\Im$ be a filter on X. Let A_x $(x \in X)$ be sets. Consider the product

$$\begin{array}{rcl} \prod_{x\in X} A_x & := & \{f = (f_x)_{x\in X} : f_x \in A_x \text{ for all } x \in X\} \\ & = & \{f : X \longrightarrow \prod_{x\in X} A_x : f(x) \in A_x \text{ for all } x \in X\}. \end{array}$$

On the set $\prod_{x\in X A_x}$ consider the relation defined by

$$f \equiv g \iff \{x \in X : f(x) = g(x)\} \in \Im.$$

Show that this is an equivalence relation.

Proof: Reflexivity and symmetry are clear. Let us show transitivity. Let $f \equiv g$ and $g \equiv h$. Then $\{x \in X : f(x) = g(x)\} \cap \{x \in X : g(x) = h(x)\} \subseteq \{x \in X : f(x) = h(x)\} \in \Im$ because the set on the left hand side is in $\Im$.

From now on we fix a filter $\Im$ on X and we let $M = \prod_{x\in X} A_x/\equiv$. For $f \in \prod_{x\in X} A_x$, we will let $[f]$ to denote its class in M.

x. Show that if $A_x = A$ for all $x \in X$ and if $\Im$ is nonprincipal filter then the map that sends an element $a \in A$ to the class of the constant function a is an injection from A into M.

Proof: Let a, $b \in A$. Assume $[(a)_{x\in X}] = [(b)_{x\in X}]$. Then $\{x \in X : a = b\} \in \Im$, so is nonempty, so $a = b$.

xi. Suppose that each A_x is a set ordered by a relation $<$. On M define the relation $<$ by,

$$[(f_x)_{x\in X}] < [(g_x)_{x\in X}] \iff \{x \in X : f_x < g_x\} \in \Im.$$

Show that this defines an order on M.

Proof: It is clear that $[f] \not< [f]$ for any $[f] \in M$. Assume $[f] < [g]$ and $[g] < [h]$. Then $\{x \in X : f_x < g_x\} \in \Im$ and $\{x \in X : g_x < h_x\} \in \Im$. So their intersection is also in $\Im$. But the set $\{x \in X : f_x < h_x\}$ contains this intersection, so is also in $\Im$. Hence $[f] < [g]$.

xii. Show that if $\Im$ is an ultrafilter and if each $(A_x, <)$ is totally ordered then so is $(M, <)$.

Proof: Let $[f]$, $[g] \in M$. Assume $[f] \neq [g]$. Then $\{x \in X : f_x = g_x\} \notin \Im$ and so (by Question v) $\{x \in X : f_x \neq g_x\} \in \Im$. Therefore, since the sets

$$\{x \in X : f_x < g_x\}$$

and

$$\{x \in X : f_x > g_x\}$$

partition the set $\{x \in X : f_x \neq g_x\}$ which is in $\Im$, one of them should be in $\Im$ by Question v again, in which case either $[f] < [g]$ or $[g] < [f]$.

xiii. Suppose that each $(A_x, <)$ has a largest element. Is it true that $(M, <)$ has a largest element?

Proof: Of course!

xiv. Suppose that each $(A_x, <)$ is well-ordered. Is it true that $(M, <)$ is well-ordered?

Proof:

Index