An Introduction to Advanced Mathematics (Short Version)

M. Yotov

April 14, 2020

$For \quad ... \quad You \quad Know \quad Who!$

These Notes constitute a version of the course *MAA 3200 Introduction to Advanced Mathematics* taught by the author at the Department of Mathematics and Statistics of FIU. The concepts of classes, sets, relations, and functions are introduced and studied with rigour. Care is taken in motivating the introduction of the Zermelo-Fraenkel axioms. The natural numbers and the principle of (finite) mathematical induction are discussed in detail. The integer, rational, and real numbers are constructed and thoroughly discussed. As a brief introduction to Advanced Calculus, the classical topology, convergent sequences of real numbers, and continuity of real valued function of a real variable are studied. The Bolzano-Weierstrass Theorem, Intermediate Value Theorem, and Weierstrass's Theorem are proved.

Please send comments and corrections to the author at yotovm@fiu.edu .

Contents

Chapter 1

Logic. Language of Proof

1.1 Propositions

We begin with an informal discussion of **propositions** in Logic: the formal approach would lead us too far beyond the scope of the course. In the definition below, we are relying on the knowledge of the reader about sentences in English. We are also assuming that the reader is able to tell if a statement, i.e., a sentence containing a claim, is true or false. The latter depends on the context in which the statement is considered. In this course, the context will be the one of Mathematics.

Definition 1.1.1 *A proposition P is a statement, i.e., a special sentence, which is either true or false.*

It is very important, for our considerations, that there are only two options for a statement: **it can either be true or false, and no third option is allowed**. Many statements can be formulated (say, in English), but not every such is a proposition (according to the definition above)! To elevate the status of a sentence from a statement to a proposition, the statement has to be, firstly, well formulated and understood (all words and symbols in the used in the sentence have to be well understood, and the criteria for telling if the statement if true or false have to be known), and, secondly, the statement has to be either true or false, no third option given. The latter is also expressed by saying that the statement has to have a well determined **truth value**: T for "true" and F for "false".

Example 1.1.1 1) How are you doing? (This is not a statement)
2) A lunar month is long less than 28 days. (This is a statement, but is not a proposition. The reason is that, for instance, that there are several different lunar months, and there is no specification of the one in the statement.)
3) The one who is reading these notes now can read English. (This is a statement. It will be a proposition provided we know what "can read English" means.)
4) There is only one even prime number. (This is a statement. For people who know what even and prime number is, it is a proposition. This proposition has truth value T.) □

In our course, as already mentioned, we will be considering math propositions only. So, it is important that the sentence, the statement, be formed by using mathematically well defined concepts, and that the claim in that statement be formulated in a mathematically appropriate way. To do that formally, we need to have **an alphabet** (including math symbols), and also **rules how to correctly construct such sentences** (so that they be propositions!).

Constructing Propositions

We explain now how to construct (more complex) propositions starting with given ones $P, Q, \ldots$. To do this we use **connectives** $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$, and **delimiters** $(,)$. Thus, one defines

$$P \vee Q, \quad P \wedge Q, \quad \neg P, \quad P \rightarrow Q, \quad P \leftrightarrow Q$$

by **assigning a truth value of each of the constructed propositions based on the truth values of the old propositions**. This is conveniently done in truth tables. In words,

$P \vee Q$ ("P **or** Q") is false only if both P and Q are false;
$P \wedge Q$ ("P **and** Q") is true only if both P and Q are true;
$\neg P$ ("**not** P") is true only if P is false;
$P \rightarrow Q$ ("**if** P, **then** Q") is false only if P is true and Q is false;
$P \leftrightarrow Q$ ("P **if, and only if**, Q") is true only if both P and Q have the same truth value: both are true or both are false.

Example 1.1.2 Consider the statements

$$P = \text{"Peter needs help with Calculus 1"} \qquad Q = \text{"Peter calls John"}$$

and suppose they are propositions (that is, we know perfectly well what they mean, as well as how to logically evaluate them). To save some further explanations on who Peter and John are, what Calculus 1 is, and what the rules for finding the truth values of P and Q are, assume P is true, and Q is false. We have the following.

- $P \vee Q$ can be expressed in English as "Peter needs help with Calculus 1 or he calls John", or as "Either Peter needs help with Calculus 1 or he calls John". This is a true statement.
- $P \wedge Q$ can be expressed in English as "Peter needs help with Calculus 1 and he calls John". This is a false statement.
- $\neg P$ can be expressed in English as "Peter does not need help with Calculus 1". This is a false statement.
- $P \rightarrow Q$ can be expressed in English as "If Peter needs help with Calculus 1, (then) he calls John", or as "When/whenever/in case Peter needs help with Calculus 1, he calls John", or as "Should Peter need help with Calculus 1, he calls John", or as "Peter calls John only if he needs help with Calculus 1", or as ... This is a false statement.
- $P \leftrightarrow Q$ can be expressed in English as "Peter calls John precisely when he needs help with Calculus 1", or as "Peter Calls John when he needs help with Calculus 1 and in no other circumstances", or as "the only reason for Peter to call John is if he needs help with Calculus 1", or as ... This is a false statement.

The newly defined propositions have names:

$P \vee Q$ is the **disjunction of** P and Q,
$P \wedge Q$ is the **conjunction of** P and Q,
$\neg P$ is the **negation/denial of** P,
$P \rightarrow Q$ is called a **conditional** proposition with **hypothesis/condition/antecedent** the proposition P and with **conclusion/consequent** - the proposition Q.
$P \leftrightarrow Q$ is called a **bi-conditional** proposition.

By using conditionals, one can express every theorem in mathematics. In Logic, the conditional $P \rightarrow Q$ can be read either as "Q if P" (another way of saying "if P, then Q"), or as "P only if Q" In English, a conditional can be explained in many, equivalent, but looking quite unrelated, ways. The students have to learn how to detect a conditional in such English expressions.

The conditionals $Q \rightarrow P$ and $\neg Q \rightarrow \neg P$ are called **converse** and **contrapositive** to $P \rightarrow Q$, respectively.
The biconditional $P \leftrightarrow Q$ is often read as, and replaced by the English expression, "P **if, and only if,** Q" or even with the shorter "P **iff** Q".

The compound proposition $P \vee Q$ is called **inclusive "or"**. This is, because its value is true not only when P or Q is true, but also when both, P and Q, are true. On the other hand, in everyday speech, when people say "something" or "something else", they usually understand the "or" exclusively: either "something" or "something else", but not both. Turns out that in math similar to those real life situations appear, and the mathematicians have introduced a special notation for the compound proposition which means that: **exclusive or (XOR)**. Formally, given propositions P and Q, denote by $P\ XOR\ Q$ the proposition $(P \wedge \neg Q) \vee (Q \wedge \neg P)$. The value of this proposition is true if, and only if, exactly one of P and Q is true.

1.2 Propositional Expressions, Tautologies

In our definition of new propositions based on old ones, we didn't need to know what the old propositions meant. That is, we didn't need to know what their truth values were. We just exhausted the collection of all combination of values those propositions could have, and determined the value of the new ones. What this formally means is that we simply considered the letters denoting the old propositions as **variables** who take on values true or false. This suggests the definition of **propositional expressions** based on an **alphabet** (p, q, r, ..., x, y, z, ..., $X_1, X_2, X_3, \ldots, Y_1, Y_2, Y_3, \ldots$), where we take symbols for our variables-propositions from, **connectives** ($\vee, \wedge, \neg, \rightarrow, \leftrightarrow$), and **delimiters** ($(,)$), and then using the five ways of constructing compound propositions from the previous subsection. Note that the variables are just symbols. In what follows we will reserve the capital letters from the English alphabet such as P, Q, R, $X_1, X_2, \ldots$, to denote propositions known from the context, or variables whose values are propositions. We specifically designate two special symbols, **the constants**, T and F. to be variables taking only value true in the former case, and only false in the latter case.

Notice the big difference between (compound) propositions and propositional expressions. The former always have a truth value - they are propositions after all! The latter are **not** propositions in general! They become propositions after we substitute every variable with a proposition. Asking of the truth value of a propositional expression doesn't make sense in general. It gets a truth value only after we assign a value to every variable in it. Thus

("February has 28 days" $\vee$ "One lunar month has 28 days") $\rightarrow$ " A week has seven days"

is a proposition, while

$$(P \vee Q) \rightarrow R$$

is a propositional expression. The former has a truth value T (why?), while the question about the truth value of the latter doesn't make sense: we do not know what P, Q, and R stand for!

So, a bit more formally now, **by definition** all symbols from the alphabet, as well as the constants F and T, are propositional expression, and if X and Y are propositional expressions, then so are (X), $X \vee Y$, $X \wedge Y$, $\neg X$, $X \rightarrow Y$, and $X \leftrightarrow Y$.

Note that the propositional expressions are constructed by using only finitely many symbols (variables, constants, connectives, and delimiters). It is reasonable therefore to denote such expressions by $P(X_1, \ldots, X_n)$ where $X_1, \ldots, X_n$ are symbols from the alphabet - the variables in the expression P. Clearly, every two, and every finitely many, fixed propositional expressions can be considered as depending on the same number of variables. This latter fact allows for a natural logical comparison of propositional expressions.

Definition 1.2.1 *The propositional expressions $P(X_1, \ldots, X_n)$ and $Q(X_1, \ldots, X_n)$ are called* **logically equivalent** *if for every n propositions $P_1, \ldots, P_n$ the truth values of $P(P_1, \ldots, P_n)$ and*

$Q(P_1, \ldots, P_n)$ *are the same. We write in such a case*

$$P(X_1, \ldots, X_n) \Leftrightarrow Q(X_1, \ldots, X_n).$$

The propositional expressions $P(X_1, \ldots, X_n)$ *is called a* **tautology** *if*

$$P(X_1, \ldots, X_n) \Leftrightarrow T,$$

and is called a **contradiction** *if*

$$P(X_1, \ldots, X_n) \Leftrightarrow F.$$

Remark 1.2.1 Note that, by the definition of the bi-conditional $P \leftrightarrow Q$, we have that the statement

$$P(X_1, \ldots, X_n) \leftrightarrow Q(X_1, \ldots, X_n) \Leftrightarrow T$$

is the same as the statement

$$P(X_1, \ldots, X_n) \Leftrightarrow Q(X_1, \ldots, X_n). \quad \square$$

Proving Tautologies/Logical Equivalences; Truth Tables

There are basically two ways of proving logical equivalences,

$$P(X_1, \ldots, X_n) \Leftrightarrow Q(X_1, \ldots, X_n),$$

equivalently - proving tautologies,

$$P(X_1, \ldots, X_n) \leftrightarrow Q(X_1, \ldots, X_n).$$

One of them is routine, but often a long process. The other is more intelligent, but relies on basic tautologies established using the routine method.

For the first one, one compares, for every possible combination $(x_1, \ldots, x_n)$ of values of the variables $X_1, \ldots, X_n$, the values $P(x_1, \ldots, x_n)$ and $Q(x_1, \ldots, x_n)$. The amount of work here depends heavily on both the number of variables, and on the structure of the propositional expressions. There is no much to do when $n = 1$ for there are two cases to consider: $x_1 = T$ and $x_1 = F$. If $n = 2$, the combinations of values are 4:

$$(T, T),\ (T, F),\ (F, T),\ (F, F).$$

When $n = 3$ the combinations of values are 8:

$$(T, T, T),\ (T, T, F),\ (T, F, T),\ (F, T, T),\ (T, F, F),\ (F, T, F),\ (F, F, T),\ (F, F, F).$$

The number of possible combinations of values rapidly increases with n being equal to 2^n. But even when n is small, like $n = 1$ or $n = 2$, it may take long to compute the values of P and Q. For instance, it takes a moment only to realize that $X \wedge Y \leftrightarrow Y \wedge X$ is a tautology, while proving that

$$(X \rightarrow Y) \leftrightarrow (\neg X \vee Y)$$

is one needs comparatively more work. To go about the proof that this is indeed a tautology, we use the fact that any such expression is constructed starting with the variables building up using connectives. In our particular case, we gradually construct

$$\neg X, \quad X \rightarrow Y, \quad \neg X \vee Y, \quad (X \rightarrow Y) \leftrightarrow (\neg X \vee Y).$$

To compute the value of this expression for a particular choice of values of X and Y, one can compute gradually the values in the building sequence of formulae. Fro instance, if $X = T$ and $Y = F$, we have for the four propositions above truth values respectively

$$F, \quad F, \quad F, \quad T.$$

Similar calculations have to be performed for the rest three combinations of values of X and Y.

There is a way to collect all these calculations very neatly in a table, called **truth table**.

• The table has $n + k$ columns where n is the number of variables in the expression we are studying, and k is the number of steps needed to build up this expression. For our example above, $n = 2$ and $k = 4$. The first n columns of the table are reserved for the variables involved in the expression.

• The rows of the table are $2^n + 1$: the first row is occupied by the expressions we are evaluating, the rest of the rows correspond to the different combinations of the values of the variables. In our case, the rows are 5. The first n positions of every row contain combinations of values of the variables. The rest of the positions contain the values of the expression placed in the first row at that position.

• The table is filled in from left to right, and from top to bottom.

The table corresponding to our example looks as follows

X	Y	$\neg X$	$X \to Y$	$\neg X \vee Y$	$(X \to Y) \leftrightarrow (\neg X \vee Y)$
T	T	F	T	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

Since the value in the last column are all T, then the expression corresponding to that column, that is, the expression

$$(X \to Y) \leftrightarrow (\neg X \vee Y)$$

is a tautology. Or, formulating it differently, but equivalently, we have the logical equivalence

$$X \to Y \Leftrightarrow \neg X \vee Y.$$

We can also put in a truth table the **definitions** of the connectives we introduced in this chapter. Here is the table

X	Y	$\neg X$	$X \wedge Y$	$X \vee Y$	$X \to Y$	$X \leftrightarrow Y$	X XOR Y
T	T	F	T	T	T	T	F
T	F	F	F	T	F	F	T
F	T	T	F	T	T	F	T
F	F	T	F	F	T	T	F

The more intelligent way of proving tautologies/logical equivalences will be demonstrated in the exercises below.

Basic Tautologies

The following summarizes the main logical equivalences between propositional expressions.

Proposition 1.2.1 *Let P, Q, and R be propositional formulae (of the same number of variables). The propositional formulae are tautologies.*

$$P \leftrightarrow P \quad P \vee P \leftrightarrow P \quad P \wedge P \leftrightarrow P \quad (\neg P) \vee P \leftrightarrow T \quad (\neg P) \wedge P \leftrightarrow F$$

$$(P \leftrightarrow Q) \leftrightarrow (Q \leftrightarrow P) \qquad (P \leftrightarrow Q) \leftrightarrow ((P \to Q) \wedge (Q \to P))$$

Transitivity of $\to$ and $\leftrightarrow$

$$((P \leftrightarrow Q) \wedge (Q \leftrightarrow R)) \to (P \leftrightarrow R) \qquad ((P \to Q) \wedge (Q \to R)) \to (P \to R)$$

Commutativity , associativity, and interaction with the constants T and F

$$(P \vee Q) \leftrightarrow (Q \vee P) \quad (P \vee (Q \vee R)) \leftrightarrow ((P \vee Q) \vee R) \quad (P \vee F) \leftrightarrow P \quad (P \vee T) \leftrightarrow T$$

$$(P \wedge Q) \leftrightarrow (Q \wedge P) \quad (P \wedge (Q \wedge R)) \leftrightarrow ((P \wedge Q) \wedge R) \quad (P \wedge F) \leftrightarrow F \quad (P \wedge T) \leftrightarrow P$$

Two distributivity laws for $\vee$ and $\wedge$

$$(P \vee (Q \wedge R)) \leftrightarrow ((P \vee Q) \wedge (P \vee R)) \qquad (P \wedge (Q \vee R)) \leftrightarrow ((P \wedge Q) \vee (P \wedge R))$$

Negations of the connectives

$$\neg(\neg P) \leftrightarrow P \qquad \neg(P \vee Q) \leftrightarrow ((\neg P) \wedge (\neg Q)) \qquad \neg(P \wedge Q) \leftrightarrow ((\neg P) \vee (\neg Q))$$

$$\neg(P \to Q) \leftrightarrow (P \wedge \neg(Q))$$

And last, but by no means least!

$$((\neg P) \to (Q \wedge (\neg Q))) \ \to \ P$$

Proof Exercise (on using truth tables!) □

Exercise 1.2.1 *Prove the claims in Proposition 1.2.1*

Remark 1.2.2 It is clear from Proposition 1.2.1 that the connectives $\vee$ and $\wedge$ behave pretty much like addition and multiplication, respectively, with T being the identity element and F - the zero element. Pay special attention to the last tautology! It can be rephrased as

$$((\neg P) \to F) \to P$$

and, because of that, instrumental for utilizing the method of **proof by contradiction** to be introduced later in the course. □

Exercise 1.2.2 *(1) Prove that the propositional formula $(\neg Q \wedge (P \to Q)) \to \neg P$ is a tautology.*

[Proof. We are demonstrating a proof without use of truth tables, but with the use of Proposition 1.2.1 and the tautology we proved before the Proposition 1.2.1. Identify the items from that Proposition we are making use of! We have

$$(\neg Q \wedge (P \to Q)) \to \neg P \quad \Leftrightarrow \quad \neg(\neg Q \wedge (\neg P \vee Q)) \vee \neg P$$

$$\Leftrightarrow \quad (\neg(\neg Q) \vee \neg(\neg P \vee Q)) \vee \neg P \quad \Leftrightarrow \quad Q \vee (\neg(\neg P \vee Q) \vee \neg P$$

$$\Leftrightarrow Q \vee \neg P \vee (\neg(\neg P \vee Q)) \quad \Leftrightarrow \quad (\neg P \vee Q) \vee \neg(\neg P \vee Q) \quad \Leftrightarrow \quad T.$$

Do the exercise using truth tables too, and compare the approaches.]

(2) Prove that the propositional formula $((P \vee Q) \wedge \neg P) \to Q$ is a tautology.

(3) Prove that the propositional formula $((P \vee Q) \wedge ((\neg P) \vee R)) \to (Q \vee R)$ is a tautology.

1.3 Propositional Functions and Quantifiers

1.3.1 Propositional Functions and Negations thereof

Propositional Functions

In forming a propositional expression, say $P(X_1, \ldots, X_n)$, the variables $X_1, \ldots, X_n$ were allowed to take on values in the collection, the **universe**, of all propositions. But we can, and will, extend the construction of propositions to include variables taking on values from other universes as well. This

will help us construct **propositional functions** $f(X_1, \ldots, X_n; x_1, \ldots, x_m)$ where $x_1, \ldots, x_m$ stand for the variables which are not propositions. Constructing these includes also additional connectives, such as the standard math symbols $+, -, \cdot, \div, \circ, <, \leq, >, \geq$, etc. All these have to be mathematically sound in the most common sense which we assume the reader possesses. A propositional function becomes a proposition if all the variables involved in its construction are given values from their respective universes. A particular case of such functions are the **open sentences**, which have no propositional variable in them: $f(x_1, \ldots, x_m)$.
The non-propositional variables can be of two types: **apparent** or **bound** variables, and **actual** or **free** variables. Roughly speaking, the apparent variables do not matter in determining the value of the proposition resulting in substituting values for all the variables in $f(x_1, \ldots, x_m)$. For instance, in the propositional function, where the variables x and y are taking on real number values,

$$f(x, y) = \text{"} \int_0^x x \cos y \; dy = 100\text{"}$$

the variable x is actual, while the variable y is apparent. As a matter of fact, the variable y, by the very meaning of the formula, is understood to take on values from 0 to x, once x is given a value. So that y is a variable, but we are not allowed to "assign" values to y. It is in this sense that y is a bound variable. We will see shortly other ways to bound free variables. The function $f(x, y)$ has no propositional variables, so it is an open sentence.

Negations of Propositional Functions

A word about **denying a propositional function**: $\neg f(X_1, \ldots, X_n; x_1, \ldots, x_m)$. The propositional functions are made by using simpler propositional functions and the connectives listed above. We know what to do when denying the logical connectives (this is part of the content of Proposition 1.1). When it comes to the mathematical connectives, such as $+, -, \cdot, \div, <, \leq, >, \geq, =$ and others, we notice that

• the first four of these are binary **operations** (that is, two elements operated upon by one of these four, produce a new element: given a and b, one gets $a + b, a - b, a \cdot b, a \div b$), and

• the last five are binary **relations** (that is, they show how two elements are related to each other: $a < b$, $a \leq b$, $a > b$, $a \geq b$, $a = b$).

When a formula is negated/denied,

the operations remain the same while **the relations get negated**

So, one has to know how to negate relations. We have in this respect that

$$\neg(<) \Leftrightarrow \geq \qquad \neg(\leq) \Leftrightarrow (>) \qquad \neg(=) \Leftrightarrow ((<) \vee (>))$$

and the three more equivalences obtained by the fact that $\neg(\neg P) \Leftrightarrow P$. As is customary to do, we denote $\neg(=)$ by $\neq$

Example 1.3.1 Consider the propositions $P =$ "Year 2025 has 365 days" and $Q =$ "$3 \cdot 15 + 74 \div 5 - 15 = \pi$". Construct a new proposition using P and Q, say $R = P \to Q$. So,

$$R = \text{"If the year 2025 has 365 days, then } 3 \cdot 15 + 74 \div 5 - 15 = \pi\text{."}$$

We know that $\neg R = \neg(P \to Q) \Leftrightarrow P \wedge \neg Q$ which, in English, sounds like

"Year 2025 has no 365 days, and $3 \cdot 15 + 74 \div 5 - 15$ is not equal to π".

If we want to formulate the same proposition without using negative expressions, that is, to express it (**in positive terms!**), then we can write

"Year 2025 has more, or less, than 365 days, and $3 \cdot 15 + 74 \div 5 - 15$ is bigger, or smaller, than π."

One can use less amount of English words to express the latter as well if they want:

"(year 2025 has more, or less, than 365 days) $\wedge$ $((3 \cdot 15 + 74 \div 5 - 15 > \pi) \vee (3 \cdot 15 + 74 \div 5 - 15 < \pi))$."

Even more variations of expressing this are possible. □

Example 1.3.2 As another example, let's find the negation of the propositional function with integral we considered in the previous subsection. Note that taking an integral of a function is an **operation**, so a negation should not change it. That is why we have

$$\neg\left(\int_0^x x\cos y\,dy = 100\right) \Leftrightarrow \int_0^x x\cos y\,dy \neq 100 \quad \square$$

1.3.2 Quantifiers; Propositions Produced by Quantifying Propositional Functions

We know that one way to make a proposition out of a propositional function is by substituting particular values for the variables in the function. In an example above, we figured out that, in the presence of bound variables, it is needed to give values to only the free variables (bounding them this way). In a sense, a propositional function becomes a proposition after **all variables in it become bound**.
A very important other way of achieving the same, making a proposition out of a propositional function, is by using **quantifiers**. The propositions we get this way are actually claims about the collection of the values of the variables we quantify which make the propositional function have value T. The latter collection is called **the truth set** of the function.
More specifically, consider, as a simplest case, a propositional function of one variable $f(x)$, and let Ω_x denote the **collection of meanings/witnesses** (the **universe of discourse**) of x. The **truth set** of $f(x)$ is the collection of all meanings of x for which $f(x)$ is true. The **quantification** of $f(x)$ produces a **claim about the truth set of** $f(x)$. Thus, the **universal quantification**

$$(\forall x)(f(x))$$

stands for the claim that **the truth set of** $f(x)$ **is the whole** Ω_x, while the **existential quantification**

$$(\exists x)(f(x))$$

stands for the claim that **the truth set has at least one member**. Respectively the symbols $\forall$ and $\exists$ are called **universal** and **existential** quantifiers.
There is also a specialization of the existential quantifier claiming that **the truth set of f(x) has only one member in itself**

$$(\exists! x)(f(x)).$$

This expression is a shorthand for the statement

$$(\exists x)(f(x)) \wedge ((\forall y)(\forall z)(f(y) \wedge f(z) \rightarrow y = z)).$$

A **counterexample** for $(\forall x)(f(x))$ is a witness x_0 for which $\neg(f(x_0))$ is true.

Note that the variable x is a free variable before the quantification, and is bound after that. So, the quantification is a process of making bound out of free variables.

Having introduced the quantifications of a function $f(x)$, it is important to know how to interpret the negations of these. The truth of the matter is as follows.

Theorem 1.3.1 *For the quantifications of the propositional function* $f(x)$ *with universe of discourse* Ω_x *for* x *we have*
(1) $\neg((\forall x)(f(x))) \Leftrightarrow (\exists x)(\neg(f(x))$,
(2) $\neg((\exists x)(f(x))) \Leftrightarrow (\forall x)(\neg(f(x))$.

Proof We are proving the claim in item (1). **The claim in (2) is left as an exercise**. We have to prove that the propositions $\neg((\forall x)(f(x)))$ and $(\exists x)(\neg(f(x))$ have the same truth value. For the truth value of $\neg((\forall x)(f(x)))$, there are two options: it is either true or it is false. We have to show therefore that if that value is T, then the value of $(\exists x)(\neg(f(x))$ is T as well, and that if that truth

value is F, then so is the truth value of $(\exists x)(\neg(f(x))$.
Suppose first that $\neg((\forall x)(f(x)))$ is true. The proposition $(\forall x)(f(x))$ can either be true or false, Since its negation is true by assumption, then $(\forall x)(f(x))$ is false. This means that not for all x is $f(x)$ true. But this means that there is an $x_0 \in \Omega_x$ for which $f(x_0)$ is false, that is, there is an $x_0 \in \Omega_x$ such that $\neg f(X_0)$ is true. The existence of such a x_0 can be stated as $(\exists x)(\neg f(x))$ is true. Suppose now that $\neg((\forall x)(f(x)))$ is false. As we know, this means that $(\forall x)(f(x))$ is true. So, there is no x such that $f(x)$ is false, This means that there is no x for which $\neg f(x)$ is true. In other words, $(\exists x)(\neg f(x))$ is false. $\square$

Exercise 1.3.1 *Prove Item (2) of Theorem 1.3.1*

Example 1.3.3 Let's find the negation of the proposition $(\exists\, !x)(f(x))$. Recall that the formula of this proposition is a shorthand of the (longer) formula

$$(\exists x)(f(x)) \wedge ((\forall y)(\forall z)(f(y) \wedge f(z) \to y = z)).$$

Therefore

$$\neg((\exists\, !x)(f(x))) \quad \Leftrightarrow \quad \neg[(\exists x)(f(x)) \wedge ((\forall y)(\forall z)(f(y) \wedge f(z) \to y = z))]. \quad \square$$

Exercise 1.3.2 *Finish the example above finding the negation of* $(\exists\, !x)(f(x))$.

The case of a function of one (free) variable is naturally extended to the general case of a function of finitely many free variables: $f(x_1, \ldots, x_m)$. In this case, one can, by using quantification, bound any number of variables. So, the result of such quantifications can be a new function (with free variables the unbound yet ones) or a proposition (when all free variables get bound. For instance

$$(\forall x)(\exists y)(f(x, y))$$

is a proposition while

$$(\exists x)(f(x, y))$$

is a function with free variable y. Note that **the order of quantification does matter**! Thus, although

$$(\forall x)(\forall y)(f(x, y)) \quad \Leftrightarrow \quad (\forall y)(\forall x)(f(x, y))$$

and

$$(\exists x)(\exists y)(f(x, y)) \quad \Leftrightarrow \quad (\exists y)(\exists x)(f(x, y))$$

(prove that as an exercise!),

$$(\forall x)(\exists y)(f(x, y)) \qquad \text{and} \qquad (\exists y)(\forall x)(f(x, y))$$

are NOT logically equivalent in general!

Example 1.3.4 Suppose $\Omega_x = \Omega_y = \mathbb{R}$. The proposition

$$(\forall x)(\exists y)(x^2 = y)$$

is not logically equivalent with

$$(\exists y)(\forall x)(x^2 = y).$$

Indeed, the first is a true statement, while the second is false. $\square$

The theorem above holds true if **one** out of **many** free variables only is quantified. Thus, we have

$$\neg((\forall x_1)(f(x_1, \ldots, x_n)) \Leftrightarrow (\exists x_1)(\neg f(x_1, \ldots, x_n))$$

and

$$\neg((\exists x_1)(f(x_1, \ldots, x_n)) \Leftrightarrow (\forall x_1)(\neg f(x_1, \ldots, x_n)).$$

Indeed, in this case both sides depend on $n-1$ free variables, and the logical equivalence of the two means that, for **any choice**, $x_2^o, \ldots, x_n^o$, of values/witnesses for the free variables, we have that quantified propositional functions of **one** variable need to have the same value, namely that

$$\neg((\forall x_1)(f(x_1, x_2^o, \ldots, x_n^o)) \Leftrightarrow (\exists x_1)(\neg f(x_1, x_2^o, \ldots, x_n^o))$$

and

$$\neg((\exists x_1)(f(x_1, x_2^o, \ldots, x_n^o)) \Leftrightarrow (\forall x_1)(\neg f(x_1, x_2^o, \ldots, x_n^o)).$$

Since this is true due to the theorem above, then we are done.
Now the negation of more general quantified propositional functions, obtained by quantifying some of the free variables, is formal and straightforward.

Example 1.3.5 (1) $\neg((\forall x)(\exists y)(x^2 = y)) \Leftrightarrow (\exists x)\neg((\exists y)(x^2 = y)) \Leftrightarrow (\exists x)(\forall y)\neg(x^2 = y)$ $\Leftrightarrow (\exists x)(\forall y)(x^2 \neq y)$. This proposition is obviously false (explain why!).

(2) $\neg((\exists y)(\forall x)(x^2 = y)) \Leftrightarrow (\forall y)\neg((\forall x)(x^2 = y)) \Leftrightarrow (\forall y)(\exists x)\neg(x^2 = y)$
$\Leftrightarrow (\forall y)(\exists x)(x^2 \neq y)$. This one is obviously true (explain why!)

(3) Negation of a propositional function with a free variable. $\neg((\forall x)(x^2 = y)) \Leftrightarrow (\exists x)(x^2 \neq y)$.

(4) In this example, we rely on certain knowledge from Calculus I: convergent sequences. Later on in this course, we will study thoroughly this concept. The definition of a convergent sequence is a fine example of a quantified propositional function. **We say that the sequence $< x_n >$ is convergent if**

$$(\exists L)(\forall \epsilon)(\exists m)(\forall n)(n \geq m \rightarrow |x_n - L| < \epsilon).$$

The propositional function is $f(L, \epsilon, m, n) =$ "$(n \geq m \rightarrow |x_n - L| < \epsilon)$". The universes of meanings for the variables are $\Omega_L = \mathbb{R}$, $\Omega_\epsilon = \mathbb{R}_{>0}$, $\Omega_m = \Omega_n = \mathbb{N}$. If the (quantified) propositional function holds true, then we say that L is the limit of $< x_n >$ and write $< x_n > \rightarrow L$. A sequence which is not convergent is called **divergent**. □

Exercise 1.3.3 *Express* **in positive terms** *what divergent sequence is.*

1.4 Methods of Proof

We are discussing in this section basic methods of proving that a proposition Q is true.

1.4.1 General Remarks

A proposition Q in Logic is proved to be true using facts already known to be true. These facts may be axioms (that is, statements that we assume are true without proof), or previously proved propositions. Therefore, proving Q (is true) is formally proving that the conditional

$$T \rightarrow Q$$

is true where T stands for an appropriate proposition P known to have truth value T. This leads us to considering methods of proving that a conditional

$$P \rightarrow Q$$

is true. Recall that a conditional $A \rightarrow B$ is false only when A is true, and B is false. So, in our attempt to prove the conditional $P \rightarrow Q$ is true, it is enough to show that the option when P is true, and Q is false is not possible. Therefore, what we have to actually show is that

$$\text{if} \quad P \quad \text{is true,} \quad \text{then} \quad Q \quad \text{is true.}$$

A proof that a conditional is true may be simple or complicated depending on the complexity of the proposition as well as on our ability to do proofs. Usually, before proving that Q is true, we establish a that several other propositions are true, and these propositions help us "get" Q. So, we have

$$P \to Q_1 \qquad P \wedge Q_1 \to Q_2 \quad \cdots \quad P \wedge Q_1 \wedge \cdots \wedge Q_n \to Q.$$

The longer the sequence of conditionals we prove before we prove Q, the more complicated the proof of $P \to Q$. However, there are two specific schemes of proving a conditional which are used in all proofs: **the direct method of proof**, and **the contrapositive method of proof**. The latter one has an important particular case called **proof by contradiction**. This section is devoted to those three methods of proof. Since all arguments in Logic are constructed using the **rules of inference**, we begin our discussion by listing, and explaining, some of these.

Vista: Later in this course, in Chapter 3, we will introduce another, quite powerful, method of proof: the Method of (Finite) Mathematical Induction. The three methods discussed in this chapter and the Method of Math Induction constitute the arsenal of methods of proof we will be using in this course. They are the basic ones used in math as well.

1.4.2 Rules of Inference

The rules under consideration are just **readings of some of the tautologies we have already seen, or interpreting quantified expressions**. Here are some typical examples.

(1) We know that the propositional formula $(P \wedge (P \to Q)) \to Q$ is a tautology. The rule based on it (**modus ponens** or **law of detachment**) says that if P is true, and if P implies Q (that is $P \to Q$ is true), then Q is true as well. We are detaching Q from $P \to Q$ knowing that P is true. Schematically, this Law can be expressed as

$$\begin{array}{l} P \to Q \\ P \\ \hline \therefore \quad Q \end{array}$$

(2) Another tautology that we know is the following one: $((\neg Q) \wedge (P \to Q)) \to (\neg P)$. The rule based on it is called **modus tollens** (that is, **denies by denying**). It says that if we know that P implies Q, and that Q is false, then P is false as well. Schematically, we have

$$\begin{array}{l} P \to Q \\ \neg Q \\ \hline \therefore \quad \neg P \end{array}$$

(3) The **hypothetical syllogism** rule is based on the transitivity of the conditional:

$$(P \to Q) \wedge (Q \to R) \to (P \to R).$$

It says that if we know that P implies Q, and that Q implies R, then P implies R. We have

$$\begin{array}{l} P \to Q \\ Q \to R \\ \hline \therefore \quad P \to R \end{array}$$

(4) The **disjunctive syllogism** rule is based on the tautology $((P \vee Q) \wedge (\neg P)) \to Q$, and says that if P is false and if one of P or Q is true, then Q is true.

$$\begin{array}{l} P \vee Q \\ \neg P \\ \hline \therefore \quad Q \end{array}$$

(5) The **resolution** rule is based on the tautology $((P \vee Q) \wedge ((\neg P) \vee R)) \to (Q \vee R)$. We leave it to the reader (as an exercise) to interpret this rule in English. We write also

$$\begin{array}{r} P \vee Q \\ \neg P \vee R \\ \hline \therefore \quad Q \vee R \end{array}$$

(6) The **universal instantiation** rule says that if the proposition $(\forall x)(P(x))$ is true, then for **any** witness x_0 of x the proposition $P(x_0)$ is true. We can also write

$$\begin{array}{c} (\forall x) f(x) \\ \hline \therefore \quad f(x_0) \text{ is true for any } x_0 \end{array}$$

(7) The rule in item (6) has a pair, called **universal generalization**, which says that if for **any** witness x_0 of x the proposition $P(x_0)$ is true, then the quantified proposition $(\forall x)(P(x))$ is also true. So, we have

$$\begin{array}{c} f(x_0) \text{ is true for any } x_0 \\ \hline \therefore \quad (\forall x) f(x) \end{array}$$

The last two rules have their counterparts in the case of the existential quantification as well.

Exercise 1.4.1 *Formulate the* **existential instantiation** *and the* **existential generalization** *rules following the model for the universal quantifier.*

1.4.3 Direct Method of Proof

This is a method for proving that $P \to Q$ is true in which **one assumes that P is true**, and, using laws of inference of Logic and other already proved math facts, **proves that Q is true** as well. Schematically, the direct method of proof looks like

$$P \Rightarrow Q_1 \Rightarrow \cdots \Rightarrow Q_n \Rightarrow Q$$

which is a short way to denote the process of proving that the conditionals in the sequence

$$P \to Q_1,\ P_1 \to Q_2,\ \cdots,\ P_{n-1} \to Q_n,\ P_n \to Q$$

are all true. Here $P_1 = P \wedge Q_1$, $P_2 = P_1 \wedge Q_2$, $\ldots$, $P_n = P_{n-1} \wedge Q_n$. Notice that we use the **hypothetical syllogism** several times to conclude from here that $P \to Q$ is true. Notice also that the proof of each of the conditionals in this sequence can be by using a direct method, or any other method of proof we discuss in this course.

Examples of Propositions Proved by Using Direct Method

These are given in a form of exercises below. To be able to understand the claims in the examples, we need a bit of definitions from elementary mathematics: Number Theory and Plane Geometry.

Elementary Number Theory
Given two integers, $m, n \in \mathbb{Z}$, we say that m **divides** n, and write $m \,|\, n$, if there is an integer $s \in \mathbb{Z}$ such that $n = ms$. We say that n is **even** if $2 \,|\, n$, and that n is **odd** otherwise.

Elementary Plane Geometry
According to the axioms of plane geometry (Incidence Geometry) we have that there are **points**, denoted by capital letters, **lines**, denoted by small letters, and an **incidence relation** between them, denoted by $\sim$ subject to several axioms. Some of them are listed here.

Axiom 1: For every two distinct points, there is a unique line which is incident with both points:

$$(\forall P)(\forall Q)(P \neq Q \to (\exists! l)(P \sim l \wedge Q \sim l)).$$

Axiom 2: Every line is incident with at least two distinct points:

$$(\forall l)(\exists P)(\exists Q)(p \neq Q \wedge P \sim l \wedge Q \sim l).$$

Axiom 3: There are three points such that there is no line incident with all three of them:

$$(\exists P)(\exists Q)(\exists R)(\forall l)(\neg(P \sim l \wedge Q \sim l \wedge R \sim l)).$$

Points incident with a line are called **collinear**. So, Axiom 3 claims that there are three **non-collinear** points.

Exercise 1.4.2 *(1) Prove that if* $0 \,|\, n$*, then* $n = 0$*. Prove also that* $(\forall m)(m \,|\, 0)$*.*

[Proof. Note that the first statement above, in strict mathematical terms, has to be written as

$$(\forall n)(0 \,|\, n \ \rightarrow \ n = 0).$$

In the proof of both claims, we are using the Universal Generalization rule of inference: we prove the conditional for every (fixed) n*, and similarly for the second claim. Starting with the conditional, we have to prove that* $P \rightarrow Q$ *has value* T *where* $P =$ "$0 \,|\, n$" *and* $Q =$ "$n = 0$"*. Assuming* P *is true, and using the definition of divisibility above, we get that there is an integer number* m *such that* $n = 0 \cdot m$*. Now using the fact (which we will prove formally later in the course) that the product of any integer number with* 0 *is* 0*, we get that* $n0 \cdot m = 0$*. This means that* Q *is true as well. The claim is proved. Designing a proof of the second claim is left to the reader.]*
(2) Consider the claim "If $m \,|\, n$ *and* $n \neq 0$*, then* $|m| \leq |n|$*". Formulate it in rigorous mathematical terms, and prove it explaining the rules of inference you are using for that.*
[Hint: $(\forall n)(\forall m)(m \,|\, n \wedge n \neq 0) \rightarrow (|m| \leq |n|)$*.]*

(3) Consider the claim "If $m \,|\, n$ *and* $m \,|\, s$*, then* $m \,|\, n + s$ *and* $m \,|\, n - s$*". Formulate the claim in mathematical terms, and prove it stating the rules of inference you are using to do that.*
[Hint: $(\forall m)(\forall n)(\forall s)((m \,|\, n \wedge m \,|\, s) \rightarrow (m \,|\, n + s \wedge m \,|\, n - s))$*.]*

(4) Prove that $(\forall m)(\forall n)(\forall s)((m \,|\, n \wedge m \,|\, n + s) \ \rightarrow \ (m \,|\, s))$*. State the rule of inference you are using for that.*
[Hint: Universal Generalization for m, n, s *separately. Here* $P =$ "$m \,|\, n \wedge m \,|\, n + s$"*, and* $Q =$ "$m \,|\, s$"*. Assuming* P *is true, we have that there are natural number* u, v *such that* $n = m \cdot u$ *and* $n + s = m \cdot v$*. Since* $n + s = m \cdot u + s$*, we have* $m \cdot u + s = m \cdot v$*. After simple arithmetic manipulations of the last equality, we get* $s = m \cdot (v - u)$*. By the definition of divisibility then we get that* $m \,|\, s$*. The claim is proved.*
Notice that if (3) above was already proved, the proof of (4) can be very short:

$$m \,|\, n + s \wedge m \,|\, n \rightarrow m \,|\, (n + s) - n.]$$

(5) Prove that if n *is even number, then so is* n^2*. Formulate the statement in formal mathematical terms. State the rules of inference you are using in the proof.*

(6) Prove that the sum of two even numbers is even. Formulate the claim in formal mathematical terms, and name the rules of inference you use in the proof.

(7) If* P *is any point, then there is a line which is not incident with* P*. Formulate this statement in formal mathematical terms. Name the rules of inference you use in the proof.*

1.4.4 Contrapositive Method of Proof

This is a scheme in which one proves $P \rightarrow Q$ is true by proving (using direct method) that the conditional $\neg Q \rightarrow \neg P$ is true instead. This is a valid approach, because as we know the contrapositive

and the conditional are logically equivalent

$$P \to Q \quad \Leftrightarrow \quad \neg Q \to \neg P.$$

Often, replacing a conditional with its contrapostive allows for a simpler proof of the theorem at hands.

Examples of Propositions Proved by Using the Contrapositive Method

Exercise 1.4.3 *(1) Formulate the statement "if n^2 is an odd number, then so is n" in formal mathematical terms, and prove it naming the rules of inference you use for it.*

(2) Formulate in strict mathematical terms the claim "there is at most one point incident with two distinct lines". Prove the claim stating the rules of inference you use for that.

[Proof. We leave the formal statement to the reader. Here $P =$ "$l \neq m$", and $Q =$ "l and m share no more than one point in common". We have then that $\neg P =$ "$l = m$", and $\neg Q =$ "l and m share at least two points in common". We will show, using direct method, that $\neg Q \to \neg P$ is true. To this end, assume $\neg Q$ is true. This means that there are two distinct points, A and B, such that $A \sim l \wedge B \sim l$ as well as $A \sim m \wedge B \sim m$. From Axiom 1 of Plane Geometry we get that there is only one line incident with two distinct points. In particular $l = m$. So $\neg P$ is true. This finishes the proof.]

1.4.5 Method of Proof by Contradiction (Reductio Ad Absurdum - RAA)

This is a very often used method of proof. It is based on the tautology

$$((\neg R) \to F) \to R,$$

we encountered and discussed earlier. Using this method amounts to showing that if $\neg R$ is true, this would lead us to finding a contradiction (proving this way that $\neg R \to F$ is true, and therefore, by the tautology above, that R is true).

To show how this method is a particular case of proof by contrapositive, recall that the goal here is to prove R (is true). For this, as we know, one has to prove the conditional

$$T \to R$$

(is true). The contrapositive of this conditional is

$$\neg R \to F$$

which is exactly what we prove (using direct method) in the proof by contradiction.

Notice that F stands for (some) false proposition, such as $S \wedge \neg S$, and we actually prove that

$$\neg R \to S \wedge \neg S$$

(is true). Schematically, we have

$$\neg R \Rightarrow \cdots \Rightarrow S \Rightarrow \cdots \Rightarrow \neg S \quad (\Rightarrow R).$$

There is one thing in this scheme which its users have to be aware of: there are "appropriate" S, and there are not that "appropriate" S to work with, and that detecting an appropriate ones depends on the skills and the experience of the person doing the proof! It is even worse, because any proposition can play the role of S. Indeed, if R is true, then its negation $\neg R$ is false, and as we know, **no matter what the proposition Q is**, the conditional $\neg R \to Q$ will be true. So, formally, one will be able to prove that $\neg R \to S$ and $\neg R \to \neg S$ are true for any S. The art here is to detect S in such a way that it is comparatively easy to prove both $\neg R \to S$ and $\neg R \to \neg S$. These are the "appropriate" propositions S to work with.

RAA for Proving $P \to Q$

The power of the method of proof by contradiction is most easy to understand when we apply it to proving $R = P \to Q$. The implementation of the tautology $\neg R \to F$ looks in this case as follows: one assumes that $\neg(P \to Q)$ is true, and proves that, for some proposition S, the contradiction $S \wedge (\neg S)$ is true as well. This absurd situation tells us that the assumption was wrong, and that $P \to Q$ is true. Note that, as we know already,

$$\neg(P \to Q) \Leftrightarrow (P \wedge \neg Q).$$

Comparing this to the direct method of proof of $P \to Q$ where one has only one hypothesis (P), we see that, assuming $\neg(P \to Q)$ is true, one gets actually one more hypothesis to work with: in addition to P, the proposition $\neg Q$ is also given to be true. Having these two hypotheses at hand, makes us much more powerful in proving things, so much so that we can even prove S and $\neg S$ for some (and theoretically - for any) S! On the other hand, if the conditional $P \to Q$ is actually false, then one will never find such an S. If several attempts to find an S such that $P \wedge \neg Q \to S \wedge \neg S$ is true fail though, it is wise to try to prove that $P \to Q$ is actually false.

Examples of Propositions Proved by Using RAA

Exercise 1.4.4 *(1) If P is any point, then there is a line l which is not incident with P. Formulate this claim in strict mathematical terms, and prove it naming the rules of inference you use for that.*

[Proof. Let $Q =$ "$(\forall P)(\exists L)(\neg(P \sim l))$". We want to show that Q is true. This is equivalent, as we know, to proving that $Q \to T$ is true. Doing this by RAA means that we assume $T \wedge \neg Q$, and show that this leads to a contradiction. Since $T \wedge \neg Q = T \wedge \neg Q \Leftrightarrow \neg Q$, we see that going by RAA, we assume $\neg Q$ and want to get to a contradiction. As we know, $\neg Q \Leftrightarrow (existsP)(\forall L)(P \sim l)$. So, what we assume is that there is a point P such that it is incident with **every line**. *We can easily show that this assumption leads to an absurd situation. Indeed, by Axiom 3 of Plane Geometry we know that there are three points, A, B, C, which are not collinear (do not belong to the same line). Our point P is not equal to at least two of these points (why?). Suppose $P \neq A$, and denote by l the line determined by A and B, and by m the line determined by A and C.By our assumption, $P \sim l$ and $P \sim m$. So that $A \sim l \wedge P \sim l$ and $l \sim m \wedge P \sim m$. By Axiom 1 of Plane Geometry we get that $l = m$. But then the points A, B and C are all incident with this line! We are done with the proof. Indeed, let $S =$ "A, B, C are three distinct non-collinear points" where A, B and C are the points provided by Axiom 3. Then, S is a true statement. We proved above that these A, B, and C are also collinear, that is, we proved that $\neg S$ is true as well.]*

(2) If l is a line, then there is at least one point P which is not incident with l. Formulate this statement on strict mathematical terms, and prove it naming the rules of inference you use for that.

(3) If P is a point, there are at least two lines incident with it. Formulate this statement on strict mathematical terms, and prove it naming the rules of inference you use for that.

(4) If n is an even number, then $n + 1$ is an odd number. Formulate this statement on strict mathematical terms, and prove it naming the rules of inference you use for that.

(5) Among two consecutive integers, that is among n and $n + 1$, one is even, and the other is odd. Formulate this statement on strict mathematical terms, and prove it naming the rules of inference you use for that.

(6) Every odd number has the form $n = 2m + 1$. Formulate this statement on strict mathematical terms, and prove it naming the rules of inference you use for that.

(7) Prove that if n^2 is even, then n is even as well. Formulate this statement on strict mathematical terms, and prove it naming the rules of inference you use for that.

(8) The sum of three odd numbers is never 0*. Formulate this statement on strict mathematical terms, and prove it naming the rules of inference you use for that. Conclude that if* a, b *and* c *are odd integers, then the equation* $aX^2 + bX + c = 0$ *has no integer solutions.*

[Proof. We are proving first that the sum of any three odd integers is never 0*. We do this using direct method (Who are the propositions* P *and* Q *here?). Let* m, n*, and* s *be odd integers. Then*

$$m = 2m_1 + 1, \quad n = 2n_1 + 1, \quad s = 2s_1 + 1$$

for some integers m_1, n_1*, and* s_1*. But then*

$$m + n + s = (2m_1 + 1) + (2n_1 + 1) + (2s_1 + 1) = 2(m_1 + n_1 + s_1 + 1) + 1 = 2a + 1$$

where $a = m_1 + n_1 + s_1 + 1$*. Therefore,* $m + n + s$ *is an odd number. Since* 0 *is even, we get that* $m + n + s$ *is never* 0*. This completes the proof of the first statement. We are proving now the second statement. This can be done using direct method too, but we will will show how to do that by using RAA. (Who are the propositions* P *and* Q *here? Who are the two hypotheses we are provided by the RAA?). So, assume that the equation* $aX^2 + bX + c = 0$ *does have an integer solution where* a, b*, and* c *are odd integers. This means that there is an integer* n *such that*

$$an^2 + bn + c = 0.$$

Equivalently, we have that $c = -an^2 - bn$*. Since* c *is odd, the integer* $-an^2 - bn$ *is odd as well. Now, there are two options for* n*: it is either even or it is odd. If* n *is even, then* n^2 *is even as well (a proven already fact), and both* an^2 *and* bn *are even. Therefore,* $-an^2 - bn$ *is even. If* n *is odd, then* n^2 *is odd as well, and both* an^2 *and* bn *are odd (remember:* a, b*, and* c *are odd by the givens!) But then* $-an^2 - bn$ *is even. This finishes the proof. (Who was the proposition* S *here?)]*

(9) Suppose* a, b, c *are integers such that* $a \neq 0, -1$*. Prove that one of the polynomials*

$$aX^2 + bX + c \quad \textit{and} \quad (a+1)X^2 + (b+1)X + (c+1)$$

has at least one non-integer root. Formulate this statement on strict mathematical terms, and prove it naming the rules of inference you use for that.

Example 1.4.1 Important one. We are proving here a fact which was known to Euclid: there is no rational number whose square is equal to 2. More professionally put, we are proving that the following proposition is true

$$(\forall x \in \mathbb{Q})(x^2 \neq 2).$$

This claim is usually formulated as *the number* $\sqrt{2}$ *is not a rational number.* Since the definition of $\sqrt{2}$ is *a positive real number whose square is* 2, we see that the two formulations are equivalent.
We will prove the claim by contradiction. To this end, assume

$$(\exists x_0 \in \mathbb{Q})(x_0^2 = 2).$$

We will see later in the course that a rational number can be represented as a **reduced** rational fraction, that is - as a quotient of two integers, $x_0 = m/n$, where n is a non-zero (actually - a positive) integer, and m and n share no positive factors different from 1 We have

$$\left(\frac{m}{n}\right)^2 = 2 \quad \Rightarrow \quad \frac{m^2}{n^2} = 2 \quad \Rightarrow \quad m^2 = 2n^2.$$

From this it follows that m^2 is even, and therefore, as we know from the exercises above, m is even as well: $m = 2m_1$. This in turn gives us

$$m^2 = 2n^2 \quad \Rightarrow \quad (2m_1)^2 = 2n^2 \quad \Rightarrow \quad 4m_1^2 = 2n^2.$$

Simplifying the last equality, by dividing by 2, we get

$$2m_1^2 = n^2$$

which tells us that n is even as well: $n = 2n_1$. But then $m = 2m_1$ and $n = 2n_1$ share a positive factor different from 1 - this contradicts the fact that m/n is a reduced fraction! □

Remark 1.4.1 The positive integers different from one which have only two divisors, 1 and themselves, are called **prime** numbers. The integer 2 is the smallest prime number. Other such numbers are $3, 5, 7, 11, 13, \ldots$. With a bit moire knowledge of the theory of numbers, one can prove that, if p is a prime number, then $\sqrt{p}$ is **not** a rational number. Moreover, it can be proved that, for any positive integer n, if $\sqrt{n}$ is not an **integer**, then $\sqrt{n}$ is not a **rational number** either. □

1.4.6 Recapitulation on Methods of Proof of $P \to Q$

As we saw in this section, every proposition in Logic, and therefore every theorem in Math, can be formulated in the form

$$P \to Q.$$

To prove this conditional is true, one needs to establish that if P is true, then Q is true. So, a proof consists of **assuming** P and **proving** Q. Making the assumption requires, of course, no much of intellectual power. The whole work goes to do the latter: proving Q (is true). This is done by using known/established already facts and the rules of inference.

In this section, we presented three basic schemes/methods of proving a conditional. Here are, once again, the differences and the similarities of these.

Suppose we have to prove $P \to Q$ (is true).

- The Direct Method of proof makes the hypothesis that P is true, and establishes that Q is true.
- The Contrapositive Method of proof does a similar thing, but applied to the conditional

$$\neg Q \to \neg P.$$

That is, the hypothesis is $\neg Q$ is true and the conclusion sought is $\neg P$ is true.

- The Method by Contradiction does also the same, but applied to the conditional

$$P \wedge \neg Q \to F.$$

That is, the hypothesis is $P \wedge \neg Q$ is true, and the conclusion sought is $S \wedge \neg S$ is true for an appropriate S.
So, in all three methods of proof, one makes a hypothesis, and proves a conclusion employing the rules of inference and already established facts in order to achieve that.

A proof of $P \to Q$, as we have experienced in doing the exercises in this section, consists of proving a chain of (intermediate) conditionals

$$P \to Q_1 \quad P_1 \to Q_2 \quad \cdots \quad P_n \to Q.$$

Decent proofs, designed to establish deep theorems in math, may consist of hundreds and even of thousands intermediate conditionals! Each of these latter are established using the three methods of proof (and the method of math induction discussed in detail in Chapter 3 of these Notes).

Chapter 2

Sets

We are introducing in this chapter, comparatively rigorously, the rudiments of Set Theory. The rest of the course heavily depends on these rudiments: Our point of vie is that every object we define in Math (such as function, numbers, relations etc.) has to be a set. In our presentation, we will rely on some reasonable intuition as well: the formal introduction of these concepts is a subject of courses on Set Theory taught at FIU.

2.1 Undefined Terms, First Axioms

Sets, denoted by $X, Y, \ldots$, are intuitively **collections of objects having some common features**. Notations used to denote such a collection

$$\mathfrak{A} = \{\mathfrak{z} \,|\, \varphi(\mathfrak{z})\}$$

where φ is a formula defining the property the elements of the collection $\mathfrak{A}$ have.
Mathematically, the situation is a bit more formal.

- We do not define what sets are. They just are.
- There is one relation between sets: the relation "belong(s) to", denoted by $\in$. We write $x \in X$ and read "**(the collection)** x **is an element of the collection** X".

The slogan here would be that "there is nothing else, but sets". That is, the elements of sets are also sets! The negation $\neg(x \in X)$ is denoted by $x \notin X$.

The situation is actually a bit more complicated: the right slogan is that "everything is a CLASS". Collections defined by certain features they possess are not sets in general, they are called **classes**. Some of the classes are sets. To distinguish between classes and sets in our considerations, we say that **sets are classes that exist**. We also refer to the classes which are not sets (so, they do not exist) as **proper classes**.

The "existence" of some classes is based on the axioms we use to build Set Theory. It is important to emphasize here that the **collections we consider are collections of sets**. But some collections may be proper classes.

The collection of all sets will be denoted by Ω. **The variables in the propositional functions we will be using in the axioms and definitions below take on values in the collection of sets** Ω.

All that said, we are not sure, as of now, if sets exist at all! To make sure they do exist, we need an axiom (the way to go in math). Although the theory can be built by accepting the existence

of a set without any further specifications thereof, we choose to postulate the existence of a special set. In the other approach, it is **proved** that this special set exists!

Definition 2.1.1 *A set with no elements in it is called* **empty set**.

Axiom 1 (*Empty Set Axiom*) *There is a set with no elements in it.*

We denote the set from this axiom with $\emptyset$.

Axiom 1 says that empty sets exist. We can not tell at this moment how many these sets are. With the help of some other axioms we will prove shortly that **the empty set is unique.**

Having assured the sets exist (at least one does!), we would like to know how to work with sets - what new sets we can construct by using old ones. We begin with the definition of a subset

Definition 2.1.2 *Given two sets X and Y, the set X is a subset of the set Y, we write $X \subseteq Y$, if* $(\forall x)(x \in X \to x \in Y)$.

Exercise 2.1.1 *(1) Prove that, for every set X, $X \subseteq X$.*
(2) Prove that $(\forall X)(\forall Y)(\forall Z)(X \subseteq Y \wedge Y \subseteq Z \to X \subseteq Z)$.

Suppose we have the two inclusions: $X \subseteq Y$ and $Y \subseteq X$. What can we say about X and Y? Yes, they have the same elements, and one may be tempted to say that $X = Y$, that is, that the two sets are identical. But that may not be the case in general! (For example, it may happen that some elements of a set are repeated, and that two sets may have the same elements, but repeated different number of times. Such sets need not be considered different in general!) We need an axiom to resolve such issues in the theory we are building!

Axiom 2 (*Extensionality Axiom*) *If two sets have the same elements, they are identical . In other words*

$$(\forall X)(\forall Y)((X \subseteq Y) \wedge (Y \subseteq X) \to (X = Y)).$$

This axiom says, in particular, that the collections we consider are insensitive to having repeated elements in themselves. For instance the sets (we will soon prove these are sets!) $\{a, b\}$ and $\{a, a, b\}$, although having different number of elements, **are identical for the theory we are developing**.

We should be aware though that sets with repeated elements appear naturally, and are widely used, in mathematics. To resolve this apparent issue, one develops the theory of **multi-sets**. We will briefly discuss this later on in the course in relation with **indexed families** of sets.

Definition 2.1.3 *The set X is a* **proper subset** *of the set Y, denoted by $X \subsetneqq Y$, if*

$$(X \subseteq Y) \wedge \neg(X = Y).$$

The negation $\neg(X = Y)$ is abbreviated, as we know, to $X \neq Y$.

Here are two theorems that can be proved at this early stage of development of Set Theory. These reveal important properties of the empty set $\emptyset$.

Theorem 2.1.1 *An empty set is a subset of every set.*

Proof. Suppose Y is an empty set (a set with no elements). According to the definition of subset, we have to show that

$$(\forall x)((x \in Y) \to (x \in X)).$$

Since the premise of the conditional in the proposition is false, this proposition is (we say **vacuously**) true. We are done. □

Theorem 2.1.2 *The empty set is unique: if X is an empty set, then $X = \emptyset$.*

Proof. To prove this theorem we will make a use of Axiom 2 after showing that $X \subseteq \emptyset \wedge \emptyset \subseteq X$. According to the definition of subset, we have to show that

$$(\forall x)((x \in X) \to (x \in \emptyset)) \quad \wedge \quad (\forall x)((x \in \emptyset) \to (x \in X)).$$

Both premises of the conditional formulae in the previous line are false: neither $\emptyset$ nor X have any elements! Therefore, both conditionals are **vacuously** true, and the universally quantified propositions are both true as well. □

We can not be sure, with the axioms we have so far, that there is a set different from the empty set. Here is an axiom which helps us overcome this inconvenience.

Axiom 3 (*Power Set Axiom*) *The collection of all subsets of a set X is a set itself, called the* **power set** *of X. In more technical terms*

$$(\forall X)(\exists Y)(\forall z)((z \in Y) \leftrightarrow (z \subseteq X)).$$

Exercise 2.1.2 *Use Axiom 2 to prove that the set Y in Axiom 3 is unique. That is if W has the same property as Y from Axiom 3, then $Y = W$.*

Notation We denote the set Y in Axiom 3 by $\mathcal{P}(X)$.

As a corollary of the Theorem 2.1.1 we get that there are sets different from the empty set.

Corollary 2.1.3 $(\forall X)(\mathcal{P}(X) \neq \emptyset)$. *More precisely,* $(\forall X)(\emptyset \in \mathcal{P}(X) \wedge X \in \mathcal{P}(X))$.

Proof. By the cited theorem, $\emptyset \subseteq X$, so that $\emptyset \in \mathcal{P}(X)$. This means that $\mathcal{P}(X)$ has at lest one element, and therefore is not empty! □

Having the power sets at our disposal, we can construct plenty of sets: $\mathcal{P}(\emptyset), \mathcal{P}(\mathcal{P}(\emptyset)), \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$, etc.

Exercise 2.1.3 *(1) List the elements of the sets $\mathcal{P}(\emptyset), \mathcal{P}(\mathcal{P}(\emptyset)), \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.*
[Hint: $\mathcal{P}(\emptyset)$ is a set having only one element - the empty set itself. So $\mathcal{P}(\emptyset) = \{\emptyset\}$. The set $\mathcal{P}(\mathcal{P}(\emptyset))$ consists of the subsets of the set $\{\emptyset\}$. There are only two such: $\emptyset$, and $\{\emptyset\}$. Note that the last two are really sets: the former - by Axiom 1, and the latter - by Axiom 3. So, $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$. Turning to the set $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$, we have to be careful! Here is why. We see that the sets $\emptyset, \{\emptyset\}$, and $\{\emptyset, \{\emptyset\}\}$ are subsets of $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$. Note that all the three are indeed sets! Are there more subsets? It is kind of obvious that $\{\{\emptyset\}\}$ is also a subset. But why is it a set, to start with? We do not have means to prove that now. For this, we need one more axiom - the Pairing Axiom, to be introduced below. So, finish the argument here using that Axiom!]
(2) Prove that $(\forall X)(\forall Y)(X \subseteq Y \to \mathcal{P}(X) \subseteq \mathcal{P}(Y))$, and that $(\forall X)(\forall Y)(X \subsetneqq Y \to \mathcal{P}(X) \subsetneqq \mathcal{P}(Y))$.

The next axioms tell us how to construct even more sets starting from given ones.

Axiom 4 (*Pairing Axiom*) *Given two sets X and Y, there is a set with only elements X and Y. That is, we have*

$$(\forall X)(\forall Y)(\exists Z)(\forall w)(w \in Z \ \leftrightarrow \ w = X \ \vee \ w = Y).$$

Exercise 2.1.4 *Prove, using Axiom 2, that the set Z the existence of which is declared in Axiom 4 is unique.*

We denote this set by $\{X, Y\}$.
In particular, given the set X, there is the set $\{X, X\}$. We denote this set by $\{X\}$, and consider it as a set of only one element.
In general, we call a set with only one element, respectively two (distinct) elements, a **singleton**, respectively - a **doubleton**. It follows from Axiom 4 that for every **set** X, there is a singleton with element X, and that for every two distinct sets X, Y, there is a doubleton with elements X and Y. By using Axiom 2 one easily shows that the singletons and the doubletons with prescribed elements are unique.

In order to be able to construct more sets, we need more axioms. Here is one.

Axiom 5 (*Union Axiom*) *Given a set X, there is a set Y with elements - the elements of the elements of X:*

$$Y = \{z \,|\, (\exists x)(x \in X \wedge z \in x)\}.$$

Exercise 2.1.5 *Prove that the set Y above is unique.*

The set Y is denoted by $\cup X$, and is called the **union of** X. So we have

$$\cup X = \{z \,|\, (\exists x)(x \in X \wedge z \in x)\}.$$

As an example, $\cup\{X\} = X$.

Exercise 2.1.6 *Prove that indeed, for any singleton $Y = \{X\}$, we have $\cup Y = X$.*

As another example, for any two sets X and Y, we have

$$\cup\{X, Y\} = \{z \,|\, z \in X \vee z \in Y\}$$

is a set. We denote the latter by $X \cup Y$ and call it the **union** of X and Y.

Exercise 2.1.7 *(1) Using Axiom 2, Axiom 4, and Axiom 5 prove that, given sets X, Y and Z, there is a unique set with elements exactly X, Y, and Z. We denote this set by $\{X, Y, Z\}$.*
(2) Compute the power set of the set $\{X, Y, Z\}$. Give arguments for your answer.

By the way, it is only after this exercise that we are able to prove that the example of sets we used after Axiom 2 is a correct one. Indeed, denote by $a = \emptyset$ and $b = \{\emptyset\}$ (by the way, $b = \mathcal{P}(\emptyset)$). Then the **sets** $\{a, b\}$, and $\{a, a, b\}$ exist. By Axiom 2 the two sets are equal.

The following axiom is very powerful, and also important. To give an idea why this power and importance, recall that the classes are defined by using a feature their elements have. In notations

$$\mathfrak{A} = \{\mathfrak{z} \,|\, \varphi(\mathfrak{z})\}$$

where φ is a formula encoding the feature.
There are two things that we have to be aware of here. The first one is the formula **has to be constructed in a special way**. The explanation of this goes beyond the scope of these notes, and the reader who wants to learn more about it is referred to any (decent) course on foundations of mathematics. Suffices it to say here that in these notes we use correctly constructed from this point of view formulae.
The second thing we have to be aware of, and be careful with, is that even when the formulae are correctly constructed, the collection they define while being a class may or may not be a set. The Axiom 4, and the Axiom 5 for instance assure that when one uses the formulae

$$\varphi(\mathfrak{z}) = "\mathfrak{z} = X \vee \mathfrak{z} = Y" \qquad \varphi(\mathfrak{z}) = "(\exists x)(x \in X \wedge \mathfrak{z} \in x)"$$

the corresponding classes are sets.

Exercise 2.1.8 *Find the formulae used in Axiom 1, and Axiom 3.*

Example 2.1.1 Here is a classical example showing that in general the collection defined by a formula is a proper class. This example was discovered by Georg Cantor, the father of Set Theory, popularized later on by Bertrand Russell, and commonly known as the Russell's paradox. Define the collection

$$M = \{z \,|\, z \notin z\}.$$

This collection **can not** be a set! Indeed, if it were a set, then either $M \in M$, and therefore $M \notin M$, or $M \in M$, and therefore $M \notin M$. (As an exercise, convince yourselves that the previous line is correct mathematically!). So, M is a proper class. It is called **Russell's class**. □

We just proved, by example, that **not every class, a collection defined by a formula, is a set**. The following axiom helps us avoid situations when the class defined by a formula does not exist.

Here is the promised axiom. It gives a safe way for determining if a class is a set.

Axiom 6 (*Separation Axiom*) *If X is a set, and if $P(x)$ is a propositional function, then the collection*

$$\{z \,|\, (z \in X) \wedge (P(z)\}$$

is a set.

The first thing we are doing after introducing Axiom 6 is to *prove* **that intersections of sets exist**. We have the following theorem

Theorem 2.1.4 *Let $X \neq \emptyset$. Then there is a unique set Y such that*

$$(\forall z)(z \in Y \leftrightarrow (\forall x)(x \in X \rightarrow z \in x)).$$

We denote this set by $\cap X$, and call it the **intersection of** *X.*

Proof Since $X \neq \emptyset$, there is an $x_0 \in X$. Then we have

$$(\forall x)(x \in X \rightarrow z \in x) \Leftrightarrow (z \in x_0) \wedge (\forall x)(x \in X \rightarrow z \in x),$$

and then by Axiom 6 the collection Y is a set. The uniqueness of Y is proved by using Axiom 2 in a standard way, and is left to the reader as an exercise. □

Exercise 2.1.9 *Prove that $\cup \emptyset = \emptyset$ while $\cap \emptyset = \Omega$. So the latter class doesn't exist!*

Definition 2.1.4 *For any two sets, X, Y, the set $\cap\{X, Y\}$ is called the* **intersection** *of X and Y, and is denoted by $X \cap Y$. The sets X and Y are called* **disjoint** *if $X \cap Y = \emptyset$.*

So, we have $X \cap Y = \{z \,|\, z \in X \wedge z \in Y\}$.

The next axiom states that Ω, the collection of all sets, is the same as the Russell's class M.

Axiom 7 (*Russell's Class Axiom*) *No set is a member of itself:*

$$(\forall x)(x \notin x).$$

This axiom allows us to write (keep in mind that the variables in all our propositional formulas are sets!)

$$\Omega = \{x \,|\, x \notin x\}.$$

This exactly means that Ω is "the same as" the Russell's class M above. (Note that formally we know how to compare sets only. This is why "the same as" is in quotation marks. In the end of this chapter we explain how to compare classes as well. Turns out $\Omega = M$.)

Remark 2.1.1 (**Truth Sets** revisited) Now, after we know things about sets, it's time to revisit our discussion of the **truth set** of a propositional expression. The truth "sets" were defined as the collections of all members of the corresponding universes of discourse which satisfy some restriction, e.g., for which the expression was true. But we have to be careful when the universe of discourse is a proper class. For instance, if we define $P(x) =$ "$x \notin x$", then we have (b/c of Axiom 7)

$$\{z \,|\, P(z)\} = \Omega$$

which as we now know is **not** a set! Axiom 6 ensures that when the universe of discourse is a set, then the things are nice: the truth set **is** a set. □

By using the above axioms, one can exhibit important constructions of sets. Here is a typical one: the successor of a set.

Definition 2.1.5 *Given a set X, the set $S(X) = X \cup \{X\}$ is called the* **successor** *set of X.*

Exercise 2.1.10 *Prove that for every set X, the successor $S(X)$ is really a set.*

It is the successor which allows us, in particular, to define the **natural numbers**! So, as everything that exists in math, the natural numbers are sets. Indeed, we have

$$\emptyset, \quad S(\emptyset) = \{\emptyset\}, \quad S(S(\emptyset)) = \{\emptyset, \{\emptyset\}\}, \quad S(S(S(\emptyset) = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \quad \ldots$$

are the sets usually, for short, denoted by $0, 1, 2, 3$, etc.
In these notations, we have that

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

The class of all natural numbers is denoted by $\mathbb{N}$.

Note that the natural numbers have the following special properties (verify these - Exercise).

• **an element of a natural number is either an empty set or is a successor of an element of that number**;

• **every element of a natural number is also a subset of that number**.

Both properties are important in characterizing the natural numbers (as we will see shortly), but the second one turns out to be very useful in developing Set Theory. It has a name:

Definition 2.1.6 *The set X is called* **transitive** *if every its element is also a subset of X:*

$$(\forall z)(\, z \in X \to z \subseteq X).$$

Exercise 2.1.11 *Prove that $\emptyset$ is a transitive set.*

So, the natural numbers defined above are transitive sets.

Exercise 2.1.12 *(1) Prove that if X and Y are transitive sets, then so are $X \cup Y$ and $X \cap Y$.*
(2) Prove more generally that
(i) if X is a set with elements transitive sets, then $\cup X$ is a transitive set as well, and that
(ii) if $X \neq \emptyset$ is a set with elements transitive sets, then $\cap X$ is a transitive set.

Using Axiom 6, one defines several sets out of given ones. Here are two examples.

Definition 2.1.7 *Given two sets, X and Y, the* **relative complement** *$X \setminus Y$ of Y in X is defined by*

$$X \setminus Y = \{z \,|\, z \in X \wedge z \notin Y\}.$$

Note: there is no complement of a set in Ω! (Exercise: Prove this!). So, "absolute" complements to a set do not exist (as sets, of course). But if we agree to call universe some (very big) set, containing all the sets we work with, then this "absolute" complement exists as well. This follows from Axiom 8 as well.

Definition 2.1.8 *Given two sets X and Y, their* **symmetric difference** $X \oplus Y$ *is defined by*

$$X \oplus Y = \{z \,|\, z \in X \cup Y \wedge z \notin X \cap Y\}.$$

It is important to note at this stage that having in disposal only the Axioms 1 - 7, we are not able to construct sets beyond the realm of **finite** sets (The proper definition of finite set will be given when we discuss pollency of sets. For now, we use our intuitive understanding of these as sets having finitely many elements.) In particular, we are not able to prove that the class of natural numbers $\mathbb{N}$ is a set (in our earlier terminology, we are not able to claim that the class $\mathbb{N}$ exists). To make this happen, we need an axiom.

Axiom 8 (*Infinity Axiom*) *There is a set X such that $\emptyset \in X$ and $(\forall x)(x \in X \to S(x) \in X)$.*

A set satisfying Axiom 8 is called **inductive**. It can be proved (Do that as an exercise!) that **all natural numbers belong to every inductive set**. Moreover, the natural numbers in any such set **can be distinguished by a formula**. Recall that the natural numbers have the following two properties: they are transitive sets, and every element of a natural number is either the empty set or is a successor of a set. So, a formula distinguishing the natural numbers in an inductive set is the following

$$P(x) = "(x = \emptyset) \vee ((\forall z)((z \in x) \to ((z \subseteq x) \wedge (z = \emptyset \vee (\exists y)(y \in x \wedge z = S(y)))))".$$

By Axiom 6 then, we get that the class $\mathbb{N}$ exists: **the collection of natural numbers is a set**.

Note that the set $\mathbb{N}$ satisfies Axiom 8. So, $\mathbb{N}$ is an inductive set, and, as we saw, it has the distinguishing property of **being a subset of every inductive set**.

Remark 2.1.2 Often Axiom 8 is stated by simply postulating that the class of natural numbers $\mathbb{N}$ is a set. $\square$

2.2 The Algebra of Sets

In this subsection, we list, and prove as exercises most of them, the main properties of the operations $\cap, \cup, \setminus, \oplus$. These should be compared to the properties of $\wedge, \vee, \neg$ and XOR respectively.

Theorem 2.2.1 *For any given sets X, Y, Z the following holds true.*

$$X \cup X = X \quad X \cap X = X \quad X \cup \emptyset = X \quad X \cap \emptyset = \emptyset \quad X \cup \Omega = \Omega \quad X \cap \Omega = X;$$

Commutativity and associativity

$$X \cap Y = Y \cap X \quad X \cap (Y \cap Z) = (X \cap Y) \cap Z$$

$$X \cup Y = Y \cup X \quad X \cup (Y \cup Z) = (X \cup Y) \cup Z;$$

Distributivity

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z) \qquad X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z);$$

De Morgan laws

$$X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z) \qquad X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z).$$

Proof. Most of these claims are straightforward, and even trivial, to prove. Use defining formulae. □

Exercise 2.2.1 *Prove the identities in Theorem 2.2.1.*

Exercise 2.2.2 *Prove that*

$$(A \setminus B) \setminus C = A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$$

while

$$A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C) = (A \setminus B) \cup (A \cap B \cap C).$$

Conclude that the operation relative complement "$\setminus$" is **not** *associative in general. [A binary operation $*$ on a set X is called associative if $(a * b) * c = a * (b * c)$.]*

Exercise 2.2.3 *This exercise, in addition to the theorem above, proves that the operations $\oplus$ and $\cap$ have the same properties as addition,$+$, and multiplication,$\cdot$, for (integer) numbers as we know them from school. The roles of 0 and 1 are played by $\emptyset$ and Ω respectively. Namely, prove that*

$$X \oplus Y = Y \oplus X \qquad X \oplus (Y \oplus Z) = (X \oplus Y) \oplus Z \qquad X \oplus X = \emptyset$$

$$X \cap (Y \oplus Z) = (X \cap Y) \oplus (X \cap Z).$$

[For the associativity of $\oplus$ prove that both sides of the equality are equal to

$$(X \setminus (Y \cup Z)) \cup (Y \setminus (X \cup Z)) \cup (Z \setminus (X \cup Y)) \cup (X \cap Y \cap Z).$$

Thus, for the LHS of the equality we have

$$\begin{aligned}(X \oplus Y) \oplus Z &= ((X \oplus Y) \setminus Z) \cup (Z \setminus (X \oplus Y)) \\ &= (((X \setminus Y) \cup (Y \setminus X)) \setminus Z) \cup (Z \setminus ((X \cup Y) \setminus X \cap Y)) \\ &= (((X \setminus Y) \setminus Z) \cup ((Y \setminus X) \setminus Z)) \cup (Z \setminus ((X \cup Y) \setminus (X \cap Y))) \\ &= ((X \setminus (Y \cup Z)) \cup (Y \setminus (X \cup Z))) \cup ((Z \setminus (X \cup Y)) \cup (X \cap Y \cap Z)).\end{aligned}$$

Do the needed manipulations to the RHS of the equality to get the same expression.]

Remark 2.2.1 The diligent student may have (actually - should have!) noticed that the above interpretation of the **class** Ω as the identity element for the operations $\oplus$ and $\cap$ is not correct: Ω doesn't exist (it's a proper class)! Even more than that: having defined intersection (and unionisation) for sets only, how should we understand $X \cap \Omega$ (and $X \cup \Omega$ as well)? This is answered the following way. Recall that classes are collections of sets having a common property. This property is given by a propositional function (a formula). For instance, the class Ω is defined by the formula "$x \notin x$". Then, the union and intersection of classes can be described by formulae as well. Thus, we have

$$X \cup \Omega = \{x \,|\, x \in X \vee x \notin x\} \qquad X \cap \Omega = \{x \,|\, x \in X \wedge x \notin x\}.$$

Now, X being a set, we get that

$$x \in X \vee x \notin x \quad \Leftrightarrow \quad x \notin x,$$

and therefore

$$X \cup \Omega = \{x \,|\, x \notin x\} = \Omega$$

and we see that a union of a set and a class is not a set in general. Actually such a union is a set if, and only if the class is a set as well (Why?).
The case of intersection of a set and a class is much more gentle - by Axiom 6 it always exists! Direct computation shows that $X \cap \Omega = X$.
In any case, if we don't want to work with proper classes at all, we can consider the family (set!) of all subsets of a fixed set X and apply the operations under discussion to the members of this set only. It is straightforward that all operations on sets we have introduced so far applied to subsets of X produce subsets of X, so that they are well defined in $\mathcal{P}(X)$. In this setting, $\emptyset$ plays the role of 0, and X - of 1 for the operations $\oplus$ and $\cap$. □

2.2.1 A Bit More on Classes

Working with classes is not the same as working with sets. Not all constructions possible for sets are possible for classes! We are listing here some of those which extend to the realm of classes.

The classes are defined by a property, given by a formula

$$\mathfrak{A} = \{\mathfrak{z} \,|\, \varphi(\mathfrak{z})\}.$$

Since we consider only collections of sets, $\mathfrak{z}$ is a set.

We say that the **set** x is an element of the class $\mathfrak{A}$, and write $x \in \mathfrak{A}$ if the proposition $\varphi(x)$ is true.

Suppose $\mathfrak{A}$ and $\mathfrak{B}$ are classes, defined by the formulae φ and ψ respectively. We say that $\mathfrak{A}$ is a sub-class of $\mathfrak{B}$, and write $\mathfrak{A} \subseteq \mathfrak{B}$, if

$$(\forall x)(x \in \mathfrak{A} \to x \in \mathfrak{B}),$$

that is, if $\varphi(x) \to \psi(x)$ is a true proposition.
We say that $\mathfrak{A} = \mathfrak{B}$ if both $\mathfrak{A} \subseteq \mathfrak{B}$ and $\mathfrak{B} \subseteq \mathfrak{A}$. Equivalently, $\mathfrak{A} = \mathfrak{B}$ if $\varphi \Leftrightarrow \psi$.

Similarly, **union** and **intersection** of classes are defined using disjunction and conjunction of formulae, respectively. In the notations above we thus have

$$\mathfrak{A} \cup \mathfrak{B} = \{x \,|\, \varphi(x) \vee \psi(x)\} \qquad \mathfrak{A} \cap \mathfrak{B} = \{x \,|\, \varphi(x) \wedge \psi(x)\}.$$

This definition can easily be extended to the case when the classes are finitely many. This can even be done for "bigger" families of classes, using the corresponding existential and universal quantifications, but we are not going that way in this course. We can also define relative complements, and simmetric difference of classes: just use the corresponding logical operations on the formuale defining the classes.

These definityions show us that the algebra of classes is actually equivalent/identical to the algebra of logical expressions. But remember that sets are the only classes that exist! These are the classes that matter for math, and this is why the theory of sets is more interesting and harder than the theory of classes (that is, via the defining formulae, more interesting than Logic).

Chapter 3

Properties of $\mathbb{N}$

The set $\mathbb{N}$ of natural numbers was introduced in the previous chapter using the most important set, $\emptyset$, and the operation successor. It was established there that $\mathbb{N}$ has interesting properties:

- $\mathbb{N}$ is an inductive, and a transitive set which is a subset of any inductive set
- every non-zero natural number is the collection of all natural numbers constructed before it (by the successor operation).

The first objective of this chapter is to define a relation $\leq$ on the elements of $\mathbb{N}$, and to show that it satisfies the **Least Element Principle (LEP)**. This important property of $(\mathbb{N}, \leq)$ is equivalent, as we prove here, to the **Principle of (Finite) Mathematical Induction (P(F)MI)** which is the basis of a method of proving some universally quantified propositions. It also allows us to use **recursion** in constructing sets. As an application of recursion we define two (arithmetic) operations, addition $+$, and multiplication $\cdot$ on $\mathbb{N}$, and prove that they have properties familiar from the arithmetic classes in elementary school. All this is done in Section 3.1 through Section 3.4.

In Mathematics, and in everyday life, the natural numbers are used for arithmetic purposes. It is not important how they are constructed. Rather, the emphasis is on what we can do using the relation $\leq$, and the operations $+$ and $\cdot$. So, in a sense, the **explicitly constructed set $\mathbb{N}$ is not what natural numbers really are**. We use in Section 3.4 the properties of $\leq, +$, and $\cdot$ to design a **definition** of natural numbers. We show there that the set $\mathbb{N}$ is an example of a set of natural numbers, and that **any other such set is unambiguously identifiable with $\mathbb{N}$**.

We close the chapter, Section 3.5, with two statements proved by P(F)MI.

3.1 The Least Element Principle (LEP) for $\mathbb{N}$

We introduce here the relation $\leq$, and discuss the important property of the relation $\leq$ on $\mathbb{N}$ that it satisfies the LEP.

3.1.1 Ordering of the Elements of $\mathbb{N}$

The method of finite induction is based on a property of the natural numbers: the natural numbers can be compared. This leads to introducing a **relation** on $\mathbb{N}$. The notion of relations between sets will be discussed in much details later in Chapter 4. What we do here will there be considered as an important example of a relation.

Definition 3.1.1 *Let $m, n \in \mathbb{N}$. We say that n* **is less than or equal to** *m, and write $n \leq m$, if $(n \in m) \vee (n = m)$. We say that n* **is less than** *m, and write $n < m$, if $n \leq m \wedge n \neq m$.*

Exercise 3.1.1 *Prove that, for $m, n \in \mathbb{N}$, we have*

$$n \in m \quad \Leftrightarrow \quad S(n) \in S(m).$$

[($\Rightarrow$) Since $n \in m$, there is an $m' \in \mathbb{N}$ such that $m = S(m')$. Therefore, $m = \{0, \ldots, m'\}$. Note that all elements of m, different from m', have successors in m. Now, there are two options for $n \in \{0, \ldots, m'\}$: either $n = m'$, and therefore $S(n) = S(m') = m \in m \cup \{m\} = S(m)$, or $n \neq m'$ and therefore $S(n) \in m \subset S(m)$. In both cases $S(n) \in S(m)$.

($\Leftarrow$) $S(m) = \{0, \ldots, m\}$, and every element of $S(m)$, different from 0, is a successor of an element of $S(m)$. Since $0 \neq n \cup \{n\} = S(n)$, and having assumed that $S(n) \in S(m)$, it follows that $n \in S(m)$ being the element whose successor is $S(n)$. We get $n \in m$ because $n \neq m$.]

This exercise shows in particular that $S(n) = S(m)$ only if $n = m$.

As usual, $\neg(n \leq m)$ and $\neg(n < m)$ are abbreviated to $n \nleq m$ and $n \not< m$ respectively.

Note that, since the natural numbers are transitive sets

$$n \in m \rightarrow m \notin n.$$

Exercise 3.1.2 *Prove the claim just made!*

The following proposition proves that the relation $\leq$ is a **partial order** on $\mathbb{N}$ In the next chapter, we will discuss relations on sets in general, and partial od=rders in particular.

Proposition 3.1.1 *For any three natural numbers m, n, and s, we have*
(1) $n \leq n$;
(2) $(n \leq m) \wedge (m \leq n) \rightarrow (n = m)$;
(3) $(n \leq m) \wedge (m \leq s) \rightarrow (n \leq s)$.

Proof (1) Let $n \in \mathbb{N}$. Since $n = n$ is true, then $n \in n \vee n = n$ is also true. Therefore, $n \leq n$.
(2) To prove this item, it is enough to show that if for two natural numbers n and m the proposition $(n \leq m) \wedge (m \leq n)$ is true, then $n = m$. The proposition $(n \leq m) \wedge (m \leq n)$ being true means that $(n \in m \vee n = m) \wedge (m \in n \vee m = n)$ is true. This is equivalent to the following disjunction of four propositions being true

$$(n \in m \wedge m \in n) \vee (n \in m \wedge m = n) \vee (n = m \wedge m \in n) \vee (n = m \wedge m = n).$$

We know already (from the exercise above) that $n \in m$ implies that $m \notin n$. Therefore, the first of the fours propositions is false. The second and the third propositions are false too due to Russell's Axiom (how?). It follows that the fourth proposition $n = m$ is true as needed.
(3) Let now n, m, and s be natural numbers for which $(n \leq m) \wedge (m \leq s)$ is true. We have to show that $n \leq s$ is true as well. Our assumption is equivalent to the following disjunction of four propositions being true

$$(n \in m \wedge m \in s) \vee (n \in m \wedge m = s) \vee (n = m \wedge m \in s) \vee (n = m \wedge m = s).$$

We consider the four propositions separately, and show that each of them implies the desired $n \leq s$. Since natural numbers are transitive sets, we have that $m \in s$ implies $m \subseteq s$. If in addition $n \in m$, then $n \in s$ as well. Therefore, $(n \in m \wedge m \in s)$ implies $n \leq s$.
Everyone of the second and the third propositions immediately implies that $n \in s$, and so $n \leq s$.
The last proposition implies $n = s$, so that again $n \leq s$. Item (3) is proved as well. $\square$

It turns out that every two natural numbers are $\leq$-comparable. Before proving this, let's make some observations regarding the natural numbers.

Lemma 3.1.2 *(1) Let $n \in \mathbb{N}$ and $s, p \in n$. Then either $s = p$ or $s < p$, or $p < s$.*
(2) Let $m, n \in \mathbb{N}$. Then there is $p \in \mathbb{N}$ such that $p = n \cap m$. That is, the intersection of two natural numbers is a natural number itself.

Proof (1) The claim is vacuously true if $n = 0$, and is obvious when $n \neq 0$ since, in this case, $n = S(n')$ is a successor of a natural number, and is therefore given by $n = \{0, 1, \ldots, n'\}$. By the very definition of the natural numbers, we have that the elements of n are $\leq$-comparable.

(2) The claim is obviously true if $n = 0$ or $m = 0$, because in this case $n \cap m = \emptyset$ is a natural number. Let's assume that $n \neq 0$ and $m \neq 0$. By item (1), every two elements of $n \cap m$ are $\leq$-comparable. Therefore, there is an element, $p' \in n \cap m$ which is the biggest there. Since $p' \in n$ and $p' \in m$, and since natural numbers are transitive sets, we have that $p' \subseteq n$ and $p' \subseteq m$. So, $p' \subseteq n \cap m$. We claim now that $n \cap m = S(p')$. Indeed, since $p' \in n \cap m$ and $p' \subseteq n \cap m$, we have that $S(p') \subseteq n \cap m$. On the other hand, p' is the largest in $n \cap m$ which implies that every element in the intersection different from p' should be less than it, and therefore should be in p'. We conclude that $n \cap m \subseteq S(p')$ as well. This proves our claim. Denoting $p = S(p')$, we get $n \cap m = p \in \mathbb{N}$. $\square$

Proposition 3.1.3 *The following statement is true (a* **dichotomy property***)*

$$(\forall n, m)((n \leq m) \vee (m \leq n)).$$

Proof Consider the natural number $p = n \cap m$. We will prove now that $p = n$ or $p = m$. The latter is obviously true if $n = 0$ or $m = 0$. So, W.L.O.G. we may assume that $n \neq 0$ and $m \neq 0$. In this case, $p = S(p')$ where p' is the largest element of $m \cap n$. Arguing by contradiction now, assume that $p \neq n$ and $p \neq m$. In this case there are $n' \in n \setminus p$ and $m' \in m \setminus p$. Since every two elements of a natural number are $\leq$-comparable, and since $m', n' \notin p$, we get that $p \leq m'$ and $p \leq n'$. Now, if $p = m'$, then $m' \leq n'$ which implies that either $m' = n'$ or $m' \in n'$, in both cases $m' \in n \cap m = p$, and so $m' < p$ which is impossible. Similarly, $p \neq n'$. Therefore, $p < n'$ and $p < m'$ which means that $p \in m' \cap n'$. Noticing that $n' \cap m' \subseteq n \cap m$, we get that $p \in n \cap m = p$ which contadicts the Russell's class axiom. This completes the proof that either $p = m$ or $p = n$. This means that either $m \subseteq n$ or $n \subseteq m$. This precisely means in turn that either $m \leq n$ or $n \leq m$. $\square$

The relation $\leq$ has an important property which, as we will see in the next section, allows the principle of math induction to be a valid method of proof. Namely, we have

Theorem 3.1.4 *Every non-empty subset of $\mathbb{N}$ has a least element*

$$(\forall X)(((X \neq \emptyset) \wedge (X \subseteq \mathbb{N}))) \rightarrow (\exists z)((z \in X) \wedge ((\forall w)(w \in X \rightarrow z \leq w))).$$

Proof Since X is a non-empty subset of $\mathbb{N}$, there is a natural number $m \in X$. Consider the set $m \cap X$. There are two options for $m \cap X$: it is either $\emptyset$, or it is distinct from $\emptyset$. If $m \cap X = \emptyset$, then all elements smaller that m, being elements of m, are not in X. This exactly means that m is the least element of X. If $m \cap X \neq \emptyset$, then $m \neq \emptyset$, so m is a successor: $m = S(m')$.Therefore $m = \{0, \ldots, m'\}$, and $m \cap X \subset \{0, \ldots, m'\}$. Then the smallest element in $\{0, \ldots, m'\}$ which is also in X is the least element of X. $\square$

The element $z \in X$ in Theorem 3.1.4 is called the **least element** of X. The least element of every non-empty subset of $\mathbb{N}$ is unique See the exercise below)!
This property of $\mathbb{N}$ is called **the least element principle** or LEP of $\mathbb{N}$.

Exercise 3.1.3 *(1) Suppose that $m \in X \subseteq \mathbb{N}$. Prove that m is a least element of X if, and only if, $m \cap X = \emptyset$.*
(2) The least element of a non-empty subset of $\mathbb{N}$ is unique.

A partial order for which every two elements are comparable, as for $\leq$, is called a **total order**. A total order which has the Least Element Property is called a **well order**. Since $\mathbb{N}$ is totally ordered and satisfies the LEP with $\leq$, we say that $(\mathbb{N}, \leq)$ is a **well ordered set**. We will return to well

ordered sets in Chapter 4. For now, we will use this property of $\mathbb{N}$ to verify a method of math induction (next section).

Exercise 3.1.4 *Prove that the relation $<$ has the following properties*

$$(\forall n)(n \not< n) \qquad (n < m) \to (m \not< n) \qquad ((n < m) \wedge (m < s)) \to (n < s),$$

and (the **trichotomy property***)*

$$(\forall n, m) \quad \textit{exactly one of the following holds:} \quad n < m, \quad m < n, \quad \textit{or} \quad n = m.$$

3.2 The Principle of Math Induction

We describe here a method for proving infinitely many propositions at a time.
Recall that the *Universal Generalization Rule of Inference* teaches that one can prove a statement like

$$(\forall x)(P(x))$$

by proving that for every witness $x_0 \in \Omega_x$ the proposition $P(x_0)$ is true. The LEP allows us to use another method of proof for such universally quantified propositional formulae **when the universe of discourse of x is a subset of the set of natural numbers**: $\Omega_x \subseteq \mathbb{N}$.
Several, equivalent, forms of this method will be given, including **reverse induction**. In all but one of these a claim about the truth set of a propositional function is stated, and proved. The universes of discourse here are subsets of the natural numbers $\mathbb{N}$. The exceptional version of the Math Induction has to do with the important notion of **least elements of subsets of** $\mathbb{N}$.

Remark 3.2.1 What we explain here is known as the method of **finite induction**. There is a generalization of this, which we will cover if time permits, and which is called method of **transfinite induction**. □

Immediate Predecessors

Recall that for a set X, its successor is defined as $S(X) = X \cup \{X\}$. By the construction of the natural numbers, we see that every non-zero such, $n \neq 0$, has an **immediate predecessor** $Pred(n)$. More formally, we have

Definition 3.2.1 *Let $0 \neq n \in \mathbb{N}$. The* **immediate predecessor** $Pred(n)$ **of** n *is defined by*

$$m = Pred(n) \quad \textit{if} \quad n = S(m).$$

Using Exercise 3.1.1, one proves that the predecessor is unique. Here are some properties of $Pred$.

Exercise 3.2.1 *(1) Prove that* $(\forall n)(n \neq 0 \to (\exists\, !m)(m = Pred(n)))$.
(2) Prove that $(\forall n)(n \neq 0 \to Pred(n) = \cup n)$.
(3) Prove that $(\forall n)(n \neq 0 \to n = S(Pred(n)))$.
(4) Prove that $(\forall n)(n = Pred(S(n)))$.

PMI

Theorem 3.2.1 *The following statements are equivalent*[1].
(1) $(\forall P(n))(P(0) \wedge (\forall n)(P(n) \to P(S(n)))) \to (\forall n)(P(n))$,
(2) $(\forall P(n))(P(0) \wedge (\forall n)(P(0) \wedge \cdots \wedge P(n) \to P(S(n)))) \to (\forall n)(P(n))$,
(3) $(\forall P(n))(\forall k)((P(k) \wedge (\forall n)((k \leq n) \to (P(n) \to P(S(n)))) \to (\forall n)(k \leq n \to P(n))))$,

[1] In the formulation of this theorem we use $S(n)$ instead of the familiar $n + 1$, because we officially introduce the operation $+$ for natural numbers only in the next section.

(4) $(\forall P(n))(\forall k)((P(k)\wedge(\forall n)((k\leq n)\rightarrow((P(k)\wedge\cdots\wedge P(n))\rightarrow P(S(n))))\rightarrow(\forall n)(k\leq n\rightarrow P(n))))$,
(5) $(\forall P(n))((\forall n)(((\forall s)(s<n\rightarrow P(s)))\rightarrow P(n))\rightarrow(\forall n)(P(n))$,
(6) $(\mathbb{N},\leq)$ *satisfies the LEP.*

Remark 3.2.2 This theorem presents six versions of math induction. Although equivalent as statements, the easiness of their applications varies: some of them are more appropriate than others in different particular problems at hands. Items (1) through (5) are claims about the truth set of a formula with universe of discourse of its variable - a subset of $\mathbb{N}$. While the claims of items (1) through (4) are traditional, with base cases, the one of (5) has no base cases. This version of math induction is called **complete induction**. Version (6) is a claim about $(\mathbb{N},\leq)$ - no truth sets here. We know that claim (6) is true. So, claims (1)-(5) are true as well. □

Proof of Theorem 3.1. We will prove that the conditionals $(1)\rightarrow(2),(2)\rightarrow(5),(5)\rightarrow(6)$, and $(6)\rightarrow(1)$ are true. This will imply that the propositions of the named four items are all equivalent to each other. As an exercise prove that $(1)\Leftrightarrow(3)$ and that $(2)\Leftrightarrow(4)$ This will complete the proof of the theorem.

$(1)\rightarrow(2)$. We are proving here that if (1) is true, then so is (2). Let the propositional formula $P(n)$ satisfy the premise of (2):

$$P(0)\wedge(\forall n)(P(0)\wedge\cdots\wedge P(n)\rightarrow P(S(n))).$$

We want to show that the consequent of (2) is true as well. To this end, define the formula $Q(n)=P(0)\wedge\cdots\wedge P(n)$. We will show that $Q(n)$ satisfies the premise of (1): $Q(0)\wedge(\forall n)(Q(n)\rightarrow Q(S(n)))$. Indeed, since $Q(0)=P(0)$, and since $P(0)$ is true, then $Q(0)$ is true. Further, the premise of (2) tells us actually that $(\forall n)(Q(n)\rightarrow P(S(n)))$. Since in general, for any two propositions p and q, we have that $p\rightarrow q\Leftrightarrow p\rightarrow p\wedge q$ (verify that!), we have that

$$(\forall n)(Q(n)\rightarrow Q(n)\wedge P(S(n))).$$

Since $Q(S(n))=Q(n)\wedge P(S(n))$ by the very definition of $Q(n)$, we get that

$$Q(0)\wedge(\forall n)(Q(n)\rightarrow Q(S(n))$$

that is, $Q(n)$ satisfies the premise of (1) as promised. But then, since we assume (1) is true, the consequent of (1) is also true for $Q(n)$: $(\forall n)(Q(n))$. By the definition of $Q(n)$, we get that $(\forall n)(P(n))$. This proves (2).

$(2)\rightarrow(5)$. We are assuming (2), and are proving (5) now. So, assume that $P(n)$ satisfies the premise of (5): $(\forall n)(((\forall s)(s<n\rightarrow P(s)))\rightarrow P(n))$. We will prove that the consequent of (5), $(\forall n)(P(n))$ is also true. Observe now that the proposition $(\forall s)(s<n\rightarrow P(s))$ is equivalent to T if $n=0$, and to $P(0)\wedge\cdots\wedge P(Pred(n)))$ if $n\neq 0$. Therefore, the proposition

$$(\forall n)(((\forall s)(s<n\rightarrow P(s)))\rightarrow P(n))$$

is equivalent to

$$P(0)\wedge(\forall n')(P(0)\wedge\cdots\wedge P(n')\rightarrow P(S(n'))).$$

This last means that $P(n)$ satisfies the premise of (2). Therefore, it satisfies the conclusion of (2) as well, that is $(\forall n)(P(n))$. This proves (5).

$(5)\rightarrow(6)$. Assuming (5), we are proving (6) now. We will argue by contradiction. So, assume $\emptyset\neq Z\subseteq\mathbb{N}$ is such that no element of Z is a least element thereof. Equivalently,

$$Z\neq\emptyset\wedge(\forall w)(w\in Z\rightarrow w\cap Z\neq\emptyset).$$

Therefore, $0\notin Z$. Consider the propositional function $P(n)=$"$n\notin Z$". We are showing next that the premise of (5),

$$(\forall n)((\forall s)(s<n\rightarrow P(s))\rightarrow P(n)),$$

is true for this $P(n)$. To this end, using the universal generalization rule of inference, we have to show that, for every natural number n, the conditional

$$(\forall s)(s < n \to P(s)) \to P(n)$$

is true. But if the hypothesis of the last conditional is true, then no natural number less than n is a member of Z, which is equivalent to $n \cap Z = \emptyset$. But then $n \notin Z$ according to the hypothesis that Z has no least element. That's why the consequence of the last conditional, $P(n)$, is also true. Since (5) was assumed to be true, and $P(n)$ satisfies the premise of (5), then $P(n)$ satisfies the consequent of (5) as well: $(\forall n)(P(n))$. This means that no natural number is a member of Z, and so $Z = \emptyset$. This contradicts the assumption that $Z \neq \emptyset$ which finishes the proof that (6) is true.

(6) $\to$ (1). We are proving here, assuming (6), that for any propositional formula $P(n)$ the proposition in (1) is true. Equivalently, for any $P(n)$, the truth set Σ of $P(n)$ satisfies $\Sigma = \mathbb{N}$. We will do this arguing by contradiction. So, let's assume that there is a formula $P(n)$ which satisfies the premise of (1)

$$P(0) \wedge (\forall n)(P(n) \to P(S(n)),$$

and whose truth set Σ is not the whole set $\mathbb{N}$. Since $\Sigma \subseteq \mathbb{N}$, the last is equivalent to $A := \mathbb{N} \setminus \Sigma \neq \emptyset$. So we have

$$\emptyset \neq A \subseteq \mathbb{N}.$$

We can invoke the LEP from (6) for A: $(\exists a_0)(a_0 \in A \wedge a_0 \cap A = \emptyset)$. Since $P(0)$ is true, we have $0 \in \Sigma$, and therefore $0 \notin A$. This in particular means that $a_0 \neq 0$, and therefore $a_0 = S(Pred(a_0))$. Since a_0 is the least element of A, and since $Pred(a_0) < a_0$, we have that $Pred(a_0) \notin A$, and therefore that $Pred(a_0) \in \Sigma$. The last inclusion is equivalent to $P(Pred(a_0))$ being true. By the premise $(\forall n)(P(n) \to P(S(n)))$ of (1), applied to $n = Pred(a_0)$, we conclude now that $P(S(Pred(a_0))) = P(a_0)$ is true as well. So, $a_0 \in \Sigma = \mathbb{N} \setminus A$ which is impossible since $a_0 \in A$. This contradiction proves that $\Sigma = \mathbb{N}$, and (1) is a true statement for any $P(n)$. $\square$

Exercise 3.2.2 *Prove that (1) $\Leftrightarrow$ (3), and that (2) $\Leftrightarrow$ (4) in the theorem above.*

There is a version of the Principle of Math Induction which is often useful. This version is called **reversed** or **backward** induction, and is due to Cauchy.

Exercise-Proposition 3.2.1 *Prove that the LEP is equivalent to the following statement*

$$(\forall n)(P(2^n)) \wedge (\forall n)(P(S(n)) \to P(n)) \quad \to \quad (\forall n)(P(n)). \quad \square$$

Remark 3.2.3 It is obvious that the hypothesis $(\forall n)(P(2^n))$ in the proposition above can be replaced by

$$(\forall n)(\exists m)(m > n \wedge P(m)),$$

or, even better, by "$P(n)$ **is true for infinitely many** $n \in \mathbb{N}$" (we are still to learn what "infinitely many" really means.) $\square$

Vista The transfinite induction mentioned above has to do with other (infinite) sets which satisfy the LEP. More precisely, if $P(x)$ is a propositional function with Ω_x being a well ordered set with relation $\leq$, then proving that $(\forall x)(P(x))$ is reduced to proving that

$$(\forall x)((\forall y < x)(P(y)) \to P(x)),$$

because the following proposition is true

$$(\forall x)((\forall y < x)(P(y)) \to P(x)) \to (\forall x)(P(x)).$$

3.3 Recursion, + and · in $\mathbb{N}$

Recursion is a method of constructing sets working step by step along well ordered set. We are illustrating this method by defining the operations addition and multiplication on $\mathbb{N}$. We will use recursion later in the course as well - when we discuss statements equivalent to the Axiom of Choice (to be introduced soon).

Definition 3.3.1 *(1) We define the sum of two natural numbers as follows*

$$(\forall m, p \in \mathbb{N})((m + 0 = m) \wedge (m + S(p) = S(m + p))).$$

(2) We define multiplication of two natural numbers as follows

$$(\forall m, p \in \mathbb{N})((m \cdot 0 = 0) \wedge (m \cdot S(p) = m \cdot p + m)).$$

Remark 3.3.1 Obviously, the multiplication is a repeated addition of the same natural number to itself. Also, and this is the mechanism of the recursion, both operations are defined step by step starting with addition (multiplication) of (by) 0, then by 1, 2, etc. That is, the operations are defined based on, already defined, operations with **smaller** natural numbers. □

The first thing that we have to convince ourselves here is that the addition and the multiplication are defined for **every two** natural numbers. Indeed, we have the following theorem.

Theorem 3.3.1 *For every two natural numbers m and n, the sum $m + n$ and the product $m \cdot n$ are well defined.*

Proof Consider the propositional functions

$$P(n, m) = (\exists s)(s = n + m) \qquad \text{and} \qquad Q(n, m) = (\exists s)(s = n \cdot m).$$

Here $\Omega_n = \Omega_m = \Omega_s = \mathbb{N}$. We have to prove that

$$(\forall n)(\forall m)(P(n, m)) \qquad \text{and} \qquad (\forall n)(\forall m)(Q(n, m)).$$

We will do this by using the universal generalization rule of inference applied to n, and then by induction on m. To this end, let n be a natural number, and consider the propositional formulae

$$P_n(m) = (\exists s)(s = n + m) \qquad \text{and} \qquad Q_n(m) = (\exists s)(s = n \cdot m).$$

In the new notations, we want to show that the propositions

$$(\forall n)(\forall m)(P_n(m)) \qquad \text{and} \qquad (\forall n)(\forall m)(Q_n(m))$$

are true. As mentioned above, we will work for any (fixed) n, and will prove, by PMI on m, that $(\forall m)(P_n(m))$ and $(\forall m)(Q_n(m))$ are true propositions.
To do this, we can use any of the equivalent versions of the PMI discussed in Theorem 3.2.1. We are showing that the first proposition, $(\forall m)(P_n(m))$, is true using item (1) of Theorem 3.2.1. The proof of the second proposition, which is very similar to what we do here, is left to the reader as an **exercise**.
Turning to the proof itself, let's check the base case: $m = 0$. We have, by the very definition of $+$, that $n + 0 = n$, so, choosing $s = n$, we get that $P_n(0)$ is true. Assume now that $P_n(m)$ is true. We have to prove that $P_n(S(m))$ is true as well. The induction hypothesis means that $n + m$ is well defined. Denoting by $s = S(n+m)$, and using the definition for addition, $S(n+m) = n+S(m)$, we see that $P_n(S(m))$ is indeed true. By the PMI we have the proposition $(\forall m)(P_n(m))$ is true. Since this was done for any n, the Universal Generalization Rule of inference gives us that $(\forall n)((\forall m)(P_n(m)))$ is true. The proof is completed. □

Exercise 3.3.1 *Prove the second proposition of the theorem above. Namely, prove that for any natural number n the following is true*

$$(\forall m)(\exists s)(s = n \cdot m).$$

Having defined the two operations on $\mathbb{N}$, we have to verify all the properties that we know from school about them. This is done in the exercises below.

Exercise 3.3.2 *(1) Prove that the operations addition and multiplication satisfy the expected properties: commutativity, associativity, distributivity of multiplication over addition, 0 and 1 being neutral elements with respect to addition and multiplication, respectively. More precisely, prove that*

(o) For every natural number m we have

$$m + 0 = 0 + m \qquad m + 1 = 1 + m \qquad m \cdot 0 = 0 \cdot m \qquad m \cdot 1 = 1 \cdot m$$

(i) For every three natural numbers m, n, p we have $m + (n + p) = (m + n) + p$
(ii) For every two natural numbers m, n we have $m + n = n + m$
(iii) For every three natural numbers m, n, p we have $(n + p) \cdot m = n \cdot m + p \cdot m$
(iv) For every three natural numbers m, n, p we have $m \cdot (n \cdot p) = (m \cdot n) \cdot p$
(v) For every two natural numbers m, n we have $m \cdot n = n \cdot m$
[Hint: Prove, by different forms of induction, the claims in the order they are given above.]

(2) Prove that, for every two natural numbers m, n,

$$0 \neq m \vee 0 \neq n \quad \rightarrow \quad 0 \neq m + n.$$

The converse of this statement is also true. Prove it.

(3) Provethat both operations, addition and multiplication, have the cancellation property. That is, for every three natural numbers m, n, p we have

$$m + p = n + p \rightarrow m = n \qquad ((p \neq 0) \wedge (n \cdot p = m \cdot p)) \rightarrow (n = m).$$

[Hint: The first claim is proved by contradiction using that a successor natural number is never 0.
Prove the cancellation property for addition by induction on $p \in \mathbb{N}$. The base case $p = 0$ is obvious. Assuming that $m + p = n + p \rightarrow m = n$ is true, let $m + S(p) = n + S(p)$. We want to prove that $m = n$. But, by the definition of addition, $m+S(p) = S(m+p)$ and $n+S(p) = S(n+p)$. So, we have $S(m+p) = S(n+p)$. By the property of predecessors, it follows then that $m+p = n+p$, and therefore, by the induction hypothesis, $m = n$.
For the multiplication, using the commutativity of this operation, we will prove, by induction on n, that $((p \neq 0) \wedge (p \cdot n = p \cdot m)) \rightarrow (n = m)$. The base case, $n = 0$ follows by contradiction: if $m \neq 0$, and $p \cdot 0 = p \cdot m$, then $m = S(m')$ and $p \cdot m = p \cdot S(m') = p \cdot m' + p \neq 0$ since $p \neq 0$. So, $0 = s \cdot 0 = s \cdot m \neq 0$ - an absurd! Assuming further that $((p \neq 0) \wedge (p \cdot n = p \cdot m)) \rightarrow (n = m)$, consider $(p \cdot S(n) = p \cdot m))$. We want to prove that $S(n) = m$. Since $S(n) \neq 0$, the base case gives that $m \neq 0$ as well, and $m = S(m')$. So, we have in this case that $p \cdot S(n) = p \cdot S(m')$ which, by the definition of multiplication is the following $p \cdot n + p = p \cdot m' + p$. By the cancellation property of addition we get that $p \cdot n = p \cdot m'$ which, by the induction hypothesis gives that $n = m'$ and therefore that $S(n) = S(m') = m$.]

(4) Prove that for the natural numbers m, n, p, the following properties hold true

$$(0 < n \wedge 0 < m) \rightarrow (0 < n \cdot m)$$

$$(n + p < m + p) \rightarrow (n < m) \qquad (n \cdot p < m \cdot p) \rightarrow (n < m)$$

$$(n < m) \Leftrightarrow (\exists p)(m = n + S(p)).$$

[Hint: The first claim follows by contradiction and cancellation (Exercise (3)).
For $(n+p < m+p) \to (n < m)$ try induction on p. The inductive step is based on the fact that, for $a, b \in \mathbb{N}$, if $S(a) \in S(b)$, then $a \in b$.
For $(n \cdot p < m \cdot p) \to (n < m)$ use commutativity of multiplication, and argue by induction on n. Notice that here necesarily we have $p \neq 0$.
For $(n < m) \Leftrightarrow (\exists p)(m = n + S(p))$, direction $(\Rightarrow)$, do induction on n, using if needed again that $S(a) < S(b) \to a < b$. The direction $(\Leftarrow)$ is obvious: $n < n + S(p) = S(n+p) = m$.]

3.4 What Are Natural Numbers; Peano's Axioms

We have constructed the set $\mathbb{N}$, consisting of what we called natural numbers, with two operations, addition and multiplication, on it and a relation, $\leq$. We proved some properties of these as well. The set $\mathbb{N}$ has numerous applications in mathematics. None of these applications uses the way natural numbers **look like**: we just use the symbols like $0, 1, 2, 3\ldots$ and some rules how to manipulate with these symbols, e.g. $2+3=5$ or $7 \cdot 5 = 35$. The applications of $\mathbb{N}$ are actually based on the fact that $\mathbb{N}$ is a set which has two operations and a relation with certain properties. So, from this stand point, *natural numbers* should be the elements of **any** set having two operations and a relation with the properties like the ones of $\mathbb{N}$.

Speaking of the properties of $\mathbb{N}$, there are some, called defining properties, which determine the rest. Collections of defining properties can be chosen in many ways, depending on the taste of the people who make the choice. We will use one of them, presumably the simplest one, to give a **definition** of natural numbers. We also include the collection called the **Peano's Axioms** - arguably the most popular one.

The discussion below is based on concepts, such as **function, injection** and **bijection** which will be introduced later in the Notes. This, we hope, will not make the presentation in this section harder or less understandable though.

3.4.1 A Definition of Natural Numbers

The basic properties of the set $\mathbb{N}$, which were used to develop the theory of this set, are the existence of the successor operation, S, the element 0 - the only one which is **not** a successor of an element of $\mathbb{N}$, and the least element principle. The last one is defined using the relation $\leq$. In order to avoid involvement of a relation as well in the definition of natural numbers, one can replace it with the equivalent, as we know, property of the principle of math induction. Having all this in mind we **define** what natural numbers are.

Definition 3.4.1 *Natural numbers is a triplet $(\tilde{\mathbb{N}}, 0, S)$ consisting of a set $\tilde{\mathbb{N}}$, and element $0 \in \tilde{\mathbb{N}}$ called* **zero element**, *and a function $S : \tilde{\mathbb{N}} \to \tilde{\mathbb{N}}$ called a* **successor function** *and having the following properties*
(S1) S is an injection (that is, $(\forall x, y \in \tilde{\mathbb{N}})(x \neq y \to S(x) \neq S(y))$;
(S2) $0 \notin Ran(S)$ (that is, $(\forall x \in \tilde{\mathbb{N}})(0 \neq S(x))$);
(S3) (Induction Principle) $(\forall M \subseteq \tilde{\mathbb{N}})((0 \in M \wedge S(M) \subseteq M) \to M = \tilde{\mathbb{N}})$.

After giving a definition, one has to make sure that the definition is meaningful, that is, that there exists an object, in our case - a set with a zero and a successor function, having the properties (S1), (S2), and (S3). It is straightforward that the set $\mathbb{N}$ with the successor operation indeed satisfies these properties. Therefore, the definition of natural numbers **is** meaningful.

The next thing to be studied is **how unique the natural numbers are**. There are definitions which allow only one object to satisfy them. As an example, consider the empty set: we defined it as a set containing no elements (and postulated it exists in Axiom 1). We then proved that this set

is unique (we did this by showing that the empty set is a subset of every set, and using the Extensionality axiom). In general however, more than one object may satisfy a definition. For example, think of the definition of singleton: a set containing only one element. There are such sets (due to some of the axioms, of course), and there are many singletons: as many as the sets are (since every set X defines a singleton $\{X\}$). For another example, there is a well known construction of a set of natural numbers, belonging to Zermelo, in which

$$0 = \emptyset, \quad 1 = \{\emptyset\}, \quad 2 = \{\{\emptyset\}\}, \quad 3 = \{\{\{\emptyset\}\}\}, \quad \text{etc.}$$

With this definition, the non-zero natural numbers are all singletons: $0 = \emptyset, 1 = \{0\}, 2 = \{1\}, 3 = \{2\}$ etc.
When the object satisfying a definition is not unique, the best one can wish for is to have, for any two such objects, an **unambiguous way to identify them**. Identifications of (distinct) sets are done using bijections between them (these are maps $\varphi : X \to Y$ which are injections and **surjections**, that is, having also that $(\forall y \in Y)(\exists x \in X)(y = \varphi(x))$). The following theorem shows that in the case of natural numbers such identifications exist.

Theorem 3.4.1 *Suppose $(\tilde{\mathbb{N}}_1, 0_1, S_1)$ and $(\tilde{\mathbb{N}}_2, 0_2, S_2)$ satisfy the definition of natural numbers. Then there is a unique map $\varphi : \tilde{\mathbb{N}}_1 \to \tilde{\mathbb{N}}_2$ such that $\varphi(0_1) = 0_2$ and $\varphi \circ S_1 = S_2 \circ \varphi$. This map is a bijection.*

Proof (Sketch) That one such map exists is straightforward: define $f : \tilde{\mathbb{N}}_1 \to \tilde{\mathbb{N}}_2$ recursively as follows

- $f(0_1) := 0_2$
- for every $0_1 \neq x \in \tilde{\mathbb{N}}_1$ define $f(x) = S_2(f(Pred_1(x)))$.

Using PMI, it is easy to prove that $(\forall x)(\exists y)(y = f(x))$, that $f \circ S_1 = S_2 \circ f$, and that f is a bijection. Here $\Omega_x = \tilde{\mathbb{N}}_1$ and $\omega_y = \tilde{\mathbb{N}}_2$.
The proof that such a map is unique, one uses induction to prove that, given maps $f, g : \tilde{\mathbb{N}}_1 \to \tilde{\mathbb{N}}_2$ satisfying the relations $f \circ S_1 = S_2 \circ f$ and $g \circ S_1 = S_2 \circ g$ and such that $f(0_1) = g(0_1) = 0_2$, then $(\forall x)(f(x) = g(x))$. The easy proof of this is left as an exercise. □

One uses this bijection to identify the triplets $(\tilde{\mathbb{N}}_1, 0_1, S_1)$ and $(\tilde{\mathbb{N}}_2, 0_2, S_2)$. The uniqueness of this map makes the identification unambiguous, or as we say in such a case - **identifies them in a canonical way**. So, we may, without a fear of ambiguity, denote (any) set of natural numbers by the familiar $\mathbb{N}$. The same applies to the operations and the relation of a set of natural numbers.

3.4.2 Peano's Axioms

An equivalent characterization of the natural numbers is given by using the Peano's Axioms. Namely we have

Theorem 3.4.2 *Suppose the set X with the properties*
(P1) $(\exists x)(x \in X)$
(P2) $(\forall y)(\exists y' \in X)$
(P3) $\neg((\exists y \in X)(y' = x))$
(P4) $(\forall y, z \in X)(y' = z' \to y = z)$
(P5) $(\forall Y \subseteq X)((x \in Y \wedge (\forall w \in X)(w \in Y \to w' \in Y) \to Y = X)$.
Then the triplet $(X, x, (\cdot)')$ satisfies the properties of the definition of natural numbers.
Conversely, if the triplet $(\tilde{\mathbb{N}}, 0, S)$ satisfies the definition of natural numbers, then the set $X = \tilde{\mathbb{N}}$ has the properties (P1)-(P5) with $x = 0$ and $y' = S(y)$.

Proof The easy, but long proof is left as an exercise to the diligent readers. □

The propositions (P1)-(P5) are called **Peano's axioms**. The set of natural numbers $\mathbb{N}$ we have constructed does satisfy the Peano's axioms (as we have proved along the way).

3.5 Two Examples

This section is devoted to two interesting examples of theorems proved by PMI. The first theorem is a statement about integers, and the second is a statement about real numbers. As we know, every object in math has to exist as a set. The integers and the real numbers are no exception. In Chapter 5, using the set $\mathbb{N}$, and some set theoretical constructions, we will define the basic number systems (integers, rational numbers, real numbers), and will prove that they exist. For the needs of this section though we will assume knowledge of the basic properties of the integers and the real numbers, so that we can state and prove the promised two theorems.

Long Division for Integers

The first theorem we are proving is the following one.

Theorem 3.5.1 (*Long Division for Integers*) *Suppose $n, m \in \mathbb{Z}$ where $m \neq 0$. Then there are unique $q, r \in \mathbb{Z}$ such that*

$$n = m \cdot q + r, \quad 0 \leq r < |m|.$$

Proof. (Existence of q and r) Consider the set $\Sigma = \{n - m \cdot q \,|\, q \in \mathbb{Z}\}$. Since $m \neq 0$, the set Σ contains non-negative integers. Indeed, if $n \geq 0$, then $n - m \cdot 0$ is a non-negative integer in Σ. If $n < 0$, and $m > 0$, then $n - m \cdot n$ is a positive integer in Σ. If, finally, $n < 0$ and $m < 0$, then $n - m \cdot (-n)$ is a positive integer in Σ. This implies that the set $S = \Sigma \cap \mathbb{N}$ is a non-empty subset of $\mathbb{N}$, and therefore has a least element $r \in S$. The latter means that there is an integer q such that $r = n - m \cdot q$. In other words, $n = m \cdot q + r$. We claim now that $r < |m|$. Indeed, if not, that is if $r \geq |m|$, then $0 \leq r' = r - m \cdot q - |m| < r$ and $r' \in S$ which is impossible due to r being the least element of S. So, we found integers q and r such that $n = m \cdot q + r$ and $0 \leq r < |m|$.
(Uniqueness of q and r) Assume that the integers q' and r' have the properties that $n = m \cdot q' + r'$ and $0 \leq r' < |m|$. we have to show that $q' = q$ and $r' = r$. We have

$$m \cdot q + r = m \cdot q' + r' (= n).$$

Therefore

$$m \cdot (q - q') = r' - r$$

which implies that

$$|m| \cdot |q - q'| = |r' - r|.$$

Assume now, by way of RAA, that either $q \neq q'$ or $r \neq r'$. Since $m \neq 0$, and using the last equality, we see that we have both $r \neq r'$ **and** $q \neq q'$. but then $|q - q'| \geq 1$, and

$$|r' - r| = |m| \cdot |q - q'| \geq |m| \cdot 1 = |m|.$$

On the other hand, the inequalities $0 \leq r < |m|$ and $0 \leq r' < |m|$ imply that $0 \leq |r' - r| < |m|$ (do you see why?), and we get

$$|m| \leq |r' - r| < |m|$$

and ultimately that $|m| < |m|$ which is a contradiction! Therefore, by RAA, we get that $q = q'$ and $r = r'$. The theorem is proved. $\square$

Definition 3.5.1 *The number q is called* **the quotient**, *and the number r is called* **the remainder** *of the division of n by m. The number n is called* **the dividend**, *and the number m is called* **the divisor** *of that division. Finding q and r is called* **long division** *process.*

A Classical Inequality

For the next result, we assume knowledge of real numbers, and of taking nth roots of (non-negative) real numbers.

Theorem 3.5.2 (*AM-GM Inequality*) *For any non-negative real numbers $a_1, a_2, \ldots, a_n$, the following result holds true*

$$\frac{a_1 + a_2 + \cdots a_n}{n} \geq \sqrt[n]{a_1 \cdot a_2 \cdots a_n},$$

and the equality happens if, and only if, $a_1 = a_2 = \cdots = a_n$.

Proof. (Sketch) The proof is a classical example (due to Cauchy) of application of the reverse induction. One first proves, using a simple induction, that the inequality is true for every $n = 2^k$ where $k \geq 1$. The base case here, $k = 1$ is an easy thing to verify (do that!), while the inductive step goes as follows

$$\frac{a_1 + \cdots + a_{2^{k+1}}}{2^{k+1}} = \frac{1}{2} \cdot \frac{(a_1 + \cdots + a_{2^k}) + (a_{2^k+1} + \cdots + a_{2^{k+1}})}{2^k}$$

$$\frac{1}{2} \cdot \left(\frac{a_1 + \cdots + a_{2^k}}{2^k} \quad + \quad \frac{a_{2^k+1} + \cdots + a_{2^{k+1}}}{2^k} \right) \geq \frac{1}{2} \cdot \left(\sqrt[2^k]{a_1 \cdots a_{2^k}} \quad + \quad \sqrt[2^k]{a_{2^k+1} \cdots a_{2^{k+1}}} \right)$$

$$\geq \sqrt{\sqrt[2^k]{a_1 \cdots a_{2^k}} \cdot \sqrt[2^k]{a_{2^k+1} \cdots a_{2^{k+1}}}} = \sqrt[2^{k+1}]{a_1 \cdots a_{2^{k+1}}}.$$

Having proven this, one shows next, and this is the reverse induction step, that if the inequality is true for $n + 1 \geq 2$, then it is true for n as well. This is achieved by applying the inequality to the numbers $a_1, \ldots, a_n, \frac{a_1 + \cdots + a_n}{n}$ noticing that

$$\frac{a_1 + \cdots a_n}{n} = \frac{a_1 + \cdots + a_n + \frac{a_1 + \cdots + a_n}{n}}{n+1}$$

and that

$$\sqrt[n]{a_1 \cdots a_n} = \sqrt[n+1]{a_1 \cdots a_n \cdot \sqrt[n]{a_1 \cdots a_n}} \quad .$$

Finish the proof. Don't forget to show that the equality happens if, and only if, $a_1 = \cdots = a_n$. □

Definition 3.5.2 *The claim in the last theorem is called* **the arithmetic-geometric mean inequality**, *and is abbreviated to* **AM-GM**.

Exercise 3.5.1 *(1) Prove that for every natural n*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

(2) Let a and b be natural numbers. Prove that, for every natural number n,

$$a + (a + b) + \cdots + (a + nb) = \frac{(2a + nb)(n + 1)}{2}.$$

(3) Let x be a real number such that $x \neq 1$. Prove that, for every natural number n,

$$1 + x + x^2 + \cdots x^n = \frac{1 - x^{n+1}}{1 - x}.$$

(4) Let a and x be real numbers such that $x \neq 1$. Prove that, for every natural number n,

$$a + ax + ax^2 + \cdots + ax^n = a\frac{1 - x^{n+1}}{1 - x}.$$

(5) Prove that, for every natural number n,

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

(6) Prove that, for every natural number n,

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

(7) (Bernoulli's inequality) Let x be a real number such that $x \geq -1$. Prove that, for every natural number n,

$$(1+x)^n \geq 1 + nx.$$

(8) Prove that, for every **odd** *natural number $n \geq 3$,*

$$(1 + 1/2)(1 - 1/3) \cdots (1 + (-1)^n/n) = 1,$$

and that for every positive **even** *natural number n,*

$$(1 - 1/2)(1 + 1/3) \cdots (1 - (-1)^n/n) = 1/2.$$

(9) Find a formula for the product below, and prove (by induction or otherwise) it is true

$$(1 - 1/4)(1 - 1/9)(1 - 1/16) \cdots (1 - 1/n^2).$$

(10) The same as in item (9), but for the expression

$$1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n!.$$

Chapter 4

Relations, Functions, and Orders

After having studied sets statically, as separate entities, in the previous two chapters, it is time to make the picture more dinamic, and introduce the **means to compare sets**. To this end, we are introducing and studying in considerable detail the concept of a **relation from a set to a set** gradually specializing it to **multi-valued functions**, **partial functions** and finallly - to **functions** from a set to a set. All these are, of course, sets, and basic set operations (union, intersection), as well as certain specific constructions (restriction, inversion, composition) can be applied to them. In all four cases, we find the conditions under which the listed operations applied to objects of certain type do not lead us out of that type. This, in the case of the operation union, leads us to conditions under which (partial) functions can be glued, and in the case of inversion naturally leads us to the concept of one-to-one patrtial functions, and to one-to-one correspondences. We pay special attention to the most important types of functions: injections, surjections, and bijections, and study them through their compositions with other functions. This way we get to the concept of left and right inverses of a function characterizing injections and surjections. Our attempt to characterize the surjections in this context leads us to introducing the **Axiom of Choice**.

Substantial part of the section is devoted to **relations on a set**, that is, to relations from a set to itself. While relations from a set to another one gives the means to **compare** these sets, relations on a set provide it with important **structures**. In this course we are interested mainly in **equivalence relations** and different types of **orders** on a set. Using the former we will construct in Chapter 5 sets of integer and rational numbers, while using the latter we will construct there a set of real numbers.

4.1 Relations from a Set to a Set

4.1.1 Ordered Pairs of Sets

The basic concept here is: **ordered pair of sets**. The following definition is due to the Poland Set Theorist and Topologist Kazimierz Kuratowski.

Definition 4.1.1 *Let x, y be sets. The set*

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

is called **the ordered pair with first component x and second component y.**

Exercise 4.1.1 *Specify the axioms we need to use in order to define the ordered pair (x, y).*

The most important property of the ordered pairs is that the two components are distinguishable set theoretically (not only graphically). We have the following fact.

Proposition 4.1.1 *For any four sets x, y, x_1, y_1,*

$$(x, y) = (x_1, y_1) \quad \Leftrightarrow \quad (x = x_1) \wedge (y = y_1).$$

Proof ($\Rightarrow$) Suppose $(x, y) = (x_1, y_1)$. Note first that (x, y) is a singleton if, and only if, $x = y$, in which case $(x, y) = \{\{x\}\}$. Indeed, $\{\{x\}, \{x, y\}\}$ is a singleton only if $\{x\} = \{x, y\}$, only if $x = y$. In such a case, $\{\{x\}, \{x, y\}\} = \{\{x\}, \{x, x\}\} = \{\{x\}, \{x\}\} = \{\{x\}\}$. We consider next two cases.

(1) $x = y$ (that is, $(x, y) = \{\{x\}\}$ is a singleton). Then (x_1, y_1) is a singleton as well, and therefore $x_1 = y_1$ with $(x_1, y_1) = \{\{x_1\}\}$. The relation $(x, y) = (x_1, y_1)$ means that $\{\{x\}\} = \{\{x_1\}\}$ which is possible only when $\{x\} = \{x_1\}$, or when $x = x_1$. We also have $x = x_1$ and $y = x = x_1 = y_1$, so $y = y_1$.

(2) $x \neq y$ (that is, (x, y) is a doubleton). In this case (x_1, y_2) is a doubleton as well, and hence $x_1 \neq y_1$. Now the equality of sets

$$\{\{x\}, \{x, y\}\} = \{\{x_1\}, \{x_1, y_1\}\}$$

is possible only if either

$$\{x\} = \{x_1\} \qquad \text{and} \qquad \{x, y\} = \{x_1, y_1\},$$

in which case we are done, because $x = x_1$ and (since $x \neq y$ and $x_1 \neq y_1$) $y = y_1$, or

$$\{x\} = \{x_1, y_1\} \qquad \text{and} \qquad \{x, y\} = \{x_1\}.$$

But this latter case is impossible, because the first equality implies that $x_1 = y_1 (= x)$ which is not the case.

($\Leftarrow$) This direction of the claim is obvious. $\square$

Remark 4.1.1 There are several definitions of ordered pair. All they are designed to distinguish between two elements making the pair. The most commonly used definition different from ours (see for instance the book on Algebra by P. Aluffi cited in the end of these Notes) is this (we decorate the notation to distinguish it from the one above)

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

As in the case of Kuratowski's definition, it is true that

$$(x, y)' = (x_1, y_1)' \quad \Leftrightarrow \quad x = x_1 \ \wedge \ y = y_1,$$

but the proof is more involved that the one for (x, y), and uses an axiom we haven't introduced here (the axiom and a sketch of a proof of the fact above is given in the last section of this chapter). This is one of the reasons we used Kuratowski's definition of ordered pair. $\square$

Exercise 4.1.2 *Prove that for no x and y is $(x, y) = (x, y)'$.*

Repeating the construction of ordered pair, one defines ordered triplets, quadruplets, etc.

Exercise 4.1.3 *(1) Define ordered triplets of sets by $(x, y, z) = ((x, y), z)$. Prove that*

$$(x, y, z) = (x_1, y_1, z_1) \qquad \Leftrightarrow \qquad x = x_1 \quad \wedge \quad y = y_1 \quad \wedge \quad z = z_1.$$

(2) Similarly, define $(x, y, z)'' = (x, (y, z))$. Prove that

$$(x, y, z)'' = (x_1, y_1, z_1)'' \qquad \Leftrightarrow \qquad x = x_1 \quad \wedge \quad y = y_1 \quad \wedge \quad z = z_1.$$

Remark 4.1.2 It is a natural question to ask when is $(x, y, z) = (x, y, z)''$? In other words, when is $((x, y), z) = (x, (y, z))$? With the introduced so far axioms we are not able to answer this question. More precisely, having the equality of the two sets is consistent with our axioms. In the end of this chapter, where we discuss a stronger version of the Russell's class axiom, we will show that with this axiom replacing the Russell's class axiom we can prove that it is actually never true that $(x, y, z) = (x, y, z)''$. $\square$

4.1.2 The Cartesian Product of Two Sets

Proposition 4.1.2 *The following holds true*

$$(\forall A)(\forall B)(\exists! C)((\forall z)(z \in C \Leftrightarrow (\exists a)(\exists b)(z = (a, b)),$$

where $\Omega_a = A, \Omega_b = B$*, and as usual* A *and* B *are sets.*

Proof The existence of C follows from the observation that $\{a\}, \{a, b\} \in \mathcal{P}(A \cup B)$, and therefore that $(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B))$. Indeed, by the Separation Axiom (Axiom 6), the class C is defined by a formula from the set $\mathcal{P}(\mathcal{P}(A \cup B))$

$$C = \{z \,|\, z \in \mathcal{P}(\mathcal{P}(A \cup B)) \wedge (\exists a)(\exists b)(a \in A \wedge b \in B \wedge z = (a, b))\}.$$

The uniqueness of C is derived in a standard way by using the Extensionality Axiom (Axiom 2). □

The set C is so important (as we will soon see), that it has a name.

Definition 4.1.2 *The* **Cartesian product**, $X \times Y$*, of two sets* X *and* Y *is defined by*

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

Exercise 4.1.4 *(1) Prove that, in general,* $X \times Y \neq Y \times X$*, but that, for any* A*,*

$$A \times \emptyset = \emptyset \times A = \emptyset.$$

(2) Prove more generally that if $X \neq \emptyset \neq Y$*, then*

$$X \times Y = Y \times X \qquad \Leftrightarrow \qquad X = Y.$$

(3) Prove that the collection

$$\{(x, y, z) \,|\, x \in X \wedge y \in Y \wedge z \in Z\}$$

is a set, and is uniquely determined by X, Y*, and* Z*. We denote this set by* $X \times Y \times Z$*. Prove more specifically that*

$$X \times Y \times Z = (X \times Y) \times Z.$$

4.1.3 Relations from a Set to a Set

The following definition is fundamental for our considerations.

Definition 4.1.3 *Given two sets* A *and* B*, a* **relation from** A **to** B *is a triplet* (A, B, R) *such that* $R \subseteq A \times B$*. A relation from* A *to* A *is called a* **relation on** A*.*

Note that, since $R \subseteq A \times B$ is a collection of ordered pairs, it **is a relation** on its own. As such, it has domain and range:

$$Dom(R) = \{a \,|\, (\exists b)((a, b) \in R)\} \qquad Ran(R) = \{b \,|\, (\exists a)((a, b) \in R\}.$$

Therefore, $Dom(R) \subseteq A$ and $Ran(R) \subseteq B$. Note that both inclusions may be strict.

In the case of relations from A to B, we have the following terminology.

Definition 4.1.4 *Given* (A, B, R)*, the set* B *is called the* **co-domain** *of* (A, B, R)*. We write* $co - Dom(R) = B$*.*

Definition 4.1.5 *Given a relation (A, B, R) and $x \in A$, define*

$$R[x] = \{y \in B \,|\, (x, y) \in R\}.$$

Obviously, $R[x] \subseteq B$ are well defined for every set x. Of course, $R[x]$ is non-empty only if $x \in Dom(R)$.

Definition 4.1.6 *The relation (B, A, S) from B to A is called the* **inverse relation of** *(A, B, R), if*

$$S = \{(b, a) \,|\, (a, b) \in R\}.$$

We may also write $(B, A, R^{-1}) = (B, A, S) = (A, B, R)^{-1}$.

From now on in these notes we will be abbreviating the notation (A, B, R) to R. Keep in mind that two relations (A, B, R) and (C, D, S) are equal if, and only if, $A = C, B = D$, and $R = S$. So, using the abbreviation we have to be aware of who the sets involved are. We will be fixing this by writing $R \subseteq A \times B$.

Example 4.1.1 (1) For every two sets, there always is relation from A to B: this is $\emptyset \subseteq A \times B$. If $A \times B \neq \emptyset$, there always is a second relation: $A \times B \subseteq A \times B$.
(2) A very important relation on a set A is the **identity relation** $i_A \subseteq A \times A$

$$i_A := \{(x, x) \,|\, x \in A\}. \quad \square$$

Exercise 4.1.5 *(1) Prove that, for any relation $R \subseteq A \times B$, $(R^{-1})^{-1} = R$.*
(2) Prove that $R[x]$ exists (i.e., is a set) for every set x.
(3) Let $R \subseteq A \times B$. Consider the set $\{R[x] \,|\, x \in A\}$. Recall that in it, we do not distinguish between $R[x]$ and $R[x']$ if $(x, x') \in R$. Similarly, consider $\{R^{-1}[y] \,|\, y \in B\}$. Prove that

$$Ran(R) = \cup\{R[x] \,|\, x \in A\} \qquad Dom(R) = \cup\{R^{-1}[y] \,|\, y \in B\}.$$

Restriction, Intersection, Union, and Composition of Relations from a Set to a Set

The restriction of relations from a set to a set is quite a flexible operation. It is not always a restriction in the intuitive sense we have from school (or life).

Let $R \subseteq A \times B$ be a relation, and let C and D be two sets.

Definition 4.1.7 *The* **restriction** *of R to $C \times D$, denoted by $R_{|C \times D}$, is defined by*

$$R_{|C \times D} := R \cap (C \times D) \subseteq C \times D.$$

If R is a relation on A, the restriction of R to C, denoted $R_{|C}$, is defined by

$$R_{|C} = R_{|C \times C} \subseteq C \times C.$$

Note that the restriction of a relation is a way to define a relation between two new sets, the relationship with the original ones being not important. Thus, if $B \subset D$ then the restriction **expands** the co-domain of the original relation. The options here are many. Also, keep in mind that the restricted relation is equal to the original one only if $A = C$ and $B = D$. (B/c this is the case if $(A, B, R) = (C, D, R_{|C \times D})$.)

Exercise 4.1.6 *(1) Prove that $(R_{|C \times D})_{|E \times F}$ is the relation*

$$R \cap ((C \cap E) \times (D \cap F)) \subseteq E \times F.$$

Conclude that, in general, $(R_{|C \times D})_{|E \times F} \neq (R_{|E \times F})_{|C \times D}$.
(2) Suppose $C \cap Dom(R) = \emptyset$ or $D \cap Ran(R) = \emptyset$. Compute the restriction $R_{|C \times D}$.

The operations intersection and union of sets provides operations on relations from a set to a set as follows.

Definition 4.1.8 *Let (A, B, R) and (C, D, S) be two relations.*
(1) The **intersection** *of these relations is defined by*

$$(A, B, R) \cap (C, D, S) := (A \cap C, B \cap D, R \cap S).$$

(2) The **union** *of the relations is defined by*

$$(A, B, R) \cup (C, D, S) = (A \cup C, B \cup D, R \cup S).$$

An operation typical for relations (not available for sets which are not collection of ordered pairs) is the composition of relations.

Definition 4.1.9 *Let $R \subseteq A \times B$ and $S \subseteq C \times D$. The* **composition**, *$S \circ R \subseteq A \times D$, of R and S is defined by*

$$S \circ R := \{(x, z) \,|\, (\exists y)((x, y) \in R \wedge (y, z) \in S\,\} \subseteq A \times D.$$

Exercise 4.1.7 *(1) Prove that, for every $R \subseteq A \times B$,*

$$R \circ i_A = i_B \circ R = R;$$

(2) Suppose L is a relation on A such that, for every $R \subseteq A \times B$ and for every $S \subseteq B \times A$,

$$R \circ L = R \quad \textit{and} \quad L \circ S = S.$$

Prove that $L = i_A$. (This shows that the relation i_A can be characterized by using composition of relations only!)
(3) Prove that the composition of relations is **associative**, *that is, for any $R \subseteq A \times B, S \subseteq B \times C$, and $T \subseteq C \times D$,*

$$T \circ (S \circ R) = (T \circ S) \circ R.$$

Remark 4.1.3 We see that the five operations, inversion, restriction, intersection, union, and composition, are available in the case of relations from a set to a set producing relations from a set to a set. □

4.2 Functions from a Set to a Set

Most of the relations from A to B, that is, most of the elements of $\mathcal{P}(A \times B)$, are not interesting as providing information about the interaction of the two sets. In this subsection, we restrict our attention to relations obeying some restrictions. For $R \subseteq A \times B$, these restrictions are described in terms of $Dom(R)$, $Ran(R)$, and $R[x]$ for $x \in A$.

4.2.1 Multivalued Functions and Correspondences

Definition 4.2.1 *The relation (A, B, R) is a* **multi-valued function** *if $Dom(R) = A$. A multi-valued function is called a* **correspondence from** *A* **to** *B if in addition $Ran(R) = B$.*

Obviously, $R \subseteq A \times B$ is a multi-valued function if, and only if, $(\forall x)(x \in A \to R[x] \neq \emptyset)$, and is a correspondence, if, and only if, the inverse $R^{-1} \subseteq B \times A$ is a multi-valued function as well.
To denote multi-valued functions, we some times write

$$R : A \rightrightarrows B$$

instead of the usual "$R \subseteq A \times B$ is a multi-valued function".

Example 4.2.1 (1) The relation (A, A, i_A) is a multivalued function
(2) The relation $(\emptyset, A, \emptyset)$ is a multivalued function, but $(A, \emptyset, \emptyset)$ is not if $A \neq \emptyset$.
(3) The relation $(A, B, A \times B)$ is a multivalued function if $B \neq \emptyset$.
(4) The relation $(\{x\}, B, R)$ is a multivalued function if, and only if, $R \neq \emptyset$. □

Exercise 4.2.1 *Prove the following*
(1) The union of two multi-valued functions is a multi-valued function.
(2) Let $R : A \rightrightarrows B$ and $S : C \rightrightarrows D$ be such that

$$(*) \qquad (\forall a \in A)(R[a] \cap C \neq \emptyset).$$

Prove that the composition $S \circ R \subseteq A \times D$ is a multi-valued function as well. Prove also that the condition $(*)$ is not only sufficient, but necessary as well in order to have the composition a multi-valued function.
(3) Let $R : A \rightrightarrows B$ and $S : C \rightrightarrows D$ be such that

$$(**) \qquad (\forall z \in A \cap C)(R[z] \cap S[z] \neq \emptyset).$$

Prove that the intersection $(A \cap C, B \cap D, R \cap S)$ is a multi-valued function as well. Prove also that the condition $(**)$ is not only sufficient, but necessary as well in order to have the intersection a multi-valued function.
(4) Consider $R : A \rightrightarrows B$. Prove that if R is a correspondence from A to B, then $i_A \subseteq R^{-1} \circ R$ and that $i_B \subseteq R \circ R^{-1}$.
(5) Let $R \subseteq A \times B$ be a multivalued function
(i) Let $C \subseteq A$. Prove that the restriction $R_{|C \times B} \subseteq C \times B$ is a multivalued function.
(ii) Let now $C \nsubseteq A$, and let D be any set. Prove that $R_{C \times D} \subseteq C \times D$ is **not** *a multivalued function.*
(iii) Prove that the restriction $R_{|C \times D} \subseteq C \times D$ is a multivalued function if, and only if,

$$C \subseteq A \qquad \wedge \qquad (\forall w)(w \in C \rightarrow R[w] \cap D \neq \emptyset).$$

(6) Let $R \subseteq A \times B$. Prove that
(i) R is a multi-valued function if, and only if, $i_A \subseteq R^{-1} \circ R$;
(ii) R is a correspondence if, and only if, $i_A \subseteq R^{-1} \circ R$ and $i_B \subseteq R \circ R^{-1}$.

4.2.2 Partial Functions from a Set to a Set

Definition 4.2.2 *The relation $R \subseteq A \times B$ is a partial function from A to B if for every x, $R[x] \subseteq B$ is an empty set, or is a singleton.*

Of course, $R[x] = \emptyset$ if $x \notin Dom(R) \subseteq A$. As for any relation $R \subseteq A \times B$ we have $Dom(R) \subseteq A$, and $Ran(R) \subseteq B$, and the inclusions may be strong. For instance, we may have $Dom(R) = \emptyset$ (in which case $Ran(R) = \emptyset$ as well!).

When $x \in Dom(R)$, we denote the only element of the set $R[x]$ by $R(x)$. We have therefore that $R[x] = \{R(x)\}$, and by definition $(x, R(x))$ is the only element of R having x as a first component. To distinguish partial functions as relations from a set to a set of a special type, we use specific notations to denote them. We often write

$$f_R : A \nrightarrow B$$

instead of (A, B, R), and set $f_R(x) = R(x)$ for $x \in Dom(R)$. Often, when R is understood from the context, we write just f instead of f_R.

Example 4.2.2 (1) The relation (A, A, i_A) is a partial function.
(2) The relations $(\emptyset, B, \emptyset)$ and $(A, \emptyset, \emptyset)$ are partial functions.
(3) Let $A \neq \emptyset$. The relation $(A, B, A \times B)$ is a partial function if, and only if, B is a empty or it is a singleton.
(4) The relation $(A, \{x\}, R)$ is always a partial function. □

Almost all operations on relations from a set to a set when applied to partial functions **produce as a result partial functions**!

Exercise 4.2.2 *Let (A, B, R_1) and (C, D, R_2) be partial functions. Prove that composition, restriction, and intersection of these partial functions is a partial function.*

When it comes to inverse of a partial function, or to union of partial functions, the result may end up to be a relations which is not a partial function anymore. The conditions needed for these to be partial functions as well are described in the following exercise, but before that - a useful terminology:

Definition 4.2.3 *The partial function $f : A \nrightarrow B$ is called* **one-to-one** *if*

$$(\forall x)(\forall y)((x \in Dom(f) \wedge y \in Dom(f) \wedge x \neq y) \rightarrow (f(x) \neq f(y))).$$

A partial function $f : A \nrightarrow B$ is called **onto** *if $Ran(f) = B$.*

Exercise 4.2.3 *(1) Prove that the inverse $(A, B, R)^{-1}$ of a partial function is a partial function if, and only if, the partial function is one-to-one.*
(2) Let (A, B, R_1) and (C, D, R_2) be partial functions. Prove that the union $(A \cup C, B \cup D, R_1 \cup R_2)$ is a partial function if, and only if,

$$(R_1)_{|(Dom(R_1) \cap Dom(R_2)) \times (B \cup D)} \qquad \textit{and} \qquad (R_2)_{|(Dom(R_1) \cap Dom(R_2)) \times (B \cup D)}$$

are equal. The union is denoted in such a case also by

$$f_{R_1} \cup f_{R_2} : A \cup C \nrightarrow B \cup D.$$

4.2.3 Functions from a Set to a Set

Definition 4.2.4 *Function from A to B is a relation $R \subseteq A \times B$ which is both a multivalued and a partial function. In other words, it is a relation such that*

$$(\forall x)(x \in A \rightarrow (R[x] \quad \textit{is a singleton})).$$

In this case, for $(x, y) \in R$ we write $y = f_R(x)$, or, when no danger of misunderstanding exists, just $y = f(x)$. Such a relation is usually denoted by $f : A \rightarrow B$. We define also the domain of f, $Dom(f) := Dom(R) = A$, and the range of f, $Ran(f) := Ran(R)$. When $y = f(x)$ we say that y **is the value of** *f* **at** *x.*

In other words $R \subseteq A \times B$ is a function when it is a partial function which has $Dom(R) = A$. The range of f is described by $\{y \,|\, (\exists x \in A)(y = f(x))\}$. Note that a function from A to B defines a **rule** assigning to every element $x \in A$ a unique element $f(x) \in B$.

According to the definition of function, **two functions are equal if, and only if, the relations they are defined by are equal**. That is, the two functions have to have the same domains, the same co-domains, and the same values at the elements of their domains: if $f_1 : A \rightarrow B$ and $f_2 : C \rightarrow D$, then

$$(f_1 = f_2) \quad \Leftrightarrow \quad ((A = C =: X) \wedge (B = D =: Y) \wedge (\forall x)(x \in X \rightarrow (f_1(x) = f_2(x)))).$$

Remark 4.2.1 In some books (such as the standard Calculus books), the definition of a function is "a rule" assigning to an element of A a unique element of B without explaining what the rule is! Moreover, in such books the set

$$R = \{(a, f_R(a)) \,|\, a \in A\} \subseteq A \times B$$

defining the function is refered to as **the graph** of the function $f_R : A \rightarrow B$. In our approach, functions are rigorously defined, and the ternminology properly used. We will not use the term graph of a function. □

Example 4.2.3 (1) For every set A, the relation i_A is a function (denoted by id_A or by 1_A).
(2) Given a relation $R \subseteq A \times B$, let the relation $\tilde{R} \subseteq A \times \mathcal{P}(B)$ be defined by

$$\tilde{R} := \{(x, y) \,|\, (x \in A) \wedge (y = R[x])\,\}.$$

This relation **is** a function from A to $\mathcal{P}(B)$ which will be denoted by

$$R[\cdot] : A \to \mathcal{P}(B). \quad \square$$

Exercise 4.2.4 *(1) Prove that, for every A, there is a unique function from $\emptyset$ to A. This function is denoted by $\emptyset_A : \emptyset \to A$. Prove also that a function from A to $\emptyset$ exists if, and only if, $A = \emptyset$.*
(2) Prove that the relation $R \subseteq A \times B$ is a function if, and only if, (a) the family of sets

$$\{R^{-1}[y] \,|\, y \in B\,\} \subseteq \mathcal{P}(A)$$

consists of pairwise disjoint elements, and (b)

$$\cup|[R^{-1}[y] \,|\, y \in B\,\} = A.$$

Inversion, Restriction, Intersection, and Union of Functions from a Set to a Set

We already know that the inverse relation of a class function need not be a class function. The same holds true in case of partial functions from a set to a set as well. In the latter case, the inverse $(A, B, R)^{-1}$ of a partial function is a partial function if, and only if, the class relation R is one-to-one. The case of a **function** from a set to a set is even more restrictive when it comes to having the inverse relation a function as well:

Exercise 4.2.5 *Let (A, B, F) be a function. The inverse relation (B, A, F^{-1}) is a function if, and only if, F is one-to-one, and for every $y \in B$ the set $F^{-1}[y]$ is non-empty.*

Definition 4.2.5 *A function (A, B, F) which is onto as a relation, that is which satisfies the property that*

$$(\forall y)(y \in B \to F^{-1}[y] \neq \emptyset),$$

is called a **surjection**. *A function which is one-to-one as a partial function is called also* **injection**. *A function which is one-to-one (injection) and onto (surjection) is called a* **bijection**.

Obviously, bijections are **one-to-one correspondences**. We have that the inverse of a function from a set to a set is a function as well if, and only if, the function is a bijection.

Exercise 4.2.6 *Prove that the function (A, B, F) is a surjection if, and only if, $Ran(F) = B$, if, and only if, $\cup\{F[x] \,|\, x \in A\} = B$.*

The other standard operations on relations we have been using such as restriction, intersection, and union have to also be cautiously applied to functions if we want to get a function as a result.

Definition 4.2.6 *Let (A, B, F) be a function, and let C and D be sets for which*

$$C \subseteq A \qquad \text{and} \qquad \{f_F(x) \,|\, x \in C\} \subseteq D.$$

The **restriction** $(f_F)_{|C \times D} : C \to D$ *is defined by* $(C, D, F_{|C \times D})$.

Exercise 4.2.7 *Verify that the definition of restriction of a function above is correct: the result is a function indeed.*

Let $f : A \to B$ and $g : C \to D$ be two functions determined by (A, B, R) and (C, D, S) respectively. The intersection $R \cap S$ is a relation form $(A \cap C)$ to $(B \cap D)$ which, as we already know, is a partial function. We also know that $Dom(R \cap S) \subseteq A \cap C$, and that the inclusions may be strict.

Definition 4.2.7 *In the notations above, the* **intersection** $f \cap g$ *is defined when* $Dom(R \cap S) = A \cap C$. *In such a case,* $f \cap g$ *denotes the relation* $(A \cap C, B \cap D, R \cap S)$.

The definition of union of two functions is very important, because it allows us to glue functions into new ones.

Definition 4.2.8 *Let* $f : A \to B$ *and* $g : C \to D$ *be two functions determined by* (A, B, R) *and* (C, D, S) *respectively. The* **union** $f \cup g$ *is defined only when the intersection* $f \cap g$ *exists. In such a case* $f \cup g$ *is determined by* $(A \cup C, B \cup D, R \cup S)$.

Exercise 4.2.8 *(1) Verify that the definition of union of two functions is correct:* $f \cup g$ *is a function indeed having a domain* $A \cup B$.
(2) Prove that if $f : A \to B$ *and* $g : C \to D$ *are two functions such that* $A \cap C = \emptyset$, *then* $f \cup g$ *does exist.*

Remark 4.2.2 The constructions restriction and union of functions are often used in the Calculus course. Instances of restrictions of functions are the restriction of the domain of a trigonometric function in order to "make it" invertible. It is common to restrict the domain and the co-domain of, say, the sine function from $\mathbb{R}$ to $[-\pi/2, \pi/2]$ and to $[-1, 1]$ in order to get an invertible function, and thus define $\sin^{-1}$. As for the union of functions, any function the students have seen being defined piecewise (analytically on several intervals) is actually an example of union of (often more than two) functions. □

Composition of Functions from a Set to a Set

Functions, being (special types of) relations can be composed. The composition of two functions in general may only be a partial function, not a function. But when restricted to its domain, it is a function.

Exercise 4.2.9 *Let* $R \subseteq A \times B$ *and* $S \subseteq C \times D$ *be functions. Let* $T = S \circ R \subseteq A \times D$. *Prove that* $T_{|Dom(T)} \subseteq Dom(T) \times D$ *is a function.*

There is an important particular case when the composition of two functions (as relations) is readily a function (without further restrictions of that composition). We say in such a case that either the functions are **composable**, or the corresponding relations are **composable as functions**.

Definition 4.2.9 *The ordered pair of functions* (f, g) *are* **composable** *(as functions), if* $Ran(f) \subseteq Dom(g)$.

Exercise 4.2.10 *(1) Prove that if* (f, g) *are composable, then their composition (as relations)* $g \circ f$ *is a function with domain* $Dom(f)$ *and co-domain* $co - Dom(g)$ *such that*

$$(\forall x \in Dom(f))((g \circ f)(x) := g(f(x))).$$

(2) Prove that composition of functions is associative. That is, if (f, g) *and* (g, h) *are composable pairs, then the pairs* $(g \circ f, h)$ *and* $(f, h \circ g)$ *are composable as well, and*

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

In particular, if $f : A \to B$, $g : B \to C$, *and* $h : C \to D$ *are functions, then*

$$h \circ (g \circ f) = (h \circ g) \circ f : A \to D.$$

Note that (f, g) and (g, f) are composable if, and only if, $Ran(f) \subseteq Dom(g)$ and $Ran(g) \subseteq Dom(f)$.

Examples of Interesting Functions

Definition 4.2.10 *Let $f : A \to B$ be a function, and let $Y \subseteq B$. The* **total pre-image of** *Y is the set $\{a \in A \,|\, f(a) \in Y\}$. This set is denoted by $f^{-1}(Y)$.*

Exercise 4.2.11 *(1) Let the function $f : A \to B$ be given by the relation $R \subseteq A \times B$. Prove that for every $Y \subseteq B$, $f^{-1}(Y) = Ran((R^{-1})_{|Y \times A})$. This fact explains the notation for the total pre-image of Y.*
(2) Prove that, for every function $f : A \to B$, the total inverse mapping $Y \mapsto f^{-1}(Y)$ defines a function $\mathcal{P}(B) \to \mathcal{P}(A)$.

Definition 4.2.11 *Given a function $f : A \to B$, we will denote by $\mathcal{P}^*(f) : \mathcal{P}(B) \to \mathcal{P}(A)$ sending $Y \in \mathcal{P}(B)$ to its total preimage under f, and will call it the* **total preimage function associated with** *f.*

A counterpart of $\mathcal{P}^*(f) : \mathcal{P}(B) \to \mathcal{P}(A)$ is the function $\mathcal{P}_*(f) : \mathcal{P}(A) \to \mathcal{P}(B)$ called the **image function associated with** f . Here is the definition[1].

Definition 4.2.12 *For a function $f : A \to B$ define $\mathcal{P}_*(f) : \mathcal{P}(A) \to \mathcal{P}(B)$ by*

$$\mathcal{P}_*(f)(S) = Ran(f_{|S}) \qquad \text{for any} \quad S \subseteq A.$$

Some of the properties of the functions $\mathcal{P}_*(f) : \mathcal{P}(X) \to \mathcal{P}(Y)$ and $\mathcal{P}^*(f) : \mathcal{P}(Y) \to \mathcal{P}(X)$ associated with $f : X \to Y$ are collected in the following exercises.

Exercise 4.2.12 *(1) Prove that $\mathcal{P}^*(i_A) = i_{\mathcal{P}(A)}$, $\mathcal{P}_*(i_A) = i_{\mathcal{P}(A)}$.*
(2) Let (f, g) be composable functions, and let $h = g \circ f$ denote their composition. Prove that
(i) the pair of functions $(\mathcal{P}_*(f), \mathcal{P}_*(g))$ is composable as well, and that $\mathcal{P}_*(h) = \mathcal{P}_*(g) \circ \mathcal{P}_*(f)$. So, for a composable pair of functions (f, g) we have

$$\mathcal{P}_*(g \circ f) = \mathcal{P}_*(g) \circ \mathcal{P}_*(f).$$

(ii) for the total inverse function $\mathcal{P}^*(h) : \mathcal{P}(D) \to \mathcal{P}(A)$ we have

$$(\forall z \in \mathcal{P}(D))(\mathcal{P}^*(h)(z) = \mathcal{P}(f)^*(\text{co-}Dom(f) \cap \mathcal{P}^*(g)(z)).$$

In particular, when co-$Dom(f) = Dom(g)$, we have that $(\mathcal{P}(g)^*, \mathcal{P}^*(f))$ is a composable pair, and

$$\mathcal{P}^*(h) = \mathcal{P}^*(f) \circ \mathcal{P}^*(g).$$

(iii) if $f : A \to B$ and $g : B \to C$, then the pairs (f, g), $(\mathcal{P}_*(f), \mathcal{P}_*(g))$, and $(\mathcal{P}^*(g), \mathcal{P}^*(f))$ are composable, and

$$\mathcal{P}^*(g \circ f) = \mathcal{P}^*(f) \circ \mathcal{P}^*(g) \qquad \mathcal{P}_*(g \circ f) = \mathcal{P}_*(g) \circ \mathcal{P}_*(f).$$

(3) Let $f : A \to B$ be a function. Prove that
(i) For every $S \in \mathcal{P}(A)$ we have $S \subseteq (\mathcal{P}^*(f) \circ \mathcal{P}_*(f))(S)$;
(ii) For every $T \in \mathcal{P}(B)$ we have $(\mathcal{P}_*(f) \circ \mathcal{P}^*(f))(T) \subseteq T$.

[1]Neither $\mathcal{P}^*(f)$ nor $\mathcal{P}_*(f)$ is a traditional notation. The former is usually denoted by f^{-1} while the latter is standardly denoted by f. The standard notations may easily lead to confusion: f^{-1} is also the notation for inverse function (to be introduced shortly), and f is the notation for $\ldots f$. We suggest the new notations to avoid unwanted confusion caused by using the same mark for two different objects first, and, second, because these notation suggest that $\mathcal{P}_*$ is a functor, and $\mathcal{P}^*$ is a co-functor from the category of sets **Set** to itself. (More about this - in the course Algebraic Structures.)

4.2.4 Most Important Functions from a Set to a Set

Among all functions (from a set to a set), three types, which we have met already in this chapter, are most important: **injection**, **surjection**, and **bijection**. In this subsection, we are studying these functions via their compositions with other functions. We are showing also that any function can be expressed, in a natural way, as composition of an injection, bijection, and a surjection. This fact makes these functions so important.

Definition 4.2.13 *Let $f : A \to B$ be a function.*
(1) f is called **one-to-one** *or an* **injection** *if*

$$(\forall x, x')((x, x' \in A) \wedge (x \neq x') \to (f(x) \neq f(x')));$$

(2) f is called **onto** *or* **surjection** *if $Ran(f) = B$;*
(3) f is called a **one-to-one correspondence** *or* **bijection** *if f is one-to-one and onto.*

Example 4.2.4 The function 1_A is a bijection. The empty map $\emptyset_B : \emptyset \to B$ is always an injection. $\emptyset_B$ is a surjection if, and only if, $B = \emptyset$. □

Exercise 4.2.13 *(1) (i) Let (f, g) be composable. Prove that if f and g are injections, then so is their composition $g \circ f$.*

(ii) Let (f, g) be a composable pair. Show, by examples, that f and g surjections does not imply that $g \circ f$ is a surjection.

(iii) Let co-$Dom(f) = Dom(g)$. Prove that (f, g) is a composable pair such that if f and g are surjections (respectively, bijections), then so is $g \circ f$.
(2) Prove that $f : A \to B$ is a bijection if, and only if, there is a function $g : B \to A$ such that

$$g \circ f = 1_A \quad f \circ g = 1_B.$$

[($\Leftarrow$) Assume g exists. Need to show that f is "one-to-one" and "onto". Suppose $f(a_1) = f(a_2)$ for some $a_1, a_2 \in A$. Then $g(f(a_1)) = g(f(a_2))$, and therefore $a_1 = a_2$. This proves that f is one-to-one. Let now $b \in B$, and let $a = g(b) \in A$. We have $f(a) = f(g(b)) = b$, so $B \subseteq Ran(f) \subseteq B$, and therefore $Ran(f) = B$. This proves that f is onto.
($\Rightarrow$) Assume f is a bijection. Need to find a $g : B \to A$ such that $f \circ g = 1_B$ and $g \circ f = 1_A$. To this end, let $R \subseteq A \times B$ be the relation defining f: $f = f_R$. Consider $R^{-1} \subseteq B \times A$. We have $Dom(R^{-1} = Ran(R) = B$, because f is onto. Also, $(\forall b \in B)(R^{-1}[b] - singleton)$, because f is one-to-one. Therefore, R^{-1} is a function. Denote this function by $g : B \to A$. Verify that this g does the job.]
(3) Prove that, for $f : A \to B$, if there is a function $g : B \to A$ as in (2), then this function is unique. This unique function is called **the inverse function** *of f, and is denoted by $f^{-1} : B \to A$.*
(4) Let $f : A \to B$ be a function. Prove that
(i) $\mathcal{P}^*(f) \circ \mathcal{P}_*(f) = id_{\mathcal{P}(A)}$ if, and only if, f is an injection.
[We know already that, for every $S \subseteq A$, $S \subseteq \mathcal{P}^*(f) \circ \mathcal{P}_*(f)(S)$. Prove that, for every S, the equality of the two sets happens if, and only if, f is one-to-one.]
(ii) $\mathcal{P}_*(f) \circ \mathcal{P}^*(f) = id_{\mathcal{P}(B)}$ if, and only if, f is a surjection.
[We know already that, for every $T \subseteq B$, $\mathcal{P}_*(f) \circ \mathcal{P}^*(f)(T) \subseteq T$. Prove that, for every T, the equality of the two sets happens if, and only if, f is onto.]
(iii) the maps $\mathcal{P}_*(f) : \mathcal{P}(A) \to \mathcal{P}(B)$ and $\mathcal{P}^*(f) : \mathcal{P}(B) \to \mathcal{P}(A)$ are inverses of each other if, and only if, $f : A \to B$ is a bijection (so, f is invertible). Verify, in such a case, that

$$\mathcal{P}^*(f^{-1}) = \mathcal{P}_*(f) \quad and \quad \mathcal{P}^*(f) = \mathcal{P}_*(f^{-1}).$$

(5) Given $f : A \to B$, prove that
(i) f is an injection if, and only if,

$$(\forall g, h : C \to A)((f \circ g = f \circ h) \to (g = h));$$

(ii) f is a surjection if, and only if,

$$(\forall g, h : B \to C)((g \circ f = h \circ f) \to (g = h)).$$

(6) Given $A \neq \emptyset$, and $f : A \to B$, prove that f is an injection if, and only if, there is a $g : B \to A$ such that $g \circ f = 1_A$. [The function g is called a **left inverse** *of f]. Show, by example, that such a function g may not be unique.*

[Let $R \subseteq A \times B$ be the relation defining f. Since f is injection, for every $b \in B$ the set $R^{-1}[b]$ is either empty, or a singleton. Since $A \neq \emptyset$, fix $a_0 \in A$. Define $g : B \to A$ as follows: $g(b) = a$ if $R^{-1}[b] = \{a\}$, and $g(b) = a_0$ if $R^{-1}[b] = \emptyset$. Verify that $g \circ f = 1_A$.]

Remark 4.2.3 After characterizing the bijections and the injections as in (2) and (6) above, one may be tempted to try to do the same for surjections as well. For this to be done, we need a new axiom! The next subsection explains the situation in detail.

Choice Functions and the Axiom of Choice

Te following concept turns out to play a central role in Set Theory.

Definition 4.2.14 *Suppose X is a set such that $\emptyset \notin X$. A function $F : X \to \cup X$ is called a* **choice function** *for X if*

$$(\forall x)((x \in X) \to (F(x) \in x)\,).$$

Note that for some sets, such as $\emptyset$ or any set containing finitely many elements (different from $\emptyset$!), the existence of a choice function is not a problem! The only way to ensure the existence of a choice function in general is via an axiom.

Axiom 9 (*Axiom of Choice*) *For every set X not containing $\emptyset$, there is a choice function*

$$F : X \to \cup X.$$

Exercise 4.2.14 *(1) Can a set X with $\emptyset \in X$ have a choice function?*
(2) Given $f : A \to B$, prove that f is surjection if, and only if, there is a $g : B \to A$ such that $f \circ g = 1_B$. [The function g is called a **right inverse** *of f. Show, by example, that the right inverse of f may not be unique.*

[Let $R \subseteq A \times B$ be the relation defining f, and consider $R^{-1} \subseteq B \times A$. Assume $B \neq \emptyset$, and consider the set

$$X = \{w \,|\, (\exists b \in B)(w = R^{-1}[b])\,\}.$$

Since f is surjection, $\emptyset \notin X$, and, according to the Axiom of Choice, there is a function

$$F : X \to \cup X \qquad \textit{such that} \qquad (\forall x \in X)(F(x) \in x).$$

Define $g : B \to A$ as follows:

$$(\forall b \in B)(g(b) = F(R^{-1}[b])).$$

Verify that $f \circ g = 1_B$. What happens when $B = \emptyset$?]
(3) Prove that ((2) $\Leftrightarrow$ Axiom of Choice).
(4) Let g be a left inverse, and h be a right inverse of the function f. Prove that $g = h$.
(5) Prove that f is a bijection if, and only if, f has a unique right inverse, if, and only if, f has a unique left inverse.

4.2.5 Indexed Families of Sets

Fulfilling a promise made earlier in the course, we are briefly discussing the concept of **indexed** families of sets, and the related concept of **multi-sets** here.

We will make a serious use of indexed families later in the course, in the chapter of topology on the real numbers.

Definition 4.2.15 Indexed family of sets *with* **index set** Λ *is a function* $F : \Lambda \to X$

The function F is the set of ordered pairs $\{(\lambda, F(\lambda)) \,|\, \lambda \in \Lambda\}$ (considered as a subset of $\Lambda \times X$ of course!). We can denote by X_λ the set $F(\lambda)$ for every $\lambda \in \Lambda$, and identify further every order pair $(\lambda, F(\lambda))$ with X_λ. With these new notations we have

$$F = \{X_\lambda \,|\, \lambda \in \Lambda\}.$$

The right-hand side of the equality above presents F as an indexed family of sets (each being an element of X), indexed by Λ. Observe also that if we consider the indexed family $\{X_\lambda \,|\, \lambda \in \Lambda\}$ as a set, it is exactly $Ran(F)$.
As a matter of fact, every set, as a collection of sets, can be represented as an indexed family of sets with index set - the set itself. Here is how this goes formally.

Example 4.2.5 Let Λ be a set. Its elements $\lambda \in \Lambda$, as we know, all are sets themselves. Let's denote by A_λ the set λ. We have then that

$$\Lambda = \{\lambda \,|\, \lambda \in \Lambda\,\} = \{A_\lambda \,|\, \lambda \in \Lambda\,\},$$

and the set Λ is now considered as an indexed family of sets with index set Λ. $\square$

Exercise 4.2.15 *Show that* $i_\Lambda : \Lambda \to \Lambda$ *is the function which represents* Λ *as an indexed family with index set* Λ*.*

Notice that when we consider a set as an indexed family of sets, such as $\Lambda = \{A_\lambda \,|\, \lambda \in \Lambda\}$ above, then the family has the important property that **its elements as members of the family are pairwise distinct**: no $A_\lambda = A_\mu$ for distinct $\lambda, \mu \in \Lambda$! In general though, for any family indexed by a set, **repetition of elements are allowed**! Remember that the notation X_λ, with $X_\lambda = F(\lambda)$, is used as another name of the ordered pair $(\lambda, F(\lambda))$, and although $X_\lambda = X_\mu$ for some $\lambda \neq \mu$ may happen, as members of the indexed family the sets X_λ and X_μ are considered different!
For instance, if $f : A \to 1$ is a function, then for every $a \in A$, we should have $f(a) = \emptyset$, and accordingly, the indexed by A family of sets $\{X_a \,|\, a \in A\}$ consists of identical elements: $X_a = \emptyset$. Therefore **as a set** the family is the singleton $\{\emptyset\}$. So the family has many elements which are all **identical as sets**, but, due to the different indices on them, are **distinct elements of the family**. This flexibility the indexed families provide leads naturally to the concept of **multi-sets** and maps between them. We are not going any deeper in this here. The students will learn a bit more about the multi-sets in the course on Algebraic Structures.

A very important, for Calculus purposes, particular case of indexed families are the sequences of sets.

Definition 4.2.16 *(1) An indexed family with indexing set* $\mathbb{N}$ *is called a* **sequence (of sets)**.
(2) An indexed family with indexing set Λ *is called* **infinite** *if there is an injection* $f : \mathbb{N} \to \Lambda$*, and is called* **finite** *otherwise.*

Given an indexed family of sets $\mathfrak{F} = \{X_i \,|\, i \in I\}$ we define the intersection of the family

$$\cap\mathfrak{F} :=: \cap\{X_i \,|\, i \in I\} := \{z \,|\, (\forall i)(z \in X_i)\}$$

(existing only when $\mathfrak{F} \neq \emptyset$), and the union of the family

$$\cup\mathfrak{F} :=: \cup\{X_i \,|\, i \in I\} := \{z \,|\, (\exists i)(z \in X_i)\}.$$

Considering the indexed family $\mathfrak{F}$ as a class function with domain I, that is,

$$\{(i, \mathfrak{F}(i)) \,|\, i \in I\},$$

we have

$$\cap\mathfrak{F} = \cap Ran(\mathfrak{F}) \qquad\qquad \cup\,\mathfrak{F} = \cup Ran(\mathfrak{F}).$$

In the notations $\Lambda = \{A_\lambda \,|\, \lambda \in \Lambda\}$ introduced above, we can restate intersection and union of a set as intersection and union of an indexed family of sets as follows: for $\Lambda \neq \emptyset$,

$$\cap\Lambda = \cap\{A_\lambda \,|\, \lambda \in \Lambda\} = \{z \,|\, (\forall\lambda \in \Lambda)(z \in A_\lambda)\}$$

as well as, for any Λ,

$$\cup\Lambda = \cup\{A_\lambda \,|\, \lambda \in \Lambda\} = \{z \,|\, (\exists\lambda \in \Lambda)(z \in A_\lambda)\}.$$

Exercise 4.2.16 *(1) Prove that for any indexed family (non-empty if needed!)* $\mathcal{A} := \{A_\lambda \,|\, \lambda \in \Lambda\}$ *we have*

$$(\forall\lambda \in \Lambda)(A_\lambda \subseteq \cup\mathcal{A} \quad \wedge \quad \cap\mathcal{A} \subseteq A_\lambda)$$

(2) Prove that for every set B *and for every indexed family* $\mathcal{A}$ *as in (1)*

$$(\cup\mathcal{A}) \cap B = \cup\{A_\lambda \cap B \,|\, \lambda \in \Lambda\} \qquad (\cup\mathcal{A}) \cup B = \cup\{A_\lambda \cup B \,|\, \lambda \in \Lambda\};$$

$$(\cap\mathcal{A}) \cap B = \cap\{A_\lambda \cap B \,|\, \lambda \in \Lambda\} \qquad (\cap\mathcal{A}) \cup B = \cap\{A_\lambda \cup B \,|\, \lambda \in \Lambda\}.$$

(3) Prove that for a set B *and a family* $\mathcal{A}$ *as in (1)*

$$B \setminus (\cap\mathcal{A}) = \cup\{B \setminus A_\lambda \,|\, \lambda \in \Lambda\} \qquad B \setminus (\cup\mathcal{A}) = \cap\{B \setminus A_\lambda \,|\, \lambda \in \Lambda\}.$$

4.3 Equivalence Relations

4.3.1 Basic Types of Relations on a Set

Definition 4.3.1 *Suppose* $R \subseteq A \times A$ *is a relation on* $A \neq \emptyset$.
(i) R *is* **reflexive** *if* $(\forall x)(x \in A \to (x, x) \in R)$;
(ii) R *is* **irreflexive** *if* $(\forall x)(x \in A \to (x, x) \notin R)$;
(iii) R *is* **symmetric** *if* $(\forall x, x')((x, x') \in R \to (x', x) \in R)$;
(iv) R *is* **asymmetric** *if* $(\forall x, x')((x, x') \in R \to (x', x) \notin R)$;
(v) R *is* **anti-symmetric** *if* $(\forall x, x')(((x, x') \in R \wedge (x', x) \in R) \to x = x')$;
(vi) R *is* **transitive** *if* $(\forall x, x'.x'')(((x, x') \in R \wedge (x', x'') \in R) \to (x, x'') \in R)$;
(vii) R *is* **connected** *if*

$$(\forall x, x')((x, x' \in A) \to ((x, x') \in R \vee (x', x) \in R \vee x = x'));$$

(viii) R *is* **trichotomous** *if it is connected, and for all* $x, x' \in A$ *exactly one of*

$$(x, x') \in R, \quad (x', x) \in R, \quad x = x'$$

holds true.

Notice that the negation of reflexive is **not** irreflexive. Neither is any of asymmetric and antisymmetric the negation of symmetric!

Exercise 4.3.1 *Can in this definition* A *be the empty set? If yes, give proof, and if no, give arguments why not.*

Example 4.3.1 (1) The (class-) relation $\in$ is irreflexive (by an axiom!).
(2) The relation $\leq$ on $\mathbb{N}$ is reflexive, anti-symmetric, transitive, and connected. It is not trichotomous.
(3) The relation $<$ on $\mathbb{N}$ is irreflexive, asymmetric, transitive, connected, and trichotomous. $\square$

4.3.2 Equivalence Relations v/s Partitions on a Set, Quotient Maps

In this subsection, we are introducing a very important type of relation on a set: the **equivalence relation**. This relation forms a convenient tool to study and construct sets. We will have several occasions to use this type of relations in this course.

Definition 4.3.2 *The relation $R \subseteq A \times A$ is an* **equivalence relation** *on A if R* **is reflexive, symmetric, and transitive**.

A useful way to characterize the equivalence relations is by using the function $R[\cdot]$. Recall that, for any relation $R \subseteq A \times B$, we defined a function $R[\cdot] : A \to \mathcal{P}(B)$ given by

$$x \in A \mapsto R[x] \in \mathcal{P}(B).$$

In general, $R[x]$ may be the empty set, or for some $x, x' \in A$ with $R[x] \neq R[x']$ we may have $R[x] \cap R[x'] \neq \emptyset$. Indeed, let R be the relation $\leq$ on $\mathbb{N}$. In this case, $R[1] \neq R[2]$, but $R[1] \cap R[2] = \{n \,|\, 2 \leq n\} \neq \emptyset$. Take as another example R to be the inverse relation of $<$ on $\mathbb{N}$. In this case $R[0] = \emptyset$.
Well, if R is an equivalence relation on A, and $A \neq \emptyset$, the function $R[\cdot] : A \to \mathcal{P}(A)$ behaves much more gently:

Theorem 4.3.1 *The relation R on $A \neq \emptyset$ is an equivalence relation if, and only if,*
(i) $(\forall x)((x \in A) \to (x \in R[x]))$ *and*
(ii) $(\forall x, x')((R[x] \neq R[x']) \to (R[x] \cap R[x'] = \emptyset))$.

Proof. ($\Rightarrow$) Assume that R is an equivalence relation on A. Since R is reflexive, for every $x \in A$ we have that $(x, x) \in R$, so that $x \in R[x]$. This proves item (i). We will prove item (ii) now. Assume $x'' \in R[x] \cap R[x']$. We want to show that $R[x] = R[x']$. Note first that, since R is symmetric, and transitive, $x \in R[x]$ and $x' \in R[x]$. Indeed, we have $(x, y) \in R \wedge (x', y) \in R$, and so $(x, y) \in R \wedge (y, x') \in R$ which gives that $(x, x') \in R$, and therefore $x' \in R[x]$. Analogously, $x \in R[x']$. But $x' \in R[x]$ implies that $R[x'] \subseteq R[x]$. That is, because $(x', y) \in R \wedge (x, x') \in R$ implies that $(x, y) \in R$, and therefore $y \in R[x]$. In a similar fashion $R[x] \subseteq R[x']$. The two inclusions of equivalence classes prove that $R[x] = R[x']$. Item (ii) is proved.

($\Leftarrow$) We have to prove now that if R is a relation on a non-empty set A and if it has the properties of items (i) and (ii), then R is reflexive, symmetric, and transitive. Item (i) says exactly that for every $x \in A$, $(x, x) \in R$. So R is reflexive. Now, proving the symmetry of R, let $(x, x') \in R$. This means that $x' \in R[x'] \cap R[x]$, and by (ii) it follows that $R[x] = R[x']$, but then $x \in R[x']$ which means that $(x', x) \in R$. In a similar fashion, for the transitivity, we have $(x, x') \in R$ and $(x', x'') \in R$ imply that $R[x] = R[x']$ and $R[x'] = R[x'']$. So, the three sets are equal $R[x] = R[x'] = R[x'']$. In particular, $R[x] = R[x'']$, and $(x, x'') \in R$. The relation R is an equivalence relation. □

Exercise 4.3.2 *Is this theorem true for $A = \emptyset$? Give reasons for your answer.*

Corollary 4.3.2 *If R is an equivalence relation on a non-empty set A, then the set $\{R[x] \,|\, x \in A\}$ consists of non-empty pair-wise disjoint sets such that*

$$\cup\{R[x] \,|\, x \in A\} = A.$$

Proof. Follows directly from the theorem above. □

Exercise 4.3.3 *Prove this Corollary.*

This corollary motivates the following definition.

Definition 4.3.3 *Let A be a non-empty set, and let $B \subseteq \mathcal{P}(A)$. Then, B is a* **partition** *of A if*
(1) $(\forall x)((x \in B) \to (x \neq \emptyset))$;
(2) $(\forall x)(\forall x')((\{x, x'\} \subseteq B \wedge x \neq x') \to (x \cap x' = \emptyset))$;
(3) $\cup B = A$.

By Corollary 4.3.2, we know that every equivalence relation R of a non-empty set A defines a partition of A. This partition is denoted by B_R. The fact of the matter is that, conversely, every partition of a non-empty set A defines a relation on A, which turns out to be an equivalence relation. Namely,

Definition 4.3.4 *Suppose B is a partition of the non-empty set A. Define $R_B \subseteq A \times A$ by declaring that for $x, x' \in A$*

$$(x, x') \in R_B \quad \textit{if} \quad (\exists w)((w \in B) \wedge (\{x, x'\} \subseteq w).$$

Proposition 4.3.3 *For any partition B of a non-empty set A, the relation R_B on A is an equivalence relation.*

Proof. An easy check that R_B is reflexive, symmetric and transitive. □

Exercise 4.3.4 *Prove this Proposition.*

The next theorem reveals the fact that the concepts of equivalence relations on a non-empty set and of partitions of that set are identical. Recall that the relations on a set A comprise a set - the power set $\mathcal{P}(A \times A)$ of $A \times A$. Therefore, the **equivalence relations** on A form a set as well (verify that! That is write down a formula defining the equivalence relations among all relations on A). Denote this set by $EquivRel(A)$. On the other hand, the **partitions** of A are a sub-collection in $\mathcal{P}(A)$, so they form a set as well (write the formula here, too!). Denote that set by $Partit(A)$. The theorem and the proposition above provide us with two maps between $EquivRel(A)$ and $Partit(A)$

$$\varphi_A : EquivRel(A) \to Partit(A) \qquad R \mapsto \varphi_A(R) := B_R$$

and

$$\psi_A : Partit(A) \to EquivRel(A) \qquad B \mapsto \psi_A(B) := R_B.$$

Exercise 4.3.5 *Describe $Partit(\emptyset)$ and $EquivRel(\emptyset)$.*

Theorem 4.3.4 *Let A be a non-empty set. The maps φ_A and ψ_A are inverses of each-other. In other words, for any equivalence relation R on A, we have $R_{B_R} = R$, and, for any partition B of A, we have $B_{R_B} = B$.*

Proof. Let R be an equivalence relation on A. To prove that $R_{B_R} = R \subseteq A \times A$ we have to show that

$$(\forall x, x' \in A)((x, x') \in R \ \leftrightarrow \ (x, x') \in R_{B_R}).$$

But, $(x, x') \in R$ is equivalent to having $R[x] = R[x'] \in B_R$. This latter implies that $(x, x') \in R_{B_R}$. Conversely, if $(x, x') \in R_{B_R}$, then there is an equivalence class $R[x''] \in B_R$ such that $x, x' \in R[x'']$. That is: $(x'', x) \in R$ and $(x'', x') \in R$. But since R is an equivalence relation, $(x, x') \in R$. This completes the proof of $R_{B_R} = R$.
The proof of the coincidence $B = B_{R_B}$ for any partition B of A is left as an exercise. □

Exercise 4.3.6 *Prove, in the notations of the previous theorem, that $B = B_{R_B}$ for any partition B on A.*

The partition determined by an equivalence relation of a non-empty set A has a special name, and numerous uses in math.

Definition 4.3.5 *Let R be an equivalence relation on $A \neq \emptyset$. The partition B_R is called* **the quotient set of A with respect to** *R, and is denoted by A/R. The function $R[\cdot] : A \to \mathcal{P}(A)$ defines a map*

$$\pi_R : A \to A/R$$

called **the quotient map**. *Note that π_R is a surjection.*

By the above, we know that $(x, x') \in R$ if, and only if, $\pi_R(x) = \pi_R(x')$.

Application of Equivalence Relations on a Set

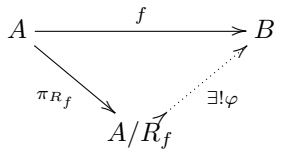
Equivalence relations play a very important role in math. We will use equivalence relations to construct the basic number systems (integers, rational, and real numbers) in the following chapters. In this sub-section we address some promises made as well as some constructions already discussed earlier in the course, and which can be treated by using equivalence relations.

As we mentioned earlier, the three types of set maps, injection, surjection, and bijection, are the most important ones. This is due to the fact that **any** set map can be expressed, in a natural way, as a composition of surjection, followed by a bijection, and an injection. The following exercise discusses some properties of equivalence relations on a set. Item (4) of the exercise, in particular, suggests how to prove this fact above.

Exercise 4.3.7 *(1) This exercise proves in effect that* **every function is a composition of an injection and a surjection both defined in a natural way**.
Let $f : A \to B$ be a function with $A \neq \emptyset$. Define a relation $R_f \subseteq A \times A$ by

$$(\forall x, x')((x, x') \in R_f \quad \textit{if} \quad (f(x) = f(x'))).$$

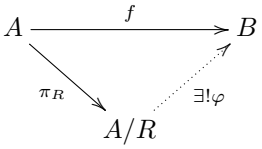
Verify that R_f is an equivalence relation on A. Prove further that there is a unique function $\varphi : A/R_f \to B$ such that $f = \varphi \circ \pi_{R_f}$. Prove that the function φ is an injection.



(2) The fact proved in this exercise describes a **universal property** *satisfied by the quotient map $\pi_R : A \to A/R$. The importance of this, and other universal properties satisfied by set maps, will be revealed in the course of Algebraic Structures where they play important roles.*
Let R be an equivalence relation on $A \neq \emptyset$, and let $\pi_R : A \to A/R$ be the corresponding quotient map. Prove that, for every function $f : A \to B$ such that

$$(\forall x, x')((x, x') \in R \to f(x) = f(x')),$$

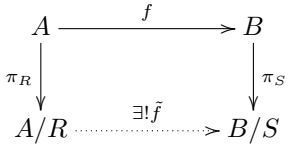
there exists a unique $\varphi : A/R \to B$ such that $f = \varphi \circ \pi_R$.



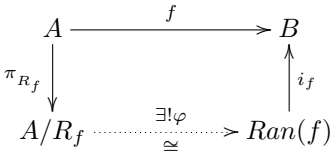
*(3) This exercise is a finer version of the previous two. The set up is as follows. Suppose R is an equivalence relation on $A \neq \emptyset$, and S is an equivalence relation on $B \neq \emptyset$. Suppose further that $f : A \to B$ is $(R - S)$-**equivariant**, that is*

$$(\forall x, x' \in A)((x, x') \in R \to (f(x), f(x')) \in S).$$

Prove that there is a unique map $\tilde{f} : A/R \to B/S$ such that $\tilde{f} \circ \pi_R = \pi_S \circ f$



(4) In this exercise, the proper claim about representing a set map as a composition of surjection, bijection, and injection in a natural way is stated. Prove it.
Let $f : A \to B$ be any set map. Let further $\pi_{R_f} : A \to A/R_f$ and $i_f : Ran(f) \to B$ be the quotient map, and the inclusion map respectively. Prove that there is a unique set map $\varphi : A/R_f \to Ran(f)$ such that $f = i_f \circ \varphi \circ \pi_{R_f}$. Moreover, φ is a bijection.



The quotient map π_{R_f} and the inclusion map i_f are defined "in a natural way" by the map f. The map φ is unique. It is in this sense that the presentation of f as a composition of the named maps is natural.
(5) Let R be (any) relation on $A \neq \emptyset$. Consider the **function** *$R[\cdot] : A \to \mathcal{P}(A)$. By (1) above, (the* **function***) $R[\cdot]$ defines an equivalence relation $R_{R[\cdot]}$ on A. Explain this equivalence relation in terms of R. Who is the quotient set $A/R_{R[\cdot]}$? The same question when R is an equivalence relation on A.*

We discussed earlier in the Notes a description of the concept of multi-set. We used for this description the notion of an indexed family of sets. The next exercise offers another description of multi-sets based on the notion of equivalence relation. It suggests to prove also that the two approaches, by indexed families of sets and by equivalence relation, are equivalent.

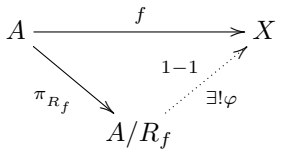
Exercise 4.3.8 *Let R be an equivalence relation on the set A. Let's agree to call two elements of A identical if they are R-related. This will be our new model of a multi-set. Consider the quotient map $\pi_R : A \to A/R$ associated with R as a function, and consider the indexed family of sets it defines. This indexed family describes a multi-set as discussed earlier in this chapter.*
Prove that the two descriptions are equivalent in the following sense.

(i) The description of multi-set using equivalence relation R on a set A determines in a natural way an indexed family of sets $\mathcal{A}$, indexed by A, i.e., $\pi_R : A \to A/R$, and

(ii) the description of a multi-set using indexed family of sets $\mathcal{A}$, indexed by a set A, i.e., $f : A \to X$, determines an equivalence relation on A
in such a way that

(*) if we begin with an equivalence relation R on A, and define the indexed family of sets, the equivalence relation on A the latter defines is R, and

(**) if we begin with an indexed family of sets $f : A \to X$, and define the equivalence relation R_f on A as in (ii), the indexed family of sets associated with the function $\pi_{R_f} : A \to A/R_f$ is naturally isomorphic to the original one. This means that the unique $\varphi : A/R_f \to X$ which exists by item (1) of the previous exercise is a one-to-one with $Ran(\varphi) = Ran(f)$



4.4 Orders

Orders on a set reflect preferences on some elements over others.

4.4.1 Different Types of Orders on a Set

Definition 4.4.1 *Let R be a relation on the set A. This relation is called*
(1) **a pre-order** *on A if R is reflexive and transitive;*

(2) **a partial order** *on A if R is reflexive, anti-symmetric, and transitive;*
(3) **a strict partial order** *on A if R is irreflexive and transitive;*
(4) **a total order** *if R is a connected partial order;*
(5) **a strict total order** *on A if R is a connected strict partial order;*
(6) **dense order** *on A if R is a total order such that*

$$(\forall x \neq y \in A)(\exists z \in A \setminus \{x, y\})(((x, z) \in R \wedge (z, y) \in R)));$$

(7) **to have the least upper bound property** *if*

$$(\forall B \subseteq A)((B \neq \emptyset \wedge \textit{ bounded above in } A) \rightarrow (B \quad \textit{has a least upper bound in } A));$$

(8) **to have the greatest lower bound property** *if*

$$(\forall B \subseteq A)((B \neq \emptyset \wedge \textit{ bounded below in } A) \rightarrow (B \quad \textit{has a greatest lower bound in } A));$$

(9) **a continuous order** *on A if R is dense, and has the least upper bound property.*
(10) **a well order** *on A if R is a partial order and*

$$(\forall B \subseteq A)((B \neq \emptyset) \rightarrow (B \textit{ has a least element w.r.t. } R))$$

where bounded below, bounded above, least element, and least upper bound are defined below.

Example 4.4.1 (1) The relation $\leq$ on $\mathbb{N}$ is a well order. This order is not dense, and has the least upper, and the greatest lower bound properties.

Indeed, the relation is a well order due to Chapter 3 of these Lecture Notes. It is not dense, because there is no natural number strictly between n and $n+1$ for every $n \in \mathbb{N}$. The least upper bound property: Let $\emptyset \neq A \subseteq \mathbb{N}$ be bounded above; so there is $m \in \mathbb{N}$ such that for every $n \in A$, we have $n \leq m$; but then $m + 1 \notin A$, and

$$B = \{m \,|\, m \in \mathbb{N} \wedge m \text{ is a l.u.b. of } A\} \neq \emptyset;$$

so, B has a least element: s; then s is an u.b. of A; it is the a l.u.b. as well, because if there were $s' < s$ such that s' is an upper bound of A, then s' would necessarily be in B, and, for the inequality above, s wouldn't be a least element of B. By the way, s is necessarily in A! Do you see this? In a similar way, one proves that the relation $\leq$ has the greatest lower bound. Do that as an exercise.
(2) The relation $<$ on $\mathbb{N}$ is a strict total order. It is not dense, and has the least upper and the greatest lower bound property.

The arguments here are similar to the ones of item (1) of this exercise.
(3) The relation $\subseteq$ on $\mathcal{P}(A)$, where A is a set, is a partial order. It has the least upper and the greatest lower bound properties.

Checking out the that the definition of partial order is satisfied is straightforward. Let $\mathcal{A} \subseteq \mathcal{P}(A)$ be a non-empty family of subsets of A. The least upper bound is, obviously, $\cup \mathcal{A}$. The greatest lower bound is, equally obviously, $\cap \mathcal{A}$. Check this out!
(4) The relation $\subset$ on $\mathcal{P}(A)$ is a strict partial order. It has the least upper and the greatest lower bound properties. The argument here is similar to the one in item (3) of this exercise. □

4.4.2 Minimal Elements, Maximal Elements, and All That Stuff

Definition 4.4.2 *Let R be a partial order on A.*
(1) $m \in A$ is **a minimal element** *w.r.t. R if $(\forall x \in A)((x, m) \in R \rightarrow x = m)$;*
(2) $M \in A$ is **a maximal element** *w.r.t. R if $(\forall x \in A)((M, x) \in R \rightarrow x = M)$;*
(3) $m \in A$ is **a least/minimum element** *w.r.t. R if $(\forall x \in A)((m, x) \in R)$;*
(4) $M \in A$ is **a greatest/maximum element** *w.r.t. R if $(\forall x \in A)((x, M) \in R)$.*
In what follows $B \subseteq A$.
(5) $u \in A$ is **an upper bound (u.b.)** *of B w.r.t. R if $(\forall z \in B)((z, u) \in R)$; B is called* **bounded**

above *in A if it has an u.b. w.r.t. R;*
(6) $l \in A$ is **a lower bound (l.b.)** *of B w.r.t. R if $(\forall z \in B)(((l,z) \in R))$; B is called* **bounded below** *in A if it has a l.b. w.r.t. R;*
(7) $u \in A$ is **a least upper bound (l.u.b.)** *of B w.r.t. R if u is the least element, w.r.t. R, of the set of upper bounds of B in A.*
(8) $l \in A$ is **a greatest lower bound (g.l.b.)** *of B w.r.t. R if l is the greatest element, w.r.t. R, of the set of lower bounds of B in A.*
(9) $B \subseteq A$ is an **initial segment in** *A w.r.t. R if*

$$(\forall y)((y \in B) \to ((\forall x \in A)((x,y) \in R \to x \in B))).$$

10) $B \subseteq A$ is a **final segment in** *A w.r.t. R if*

$$(\forall y)((y \in B) \to ((\forall x \in A)((y,x) \in R \to x \in B))).$$

Example 4.4.2 (1) It is important in the definitions of least upper and of greatest lower bound property to have $B \neq \emptyset$. Indeed, if $A = \mathbb{N}$, and if the relation is $\leq$ or $<$, then every natural number is an upper and a lower bound of $B = \emptyset \subseteq \mathbb{N}$ Therefore, the least upper bound of B in this case is $0 \in \mathbb{N}$ while the greatest lower bound does not exist.
(2) Every natural number is an initial segment of $(\mathbb{N}, <)$. Indeed, let $n \in \mathbb{N}$, and $m \in n$. For and $s \in \mathbb{N}$ such that $s < m$, we have, by the transitivity if $<$, that $s < n$ as well. By the very definition of $<$, we have that $s \in n$. Similar statement holds true for the relation $\leq$ as well.
(3) Consider $A = \mathcal{P}(X)$ with the relation $\subseteq$ or $\subsetneq$. Let $Y \subseteq X$. Then $\mathcal{P}(Y)$ is an initial segment of A. Indeed, if $Z \in \mathcal{P}(Y)$, then $Z \subseteq Y$, and if $W \subseteq Z$, respectively $W \subsetneq Z$, then $W \subseteq Y$, respectively $W \subsetneq Y$, and therefore $W \in \mathcal{P}(Y)$. The initial segment $\mathcal{P}(Y)$ has Y as its maximum element, i.e. the element. The set $\mathcal{P}(Y) \setminus \{Y\}$ is also an initial segment in $\mathcal{P}(X)$ with the aforementioned relations (check this out), it doesn't have a maximum element, but still has a least upper bound, the set Y itself.
(4) Any set is a partially ordered set w.r.t. inclusion among its elements (these are all sets!). With this order, every $A \neq \emptyset$ has greatest lower bound, given by $\cap A$. Any set A, empty or not, has a least upper bound, given by $\cup A$. $\square$

Exercise 4.4.1 *(1) Prove that if R is a partial order on A, then the relation R' on A define by*

$$(\forall x, x' \in A)((x,x') \in R' \quad \textit{if} \quad ((x,x') \in R) \wedge (x \neq x'))$$

is a strict partial order on A. Conversely, prove that if R is a strict partial order on A, then the relation R' on A defined by

$$(\forall x, x' \in A)((x,x') \in R' \quad \textit{if} \quad ((x,x') \in R) \vee (x = x'))$$

is a partial order on A.
(2) Prove that if R is a pre-order on A, then $R \cap R^{-1}$ is an equivalence relation on A.
(3) Prove that the least upper bounds and the greatest lower bounds are unique whenever they exist.
(4) Prove that if R is a well order on A, then R is a total order which has the least upper bound, and the greatest lower bound properties.
(5) Prove that the relation $\leq$ on $\mathbb{N}$ is not continuous.
(6) Prove that the initial segments of $\mathbb{N}$ w.r.t. either $\leq$ or $<$ are the elements of $\mathbb{N}$ and the set $\mathbb{N}$ itself.
(7) Let B be an initial segments of $\mathcal{P}(X)$ w.r.t. either $\subseteq$ or $\subsetneq$. Prove that if B has maximum element Y in $\mathcal{P}(X)$, then $B = \mathcal{P}(Y)$.
(7') There are many other types of initial segments in $\mathcal{P}(X)$. Let $\{X_\lambda \mid \lambda \in \Lambda\}$ be a family of subsets of X. Prove that $B = \cup\{\mathcal{P}(X_\lambda) \mid \lambda \in \Lambda\}$ is an initial segment in $\mathcal{P}(X)$. As matter of fact, any initial segment in $\mathcal{P}(X)$ is a set of this form: a union of power sets of a family of sub-sets of X.
(8) Let R be a relation on $A \neq \emptyset$ which is a pre-order, a partial order, a total order, or a strict order (partial or total). Consider the **function** *$R[\cdot] : A \to \mathcal{P}(A)$. Explain, in terms of R, the equivalence relation, $R_{R[\cdot]}$, on A determined by that function. Who is the quotient set $A/R_{R[\cdot]}$ (in all cases of R above)?*

4.4.3 Axiom of Choice, Well Orders, Zermelo's Theorem, Zorn's Lemma

In this subsection, we are discussing two theorems which are equivalent to the Axiom of Choice: **Zermelo's Theorem** and **Zorn's Lemma**. The importance of these theorems stems from their wide applicability in different situations in mathematics.

The formulation of Zorn's Lemma needs some preliminaries.

Definition 4.4.3 *Suppose R is a partial order on A, $x, x' \in A$, and $B \subseteq A$.*
(1) The elements x, x' are **(R-)comparable** *if $R_{|\{x,x'\}}$ is a total order on $\{x, x'\}$;*
(2) The subset B is **a chain/an R-chain** *if $R_{|B}$ is a total order on B.*

Consider the following propositions

(Zermelo) Every non-empty set is well orderable.

(Zorn) If R is a partial order on A such that every R-chain B has an upper bound in A, then A has a maximal element.

The German set theorist Ernst Friedrich Ferdinand Zermelo proved, in 1904, the Zermelo's Theorem to the effect that the **Axiom of Choice** is equivalent to **(Zermelo)**. The German algebraist Max Zorn proved, in 1935, the Zorn's Lemma that the **Axiom of Choice** is equivalent to **(Zorn)**. Thirteen years earlier, in 1922, this theorem was proved by the Polish set theorist Kazimierz Kuratowski.

Problem. Using the theory of Axioms 1-8, prove that the **Axiom of Choice**, **(Zermelo)**, and **(Zorn)** are equivalent propositions.

[**Sketch of a Proof**. **(Zorn)⇒(Zermelo)**. Let $X \neq \emptyset$ be given. Assuming **(Zorn)**, we want to show that there is an order R on X which is a well order. The idea of the proof is to consider all subsets of X which have well orders on them, and choose a largest one among them. Turns out, any such largest one has necessarily to be X. So, consider the set

$$\Sigma = \{(Y, S) \,|\, (Y \subseteq X) \wedge (S \subseteq Y \times Y \text{ − well order})\}.$$

For every $(Y, S) \in \Sigma$ and for $y \in Y$, call **initial segment** of y in Y the set

$$Pred_S(y) = \{w \in Y \,|\, (w, y) \in S \wedge w \neq y\}.$$

Define a relation $\preceq$ on Σ as follows

$$(Y, S) \preceq (Y', S') \quad \text{if} \quad (Y \subseteq Y') \wedge (S = S'_{|Y}) \wedge (\forall y \in Y)(Pred_S(y) = Pred_{S'}(y)).$$

This relation is a partial order on Σ (Check this out!). We are verifying next that the premise of **(Zorn)** holds true for $(\Sigma, \preceq)$. To this end, let $\Lambda = \{(Y_\lambda, S_\lambda) \,|\, \lambda \in \Lambda\}$ be a chain in $(\Sigma, \preceq)$. We want to show that Λ has an upper bound in Σ. Let $Y = \cup\{Y_\lambda | \lambda \in \Lambda\}$. Observe that

$$(\forall \lambda \in \Lambda)(\ S_\lambda \subseteq Y_\lambda \times Y_\lambda \subseteq Y \times Y),$$

so that the set $S = \cup\{S_\lambda \,|\, \lambda \in \Lambda\} \subseteq Y \times Y$ defines a relation on Y.

Exercise 4.4.2 *Prove that the relation S can be described also by $(y_1, y_2) \in S$ if, and only if, there is a $\lambda \in \Lambda$ such that $(y_1, y_2) \in S_\lambda$.*

It is straightforward now that S is a total order on Y. This order is actually a well order on Y. Indeed, let $\emptyset \neq Z \subseteq Y$, and let $z_0 \in Z$. By the definition of Y, there is a $\lambda_0 \in \Lambda$ such that $z_0 \in Y_{\lambda_0}$. We claim that

$$Pred_S(z_0) = Pred_{S_{\lambda_0}}(z_0).$$

The inclusion $Pred_{S_{\lambda_0}}(z_0) \subseteq Pred_S(z_0)$ follows from $S_{\lambda_0} \subseteq S$. For the opposite inclusion, let $w \in Pred_S(z_0)$, that is, $(w, z_0) \in S$. By the definition of S, there is a $\mu \in \Lambda$ such that $(w, z_0) \in S_\mu$. Since Λ is a chain in $(\Sigma, \preceq)$, either $(Y_{\lambda_0}, S_{\lambda_0}) \preceq (Y_\mu, S_\mu)$ or $(Y_\mu, S_\mu) \preceq (Y_{\lambda_0}, S_{\lambda_0})$. In either case, by the definition of $\preceq$, we have that $w \in Pred_{S_{\lambda_0}}(z_0)$. This finishes the proof of the claim.
Returning to proving that S is a well order, we are showing that Z has a least element. If z_0 is a least element, we are done. If not, $Pred_S(z_0) \neq \emptyset$, and therefore

$$\emptyset \neq Pred_S(z_0) \cap Z = Pred_{S_{\lambda_0}}(z_0) \cap Z \subseteq Y_{\lambda_0},$$

and therefore $Pred_S(z_0) \cap Z$ has a least element y_0. Since S is a total order on Y, the element y_0 is a least element of Z as well (Prove that!). This finishes the proof that (Y, S) is a well order. This implies that $(Y, S) \in \Sigma$, and that it is an upper bound for Λ.
Having verified that the premise of **(Zorn)** holds true for $(\Sigma, \preceq)$, we conclude that there is a maximal element $(Y_0, S_0) \in \Sigma$. Our last claim is that $Y_0 = X$. This follows from the next Exercise.

Exercise 4.4.3 *Let $Y_0 \subsetneqq X$, and let $z' \in X \setminus Y_0$. Define a relation S' on $Y' = Y_0 \cup \{z'\}$ as follows*

$$S' = S_0 \cup \{(y, z') \,|\, y \in Y_0\} \cup \{(z', z')\}.$$

Prove that $(Y', S') \in \Sigma$, and that $(Y_0, S_0) \preceq (Y', S')$.

Conclude from this Exercise that $Y_0 = Y'$ which is an absurd by the construction of Y'. This finishes the proof of **(Zorn)⇒Zermelo)**.

(Zermelo)⇒(Axiom of Choice). Given X such that $\emptyset \notin X$ we want, assuming **(Zermelo)**, to prove that there is a choice function $F : X \to \cup X$. According to **(Zermelo)**, every element of X is well orderable. Consider, for every $x \in X$, a well order S_x on it, and denote by $x_0 \in x$ the corresponding least element. The function $F : X \to \cup X$ is readily defined: $(\forall x \in X)(F(x) = x_0)$. This completes the proof of **(Zermelo)⇒(Axiom of Choice)**.]

Ideally, we have to prove also that **(Axiom of Choice)⇒(Zorn)** in order to complete the proof of the claim in the Problem. But this implication is really tricky to prove, if no deeper theory of ordinal numbers is used. We leave it to the really diligent students to supply a proof for themselves.

We end this subsection proving that **(Zermelo)⇒(Zorn)**. Our argument (borrowed from Aluffi's book "Algebra, Chapter 0") uses recursion in a significant way.

Proof of **(Zermelo)⇒(Zorn)**. Given a partially ordered set (X, R) which satisfies the premise of **(Zorn)**, we have to prove, using **(Zermelo)**, that (X, R) has a maximal element. By **(Zermelo)**, there is a well order S on X. We are constructing next a chain in (X, R). We are doing that using a function defined recursively, with respect to the order S, on X. To this end, let $x_0 \in X$ be the S-least element of X, and define $F(x_0) = \{x_0\}$. We define $F(x)$ for $x \in X, x \neq x_0$ the following (recursive) way. Suppose F has been defined on $Pred_S(x)$, and consider the set

$$\Sigma_x = \{x\} \cup \{F(y) \,|\, y \in Pred_S(x)\}.$$

If Σ_x is an R-chain, then define $F(x) = \{x\}$. If Σ_x is not an R-chain, define $F(x) = \emptyset$. We claim first that $Dom(F) = X$. Indeed, if not, then

$$\emptyset \neq Y = X \setminus Dom(F) \subseteq X,$$

and since S is a well order, there is an S-least element y_0. Obviously, $Pred_S(y_0) \cap Y = \emptyset$, and therefore F is defined on $Pred_S(y_0)$. But then it is defined for y_0 as well, which means that $y_0 \notin Y$ which contradicts the definition of y_0 as the least element of Y. This proves that $Dom(F) = X$. The chain in (X, R) is defined by $\Lambda = \cup Ran(X)$ (verify as an **exercise** that Λ is indeed an R-chain in X). Since (X, R) satisfies the premise of **(Zorn)**, Λ has an R-upper bound $x' \in X$. We finish our

proof showing that x' is an R-maximal element of X. Observe first that any upper bound y of Λ belongs to Λ. That's because $\Sigma_y \subseteq \Lambda \cup \{y\}$, which implies that Σ_y is an R-chain, and consequently, $F(y) = \{y\}$. Let now $(x', x'') \in R$. Then x'' is an upper bound of Λ as well, and by the just proven property of the upper bounds of Λ, $x'' \in \Lambda$. But then $(x'', x') \in R$ as well, and since R is anti-symmetric, $x' = x''$. This completes the proof of **(Zermelo)⇒(Zorn)**. □

4.4.4 Concluding Remarks

On the Axioms we Introduced

In the previous three chapters, we presented a development of Set Theory based on axioms. In our presentation, we haven't introduced one axiom (the **Axiom of Replacement**, and have used a weaker version of another one: the **Axiom of Foundation**. Both axioms are not needed for our course. The former is useful when working with **Class relations** and with **Class functions**. These are covered in the more complete version of these lecture notes. The latter we discuss briefly here. The Axiom of Foundation states that **every non-empty set is well founded**, that is

$$(\forall X)(X \neq \emptyset \to (\exists x)(x \in X \ \wedge \ x \cap X = \emptyset)).$$

Our Axiom 7 follows from the Axiom of Foundation applying it to the singleton $\{x\}$. Indeed, according to the Axiom of Foundation, $\{x\}$ has an element (there is only one element in it: x) which intersects with the set emptily, that is, $x \cap \{x\} = \emptyset$. The last relation means that $x \notin x$.
The theory of Axioms 1 through 8, with the Axiom of Foundation instead Axiom 7,and with the Axiom of Replacement is the Zermelo-Fraenkel axiomatic Set Theory (ZF). The theory of Axioms 1 through 10 is the aximatic Set Theory of Zermelo-Fraenkel with Axiom of Choice (ZFC). The axioms of ZFC are generally accepted to deal with sets.

As promised in Remark 4.1.2, using the Foundation Axiom we can answer the question if

$$((x, y), z) = (x, (y, z))$$

for some sets x, y and z. Indeed, the equality of the two sets is equivalent to

$$x = (x, y) \quad \text{and} \quad z = (y, z)$$

or, equivalently to

$$x = \{\{x\}, \{x, y\}\} \quad \text{and} \quad z = \{\{y\}, \{y, z\}\}.$$

Since $x \cap \{x\} = \emptyset$, the Foundation Axiom is satisfied by the set x. The same Axiom applied to the set z tells us that $y \notin z$. Contrapositively, if $y \in z$, the equality $z = \{\{y\}, \{y, z\}\}$ is impossible. Therefore, $((x, y), z) = (x, (y, z))$ is also impossible in such a case. As a matter of fact, the latter equality is never possible, even when $y \notin z$, but to prove this we need theory going far beyond the scope of our these Lecture Notes, and which is presented in any decent course on Set Theory.

What Is Coming Next in These Lecture Notes

We already know that the relation $\leq$ on $\mathbb{N}$ has least upper and greatest lower bound properties, but is not dense (verify that!), so - not continuous. In the next part of the course, we will construct, using set theory, the smallest field extension of $\mathbb{N}$ which will inherit the relation $\leq$ from $\mathbb{N}$ as a continuous relation. This extension is needed for the problems in Calculus related to limits of sequences and functions.

We will first construct the set of integers $\mathbb{Z}$ for the purposes of arithmetic. It will inherit the relation $\leq$ from $\mathbb{N}$. On $\mathbb{Z}$ the relation $\leq$ will still not be a dense relation, having both types of bounds. We will construct next the set of rational numbers, $\mathbb{Q}$, again for arithmetic reasons. This set will be a field, the relation $\leq$ will there be dense, but with no least upper and greatest lower bound properties, and therefore - not continuous. Finally, we will construct the set of real numbers

$\mathbb{R}$. The relation $\leq$ will have the needed property of being continuous there.

The sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$ are completely different sets, not sharing any elements. But we will also construct natural injections $\mathbb{N} \to \mathbb{Z}$, $\mathbb{Z} \to \mathbb{Q}$, and $\mathbb{Q} \to \mathbb{R}$ which will allow us to enjoy the usual picture we are familiar with since preschool:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Chapter 5

Construction of the Standard Number Systems

In this chapter, we are giving the construction of the sets of integer numbers, $\mathbb{Z}$, rational numbers, $\mathbb{Q}$, and real numbers, $\mathbb{R}$. For this we use set theoretical tools. The idea is to construct the number systems in such a way that they have two operations - addition and multiplication, and order - all inherited from the set of natural numbers $\mathbb{N}$. In technical terms, the integers form a ring, while the rationals and the reals form fields (that is, in them one can divide by non-zero elements). That's why they are better, from point of view Algebra, than the naturals. On the other hand, the field of reals is better, from point of view of Calculus, than the field of rationals, because in it,contrary to the rationals, limits of sequences exist.
All these sets are "essentially unique", in a sense described below, with their properties. For instance, the set of integers is the smallest ring containing the naturals, the set of rationals is the smallest field containing the integers as a sub-ring, and the set of real numbers is the smallest ordered and complete field which contains the rational numbers as a dense sub-field.

5.1 The Integers

5.1.1 Motivations; Definition of the Set of Integers

In doing arithmetic in $\mathbb{N}$, one is led to consider equations of the type

$$mX + n = s$$

where $m, n, s \in \mathbb{N}$. Assuming, for simplicity, that $m = 1$, one needs to be able to solve the equation

$$X + n = s.$$

Within $\mathbb{N}$ this can be solved only if $n \leq s$. To get a solution without this restriction, we need to **expand** the set of natural numbers so that **all the solutions to that equation for $s < n$ be in it**. Call the expansion X. So, we have $\mathbb{N} \subseteq X$.
The set X has to be constructed in such a way that it retains most of the properties of $\mathbb{N}$. In particular, two operations, addition and multiplication, and a relation, $\leq$, have to be defined on X so that their restriction to $\mathbb{N}$ coincides with the usual operations and the relation on $\mathbb{N}$. The operations on X have to be commutative and associative, they need to have $0, 1 \in \mathbb{N} \subseteq X$ as respective neutral elements, and the multiplication should distribute over the addition. Also, notice that in order to be able to solve the (simplified) equation above, it is enough to have that for every $n \in \mathbb{N}$, there is a $y \in X$ such that $n + x = 0$, and therefore this latter property has to be a feature of X as well. Furthermore, the relation $\leq$ has to be a total order on X with the properties of additive and multiplicative cancellation.
Obviously, any such expansion X of $\mathbb{N}$ will allow us to solve that equation. The **set of integers** is

determined as being a **minimal** such expansion. The minimality can be described by the property that for every $y \in X$ either $y \in \mathbb{N}$, or there is an $n \in \mathbb{N}$ such that $y + n = 0$.
After these preliminary considerations we are ready to give a definition of the set of integers.

Definition 5.1.1 *A set X with two operations $+_X : X \times X \to X$ and $\cdot_X : X \times X \to X$ is called a* **set if integers** *if*
(1) $(X, +_X)$ is a **commutative group**. *That is, $+_X$ is commutative, associative, with neutral element, 0_X, and for every $x \in X$ there is a $y \in X$ such that $x + y = 0_X$;*
(2) $(X, +_X, \cdot_X)$ is a **commutative ring**. *That is, $\cdot_X$ is also commutative, associative with neutral element, 1_X ($1_X \neq 0_X$), and is distributive over $+_X$;*
(3) There is an injection $\varphi_X : \mathbb{N} \to X$ which is a **homomorphism**. *That is for every $n, m \in \mathbb{N}$*

$$\varphi_X(n+m) = \varphi_X(n) +_X \varphi_X(m), \quad \varphi_X(n \cdot m) = \varphi_X(n) \cdot_X \varphi_X(m) \quad \text{and} \quad \varphi_X(1) = 1_X;$$

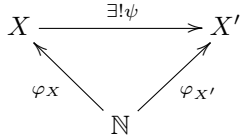
(4) $(\forall\, y \in X)(\exists\, m, n \in \mathbb{N})(y + \varphi_X(n) = \varphi_X(m))$.

Note that there is no mentioning of any relation $\leq$ in this definition. In fact (see the exercise below), such a relation is uniquely determined if we want φ_X to be a **monotone** map, that is for $m \leq n \in \mathbb{N}$ we have $\varphi_X(m) \leq \varphi_X(n)$.

Exercise 5.1.1 *Suppose X is a set of integers, with corresponding map $\varphi_X : \mathbb{N} \to X$, and let $x, y \in X$. Define $x \leq y$ if either $x = \varphi_X(n), y = \varphi_X(m)$ and $n \leq m$, or $x \notin Ran(\varphi_X)$ and $y \in Ran(\varphi_X)$, or $x + \varphi_X(n) = 0, y + \varphi_X(m) = 0$ and $m \leq n$. Prove that $\leq$ defines a total order on X.*

A very important fact is that the set of integers is **essentially unique**. This means that every two such sets can be identified by a uniquely determined bijection. Next theorem gives the precise claim.

Theorem 5.1.1 *Let X and X' be two sets of integers, then there is a unique map $\psi : X \to X'$ such that the triangle commutes (that is, $\varphi_{X'} = \psi \circ \varphi_X$)*



In addition the map ψ is a homomorphism which is a bijection (so, ψ is an isomorphism of rings).

Proof (Sketch) (1) (**Existence** of ψ). Let $x \in X$ and let $x + \varphi_X(m) = \varphi_X(n)$ for some (non-unique!) $m, n \in \mathbb{N}$. There is a unique $x' \in X'$ such that $x' + \varphi_{X'}(m) = \varphi_{X'}(n)$. Define $\psi(x) = x'$. This definition is correct, because if $x + \varphi_X(m_1) = \varphi_X(n_1)$, then $x' + \varphi_{X'}(m_1) = \varphi_{X'}(n_1)$ as well. It is straightforward to check that for this map ψ one has $\varphi_{X'} = \psi \circ \varphi_X$. The himomorphism and bijection claims are left to the reader to prove. (2) (**Uniqueness** of ψ) Suppose $\psi' : X \to X'$ is another such map. By the commutativity relation $\varphi_{X'} = \psi' \circ \varphi_X$ we get that
if $x \in Ran(\varphi_X)$, then

$$\psi'(x) = (\psi' \circ \varphi_X)(m) = \varphi_{X'}(m) = (\psi \circ \varphi_X)(m) = \psi(x)$$

and if $x \notin Ran(\varphi_X)$, then $x + \varphi_X(m) = \varphi_X(n)$, and since ψ' is a homomorphism, we have on one hand

$$\psi'(x + \varphi_X(m)) = \psi'(x) + (\psi' \circ \varphi_X)(m) = \psi'(x) + \varphi_{X'}(m),$$

and on other $\psi'(x + \varphi_X(m)) = (\psi' \circ \varphi_X)(n) = \varphi_{X'}(n)$. This gives us that

$$\psi(x) + \varphi_{X'}(m) = \varphi_{X'}(n) \quad \text{and} \quad \psi'(x) + \varphi_{X'}(m) = \varphi_{X'}(n)$$

which immediately implies that $\psi'(x) = \psi(x)$. $\square$

Again - the theorem says that if integers exist, they are essentially unique. What remains to prove now is that a set of integers exists. This is what we are doing in the following sub-sections. The resulting set, as well as any other set of integers, will be denoted by $\mathbb{Z}$.

Remark 5.1.1 The concepts of a (commutative) group and a (commutative) ring are examples of **algebraic structures** more about which one learns in the courses on Algebraic Structures and Topics in Algebraic Structures. Both, the group $(\mathbb{Z}, +)$, and the ring $(\mathbb{Z}, +, \cdot)$ play central roles in Algebra. □

To solve the original, non-simplified, equation from the beginning of this sub-section, we will have to **expand the integers to include all solutions to that equation** (with the sole restriction $m \neq 0$). This way, we will get the set of rational numbers, which are a **field** - an example of yet another algebraic structure.

The moral here is: the integers and the rational numbers are constructed for the needs of Arithmetic and Algebra.

5.1.2 Construction of a Set of Integers: $\mathbb{Z}$

The Set $\mathbb{Z}$

Consider the set $X = \mathbb{N} \times \mathbb{N}$. Define the relation $R \subseteq X \times X$ by

$$((n, m), (n', m')) \in R \quad \text{if} \quad n + m' = n' + m.$$

Exercise 5.1.2 *Prove that R is an equivalence relation on X.*

Definition 5.1.2 *The quotient set $X/R = (\mathbb{N} \times \mathbb{N})/R$ is called* **the set of integers***, and is denoted by $\mathbb{Z}$.*

Exercise 5.1.3 *(1) Prove that if $m \leq n$, so that $n = m + s$ for some $s \in \mathbb{N}$, then $R[(n, m)] = R[(s, 0)]$. Prove also that $(\forall s_1, s_2 \in \mathbb{N})((s_1 \neq s_2) \to R[(s_1, 0)] \neq R[(s_2, 0)])$.*
(2) Prove that if $n \leq m$, so that $m = n + s$ for some $s \in \mathbb{N}$, then $R[(n, m)] = R[(0, s)]$. Prove also that $(\forall s_1, s_2 \in \mathbb{N})((s_1 \neq s_2) \to R[(0, s_1)] \neq R[(0, s_2)])$.
(3) Conclude from (1) and (2) that

$$\mathbb{Z} = \{R[(s, 0)], R[(0, s)], R[(0, 0)] \mid 0 \neq s \in \mathbb{N}\},$$

and that the RHS of the equality is a family of disjoint sets. In other words, every integer has a unique representative (n, m) where at least one of the components of the order pair is 0.

The Ordered Ring $\mathbb{Z}$

We introduce next two operation and a relation on $\mathbb{Z}$ which will make this set and ordered ring.

Definition 5.1.3 *(1) The* **addition** $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *is defined by*

$$R[(n, m)] + R[(n', m')] := R[(n + n', m + m')].$$

(2) The **multiplication** $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *is defined by*

$$R[(n, m)] \cdot R[(n', m')] := R[(nn' + mm', nm' + n'm)].$$

The **relation** $\leq$ *on $\mathbb{Z}$ is defined by*

$$R[(n, m)] \leq R[(n', m')] \quad \text{if} \quad n + m' \leq n' + m.$$

In this definition, there is a hidden problem which has to be dealt with. Namely, all the three items of the definition use **particular representatives** of the classes involved in order to define the RHSs in (1) and (2) or check the relation in (3)! The first thing to convince ourselves here is that **no choices affect the results** in each of the three items.

Proposition 5.1.2 *The definitions of the two operations, $+$ and $\cdot$, and of the relation $\leq$ above do not depend on any choices made.*

Proof. (Sketch) For the addition, we have to show that if $R[(n,m)] = R[(n_1,m_1)]$ and if $R[(n',m')] = R[(n'_1,m'_1)]$, then $R[(n+n',m+m')] = R[(n_1+n'_1,m_1+m'_1)]$. But the first two equalities mean that $n+m_1 = n_1+m$ and $n'+m'_1 = n'_1+m'$ which immediately implies that

$$(n+m_1)+(n'+m'_1) = (n_1+m)+(n'_1+m') = (n_1+n'_1)+(m+m')$$

due to the commutativity and associativity of addition in $\mathbb{N}$. This proves our claim.
For the multiplication, one has to show that

$$R[(nn'+mm', nm'+n'm)] = R[(n_1n'_1+m_1m'_1, n_1m'_1+n'_1m_1)]$$

which is left as an **exercise**.
For the relation, one has to show that if $R[(n,m)] \leq R[(n',m')]$, then $R[(n_1,m_1)] \leq R[(n'_1,m'_1)]$ as well. We have, by the hypothesis, that $n+m' \leq n'+m$, and that $n+m_1 = m+n_1$ and $n'+m'_1 = m'+n'_1$. We want to show that $n_1+m'_1 \leq n'_1+m_1$. To this end, observe that

$$n+m' \leq m+n' \quad \Rightarrow \quad (n+m')+(n'_1+m_1) \leq (m+n')+(n'_1+m_1)$$

$$\Rightarrow (n+m_1)+(m'+n'_1) \leq (m+n')+(n'_1+m_1) \quad \Rightarrow \quad (n_1+m)+(n'+m'_1) \leq (m+n')+(n'_1+m_1)$$

$$\Rightarrow \quad (m+n')+(n_1+m'_1) \leq (m+n')+(n'_1+m_1) \quad \Rightarrow \quad n_1+m'_1 \leq n'_1+m_1.$$

All the implications are due to the properties of addition and $\leq$ in $\mathbb{N}$. $\square$

Exercise 5.1.4 *Verify that if*

$$R[(n,m)] = R[(n_1,m_1)] \qquad \textit{and} \qquad R[(n',m')] = R[(n'_1,m'_1)],$$

then

$$R[(nn'+mm', nm'+n'm)] = R[(n_1n'_1+m_1m'_1, n_1m'_1+n'_1m_1)].$$

The following theorem establishes some of the properties of the two operations, $+, \cdot$. According to these, $(\mathbb{Z},+,\cdot)$ **is a (commutative) ring** with zero the class $R[(0,0)]$, and identity - the class $R[(1,0)]$.

Theorem 5.1.3 *Let $x,y,z \in \mathbb{Z}$. The following hold true for $(\mathbb{Z},+,\cdot)$:*
(1) The addition is commutative, associative, has a neutral element, and every element has an opposite:

$$x+y = y+x \qquad x+(y+z) = (x+y)+z$$

$$(\forall x)(x+R[(0,0)] = x) \qquad (\forall x)(\exists x')(x+x' = R[(0,0)]).$$

(2) The multiplication is commutative, associative, and has a neutral element

$$x \cdot y = y \cdot x \qquad x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

$$(\forall x)(x \cdot R[(1,0)] = x).$$

(3) The multiplication distributes over the addition

$$x \cdot (y+z) = x \cdot y + x \cdot z.$$

Proof. See the exercise below. □

Exercise 5.1.5 *Prove the just stated theorem.*

Exercise 5.1.6 *(1) Prove that the neutral element of the addition is unique. That is*

$$((\forall w)(\forall x)(x + w = x)) \to (w = R[(0, 0)]).$$

This unique element is denoted by $0_{\mathbb{Z}}$.
(2) Prove that the neutral element of the multiplication is unique. That is

$$((\forall w)(\forall x)(x \cdot w = x)) \to (w = R[(1, 0)]).$$

This unique element is denoted by $1_{\mathbb{Z}}$.
(3) Prove that the opposite elements are unique. That is

$$(\forall R[(n, m)])(\forall x)((R[(n, m)] + x = 0_{\mathbb{Z}}) \to (x = R[(m, n)])).$$

The opposite element of x *is denoted by* $-x$. *Prove also that*

$$(\forall x)(-(-x) = x).$$

(4) Prove that, for $x, y \in \mathbb{Z}$ *we have*

$$(-x)y = x(-y) = -(xy) \qquad \textit{and} \qquad (-x)(-y) = xy.$$

We are ready to solve the equation, for any $a, b \in \mathbb{Z}$,

$$X + a = b,$$

as promised. The (unique!) solution is given by $X_0 = b + (-a)$.

The next theorem establishes the main properties of the relation $\leq$ including its relationship with the two operations on $\mathbb{Z}$.

Theorem 5.1.4 *The relation* $\leq$ *on* $\mathbb{Z}$ *has the following properties.*
(1) It is **a total order**, *which* **has the least upper and the greatest lower bound properties**;
*(2) (***Additive Cancellation***)* $(\forall x, y, z \in \mathbb{Z})((x + z \leq y + z) \Leftrightarrow (x \leq y))$;
*(3) (***Monotonicity of Addition***)* $((a \leq b) \wedge (c \leq d)) \to (a + c \leq b + d)$, *and if in addition* $(a < b) \vee (c < d)$, *then* $a + c < b + d$;
(4) $(0_{\mathbb{Z}} < a \cdot b) \Leftrightarrow ((0_{\mathbb{Z}} < a) \wedge (0_{\mathbb{Z}} < b)) \vee (a < 0_{\mathbb{Z}}) \wedge (b < 0_{\mathbb{Z}}))$.
*(5) (***Monotonicity of Multiplication***)* *Let* $y < z$. *Prove that for every* $0_{\mathbb{Z}} < x \in \mathbb{Z}$ *we have* $y \cdot x < z \cdot x$. *Prove also that if* $x < 0_{\mathbb{Z}}$, *then* $z \cdot x < y \cdot x$.

Proof. (1): Showing that the order is total. Let $x = R[(m, n)]$ and $y = R[(m', n')]$. Since $\mathbb{N}$ is totally ordered, we have for the natural numbers $m + n'$ and $m' + n$ that

$$\text{either} \quad m + n' \leq m' + n \quad \text{or} \quad m' + n \leq m + n'.$$

In the first case we have $x \leq y$ while in the second we have that $y \leq x$. In any case, x and y are $\leq$-comparable.
Showing that $(\mathbb{Z}, \leq)$ has the greatest lower bound property. Let $A \subseteq \mathbb{Z}$ be a bounded below non-empty subset. So, there is a $x_0 \in \mathbb{Z}$ such that for every $y \in A$ we have $x_0 \leq y$. Consider the set

$$A' = \{y + (-x_0) \,|\, y \in A\}.$$

This set is obviously bounded below by $0_{\mathbb{Z}}$. Therefore, for every $z \in A'$ we have $z = R[(m, n)]$ such that $n \leq m$. As we know then there is an $s \in \mathbb{N}$ such that $n + s = m$, and therefore $z = R[(s, 0)]$ as well. Now consider the set

$$A'' = \{s \in \mathbb{N} \,|\, R[(s, 0)] \in A'\}.$$

We have that $\emptyset \neq A'' \subseteq \mathbb{N}$, and has therefore a least element s_0. Let $z_0 = R[(s_0, 0)] \in A'$ be the corresponding element in A'. By the definition of A', we have that $z_0 = x_0 + y_0$ where $y_0 \in A$. We will show that y_0 is a greatest lower bound of A. Indeed, let $y \in A$, and let $z = x_0 + y$ be its corresponding element in A'. We have $z_0 \leq z$ in A'. So, $x_0 + y_0 \leq x_0 + y$ in $\mathbb{Z}$. By item (2) we get that $y_0 \leq y$. We just proved that y_0 is a lower bound of A. Since $y_0 \in A$, it is the greatest lower bound of A.
Proving that $\mathbb{Z}$ has the least upper bound property is left as an exercise.
(2) Let $x = R[(m, n)], y = R[(m', n')]$ and $z = R[(m'', n'')]$. The direction ($\Leftarrow$) is straightforward, and is left as an easy exercise. Proving ($\Rightarrow$). We have

$$x + z = R[(m + m'', n + n'')] \quad \text{and} \quad y + z = R[(m' + m'', n' + n'')].$$

Therefore $x + z \leq y + z$ means that

$$m + m'' + n' + n'' \leq m' + m'' + n + n''.$$

By the cancellation property for the addition in $\mathbb{N}$, we have that $m + n' \leq m' + n$ which means that $x = R[(m, n)] \leq R[(m', n')] = y$ as claimed.
(3) The inequalities $a \leq b$ and $c \leq d$ give that

$$a + c \leq b + c \quad \text{and} \quad b + c \leq b + d$$

which imply that $a + c \leq b + d$. The second claim in (3) is done by, say, RAA, and is left as an exercise.
(4) The direction ($\Leftarrow$) is straightforward. The opposite direction, ($\Rightarrow$) is proved by RAA, and is left as an exercise.
(5) This follows directly from item (4). Indeed, $y < z$ means that $0_{\mathbb{Z}} < z + (-y)$, and by (4), since $0_{\mathbb{Z}} < x$, we have

$$0_{\mathbb{Z}} < (z + (-y)) \cdot x = zx + (-y)x = zx + (-(yx)).$$

Therefore $yx < (zx + (-(yx))) + yx = zx$ and $yz < xz$ as claimed. The second claim in item (5) is left as an exercise. □

Exercise 5.1.7 *(1) Let $A \subseteq \mathbb{Z}$, and $B = \{x \mid -x \in A\}$. Prove that A is bounded above if, and only if, B is bounded below. Conclude that if A is bounded above, then A has a least upper bound (which belongs to A).*

[Use that $\mathbb{Z}$ has the greatest lower bound property.]

(2) Prove the second claim in item (3) of the theorem above.
(3) Prove item (4) of the theorem above.
(4) Prove the second claim in item (5) of the theorem above.

Remark 5.1.2 A ring with a total partial order $(R, +, \cdot, \leq)$ is called an **ordered ring** if for every $x, y, z \in R$ we have that $(x < y \rightarrow x + z < y + z)$ and $((x < y) \wedge (0 < z)) \rightarrow (xz < yz)$. The theorem above confirms in particular that $(\mathbb{Z}, +, \cdot, <)$ is an **ordered ring**. It can be proved that any ordered ring has a copy of $(\mathbb{Z}, +, \cdot, \leq)$ in itself. □

Exercise 5.1.8 *(1) Prove that if $(a < 0_{\mathbb{Z}}) \wedge (b < 0_{\mathbb{Z}})$, then $a + b < 0_{\mathbb{Z}}$. Similarly, if $(0_{\mathbb{Z}} < a) \wedge (0_{\mathbb{Z}} < b)$, then $0_{\mathbb{Z}} < a + b$.*
(2) Prove that for any $0 \neq s \in \mathbb{N}$

$$0_{\mathbb{Z}} < R[(s, 0)] \quad \wedge \quad R[(0, s)] < 0_{\mathbb{Z}}.$$

(3) Prove that $\leq$ is not a dense relation.
(4) Define the function $|\bullet| : \mathbb{Z} \rightarrow \mathbb{Z}$ by

$$|x| = \begin{cases} x & \text{if} \quad 0_{\mathbb{Z}} \leq x \\ -x & \text{if} \quad x < 0_{\mathbb{Z}} \end{cases}$$

Prove that
(i) $(\forall x)(0_{\mathbb{Z}} \leq |x| \wedge (|x| = 0_{\mathbb{Z}} \to x = 0_{\mathbb{Z}})$*;*
(ii) $(\forall x, y)(|x \cdot y| = |x| \cdot |y|)$*;*
(iii) $(\forall x, y)(|x + y| \leq |x| + |y|)$.

Definition 5.1.4 *The set* $\mathbb{Z}_+ := \{x \in \mathbb{Z} \,|\, 0_{\mathbb{Z}} < x\}$ *is called* **the set of positive integers**. *The set* $\mathbb{Z}_- := \{x \in \mathbb{Z} \,|\, x < 0_{\mathbb{Z}}\}$ *is called* **the set of negative integers**. *The set* $\mathbb{Z}_{\geq 0} := \{x \in \mathbb{Z} \,|\, 0_{\mathbb{Z}} \leq x\}$ *is called* **the set of non-negative integers**.

In these notations, $\mathbb{Z}_{\geq 0} = \{R[(s,0)] \,|\, s \in \mathbb{N}\}$, $\mathbb{Z}_+ = \{R[(s,0)] \,|\, 0 \neq s \in \mathbb{N}\}$, and $\mathbb{Z}_- = \{R[(0,s)] \,|\, 0 \neq s \in \mathbb{N}\}$.

Natural Numbers as a Subset of the Integers

It is obvious by the construction of $\mathbb{Z}$ that $\mathbb{N}$ and $\mathbb{Z}$ are disjoint sets. It is convenient though to identify a subset of $\mathbb{Z}$ which has the same properties as $\mathbb{N}$ does, that is **a copy of** $\mathbb{N}$ in $\mathbb{Z}$. This is done by designing a function from $\mathbb{N}$ to $\mathbb{Z}$ such that both operations and the relation on $\mathbb{N}$ are mapped to the corresponding ones in $\mathbb{Z}$. Such a function is called a **monotone homomorphism**. More specifically, we have the following.

Theorem 5.1.5 *Consider the function* $\varphi_{\mathbb{Z}} : \mathbb{N} \to \mathbb{Z}$ *defined by*

$$(\forall n)(\varphi_{\mathbb{Z}}(n) = R[(n,0)].$$

This function is a monotone homomorphism w.r.t. the operations $+, \cdot$ *and the relation* $\leq$*:*

$$\varphi_{\mathbb{Z}}(n + n') = \varphi_{\mathbb{Z}}(n) + \varphi_{\mathbb{Z}}(n') \qquad \varphi_{\mathbb{Z}}(n \cdot n') = \varphi_{\mathbb{Z}}(n) \cdot \varphi_{\mathbb{Z}}(n')$$

$$n \leq n' \quad \Leftrightarrow \quad \varphi_{\mathbb{Z}}(n) \leq \varphi_{\mathbb{Z}}(n').$$

Also, $\varphi_{\mathbb{Z}}$ *is an injection with* $Range(\varphi_{\mathbb{Z}}) = \mathbb{Z}_{\geq 0}$.

Proof. Straightforward and simple. Note that $\varphi_{\mathbb{Z}}(0) = 0_{\mathbb{Z}}$ and $\varphi_{\mathbb{Z}}(1) = 1_{\mathbb{Z}}$. □

Using $\varphi_{\mathbb{Z}}$ we identify $\mathbb{N}$ to $\mathbb{Z}_{\geq 0}$, and denote every element of the latter by the name of the element of the former it is identified with: $n := R[(n,0)]$. According to the notations we accepted then $-n := R[(0,n)]$, so that

$$\mathbb{Z} = \mathbb{Z}_- \sqcup \{0_{\mathbb{Z}}\} \sqcup \mathbb{Z}_+ = \{0, -1, 1, -2, 2, \ldots, -n, n, \ldots\},$$

and we are in the realm of the notations we have been used to since pre-school.

The Operation Subtraction in $\mathbb{Z}$

Speaking of pre-school, we have been taught that there is a third operation on $\mathbb{Z}$: subtraction! The definition of this is as follows

$$- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

$$(x, y) \mapsto x - y := x + (-y).$$

Notice that this operation is an "ugly" one: it is neither commutative, nor associative! It is maybe worthwhile mentioning that every integer is a difference of two natural numbers. Indeed, if $x = R[(n,m)]$, then $x = n - m$. Keep in mind though that this presentation is by no means unique! (Why?) Looking back in our construction of $\mathbb{Z}$, we see that the definition of integers we used was "modeled" on this, post-factum, presentation.

5.2 The Rational Numbers

5.2.1 Motivations; Definition of the Set of Rational Numbers

Having defined and constructed the set of integers, we turn in this section to solving the equation

$$aX + b = c$$

for integer numbers a, b and c. Obviously, this problem reduces to solving

$$aX = d \qquad (d = c - b).$$

We observe first that if $a = 0$, then solution exists only if $d = 0$, and if this is the case, every integer is a solution. So, the interesting case to consider is when $a \neq 0$. In this case, solution in integers may or may not exist. If we want to be able to always find a solution, then we have to, as we did in the case of the integers, to expand the integers to a set which has the properties of $\mathbb{Z}$, so it should be a ring having $\mathbb{Z}$ as a sub-ring, and which contains the solutions to our equation for every $a \neq 0$ and d. As it was in the case of the integers, we want this expansion to be minimal: ideally, it should contain no more than the solutions to the equation above.
We observe second that to solve the equation above, it is enough the expansion of $\mathbb{Z}$ to have the property that for every non-zero integer n there exists an element x of the expansion so that $n \cdot x = 1$. Any such expansion of $\mathbb{Z}$ is called **a set of rational numbers**. Here is the expected definition.

Definition 5.2.1 *Let $(Y, +_Y, \cdot_Y)$ be a commutative ring. It is called* **a set of rational numbers**, *and denoted by $\mathbb{Q}$, if*
(1) $(\forall\, 0 \neq y \in Y)(\exists w \in Y)(y \cdot_Y w = 1_Y)$. A commutative ring with this property is called a **field**;
(2) There is an injection $\varphi_Y : \mathbb{Z} \to Y$ which is a ring homomorphism, that is,

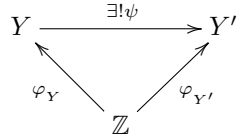
$$\varphi_Y(m+n) = \varphi_Y(m) +_Y \varphi_Y(n) \qquad \varphi_Y(m \cdot n) = \varphi_Y(m) \cdot_Y \varphi_Y(n) \qquad \varphi_Y(1) = 1_Y;$$

(3) $(\forall x \in Y)(\exists m, n \in \mathbb{Z})((n \neq 0) \wedge (\varphi_Y(n) \cdot_Y x = \varphi_Y(m)))$.

As it was in the case of the integers, there is no mentioning about a relation $\leq$ on Y, but it is automatically induced by φ_Y. This will be explained in the following sub-section.

The first thing to prove here is that the sets of rational numbers are canonically identifiable with each other. Here is the respective theorem.

Theorem 5.2.1 *For every two sets of rational numbers Y and Y', there is a unique map $\psi : Y \to Y'$ such that $\psi \circ \varphi_Y = \varphi_{Y'}$. That is, the triangle below commutes.*



The map ψ is a bijective homomorphism of rings (so, it is an **isomorphism** *of rings).*

Proof (Sketch) The proof is similar to the one for integers in the previous subsection. (1) (**Existence of** ψ) If $y \in Y$ is such that $y \in Ran(\varphi_Y)$, and $y = \varphi_Y(n)$, then define $\psi(y) = \varphi_{Y'}(n)$. If $y \notin Ran(\varphi_Y)$, then let (the non-unique!) $n, m \in \mathbb{Z}$ such that $n \neq 0$, and $y \cdot_Y \varphi_Y(n) = \varphi_Y(m)$. There is a unique $y' \in Y'$ such that $y' \cdot_{Y'} \varphi_{Y'}(n) = \varphi_{Y'}(m)$. Define in this case $\psi(y) = y'$. Again, one proves that this definition is correct: does not depend on the choice of m and $n \neq 0$ above. Then, one also checks that this ψ is a bijection and a ring homomorphism. (2) (**Uniqueness of** ψ) Let ψ' be another such map. We have to show that $\psi' = \psi$. Let $y \in Y$, and let $n \neq 0$ and m be integers so that $y \cdot_Y \varphi_Y(n) = \varphi_Y(m)$. Since ψ' is a homomorphism, we have

$$\psi'(y \cdot_Y \varphi_Y(n)) = \psi'(\varphi_Y(m)) \quad \Rightarrow \quad \psi'(y) \cdot_{Y'} \psi'(\varphi_Y(n) = \psi'(\varphi_Y(m))$$

$$\Rightarrow \quad \psi'(y) \cdot_{Y'} \varphi_{Y'}(n) = \varphi_{Y'}(m)$$

which, together with $\psi(y) \cdot_{Y'} \varphi_{Y'}(n) = \varphi_{Y'}(m)$ implies that $\psi'(y) = \psi(y)$. Since this is true for every $y \in Y$, the two functions are equal. □

The theorem says that if a set of rational number exists, then it is essentially unique. What we have to prove next is that a set of rational numbers does exist. We are doing this in the next sub-section.

5.2.2 Construction of a Set of Rational Numbers: $\mathbb{Q}$

The Set $\mathbb{Q}$

Consider the set $X = \mathbb{Z} \times \mathbb{Z}_+$. Define a relation R on X by

$$((x, n), (y, m)) \in R \quad \text{if} \quad x \cdot m = y \cdot n.$$

Exercise 5.2.1 *Prove that R is an equivalence relation on X.*

Definition 5.2.2 *The quotient set $X/R = (\mathbb{Z} \times \mathbb{Z}_+)/R$ is called* **the set of rational numbers**, *and is denoted by $\mathbb{Q}$.*

Remark 5.2.1 As it was in the case of integers, every rational number has a special, uniquely determined representative. This representative is an ordered pair $(x, n) \in \mathbb{Z} \times \mathbb{Z}_+$ such that the integers x and n share no common factors, different from ± 1. To prove this, one needs certain knowledge from elementary number theory, and we omit it here. □

The Ordered Field $\mathbb{Q}$

We are introducing next two operations, addition and multiplication, and a relation, $\leq$, on $\mathbb{Q}$ which will make the set an ordered field.

Definition 5.2.3 *(1) The* **addition** $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ *is defined by*

$$R[(x, n)] + R[(y, m)] := R[(xm + yn, nm)].$$

(2) The **multiplication** $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ *is defined by*

$$R[(x, n)] \cdot R[(y, m)] := R[(xy, nm)].$$

(3) The **relation** $\leq$ *is defined by*

$$R[(x, n)] \leq R[(y, m)] \quad \textit{if} \quad xm \leq yn.$$

Proposition 5.2.2 *The definitions of the two operations, $+, \cdot$, and of the relation $\leq$ do not depend on any choices made to formulate them.*

Proof. A straightforward exercise. □

Exercise 5.2.2 *Prove the Proposition above.*

The following theorem collects some of the properties of the operations $+, \cdot$, and actually states that $\mathbb{Q}$ is a **field**.

Theorem 5.2.3 *Let $x, y, z \in \mathbb{Q}$. The following holds true for $(\mathbb{Q}, +, \cdot)$*
(1) The addition is commutative, associative, has a neutral element, and every element has an opposite:

$$x + y = y + x \qquad x + (y + z) = (x + y) + z$$

$$(\forall x)(x + R[(0,1)] = x) \qquad (\forall x)(\exists x')(x + x' = R[(0,1)]).$$

(2) The multiplication is commutative, associative, has a neutral element, and every non-zero rational number has a reciprocal:

$$x \cdot y = y \cdot x \qquad x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

$$(\forall x)(x \cdot R[(1,1)] = x) \qquad (\forall x)((x \neq R[(0,1)]) \to (\exists y)(x \cdot y = R[(1,1)])).$$

(3) The multiplication distributes over the addition

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

Proof. The proof is straightforward , and is left as an exercise. □

Exercise 5.2.3 *Prove the theorem above.*

Remark 5.2.2 As stated already, the claims in the theorem above mean that $(\mathbb{Q}, +, \cdot)$ is a **field**. A field is a commutative ring such that every non-zero element has a reciprocal. The ring $\mathbb{Z}$ is not a field. □

Exercise 5.2.4 *(1) Prove that the neutral element of the addition is unique. That is*

$$((\forall w)(\forall x)(x + w = x)) \to (w = R[(0,1)]).$$

This unique element is denoted by $0_{\mathbb{Q}}$.
(2) Prove that the neutral element of the multiplication is unique. That is

$$((\forall w)(\forall x)(x \cdot w = x)) \to (w = R[(1,1)]).$$

This unique element is denoted by $1_{\mathbb{Q}}$.
(3) Prove that the opposite elements are unique. That is

$$(\forall R[(x,n)])(\forall w)((R[(x,n)] + w = 0_{\mathbb{Q}}) \to (w = R[(-x,n)])).$$

The opposite element of x is denoted by $-x$. Prove also that

$$(\forall x)(-(-x) = x).$$

(4) Prove that the reciprocal elements are unique, when they exist. That is

$$(\forall x \neq 0_{\mathbb{Q}})(\forall y, z)((x \cdot y = 1_{\mathbb{Q}} \wedge x \cdot z = 1_{\mathbb{Q}}) \to (y = z)).$$

The unique reciprocal element corresponding to $x \neq 0_{\mathbb{Q}}$ is denoted by x^{-1}. Prove also that

$$(\forall x \neq 0_{\mathbb{Q}})((x^{-1})^{-1} = x).$$

(5) Prove that for $x, y \in \mathbb{Q}$ we have

$$(-x)y = x(-y) = -(xy) \quad \textit{and} \quad (-x)(-y) = xy.$$

(6) Prove that for every non-zero $x, y \in \mathbb{Q}$ we have

$$(xy)^{-1} = x^{-1}y^{-1}.$$

We are ready to solve the equation, even for any $a \neq 0_{\mathbb{Q}}, d \in \mathbb{Q}$,

$$aX = d,$$

as promised. The (unique!) solution is given by $X_0 = d \cdot a^{-1}$.

The next theorem establishes the main properties of the relation $\leq$ including its relationship with the two operations on $\mathbb{Q}$.

Theorem 5.2.4 *The relation $\leq$ on $\mathbb{Q}$ has the following properties.*
(1) It is **a total order**, *which is* **dense**;
*(2) (***Additive Cancellation***)* $(\forall x, y, z \in \mathbb{Q})((x + z \leq y + z) \Leftrightarrow (x \leq y))$;
*(3) (***Monotonicity of Addition***)* $((a \leq b) \wedge (c \leq d)) \rightarrow (a + c \leq b + d)$, *and if in addition* $(a < b) \vee (c < d)$, *then* $a + c < b + d$;
(4) $(0_{\mathbb{Q}} < a \cdot b) \Leftrightarrow ((0_{\mathbb{Q}} < a) \wedge (0_{\mathbb{Q}} < b)) \vee (a < 0_{\mathbb{Q}}) \wedge (b < 0_{\mathbb{Q}}))$.
*(5) (***Monotonicity of Multiplication***)* *Let $y < z$, and if x be rational numbers. If $0_{\mathbb{Q}} < x$, then $y \cdot x < z \cdot x$, and if $x < 0_{\mathbb{Q}}$, then $z \cdot x < y \cdot x$.*

Proof. We are proving item (1) only. The rest are left as an exercise. To prove (1), let $x, y \in \mathbb{Q}$ such that $x = R[(a, n)]$ and $y = R[(b, m)]$ The numbers am and bn are integers, so either $am \leq bn$ or $bn \leq am$. In the former case $x \leq y$, in the latter case $y \leq x$. The order $\leq$ on $\mathbb{Q}$ is total. The order is also dense. Indeed, let $x < y$ be two rational numbers. By item (2) we get that $x + x < x + y$ and $x + y < y + y$. Therefore $x < (x + y)/2 < y$, and we are done (notice that $(x + y)/2 \in \mathbb{Q}$). □

Exercise 5.2.5 *Prove items (2), (3), (4), and (5) of the theorem above.*

Remark 5.2.3 A field with a total partial order $(L, +, \cdot, \leq)$ is called an **ordered field** if for every $x, y, z \in R$ we have that $x < y \rightarrow x + z < y + z$ and $x < y \wedge 0 < z \rightarrow xz < yz$. The theorem above confirms in particular that $(\mathbb{Q}, +, \cdot, \leq)$ ordered field. It can be shown that every ordered field has a copy of $(\mathbb{Q}, +, \cdot, \leq)$ in itself. □

Exercise 5.2.6 *(1) Prove that if $(a < 0_{\mathbb{Q}}) \wedge (b < 0_{\mathbb{Q}})$, then $a + b < 0_{\mathbb{Q}}$. Similarly, if $(0_{\mathbb{Q}} < a) \wedge (0_{\mathbb{Q}} < b)$, then $0_{\mathbb{Q}} < a + b$.*
(2) Prove that

$$0_{\mathbb{Q}} < R[(x, n)] \quad \Leftrightarrow \quad x \in \mathbb{Z}_+.$$

(3) Prove that $(\mathbb{Q}, \leq)$ has the least upper bound property if, and only if, it has the greatest lower bound property.
(4) Define the function $|\bullet| : \mathbb{Q} \rightarrow \mathbb{Q}$ by

$$|x| = \begin{cases} x & \text{if} \quad 0_{\mathbb{Q}} \leq x \\ -x & \text{if} \quad x < 0_{\mathbb{Q}} \end{cases}$$

Prove that
(i) $(\forall x)(0_{\mathbb{Q}} \leq |x| \wedge (|x| = 0_{\mathbb{Q}} \rightarrow x = 0_{\mathbb{Q}}))$;
(ii) $(\forall x, y)(|x \cdot y| = |x| \cdot |y|)$;
(iii) $(\forall x, y)(|x + y| \leq |x| + |y|)$.

The Set $\mathbb{Z}$ as a Subset of $\mathbb{Q}$

It is obvious by the construction of $\mathbb{Q}$ that $\mathbb{Z}$ and $\mathbb{Q}$ are disjoint sets. It is convenient though to identify a subset of $\mathbb{Q}$ which has the same properties as $\mathbb{Z}$ does, that is **a copy of** $\mathbb{Z}$ in $\mathbb{Q}$. This is done by designing a function from $\mathbb{Z}$ to $\mathbb{Q}$ such that both operations and the relation on $\mathbb{Z}$ are mapped to the corresponding ones in $\mathbb{Q}$. Such a function is called a **monotone homomorphism**. More specifically, we have the following.

Theorem 5.2.5 *Consider the function $\varphi_{\mathbb{Q}} : \mathbb{Z} \to \mathbb{Q}$ defined by*

$$(\forall x)(\varphi_{\mathbb{Q}}(x) = R[(x,1)].$$

This function is a monotone homomorphism w.r.t. the operations $+, \cdot$ and the relation $\leq$:

$$\varphi_{\mathbb{Q}}(x + x') = \varphi_{\mathbb{Q}}(x) + \varphi_{\mathbb{Q}}(x') \qquad \varphi_{\mathbb{Q}}(x \cdot x') = \varphi_{\mathbb{Q}}(x) \cdot \varphi_{\mathbb{Q}}(x')$$
$$x \leq x' \quad \Leftrightarrow \quad \varphi_{\mathbb{Q}}(x) \leq \varphi_{\mathbb{Q}}(x').$$

Also, $\varphi_{\mathbb{Q}}$ is an injection with $Ran(\varphi_{\mathbb{Q}}) = \{R[(x,1)] \,|\, x \in \mathbb{Z}\}$..

Proof. Straightforward and simple. Note that $\varphi_{\mathbb{Q}}(0) = 0_{\mathbb{Q}}$ and $\varphi_{\mathbb{Q}}(1) = 1_{\mathbb{Q}}$. □

Exercise 5.2.7 *Prove the theorem above.*

Remark 5.2.4 Identifying $\mathbb{Z}$ with $Ran(\varphi_{\mathbb{Q}})$ makes the former a **subring** of the field $\mathbb{Q}$. More about these - in the Algebra course. □

Exercise 5.2.8 *Show that for every integers $x \in \mathbb{Z}$, $\varphi_{\mathbb{Q}}(|x|) = |\varphi_{\mathbb{Q}}(x)|$.*

Using $\varphi_{\mathbb{Q}}$ we identify $\mathbb{Z}$ to $\{R[(x,1)] \,|\, x \in \mathbb{Z}\}$, and denote every element of the latter by the name of the element of the former it is identified with: $x := R[(x,1)]$. According to the notations we accepted then $-x := R[(-x,1)]$. On the other hand, every rational number $R[(x,n)]$ is a product of two numbers from $\{R[(x,1)] \,|\, x \in \mathbb{Z}\}$:

$$R[(x,n)] = R[(x,1)] \cdot R[(n,1)]^{-1}.$$

Recalling that

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

we arrive at the realm of the notations of **rational fractions** we have been used to since pre-school:

$$\mathbb{Q} = \{(m) \cdot n^{-1}, (-m) \cdot n^{-1} \,|\, m \in \mathbb{Z}_{\geq 0}, n \in \mathbb{Z}_+\} = \{m/n, (-m)/n \,|\, m \in \mathbb{Z}_{\geq 0}, n \in \mathbb{Z}_+\}.$$

Exercise 5.2.9 (**Archimedes Property of** $\mathbb{Q}$) *Prove that for any $x \in \mathbb{Q}$, there is a $y \in \mathbb{Z}_+$ such that $x < y$.*

[Hint: If $x = m/n$ for $m \in \mathbb{Z}$, let $y = |m| + 1$.]

Note that many rational fractions correspond to a rational number. As remarked in the beginning of this sub-section, every rational number $R[(x,n)]$ has a unique representative: $(x', n') \in R[(x,n)]$ determined by x' and n' not sharing common factors different from ± 1. The rational fraction x'/n' represents that special element, and is called **reduced fraction**. So, every rational number has a unique reduced fraction representing it.
In the new notations,

$$\frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{m_1 n_2 + m_2 n_1}{n_1 n_2} \qquad \frac{m_1}{n_1} \cdot \frac{m_2}{n_2} = \frac{m_1 m_2}{n_1 n_2}.$$

The operations Subtraction and Division in $\mathbb{Q}$

Speaking of pre-school, we have been taught that there is two more operations on $\mathbb{Q}$: subtraction, and division! The definitions of these are as follows

$$- : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \qquad \div : \mathbb{Q} \times \mathbb{Q}^{\times} \to \mathbb{Q}$$
$$(x,y) \mapsto x - y := x + (-y) \qquad (x,y) \mapsto x \div y := x \cdot y^{-1}$$

Here $\mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0_{\mathbb{Q}}\}$ is the set of non-zero rational numbers. Notice that the additional operations are "ugly": they are neither commutative, nor associative!

Similarly to what we had for integers, every rational number can be presented as a quotient of an integer and a natural number: $x = m/n = m \div n$. This presentation is not unique. Looking back in our definition of rational numbers we see that it was modeled on this, post-factum, presentation.

$(\mathbb{Q}, \leq)$ is not Continuous

We end up the subsection on rational numbers proving that we have to work more in order to get a field with continuous order on it.

Example-Proposition 5.2.3 *The relation $\leq$ on $\mathbb{Q}$ is not continuous. More precisely, it doesn't have the least upper bound property.*

Proof It's enough to exhibit a bounded above non-empty subset of $\mathbb{Q}$ which has no l.u.b. To this end, let $X = \{x \in \mathbb{Q} \,|\, 0 < x \wedge x^2 \leq 2\}$. This set is non-empty and is bounded above: $1 \in X$, and $(\forall x)(x \in X \to x < 2)$. We are showing next that X has no l.u.b. in $\mathbb{Q}$.

(1) We claim first that if $y \in \mathbb{Q}$ is an upper bound of X, then $2 < y^2$.
By way of contradiction, assume that $y^2 \leq 2$. Since, as we know, there are no rational numbers z such that $z^2 = 2$ (Euclid's theorem), then $y^2 < 2$. Obviously, we have $y = m/n$ for some positive integers m, n. Also, $0 < 2 - y^2 \in \mathbb{Q}$, so $2 - (m/n)^2 = a/b$ for positive integers a and b.
Observe that, for every positive integer s we have

$$y^2 = \left(\frac{m}{n}\right)^2 < \left(\frac{sm+1}{sn}\right)^2 = \left(\frac{m}{n} + \frac{1}{sn}\right)^2 = \left(\frac{m}{n}\right)^2 + 2\frac{m}{n}\cdot\frac{1}{sn} + \left(\frac{1}{sn}\right)^2$$

$$= \left(2 - \frac{a}{b}\right) + 2\frac{m}{n}\cdot\frac{1}{sn} + \left(\frac{1}{sn}\right)^2$$

the third equality, because $(m/n)^2 = 2 - a/b$. Since $(1/sn)^2 \leq 1/sn$, and that $1/sn \leq 1/s$, we have that the last expression is

$$\leq \left(2 - \frac{a}{b}\right) + 2\frac{m}{n}\cdot\frac{1}{s} + \frac{1}{sn} = 2 + \left(\frac{2m+1}{sn} - \frac{a}{b}\right).$$

When $s = b(2m+1)$, we get that

$$2 + \left(\frac{2m+1}{sn} - \frac{a}{b}\right) = 2 + \left(\frac{1}{bn} - \frac{an}{bn}\right) \leq 2.$$

Combining all inequalities and equalities above, we arrive at (for $s = b(2m+1)$ and $a/b = 2-(m/n)^2$)

$$y^2 = \left(\frac{m}{n}\right)^2 < \left(\frac{sm+1}{sn}\right)^2 \leq 2.$$

This result implies in particular that, for the chosen s, the rational number $z = (sm+1)/(sn)$ belongs to X. It also imlies that $y < z$. This latter is impossible, because y, an upper bound of X, is actually smaller than that rational number - a contradiction! Therefore, every upper bound y of X satisfies $2 < y^2$.

(2) We claim now that there is no upper bound $y \in \mathbb{Q}$ of X which has $2 < y^2$. The argument is similar to the one in (1): for every upper bound $y = m/n$ we will find, for appropriate $s \in \mathbb{N}$, another upper bound in the form $y' = (sm-1)/(sn) \in \mathbb{Q}$ of X. Note that in this case $2 > y^2$, and so $2 - (m/n)^2 = c/d$ is a positive rational number.
We have in these notations

$$\left(\frac{m}{n}\right)^2 > \left(\frac{ms-1}{ns}\right)^2 = \left(\frac{m}{n} - \frac{1}{ns}\right)^2 = \left(\frac{m}{n}\right)^2 - \frac{1}{ns}\left(2\frac{m}{n} - \frac{1}{ns}\right) > \left(\frac{m}{n}\right)^2 - \frac{2m}{n^2 s},$$

and so,

$$\left(\frac{ms-1}{ns}\right)^2 - 2 > \left(\left(\frac{m}{n}\right)^2 - 2\right) - \frac{2m}{n^2 s} = \frac{c}{d} - \frac{2m}{n^2 s}.$$

Choosing $s = 2md$, we get that

$$\frac{c}{d} - \frac{2m}{n^2 s} = \frac{c}{d} - \frac{1}{n^2 d} \geq 0.$$

Therefore, for the chosen s, we have

$$2 < \left(\frac{ms-1}{ns}\right)^2 < y^2$$

as promised. □

Vista: Solving All Algebraic Equations Our motivation for constructing the rational numbers came from the need for being able to solve all linear equations of one unknown with integer coefficients. In our construction, we added all solutions to such equations. The resulting extension naturally turned out to be a field. And indeed, $\mathbb{Q}$ is up to an isomorphism of fields, the smallest field where we can solve all linear equations with integer coefficients. If we want to be methodical in our study of number systems, we have to try to solve quadratic equations, cubic equations, and in general, ant degree equations with integer coefficients as well. This can certainly be done, and the methods for doing that are purely algebraic (more about this in the course of Galois Theory). The resulting extension of the integer numbers, naturally containing $\mathbb{Q}$, is again a field, called the field of **algebraic numbers**, and denoted by **A**. This field is, up to isomorphism, the smallest field containing the solutions to all polynomial equations with integer coefficients ($n \geq 1$)

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \qquad \text{where} \qquad a_n, \ldots, a_0 \in \mathbb{Z}.$$

What is more significant about the field **A** is that it is **algebraically closed**, that is it consists of the solutions to all polynomial equations with coefficients in itself. In other words, there is no need to extend **A** if we want to solve polynomial equations with coefficients in **A**.

5.3 The Real Numbers

In this section we construct the important for Calculus, and for the whole math!, set of real numbers. The construction is based on the notion of **Dedekind cut**. An Alternative definition is presented later on in Chapter 8 as well. The rest of the course will be devoted to studying this set.

5.3.1 Motivations; Definition of the Set of Real Numbers

Before giving a definition of real numbers, we discuss what we want properties this set is desirable to have.

As we know the set of rational numbers $\mathbb{Q}$ is an ordered field containing the integers $\mathbb{Z}$ as an ordered subring. This field $\mathbb{Q}$ is better than the ring $\mathbb{Z}$, because we can solve linear equations in it. For this we didn't need the order on $\mathbb{Q}$, and as we know the order on both $\mathbb{Z}$ and $\mathbb{Q}$ is determined by the fact that they have the natural numbers $\mathbb{N}$ as a subset. The order on $\mathbb{Q}$ unfortunately is not convenient for doing Calculus where limits of sequences are important: the order doesn't have the least upper bound property, and so, although being dense, is not continuous).
The goal in constructing real numbers therefore is to extend the rational numbers in such a way that we keep the properties the latter have (related to addition, multiplication, and the order), but to have the order continuous. So, the real numbers should be an ordered field containing the rationals as an ordered sub-field, and having the order continuous.
We would also like to have, as it was in the case of $\mathbb{Z}$ extending $\mathbb{N}$, and of $\mathbb{Q}$ extending $\mathbb{Z}$, **the real numbers as economically defined as possible**. Recall that in the case of integers we used the addition as a means to define minimality:

$$(\forall m \in \mathbb{Z})(\exists s \in \mathbb{N})(m + s \in \mathbb{N}).$$

In the case of rational numbers, we used the other operation to define the minimality:

$$(\forall x \in \mathbb{Q})(\exists n \in \mathbb{Z})(0 < n \wedge n \cdot x \in \mathbb{Z}).$$

Both these minimality conditions were based on algebra (solving equations). It is natural therefore to define the minimality of the real numbers using the **relation**. The way to assure this minimality here is by demanding to have the rational numbers a **dense** subset of the real numbers.

Our discussion motivates the following definition of what real numbers are.

Definition 5.3.1 *An ordered filed $(K, +, \cdot, \leq)$ with continuous order is called* **a set/field of real numbers** *if there is a monotone homomorphism $\varphi_K : \mathbb{Q} \to K$ such that $Ran(\varphi_K) \subseteq K$ is a dense subset.*

Recall that **monotone homomorphism** means that for every $x, y \in \mathbb{Q}$ we have

$$\varphi_K(x+y) = \varphi_K(x) + \varphi_K(y) \qquad \varphi_K(x \cdot y) = \varphi_K(x) \cdot \varphi_K(y) \qquad \varphi_K(1) = 1_K \quad \text{and}$$

$$x \leq y \quad \Leftrightarrow \quad \varphi_K(x) \leq \varphi_K(y).$$

There is a bit of terminology which makes this definition more structured. Here it is.

Definition 5.3.2 *(1) An ordered field $(K, +, \cdot, \leq)$ with a continuous order $\leq$ is called a* **complete ordered** *field.*
(2) A monotone homomorphism $f : \mathbb{Q} \to K$ where K is a complete ordered field is called an **ordered completion** *of $\mathbb{Q}$ if $Ran(f) \subseteq K$ is a dense subset.*

Therefore **a set of real numbers is any ordered completion of $\mathbb{Q}$.**

Remark 5.3.1 Recall that a field L is ordered if there is a total partial order $\leq$ on it which respects the operations of the field. That is, for every $x, y, z \in L$ we have

$$x \leq y \ \to \ x + z \leq y + z \qquad \text{and} \qquad x \leq y \wedge 0 \leq z \ \to \ x \cdot z \leq y \cdot z.$$

It is not hard to conclude from here that $0 \leq 1$, and therefore that $0 < 1$. With a little bit more work one shows then that there is a unique ring homomorphism $\varphi_L : \mathbb{Q} \to L$, and that in addition this homomorphism is monotone (and so - injective). If furthermore the relation $\leq$ is continuous, then $Ran(\varphi_L)$ is dense in L. So, any complete ordered field contains a unique copy of the rational numbers as a subring. If there is no harm caused, this unique copy is identified with $\mathbb{Q}$. Therefore, **any complete ordered field L which has $\mathbb{Q}$ as a dense subset is a completion of $\mathbb{Q}$.** □

The potential ambiguity caused by the non-uniqueness of the set of real numbers is taken care of by the minimality property of this set: the real numbers are **essentially unique**. Here is the corresponding theorem.

Theorem 5.3.1 *Suppose $\varphi_{K_1} : \mathbb{Q} \to K_1$ and $\varphi_{K_2} : \mathbb{Q} \to K_2$ are two ordered completions of $\mathbb{Q}$. Then there is a unique map $\psi : K_1 \to K_2$ such that $\psi \circ \varphi_{K_1} = \varphi_{K_2}$. Moreover, this map is a bijection, and is a monotone homomorphism (that is, ψ is an* **isomorphism of ordered fields**).

Proof The proof will be given in the end the this section. □

By using this unique map, we an identify the fields K_1 and K_2 not only as sets, but, due to the map being an isomorphism of ordered fields, as ordered fields as well. We will construct in the following section a set of real numbers using Dedekind cuts. Later in the course, we will construct a set of real numbers based on Cauchy sequences of rational numbers. The two sets are, of course, different, but, due to the theorem above, can be **canonically/unambiguously** identified.

Speaking of the **concrete construction** of real numbers, motivations for that come both, from algebra and from geometry. The former is related to formalizing the notion of limits of sequences, and ensure they exist. That can be done purely algebraically, by using a method suggested by Cantor, among other mathematicians of his time, and is based on the algebra of sequences of rational

numbers. We will discuss this method when we introduce rigorously the basics of sequences and their limits. Turning point in this approach is the notion of **Cauchy sequences**: the ones that we want to have limits.
The geometric approach follows the lead of ancient Greek mathematicians in their attempt to ensure non-existence of gaps on the lines in the Euclidean geometry. More about all this can be learned in the course on College Geometry, but in a nutshell it can be described as follows. The Greeks were interested in positive numbers only. The reason for this was purely geometric. Any two points on a given line define a segment. The segment has a length - a positive number. Numbers for Greeks were synonymous with lengths of segments. Having chosen a segment of unit length, the Greeks were able to construct segments of length a (positive) rational number, and these segments corresponded to points on a ray. For some time, the Greeks thought that no more points existed on that ray. Equivalently, they thought that every segment has a length expressible as a rational number. But after proving that $\sqrt{2}$, the length of the diagonal of a square of side lengths 1, was not a rational number, they realized that was not the case...
Our (first) construction of the set of real numbers, based on the theory of **Dedekind cuts**, follows the steps of the great Greek mathematicians: we will define numbers corresponding to every point on that ray.

5.3.2 Construction of a Set of Real Numbers: $\mathbb{R}$

Definition 5.3.3 *A* **Dedekind cut** *is an ordered pair (α, β) of subsets of $\mathbb{Q}$ such that*
(1) $\{\alpha, \beta\}$ is a partition of $\mathbb{Q}$, that is

$$\alpha \cup \beta = \mathbb{Q} \qquad \alpha \neq \emptyset \neq \beta \qquad \alpha \cap \beta = \emptyset;$$

(2) $(\forall a \in \alpha)(\forall b \in \beta)(a < b)$;
(3) α has no maximum element in $\mathbb{Q}$. In other words,

$$\neg((\exists x \in \mathbb{Q})(\alpha = \{y \in \mathbb{Q} \,|\, y \leq x\})).$$

For every Dedekind cut (α, β), the set α is an initial segment in $\mathbb{Q}$, and the set $\beta = \mathbb{Q} \setminus \alpha$ is the relative complement of α. It is straightforward that β is a final cut of $(\mathbb{Q}, \leq)$. Obviously, the Dedekind cut (α, β) is uniquely determined by either α or β. **In what follows, we will identify the cut (α, β) with the initial segment α.** In these terms, **a Dedekind cut is a non-empty initial segment in $\mathbb{Q}$ which is a proper subset of $\mathbb{Q}$**, and has no maximal element.

We define the set that we will prove constitutes a set of real numbers.

Definition 5.3.4 *The set $\mathbb{R}$ of* **real numbers** *is defined by*

$$\mathbb{R} := \{\alpha \,|\, \alpha \quad \textit{is a Dedekind cut}\}.$$

The set β of a pair (α, β) has the property that

$$(\forall x)((x \in \beta) \to (\forall z \in \mathbb{Q})((x \leq z) \to z \in \beta)),$$

and it is natural to call β a **final** segment in $\mathbb{Q}$.

There are Dedekind cuts determined by rational numbers.

Definition 5.3.5 *Let $x \in \mathbb{Q}$. The set $\{z \in \mathbb{Q} \,|\, z < x\}$ is called a* **rational cut**, *and is denoted by x^*.*

Exercise 5.3.1 *(1) Prove that a rational cut is a Dedekind cut.*
(2) Prove that $(\forall x, y \in \mathbb{Q})((x \neq y) \to (x^* \neq y^*))$.
(3) Show that for every $x \in \mathbb{Q}$, the set x^* has a least upper bound (in $\mathbb{Q}$) - the rational number x itself. Moreover, prove that a Dedekind cut α is rational if, and only if, α has a l.u.b. in $\mathbb{Q}$.

The Exercise teaches us that the rational cuts are characterized as those Dedekind cuts who have l.u.b. in $\mathbb{Q}$. A natural question here is: are there non-rational (called **irrational**) cuts? The answer is Yes as the following exercise suggests to prove.

Exercise 5.3.2 *Prove that*

$$\alpha := \{y \in \mathbb{Q} \,|\, (y \leq 0) \vee (y^2 \leq 2)\}$$

is a non-rational Dedekind cut.

5.3.3 The Relation $\leq$ on $\mathbb{R}$

Definition 5.3.6 *Let $\alpha, \beta \in \mathbb{R}$. we say that α* **is less than or equal to** *β, and write $\alpha \leq \beta$, if $\alpha \subseteq \beta$.*

The following theorem says that $(\mathbb{R}, \leq)$ is a **continuous relation**! But before that - some of the properties of families of initial segments in $\mathbb{Q}$ in exercises.

Exercise 5.3.3 *Let $\mathcal{A} := \{\alpha_\lambda \,|\, \lambda \in \Lambda\}$ be a non-empty family of initial segments in $\mathbb{Q}$. Prove that*
(1) If $\cap\mathcal{A} \neq \emptyset$, then $\cap\mathcal{A}$ is an initial segment in $\mathbb{Q}$;
(2) If $\cup\mathcal{A} \neq \mathbb{Q}$, then $\cup\mathcal{A}$ is a bounded above initial segment of $\mathbb{Q}$.

Theorem 5.3.2 *The relation $\leq$ is a total order on $\mathbb{R}$, it is dense, and has the least upper bound property.*

Proof. That the relation $\leq$ is a partial order is immediate (an exercise to do below). We are verifying it's connected: given $\alpha, \beta \in \mathbb{R}$, either $\alpha \leq \beta$ or $\beta \leq \alpha$. To this end, suppose $\neg(\alpha \leq \beta)$. This means that $\alpha \nsubseteq \beta$ which happens only when there is a rational number $x \in \alpha \setminus \beta$. Since β is an initial segment of $\mathbb{Q}$, for every $y \in \beta$ we have $y < x$. For the reason that α is an initial segment in $\mathbb{Q}$ now, all elements $y \in \beta$, being less than $x \in \alpha$, belong to α. Therefore $\beta \subseteq \alpha$, and $\beta \leq \alpha$.
That the relation $\leq$ is dense follows from the fact that **the rational cuts** are dense in $\mathbb{R}$ - an exercise to do below.
We are showing that the relation $\leq$ has the least upper bound property. Let $X \subseteq \mathbb{R}$ be a non-empty bounded above subset. The elements of X are Dedekind cuts, so $X = \{\alpha_x \,|\, x \in X\}$. The set X is bounded above: there is $y \in \mathbb{R}$ such that for every $x \in X$ we have $x \leq y$. And, of course, $y = \alpha_y$ is a Dedekind cut. Consider the set

$$z = \cup X = \cup\{\alpha_x \,|\, x \in X\} \subseteq \mathbb{Q}.$$

Obviously $z \subseteq \alpha_y$, it is an initial segment in $\mathbb{Q}$ as a union of such, and has no maximum element, because the sets α_x don't have maximum elements (fill in the details as an exercise). This means that $z = \beta$ is a Dedekind cut. Since, for every $x \in X$, we have $\alpha_x \subseteq \beta$, the real number z is an upper bound of X. We are showing now that z is the least upper bound of X. Indeed, if that's not the case, there should exist an upper bound $w \in \mathbb{R}$ of X such that $w < z$. But this leads to

$$\cup X \subseteq w \subsetneq z = \cup X$$

which in turn leads to $\cup X \subsetneq \cup X$ - a contradiction. The theorem is proved. □

The following exercise is a prelude to defining the monotone homomorphism $\varphi_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{R}$ needed to show that $\mathbb{R}$ is a set of real numbers.

Exercise 5.3.4 *(1) Prove that $(\mathbb{R}, \leq)$ is a partial order.*
(2) Prove that **the rational cuts are dense in** $\mathbb{R}$ *as well. That is, for every two* **distinct** *real numbers α and β, there is a rational number $x \in \mathbb{Q}$ such that*

$$\alpha < x^* < \beta \qquad \vee \qquad \beta < x^* < \alpha.$$

(3) Prove that the set z in the proof above is a Dedekind cut.
(4) (**Archimedes property for** $\mathbb{R}$) *Prove that for every Dedekind cut α, there is a natural number n such that $\alpha < n^*$.*

Definition 5.3.7 *The* **positive real numbers** *are defined by*

$$\mathbb{R}_+ := \{\alpha \in \mathbb{R} \,|\, 0^* < \alpha\}.$$

The **negative real numbers** *are defined by*

$$\mathbb{R}_- := \{\alpha \,|\, \alpha < 0^*\}.$$

So, we have $\mathbb{R} = \mathbb{R}_- \sqcup \{0^*\} \sqcup \mathbb{R}_+$.

The set $\mathbb{R}$ contains a copy of the rational numbers, and has a continuous relation on it. We have to define next two operations on $\mathbb{R}$, extending the addition and the multiplication on $\mathbb{Q}$, and show that they have properties similar to their counterparts in $\mathbb{Q}$. This is harder than anything we have done in this course so far. We do that in the next subsection.

5.3.4 The Operations Addition and Multiplication in $\mathbb{R}$

Before we introduce the operation addition on $\mathbb{R}$, let's "play" a bit with real numbers.

Exercise-Proposition 5.3.5 *Let α and β be real numbers. Prove that the set*

$$X := \{y \in \mathbb{Q} \,|\, (\exists z \in \alpha)(\exists w \in \beta)(y = z + w)\}$$

is a bounded above initial segment in $\mathbb{Q}$ which has no maximum element. So, $X = \gamma \in \mathbb{R}$.

Exercise-Proposition 5.3.6 *Let α be an initial segment in $\mathbb{Q}$, and let $\overline{\alpha} := \{x \in \mathbb{Q} \,|\, -x \in \alpha\}$. Denote the relative complement of $\overline{\alpha}$ in $\mathbb{Q}$ by $Y := \mathbb{Q} \setminus \overline{\alpha}$. Prove that Y is an initial segment as well. In particular, if Y has no maximum element, then it s a real number.*

Definition 5.3.8 *Let $\alpha \in \mathbb{R}$, and let $Y := \mathbb{Q} \setminus \overline{\alpha}$. Define*

$$-\alpha = \begin{cases} Y & \text{if } Y \text{ has no maximum element} \\ Y \setminus \{m\} & \text{if } m \text{ is the maximum element of } Y \end{cases}$$

Exercise 5.3.5 *(1) Let $\alpha \in \mathbb{R}$, define $Z := \{x \in \mathbb{Q} \,|\, (\exists y \in \alpha)(\exists z \in -\alpha)(x = y + z)\}$. Prove that $Z = 0^*$.*

[Hint: Notice that $z \in a\alpha$ implies that $-z \notin \alpha$, and that therefore it is an upper bound for α. If in addition $y \in \alpha$, we have $y < -z$ which implies $y + z < 0$, and therefore $y + z \in 0^*$. This proves $Z \subseteq 0^*$. Conversely, if $x < 0$, there is a $y \in \alpha$ such that $y + (-x) \notin \alpha$ (here, one may have to use the Archimedes property of $\mathbb{Q}$). Therefore, $-(y + (-x)) \notin \overline{\alpha}$, and so, $z := x - y \in -\alpha$. This shows that $x = y + z$ where $y \in \alpha$ and $z \in -\alpha$. We get that $0^* \subseteq Z$.]
(2) Prove that $-(-\alpha) = \alpha$, and that $\alpha \in \mathbb{R}_+ \Leftrightarrow -\alpha \in \mathbb{R}_-$.

These exercises, and the Propositions above motivate the following definition.

Definition 5.3.9 *The operation* **addition** $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ *is defined by*

$$(\alpha, \beta) \mapsto \alpha + \beta := \{y \in \mathbb{Q} \,|\, (\exists z \in \alpha)(\exists w \in \beta)(y = z + w)\}.$$

And indeed, we have the following theorem.

Theorem 5.3.3 *The operation addition on $\mathbb{R}$ is commutative, associative, with a (unique!) neutral element, $0_{\mathbb{R}} = 0^*$, and with (unique!) opposite elements (the opposite of α is $= -\alpha$.)*

Proof In class and as an exercise. □

Moreover, the interaction of the addition with the relation $\leq$ is also nice.

Theorem 5.3.4 *For every four real numbers α, β, γ, and δ we have*

$$\alpha \leq \beta \quad \Leftrightarrow \quad \alpha + \gamma \leq \beta + \gamma;$$

$$(\alpha \leq \beta) \wedge (\gamma \leq \delta) \rightarrow (\alpha + \gamma \leq \beta + \delta)$$

where if there is a strict inequality anywhere on the LHSs above, then the inequality on the corresponding RHS is strict as well.

Proof. In class and as an exercise. □

We turn now to the definition of **multiplication** on $\mathbb{R}$. As it was in the case of addition, we need to prepare our ground for the corresponding definition.

Exercise-Proposition 5.3.7 *Let $\alpha, \beta \in \mathbb{R}_+$, Consider the sets*

$$X_{(\alpha,\beta)} := \{x \in \mathbb{Q} \,|\, (\exists y \notin \alpha)(\exists z \notin \beta)(x = y \cdot z)\}.$$

and $Y_{(\alpha,\beta)} := \mathbb{Q} \setminus X_{(\alpha,\beta)}$. Then $\emptyset \neq Y_{(\alpha,\beta)} \subset \mathbb{Q}$, and is an initial segment in $\mathbb{Q}$.

Proof. In class and as an exercise. □

Let's define, **for positive real numbers only!**, the following operation

Definition 5.3.10 *Let $\alpha, \beta \in \mathbb{R}_+$. Define, in the notations of the Proposition-Exercise above,*

$$\alpha \odot \beta = \begin{cases} Y_{(\alpha,\beta)} & \text{if} \quad Y_{(\alpha,\beta)} \quad \text{has no maximum element} \\ Y_{(\alpha,\beta)} \setminus \{m\} & \text{if} \quad m \quad \text{is the maximum element of} \quad Y_{(\alpha,\beta)} \end{cases}$$

Again for positive real numbers only we do the following.

Exercise-Proposition 5.3.8 *Let $\alpha \in \mathbb{R}_+$. Consider the family of positive rational cuts*

$$\mathcal{A} := \{x^* \,|\, (x \in \mathbb{Q}) \wedge (0^* < (x^{-1})^* < \alpha)\}.$$

Then $\cap\mathcal{A}$ is a non-empty bounded initial segment in $\mathbb{Q}$ containing a positive rational number.

Proof. In class and as an exercise. □

Definition 5.3.11 *Let $\alpha \in \mathbb{R}_+$. Define, in the notations of the previous Proposition-Exercise,*

$$\tilde{\alpha} = \begin{cases} \cap\mathcal{A} & \text{if} \quad \cap\mathcal{A} \quad \text{has no maximum element} \\ \cap\mathcal{A} \setminus \{m\} & \text{if} \quad m \quad \text{is the maximum element of} \quad \cap\mathcal{A} \end{cases}$$

Note that, for $\alpha \in \mathbb{R}_+$, the $\tilde{\alpha}$ is **a positive real number**.

Exercise 5.3.6 *Prove that $(\forall \alpha \in \mathbb{R}_+)(\alpha \odot \tilde{\alpha} = 1^*)$.*

We have enough reasons now to make the following definition.

Definition 5.3.12 *The* **multiplication** $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ *is defined by*

$$(\alpha, \beta) \mapsto \alpha \cdot \beta = \begin{cases} \alpha \odot \beta & \text{if} \quad \alpha, \beta \in \mathbb{R} \\ -((-\alpha) \odot \beta) & \text{if} \quad \alpha \in \mathbb{R}_-, \beta \in \mathbb{R}_+ \\ (-\alpha) \odot (-\beta) & \text{if} \quad \alpha, \beta \in \mathbb{R}_- \\ 0^* & \text{if} \quad \alpha = 0^* \vee \beta = 0^* \end{cases}$$

The anticipated theorem here is the following one.

Theorem 5.3.5 *The multiplication* $\cdot$ *on* $\mathbb{R}$ *is commutative, associative, has a(unique) neutral element,* $1_{\mathbb{R}} = 1^*$*, distributes over the addition, and every non-zero real number,* α*, has a unique (!) reciprocal,*

$$\alpha^{-1} = \begin{cases} \tilde{\alpha} & \text{if} \quad \alpha \in \mathbb{R}_+ \\ -(\widetilde{-\alpha}) & \text{if} \quad \alpha \in \mathbb{R}_- \end{cases}$$

Proof. In class, and a slightly harder exercise. □

We know now that $\mathbb{R}$ is a field, and that the relation $\leq$ is continuous. To have the picture complete, we need to know the way the multiplication interacts with the relation. We have the following result.

Theorem 5.3.6 *Let* $\alpha, \beta \in \mathbb{R}$*,* $\gamma \in \mathbb{R}_+$*, and* $\delta \in \mathbb{R}_-$*. We have*

$$(\alpha \leq \beta) \quad \to \quad (\alpha \cdot \gamma \leq \beta \cdot \gamma) \quad \wedge \quad (\beta \cdot \delta \leq \alpha \cdot \delta).$$

Proof. In class, and an exercise. □

The Set $\mathbb{Q}$ as a subset of $\mathbb{R}$

As it was with the case of integers and rationals, the set $\mathbb{R}$ has nothing to do with the set $\mathbb{Q}$. But, again as it was before, we can construct a function with domain $\mathbb{Q}$ which locates an "exact" copy of $\mathbb{Q}$ in $\mathbb{R}$. To this end, consider the map

$$\varphi_{\mathbb{R}} : \mathbb{Q} \to \mathbb{R}$$

$$x \in \mathbb{Q} \mapsto \varphi_{\mathbb{R}}(x) := x^*.$$

Theorem 5.3.7 *The map* $\varphi_{\mathbb{R}} : \mathbb{Q} \to \mathbb{R}$ *is a monotone homomorphism of ordered fields. That is*

$$\varphi_{\mathbb{R}}(x + y) = \varphi_{\mathbb{R}}(x) + \varphi_{\mathbb{R}}(y), \qquad \varphi_{\mathbb{R}}(x \cdot y) = \varphi_{\mathbb{R}}(x) \cdot \varphi_{\mathbb{R}}(y)$$

$$\varphi_{\mathbb{R}}(1) = 1_{\mathbb{R}}, \qquad x \leq y \quad \Leftrightarrow \quad \varphi_{\mathbb{R}}(x) \leq \varphi_{\mathbb{R}}(y).$$

Proof. An easy one even for an exercise! □

The needed copy of $\mathbb{Q}$ in $\mathbb{R}$ is the the range $Ran(\varphi_{\mathbb{R}})$, the rational cuts in $\mathbb{R}$. We may, and will, assume from now on that $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Recall that this copy of $\mathbb{Q}$ is **dense in** $\mathbb{R}$.

Exercise 5.3.7 *(1) Define the* **absolute value function** $|\bullet| : \mathbb{R} \to \mathbb{R}$ *the usual way, and prove that, for every* $x \in \mathbb{Q}$*,*

$$|\varphi_{\mathbb{R}}(x)| = \varphi_{\mathbb{R}}(|x|).$$

(2) Prove that $\mathbb{R}$ *has the* **Archimedean property** *that*

$$(\forall x \in \mathbb{R})(\exists n \in \mathbb{N})(x < n).$$

The Operations Subtraction and Division on $\mathbb{R}$

Following the tradition, we end this subsection by mentioning the existence of two more operations on $\mathbb{R}$: subtraction and division. Denoting $\mathbb{R}^\times = \mathbb{R}_- \cup \mathbb{R}_+$, we have

$$- : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \qquad (\alpha, \beta) \mapsto \alpha - \beta := \alpha + (-\beta)$$

and

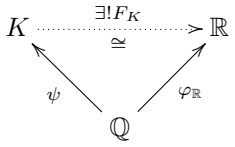
$$\div : \mathbb{R} \times \mathbb{R}^\times \to \mathbb{R} \qquad (\alpha, \beta) \mapsto \alpha \div \beta =: \alpha/\beta := \alpha \cdot \beta^{-1}.$$

Again respecting the tradition we emphasize that these two operations are "ugly": they are neither commutative, nor associative.

Completions of $\mathbb{Q}$, and Uniqueness of the Real Numbers

As it was the case of integers and rationals, the real numbers are **essentially unique**. Here is what that means.

Theorem 5.3.8 *Let K be a field with continuous order $\leq_K$ on it, and such that there is a monotone homomorphism $\psi : \mathbb{Q} \to K$ with $Ran(\psi)$ dense in K. Then, there is a unique monotone map $F_K : K \to \mathbb{R}$ such that $F_K \circ \psi = \varphi_{\mathbb{R}}$.*



The homomorphism F_K is a field homomorphism which is a bijection. This unique monotone map is used to identify K and $\mathbb{R}$ in a unique way. We say in this case that K and $\mathbb{R}$ are **canonically identifiable**. *In this sense is $\mathbb{R}$ essentially unique.*

Before we give a sketch of a proof, recall a useful terminology.

Definition 5.3.13 *The ordered field $(K, +, \cdot \leq)$ is called a* **completion** *of $\mathbb{Q}$, if*
(1) $(K, \leq)$ is a continuous order, and
(2) There is a monotone homomorphism $\psi : \mathbb{Q} \to K$ with $Ran(\psi) \subseteq K$ a $\leq$-dense subset.

The theorem above states that **the completion of $\mathbb{Q}$ is essentially unique**. Later on in the course, we will give a sketch of the construction of a completion $\mathbb{R}_{\mathcal{C}}$ of $\mathbb{Q}$ invented by Cantor (the details occupy Chapter 8 of the complete LN). Due to this theorem, the two completions, $\mathbb{R}$ and $\mathbb{R}_{\mathcal{C}}$, are canonically identifiable.

Proof of Theorem (Sketch) The idea of constructing F_K is simple and natural. First off, observe that the relation $\varphi_{\mathbb{R}} = F_K \circ \psi$ determines uniquely the map F_K on $Ran(\psi) \subseteq K$. On the other hand, the elements of K define Dedekind cuts as follows: for $x \in K$ define

$$D_x = \{y \in \mathbb{Q} \,|\, \psi(y) < x\} \subseteq \mathbb{Q}.$$

But any Dedekind cut IS a real number, so we define $F_K(x) = D_x \in \mathbb{R}$. It is straightforward that if $x = \psi(q) \in Ran(\psi)$, then

$$D_x = D_{\psi(q)} = \varphi_{\mathbb{R}}(q),$$

so that with this definition of F_K we have $\varphi_{\mathbb{R}} = F_K \circ \psi$. A direct check shows that F_K is monotone. This proves the existence of F_K.
The uniqueness of F_K follows from the relation $\varphi_{\mathbb{R}} = F_K \circ \psi$, and the restriction on F_K to be monotone. Indeed, under these conditions, the map F_K should map the subset

$$\tilde{D}_x = Ran(\psi) \cap \{y \in K \,|\, y < x\}$$

bijectively to $\varphi_{\mathbb{R}}(\psi^{-1}(\tilde{D}_x)) = \varphi_{\mathbb{R}}(D_x)$.
The map F_K is one-to-one, because it is monotone. It is onto, because $(K, \leq)$ is continuous: every Dedekind cut of $\mathbb{Q}$ defines, through ψ, a bounded above initial segment of $(Ran(\psi), \leq)$, and therefore, through the least upper bound of this segment, an element $x \in K$ which is mapped by F_K to the real number determined by that Dedekind cut.
Finally, F_K is a homomorphism of fields for the reason that the subsets $\tilde{D}_x \subseteq K$ play the role of Dedekind cuts of $Ran(\psi)$, and that the operations addition and multiplication on K can be identified with the respective operations on Dedekind cuts the same way it was done for $\mathbb{R}$. □

We are ready to prove now the theorem formulated in the beginning of this section.

Theorem 5.3.9 *Suppose $\varphi_{K_1} : \mathbb{Q} \to K_1$ and $\varphi_{K_2} : \mathbb{Q} \to K_2$ are two completions of $\mathbb{Q}$. then there is a unique map $\psi : K_1 \to K_2$ such that $\psi \circ \varphi_{K_1} = \varphi_{K_2}$. Moreover, this map is a bijection, and is a monotone homomorphism (that is, ψ is an* **isomorphism of ordered fields**).

Proof The argument is based on the result from the previous theorem. **Existence of ψ.** By the theorem above, there are unique maps $F_{K_i} : K_i \to \mathbb{R}$ such that $\varphi_{\mathbb{R}} = F_{K_i} \circ \varphi_{K_i}$ for $i = 1, 2$. We know that $F_{K_i}, i = 1, 2$ are monotone isomorphisms as well. Let $\psi = F_{K_2}^{-1} \circ F_{K_1} : K_1 \to K_2$. It is straightforward that ψ is a monotone isomorphism (as a composition of such!). We also have

$$\psi \circ \varphi_{K_1} = (F_{K_2}^{-1} \circ F_{K_1}) \circ \varphi_{K_1} = F_{K_2}^{-1} \circ (F_{K_1} \circ \varphi_{K_1})$$

$$= F_{K_2}^{-1} \circ \varphi_{\mathbb{R}} = F_{K_2}^{-1} \circ (F_{K_2} \circ \varphi_{K_2}) = \varphi_{K_2},$$

so that ψ satisfies the condition from the theorem. **Uniqueness of ψ.** Suppose there is another (set) map $\psi' : K_1 \to K_2$ such that $\psi' \circ \varphi_{K_1} = \varphi_{K_2}$. We have

$$(F_{K_2} \circ \psi') \circ \varphi_{K_1} = F_{K_2} \circ (\psi' \circ \varphi_{K_1}) = F_{K_2} \circ \varphi_{K_2} = \varphi_{\mathbb{R}} = F_{K_1} \circ \varphi_{K_1},$$

and so

$$(F_{K_2} \circ \psi') \circ \varphi_{K_1} = \varphi_{\mathbb{R}} \quad \text{and} \quad F_{K_1} \circ \varphi_{K_1} = \varphi_{\mathbb{R}}.$$

But this means that the maps $F_{K_2} \circ \psi'$ and F_{K_1} have to be the same, and so, $\psi' = F_{K_2}^{-1} \circ F_{K_1} = \psi$. The uniqueness is proved. □

Remark 5.3.2 An ordered field $(L, +, \cdot, \leq)$ contains, as mentioned already, a copy of $(\mathbb{Q}, +, \cdot, \leq)$ in itself. If in addition the copy of $\mathbb{Q}$ is dense in L, and if $\leq$ is continuous, then L is a completion of $\mathbb{Q}$. The theorem above gives than that this L is canonically isomorphic with $\mathbb{R}$. □

Having constructed the real numbers $\mathbb{R}$, we are ready to begin our introduction to Advanced Calculus.

Vista: Other Completions of $\mathbb{Q}$. In this section we constructed the only, up to isomorphism, ordered completion of the field of rational numbers. The starting point was the total order on $\mathbb{Q}$ induced by the order on $\mathbb{N}$. The goal was to find an extension of $\mathbb{Q}$ where "limits of sequences exist". More precisely, as we will see in the next Chapter, we want every **Cauchy** sequence to have a limit. Cauchy sequences are defined using the absolute value function on $\mathbb{Q}$ (extended to $\mathbb{R}$). Turns out, every function on $\mathbb{Q}$ like the absolute value one, determines corresponding Cauchy sequences (of rational numbers). Moreover, a method invented by Cantor produces an extension of $\mathbb{Q}$ in which every Cauchy sequence has a limit (see Chapter 8 of the complete LNs). The amazing fact here is that all absolute value-like functions, with the exception of the one that we used here, have number theoretical nature! The list of such functions contains essentially the absolute value defined in this Chapter, and the **p-adic** absolute values for p a prime number (a Theorem by Alexander Ostrowski). Those completions are denoted by $\mathbb{Q}_p$, and are called **p-adic numbers**. They are not ordered, of course! The set $\mathbb{R}$ is one of denumerably many completions of $\mathbb{Q}$, and it is the only **transcendental**, that is, non-algebraic, one. Essentially, all methods developed to study $\mathbb{R}$ and the functions on it have been extended to study $\mathbb{Q}_p$. A bit more about all this can be learned in the course MAS 4203 Number Theory.

Chapter 6

Topology on the Real Line

We are discussing in this chapter some basic and important concepts from Topology which are traditionally included in the courses of Advanced Calculus. These include topological and metric spaces in general, and topologies on $\mathbb{R}$ in particular, sequences in $\mathbb{R}$, convergent sequences in $\mathbb{R}$, and Cauchy sequences in $\mathbb{R}$. Our discussions are rigorous, but quite introductory to this circle of concepts and ideas. We will give several examples of topological spaces, but our emphasis will be on studying the **classical topology** on the set of real numbers. Our main tool in doing so will be sequences of real numbers, but whenever possible, and pedagogically feasible, we will use methods applicable in greater generality as well. These latter will give the idea of how the facts and concepts related to the topology of the real numbers can be generalized to other topological spaces.
There are two important results in this chapter: Bolzano-Weierstrass' theorem, that every bounded indexed family of real numbers has an accumulation point, and the theorem characterizing the convergent sequences of real numbers as Cauchy sequences. The former theorem will be used in next chapter when we study limits and continuity of functions. The latter theorem will be used as a motivation to give, in the concluding these Lecture Notes chapter, the construction of the real numbers by using Cauchy sequences of rational numbers which is due to Georg Cantor.

6.1 The Classical Topology on $\mathbb{R}$

Speaking of **topologies** on a set, there are many such that can be defined on $\mathbb{R}$. One of them, the so called **classical topology**, is an object of considerations in Advanced Calculus.
The **classical topology** on $\mathbb{R}$ is defined by using the total order on $\mathbb{R}$, and the function **absolute value** on $\mathbb{R}$. The most useful properties of this function are collected in the following proposition.

Proposition 6.1.1 *The function $|\bullet| : \mathbb{R} \to \mathbb{R}$ has the following properties.*
(i) Range$(|\bullet|) = \mathbb{R}_+ \cup \{0\}$, and only $0 \in \mathbb{R}$ is mapped to 0;
(ii) The function is **multiplicative***: $|x \cdot y| = |x| \cdot |y|$;*
(iii) The function satisfies the **triangle inequality***: $|x + y| \leq |x| + |y|$;*
(iv) The function satisfies also the inequality: $||x| - |y|| \leq |x - y|$.

Proof. Items (i) and (ii) are straightforward from the definition of $|\bullet|$ in the previous chapter. For item (iii), notice that if x and y have the same sign, that is, they are both non-negative, or both negative, then $|x + y| = |x| + |y|$. Finally, if x and y have opposite signs, and say $|x| \leq |y|$, then $|x + y| = |y| - |x| < |y| + |x|$ (why?) which completes the proof of (iii). The proof of (iv) follows from (iii). Indeed, we have by (iii) that

$$|y| = |x + (y - x)| \leq |x| + |y - x| \quad \text{and} \quad |x| = |y + (x - y)| \leq |y| + |x - y|$$

which give us that

$$-(|x| - |y|) \leq |y - x| \quad \text{and} \quad |x| - |y| \leq |x - y|.$$

The last two inequalities are equivalent to $||x| - |y|| \leq |x - y|$. $\square$

Exercise 6.1.1 *Give all details in the proof of item (iii) above.*

Note that the items (i) and (iv) can be used to prove the following.

Proposition 6.1.2 *The function $d : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined by $d(x, y) = |x - y|$ has the properties.*
(d1) $(\forall x, y \in \mathbb{R})(d(x, y) \geq 0 \quad \wedge \quad (d(x, y) = 0 \Leftrightarrow x = y))$. *That is, d is* **positive**;
(d2) $(\forall x, y \in \mathbb{R})(d(x, y) = d(y, x))$. *That is d is* **symmetric**;
(d3) $(\forall x, y, z \in \mathbb{R})(d(x, y) + d(y, z) \geq d(x, z))$. *That is d satisfies the* **triangle inequality**.

Exercise 6.1.2 *Prove the preceding proposition.*

The function d makes out of $\mathbb{R}$ a very special set - **a metric space**.

Definition 6.1.1 *A pair (X, d) where X is a set and $d : X \times X \to \mathbb{R}$ is called a* **metric space, with a metric** *d if the function d has the properties (d1), (d2), and (d3), that is, if it is* **positive**, **symmetric**, *and satisfies the* **triangle inequality**.

It is this metric on $\mathbb{R}$ which defines the classical topology on it. The following definition introduces concepts needed to define thisl topology.

Definition 6.1.2 *(1) For $a, b \in \mathbb{R}, a < b$, define the open intervals in $\mathbb{R}$ by*

$$(a, b) = \{x \in \mathbb{R} \,|\, a < x < b\},$$

$$(a, \infty) = \{x \in \mathbb{R} \,|\, a < x\}, \quad (-\infty, b) = \{x \in \mathbb{R} \,|\, x < b\};$$

(2) Let $\epsilon > 0$ be a real number, and $a \in \mathbb{R}$. Call $(a - \epsilon, a + \epsilon)$ the **epsilon nbhd of** *a;*
(3) Let $U \subseteq \mathbb{R}$. Call U **a nbhd of** *$a \in \mathbb{R}$ if $(a - \epsilon, a + \epsilon) \subseteq U$ for some positive ϵ;*
(4) The subset $U \subseteq \mathbb{R}$ is called **an open subset of** $\mathbb{R}$ *if it is a nbhd of each one of its points.*

Example 6.1.1 Every epsilon nbhd is an open subset of $\mathbb{R}$. Indeed, let $b \in (a - \epsilon, a + \epsilon)$. We have that $a - \epsilon < b < a + \epsilon$. Let $\epsilon_1 = min\{b - (a - \epsilon), (a + \epsilon) - b\}$. Obviously, $0 < \epsilon_1 \leq \epsilon$. We claim that

$$(b - \epsilon_1, b + \epsilon_1) \subseteq (a - \epsilon, a + \epsilon).$$

To this end, let $x \in (b - \epsilon_1, b + \epsilon_1)$. This means that $b - \epsilon_1 < x < b + \epsilon_1$ or, equivalently that $|x - b| < \epsilon_1$. We have now

$$|x - a| = |(x - b) + (b - a)| \leq |x - b| + |b - a| < \epsilon_1 + |b - a|.$$

By the definition of ϵ_1 we have that

$$\epsilon_1 \leq b - a + \epsilon \quad \text{and} \quad \epsilon_1 \leq a + \epsilon - b$$

which amounts to $a - b \leq \epsilon - \epsilon_1$ and $-(a - b) \leq \epsilon - \epsilon_1$, and ultimately to $|a - b| \leq \epsilon - \epsilon_1$. To compete our argument, observe that $|x - a| < \epsilon_1 + |b - a| \leq \epsilon_1 + (\epsilon - \epsilon_1) = \epsilon$, and so $x \in (a - \epsilon, a + \epsilon)$. $\square$

Exercise 6.1.3 *(1) Verify that ϵ- neighbourhoods can be defined in terms of the metric d on $\mathbb{R}$:*

$$(a - \epsilon, a + \epsilon) = \{x \in \mathbb{R} \,|\, d(x, a) < \epsilon\}.$$

(2) Prove that
(i) The empty subset of $\mathbb{R}$, and $\mathbb{R}$ itself are open subsets of $\mathbb{R}$;
(ii) The union of **any** *family of open subsets of $\mathbb{R}$ is an open subset of $\mathbb{R}$;*
[Let $\mathcal{A} = \{U_\lambda \,|\, \lambda \in \Lambda\}$ be a family of open subsets of $\mathbb{R}$, and let $x \in \cup\mathcal{A} = \cup_{\lambda \in \Lambda} U_\lambda$. We want to show that, for some $\epsilon > 0$, we have $(x - \epsilon, x + \epsilon) \subseteq \cup\mathcal{A}$. But this is obviously the case, because there is a λ_0 such that $x \in U_{\lambda_0}$, and since U_{λ_0} is an open subset of $\mathbb{R}$, there is an $\epsilon > 0$ such that $(x - \epsilon, x + \epsilon) \subseteq U_{\lambda_0} \subseteq \cup\mathcal{A}$.]
(iii) The intersection of any **finite** *family of open subsets of $\mathbb{R}$ is an open subset of $\mathbb{R}$.*
[Let $U_1, \ldots, U_n$ be open subsets of $\mathbb{R}$, and let $x \in U_1 \cap \cdots \cap U_n$. Since, for every $i = 1, \ldots, n$, the set U_i is open, there is an $\epsilon_i > 0$ such that $(x - \epsilon_i, x + \epsilon_i) \subseteq U_i$. Therefore, $\cap_{i=1}^n (x - \epsilon_i, x + \epsilon_i) \subseteq \cap_{i=1}^n U_i$. we complete the argument noticing that, for $\epsilon = min\{\epsilon_1, \ldots, \epsilon_n\}$, we have $(x - \epsilon, x + \epsilon) \subseteq \cap_{i=1}^n U_i$.]

We define next the concept of a topological space. The previous exercise will assure then that the open subsets of $\mathbb{R}$ defined above constitute a topology on $\mathbb{R}$.

Definition 6.1.3 *Let X be a set, and let $\mathcal{T}_X = \{U_\lambda \,|\, \lambda \in \Lambda\} \subseteq \mathcal{P}(X)$. We say that $\mathcal{T}_X$ is* **a topology on** *X, and that* **the elements of** *$\mathcal{T}_X$ are* **the open subsets of** *X if*
(i) $\emptyset, X \in \mathcal{T}_X$;
(ii) If $U_1, \ldots, U_k \in \mathcal{T}_X$, then $U_1 \cap \cdots \cap U_k \in \mathcal{T}_X$;
(iii) If $\mathcal{A} \subseteq \mathcal{T}_X$, then $\cup\mathcal{A} \in \mathcal{T}_X$.
The pair $(X, \mathcal{T}_X)$ is called then a **topological space**.

When there is no risk of confusion about who the family $\mathcal{T}_X$ is we abbreviate $(X, \mathcal{T}_X)$ to X.

Example 6.1.2 (1) By the definition of topology on X, the sets $\emptyset$ and X are open. In fact, the collection $\mathcal{T}_X = \{\emptyset, X\}$ trivially satisfies (i), (ii), and (iii) from the Definition above, and **is**, therefore, a topology on X. Having the minimum possible open sets, this topology is not interesting for applications, and is rightfully called the **trivial topology** on X .
(2) On the other extreme, the collection $\mathcal{T}_X = \mathcal{P}(X)$ also satisfies the conditions (i), (ii), and (iii) from the Definition of topology on X. If the trivial topology is the "smallest" topology on X, the topology $\mathcal{T}_X = \mathcal{P}(X)$ is the "largest' possible one in which **every subset of** X is open. It is straightforward that this topology is characterized by having every singleton subset $\{x\} \subseteq X$, where $x \in X$, is an open subset of X. For this reason, this topology is called the **discrete topology on** X.

Now we are formally introducing the classical topology on $\mathbb{R}$.

Definition 6.1.4 *The* **classical topology on** $\mathbb{R}$ *is defined by*

$$\mathcal{T}_{\mathbb{R}} :=: \mathcal{C} := \{U \subseteq \mathbb{R} \,|\, (\forall x \in U)(U \text{ is a nbhd of } x)\} \subseteq \mathcal{P}(\mathbb{R}).$$

Vista: As we have seen already, the classical topology on $\mathbb{R}$ is determined by the metric on $\mathbb{R}$. Indeed, recall that a set is open in that topology, if every point of that set has an ϵ-nbhd contained in the set, and that the ϵ-nbhds are of the form $U = \{x \,|\, x \in \mathbb{R} \wedge d(x_0, x) < \epsilon\}$. Because of this last description, the classical topology on $\mathbb{R}$ is called **metric** topology. Moreover, it is true that **every metric space** determines its **metric** topology, and a topological space $(X, \mathcal{T}_X)$ whose topology is determined by a metric d on it is called **metrizable**. Metrizable topological spaces enjoy very nice properties, and were considered as a (dream-) model of what nice and useful topological space should look like. Some of the properties of the metrizable classical topology of $\mathbb{R}$ are studied below. □

Exercise 6.1.4 *Prove that if $a \neq b$ are two real numbers, then there are open subset $a \in U_a$ and $b \in U_b$ of $\mathbb{R}$, such that $U_a \cap U_b = \emptyset$.*

Definition 6.1.5 *A topological space $(X, \mathcal{T}_X)$ is called* **Hausdorff**, *or* **separated**, *(or a T_2-space) if for every $x_1 \neq x_2 \in X$ there are open subsets $x_1 \in U'$ and $x_2 \in U''$ such that $U' \cap U'' = \emptyset$.*

Example 6.1.3 The set of real numbers with the classical topology, $(\mathbb{R}, \mathcal{C})$, is a separated topological space. □

Not every topological space is Hausdorff. Moreover, some of very useful and "natural" topological spaces are not separated. The example below explains a topology on $\mathbb{R}$ which is important for such areas of math as Algebraic Geometry, and which is not Hausdorff.

Example 6.1.4 (**Zariski topology** on $\mathbb{R}$). By definition, the open sets in this topology are all subsets $U \subseteq \mathbb{R}$ such that $\mathbb{R} \setminus U$ is either finite, or the whole $\mathbb{R}$. The open sets of this topology are called **Zariski open** subsets. Let's verify that this is a topology on $\mathbb{R}$. It is immediate that $\emptyset$ and $\mathbb{R}$ are open in this topology. Suppose U, V are Zariski open subsets of $\mathbb{R}$. Since

$$\mathbb{R} \setminus U \cap V = \mathbb{R} \setminus U \cup \mathbb{R} \setminus V$$

is either finite or the whole $\mathbb{R}$ (why?), then, by an easy induction, the intersection of any finite family of Zariski open subsets of $\mathbb{R}$ is Zariski open. Finally, for any family $\mathcal{U} = \{U_\lambda \,|\, \lambda \in \Lambda\}$ of Zariski open subsets of $\mathbb{R}$, we have

$$\mathbb{R} \setminus \cup\mathcal{U} = \cap\{\mathbb{R} \setminus U_\lambda \,|\, \lambda \in \Lambda\}$$

which is an intersection of sets such that either all they are equal to $\mathbb{R}$ or at least one of them is finite. Therefore, the complement of $\cup\mathcal{U}$ is either $\mathbb{R}$ or a finite set, and so, $\cup\mathcal{U}$ is Zariski open. A very important feature of the Zariski topology on $\mathbb{R}$ is that **every two non-empty Zariski open subsets intersect non-trivially**

$$U \neq \emptyset, \quad V \neq \emptyset \quad \text{(Zariski open)} \quad \Rightarrow \quad U \cap V \neq \emptyset.$$

(Indeed, $\mathbb{R} \setminus U \cap V = \mathbb{R} \setminus U \cup \mathbb{R} \setminus V \neq \mathbb{R}$, because it is a finite set(why?).) Therefore, the Zariski topology is **not** separated. Or, in other words, "Zariski is not Hausdorff". □

A very important, and closely related to the topology of a topological space, are the closed subspaces.

Definition 6.1.6 *Let $(X, \mathcal{T}_X)$ be a topological space. The subset $V \subseteq X$ is called a* **closed subset** *of X if $X \setminus V \in \mathcal{T}_X$.*

Remark 6.1.1 The notion of closed set is **not** the negation of the concept of open set. So, in general a subset of a topological space can neither be open, nor closed! Moreover, usually most of the subsets are neither open nor closed! For instance the subset $(a, b] = \{\, x \in \mathbb{R} \,|\, a < x \leq b \,\}$ is neither closed nor open in $\mathbb{R}$ (prove that!). □

It is obvious that knowing the open subset of a topological space X is equivalent to knowing the closed subsets. Therefore the topology of X should be describable in terms of closed subsets only. The corresponding description is given in item (iv) of the exercise below.

Exercise 6.1.5 *1) Show that every one-point subset of the $\mathbb{R}$ is closed in the classical topology. Conclude that every finite subset of $\mathbb{R}$ is a closed subset in the classical topology.*
2) A topological space $(X, \mathcal{T}_X)$ the one-point subsets of which are closed is called **Fréchet** *(or a T_1-) topological space. Prove that every Hausdorff space is a Fréchet space. Conclude by 1) then that $(\mathbb{R}, \mathcal{C})$ is a Fréchet space.*
2') Prove that the Zariski topology on $\mathbb{R}$ is Fréchet. Conclude that there are Fréchet topological spaces which are not Hausdorff. "Fréchet is not Hausdorff" either.
3)Prove that $(X, \mathcal{T}_X)$ is a Fréchet topological space if, and only if,

$$(\forall x, y \in X)((x \neq y) \rightarrow (\exists U, V \in \mathcal{T}_X)((x \in U \wedge y \notin U) \wedge (x \notin V \wedge y \in V))$$

4) Prove, for a topological space $(X, \mathcal{T}_X)$, that
(i) The empty set, $\emptyset$, and X are closed in X;
(ii) If $\mathcal{D}$ is a **finite** *family of closed subsets of X, then $\cup\mathcal{D}$ is a closed subset of X;*
(iii) If $\mathcal{B}$ is a **non-empty** *family of closed subsets of X, then $\cap\mathcal{B}$ is a closed subset of X.*
5) Let X be a set, and let $\mathcal{F} \subseteq \mathcal{P}(X)$ have the properties (1), (ii), and (iii) from item 4) of this exercise. Prove that the family $\mathcal{A} = \{X \setminus V \,|\, V \in \mathcal{F}\}$ defines a topology $\mathcal{T}_X$ on X such that $\mathcal{F}$ consists of the closed subsets of X. Conclude that a topology of a set X can be defined by exhibiting a family of subsets of X satisfying (i), (ii), and (iii) from 4) above.
6) Let X be a set, and let $\mathcal{F} \subseteq \mathcal{P}(X)$ be defined as follows

$$\mathcal{F} = \{Y \subseteq X \,|\, Y = X \ \vee \ Y \, is \, finite \,\}.$$

Prove that X has a topology whose closed subsets constitute $\mathcal{F}$. This topology is known as the **finite complement topology** *on X . (Note that the Zariski topology on $\mathbb{R}$ is the finite complement topology on $\mathbb{R}$.)*

6.2 Sequences of Real Numbers

This subsection treats rigorously concepts that are, presumably, known to the students from the courses of Calculus... All these concepts are important, because they offer an useful way to describe the classical topology on $\mathbb{R}$. Most of the definitions we give and the propositions we prove can be generalized, word for word, to any metric space.

6.2.1 Convergent Versus Cauchy Sequences I

We begin with a general definition.

Definition 6.2.1 *A* **sequence of elements of a set** X*, or just* **a sequence in** X*, is called any function* $f : \mathbb{N} \to X$*. A sequence in* X *is called* **stationary** *or* **constant** *if the function* f *is a constant function*

We abbreviate the notation of a sequence: instead of $f : \mathbb{N} \to X$, we write $< x_n >$ where $x_n = f(n)$. Sequences can be considered in an equivalent way as **indexed families** with indexing set $\mathbb{N}$:

$$< x_n >= \{x_n \,|\, n \in \mathbb{N}\}.$$

So, two **members of the sequence** $< x_n >$ are distinct if their indices are distinct.
In this course, we will be interested in sequences in $\mathbb{R}$.

The most important sequences for us will be the **convergent** to real numbers ones.

Definition 6.2.2 *Let* L *be a real number, and* $< x_n >$ *be a sequence of real numbers. We say that* $< x_n >$ **converges to** L*, and that* L *is* **a limit of** $< x_n >$*, if*

$$(\forall \epsilon > 0)(\exists n_0 \in \mathbb{N})(\forall n \in \mathbb{N})(n_0 \leq n \to |x_n - L| < \epsilon).$$

We write in such a case: $< x_n > \to_n L$.

Exercise 6.2.1 *1) Prove that every stationary sequence in* $\mathbb{R}$ *is convergent.*
2) Prove that the sequence $f : \mathbb{N} \to \mathbb{R}$ *defined by* $f(n) = 1/2^n$ *converges to* 0.

Exercise 6.2.2 *Prove that, in the definition of convergent sequence, the* ϵ*-nbhd of* L *can be replaced by* **any** *nbhd of* L*. More precisely, prove that the sequence* $< x_n >$ *is convergent if, and only if, there is a real number* L *with the following property: for every nbhd* U *of* L*, there exists an* $n_0 \in \mathbb{N}$ *such that* $x_n \in U$ *for all* $n \geq n_0$.

The last exercise shows how the concept of convergent sequence of real numbers can be generalized to any topological space: **the element** $y \in X$ **is a limit of the sequence** $< x_n >$**, with** $x \in X$ **for all** $n \in \mathbb{N}$**, if every nbhd** U **of** y **contains all but finitely many members of the sequence.**

It is very important that $\mathbb{R}$ is a separated topological space. Because of this, a convergent sequence has a unique limit.

Proposition 6.2.1 *Suppose* $< x_n >$ *is a sequence in* $\mathbb{R}$*. If* $< x_n > \to_n L_1$*, and* $< x_n > \to_n L_2$*, then* $L_1 = L_2$.

Proof. Assume, by RAA, that $L_1 \neq L_2$, denote by $\epsilon = |L_1 - L_2|/2$. By the definition of limit, applied to L_1 and L_2, for this ϵ there are natural numbers $n_1, n_2 \in \mathbb{N}$ such that

$$(\forall n \in \mathbb{N})(n \geq n_1 \to |x_n - L_1| < \epsilon) \quad \text{and} \quad (\forall n \in \mathbb{N})(n \geq n_2 \to |x_n - L_2| < \epsilon).$$

Choose any natural number $n > max\{n_1, n_2\}$. We have

$$2\epsilon = |L_1 - L_2| = |L_1 - x_n + x_n - L_2| \leq |L_1 - x_n| + |x_n - L_2| < \epsilon + \epsilon = 2\epsilon,$$

and therefore: $2\epsilon < 2\epsilon$ - a contradiction. $\square$

Example 6.2.1 To see how important the Hausdorff condition for the concept of limits of sequences is, consider the following "pathological" example. Suppose $< x_n >$ is a sequence in $\mathbb{R}$ consisting of **pairwise distinct** elements: $x_n \neq x_m$ for every $m \neq n$. Then, **every real number is a limit of this sequence in the Zariski topology on** $\mathbb{R}$! In other words, in the Zariski topology,

$$\forall L \in \mathbb{R}\,(< x_n > \to_n L).$$

Indeed, every open nbhd U of L is non-empty (for $L \in U$), and hence $\mathbb{R} \setminus U = \{r_1, \ldots, r_k\}$ is a finite set. This means that $\{x_n \,|\, n \in \mathbb{N}\} \cap \mathbb{R} \setminus U$ is finite, and, therefore, U does not contain no more than finitely many members of $< x_n >$. This means that there is a natural number N such that for all $n \geq N$ we have $x_n \in U$.
We know that the Zariski topology on $\mathbb{R}$ is not Hausdorff, but is Fréchet. This example shows therefore that the concept of **convergent** sequences in Fréchet topological spaces is not an interesting concept: it may have examples of "pathologically looking" sequences. □

We worked a lot to construct the real numbers as a number system with continuous relation on it. Here is the first benefit we can get from that: a **sufficient condition for a sequence to have a limit**.

Definition 6.2.3 *(1) The sequence $< x_n >$ is called* **increasing**, *respectively* **decreasing**, *if for every $n < m \in \mathbb{N}$ we have $x_n \leq x_m$, respectively $x_m \leq x_n$.*
(2) The sequence $< x_n >$ is called **monotone** *if it is either an increasing or a decreasing sequence. A sequence is called* **strictly** *increasing/decreasing/monotone, if the inequalities in (1) and (2) are all strict.*

Here is the important result.

Theorem 6.2.2 *If the sequence $< x_n >$ is monotone and bounded, then it is convergent, that is, there is a real number L such that $< x_n > \to_n L$.*

Proof. If the sequence is, say, increasing, then it is bounded above (because the sequence is bounded), and therefore has a l.u.b. L in $\mathbb{R}$. We are showing next that $< x_n > \to_n L$. To this end, let $\epsilon > 0$. The number $L - \epsilon$, being smaller than the least upper bound of the sequence, is **not** an upper bound of that sequence. This means that there is a natural number n_0 such that $L - \epsilon < x_{n_0} <\leq L$. Since the sequence is increasing, for all $n_0 \leq n \in \mathbb{N}$ we have $x_{n_0} \leq x_n$ and therefore

$$L - \epsilon < x_{n_0} \leq x_n \leq L < L + \epsilon.$$

These inequalities for x_n can be rewritten as $|x_n - L| < \epsilon$. The proof is completed. □

Convergent sequences (of real numbers, in the classical topology) are really special. They have the following feature.

Proposition 6.2.3 *If $< x_n >$ is convergent (with limit L), then*

$$(\forall \epsilon > 0)(\exists n_0 \in \mathbb{N})(\forall m, n \in \mathbb{N})(m, n \geq n_0 \to |x_n - x_m| < \epsilon).$$

Notice the important fact that L does not take part in the feature of $< x_n >$!

Proof. The results is based on the triangle inequality: for every $n, m \in \mathbb{N}$

$$|x_n - x_m| = |(x_n - L) + (L - x_m)| \leq |x_n - L| + |x_m - L|.$$

If we can make the summands on the RHS be less than $\epsilon/2$, we will be done. But arranging the latter is not a problem, since $< x_n > \to_n L$. □

It turns out, sequences with the feature just described are the most important ones in Calculus! They bare the name of the guy who introduced them... long ago.

Definition 6.2.4 *The sequence of real numbers $< x_n >$ is called* **a Cauchy sequence** *if*

$$(\forall \epsilon > 0)(\exists n_0 \in \mathbb{N})(\forall m, n \in \mathbb{N})(m, n \geq n_0 \rightarrow |x_n - x_m| < \epsilon).$$

So, by the proposition above, every convergent sequence or real numbers is Cauchy! The truth of the matter is that, conversely: **Every Cauchy sequence of real numbers has a limit in** $\mathbb{R}$. This fact is based on an important property of the classical topology of $\mathbb{R}$, called **Bolzano-Weierstrass' theorem**. To formulate this theorem, we need a concept which makes many of the arguments used more transparent: accumulation points.

6.2.2 Accumulation Points of Sets

Definition 6.2.5 *Let $A \subseteq X$ where $(X, \mathcal{T}_X)$ is a topological space. The point $x \in X$ is* **an accumulation point of** *A if every open subset $U \subseteq X$ with $x \in U$ has infinitely many elements of A, that is the set $U \cap A$ has infinitely many elements.*

Obviously, x is an accumulation point of A if and only if every **nbhd** of x contains infinitely many elements from A. It is equally obvious that if x is an accumulation point of a subset of A, then it is an accumulation point of A itself. One more thing, which is also obvious, is that finite sets have no accumulation points!

Example 6.2.2 The two extreme topologies on a set X, namely, the trivial topology and the discrete topology provide examples where the concept of accumulation point is not "interesting". What this means is that this concept doesn't distinguish points in relation with an infinite subset $A \subseteq X$ as in accumulation points of A. And indeed, **in the trivial topology, every element of X is an accumulation point**, while **in the discrete topology no element of X is an accumulation point of A.** □

Example 6.2.3 Our running example of $\mathbb{R}$ with the Zariski topology shows that the notion of accumulation points is not interesting even for some (non-trivial) topologies. Indeed, if $A \subseteq \mathbb{R}$ is an infinite subset, then **every real number** L is an accumulation point of A. This is, because every non-empty Zariski open subset of $\mathbb{R}$, in particular, every Zariski open nghd of L, intersects A in infinitely many points! We will show below that, on the contrary, the accumulation points are a fine and useful concept for the classical topology of $\mathbb{R}$. □

Nevertheless, as we will see shortly, the concept of accumulation point of a set will be very useful in our study of the classical topology on $\mathbb{R}$.

For those who are are uncomfortable with thinking of sets with infinitely many elements, here is a characterization of the accumulation points not appealing to infinite sets. Of course, we have to put a (mild) restricction on the topological space for that.

Exercise-Proposition 6.2.3 *Let $(X, \mathcal{T}_X)$ be a Fréchet space, and let $x \in X$. Then x is an accumulation point of $A \subseteq X$ if, and only if, for every open subset $U \subseteq X$ such that $x \in U$, the intersection $U \cap A$ has at least two elements. In the case of $(\mathbb{R}, \mathcal{C})$, this is also equivalent to "every ϵ-nbhd of x contains at least two elements of A".*

Proof One of the directions of the first statement is obvious. The other follows by induction, and is based on the fact that, In a Fréchet space, if $U \subseteq X$ is open, and $y \in U$, then $U \setminus \{y\}$ is open as well. The second statement, about the space $(\mathbb{R}, \mathcal{C})$, is straightforward. □

The accumulation points of **subsets of** $\mathbb{R}$ have the following characterization in terms of sequences. Sometimes this description helps to prove theorems related to accumulation points in a faster and easier fashion.

Theorem 6.2.4 *Suppose $\emptyset \neq X \subseteq \mathbb{R}$, and $r \in \mathbb{R}$. Then, r is an accumulation point of X if, and only if, there is a sequence $< x_n > \subseteq X \setminus \{r\}$ such that $< x_n > \to_n r$.*

Proof. ($\Leftarrow$) Assuming a sequence of elements of X, every member of which is distinct from r, has a limit r, we have to show that every nbhd of r has at least two elements of X. As usual, it is enough to prove that for nbhds of the type $(r-\epsilon, r+\epsilon)$. To this end, let $\epsilon > 0$ be fixed. By the definition of limit, there is a natural number n_0 such that for every natural number $n \geq n_0$ we have $x_n \in (r-\epsilon, r+\epsilon)$, or equivalently $|r - x_n| < \epsilon$. In particular $x_{n_0} \in (r-\epsilon, r+\epsilon)$. Denote by $\epsilon_1 = |r - x_{n_0}|$. This number is strictly positive, because all members of the sequence are distinct from r. We have also that $\epsilon_1 < \epsilon$. Now, there is a natural number n_1 such that for every natural $n \geq n_1$ we have $x_n \in (r-\epsilon_1, r+\epsilon_1)$. In particular $x_{n_1} \in (r-\epsilon_1, r+\epsilon_1)$. From this it follows that $x_{n_0} \neq x_{n_1}$ and that $x_{n_0}, x_{n_1} \in (r-\epsilon, r+\epsilon)$.
($\Rightarrow$) Knowing that r is an accumulation point of X, we want to construct a sequence $\{x_n \,|\, n \in \mathbb{N}\} \subseteq X \setminus \{r\}$ such that $< x_n > \to_n r$. We prove here a bit more: the members of the sequence are pairwise distinct real numbers. Consider, for every $n \in \mathbb{Z}_+$, the nbhds $U_n = (r - 1/n, r + 1/n)$ of r. For every n, $U_n \cap X$ has infinitely many elements. Recursively, having chosen $x_{k-1} \in U_k \cap (X \setminus \{r\})$ for $k = 0, 1, \ldots, n$, we choose $x_n \in U_{n+1} \cap (X \setminus \{r, x_0, \ldots, x_{n-1}\}$. By construction, the sequence $\{x_n \,|\, n \in \mathbb{N}\}$ consists of pairwise disjoint elements. Proving that $< x_n > \to_n r$ is left as an exercise. □

Exercise 6.2.3 *Prove that the sequence constructed in part ($\Rightarrow$) of the proof above is convergent with a limit r.*

As a first application of the previous theorem, we are giving a description of the closed subsets of $\mathbb{R}$.

Theorem 6.2.5 *The subset $V \subseteq \mathbb{R}$ is closed if, and only if, V contains all its accumulation points*

$$(\forall x)((x - \text{ accumulation point of } V) \to (x \in V)).$$

Proof. We have to prove two things:
(1) If V is closed, then it contains all its accumulation points, and
(2) If V contains all its accumulation points, then V is closed in $\mathbb{R}$.
To prove (1), and arguing by contradiction, assume $r \notin V$ is an accumulation point of V. Since V is closed in $\mathbb{R}$, its complement $\mathbb{R} \setminus V$ is open, and is a nbhd of r. By the previous theorem, there is a sequence $< v_n > \subseteq V$ with limit r. But then every nbhd of r should contain (even infinitely many) elements of the sequence. The last is **not** true for $\mathbb{R} \setminus V$ - a contradiction. This proves item (1).
To prove (2), arguing again by contradiction, assume V is not closed. So, $\mathbb{R} \setminus V$ is not open, that is, there is a point $x \in \mathbb{R} \setminus V$ for which $\mathbb{R} \setminus V$ is **not** a nbhd. This means in turn that, for every positive integer n, the intersection $V \cap (x - 1/n, x + 1/n)$ is non-empty. Define a sequence $< v_n >$ by $v_0 = v_1 \in V \cap (x-1, x+1)$ and for $n \geq 2$, $v_n \in V \cap (x - 1/n, x + 1/n)$. Obviously, $< v_n > \to_n x$ and, since $x \notin V$, $< v_n > \subseteq V \setminus \{x\}$. By the previous theorem, x is an accumulation point of V, and therefore, by our hypothesis about V, it belongs to V. So, $x \notin V \wedge x \in V$ - an absurd. □

The following is an important property of the classical topology on $\mathbb{R}$.

Theorem 6.2.6 (Bolzano-Weierstrass (for sets of real numbers)) *Every infinite and bounded subset $A \subseteq \mathbb{R}$ has an accumulation point.*

Proof. Since A is bounded, we have that $A \subseteq [a, b]$ for some real numbers a, b. The idea of the proof is to construct two sequences, one of which, $< a_n >$, being increasing, and the other, $< b_n >$, decreasing, and having the following properties.

$$(\forall n, m \in \mathbb{N})((a_n \leq b_m),$$

$$(\forall n \in \mathbb{N}) \left(b_n - a_n = \frac{b-a}{2^n} \right),$$

and

$$(\forall n \in \mathbb{N})(A \cap (a_n, b_n) \quad \text{is infinite}).$$

Suppose, we have constructed these sequences. Both they are monotone and bounded, so, they are convergent

$$< a_n > \to_n L_1 \quad \text{and} \quad < b_m > \to_m L_2.$$

Since the sequence $< a_n >$ consists of lower bounds of the sequence $< b_m >$, and since L_1 is the least upper bound of $\{a_n \,|\, n \in \mathbb{N}\}$, we immediately get that L_1 is a lower bound of $\{b_m \,|\, m \in \mathbb{N}\}$. Analogously, L_2 is an upper bound of $\{x_n \,|\, n \in \mathbb{N}\}$. From this we get that $L_1 \leq L_2$. On the other hand, since for every $n \in \mathbb{N}$

$$0 \leq L_2 - L_1 \leq b_n - a_n = \frac{b-a}{2^n},$$

we get that $L_1 = L_2 (=: L)$. We claim now that L is an accumulation point for A. Indeed, let $\epsilon > 0$ be given. Since $L - \epsilon = L_1 - \epsilon$ is not an upper bound of $\{a_n \,|\, n \in \mathbb{N}\}$ there is $n_1 \in \mathbb{N}$ such that $L - \epsilon < a_{n_1} \leq L$. Analogously, $L + \epsilon = L_2 + \epsilon$ is not a lower bound of $\{b_m \,|\, m \in \mathbb{N}\}$, there is $n_2 \in \mathbb{N}$ such that $L \leq b_{n_2} < L + \epsilon$. Denoting by n_0 the maximum of n_1 and n_2, we get that

$$L - \epsilon < a_{n_0} \leq L \leq b_{n_0} < L + \epsilon.$$

In other words, $(a_{n_0}, b_{n_0}) \subset (L - \epsilon, L + \epsilon)$. But then

$$A \cap (a_{n_0}, b_{n_0}) \;\subset\; A \cap (L - \epsilon, L + \epsilon)$$

which immediately implies that the ϵ-nbhd of L has infinitely elements of A. This completes the proof that L is an accumulation point of A.
We are constructing the sequences $< a_n >$ and $< b_m >$ now. We do this recursively.
Define $a_0 = a$ and $b_0 = b$. We obviously have that $0 < b_0 - a_0 = (b-a)/2^0$ and $A \cap (a_0, b_0) = A$ is an infinite set.
Suppose we have defined a_n and b_n such that

$$a_{n-1} \leq a_n < b_n \leq b_{n-1}, \qquad b_n - a_n = \frac{b-a}{2^n}, \quad \text{and} \quad A \cap (a_n, b_n) \text{ is an infinite set.}$$

We have $[a_n, b_n] = [a_n, (a_n + b_n)/2] \cup [(a_n + b_n)/2, b_n]$ and so,

$$A \cap [a_n, b_n] = (A \cap [a_n, \frac{a_n + b_n}{2}]) \cup (A \cap [\frac{a_n + b_n}{2}, b_n]) \quad \text{is an infinite set.}$$

Define a_{n+1} and b_{n+1} as follows. If $A \cap [a_n, \frac{a_n+b_n}{2}]$ is infinite, then $a_{n+1} = a_n$ and $b_{n+1} = (a_n + b_n)/2$. If $A \cap [a_n, \frac{a_n+b_n}{2}]$ is finite, denote $a_{n+1} = (a_n + b_n)/2$ and $b_{n+1} = b_n$. It is straightforward to check that

$$a_n \leq a_{n+1} < b_{n+1} \leq b_n, \qquad b_{n+1} - a_{n+1} = \frac{b-a}{2^{n+1}}, \quad \text{and} \quad A \cap (a_{n+1}, b_{n+1}) \text{ is an infinite set.}$$

Using induction, we see that the constructed sequences $< a_n >$ and $< b_m >$ have the promised properties. The proof of the theorem is complete. □

Exercise 6.2.4 (*) *Here is another, more direct, way of proving the Bolzano-Weierstrass Theorem.*
(1) Define $\Sigma = \{r \,|\, (-\infty, r] \cap A \text{ is } finite\} \subseteq \mathbb{R}$. Prove that $\emptyset \neq \Sigma$, and that Σ is bounded above.
(2) Denote by s the least upper bound of Σ, and prove that, for every $\epsilon > 0$, the set $(s, s + \epsilon) \cap A$ is infinite. Conclude that s is an accumulation point of A.

Bolzano-Weierstrass theorem is instrumental in proving many results in Calculus. To see it work, we need to extend the concept of accumulation point from sets to **multisets** of real numbers, and in particular - to sequences.

6.2.4 Accumulation Points of Sequences

We use here "multiset" and "indexed family" interchangeably. As we know, they mean the same thing.

Definition 6.2.6 *Let $\mathcal{A} = \{x_\lambda \in \mathbb{R} \,|\, \lambda \in \Lambda\}$ be an indexed family of real numbers, and let $L \in \mathbb{R}$. The number L is called an* **accumulation point of** $\mathcal{A}$ *if for every* **nbhd** U *of L we have that*

$$\{\lambda \in \Lambda \,|\, x_\lambda \in U\}$$

is an infinite set.

A bit informally, L is an accumulation point of an multiset if every nbhd of L contains infinitely many **members** of the multiset. Obviously, for $\mathcal{A}$ to have an accumulation point, Λ has to be infinite.

The accumulation points of multisets can be studied in utmost generality, for any infinite indexing set Λ, but in our course we are interested in the smallest possible infinite such set: $\Lambda \subseteq \mathbb{N}$. So, from this point on, we consider **sequences** or real numbers only.

First we restate the definition of an accumulation point of a sequence.

Proposition 6.2.7 *The real number L is an accumulation point of the sequence $< x_n >$ if, and only if,*

$$(\forall \epsilon > 0)(\forall n \in \mathbb{N})(\exists n_0 \in \mathbb{N})(n_0 > n \wedge |x_{n_0} - L| < \epsilon).$$

Proof ($\Rightarrow$) Assume L is an accumulation point of $< x_n >$. Every nbhd of L contains infinitely many members of $< x_n >$. Note that "infinitely many members of $< x_n >$ are in the nbhd" is equivalent to "for every $n \in \mathbb{N}$ there is $n_0 > n$ such that x_{n_0} is in that nbhd. So, in particular, for every $\epsilon > 0$ the nbhd $(L - \epsilon, L + \epsilon)$ of L has this property.
($\Leftarrow$) The claim follows from the fact that every nbhd of L, by definition of nbhd, has a subset of the form $(l - \epsilon, L + \epsilon)$ for an appropriate $\epsilon > 0$. $\square$

It is obvious that the limit of a convergent sequence is an accumulation point of that sequence. The opposite is not true in general: a real number may be an accumulation point without being a limit of a sequence as the following example shows.

Example 6.2.4 Consider the sequence $< x_n >$ be defined by the function $f : \mathbb{N} \to \mathbb{R}$ where $f(2n) = n$ and $f(2n + 1) = 1/(n + 1)$. The real number $L = 0$ is an accumulation point of $< x_n >$, but is not its limit. $\square$

Exercise 6.2.5 *Prove the claim about $L = 0$ in the example above. Prove also that $< x_n >$ has only one accumulation point, and that it does not have a limit.*

We will characterize shortly the convergent sequences in terms of accumulation points only. Here is a first useful claim.

The fact that $\mathbb{N}$ is totally ordered helps us define sub-families of sequences which are sequences as well. Recall that sequences are just functions with domain $\mathbb{N}$ and co-domain $\mathbb{R}$.

Definition 6.2.7 *The sequence $g : \mathbb{N} \to \mathbb{R}$ is a* **subsequence** *of $f : \mathbb{N} \to \mathbb{R}$ if there is a* **strictly increasing** *function $h : \mathbb{N} \to \mathbb{N}$ such that $g = f \circ h$.*

In other words, $g(k) = f(h(k))$ for all $k \in \mathbb{N}$. Denoting $n_k = h(k)$, and using the standard notations $x_n = f(n)$, and $g(k) = y_k$, we get $y_k = x_{n_k}$. So that a subsequence of $< x_n >$ is a sequence $< x_{n_k} >$ where $n_0 < n_1 < \cdots < n_k < \cdots$ are natural numbers.

The following proposition is the counterpart, in the case of **sequences** in $\mathbb{R}$, of the theorem characterizing the accumulation points of **sets** in $\mathbb{R}$ via sequences in the sets converging to those points.

Proposition 6.2.8 *The real number L is an accumulation point of the sequence $< x_n >$ if, and only if there is a subsequence $< x_{n_k} >$ of $< x_n >$ which converges to L.*

Proof Let $< x_n >$ be defined by $f : \mathbb{N} \to \mathbb{R}$. To prove the "only if" part of the claim, assume L is an accumulation point of $< x_n >$. Consider the set $A = \{n \in \mathbb{N} \,|\, x_n = L\}$. We consider two cases: A is finite, and A is infinite. For the latter case notice that $A \subseteq \mathbb{N}$, as well as $A \setminus B \subseteq \mathbb{N}$ have least elements for every **finite** subset $B \subset A$. Define the function $g : \mathbb{N} \to \mathbb{N}$ recursively as follows. Define $g(0)$ to be the least element of A, and, having defined $g(0), g(1), \ldots, g(k)$, set $g(k+1)$ to be the least element of $A \setminus \{g(0), \ldots, g(k)\}$. Obviously, the function g is strictly monotone, and therefore defines a subsequence $< x_{n_k} >$ of $< x_n >$ by $n_k = f(g(k))$. The sequence $< y_k >$ with $y_k = x_{n_k}$, being stationary (i.e., $y_k = L$ for every k), converges to L.
For the case when A is finite, L - an accumulation point of $< x_n >$ is equivalent to L being an accumulation point of $Ran(f)$. Let $\epsilon_n = 1/2^n$ for $n \in \mathbb{N}$. Consider the sets $B_n = \{m \in \mathbb{N} \,|\, x_m \in (L - \epsilon_n, L + \epsilon_n)\}$ where $n \in \mathbb{N}$. All these sets are infinite, and $B_{n+1} \subseteq B_n$ for every $n \in \mathbb{N}$ (Why?). Define the function $h : \mathbb{N} \to \mathbb{N}$ recursively as follows. Set $h(0)$ to be the least element of B_0, and, having defined $h(0), h(1), \ldots, h(k)$, define $h(k+1)$ to be the least element of $B_{k+1} \setminus \{h(0), h(1), \ldots, h(k)\}$. It is straightforward by the construction used that h is a strictly monotone function. Then the sequence $< z_k >$ corresponding to $f \circ h : \mathbb{N} \to \mathbb{R}$ is a subsequence of $< x_n >$, and satisfies the relation

$$|z_k - L| < \epsilon_k = \frac{1}{2^k}$$

and therefore converges to L. This completes the proof of the "only if" part of the proposition. For the "if" part, notice that if L is a limit of a sub-sequence $< x_{n_k} >$ of $< x_n >$, then every nbhd of L contains all but finitely many members of the subsequence, and therefore contains infinitely members of the sequence $< x_n >$. So, L is an accumulation point of $< x_n >$. □

Following is the promised Bolzano-Weierstrass theorem for accumulation points of multisets. We will apply this theorem in the realm of sequences, but will prove it in the general set-up 0f indexed families of real numbers - the proof in the general case is not more complicated than the one for sequences!

Theorem 6.2.9 (**Bolzano-Weierstrass (for multisets of real numbers)**) *If the multiset of real numbers $\mathcal{A}$ is infinite and bounded, then it has an accumulation point. In other words, if $\mathcal{A} = \{x_\lambda \,|\, \lambda \in \Lambda\}$ is an indexed family such that Λ is an infinite set, and there are $m, M \in \mathbb{R}$ so that for every $\lambda \in \Lambda$ we have $m \leq x_\lambda \leq M$, then $\mathcal{A}$ has an accumulation point.*

Proof Let the multiset $\mathcal{A}$ be defined by the function $f : \Lambda \to \mathbb{R}$. There are two cases to consider: $Ran(f)$ finite, and $Ran(f)$ infinite. In the former case, $Ran(f) = \{L_1, \ldots, L_s\}$. Denote by $\Lambda_i = \{\lambda \in \Lambda \,|\, x_\lambda = L_i\}$. Since obviously $\Lambda = \Lambda_1 \sqcup \cdots \sqcup \Lambda_s$, at least one of the sets $\Lambda_i, i = 1, \ldots, s$ is infinite, and so one of the numbers $L_1, \ldots, L_s$ is an accumulation point of $\mathcal{A}$: every nbhd of this L_i has infinitely many members of the family. In the latter case for $Ran(f)$, since it is bounded, with the help of Bolzano-Weierstrass theorem we get a real number L which is an accumulation point of $Ran(f)$, and therefore - an accumulation point of $\mathcal{A}$. □

6.2.5 Convergent Versus Cauchy Sequences II

We are completing in this subsection the comparison between convergent and Cauchy sequences of real numbers. Before that we give, as promised earlier, a characterization of convergent sequences in terms of accumulation points only.

Theorem 6.2.10 *A sequence is convergent if, and only if, it is bounded and has a unique accumulation point.*

Proof ($\Rightarrow$) Let $< x_n > \to L$. We show that L is the only accumulation point of $< x_n >$. Indeed, by RAA, if L' is another one, let $\epsilon = |L - L'|/2 > 0$. By the definition of limit, there are only finitely

many members of $< x_n >$ outside $(L-\epsilon, L+\epsilon)$. Therefore, there are no more than finitely many members of $< x_n >$ in $(L'-\epsilon, L'+\epsilon)$ which contradicts the fact that L' is an accumulation point of $< x_n >$. On the other hand, as we already know, a convergent sequence is bounded. The proof of the only if part of the theorem is complete.
($\Leftarrow$) Conversely, let $< x_n >$ be a bounded sequence which has a unique accumulation point L. We will show that $< x_n > \to L$. To this end, observe first that, for every $\epsilon > 0$, the set $A_\epsilon = \{x_n \,|\, x_n \notin (L-\epsilon, L+\epsilon)\}$ is bounded. If this set is infinite, then it would contain a subsequence of $< x_n >$ which, being bounded as a part of $< x_n >$, would have an accumulation point L' itself. The number L' is clearly an accumulation point of $< x_n >$ as well. Therefore, we should have $L' = L$. But $L' \notin (L-\epsilon, L+\epsilon)$, and can not be equal to L - a contradiction! So, A_ϵ is finite for every $\epsilon > 0$. But this is equivalent to having $< x_n > \to_n L$. $\square$

We are closing this subsection by proving that convergent sequences of real numbers and Cauchy sequences is the same thing.

Theorem 6.2.11 *A sequence $< x_n >$ in $\mathbb{R}$ is convergent if, and only if, it is Cauchy sequence.*

Proof. The "only if" part of the theorem was proved earlier. For the "if" part, assume $< x_n >$ is a Cauchy sequence. Since every Cauchy sequence is bounded, it has an accumulation point. To complete the proof, we have to only show that a Cauchy sequence has **only one** accumulation point. Arguing by RAA, assume L and L' are two distinct accumulation points of $< x_n >$. By the definition of Cauchy sequence we have that

$$(\forall \epsilon > 0)(\exists n_0)(\forall m, n)((m, n \geq n_1) \to (|x_m - x_b| < \epsilon)).$$

Also, by the characterization of the accumulation points of sequences we have

$$(\forall \epsilon > 0)(\forall m_0)(\exists n, m)(n, m > m_0 \ \wedge \ |L - x_n| < \epsilon \ \wedge \ |L' - x_m| < \epsilon).$$

To get a contradiction, let $\epsilon = |L - L'|/3$, and let n_0 be chosen as above. Choose $m_0 = n_0$ and let $m, n > n_0$ such that $\wedge\, |L - x_n| < \epsilon \ \wedge \ |L' - x_m| < \epsilon$. We have, using the triangle inequality, that

$$3\epsilon = |L - L'| = |L - x_n + x_n - x_m + x_m - L'|$$

$$\leq |L - x_n| + |x_n - x_m| + |x_m - L'| < \epsilon + \epsilon + \epsilon.$$

So, $3\epsilon < 3\epsilon$ - an absurd. This completes the proof of the "if" part, and of the theorem. $\square$

6.3 Arithmetic Operations and a Relation on Sequences

The convergent sequences have many of the properties of the real numbers: we can add, multiply and compare sequences pretty much the way we do with real numbers. As a direct consequence, we can introduce subtraction and division of (convergent) sequences as well. We will see that **the arithmetic operations and the relation between** *convergent* **sequences can be translated into the usual arithmetics operations and relation** ($\leq$) **between their limits**. It is this translation which lies in the basis of Cantor's construction of the reals...

We know that sequences of real numbers are just functions from $\mathbb{N}$ to $\mathbb{R}$. Since $\mathbb{R}$ is a ring, we can define operations between sequences of real numbers. As a matter of fact, the domain, $\mathbb{N}$, of these functions doesn't matter in this definition! We can do the same for functions with values in $\mathbb{R}$ (real valued functions) and with any, non-empty, domain X. The set of these functions is denoted by $\mathcal{F}(X, \mathbb{R})$.

Definition 6.3.1 *Define operations addition, $+$, and multiplication, $\cdot$, on $\mathcal{F}(X, \mathbb{R})$ as follows. Let $f, g \in \mathcal{F}(X, \mathbb{R})$.*
(1) $f + g : X \to \mathbb{R}$ is such that $(\forall x \in X)((f+g)(x) = f(x) + g(x))$
(2) $f \cdot g : X \to \mathbb{R}$ is such that $(\forall x \in X)((f \cdot g)(x) = f(x) \cdot g(x))$.

Exercise 6.3.1 *Prove that $(\mathcal{F}(X,\mathbb{R}),+,\cdot)$ is a ring. That is, the operations are commutative and associative, have neutral elements, every element has opposite, the multiplication is distributive over the addition. Show also that unless X is a singleton, $(\mathcal{F}(X,\mathbb{R}),+,\cdot)$ is not a field.*

Definition 6.3.2 *We say that the sequence $< x_n >$* **is less than or equal to the sequence** *$< y_n >$, and we write $< x_n > \leq < y_n >$. if*

$$(\exists n_0 \in \mathbb{N})(\forall n \in \mathbb{N})(n \geq n_0 \to x_n \leq y_n).$$

When $X = \mathbb{N}$, we agreed to denote the functions $f : \mathbb{N} \to \mathbb{R}$ by $< x_n >$ where $x_n = f(n)$. The propositions bellow are stated in these notations. Thus, if in addition $y_n = g(n)$, $z_n = (f+g)(n)$, and if $w_n = (f \cdot g)(n)$, then $< z_n > = < x_n + y_n >$, and $< w_n > = < x_n \cdot y_n >$.

The following theorem establishes the fact of the translation promised above.

Theorem 6.3.1 *Suppose $< x_n > \to_n L$ and $< y_n > \to_n M$. Then we have*
(1) $< x_n + y_n > \to_n L + M$;
(2) $< x_n \cdot y_n > \to_n L \cdot M$;
(3) If $M \neq 0$, then $(\exists n_0)(\forall n \in \mathbb{N})((n \geq n_0) \to (|y_n| \geq |M|/2))$;
(4) If $M \neq 0$, and $y_n \neq 0$ for all $n \geq n_0$, the any sequence $< z_n >$ with $z_n = 1/y_n$ for $n \geq n_0$ is convergent, and $< z_n > \to_n 1/M$;
(5) If $< x_n > \leq < y_n >$, then $L \leq M$
(6) We have

$$L < M \quad \Leftrightarrow \quad (\exists \epsilon > 0)(\exists n_0 \in \mathbb{N})(\forall n \in \mathbb{N})((n \geq n_0) \to (\epsilon < y_n - x_n));$$

(7) If $L = M$, and if the sequence $< z_n >$ has the property that

$$(\exists n_0 \in \mathbb{N})(\forall n \in \mathbb{N})((n \geq n_0) \to (x_n \leq z_n \leq y_n)),$$

then $< z_n > \to_n L$ as well.

Proof All items in the theorem, with the exception of (6), are standard, and the proofs are routine. They are left as an exercise. Item (6) is needed in order to introduce relation between Cauchy sequences later on, when we do Cantor's construction of the reals. We are proving (6) now. Direction ($\Rightarrow$). Let $\epsilon = \delta/3$. There is an n_1 such that $|x_n - L| < \epsilon$ for all $n \geq n_1$. Similarly, there is an n_2 such that $|y_n - M| < \epsilon$ for all $n \geq n_2$. Denoting $n_0 = max\{n_1, n_2\}$, and taking any $n \geq n_0$, we have

$$x_n < L + \epsilon = L + (M - L)/3 = (2L + M)/3$$

and

$$y_n > M - \epsilon = M - (M - L)/3 = (L + 2M)/3.$$

Therefore, for the chosen n, we get

$$y_n - x_n > (L + 2M)/3 - (2L + M)/3 = (M - L)/3 = \epsilon.$$

In the opposite direction, ($\Leftarrow$), we have, by item (5), first that $L \leq M$ Assuming, by RAA, that $M = L = A$, then the sequence $< z_n >$ defined by $z_{2n} = x_n$ and $z_{2n+1} = y_n$ is convergent with limit A. But then the $\epsilon/2-$nbhd of A contains all but finitely many members of $< z_n >$. In particular, for $n \geq n_0$, we have

$$|z_n - z_{n+1}| = |z_n - A + A - z_{n+1}| \leq |z_n - A| + |z_{n+1} - A| < \epsilon/2 + \epsilon/2 = \epsilon.$$

This implies that $|x_n - y_n| < \epsilon$ for all $n \geq n_0$ which is not possible due to the inequality $\epsilon < y_n - x_n$ for all big n too. This contradiction finishes the proof of item (6). $\square$

Exercise 6.3.2 *Prove items (1)-(5) and item (7) in the theorem above.*

Exercise 6.3.3 *(1) Show that if* $< x_n > \to_n L$, *and if* $a \in \mathbb{R}$, *then* $< a \cdot x_n > \to_n a \cdot L$.
(2) If, in addition to (1), $< y_n > \to_n M$, *then* $< x_n - y_n > \to_n L - M$.
(3) If, in addition to (2), $M \neq 0$, *and* $n_0 \in \mathbb{N}$ *is such that* $(\forall n \in \mathbb{N})(n \geq n_0 \to y_n \neq 0)$, *then for* **any** *sequence* $< z_n >$ *with* $z_n = x_n/y_n$ *for* $n \geq n_0$, *we have* $< z_n > \to_n L/M$.

Remark 6.3.1 As we know, the set $\mathcal{F}(\mathbb{N}, \mathbb{R})$ is a commutative ring. The theorem above implies that the sub-set of **convergent in** $\mathbb{R}$, that is, Cauchy, sequences has a structure of a commutative ring, with the inherited from $\mathcal{F}(\mathbb{N}, \mathbb{R})$ operations, as well. Denote this set by $Cauchy(\mathbb{R})$. Because of just explained property of $Cauchy(\mathbb{R})$, we say that it is a sub-ring of $\mathcal{F}(\mathbb{N}, \mathbb{R})$. Both rings are not fields: not all non-zero elements of these have reciprocals. Also, the order $\leq$ is only a partial order. Although, by the cited theorem, the arithmetic properties of Cauchy sequences can be nicely matched with the operations on their limits, the ring $Cauchy(\mathbb{R})$ is far from being a copy of $\mathbb{R}$. But if one identifies the Cauchy sequences having the same limit, then, that's a theorem now, the resulting set can be identified to $\mathbb{R}$. As we'll see shortly, Cantor's construction of $\mathbb{R}$ follows this path, but works with Cauchy sequences in $\mathbb{Q}$ only. □

We close this subsection by proving some facts relating properties of sub-sequences of a sequence to the convergence of that sequence.

Theorem 6.3.2 *(1) If the sequence* $< x_n >$ *is convergent to* L, *then every its subsequence* $< x_{n_k} >$ *is convergent to* L;
(2) The sequence $< x_n >$ *is convergent if, and only if, every its subsequence* $< x_{n_k} >$ *is convergent;*
(3) Suppose that $< x_n >$ *is bounded, and that all its convergent subsequences have the same limit* L. *Then* $< x_n > \to_n L$, *and therefore,* **every** *sub-sequence of* $< x_n >$ *is convergent (to* L*). (In the hypothesis for (3), we do not impose the restriction that* **all** *subsequences be convergent. The restriction is: those subsequences which are convergent all have the same limit.)*

Proof. The proofs of (1) and (2) are easy, and are left as an exercise. We are proving item (3) now. First off, since $< x_n >$ is bounded, it does have a convergent subsequence. So, the set of convergent subsequences of $< x_n >$ is not empty, and, by the hypothesis, all they have the same limit L. If, arguing by RAA, we assume that $< x_n >$ is not convergent itself, then there is an $\epsilon-$nbhd of L which does not contain infinitely many elements of $< x_n >$. Therefore, there is a subsequence of $< x_n >$ outside of that $\epsilon-$nbhd of L. The latter subsequence is bounded, as a subsequence of $< x_n >$, and has a convergent subsequence itself. The limit of this subsequence can not be L, because all its elements are no closer than ϵ to L. On the other hand, new subsequence is a subsequence of $< x_n >$, and its limit should therefore be L - a contradiction. □

Exercise 6.3.4 *Prove items (1) and (2) of the previous theorem.*

6.4 Intro to Cantor's Real Numbers

One of the morals we can draw from the previous section is that with the operations addition and multiplication, and with the relation $\leq$ for sequences, the convergent sequences of real numbers share many, if not all, of the properties of real numbers. The link between the two, sequences on one hand and real numbers on other, is given by the limits of the convergent sequences. Having in mind that **convergent** and **Cauchy** are synonyms as far as sequences are concerned, we see that Cauchy sequences, with the two operations and the relation above, behave much like real numbers. This observation leads naturally to another way of constructing the real numbers: instead of Dedekind cuts, one, following Cantor, can work with Cauchy sequences of **rational** numbers. Of course, in this approach one is bound to work with **rational** numbers only: they are constructing the real numbers anew, and should know nothing about them in this construction.

So, one considers Cauchy sequences of rational numbers, but for that they have to define these sequences in terms of rational numbers only. This can easily be done by modifying the definition we introduced in section 6.2:

Definition 6.4.1 *The sequence of rational numbers* $< x_n >$ *is called* **a Cauchy sequence** *if*

$$(\forall\ 0 < \epsilon \in \mathbb{Q})(\exists n_0 \in \mathbb{N})(\forall m, n \in \mathbb{N})(m, n \geq n_0 \rightarrow |x_n - x_m| < \epsilon).$$

Now, some of these Cauchy sequences will have a limit in $\mathbb{Q}$, but most of them wont. Also, in the cases when the limit exists, there are many Cauchy sequences with the same limit, and in order to speak of the limits and of sequences interchangeably, one has to identify **all** Cauchy sequences having the same limit, and associate this class of identified sequences with their common limit. It turns out that two sequences, $< x_n >$ and $< y_n >$ have to be identified if and only if

$$< x_n - y_n > \rightarrow_n 0.$$

Notice that the sequence $< x_n - y_n >$ is a Cauchy sequence of **rational** numbers. Since $0 \in \mathbb{Q}$, one can express the condition for identification of Cauchy sequences entirely in the realm of $\mathbb{Q}$.
A sequence with limit 0 is called a **null** sequence. So, more formally, one introduces a relation between Cauchy sequences as follows

$$< x_n > \sim < y_n > \qquad \text{if} \qquad < x_n - y_n > \quad \text{is null.}$$

This relation turns out to be an equivalence relation on the set $\mathcal{C}auchy(\mathbb{Q})$ of Cauchy sequences of rational numbers. The corresponding quotient set is the set of Cantor real numbers

$$\mathbb{R}_{\mathcal{C}} = \mathcal{C}auchy(\mathbb{Q})/\sim .$$

The operations addition and multiplication and the relation $\leq$ on $\mathcal{C}auchy(\mathbb{Q})$ descend to $\mathbb{R}_{\mathcal{C}}$ to make out of it an ordered field. Also, associating with every rational number x the class of the **stationary** sequence $< x_n >$, $x_n = x$, one gets a natural map

$$\psi_{\mathbb{Q}} : \mathbb{Q} \rightarrow \mathbb{R}_{\mathcal{C}}$$

which is easily seen to be a monotone homomorphism, with $Ran(\psi_{\mathbb{Q}}) \subseteq \mathbb{R}_{\mathcal{C}}$ a **dense** subset. Finally, and this is the hardest in this approach to prove, one shows that the relation $\leq$ has the least upper bound property, so $\leq$ is continuous.
This all means that $\mathbb{R}_{\mathcal{C}}$ is another **ordered completion** of $\mathbb{Q}$, and therefore, as we already know, is canonically identifiable with $\mathbb{R}$.

The full story of the set $\mathbb{R}_{\mathcal{C}}$ is revealed, naturally, in (the last chapter of) the full version of the LN.

Chapter 7

The Sets $\mathcal{F}(X, Y)$, $X, Y \subseteq \mathbb{R}$

The functions we are discussing in this chapter have domains and co-domains subsets of the set of real numbers:

$$f : X \to Y \qquad X, Y \subseteq \mathbb{R}.$$

Such functions are called **real valued functions of one real variable**. Without much loss of generality, we will consider the co-domains to be just $\mathbb{R}$. When the distinction is important, we will consider smaller co-domains as well. Keep in mind though that two functions are equal when they have the same domains, co-domains, and the same values. So, the co-domains do matter! Our ultimate goal here would be to understand as much as possible the properties of **continuous functions**. But there is an important intermediate step in doing this: understanding **functions which have limit at a point**. Although the notion of limit of a function is considered as an intermediate step on the way toward continuous functions, it is actually more subtle than continuity. We are discussing the latter using the language of sequences of real numbers. So, the knowledge from Chapter 6 is of great importance here.

7.1 Limits of Functions

We begin with a definition. Notice that **limit is defined only for accumulation points of the domain of a function**! We begin with an $\epsilon - \delta$ (read as "epsilon-delta") definition. There are no sequences involved in it. But we will quickly switch to using those, restating the notion of limits in that language.

Definition 7.1.1 (**Limit of a function.** $\epsilon - \delta$) *Let $f : X \to \mathbb{R}$ with $X \subseteq \mathbb{R}$, and $L \in \mathbb{R}$. Let further $x' \in \mathbb{R}$ be an* **accumulation point of** *X. We say that f* **has a limit** *L at x_0, and write $\lim_{x \to x'} f(x) = L$, if*

$$(\forall \epsilon > 0)(\exists \delta > 0)(\forall x \in X)(0 < |x - x'| < \delta \to |f(x) - L| < \epsilon).$$

Important: the number x' in the Defintion above need not belong to X, but it **should be an accumulation point of** X. This has to be the case even when $x' \in X$. The question whether there is a limit of a function at a point which is not an accumulation point of the domain of that function makes no sense!

An instance of x' being an accumulation point of X is when, for some $\epsilon > 0$, the punctured epsilon nbhd of x', or half of it, is a subset of X: $(x' - \epsilon, x' + \epsilon) \setminus \{x'\} \subseteq X$, or $(x' - \epsilon, x') \subseteq X$, or $(x', x' + \epsilon) \subseteq X$. This are the cases considered in any standard Calculus book. Needless to say, these represent very incompletely the whole variety of possible cases of x' being an accumulation point of X.

Example 7.1.1 Suppose the function f has a domain which is discrete subset of $\mathbb{R}$, that is, suppose $Dom(f)$ has no accumulation points. Then f has no limit at any real number. (We will see shortly that such a function, not having limits at all, is actually **continuous**).

Exercise 7.1.1 *(1) Prove that* $\lim_{x\to x'} f(x) = L$ *if, and only if,* x' *is an accumulation point of* X*, and* $(\forall \epsilon > 0)(\exists \delta > 0)$ *such that*

$$\mathcal{P}(f)_* \left((x' - \delta, x' + \delta) \cap (X \setminus \{x'\})\right) \subseteq (L - \epsilon, L + \epsilon).$$

(2) Prove that $\lim_{x\to x'} f(x) = L$ *if, and only if,* x' *is an accumulation point of* X*, and* $(\forall \epsilon > 0)$ *the total pre-image* $\mathcal{P}^*(f)((L - \epsilon, L + \epsilon))$ *is a non-empty (may be punctured) nbhd of* x'*, that is*

$$\mathcal{P}^*(f)((L - \epsilon, L + \epsilon)) = X \cap U$$

where U *is a nbhd of* x' *in* $\mathbb{R}$*.*

Led by the need for satisfying the restriction $0 < |x - x'|$ in the definition of limit, we introduce appropriate sequences to be used in our reasonings below. Such sequences exist only for x' which are accumulation points of the domain of f.

Definition 7.1.2 *Let* $f : X \to \mathbb{R}$*, and* $x' \in \mathbb{R}$*. The sequence* $< x_n >$ *is called* **a good sequence for** f **at** x' *if*
(1) $< x_n > \subseteq X \setminus \{x'\}$*;*
(2) $< x_n > \to_n x'$*.*

Observe that good sequences for f at x' exist if, and only if, x' is an accumulation point for X.

Exercise 7.1.2 *Show that if* $< x_n >$ *and* $< y_n >$ *are good sequence for* f *at* x'*, then so is the sequence* $< z_n >$ *defined by*

$$z_n = \begin{cases} x_k & \text{if } n = 2k \\ y_k & \text{if } n = 2k + 1 \end{cases}$$

Here is the reformulation of limit at x' in terms of sequences.

Theorem 7.1.1 (**Limit of Function**; **Sequential Approach**) *Let* $f : X \to \mathbb{R}$ *be a function with* $x' \in \mathbb{R}$ *- an accumulation point of* X*.*
(1) Assume that, for every good sequence $< x_n >$ *for* f *at* x'*, the sequence* $< f(x_n) >$ *is convergent. Then the limit of any such* $< f(x_n) >$ *is independent of the sequence.*
(2) $\lim_{x\to x'} f(x)$ *exists if, and only if, for every good sequence* $< x_n >$ *for* f *at* x'*, the sequence* $< f(x_n) >$ *is convergent. In such a case, we have*

$$< f(x_n) > \to_n \lim_{x\to x'} f(x).$$

Proof. For item (1) we have to show that for any good sequence $< x_n >$, the limit of $< f(x_n) >$ is equal to L which is the same for all such sequences. To this end, let $< f(x_n) > \to_n L_1$ and $< f(y_n) > \to_n L_2$ for the good sequences $< x_n >$ and $< y_n >$. As we know from a previous exercise, the sequence $< z_n >$ where $z_{2n} = x_n$ and $z_{2n+1} = y_n$, is a good sequence as well. So $< f(z_n) > \to_n L_3$. We know that a subsequence of any convergent sequence is convergent to the same limit. Since both $< f(z_{2n}) >$ and $< f(z_{2n+1}) >$ are subsequences of $< f(z_n) >$, they are convergent both to L_3. This immediately gives that $L_1 = L_2 = L_3$.
Proof of item (2). Assume $\lim_{x\to x'} f(x) = L$. We have to show that, for every good sequence of f at x', we have $< f(x_n) >$ is convergent. We will prove that actually $< f(x_n) > \to_n L$. Let $\epsilon > 0$. By the definition of limit of a function at a point we have that there is a δ such that

$$y \in (x' - \delta, x' + \delta) \cap (X \setminus \{x'\}) \to f(y) \in (L - \epsilon, L + \epsilon).$$

But since $< x_n >$ is a good sequence for f at x', there is n_0 such that for $n \geq n_0$ we have $x_n \in (x'-\delta, x'+\delta)$. This immediately implies that, for $n \geq n_0$, we have $f(x_n) \in (L-\epsilon, L+\epsilon)$. Since this is true for any ϵ, we get that $< f(x_n) > \to_n L$ as promised. To prove the other direction in (2), assume that, for every good sequence of f at x', we have the sequence $< f(x_n) >$ is convergent. By item (1) we have that all these sequences converge to the same real number, call it L. We will prove now that $\lim_{x\to x'} f(x) = L$. Arguing by RAA, assume there is an $\epsilon_0 > 0$ such that for every $\delta > 0$ there is an $y \in (x'-\delta, x'+\delta) \cap (X \setminus \{x'\})$ such that $|f(y)-L| \geq \epsilon_0$. Choosing $\delta = 1, 1/2, \ldots, 1/n, \ldots$ we get a good sequence $< y_n >$ with $y_n \in (x'-1/n, x'+1/n) \cap (X \setminus \{x'\})$. But then, by our assumption, $< f(y_n) > \to_n L$. On the other hand, for all n, we have $|f(y_n) - L| \geq \epsilon_0$. This contradiction finishes the completes our argument. $\square$

Knowing the relation between convergent and Cauchy sequences, we can reformulate item (2) of the last theorem as follows.

Corollary 7.1.2 *Let $f : X \to \mathbb{R}$ be a function, and let $x' \in \mathbb{R}$ be an accumulation point of X. Then, $\lim_{x\to x'} f(x)$ exists if, and only if, for every good sequence $< x_n >$ for f at x', the sequence $< f(x_n) >$ is a Cauchy sequence.*

Proof Obvious. $\square$

The two ways of expressing the concept of limit of a function are useful in different situations. In what follows, we use the sequential approach to prove properties of functions having limits at a point (the same point for all functions involved!).

Theorem 7.1.3 *Let $f, g : X \to \mathbb{R}$ be two functions, and let $x' \in \mathbb{R}$ be an accumulation point of X. Suppose $\lim_{x\to x'} f(x) = L$ and $\lim_{x\to x'} g(x) = M$. We have*
(1) $\lim_{x\to x'}(f+g)(x) = L + M$,
(2) $\lim_{x\to x'}(f \cdot g)(x) = L \cdot M$,
(3) If $M \neq 0$, then there is a $\delta > 0$ such that $(\forall x \in X)((0 < |x - x'| < \delta) \to (|g(x)| > |M|/2))$,
(4) If $M \neq 0$, then $\lim_{x\to x'}(f \div g)(x) = L \div M$,
(5) If there is a $\delta > 0$ such that for all $x \in X$ for which $0 < |x - x'|$ we have $f(x) \leq g(x)$, then $L \leq M$,
(6) (**Squeeze Theorem**) *Suppose $h : X \to \mathbb{R}$ as well, and that there is a $\delta > 0$ such that for all $x \in X$ and $0 < |x - x'| < \delta$ we have $f(x) \leq h(x) \leq g(x)$. If $L = M$, then h has a limit at x', and $\lim_{x\to x'} h(x) = L(= M)$.*

Proof. The model of proving these claims is as follows. Choose a good sequence for both f and g at x', and, using Theorem 7.1.1, reduce proving the corresponding claim to a claim about converging sequences. Items (1), (2), (4), (5), and (6) follow directly from the similar claims about sequences discussed in the previous section. We are doing item (3) directly, without using sequences. Let $\epsilon = |M|/2$. By the definition of $\lim_{x\to x'} g(x) = M$ we have that there is a $\delta > 0$ such that

$$x \in (x' - \delta, x' + \delta) \cap (X \setminus \{x_0\}) \quad \to \quad g(x) \in (M - \epsilon, M + \epsilon).$$

Notice now that if $M > 0$, then $(M-\epsilon, M+\epsilon) = (|M|/2, 3|M|/2)$, and if $M < 0$, then $(M-\epsilon, M+\epsilon) = (-3|M|/2, -|M|/2)$. Therefore, for all $x \in (x' - \delta, x' + \delta) \cap (X \setminus \{x'\})$ we have $g(x) > |M|/2$ when $M > 0$, and $g(x) < -|M|/2$ when $M < 0$. In both cases $|g(x)| > |M|/2$. This completes the proof of (3). $\square$

Exercise 7.1.3 *Prove items (1), (2), (4), (5), and (6) of the previous theorem.*

Functions and sequences which converge to 0 have a very useful for technical purposes property. Here it comes.

Theorem 7.1.4 *(1) Suppose $< x_n >$ is bounded, and that $< y_n > \to_n 0$. Then we have $< x_n \cdot y_n > \to_n 0$ as well.*

(2) Suppose $f, g : X \to \mathbb{R}$ are such that $\lim_{x\to x'} f(x) = 0$, and that g is bounded in a punctured nbhd of x'. Then we have $\lim_{x\to x'}(f \cdot g)(x) = 0$ as well.

Proof. Item (2) follows immediately from item (1). Item (1) is standard. Both are left as an exercise. □

Exercise 7.1.4 *Prove the previous theorem.*

7.2 Compact Subsets of $\mathbb{R}$

The concept of sub-sequences allows us to define a very special type of widely used subsets of $\mathbb{R}$ - the **compact** subsets. We will have application of these subsets in the section of continuous function when we prove a theorem of Weierstrass.

We know from the theorem of the previous subsection that a sub-set of $\mathbb{R}$ is closed if, and only if, it contains all its accumulation points. In particular, if a subset has no accumulation points, then it is closed. This happens when the subset is finite (for only infinite subsets can have accumulation points). Of course, we knew finite sets are closed without appealing to that theorem: this follows at once from the fact every point in $\mathbb{R}$ is closed, and that, for every topological space, a union of finite closed subsets is closed. On the other hand, there are infinitely closed subsets of $\mathbb{R}$ which do not have accumulation points (for instance, $\mathbb{N} \subset \mathbb{R}$). By the contra-positive of Bolzano-Weierstrass' theorem, in the latter case the set should be unbounded. Turns out that the sub-sets of $\mathbb{R}$ which are closed and bounded are very important - they are compact!

Definition 7.2.1 *The subset $C \subseteq \mathbb{R}$ is called* **a compact** *subset if every sequence $< x_n > \subseteq C$ has a convergent sub-sequence with limit in C: $< x_{n_k} > \to_k c_0 \in C$.*

The proof of the following characterization of compact subsets of $\mathbb{R}$ uses the Bolzano-Weierstrass theorem in a significant way.

Theorem 7.2.1 *A set $X \subseteq \mathbb{R}$ is compact if, and only if it is closed and bounded.*

Proof. We prove first that X - closed and bounded in $\mathbb{R}$ implies that X is compact. To this end, let $f =< x_n > \subseteq X$ be a sequence in X. Since X is bounded, the sequence is also bounded, and therefore has an accumulation point x. This x is an accumulation point of X as well, and since X is closed, $x \in X$. By the characterization of the accumulation points of sequences, we get that $< x_n >$ has a subsequence converging to L. So, X is compact. The opposite direction, that X compact implies that X is closed and bounded, can be proved as follows. Let y be an accumulation point of X. Then, there is a sequence in $X$is sequence has a subsequence which converges to a point $x \in X$. But x being a limit of the subsequence, is an accumulation point thereof, and is therefore an accumulation point of the sequence as well. Since every convergent sequence has a unique accumulation point, we get that $x = y$, and that $y \in X$. This means that X contains all of its accumulation points, and therefore is closed. To prove that X is also bounded, notice (and prove it!) that an unbounded sub-set of $\mathbb{R}$ has a an infinite sub-set without accumulation points, and so no sequence in that sub-set can be convergent. □

Exercise 7.2.1 *Fill in the gaps in the proof of the theorem above.*

7.3 Compact Subsets of a Topological Space

One can go even further and show that the compactness can actually be explained without mentioning sequences at all! That is this concepts can be generalized to any topological space. We need a definition first.

Definition 7.3.1 *Let Y be a sub-set of a topological space $(X, \mathcal{T}_X)$. An* **open cover of** *Y is a family $\mathcal{U} \subseteq \mathcal{T}_X$ such that $Y \subseteq \cup\mathcal{U}$. The family $\mathcal{V} \subseteq \mathcal{T}_X$ is called a sub-cover of $\mathcal{U}$ if $\mathcal{V}$ is an open cover of Y and $\mathcal{V} \subseteq \mathcal{U}$. The open cover $\mathcal{U}$ of Y is called* **finite** *if $\mathcal{U}$ is a finite set.*

We have the following result.

Theorem 7.3.1 *A sub-set C of $\mathbb{R}$ is compact if, and only if, every open cover of C has a finite sub-cover.*

Proof ($\Leftarrow$) Assume every open cover of C has a finite sub-cover, and $\{x_n \,|\, n \in \mathbb{N}\}$ is a sequence in C. We have to prove that the sequence has an accumulation point in C (this being equivalent to the sequence having a convergent in C sub-sequence). By RAA, assume there is no such a point. This means that every point $y \in C$ has a nbhd U_y which contains finitely many members of the sequence. The family $\{U_y \,|\, y \in C\}$ is an open cover of C. So, according to our assumption, there are finitely many points $y_1, \ldots, y_m \in C$ such that $C = U_{y_1} \cup \cdots \cup U_{y_m}$. Therefore every member of the sequence belongs to one of these finitely many sets. Since each set U_{y_j} contains finitely many members of the sequence, it follows that the sequence has finitely many members - an absurd!
($\Rightarrow$) Assuming that C is compact, that is, every sequence in C has a sub-sequence converging in C, and that $\mathcal{U} = \{U_\lambda \,|\, \lambda \in \Lambda\}$ is an open cover of C, we have to prove that $\mathcal{U}$ has a finite subset which is also a cover of C. If $\mathcal{U}$ is a finite set, we are done. So, we may assume that $\mathcal{U}$ is infinite. We consider first the case $\mathcal{U}$ is denumerable: $\mathcal{U} = \{U_n \,|\, n \in \mathbb{N}\}$, and argue by contradiction. So suppose there is no a finite subset of $\mathcal{U}$ which is also a cover. This means that for every $n_1, \ldots, n_k$

$$U_{n_1} \cup \cdots \cup U_{n_k} \subsetneqq C.$$

We are constructing a sequence in C which is not convergent in C. Choose c_0 to be any element of C, and let U_{n_0} contain c_0. Note that the latter exists, because $\cup_{n\in\mathbb{N}} U_n = C$. Choose for c_1 any element of C which is not in U_{n_0}, and let U_{n_1} be such that $c_1 \in U_{n_1}$. Having chosen $c_0, c_1, \ldots, c_m$ with the corresponding $U_{n_0}, U_{n_1}, \ldots, U_{n_m}$, choose for c_{m+1} an element of C which is not in $U_{n_0} \cup U_{n_1} \cup \cdots \cup U_{n_m}$, and find $U_{n_{m+1}}$ that contains c_{m+1}. Since for every $m \in \mathbb{N}$ we have

$$u_{n_m} \cap \{c_n \,|\, n \in \mathbb{N}\} \subseteq \{c_0, c_1, \ldots, c_n\}$$

we immediately conclude that $< c_n >$ is not convergent in C. (fill in the details as an exercise).
The most general case, when $\mathcal{U}$ is not countable follows from the "countable" case through the following lemma.

Lemma 7.3.2 *If $C \subseteq \mathbb{R}$ is a compact sub-set, then every cover of open subsets of C has a countable sub-cover.*

The proof of lemma is a little bit involved. We will prove it in 4 steps.
Step (1): For every positive integer n, there are finitely many points $\{c_1^{(n)}, \ldots, c_{k_n}^{(n)}\} \subseteq C$ such that

$$C \subseteq \cup_{i=1}^{k_n} \left(c_i^{(n)} - \frac{1}{n}, c_i^{(n)} + \frac{1}{n} \right).$$

Therefore, for every $c \in C$ there is a $1 \leq j \leq k_n$ so that $|c - c_j^{(n)}| < 1/n$. Observe now that the family of intervals

$$\{V_{n,j} = (c_j^{(n)} - 1/n, c_j^{(n)} + 1/n) \,|\, 1 \leq n \in \mathbb{N},\, 1 \leq j \leq k_n\}$$

contains countably many elements.
Step (2): Let $V \subseteq \mathbb{R}$ be an open sub-set, and let $c \in C \cap V$. There exist n, j such that

$$c \in V_{n,j} \subseteq V.$$

Since $c \in V$, and V is open in $\mathbb{R}$, there is an $\epsilon > 0$ such that $(c - \epsilon, c + \epsilon) \subseteq V$. Since $\mathbb{R}$ has the Archimedean property, there is an $n \in \mathbb{N}$ such that $n > 2/\epsilon$. By Step (1), there is a

$c \in (c_j^{(n)} - 1/n, c_j^{(n)} + 1/n) = V_{n,j}$. We have then that $c \in V_{n,j} \subseteq (c - \epsilon, c + \epsilon) \subseteq V$ (verify this as an exercise!). The proof of Step (2) is complete.
Step (3): Let $\mathcal{U} = \{u_\lambda \,|\, \lambda \in \Lambda\}$ be an open cover of C. Consider the set of pairs

$$\Sigma = \{(n, j) \,|\, (\exists \lambda \in \Lambda)(V_{n,j} \subseteq U_\lambda\},$$

and notice that Σ is a countable set. Define, using the Axiom of Choice in general, $\varphi : \Sigma \to \Lambda$ by $\varphi((n, j)) = \mu \in \Lambda$ such that $V_{n,j} \subseteq U_\mu$. Since Σ is countable, the set $Ran(\varphi)$ is countable as well.
Step (4): The family $\mathcal{V} = \{U_\lambda \,|\, \lambda \in Ran(\varphi)\}$ is a (countable) sub-cover of $\mathcal{U}$.
To prove this claim, we have to show that $C \subseteq \cup\mathcal{V}$. To this end, let $c \in C$. There is a $\lambda_0 \in \Lambda$ such that $c \in U_{\lambda_0}$. By Step (2), there is a triplet (n_0, j_0) such that $c \in V_{n_0,j_0} \subseteq U_{\lambda_0}$. So, $(n_0, j_0) \in \Sigma$. By the definition of φ we have that $V_{n_0,j_0} \subseteq U_{\varphi((n_0,j_0))}$, and therefore $c \in U_{\varphi((n_0,j_0))}$. This immediately implies that $c \in \cup\mathcal{V}$. Since c is any point in C, we get what we wanted to prove: $C \subseteq \cup\mathcal{V}$.

The theorem is proved. □

This theorem motivates the following definition.

Definition 7.3.2 *Let C be a subset of a Hausdorff topological space $(X, \mathcal{T}_X)$. C is called* **compact** *if every open cover of C has a finite sub-cover. The space X is called compact if it is compact as a sub-set of itself.*

We know that in $\mathbb{R}$ compact subsets are closed and bounded. The generalization of boundedness to a general topological space is involved, and we will skip its discussion here. On the other hand, closed subsets are given by the topology of X. We have the following result relating compact subsets to close subsets of X when X is separated.

Theorem 7.3.3 *Let K be a compact sub-set of the separated topological space $(X, \mathcal{T}_X)$. Then, K is closed in X.*

Proof It is equivalent to showing that $X \setminus K$ is open in X. To this end, let $y \in X \setminus K$. We have to show that y has a nbhd which is disjoint with K. For every $x \in K$, let U_x, V_x be open subsets such that $x \in U_x$, $y \in V_x$, and $U_x \cap V_x = \emptyset$. Such open sets exist, because X is a separable topological space. Now, the family $\mathcal{U} = \{U_x \,|\, x \in K\}$ is an open cover of K, and since K is compact, $\mathcal{U}$ has a finite sub-cover. That is, there are $x_1, x_2, \ldots, x_s \in K$ such that $K \subseteq U_{x_1} \cup \cdots \cup U_{x_s}$. Let $V = V_{x_1} \cap \cdots \cap V_{x_s}$. Obviously $y \in V$, and

$$V \cap (U_{x_1} \cup U_{x_2} \cup \cdots \cup U_{x_s}) = \emptyset.$$

Therefore $V \cap K = \emptyset$ as well, and we are done. □

7.4 Continuity of Functions

The concept of continuity is simpler than the one of limit! Here is the "epsilon-delta" definition of the concept. Enjoy!

Definition 7.4.1 *Let $f : X \to \mathbb{R}$ be a function, and let $x_0 \in X$. We say that f* **is continuous at** *x_0 if*

$$(\forall \epsilon > 0)(\exists \delta > 0)(\forall x \in X)((|x - x_0| < \delta) \to (|f(x) - f(x_0)| < \epsilon)).$$

The function f is called **continuous**, *if it is continuous at every point $x_0 \in X$.*

Exercise 7.4.1 *(1) Prove that the function $f : X \to \mathbb{R}$ is continuous at $x_0 \in X$ if, and only if, for every nbhd V of $f(x_0)$ the total pre-image $\mathcal{P}^*(f)(V)$ is a nbhd of x_0. By definition, this means that, for every such nbhd V, there is a nbhd U of x_0 in $\mathbb{R}$ such that*

$$\mathcal{P}^*(f)(V) = X \cap U.$$

(2) Prove that $f : X \to \mathbb{R}$ is continuous if, and only if, for every open subset $V \subseteq \mathbb{R}$, the total pre-image $\mathcal{P}^*(f)(V) \subseteq X$ is an open subset. Again by definition this means that, for every such V, there is an open subset $U \subseteq \mathbb{R}$ such that

$$\mathcal{P}^*(f)(V) = X \cap U.$$

This exercise motivates the following definition for **any topological spaces**.

Definition 7.4.2 *Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be two topological spaces, and let $f : X \to Y$ be a set map.*
(1) The map is continuous at $x_0 \in X$ if for every $V \in \mathcal{T}_Y$ such that $f(x_0) \in V$, there is a $U \in \mathcal{T}_X$ with $x_0 \in U$ and $U \subseteq \mathcal{P}^*(f)(V)$.
(2) The map is continuous if it is continuous at every point of X. Equivalently, f is continuous if for every $V \in \mathcal{T}_Y$ we have $\mathcal{P}^*(f)(V) \in \mathcal{T}_X$.

Returning to the case at hands, $X, Y \subseteq \mathbb{R}$, notice that the only restriction on x_0 in the definition of continuity of f at x_0 is that $x_0 \in X$. There is no need for f to be defined in a **punctured nbhd** of x_0, as is a standard approach in popular Calculus books. Also, comparing to the defintion of limit of f at x_0, we have L determined by f itself: $L = f(x_0)$, and x_0 need not be an accumulation point of X. Moreover, having a limit and being continuous at x_0 are independent features of f at x_0 in general. For instance, it is possible for f to have a limit at x_0 without being continuous at it, as well as it is possible for f to be continuous at x_0 without having a limit at it! **The concept of limit and of continuity of f at a point, x_0, are related only if $x_0 \in X$ is an accumulation point of X.** Here is the link between the two concepts explained.

Theorem 7.4.1 *Let $f : X \to \mathbb{R}$, and $x' \in X$ be an accumulation point of X. Then the following statements are equivalent.*
(1) f is continuous at x';
(2) If $< x_n >$ is a good sequence for f at x', then $< f(x_n) >$ converges to $f(x')$;
(3) f has a limit at x', and $\lim_{x \to x'} f(x) = f(x')$;

Proof. Follows directly from the definitions, and from the properties of limits of a function at a point and good sequences of a function at a point. □

Exercise 7.4.2 *Prove the previous theorem.*

As a contrast verify the following.

Exercise 7.4.3 *Suppose $f : X \to \mathbb{R}$, $x' \in X$ which is not an accumulation point of X. Then f is continuous at x'. Conclude that if X is a discrete subset of $\mathbb{R}$, i.e., X has no accumulation points in $\mathbb{R}$, then f is a continuous function. Moreover, f has no limit at any real number!*

The following theorem is a direct consequences of Theorem 7.1.3.

Theorem 7.4.2 *Let $f, g : X \to \mathbb{R}$ be two continuous at $x_0 \in X$ functions. Then, we have*
(1) $f + g$ is continuous at x_0,
(2) $f \cdot g$ is continuous at x_0,
(3) If $g(x_0) \neq 0$, then there is a $\delta > 0$ such that $(\forall x \in X)((|x - x_0| < \delta) \to (|g(x)| \geq |g(x_0)|/2))$;
(4) If $g(x_0) \neq 0$, then $f \div g$ is continuous at x_0;
(5) Suppose $h : X \to \mathbb{R}$ as well, and that there is a $\delta > 0$ such that for all $x \in X$ and $|x - x_0| < \delta$, we have $f(x) \leq h(x) \leq g(x)$. If $f(x_0) = g(x_0)$, then h is continuous at x_0 as well.

Proof. Straightforward, using sequences. □

Exercise 7.4.4 *Prove the previous theorem.*

One of most important theorems related to continuous functions is the following one. The property of continuous functions described in this theorem actually characterizes the continuous functions!

Theorem 7.4.3 (**Intermediate Value Theorem**) *Suppose $f : X \to \mathbb{R}$ is a continuous function, and $[a; b] \subseteq X$. Then*

$$(\forall y)((f(a) \leq y \leq f(b) \vee f(b) \leq y \leq f(a)) \to (\exists c)(a \leq c \leq b \wedge y = f(c))).$$

Proof. If $y = f(a)$ or $y = f(b)$, there is nothing to be proved: we choose $c = a$ or $c = b$ respectively. So, let's assume that $f(a) < y < f(b)$. In this case, considering the function $g(x) = f(x) - y$, the statement of the theorem is equivalent to proving that if $g(a) \cdot g(b) < 0$, then there is a $c \in (a, b)$ such that $g(c) = 0$. We are proving therefore the following statement:

Suppose $g(x)$ is continuous in $[a, b]$, and that $g(a) \cdot g(b) < 0$. Then, there is a $c \in (a, b)$ such that $g(c) = 0$.

The idea of the proof is to define two sequences, $< x_n >$ and $< y_n >$, of elements of (a, b) such that $< x_n >$ is increasing, $< y_n >$ is decreasing, for every n, $x_n < y_n$, the two sequences have the same limit, c, and f takes on positive values only on one of the sequences, and negative values only on the other one. All this arranged will force $f(c) = 0$, because if say $f(x_n) < 0$ and $f(y_n) > 0$ then $< f(x_n) > \to_n f(c) \leq 0$, and $< f(y_n) > \to_n f(c) \geq 0$. Also, notice that in this case $a < x_n \leq c \leq y_m < b$, so that $c \in (a, b)$ as needed.

Construction of the sequences $< x_n >$ and $< y_n >$. W.L.O.G. we may assume that $f(a) < 0$ (and therefore that $f(b) > 0$). We construct the sequences by induction (recursion, actually). Define $x_0 = a$ and $y_0 = b$. Assume we have defined $x_0, \ldots, x_n$ and $y_0, \ldots, y_n$ in such a way that

$$x_0 \leq \cdots \leq x_n, \quad y_0 \geq \cdots \geq y_n, \quad y_k - x_k = \frac{b-a}{2^k}, \quad f(x_k) < 0 < f(y_k) \quad k = 0, \ldots n.$$

We are defining x_{n+1} and y_{n+1} as follows. Consider the midpoint $x' = (x_n + y_n)/2$ of the interval $[x_n, y_n]$. If $f(x') = 0$, then we choose $c = x'$, and are done. So, assume that $f(x') \neq 0$. If $f(x') < 0$, we define $x_{n+1} = x'$ and $y_{n+1} = y_n$. If $(x') > 0$, we define $x_{n+1} = x_n$, and $y_{n+1} = x'$. In any case, we have that

$$x_n \leq x_{n+1}, \quad y_n \geq y_{n+1}, \quad f(x_{n+1}) < 0 < f(y_{n+1}), \quad y_{n+1} - x_{n+1} = \frac{b-a}{2^{n+1}}$$

as needed. This way we construct the two sequences, and therefore complete the proof. □

Exercise 7.4.5 (*) *The important Intermediate Value Theorem can be proved many ways. One of them is sketched here.*
(1) W.L.O.G., we may assume that $f(a) < y < f(b)$. Consider in this case the set

$$\Sigma = \{r \mid (\forall x)(x \in (a, r) \to f(x) < y)\}$$

and prove that it is non-empty, and bounded above.
(2) Let s be the least upper bound of Σ. Construct good sequences for f at s, $< x'_n >$ and $< x''_n >$, such that $f(x'_n) < y < f(x''_n)$.
(3) Conclude the proof using that f is continuous at s, and applying item (5) of Theorem 6.3.1.

This theorem has a geometric (topological) meaning.

Corollary 7.4.4 *Suppose $X \subseteq \mathbb{R}$ is an interval, no matter open, closed or semi-open/semi-closed. If $f : X \to \mathbb{R}$ is a continuous function, then $Ran(f) \subseteq \mathbb{R}$ is also an interval. That is, if $y_1, y_2 \in Ran(f)$ with $y_1 < y_2$, then*

$$(\forall y)((y_1 < y < y_2) \to (\exists x \in X)(y = f(x))).$$

Proof. To $a, b \in X$ such that $y_1 = f(a)$ and $y_2 = f(b)$ apply the Intermediate Value Theorem. □

Exercise 7.4.6 *Complete the proof of the previous corollary.*

As mentioned before, the compact subsets of $\mathbb{R}$ are very useful when working with continuous functions. This is so, partially for the following reason.

Theorem 7.4.5 *Let $X \subseteq \mathbb{R}$ be a subset, $K \subseteq X$ be a compact subset, and let $f : X \to \mathbb{R}$ be a continuous function. Then $f(K) \subseteq \mathbb{R}$ is also compact.*

Proof. We need to show that every sequence $< y_n > \subseteq f(K)$ has a convergent in $f(K)$ subsequence.. But there is a sequence $< x_n > \subseteq K$ such that $(\forall n)(y_n = f(x_n))$. Since K is compact, there is a subsequence $< x_{n_k} > \to_k x' \in K$. Since f is continuous, then $< f(x_{n_k}) > \to_k f(x') \in f(K)$. So, $< y_{n_k} >$ is a subsequence of $< y_n >$ which is convergent in $f(K)$ as needed. □

Exercise 7.4.7 *Prove this theorem using the equivalent description of compact subsets in terms of open covers.*

Here is a theorem which provides an excellent finale to our Introduction to Advanced Calculus part of the Notes!

Theorem 7.4.6 (**Weierstrass**) *Let $f : X \to \mathbb{R}$ be a continuous function with $X \subseteq \mathbb{R}$ - a compact subset. Then, f attains its* **minimum** *and* **maximum** *values on X. In other words,*

$$(\exists x_1, x_2 \in X)(\forall x \in X)(f(x_1) \leq f(x) \leq f(x_2)).$$

Proof. We know that $Ran(f)$ is compact in $\mathbb{R}$, so it is closed and bounded. The boundedness gives us that $Ran(f)$ has l.u.b., M, and g.l.b., m. The closeness of $Ran(f)$ gives us that $m, M \in Ran(f)$. Note that m is the minimum, and that M is the maximum of f on X. □

Example 7.4.1 Since $[a, b] \subseteq \mathbb{R}$ is closed and bounded, then it is compact. If $f : [a, b] \to \mathbb{R}$ is a continuous function, then f attains its extreme values, the minimum and the maximum, on $[a, b]$. □

Exercise 7.4.8 *Let $f : [a, b] \to \mathbb{R}$ be a continuous function. Prove that $Ran(f) = [m, M]$ where m is the minimum, and M is the maximum of f on $[a, b]$.*

$\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Index