Introduction to Mathematical Reasoning

Adrien Deloro

Fall 2007, Fall 2008

Contents

Chapter I

Hieroglyphs

- *'Take some more tea', the March Hare said to Alice, very earnestly.*
- *'I've had nothing yet', Alice replied in an offended tone, 'so I can't take more.'*
- *'You mean you can't take* less*', said the Hatter: 'it's very easy to take more than nothing.'*

In this chapter we learn *how to write mathematics.*

First of all, *what* should we write? Not all sentences are relevant for us; we must determine which can be treated by logic. These are called propositions and dealt with in §I.1. Then we shall turn to the alphabet of mathematics, an alphabet with very few symbols. In §I.2 we introduce the connectives used to link two sentences, like in any language. As mathematicians often say "there is" and "for all", we shall also work with quantifiers in §I.3.

Hence the aim of this first chapter is neither to know what is true nor to write your first proofs, but to be able to deal with sentences made of mathematical symbols. It is as annoying as solfeggio, but as useful and easier.

Main goals: Learn mathematical language:

- Determine if a sentence is a proposition or not.
- Translate from English to mathematics and back.
- Find the truth table of a given proposition.
- Compute the negation of a given proposition.
- Manipulate logic expressions.

Notions. Proposition, Connective, Quantifier, Truth table

LECTURE 1 (INTRODUCTION. PROPOSITIONS. CONNECTIVES: $\neg$, $\wedge$, $\vee$.)

I.1 Propositions

Only some sentences are subject to logic treatment. Let us study a few examples.

Example I.1.1.

Sentence	Belongs to logic?	True/False?
$0 = 0$	Y	T
I am here.	N	/
π is equal to 3.	Y	F
Kangaroos lay eggs.	Y	F
$x = 0$	N	/
Hence $2 > 0$.	N	/

Remark I.1.2.

- Though "I am here" sounds true to any person saying it, it is a somehow fuzzy sentence since its actual meaning depends on the person saying it.
- Of course $\pi \neq 3$. But the sentence "$\pi = 3$" makes good sense, even though we know it is false. We plainly understand the meaning of the statement.
- "$x = 0$" is not a proposition. Who is x? (Does "He is young" make sense to you? Who is "he"?) The meaning depends on something undefined.
- The sentence starting with "Hence" is obviously part of something else. It bears no sense as is.

The sentences that sound relevant for our purposes are those whose meaning is not fuzzy. They are the sentences one could describe as either "true" or "false".

Definition I.1.3 (proposition, truth value)**.** A proposition is a sentence which is either true or false. "True" or "False" is the truth value of the proposition.

Unfortunately one has to make a digression.

Remark I.1.4. Consider the sentence "Every even number is the sum of two prime numbers". This is a proposition, as we certainly understand its meaning. But nobody - so far - ever knew if it is true or false! (The statement is very famous and known as "Goldbach's Conjecture".)

Hence our apparently easy definition of a proposition actually relies on something very uneasy to define, which is "truth". On the other hand we shall not study such conjectures, and you should be able to determine the truth value of all propositions met in class.

Exercise I.1

In mathematics we consider only propositions. We try to determine which are true and which are false, by giving either proofs or refutations. This will be explained in Chapter II. The goal of the present chapter is merely to manipulate propositions.

Caution! For the sake of pedagogy we shall sometimes use sentences that are not propositions. This is because they provide striking examples which are easily remembered.

Remark I.1.5 (Alternate Expressions)**.** Here are some alternate expressions:

"P is not false", "P holds", "it is the case that" [state P]
- all mean "P is true".

Similarly:

"P is not true", "P does not hold", "it is not the case that" [state P]
- all mean "P is false".

Example I.1.6.
- *'Does the proposition "kangaroos lay eggs" hold?'*
- *'No, it is not the case that kangaroos lay eggs.'*

I.2 Connectives

We can assemble propositions to build more complex propositions. This is what we do every day in English, when using "and" or "or" to connect sentences.

The result of such a joining of expressions is called a *compound proposition*, or a *propositional form* when one wants to stress that it was built from more elementary propositions.

We shall introduce five connectives : not (§I.2.1), and (§I.2.2), or (§I.2.3), implies (§I.2.6), if and only if (§I.2.7). The first three are easily understood. But you might have to pay special attention to the fourth one.

I.2.1 Not

Definition I.2.1 (negation)**.** Let P be a proposition. The negation of P (write $\neg P$, pronounce "not-P") is the proposition that is true if P is false, and false if P is true.

Remark I.2.2. Some old-fashioned authors write $\sim P$ instead of $\neg P$.

Read the following example carefully as it is a very common mistake to think that $x \geq y$ is the negation of $y \geq x$ (actually it is not).

Example I.2.3. Let x and y be real numbers.

- The negation of "$x + 0 = y$" is "$x + 0 \neq y$".
- The negation of "$x > y$" is "$x \leq y$".

It is convenient to encode the properties of the negation in a *truth table*. This merely is an array giving the truth value of a compound proposition, depending on the truth values of its components.

Truth table of $\neg P$:

P	$\neg P$
F	T
T	F

Remark I.2.4. P and $\neg\neg P$ always have the same truth value!

I.2.2 And

Definition I.2.5 (conjunction)**.** Let P and Q be propositions. The conjunction of P and Q (write $P \wedge Q$, pronounce "P and Q") is the proposition that is true if both P and Q are true, false otherwise.

Remark I.2.6. Old-fashioned authors write P & Q. Not recommended.

Convention I.2.7. Before we write the truth table of $\wedge$, we make a remark and adopt a very natural convention. In order to write truth tables with several variables (below, P and Q are our two variables), it will be useful to use *always the same* enumeration of the different entries (below, FF, FT, TF, TT).

Replacing "True" by 1 and "False" by 0, the ordering of entries is very natural: 00, 01, 10, 11. If you think you don't know about binary numeration (and anyway your computer does), just count numbers that use only zeros and ones.

Example I.2.8. The standard enumeration of entries with three variables is
Exercise I.3 $FFF, FFT, FTF, FTT, TFF, TFT, TTF, TTT$.

Here is the truth table of conjunction.

Truth table of $P \wedge Q$:

P	Q	$P \wedge Q$
F	F	F
F	T	F
T	F	F
T	T	T

Caution! In English, there are two ways to use "and". One is for connecting sentences, the other is for enumerations (eg. "You *and* me"). In mathematics *we only have the connective.* This means that when you mean "Let a and b be two numbers", you *may not* write "Let $a \wedge b \dots$".

On the other hand, for a mathematician, "4 is greater than 1 and 2" is short for "4 is greater than 1 and 4 is greater than 2".

Remark I.2.9. You see how poor mathematical language is. The English "but" would be translated by "and", losing the nuance of opposition in it.

Example I.2.10. We compute the truth table of $P \wedge \neg Q$.

P	Q	$P \wedge \neg Q$
F	F	F
F	T	F
T	F	T
T	T	F

I.2.3 Or

Definition I.2.11 (disjunction)**.** Let P and Q be propositions. The disjunction of P and Q (write $P \vee Q$, pronounce "P or Q") is the proposition that is true as soon as P, or Q, is true, and false only when P and Q are both false.

Truth table of $P \vee Q$:

P	Q	$P \vee Q$
F	F	F
F	T	T
T	F	T
T	T	T

Caution!

- The mathematical "or" may not be used for enumerations. So "x is equal to 1 or 2" stands for "x is equal to 1 or x is equal to 2".
- The mathematical "or" is inclusive, i.e. it means "P or Q *or both*". In English, "or" is sometimes used to implicitely say "or. . . , *but not both*". (Eg. When you say "Will you come on Monday or on Tuesday?" you're not expecting "both" as an answer.)

  For us "or" will always have the meaning of "possibly both".

  When we want to specify "not both" we use "either. . . or. . . ". Yet we do not introduce a specific connective.

As an illustration of the truth tables method, check the following:

Properties I.2.12 (Hamlet's Principle)**.** *$P \vee \neg P$ is always true.*

For a mathematician, "to be or not to be" is a slam dunk: it is always true.

Exercise I.4

Example I.2.13 (Famous mathematical joke)**.** - *'Is it a boy or a girl?'* - *'Yes.'*

End of Lecture 1.

Lecture 2 (Equivalence of Compound Propositions. Implies)

I.2.4 Well-formed expressions and parentheses

With the three connectives met so far we can build compound sentences, for example $P \vee \neg Q$, etc. The expressions that make sense are sometimes called *well-formed*. It is not very interesting to define of this notion, as it is always obvious to determine whether a propositional form is well-formed or not.

Example I.2.14.

Expression	Well-formed?
$\neg$	N
$\neg\neg\neg P$	Y
$\neg P \vee Q$	Y
$\wedge Q$	N
$P \vee \wedge Q$	N

And what if we assemble compound propositions? One should then use parentheses. On the other hand, if we want to drop some of the parentheses, we shall need a convention, because the sense of $\neg P \vee Q$ is not clear at first sight: does one mean $(\neg P) \vee Q$ or $\neg(P \vee Q)$?

Convention I.2.15. The abbreviation rule :

Priority is given to $\vee$*, then to* $\wedge$*, then to* $\neg$*.*

Example I.2.16.

$\neg\neg\neg P$	stands for	$\neg(\neg(\neg(P)))$
$\neg P \vee Q$	stands for	$(\neg P) \vee Q$
$\neg P \vee Q \wedge R$	stands for	$(\neg P) \vee (Q \wedge R)$.

Remark I.2.17 (Analogy)**.** The meaning of $-1 + 2.3$ is $(-1) + (2.3)$. So you may think that it is just the same rule as for arithmetical operations, using the following analogies :

$\neg$	$-$
$\wedge$	$\cdot$
$\vee$	$+$

where $-$ stands for "opposite", not for subtraction. The analogy is no coincidence, and it can be a great help.

Remember that you are expected to drop extra parentheses in front of a negation (hence "$(\neg P) \vee Q$" should be written "$\neg P \vee Q$"), but we won't really care about having many parentheses to make things clear between $\vee$'s and $\wedge$'s. It is easier for everyone, and parentheses are so cheap anyway. So here is the golden rule:

Better too many parentheses than relying on these conventions.

I.2.5 Equivalence of propositional forms

It is obvious that $P \vee Q$ and $Q \vee P$ convey the same meaning, though they are two distinct compound propositions. (In a similar vein, following the analogy of remark I.2.17, "$1 + 2$" and "$2 + 1$" yield the same result, but are different expressions.) We introduce a notion of "having the same meaning".

Definition I.2.18 (equivalence)**.** Two propositional forms are said to be equivalent if they have the same truth table.

We noticed earlier that P and $\neg\neg P$ are equivalent (Remark I.2.4)!

Example I.2.19.

$$\begin{array}{lll} \neg(\neg P \wedge Q) & \text{is equivalent to} & P \vee (\neg Q) \\ (P \vee Q) \wedge R & \text{is equivalent to} & R \wedge (Q \vee P) \end{array}$$

It is clear from a simple computation of truth tables!

The following phenomenon is analogous (recall Remark I.2.17) to the well-known algebraic identities $x + (y + z) = (x + y) + z$ and $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

Properties I.2.20 (Associativity of $\vee$ and $\wedge$)**.**

$$\begin{array}{lll} P \vee (Q \vee R) & \textit{is equivalent to} & (P \vee Q) \vee R. \\ P \wedge (Q \wedge R) & \textit{is equivalent to} & (P \wedge Q) \wedge R. \end{array}$$

The following correspond to the identities $x + y = y + x$ and $x \cdot y = y \cdot x$.

Properties I.2.21 (Commutativity of $\vee$ and $\wedge$)**.**

$$\begin{array}{lll} Q \vee P & \textit{is equivalent to} & P \vee Q. \\ Q \wedge P & \textit{is equivalent to} & P \wedge Q. \end{array}$$

The next properties are a little more puzzling.

Properties I.2.22 (Distributivity of $\vee$ and $\wedge$)**.**

$$\begin{array}{lll} P \wedge (Q \vee R) & \textit{is equivalent to} & (P \wedge Q) \vee (P \wedge R). \\ P \vee (Q \wedge R) & \textit{is equivalent to} & (P \vee Q) \wedge (P \vee R). \end{array}$$

Let us follow the analogy (Remark I.2.17) again. The first statement is analogous to $2 \cdot (3+5) = (2 \cdot 3) + (2 + \cdot 5)$. But the second one has no counterpart with numbers since in the reals $2 + (3 \cdot 5) \neq (2 + 3) \cdot (2 + 5)$. This is good news. It means than *propositional calculus is even easier than arithmetic*!

The following properties are essential when computing negations.

Properties I.2.23 (De Morgan's laws)**.**

$$\begin{array}{lll} \neg(P \wedge Q) & \textit{is equivalent to} & \neg P \vee \neg Q. \\ \neg(P \vee Q) & \textit{is equivalent to} & \neg P \wedge \neg Q. \end{array}$$

Remember that:

> *"The negation of a conjunction is the disjunction of negations."*
> *"The negation of a disjunction is the conjunction of negations."*

Example I.2.24.

- In case you did not understand, check the following. The negation of "beautiful and useful" is *not* "ugly and useless". It is "ugly *or* useless".
- "No stopping or standing" *should* be written "No (stopping or standing)" according to Convention I.2.15. If it were, its meaning would become clear: "No stopping and no standing".

Exercise I.14

I.2.6 Implies

The fourth connective is generally misunderstood. You should devote some extra attention to it.

Definition I.2.25 (implication)**.** Let P and Q be propositions. The implication $P \Rightarrow Q$ (pronounce "P implies Q") is the proposition that is true if: whenever P holds, then so does Q.

Caution! No backwards arrows. "$\Leftarrow$" is *forbidden*.

Before the remarks, we write the table. Learn it immediately!

Truth table of $P \Rightarrow Q$:

P	Q	$P \Rightarrow Q$
F	F	T
F	T	T
T	F	F
T	T	T

You might be surprised by the two first lines. But the fact is that the
Ex I.5-I.7 definition says nothing about the cases in which P does not hold.

Example I.2.26 (Indiana Jones' principle)**.** When the nazi butler says to Indy "If you are a Scottish lord, then I am Mickey Mouse!", he is *right* (see the movie for details).

Remark I.2.27. The logic *material implication* has nothing to do with causality, or what philosophers would call *indicative implication*. Ours (purely abstract) does not deal with "relevant" causes and consequences!

Thus "$P \Rightarrow Q$" does not mean "P has Q as an arguable consequence". It is only about P never holding without Q. In particular:

False implies anything.
Anything implies True.

Practice a lot before you get used to it.

Example I.2.28.

- "If hens have teeth, then I am Santa Claus" is *true*.
- "If hens have teeth, then $1 + 1 = 2$" is *true*.
- "If $1 + 1 = 2$, then I am Santa Claus" is *false*.
- "If $1 + 1 = 2$, then $0 = 0$" is *true*.

Remark I.2.29 (Alternate Expressions)**.**

"If P, then Q", "P is a sufficient condition for Q to hold",
"Q is a necessary condition for P to hold" - all mean "P implies Q".

Caution! Two common mistakes:

- "$P \Rightarrow Q$ may *not* be read "P, hence Q". Can you make the difference between "If hens have teeth, then I am Santa Claus" and "Hens have teeth, hence I am Santa Claus"?
- "$P \Rightarrow Q$ may not be read "P then Q" either: this hardly is English. Remember: *If you want to use 'then', then you must use 'if'.*

Now, using truth tables, we show how the connectives relate to each other: Exercise I.9

Properties I.2.30 ("Don't move or I shot!"). *$P \Rightarrow Q$ is equivalent to $\neg P \vee Q$.*

Remark I.2.31. "Don't move or I shot!" means "*If* you move, *then* I shot!".

As an application of this equivalence we can compute the negation of an implication, using De Morgan's law:

> Since $P \Rightarrow Q$ is equivalent to $\neg P \vee Q$, one gets that $\neg(P \Rightarrow Q)$ is equivalent to $\neg(\neg P \vee Q)$, which is equivalent to $P \wedge \neg Q$. Hence:

Properties I.2.32. *$\neg(P \Rightarrow Q)$ is equivalent to $P \wedge \neg Q$.*

Remark I.2.33. Perhaps we should comment on that property. An implication is a general statement like "whenever P is true, also Q is true" - the typical shape of a theorem. What is the negation of this? it amounts to *refuting* the theorem. And how do you do this? just provide a *counter-example*, that is something that satisfies P, but not Q. So we have another way to understand that $\neg(P \Rightarrow Q)$ is equivalent to $P \wedge \neg Q$. Exercise I.14, I.20

We define two notions related to implication.

Definition I.2.34 (converse)**.** The converse of an implication $P \Rightarrow Q$ is the proposition $Q \Rightarrow P$.

Of course the converse doesn't have the same truth table as the original implication, hence it is not equivalent to it.

Definition I.2.35 (contrapositive)**.** The contrapositive of an implication $P \Rightarrow Q$ is the proposition $\neg Q \Rightarrow \neg P$.

Now using truth tables (check!), we see that

Properties I.2.36. *An implication is equivalent to its contrapositive, i.e.*

$$P \Rightarrow Q \text{ is equivalent to } \neg Q \Rightarrow \neg P.$$

The latter property will be extremely important. Exercise I.19, I.21, I.22

End of Lecture 2.

Lecture 3 (If and only if. Check-up on connectives.)

I.2.7 If and only if

This is perhaps more of an abbreviation than a connective.

Definition I.2.37 (equivalence)**.** Let P and Q be propositions. The equivalence $P \Leftrightarrow Q$ (pronounce "P is equivalent to Q") is the proposition that is true if P and Q have same truth value, and false otherwise.

Truth table of $P \Leftrightarrow Q$:

P	Q	$P \Leftrightarrow Q$
F	F	T
F	T	F
T	F	F
T	T	T

Exercises I.8, I.15

Remark I.2.38. You may think there is something wrong - we have defined equivalence twice (Definitions I.2.18 and I.2.37)! This is not exactly the case. The first time (Definition I.2.18), we did not define equivalence as a connective (this we just did, in Definition I.2.37). So the first definition was about a notion, and the second about a symbol. To reassure those who find it is a schizophrenic way to proceed :

$$\left.\begin{array}{c}P \text{ and } Q \text{ are equivalent}\\ \text{(as propositions)}\end{array}\right\} \quad \text{if and only if} \quad \left\{\begin{array}{c}(P \Leftrightarrow Q) \text{ is true}\\ \text{(as a proposition)}\end{array}\right.$$

So our definitions are perfectly consistent, and even rational!

Nonetheless, the *symbol* "$\Leftrightarrow$" is used only as a connective. When you are asked to prove that two propositions P and Q are equivalent, you may be trying to prove that the *new* proposition $P \Leftrightarrow Q$ is true - it is not literally the same question, but it is... an equivalent question.

You may note that we have used "if and only if" as a notion in Remark I.2.38, and now we're using it as a connective. So we are still being schizophrenic, but "*Though this be madness, yet there is method in 't.*"

And of course, as the notation itself suggests -

Remark I.2.39. The compound proposition "P is equivalent to Q" is, as a proposition, equivalent to the proposition "P implies Q and Q implies P". In a nutshell,

$$\text{"}P \Leftrightarrow Q\text{"} \qquad \text{if and only if} \qquad \text{"}(P \Rightarrow Q) \wedge (Q \Rightarrow P)\text{"}.$$

Caution! No backwards arrows. "$\Leftarrow$" is *forbidden.*

Remark I.2.40 (Alternate Expressions)**.**

"P is a necessary and sufficient condition for Q to hold",
"Q is a necessary and sufficient condition for P to hold",
"P if and only if Q"
- all mean "P is equivalent to Q".

Exercises I.10, I.11

I.2.8 Check-up

Before moving to quantifiers, make sure you master the following:

$\neg\neg P$	is equivalent to	P	involutivity of $\neg$
$P \wedge (Q \wedge R)$	" "	$(P \wedge Q) \wedge R$	associativity of $\wedge$
$P \vee (Q \vee R)$	" "	$(P \vee Q) \vee R$	associativity of $\vee$
$P \wedge Q$	" "	$Q \wedge P$	commutativity of $\wedge$
$P \vee Q$	" "	$Q \vee P$	commutativity of $\vee$
$(P \vee Q) \wedge R$	" "	$(P \wedge R) \vee (Q \wedge R)$	distributivity
$(P \wedge Q) \vee R$	" "	$(P \vee R) \wedge (Q \vee R)$	distributivity
$\neg(P \wedge Q)$	" "	$\neg P \vee \neg Q$	De Morgan's Law
$\neg(P \vee Q)$	" "	$\neg P \wedge \neg Q$	De Morgan's Law
$P \Rightarrow Q$	" "	$\neg P \vee Q$	
$\neg(P \Rightarrow Q)$	" "	$P \wedge \neg Q$	

Check that you know how to use them when P and Q are compound.

What will exercises be about?

- Analyse English sentences and be able to write them in symbolic form. E.g. "If you like apples, you must like pears and dislike bananas".
- Simplify forms, e.g. "simplify $(P \wedge Q) \vee (Q \wedge P) \vee (P \Rightarrow Q)$".
- Compute negations, e.g. "what is the negation of $(P \vee Q) \Rightarrow (R \wedge S)$"?
- Mixing these questions, a typical exercise is: write the negation of "If you like apples, you must like pears and dislike bananas".

The aim of this type of exercises is to provide a readable form. For example, $\neg\left[(P \vee Q) \Rightarrow (R \wedge S)\right]$ is *not* a relevant answer to the third question; provide something like $(P \vee Q) \wedge (\neg R \vee \neg S)$.

Exercises I.3 through I.22

End of Lecture 3.

Lecture 4 (Introduction to Quantifiers. $\forall$. $\exists$)

I.3 Quantifiers

Quantifying a proposition P is building another proposition that says how many "things" satisfy P.

For example you certainly have already noticed that as soon as x is a real number, then x^2 is non-negative. So we might be willing to say "for any real number x, one has $x^2 \geq 0$".

On the other hand, if you consider the real equation "$x^5 + x - 2 = 0$", you may want to say that it has a real solution (it is the case that such a solution exists; if you don't see why, don't panic). Then you say: "there is a real number x that satisfies the equation $x^5 + x - 2 = 0$".

It turns out that for common mathematical purposes, the two phrases "all things satisfy P" and "there exists (at least one) a thing satisfying P" suffice.

I.3.0 Prerequisites

From now on we shall mostly deal with examples borrowed from mathematics, i.e. talk about real numbers (for instance) instead of kangaroos. In order to do this we need some very common notations. We will use throughout the following symbols:

- The "$\in$" symbol, introduced by Peano, denotes membership. It is no longer (though it originally was) the Greek letter epsilon "ε", so make the difference obvious when writing. Hence if you have two mathematical objects x and A, "$x \in A$" is to be read "x is in A", or "x is an element of A", or "x belongs to A". On the other hand, you *may not* use expressions like "A contains x" or "x is included in A".

- $\mathbb{N}$ denotes the set of all natural numbers, that is $\mathbb{N} = \{1, 2, 3, \dots\}$. So "$x \in \mathbb{N}$" should be spelt: "$x$ is in N", or "x is a natural number", or "x is a positive integer".

- $\mathbb{R}$ denotes the set of all real numbers, that is the numbers on the line. So "$x \in \mathbb{R}$" should be spelt: "x is in R", or "x is a real number".

It is interesting to quantify a sentence P only if P actually *depends on something*. Take for example "$x > 0$"; as long as we don't know who's x, it makes no precise sense. We call such a sentence a *proposition depending on a variable* (here x), that is a sentence that becomes a proposition as soon as we assign a meaning to its variables.

Example I.3.1.

- "$x + y = y + x$" is a proposition in the variables x and y.

- "$x + y$" is not a proposition in any variables: even if we assign values to x and y, it still doesn't state anything.

If a proposition depending on x, say $P(x)$, becomes a true proposition when we assign to x a certain value, say a, we say that *a satisfies P*.

Example I.3.2.

- 2 satisfies "n is even".

- 0 as x and 1 as y satisfy "$x + y = y + x$".

I.3.1 For all

Definition I.3.3 (universal quantification)**.** Let A be a set and $P(x)$ be a proposition depending on an variable x. The universally quantified proposition $\forall x \in A, P(x)$ (pronounce "for any x in A, $P(x)$") is the proposition that is true if it the case that for any x in A, $P(x)$ holds.

The upside-down letter $\forall$ is called the *universal quantifier*.

Remark I.3.4. The comma "," after the quantification "$\forall x \in A$" is here for clarity, and entirely optional.

Example I.3.5.

- "$\forall x \in \mathbb{R}, x^2 \geq 0$" ("for any x in R, x-square is greater than or equal to 0") is the proposition stating that the square of any real number is non-negative. (It is true.)
- "$\forall x \in \mathbb{R}, x = 1$" ("for any x in R, x equals 1") is the proposition stating that all real numbers are equal to 1. (It is false.)

Remark I.3.6. In some books the set A does not appear. It is pedagogically speaking not a very good idea, because so far x is just a "thing", and we could too easily forget what we are talking about. This is why it looks wiser to relativise (or *bound*), the quantifier to the set A.

For instance, the absolute sentence "$\exists x, x + x = 1$", which is true if we relativise it to the real numbers, is false among integers! this is a good reason to dislike absolute sentences, and use only relative, or bounded, quantifiers.

Remark I.3.7 (Alternate Expressions)**.**

"for all x in A", "for any element x of A", "for all x belonging to A"
- are possible ways to read "$\forall x \in A$"

An important special case is when dealing with common sets like $\mathbb{N}$ or $\mathbb{R}$:

"for any x in N" etc., "for all positive integer x", "for any natural number x"
- are possible ways to read "$\forall x \in \mathbb{N}$"

Example I.3.8. Read the following aloud:

- $\forall k \in \mathbb{N},\ k > k + 1 \Rightarrow k = 0$.
- $\forall y \in \mathbb{R},\ y > 0 \Leftrightarrow 2 \cdot y > y$.

Which are true?

We know that for any two real numbers x and y, one has $x + y = y + x$. This is written: "$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y = y + x$", and may be read:

> "For any real number x, for any real number y, x plus y is equal to y plus x."

As it sounds a bit long, if you feel confident, you may read:

"For any real numbers x and y, x plus y equals y plus x".

Similarly, "$\forall x \in \mathbb{R}, \forall n \in \mathbb{N}, \dots$" may be read:

"for any real number x and any positive integer $n\dots$"

Caution! The enumerative "and" *may not* be written as a connective, i.e.

Exercise I.23 "$\forall x \wedge y$" is *absolutely forbidden.*

I.3.2 There exists

Definition I.3.9 (existential quantification)**.** Let A be a set and $P(x)$ be a proposition depending on an variable x. The existentially quantified proposition $\exists x \in A, P(x)$ (pronounce "there exists x in A *such that* $P(x)$") is the proposition that is true if it the case that there is some x in A such that $P(x)$ holds.

The reversed letter $\exists$ is called the existential quantifier.

Caution! Don't forget to say "such that" - if you don't, your sentence is not English.

Remark I.3.10. This is why you might like to put commas. When you find a comma after $\forall$, don't pronounce it. But when the comma lies after a $\exists$, it reads "such that".

Example I.3.11.

- "$\exists x \in \mathbb{R}, x^2 = 2$" ("there exists x in R *such that* x-square is equal to 2") is the proposition stating that 2 has a real square-root. (It is true.)
- "$\exists k \in \mathbb{N}\ 2 \cdot k = 3$" ("there exists k in N *such that* 2 times k is equal to 3") is the proposition stating that 2 divides 3. (It is false.)

Remark I.3.12 (Alternate Expressions)**.**

"there exists an x in A *such that*", "there exists an element x of A *such that*", "there is an x in A *such that*", "there is some x belonging to A *such that*" - are possible ways to read "$\exists x \in A$".

And of course, when dealing with known sets:

"There exists a positive integer k *such that*", etc.

Example I.3.13. Read the following aloud:

- $\exists k \in \mathbb{N}, 2 \cdot k = 5$.
- $\exists y \in \mathbb{R}, y > 0 \wedge y < 1$.

Exercise I.24 Which are true?

There is a short way to read nested ∃-quantifiers.

Example I.3.14. If we want to express that some given (say, positive) real number x is bounded between two integers, we write:

$$\exists k \in \mathbb{N}, \exists \ell \in \mathbb{N}, k < x < \ell$$

which reads

> "there exists a natural number k such that there exists a natural number ℓ such that k is smaller than x that is smaller than ℓ".

This doesn't sound so good. A more natural way to read it would be:

> "there exist a natural number k and a natural number ℓ such that..."

or even:

> "there exist natural numbers k and ℓ such that ..."

Caution! Anyone who uses "$\wedge$" to denote the enumerative "and" will be shot.

Caution! Sometimes renaming is necessary. Read the following example.

Example I.3.15 (renaming is important)**.** Let us write in symbols:

> "there exists a natural number smaller than x, and there exists a natural number bigger than x"?

If we translate the first half of the sentence, we write:

$$\exists k \in \mathbb{N}, k < x.$$

If now we translate the second half, we write:

$$\exists k \in \mathbb{N}, x < k.$$

And combining, we get a jam. Our x is supposed to be the same in the two propositions, so this is no problem. But we have this k now playing two different roles. Of course calling all your children Jessie would lead to confusions. So it is reasonable to change one name. Hence we write

$$(\exists k \in \mathbb{N}, k < x) \wedge (\exists \ell \in \mathbb{N}, x < \ell)$$

and everything is clear again. Exercise I.25

Notation I.3.16 (A liberty with notation)**.** An important set in mathematics is the set $\mathbb{R}_+^*$ of all positive real numbers. As it is sometimes boring to write $x \in \mathbb{R}_+^*$, we adopt the following convention:

"$\forall x > 0$"	stands for	"$\forall x \in \mathbb{R}_+^*$",
"$\exists x > 0$"	stands for	"$\exists x \in \mathbb{R}_+^*$".

Example I.3.17. "$\forall \varepsilon > 0, \exists \delta > 0, \delta < \varepsilon$" reads "for any positive real number epsilon, there exists a positive real number delta smaller than epsilon", or shorter: "for any positive epsilon, there exists a positive delta which is smaller".

End of Lecture 4.

Lecture 5 (∃!. Interactions and negations.)

I.3.3 A useful abbreviation

Before we get to serious things here is a useful abbreviation, which is not strictly speaking a quantifier.

Notation I.3.18. Let A be a set and $P(x)$ be a proposition depending on an variable x. Then $\exists! x \in A, P(x)$ (pronounce "there exists one and only one x in A *such that* $P(x)$") stands for:

$$\exists x \in A, (P(x) \wedge \forall y \in A, P(y) \Rightarrow x = y)\,.$$

This formula means that there is an x in A that satisfies P, of course, *but also that any other y in A satisfying P has to be equal to x*... hence that x *is the only element of A satisfying P.*

Remark I.3.19 (Alternate Expressions)**.**

"there is exactly one x in A *such that*", "there is a unique x in A *such that*" - are other possible ways to read "$\exists! x \in A$".

Example I.3.20. Read aloud:

- $\forall x \in \mathbb{R}, \exists! y \in \mathbb{R}, x = y$.
- $\exists! n \in \mathbb{N}, \neg(\exists k \in \mathbb{N}, n = k + 1)$.

Which are true?

Caution! Remember how mathematicians say "unique": "if there are two, they are the same". Dedicate some time to understanding what $\exists!$ stands for. Exercises I.30, I.31

I.3.4 How quantifiers interact

We show that it is possible to interchange to consecutive $\forall$'s, and that it is possible to interchange two consecutive $\exists$'s.

Caution! Never interchange an $\forall$ with an $\exists$.

Properties I.3.21. *Let A, B be sets and $P(x, y)$ be a proposition depending on two variables. Then*

(i). *"$\forall x \in A, \forall y \in B, P(x, y)$" is equivalent to "$\forall y \in B, \forall x \in A, P(x, y)$".*

(ii). *"$\exists x \in A, \exists y \in B, P(x, y)$" is equivalent to "$\exists y \in B, \exists x \in A, P(x, y)$".*

Proof. This is a brief incursion into Chapter II. We do nothing unreasonable; not understanding now would not mean being hopeless, though it might announce future difficulties.

Before we start - quantifiers operate with "general" elements, say x. When we want to *fix* a specific one, it is very customary to use subscript notation x_0.

(i). Suppose that $\forall x \in A, \forall y \in B, P(x,y)$ holds. We wish to see that $\forall y \in B, \forall x \in A, P(x,y)$ holds too. By definition, we want to see that for any $y_0 \in B$, the proposition $\forall x \in A, P(x, y_0)$ holds. By definition, this amounts to seeing that for any $x_0 \in A$, $P(x_0, y_0)$ holds.

So we fix $y_0 \in B$ and we fix $x_0 \in A$. Since $\forall x \in A, \forall y \in B, P(x,y)$ holds, we know that for our particular $x_0 \in A$, $\forall y \in B, P(x_0, y)$ holds. Therefore for our particular $y_0 \in B$, $P(x_0, y_0)$ holds. Since we picked any $x_0 \in A$, this means that $\forall x \in A, P(x, y_0)$ holds. Since we picked any $y_0 \in B$, this means that $\forall y \in B, \forall x \in A, P(x,y)$ holds.

We have thus showed that if $\forall x \in A, \forall y \in B, P(x,y)$ holds, then $\forall y \in B, \forall x \in A, P(x,y)$ holds too. The converse implication is similar.

(ii). More intuitively: if "$\exists x \in A, \exists y \in B, P(x,y)$" holds, it means that there are an element $x \in A$ and an element $y \in B$ such that $P(x,y)$ holds. But a choice of x and a choice of y is like a choice of y and a choice of x, so we also have $\exists y \in B, \exists x \in A, P(x,y)$.

So if $\exists x \in A, \exists y \in B, P(x,y)$ holds, then $\exists y \in B, \exists x \in A, P(x,y)$ holds too. The converse implication is of course similar.

So consecutive "quantification blocks" *of the same nature* may be freely exchanged. *It is not the case with different quantifiers.*

Caution! Never interchange an $\forall$ with an $\exists$.

Counter-example I.3.22. Read aloud:

- $\exists x \in \mathbb{R}, \forall n \in \mathbb{N}, n = x^2$.
- $\forall n \in \mathbb{N}, \exists x \in \mathbb{R}, n = x^2$.

Which is true? Which is false?

Example I.3.23. The proposition "$\forall x > 0, \exists k \in \mathbb{N}, \exists \ell \in \mathbb{N}, k < x < \ell$" is equivalent to "$\forall x > 0, \exists \ell \in \mathbb{N}, \exists k \in \mathbb{N}, k < x < \ell$". But $\forall$ *must come first.*

Caution! "$\exists!$" is *not* a quantifier, but an abbreviation! There are no rules; always go back to the definition!

Counter-example I.3.24.

- Consider the proposition: "$\exists! x \in \mathbb{R}, \exists! y \in \mathbb{R}, x = y^2$".

  When $x_0 \in \mathbb{R}$ is fixed, the proposition "$\exists! y \in \mathbb{R}, x_0 = y^2$" states that x_0 has a unique square root. There is exactly one real number which has a unique square root (namely 0), so the proposition is *true*.

- We now revert $\exists!$, getting the proposition "$\exists! y \in \mathbb{R}, \exists! x \in \mathbb{R}, x = y^2$".

  When $y_0 \in \mathbb{R}$ is fixed, the proposition "$\exists! x \in \mathbb{R}, x = y_0^2$" means that y_0 has a unique square. This is certainly true of any $y_0 \in \mathbb{R}$, and this is many! So the proposition is *false*.

I.3.5 Computing negations

Let A be a set and $P(x)$ a proposition depending on x. Suppose that there is no $x \in A$ such that $P(x)$ holds ("$\neg\exists x \in A, P(x)$"). Now pick any $x \in A$. Can $P(x)$ hold? No, by assumption. Hence $\neg P(x)$ holds. As we picked any x in A, the following holds: "$\forall x \in A, \neg P(x)$".

Properties I.3.25. *Let A be a set and $P(x)$ a proposition depending on x. Then:*

- $\neg(\forall x \in A, P(x))$ *is equivalent to* $\exists x \in A, \neg P(x)$.
- $\neg(\exists x \in A, P(x))$ *is equivalent to* $\forall x \in A, \neg P(x)$.

Caution! $\not\forall$ and $\nexists$ are absolutely forbidden.

Example I.3.26. As an application, we compute the negation of the following proposition:

$$P : \text{“}\forall x \in \mathbb{R}, \exists n \in \mathbb{N}, \forall y \in \mathbb{R}, |y| > n \Rightarrow |y| > |x|\text{”}$$

P is successively equivalent to:

$$\begin{array}{cccc}
\underbrace{\neg\forall x \in \mathbb{R},}_{\text{turns into a } \exists\neg} & \exists n \in \mathbb{N}, & \forall y \in \mathbb{R}, & |y| > n \Rightarrow |y| > |x|, \\
\exists x \in \mathbb{R}, & \underbrace{\neg\exists n \in \mathbb{N},}_{\text{turns into a } \forall\neg} & \forall y \in \mathbb{R}, & |y| > n \Rightarrow |y| > |x|, \\
\exists x \in \mathbb{R}, & \forall n \in \mathbb{N}, & \underbrace{\neg\forall y \in \mathbb{R},}_{\text{turns into a } \exists\neg} & |y| > n \Rightarrow |y| > |x|, \\
\exists x \in \mathbb{R}, & \forall n \in \mathbb{N}, & \exists y \in \mathbb{R}, & \neg(|y| > n \Rightarrow |y| > |x|), \\
\exists x \in \mathbb{R}, & \forall n \in \mathbb{N}, & \exists y \in \mathbb{R}, & |y| > n \wedge \neg(|y| > |x|), \\
\exists x \in \mathbb{R}, & \forall n \in \mathbb{N}, & \exists y \in \mathbb{R}, & |x| \geq |y| > n.
\end{array}$$

Exercise I.29

Caution! It is a common mistake to believe that the negation of "$\exists x > 0, P(x)$" is "$\forall x \leq 0, \neg P(x)$"; but it is *not*. Remember that "$\exists x > 0$" actually stands for "$\exists x \in \mathbb{R}_+^*$". Hence the negation of "$\exists x > 0, P(x)$" is "$\forall x > 0, \neg P(x)$".

Exercise I.26

I.4 Remarks and Exercises

- Words that were used (check that you understand their meaning).
  - proposition (Definition I.1.3)
  - connective: negation (Definition I.2.1) , conjunction (I.2.5), disjunction (I.2.11), implication (I.2.25), equivalence (I.2.37)
  - converse (Definition I.2.34), contrapositive (Definition I.2.35)

  - equivalence of two propositions (Definition I.2.18)
  - quantification: universal (Definition I.3.3), existential (I.3.9)

- The statement of the Pythagorean Theorem is

  Theorem. *For any right triangle, the square of the hypotenuse is the sum of the squares of the two other sides.*

  So far we did not discuss truth seriously, but in any case you should believe this is a clean mathematical statement, i.e. a proposition. So mathematics are perhaps not about equations.

- Truth tables are useless. We teach them for two purposes:
  - They make students feel confident, in spite of Math 300's horrible reputation that could discourage you.
  - They help us convince you that sentences like "If hens have teeth, then I am Santa Claus" are *true*. You wouldn't believe it otherwise.

  If you now feel comfortable with implications and negations, you may forget about truth tables.

End of Lecture 5.

Lecture 6 (Exercises)

End of Lecture 6.

Exercises on Chapter I.

1 Basic exercises (no quantifiers)

1.1 Propositions

(S) **Exercise I.1.** Which of the following are propositions?

1. Hello!
2. How are you?
3. I am fine.
4. Paul (SSN 142-19-6471) is fine.
5. This number is positive.
6. -1 is positive.
7. There are no free lunches.
8. When it rains, π is a circle.

Exercise I.2. Determine if the following are propositions. When they are, try to find their truth values.

1. We all live in a yellow submarine.
2. $1^2 = 1$.
3. $\sin^2 x + \cos^2 x = \tan^2 x$.
4. $\forall n \in \mathbb{N}, n \in \mathbb{R}$.
5. $\forall x \wedge y \in \mathbb{R}, x + y = y + x$.
6. Every triangle is a square.
7. There are only two real numbers the square of which equal themselves.

1.2 Truth tables

Exercise I.3. Enumerate entries of a truth table using four variables.

Let P, Q, R denote propositions.

(S) **Exercise I.4.** Write truth tables for the following:

1. $(P \wedge \neg Q) \wedge \neg R$
2. $(\neg P \vee Q) \wedge (\neg Q \vee R)$

Exercise I.5. Write truth tables for the following:

1. $P \Rightarrow \neg Q$
2. $\neg P \Rightarrow Q$
3. $\neg P \Rightarrow \neg Q$

(S) **Exercise I.6.** Compute the truth tables of the following:

1. $(P \vee Q) \Rightarrow (P \wedge Q)$
2. $(\neg P \wedge Q) \Rightarrow (Q \wedge R)$
3. $P \Rightarrow (Q \Rightarrow R)$
4. $P \Leftrightarrow (Q \Leftrightarrow R)$

Exercise I.7. Write the truth tables of the following :

1. $(P \wedge Q) \vee (P \vee Q)$
2. $(P \wedge Q) \wedge (P \vee Q)$
3. $(P \wedge Q) \Rightarrow R$
4. $(P \Rightarrow Q) \vee R$

(S) **Exercise I.8.** Find a form whose truth table is:

P	Q	?
F	F	F
F	T	T
T	F	T
T	T	F

1.3 Translations

(S) **Exercise I.9.** Write the following sentences as compound propositional forms, using symbolic connectives (and parentheses):

1. "I think therefore I am."
2. "If it rains and I am home, then I play the piano or listen to the radio."
3. "Paul was neither silly nor stupid, but George was a fool and so was Ringo."
4. "Whenever I do not see kangaroos around, I turn off the light; if in addition there is no party around, I sleep pacefully."
5. "I take the subway because I don't have a car."
6. "Either you come or I go and get you."

Exercise I.10. Same exercise: convert the following English sentences into their symbolic form (you may introduce notations; you need not explain it).

1. "My watch is on time although I did not set it."
2. "When she is asleep my cat dreams or purrs."
3. "My new car is red but I don't know how to drive."
4. "I am bored since everytime I go to the movies, I am bored."
5. "You're allowed to drive only if you have a license."
6. "I want salt and pepper but no sauce."
7. "Your being here is no explaination for such a mess."
8. "Mike turns off the light exactly when he wants to sleep."

Exercise I.11. Same exercise.

1. "P does not imply Q."
2. "It is not the case that P does not imply Q."
3. "P is a sufficient condition for Q to imply R."
4. "When P holds, Q cannot imply R."
5. "P is a necessary and sufficient condition for P to be false."
6. "It is not the case that the following occurs: the negation of P together with the negation of Q imply the negation of the following assertion: R is not true."

(S) **Exercise I.12.** Make up English sentences whose translations into symbols would be the following:

1. $P \wedge (Q \Rightarrow \neg P)$
2. $(P \vee Q) \wedge (Q \Leftrightarrow R)$

Exercise I.13. Write ten propositional forms and find an example for each, in the fashion of Exercise I.12.

1.4 Negations

(S) **Exercise I.14.** Compute and simplify the negations of the following propositions.

1. $(P \wedge Q) \vee (P \vee Q)$
2. $(P \wedge Q) \wedge (P \vee Q)$
3. $(P \wedge Q) \vee (R \wedge S)$
4. $(P \vee \neg Q) \wedge (\neg R \vee S)$

(S) **Exercise I.15.** Write the negations of the following propositional forms:

1. $(P \wedge Q) \Rightarrow R$
2. $(P \Rightarrow Q) \vee R$
3. $P \Rightarrow (Q \Leftrightarrow R)$.

For the last one, you *may not* use arrows, only $\neg$, $\vee$, and $\wedge$.

Exercise I.16. Compute the negations of:

1. $(\neg P \Leftrightarrow Q) \Rightarrow R$
2. $(P \Rightarrow Q) \wedge (P \vee Q)$
3. $(P \Leftrightarrow Q) \Leftrightarrow (R \Leftrightarrow S)$
4. $(P \Rightarrow Q) \Rightarrow (Q \Rightarrow R)$

(S) **Exercise I.17.** What are the negations of:

1. "When it rains or snow, I avoid kangaroos and read Lewis Carroll."
2. "Tarski shaves Gödel if and only if Gödel shaves Tarski."

Exercise I.18. Compute without writing intermediate steps the negations of:

1. $(\neg P \Leftrightarrow Q) \Rightarrow R$
2. $(P \Rightarrow Q) \wedge (P \vee Q)$
3. $(P \Leftrightarrow Q) \Leftrightarrow (R \Leftrightarrow S)$.

1.5 Miscallenea manipulations

(S) **Exercise I.19.** Provide the negation, converse, and contrapositive of the following:

1. $P \Rightarrow (Q \Rightarrow R)$
2. $(P \Rightarrow Q) \Rightarrow R$
3. $(P \Rightarrow Q) \Rightarrow (R \Rightarrow S)$.

(S) **Exercise I.20.** Rewrite the propositions below using only $\neg$, $\wedge$, $\vee$, and the following convention:

> *express the forms as disjunctions of smaller terms*
> (which use only conjunctions and negations).

1. $P \Rightarrow (Q \Rightarrow R)$
2. $(P \Rightarrow Q) \Rightarrow R$
3. $(P \Rightarrow Q) \Rightarrow (R \Rightarrow S)$
4. $P \wedge \neg(Q \Rightarrow R)$
5. $(P \Rightarrow Q) \wedge \neg R$
6. $(P \Rightarrow Q) \wedge \neg(R \Rightarrow S)$
7. $(Q \Rightarrow R) \Rightarrow P$
8. $R \Rightarrow (P \Rightarrow Q)$
9. $(R \Rightarrow S) \Rightarrow (P \Rightarrow Q)$
10. $\neg(Q \Rightarrow R) \Rightarrow \neg P$
11. $\neg R \Rightarrow \neg(P \Rightarrow Q)$
12. $\neg(R \Rightarrow S) \Rightarrow \neg(P \Rightarrow Q)$

For example, $P \Rightarrow (Q \Rightarrow R)$ becomes $\neg P \vee \neg Q \vee R$,
$(P \Rightarrow Q) \Rightarrow R$ becomes $(P \wedge \neg Q) \vee R$,
$(P \Rightarrow Q) \Rightarrow (R \Rightarrow S)$ becomes $(P \wedge \neg Q) \vee \neg R \vee S$.

Exercise I.21. Let P, Q, R, S be propositions. Consider the proposition:

$$A = [(P \vee Q) \Rightarrow (R \wedge \neg S)]$$

1. State and simplify the negation of A.
2. State and simplify the converse of A.
3. State and simplify the contrapositive of A.

(S) **Exercise I.22.** Prove *without using truth tables* that the following propositional forms are equivalent:

1. $(P \vee Q) \Rightarrow \neg R$ and $R \Rightarrow (\neg P \wedge \neg Q)$.
2. $\neg[P \vee \neg(Q \Rightarrow R)]$ and $(\neg P \wedge \neg Q) \vee (\neg P \wedge R)$

2 Exercises involving quantifiers

2.1 Easy translations

Exercise I.23. Write the following in English:

1. $\forall k \in \mathbb{N}, \forall \ell \in \mathbb{N}, \forall x \in \mathbb{R}, x = k + \ell$.
2. $\forall k \in \mathbb{N}, \forall z \in \mathbb{R}, |z| \geq n + 1 \Rightarrow |z| > n$.
3. $\forall x \in \mathbb{R}, \neg (\forall k \in \mathbb{N}, |x| > k)$.

Which are true?

(S) **Exercise I.24.** Write the following in English:

1. $\forall x \in \mathbb{R}, \exists n \in \mathbb{N}, \forall y \in \mathbb{R}, |y| > n \Rightarrow |y| > |x|$.
2. $\exists n \in \mathbb{N}, \forall k \in \mathbb{N}, \exists \ell \in \mathbb{N}, k = n \cdot \ell$.

3. $\exists n \in \mathbb{Z}, \forall x \in \mathbb{R}, |x| < n \Rightarrow \exists y \in \mathbb{R}, 0 = 1$.

Find an integer n making the second statement true. Same for the third.

(S) **Exercise I.25.** Write in symbols the following sentences:

1. There exists an even integer and there exists an odd integer.
2. For any real number, there is an integer bigger than it.
3. There is a real number that doesn't have a real square root.

(By the way do you know how to *prove* these propositions?)

(S) **Exercise I.26.** Let $(u_n)_{n\in\mathbb{N}}$ be a sequence of real numbers. The sequence *converges to* $\ell \in \mathbb{R}$ if:

$$\forall \epsilon > 0,\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geq n_0 \Rightarrow |u_n - \ell| < \epsilon.$$

1. Translate the expression into English.
2. Give the negation of the expression.
3. Translate the negation into English.

Exercise I.27. A sequence of real numbers $(a_n)_{n\in\mathbb{N}}$ is a *Cauchy sequence* if

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall m, n \geq N, |a_m - a_n| < \varepsilon.$$

1. Translate the definition of "Cauchy sequence" into English.
2. Negate the definition of "Cauchy sequence".
3. Translate the negation into English.

Remark. The notation is quick-and-dirty for:

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall (m, n) \in \mathbb{N}^2, (m \geq N \wedge n \geq N) \Rightarrow |a_m - a_n| < \varepsilon.$$

You may use it or not.

(S) **Exercise I.28.** Let $(u_n)_{n\in\mathbb{N}}$ be a sequence of real numbers. A real number $\ell \in \mathbb{R}$ is *adherent to* to the sequence if:

$$\forall \varepsilon > 0, \forall n_0 \in \mathbb{N}, \exists n \geq n_0, |u_n - \ell| < \varepsilon.$$

Take the negation of the property, then translate the negation into English.

Remark. The notation is quick-and-dirty for : $\exists n \in \mathbb{N}, n \geq n_0 \wedge |u_n - \ell| < \varepsilon$.

2.2 Abstract translations

(S) **Exercise I.29.** Let A be a set and P a proposition depending on a variable. Write the negation of $\exists! x \in A, P(x)$.

(S) **Exercise I.30.** Let A be a set and P a proposition depending on a variable. Write the following in symbols:

There are exactly *two* elements of A that satisfy P.

Exercise I.31. Let A be a set and P a proposition depending on a variable. Write the following in symbols:

There are exactly *three* elements of A that satisfy P.

2.3 Around functions

Exercise I.32. Let $f : \mathbb{R} \to \mathbb{R}$ be a real function. f *has limit* $+\infty$ *at* $+\infty$ if:

$$\forall M \in \mathbb{R},\ \exists A \in R,\ \forall x \in \mathbb{R},\ x > A \Rightarrow f(x) > M.$$

1. Translate this definition into English.
2. Take the negation of the translation.
3. Translate the negation into symbols.

(S) **Exercise I.33.** A real function $f : \mathbb{R} \to \mathbb{R}$ *has limit* ℓ *at* a if:

$$\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x \in \mathbb{R},\ |x - a| < \delta \Rightarrow |f(x) - \ell| < \varepsilon.$$

Write in symbols the following sentences:

1. f has a limit at a.
2. f has a limit everywhere (i.e., at every point of $\mathbb{R}$).

(S) **Exercise I.34.**

- A function $f : \mathbb{R} \to \mathbb{R}$ is *continuous at* $a \in \mathbb{R}$ if:

$$\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x \in \mathbb{R},\ |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

- A function is *continuous on* $\mathbb{R}$ if it is continuous at every $a \in \mathbb{R}$.
- A real function f is *uniformly continuous on* $\mathbb{R}$ if:

$$\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x \in \mathbb{R},\ \forall y \in \mathbb{R},\ |y - x| < \delta \Rightarrow |f(y) - f(x)| < \varepsilon.$$

1. Translate into English “continuity at a” and “uniform continuity on $\mathbb{R}$”.
2. Write a symbolic definition of “continuity on $\mathbb{R}$”.

3. Give negations for all three formulas (continuity at a, on $\mathbb{R}$, uniform continuity on $\mathbb{R}$).

4. Translate these negations into English.

(S) **Exercise I.35.**

- Recall from Exercise I.33 that when g is a real function, and a and ℓ are real numbers, one says that g has limit ℓ at a if:

$$\forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |g(x) - \ell| < \varepsilon.$$

- The *difference quotient* of a real function f at a point $a \in \mathbb{R}$ is the expression, defined for $x \in \mathbb{R} \setminus \{a\}$:

$$\tau_{f,a}(x) := \frac{f(x) - f(a)}{x - a}.$$

1. The function f is *differentiable at a* if this quotient has a limit at a. Write this in symbols, then translate what you have written into English.

2. f is *differentiable on* $\mathbb{R}$ if it is differentiable at every $a \in \mathbb{R}$. Write in symbols: f is differentiable on $\mathbb{R}$. Then translate into English.

3. Also write: f is not differentiable on $\mathbb{R}$. Then translate.

(S) **Exercise I.36.** Let f be a function from $\mathbb{R}$ to $\mathbb{R}$ ($f : \mathbb{R} \to \mathbb{R}$). Write the following properties in symbols, and give translations in English.

1. f is a constant function.
2. f is not a constant function.
3. f is increasing.
4. f is not increasing.
5. f is increasing or decreasing.
6. f is bounded above.

Chapter II

Proofs (and refutations)

. . . cujus rei demonstrationem mirabilem sane detexi.
Hanc marginis exiguitas non caperet.

We master a new language. Though our vocabulary is still poor, we know how to construct sentences, with no limit on their complexity. So we know how to *state* propositions. We now turn to learning how to *prove* them.

Caution! Symbolic language is *only for statements*. Proofs are arguments that establish such statements and must be written only *in English*.

Main goals: Write mathematical proofs:

- Understand how to prove easy propositions.
- Be able to write a proper induction proof.

Notions. Proof, Contradiction proof, Induction proof

LECTURE 7 (BASIC PROOFS)

Caution! Symbolic language is *only for statements*. Proofs are arguments that establish such statements and must be written only *in English*.

II.1 Basic Proofs

Modern mathematics focus on proofs, the only criterion of mathematical truth a contemporaneous mathematician will tolerate. A formal definition would not help here, and you will learn through practice. Let us just say that a proof is an argumentation *carried in English* that convinces even picky graders.

Example II.1.1.

> "Let me prove that the sum, for all divisors d of n, of the number of integers smaller than and coprime to d is n.
>
> Consider the fractions $\frac{1}{n}, \ldots, \frac{n}{n}$ and write them in irreducible form. Then any divisor d of n appears as a quotient exactly as many times as there are integers smaller than d and coprime to it (non-divisors of n cannot appear). Since there are n fractions, we get that the sum over d dividing n of the number of integers smaller than and coprime to d is n."

This is a high-class proof, and understanding it is not our purpose. Notice however that it uses no symbolic connectives. On the other hand, it makes intensive use of words like "since", 'as", "because", "hence", "therefore". Let us insist that symbolic language is only for statements; proofs must be written in English.

The proof of Example II.1.1 may be remembered as a reference, but not as a model. On the one hand, we shall be dealing with simpler arguments (conceptuality has nothing to do with length!), and on the other hand, it has been extremely purified. You should write "clumsier" proofs at first.

A *refutation* of a proposition P is just a proof of $\neg P$.

Remark II.1.2. Of course if you are told in an exercise either to prove P, or to refute P, it is easy and it makes no difference to you, since you will possibly deal with $\neg P$ instead of P. But if you don't know *which* of P and $\neg P$ is true, then you don't know *which* to prove and things get harder - because a proof of P and a proof of $\neg P$ do not start similarly!

We shall sketch a couple of techniques to prove propositions. Notice that the techniques you will use depend on the shape of what you have to prove.

Caution! Those are guidelines, not recipes. Proving something interesting always involves intuition. Commenting on the shape of the proposition you want to prove is not as useful as *deeply understanding its meaning.* For the exercises, the formal approach may be enough at first, but you should also *train your intuition.*

II.1.1 How to prove $P \wedge Q$

Proof of P ∧ Q:

- Prove P.
- Prove Q.
- Conclude that you have proved $P \wedge Q$.

II.1.2 How to prove $P \Rightarrow Q$

Direct proof of P ⇒ Q:

- Assume P.
- Prove Q.
- Conclude that $P \Rightarrow Q$.

Caution! Don't forget the conclusion. In general, it is a reasonable thing to 1)state what you will prove, 2)prove it, and then 3)tell that you have proved it. It is elephant-like, but no one can argue with that.

Example II.1.3. Let x be a real number. Prove that

$$\sin x = 1 \Rightarrow \cos x = 0.$$

> "Assume that $\sin x = 1$. Then since $\sin^2 x + \cos^2 x = 1$, we find that $1 + \cos^2 x = 1$, hence $\cos^2 x = 0$, and thus $\cos x = 0$. Therefore we have proved that $\sin x = 1 \Rightarrow \cos x = 0$. QED"

Remark II.1.4. QED stands for the Latin words (cf. "Delenda Est Carthago"):

$$\underbrace{\text{Quod}}_{\text{What}}\ \underbrace{\text{Erat}}_{\text{Was}}\ \underbrace{\text{Demonstrandum}}_{\text{To be proved}}.$$

In a proof you may freely use:

- Propositions that are always true (for example, because of truth tables).
- Your *current* assumptions.
- Things you have already proved *under the same assumptions.*
- Well-known results (eg. above, the fact that $\sin^2 x + \cos^2 x = 1$)

Remember that $P \Rightarrow Q$ is equivalent to its contrapositive $\neg Q \Rightarrow \neg P$ (Properties I.2.36). Sometimes this implication is actually easier to prove.

Contraposition Proof of P ⇒ Q:

- Assume $\neg Q$.
- Prove $\neg P$.
- Conclude that $\neg Q \Rightarrow \neg P$, and hence that $P \Rightarrow Q$.

Example II.1.5. Let x be a real number. Prove that

$$\cos x \neq 0 \Rightarrow \sin x \neq 1.$$

"Assume that $\sin x = 1$. Then since $\sin^2 x + \cos^2 x = 1$, we find that $1 + \cos^2 x = 1$, hence $\cos^2 x = 0$, and thus $\cos x = 0$. Therefore we have proved that $\sin x = 1 \Rightarrow \cos x = 0$, which is the contrapositive of $\cos x \neq 0 \Rightarrow \sin x \neq 1$. QED"

II.1.3 How to prove $P \Leftrightarrow Q$

Remember that "P is equivalent to Q" means "P implies Q and Q implies P", so it is easy to imagine what to do.

Proof of P $\Leftrightarrow$ Q:

- Prove $P \Rightarrow Q$.
- Prove $Q \Rightarrow P$.
- Conclude that $P \Leftrightarrow Q$.

Caution! Recall that the backwards arrow "$\Leftarrow$" is forbidden.

Example II.1.6. Let x be a real number. Prove that

$$\cos x = 0 \;\Leftrightarrow\; \sin x = \pm 1.$$

"Assume first that $\cos x = 0$. Then since $\sin^2 x + \cos^2 x = 1$, we find that $0 + \sin^2 x = 1$, hence $\sin^2 x = 1$, and thus $\sin x = \pm 1$. Therefore we have proved that $\cos x = 0 \;\Rightarrow\; \sin x = \pm 1$.

Now assume that $\sin x = \pm 1$. Then since $\sin^2 x + \cos^2 x = 1$, we find that $\cos^2 x + 1 = 1$, hence $\cos^2 x = 0$, and thus $\cos x = 0$. Therefore we have proved that $\sin x = \pm 1 \;\Rightarrow\; \cos x = 0$.

As a conclusion , we have proved that $\cos x = 0 \;\Leftrightarrow\; \sin x = \pm 1$ QED"

Remark II.1.7. In Example II.1.6, between the two parts we have "cleared assumptions". This is expressed implicitly by "*Now* assume...". Exercise II.1

End of Lecture 7.

Lecture 8 (Case Division. Proof of $\vee$. Contradiction Proofs)

II.1.4 Case division

Inelegant proofs, when you feel you have to deal with different cases.

Example II.1.8. Let n be an integer. Let us prove that $\frac{n(n+1)}{2}$ is an integer.

"There are two cases. [Here, we begin a "case division".]

- If n is even, then $\frac{n+1}{2}$ is an integer, and so is $\frac{n(n+1)}{2}$.

- If n is odd, then $n+1$ is even, and in that case $\frac{n+1}{2}$ is an integer, whence $\frac{n(n+1)}{2}$ is an integer too.

[We have successfully argued in each case; it remains to conclude.] In either case, $\frac{n(n+1)}{2}$ is an integer. QED"

Caution! Always make sure that your different cases cover all possibilities! (They *may* overlap, but they *must* cover all cases.)

II.1.5 How to prove $P \vee Q$

Proving a disjunction is trickier. At first sight it seems that you need to prove P or to prove Q, but which should you try? And if you think that you can prove P, then you have something stronger (since $P \Rightarrow P \vee Q$ but the converse does not necessarily hold).

But since $A \Rightarrow B$ is equivalent to $\neg A \vee B$ (Properties I.2.30), we may interpret $P \vee Q$ as $\neg P \Rightarrow Q$.

Proof of P $\vee$ Q:

- Assume $\neg P$.
- Prove Q.
- Conclude that $\neg P \Rightarrow Q$, and hence that $P \vee Q$.

Since $P \vee Q$ is equivalent to $Q \vee P$, we also have the symmetric method.

Another proof of P $\vee$ Q:

- Assume $\neg Q$.
- Prove P.
- Conclude that $\neg Q \Rightarrow P$, and hence that $P \vee Q$.

Example II.1.9. Let m, n be integers. Prove that if mn is even then m or n is even.

"We assume that mn is even, and we prove that m or n is even.

To do that, we assume that m is *not* even, that is m is odd.

Since mn is even, 2 divides mn, hence 2 divides m or n. As m is odd, 2 does not divide it, so 2 divides n. Hence n is even.

Assuming that m is not even we have proved that n is. This can also be expressed as (m is even) $\vee$ (n is even).

So assuming that mn is even, we have proved that m or n is even. QED"

II.1.6 Proof by contradiction

A proof by contradiction of P relies on the underlying principle that if $\neg P$ is false, then P is true. So we assume $\neg P$ (what we want to *refute*!), and prove that it implies something absurd, impossible. We then conclude that $\neg P$ can't hold, and hence that P (what we want to prove) holds.

It runs as follows:

Contradiction Proof of P:

- Assume $\neg P$.
- Prove a contradiction.
- Conclude that since you have reached a contradiction, $\neg P$ can't hold, and therefore P does hold.

What is a suitable "contradiction"?

Acceptable Contradictions: A contradiction is reached with:

- A proposition that is always false (for example, because of truth tables).
- The negation of one of your *current* assumptions.
- The negation of something you have already proved *under the "absurd" assumptions.*
- Something not compatible with well-known results.

Example II.1.10. Let us prove that $\sqrt{2}$ is not a rational number.

> "We assume that $\sqrt{2}$ is rational, and prove a contradiction.
>
> If $\sqrt{2}$ is rational, then it can be written $\sqrt{2} = \frac{a}{b}$, where a and b are coprime integers.
>
> Raising to the square and multiplying, we find $a^2 = 2b^2$. In particular, 2 divides a^2. But this implies that 2 divides a. Hence 4 divides $a^2 = 2b^2$, and therefore 2 divides b^2. Now this implies that 2 divides b. So we have found that 2 divides both a and b, which can't be coprime. This is a contradiction to the definition of a and b.
>
> Hence $\sqrt{2}$ is not a rational number. QED"

Exercises II.2, II.3

This example had an amazing historical importance and must be learnt.

END OF LECTURE 8.

LECTURE 9 (PROOFS INVOLVING QUANTIFIERS)

II.2 Proofs Involving Quantifiers

II.2.1 How to prove $\forall x \in A, P(x)$

Recall that "$\forall x \in A, P(x)$" stands for "for all/any x in A, $P(x)$ holds". If we want to prove such a statement we need to actually prove $P(x)$ for any x in A. This is done by taking x arbitrary, with no extra assumptions.

Caution! When proving $\forall x \in A, P(x)$, taking an example is not allowed!

Direct proof of $\forall \mathbf{x} \in \mathbf{A}, \mathbf{P}(\mathbf{x})$:

- Take any x in A.

  (This is expressed by the ritual formula "Let $x \in A$.")

- Prove that $P(x)$ holds, without assuming anything special on x.

- Conclude that for any x in A, $P(x)$ holds.

This *must* be written:

"**Let $\mathbf{x} \in \mathbf{A}$.**" [Prove $P(x)$] "**Hence, $\mathbf{P}(\mathbf{x})$ holds. Since this is true for any $\mathbf{x} \in \mathbf{A}$, we have proved $\forall \mathbf{x} \in \mathbf{A}, \mathbf{P}(\mathbf{x})$.**"

Example II.2.1. Let us show that $\forall n \in \mathbb{N}, (n \text{ is odd } \Rightarrow n+1 \text{ is even})$.

"**Let n** $\in \mathbb{N}$. [We want to show: "n odd $\Rightarrow n+1$ even".]

Suppose that n is odd. Then $n+1$ is clearly even.

Therefore "n odd $\Rightarrow n+1$ even."

As this is true for any n $\in \mathbb{N}$**, we have proved:**

$\forall \mathbf{n} \in \mathbb{N}$, (**n is odd** $\Rightarrow \mathbf{n+1}$ **is even**). QED"

Remark II.2.2. In the proof of Example II.2.1, "Let $n \in \mathbb{N}$" actually means "I have no idea which n I am talking about, but I will pretend I do". On the other hand, since this is supposed to be a "general" (universal) proof, we don't assume anything special about n (that is, we *may not* take examples).

II.2.2 How to prove $\exists x \in A, P(x)$

Caution!

- Unlike universal proofs (that is, proofs of propositions which have the form $\forall x \in A, P(x)$), these "existential proofs" might rely on intuition. You need to find an example, and this requires deep understanding of the problem.

- Attention, "let" will be used in a very different sense from the "general" let of Remark II.2.2.

Direct proof of $\exists \mathbf{x} \in \mathbf{A}, \mathbf{P}(\mathbf{x})$:

- [you must think, interpret, and guess which x will do]
- Define the x you think will satisfy P

  (This is expressed by the ritual formula "Let x be" [its definition]).
- Prove that *for this special* x, $P(x)$ holds (use its properties!)
- Conclude that there exists an x in A such that $P(x)$ holds.

This *must* be written:

"**Let x be**"[define x]. [If it is not obvious that x is in A, you must prove it.] [Prove $P(x)$]. "**Hence, $\mathbf{P}(\mathbf{x})$ holds. We have proved $\exists \mathbf{x} \in \mathbf{A}, \mathbf{P}(\mathbf{x})$.**"

Example II.2.3. Let us prove that $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x \neq y^2$.

[Oh... I have to think before I start writing. What does this mean? I am looking for a real number x such that for any real number y, y squared is not x. In other words, I am looking for a real number that does not have a real square root. Now my intuition suggests me that -1 will do. I briefly check that it works, and then start writing the proof:]

> "**Let $\mathbf{x} = -1$.** Let $y \in \mathbb{R}$. Since $y^2 \geq 0$, we have that $y^2 \neq -1$. As this is true for any $y \in \mathbb{R}$, we have $\forall y \in \mathbb{R}, y^2 \neq -1$. **Hence $\mathbf{x} = -1$ meets our requirements, and we have proved $\exists \mathbf{x} \in \mathbb{R}, \forall \mathbf{y} \in \mathbb{R}, \mathbf{x} \neq \mathbf{y}^2$** QED"

Caution! In the proof of Example II.2.3, "Let $x = -1$" means "I define x to be -1." This is *very different* from "Let $y \in \mathbb{R}$" which, like in the proof at the end of §II.2.1, means "I take any, but I don't choose it".

Remark II.2.4. In English, "let" has two very different meanings:

- The "general" let, as in "let n be an integer". This is used in proofs of $\forall$-statements.
- The "particular" let, as in "let $n = 2$". This one is used in definitions, and in proofs of $\exists$-statements.

Exercises II.4-II.7

Remark II.2.5. As you remember from Properties I.3.25, the negation of a proposition starting with a $\forall$ starts with a $\exists$, and vice-versa. This is why when you don't know whether you must prove or refute something, it is not the same approach.

End of Lecture 9.

Lecture 10 (Proofs and Quantifiers, continued)

II.2.3 A Serious Example

Example II.2.6. A real function $f : \mathbb{R} \to \mathbb{R}$ is said continuous if

$$\forall a \in \mathbb{R}, \forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

Let c, d be real numbers. Let $f(x) = cx + d$. We show that f is continuous.

Proof. Since this is just an example, we proceed with no intuition at all, merely analysing the structure of the sentence we are proving. Here is a useful hint: if $c = 0$, we shall take $\delta = 1$. If $\delta \neq 0$, we shall take $\delta = \frac{\varepsilon}{|c|}$ (the latter value does depend on ε). Case division will help. Ready?

- We want to prove:

$$\forall a \in \mathbb{R}, \forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

- Let $a \in \mathbb{R}$ [“general” let]. We want to prove:

$$\forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

- Let $\varepsilon > 0$ [“general” let]. We want to prove:

$$\exists \delta > 0, \forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

- If $c = 0$, let $\delta = 1$ [“particular” let]. If $c \neq 0$, let $\delta = \frac{\varepsilon}{|c|}$ [“particular” let]. We want to check that this value of δ meets our requirements, in other words we want to prove:

$$\forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

- Let $x \in \mathbb{R}$ [“general” let]. We want to prove:

$$|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

- So we assume that $|x - a| < \delta$, and we will prove that $|f(x) - f(a)| < \varepsilon$.
- There are two cases: [begin case division]
  - If $c = 0$, then $|f(x) - f(a)| = |0x + d - (0a + d)| = 0 < \varepsilon$.
  - Now if $c \neq 0$, then $|f(x) - f(a)| = |cx + d - (ca + d)| = |c \cdot (x - a)|$, so $|f(x) - f(a)| = |c| \cdot |x - a| < |c| \cdot \delta = \varepsilon$.

  [end of case division]. In either case $|f(x) - f(a)| < \varepsilon$.
- Hence we have proved that

$$|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

- Since this is true for any $x \in \mathbb{R}$, we have proved that

$$\forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

- Hence δ meets our requirements, and we conclude that

$$\exists \delta > 0, \forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

- As this is true regardless of ε [*Attention: "regardless" means that it is true for all ε, though the value we assigned to δ depends on ε*], we have proved

$$\forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

- Now this is true for any real number a, and therefore

$$\forall a \in \mathbb{R}, \forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon \quad \text{QED}$$

Don't forget: state what you want to prove, prove it, and eventually claim that you have proved it. It is extremely clumsy but no one can argue with that.

II.2.4 Contradiction and quantifiers

It is sometimes useful to apply the "Contradiction Proof" technique to universal statements. The following relies on the fact that the negation of $\forall x \in A, P(x)$ is $\exists x \in A, \neg P(x)$ (Properties I.3.25). So if you assume the negation, you get *for free* an x to find a contradiction with.

Proof by contradiction of $\forall \mathbf{x} \in \mathbf{A}, \mathbf{P}(\mathbf{x})$:

- Assume that there is x in A that *does not* satisfy P.

  (This is expressed by: "Let $x \in A$ such that $P(x)$ does not hold.")

- Prove a contradiction.

- Conclude that since this is impossible, $\forall x \in A, P(x)$ holds.

This *must* be written:

"**Let $\mathbf{x} \in \mathbf{A}$ such that $\neg\mathbf{P}(\mathbf{x})$.**" [Prove a contradiction.] "**Hence $\neg\mathbf{P}(\mathbf{x})$ leads to a contradiction. So $\mathbf{P}(\mathbf{x})$ holds. As this is true for any $\mathbf{x} \in \mathbf{A}$, we have proved $\forall \mathbf{x} \in \mathbf{A}, \mathbf{P}(\mathbf{x})$.**"

Remark II.2.7. This is an abstract proof, because you do not have the slightest idea of who is the x you assume you have (a good reason for that impossibility is that you are actually trying to prove that such an x cannot exist).

There is a "dual" technique with existential quantifiers.

Proof by contradiction of $\exists \mathbf{x} \in \mathbf{A}, \mathbf{P}(\mathbf{x})$:

- Assume that for all x in A, x *does not* satisfy P.
- Prove a contradiction.
- Conclude that since this is impossible, $\exists x \in A, P(x)$ holds.

Remark II.2.8. So this is an existence proof of x which yields no suitable x! It is called a *non-constructive* proof.

Exercises II.9 through II.13

END OF LECTURE 10.

LECTURE 11 (EXERCISES)

END OF LECTURE 11.

LECTURE 12 (ME1)

END OF LECTURE 12.

LECTURE 13 (INDUCTION PROOFS)

II.3 Proof by induction

"Mathematical induction" has nothing to do with the common meaning of induction. It relies on the following result.

Theorem II.3.1 (Induction Principle)**.** *Let $P(n)$ be a proposition depending on an integer n. Suppose*

- $P(1)$
- $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$

Then $\forall n \in \mathbb{N}, P(n)$ holds.

II.3.1 Prerequisite - a piece of notation

Though it has nothing to do with proofs, we introduce an extremely useful notation. Since many exercises on induction will involve sums, we introduce a convenient symbol. If you already know how to "spell" integrals, sums are even easier.

When a and b are integers and $u(k)$ is a function of the integer k, we let

$$\sum_{k=a}^{b} u(k)$$

(pronounce "the *sum* for k ranging from a to b of $u(k)$") be - the sum for k ranging from a to b of $u(k)$, that is

$$\sum_{k=a}^{b} u(k) = u(a) + u(a+1) + \cdots + u(b).$$

The purpose of this notation is to get rid of the somehow fuzzy dots. Σ (Capital sigma, Greek letter S) stands for "sum" when dealing with concrete sums, like $\int$ stands for "sum" when dealing with integrals.

Example II.3.2.

- $\sum_{k=1}^{n} 0 = 0$
- $\sum_{k=1}^{n} 1 = n$
- $\sum_{k=1}^{n} (-1)^k = \begin{cases} 0 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd.} \end{cases}$

If you don't understand the latter we shall prove it by induction.

II.3.2 Induction

Consider a property $P(n)$ depending on an integer n, and suppose that you need to prove $\forall n \in \mathbb{N},\ P(n)$. In certain cases, there is an easier way to do that than just taking any n, and proving $P(n)$ (which would be the "direct proof"). Induction is an extremely efficient technique if you have the feeling that proving $P(n)$ is easier if already established for smaller values than n.

Caution! n has to be a positive integer!

Proof by induction of $\forall \mathbf{n} \in \mathbb{N}, \mathbf{P(n)}$:

- Basic step/Initialization: [almost nothing to do!]
  Prove that $P(1)$ holds.
- Inductive step/Heredity: [in general not too hard!]
  Prove "$\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$", in other words:
  Let $n \in \mathbb{N}$. Assume $P(n)$, and prove $P(n+1)$.
  ($P(n)$ is sometimes called the *inductive hypothesis*.)
- Conclude. This is done with the ritual words:

  "**We have proved $\mathbf{P(1)}$ and $\forall \mathbf{n} \in \mathbb{N},\ \mathbf{P(n) \Rightarrow P(n+1)}$. By induction, we have proved $\forall \mathbf{n} \in \mathbb{N},\ \mathbf{P(n)}$.**"

Remark II.3.3. Induction is extremely easy for two reasons:

- All you do is remember the model of the proof, and fill up the form.
- The answer is given in the exercise, you don't have to invent a formula.

Example II.3.4. We prove by induction that

$$\sum_{k=1}^{n}(-1)^k = \begin{cases} 0 & \text{if} \quad n \text{ is even} \\ -1 & \text{if} \quad n \text{ is odd.} \end{cases}$$

[First call the property $P(n)$, it will save paper:]

"For any integer n, let $P(n)$ be the property:

$$\sum_{k=1}^{n}(-1)^k = \begin{cases} 0 & \text{if} \quad n \text{ is even} \\ -1 & \text{if} \quad n \text{ is odd.} \end{cases}$$

We prove by induction: $\forall n \in \mathbb{N}, P(n)$.

- **Basic step/Initialization:**
  We prove that $P(1)$ holds. Indeed, when $n = 1$, n is odd and

  $$\sum_{k=1}^{1}(-1)^k = -1$$

  so $P(1)$ is true.
- **Inductive step/Heredity:**
  We now prove the inductive step. Let $n \in \mathbb{N}$. We assume $P(n)$, and we prove $P(n+1)$.
  For this we do case division.
  - If n is even, then our inductive hypothesis $P(n)$ means that $\sum_{k=1}^{n}(-1)^k = 0$. In particular, $n+1$ is odd and

    $$\sum_{k=1}^{n+1}(-1)^k = \left(\sum_{k=1}^{n}(-1)^k\right) + (-1)^{n+1} = 0 - 1 = -1$$

    so $P(n+1)$ is true.
  - If n is odd, then our inductive hypothesis $P(n)$ means that $\sum_{k=1}^{n}(-1)^k = -1$. In particular, $n+1$ is even and

    $$\sum_{k=1}^{n+1}(-1)^k = \left(\sum_{k=1}^{n}(-1)^k\right) + (-1)^{n+1} = -1 + 1 = 0,$$

    so $P(n+1)$ is true again.

  This concludes the case division. So we have $P(n) \Rightarrow P(n+1)$, and since this is true for any n, we have thus proved:

  $$\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1).$$

  This concludes the heredity step.

- **Conclusion:**
  We have thus proved $\mathbf{P(1)}$ and $\forall \mathbf{n} \in \mathbb{N}, \mathbf{P(n)} \Rightarrow \mathbf{P(n+1)}$.
  By induction, we have proved $\forall \mathbf{n} \in \mathbb{N},\ \mathbf{P(n)}$. QED"

Caution! Two common mistakes:

- Do not forget to define the proposition $P(n)$.
- $P(n)$ is a proposition, which may hold or not. *It is not a number.*

Example II.3.5.

For any integer n, let $P(n)$ be the property:

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

We prove by induction: $\forall n \in \mathbb{N}, P(n)$.

- Basic step/Initialization:
  We prove $P(1)$. Indeed, when $n = 1$,

$$\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}$$

  so $P(1)$ is true.
- Inductive step/Heredity:
  We now prove the inductive step. Let $n \in \mathbb{N}$. We assume $P(n)$, and prove $P(n+1)$. We have

$$\sum_{k=1}^{n+1} k = \left(\sum_{k=1}^{n} k\right) + (n+1) = \frac{n(n+1)}{2} + (n+1)$$

  because of the inductive hypothesis $P(n)$, and therefore

$$\sum_{k=1}^{n+1} k = (n+1)\left(\frac{n}{2} + 1\right) = (n+1)\frac{n+2}{2} = \frac{(n+1)((n+1)+1)}{2}$$

  Hence $P(n+1)$ is true.
  So we have proved that $P(n) \Rightarrow P(n+1)$, and since this is true for any n, we have thus proved

$$\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1).$$

  This concludes the heredity step.
- Conclusion: We proved $P(1)$ and $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$.
  By induction, we have proved $\forall n \in \mathbb{N},\ P(n)$. QED

Exercise II.14

Remark II.3.6. To recover form the essential clumsiness of the latter proof, let us give an elegant one.

Write

$$\begin{array}{rcccccc} S & = & 1 & + & \dots & + & n \\ & = & n & + & \dots & + & 1 \end{array}$$

and hence

$$2S = (n+1) + \cdots + (n+1) = n(n+1).$$

II.3.3 Variant: Induction not starting from 1

Notation II.3.7. "$\forall n \geq 2,\ P(n)$" (pronounce "for all n bigger than or equal to 2, P of n") stands for "$\forall n \in \mathbb{N},\ n \geq 2 \Rightarrow P(n)$".

Remark II.3.8. It is not obvious that n should be a natural integer, since the set $\mathbb{N}$ is not actually present in the notation. This is because habit dictates that n denotes a natural number.

Notation II.3.9. "$\exists n \geq 2, P(n)$" (pronounce "there is an n greater than or equal to n such that P of n") stands for "$\exists n \in \mathbb{N}, n \geq 2 \wedge P(n)$". Exercise II.11

Similarly, "$\forall x > -\pi, P(x)$" (pronounce "for all x bigger than negative π, P of x") stands for "$\forall x \in \mathbb{R}, x > -\pi \Rightarrow P(x)$". "$\exists x > -\pi, P(x)$" (pronounce "there is an x greater than $-\pi$ such that P of x") stands for "$\exists x \in \mathbb{R}, x > -\pi \wedge P(x)$".

Last but not least, "let $x > -\pi$" means "let $x \in \mathbb{R}$ be greater than π".

Caution! Though it is not explicit, we will understand (by convention, or by habit) that n denotes anatural number, that x is a real number, etc.

The following exemple shows how it is possible to do induction from a value bigger than 1. Notice it is all the same except that everything starts from 4 instead of 1, and that we make use of the notations just defined.

Example II.3.10. We prove that $\forall n \geq 4, n^2 - 3n \geq 4$.

"We do induction on $n \geq 4$. For a natural number $n \geq 4$, let $P(n)$ be the property: $n^2 - 3n \geq 4$.

- First step [Notice that our first step is now $n = 4$.]:
  Since $4^2 - 3.4 = 16 - 12 = 4 \geq 4$, $P(4)$ holds.
- Heredity/Inductive step [We show $\forall n \geq 4, P(n) \Rightarrow P(n+1)$]:
  Let $n \geq 4$. We assume $P(n)$, and we prove $P(n+1)$.
  We have

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

  [Since we know, by our inductive hypothesis, something about $n^2 - 3n$, it is not a good idea to collect terms. Instead:]

We write

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

Now the first term is bigger than or equal to 4 by our inductive hypothesis $P(n)$, and the second one is non-negative because $n \geq 4 \geq 1$.

Hence we get

$$(n+1)^2 - 3(n+1) = \underbrace{(n^2 - 3n)}_{\geq 4} + \underbrace{(2n-2)}_{\geq 0} \geq 4 + 0 \geq 4,$$

and $P(n+1)$ is proved.

Assuming $P(n)$, we proved $P(n+1)$, so $P(n) \Rightarrow P(n+1)$ holds. As this is true for any $n \geq 4$, we have $\forall n \geq 4, P(n) \Rightarrow P(n+1)$.

- Conclusion:

  We have therefore proved $P(4)$ and $\forall n \geq 4, P(n) \Rightarrow P(n+1)$.

Exercise II.16 By induction, we have proved $\forall n \geq 4, P(n)$. QED "

Remark II.3.11. Here is another proof of Example II.3.10. Induction proofs are always a bit clumsy, so a direct proof is likely to be more elegant.

> "We have to prove $\forall n \geq 4, n^2 - 3n \geq 4$, in other words, we prove $\forall n \geq 4, n^2 - 3n - 4 \geq 0$.
>
> The resolution of the equation $X^2 - 3X - 4 = 0$ will certainly help. Its discriminant is $3^2 + 4 \cdot 4 = 25$, hence there are two (real) solutions, namely $\frac{3 \pm 5}{2}$, that is -1 and 4. Now if we draw the function $f(x) = x^2 - 3x - 4$, it is a parabola whose concavity is oriented upwards. This means that *outside* of the interval defined by the solutions of $f(x) = 0$, f takes non-negative values.
>
> In particular, $\forall x \in \mathbb{R}, x \geq 4 \Rightarrow f(x) \geq 0$. This remains true when we restrict to integers, so $\forall n \in \mathbb{N}, n \geq 4 \Rightarrow n^2 - 3n - 4 \geq 0$. QED"

End of Lecture 13.

Lecture 14 (Complete induction and proof of PMI.)

II.3.4 Complete Induction

Complete induction seems at first stronger than induction. It is actually as strong (because the two principles are equivalent).

Theorem II.3.12 (Complete Induction Principle)**.** *Let $P(n)$ be a proposition depending on an integer n. Suppose*

- $P(1)$

- $\forall n \in \mathbb{N}, [(\forall k \leq n,\ P(k)) \Rightarrow P(n+1)]$

Then $\forall n \in \mathbb{N}, P(n)$ *holds.*

Remark II.3.13. Notice - induction requires a property which:

- starts to be true at some point (often 1, but not always; Example II.3.10);
- if true at some step, is also true at the next step ("heredity").

So you may think of induction as "propagation of truth from point to point".

On the other hand, complete induction requires a property that:

- starts to be true at some point;
- if true on some *interval* of natural numbers, is also true at the point right after the interval.

So complete induction works like "adding a point of truth after a full interval".

As an application of complete induction, let us prove the following:

Proposition II.3.14. *Every natural number greater than* 1 *has a prime factor.*

Remark II.3.15. It is clear that "classical" induction can't help here, because classical induction relates $n+1$ to n. But in general, if you have a prime factor of n, you are sure that it is *not* a prime factor of $n+1$ So it is obvious that a proof by induction would fail.

> "We prove Proposition II.3.14. For any natural number n greater than 1, let $P(n)$ be the property:
>
> $$n \text{ has a prime factor}$$
>
> We prove $\forall n \geq 2, P(n)$ by complete induction on $n \geq 2$.
>
> - First step [Here, of course, the first step is 2]:
>   Since 2 divides 2 and is a prime number, 2 is a prime factor of 2. Hence $P(2)$ holds.
> - Inductive step:
>   Let $n \in \mathbb{N}$ be greater than 1. We assume $\forall k \geq 2, k \leq n \Rightarrow P(k)$, and prove $P(n+1)$.
>   [begin case division]
>   - If no natural number between 1 and $n+1$ divides $n+1$, then $n+1$ is a prime number. Since $n+1$ divides $n+1$, $n+1$ is a prime factor of $n+1$, hence $P(n+1)$ holds.

– Now if some natural number, say k, between 1 and $n+1$ divides $n+1$, we may apply our induction hypothesis to k. (This argument would *not* work with "classical" induction.) In particular there is a prime factor, say p, of k. Now p is a prime number and it divides k which divides $n+1$, so p is a prime factor of $n+1$. Thus $n+1$ has a prime factor, and $P(n+1)$ holds again.

In both cases $P(n+1)$ holds. This concludes the case division. [end case division]
Assuming $\forall k \geq 2, k \leq n \Rightarrow P(k)$ we have proved $P(n+1)$. Since this is true for any $n \geq 2$, we have actually proved

$$\forall n \in \mathbb{N}, [(\forall k \geq 2, k \leq n \Rightarrow P(k)) \Rightarrow P(n+1)].$$

- Conclusion:
  Hence $P(2)$ and $\forall n \in \mathbb{N}, [(\forall k \geq 2, k \leq n \Rightarrow P(k)) \Rightarrow P(n+1)]$ hold. By complete induction, we have proved $\forall n \in \mathbb{N}, P(n)$. QED"

Appendix 1: proof of the complete induction principle

Chapter II is at an end, and we will now prove our first theorem. Notice that it is not a theorem on numbers (like the examples we gave in order to understand how to write proofs), but a theorem on *propositions about numbers*. So this is already high-class mathematics.

We prove the Complete Induction Principle using the Induction Principle.

Proof. Let $P(n)$ be a proposition depending on an integer n such that $P(1)$ and $\forall n \in \mathbb{N}, [(\forall k \leq n,\ P(k)) \Rightarrow P(n+1)]$ are true. We show $\forall n \in \mathbb{N}, P(n)$.

[Who likes such an hypothesis? all I know is the "classical" induction principle, the rest is beyond my understanding... so I will try to apply the induction principle... But to which proposition? Obviously the hypothesis on P is too complicated. I really don't like the "$\forall k \leq n,\ P(k)$". So I'll call it $Q(n)$. Oh wait... something interesting is going on... perhaps I can do "classical" induction and prove Q...]

Let $Q(n)$ be the property "$\forall k \leq n,\ P(k)$". We notice that:

$$[\forall n \in \mathbb{N}, Q(n)] \ \Rightarrow\ [\forall n \in \mathbb{N}, P(n)]\,.$$

Indeed, let us assume "$\forall n \in \mathbb{N},\ Q(n)$", and prove "$\forall n \in \mathbb{N},\ P(n)$". Let $n \in \mathbb{N}$, we want to prove $P(n)$. Now by hypothesis, we have that $Q(n)$ holds, in other words: $\forall k \leq n,\ P(k)$. Applying this to $k = n$, we get $P(n)$. So $(\forall n \in \mathbb{N}, Q(n)) \Rightarrow (\forall n \in \mathbb{N}, P(n))$, as announced.

Hence it is enough, in order to prove that P holds everywhere, to prove that $Q(n)$ is true for every integer n. Let us do that by "classical" induction.

- Initialization:

  Since $Q(1)$ states something about 1 and all natural integers *below* 1 (and there are none), it is easily checked that $Q(1)$ is actually equivalent to $P(1)$, hence (by assumption on P) true.

- Inductive step:

  Let $n \in \mathbb{N}$; we assume $Q(n)$ and we prove $Q(n+1)$.

  Some attention reveals that $Q(n)$ is equivalent to $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$.

  Now by our second assumption on P, we know $\forall n \in \mathbb{N}, Q(n) \Rightarrow P(n+1)$. Since we have assumed $Q(n)$, we get that $P(n+1)$ is true. But $Q(n)$ is true and equivalent to $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$. Hence $P(1) \wedge P(2) \wedge \cdots \wedge P(n) \wedge P(n+1)$ is true, and is equivalent to $Q(n+1)$. So $Q(n+1)$ is true.

  Hence, assuming $Q(n)$, we have proved $Q(n+1)$. Since this is true for any $n \in \mathbb{N}$, we have established $\forall n \in \mathbb{N}, Q(n) \Rightarrow Q(n+1)$.

- Conclusion:

  We have proved $Q(1)$ and $\forall n \in \mathbb{N}, Q(n) \Rightarrow Q(n+1)$. By "classical" induction, this implies $\forall n \in \mathbb{N}, Q(n)$. Now we have already noticed that this also implies $\forall n \in \mathbb{N}, P(n)$. QED

Appendix 2: proof of the induction principle

We now prove the induction principle. But since there are no free lunches, we must make use of the following axiom.

Axiom II.3.16. *Every non-empty set of* $\mathbb{N}$ *has a least element.*

Caution!

- This is not true for the empty set (since there are no elements at all in it).
- This is not true with subsets of $\mathbb{R}$. For example, take $(0, 1]$. If it were to have a least element, this would be 0 for sure. But since 0 does not belong to the interval $(0, 1]$, the latter has no least element.(0 is a "lower bound", but not an element of $(0, 1]$.)

Proof. Let $P(n)$ be a proposition depending on an integer n such that $P(1)$ and $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$ are true. We show $\forall n \in \mathbb{N}, P(n)$ holds.

[Well.. If there is a counter-example, I mean some n such that $P(n)$ does *not* hold, then there must a least one... but the one *before* the least one would not be a counter-example... and then the inductive step would... oh, perhaps we could use that to do a contradiction proof.]

Let E be the set of n not satisfying P; in symbols,

$$E = \{n \in \mathbb{N} : \neg P(n)\}$$

We assume that E is not empty, and prove a contradiction. Since E is a non-empty set of $\mathbb{N}$, it has a least element, say m.

By assumption, $P(1)$ holds, so m can't be 1. Hence $m > 1$. In particular, $m - 1 \in \mathbb{N}$. Since m is the *least* element of E, $m - 1 \notin E$. This means that $P(m - 1)$ *does* hold. Now by assumption, P is such that:

$$\forall n \in \mathbb{N}, P(n) \Rightarrow P(n + 1).$$

In particular, applying this statement to $n = m - 1$, we have:

$$P(m - 1) \Rightarrow P((m - 1) + 1)$$

Since $P(m-1)$ is true, so is $P((m-1)+1)$. But the latter is just $P(m)$. Hence $P(m)$ holds; and hence m can't be an element of E. This is a contradiction.

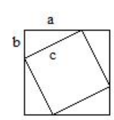
So E is empty; there are no counter-examples to $P(n)$. Hence $\forall n \in \mathbb{N}, P(n)$.
QED

Caution!

- Understanding a proof may take some time. In any case, it requires efforts from you.
- Proofs must be *learnt*. As long as you are not able to write a proof without looking at your notes, you haven't understood it.

II.4 Remarks and Exercises

Here is a proof of the Pythagorean theorem. Consider the following picture.



The area of the big square is $(a + b)^2$; it is also the sum of the area of the little square, and the four little right triangles.

Hence $(a + b)^2 = c^2 + 4\frac{ab}{2}$. This simplifies to $a^2 + b^2 = c^2$.

End of Lecture 14.

Lecture 15 (Review)

End of Lecture 15.

Exercises on Chapter II.

1 Basic proofs

(S) **Exercise II.1.** Let P, Q, R denote propositions. Prove the following:

1. $P \Rightarrow P \vee Q$.
2. $P \wedge Q \Rightarrow P$.
3. $[(P \Rightarrow Q) \wedge P] \Rightarrow Q$.
4. $(P \Rightarrow \neg P) \Rightarrow \neg P$.

(S) **Exercise II.2.** Prove that $\sqrt{3}$ is not a rational number.

(S) **Exercise II.3.** Prove that $\sqrt[3]{5}$ is not a rational number.

2 Proofs involving quantifiers

2.1 Easy proofs

(S) **Exercise II.4.** Prove the following statements:

1. There exists an even integer and there exists an odd integer.
2. For any real number, there is an integer bigger than it.
3. There is a real number that doesn't have a real square root.

(S) **Exercise II.5.** Here is a proof of:

$$\forall m \in \mathbb{N}, \forall n \in \mathbb{N}, m \text{ and } n \text{ are even} \Rightarrow m + n \text{ is even.}$$

> "Let m and n be integers. We assume that m and n are even, and we prove that so is $m + n$. Since m is even, there is an integer k such that $m = 2k$. Similarly, there exists an integer ℓ with $n = 2\ell$. Hence we have that $m+n = 2k+2\ell = 2(k+\ell)$, and therefore $m+n$ is even. QED"

Write a proof of:

$$\forall m \in \mathbb{N}, \forall n \in \mathbb{N}, m \text{ is odd and } n \text{ is even} \Rightarrow m + n \text{ is odd.}$$

You may use the fact that a natural number m is odd if and only if there is a non-negative integer k such that $m = 2k + 1$.

(S) **Exercise II.6.**

1. Let P be the proposition: $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x = y + 1$.
   (a) Translate P into English.
   (b) Prove that P is true.
2. Let Q be the proposition: $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, x = y + 1$.
   (a) Translate Q into English.
   (b) Prove that Q is false.

(S) **Exercise II.7.**

1. Prove that between two distinct integers there is always a real number.
2. Is this still true with real numbers?

2.2 Abstract proofs

Exercise II.8. Let A, B be sets and $P(x, y)$ be a proposition depending on x and y. Write a formal proof of the equivalence of $\exists x \in A, \exists y \in B, P(x, y)$ with $\exists y \in B, \exists x \in A, P(x, y)$.

(S) **Exercise II.9.** Let A be a set and $R(x, y)$ be a proposition depending on two variables. Let

$$S : \text{“} [\exists x \in A, \forall y \in A, R(x, y)] \Rightarrow [\forall y \in A, \exists x \in A, R(x, y)] \text{”}$$

1. Prove S.
2. State in symbols the *converse* of S.
3. Give a counter-example to the converse of S.
4. Find a special case (depending on A) in which the converse of S holds.

(S) **Exercise II.10.** Let A be a (non-empty) classroom, and P be the proposition:

> There is a student in A such that if he (or she) is a smoker,
> then every student in A is a smoker.

1. Translate P into symbols (let $S(x)$ be the property for x to be a smoker).
2. Prove P.
3. Is it still true with an empty classroom?

Exercise II.11. Let $P(x)$ be a proposition depending on a real number x. Prove that $\neg(\forall x \geq 0, P(x))$ is equivalent to $\exists x \geq 0, P(x)$.

2.3 More technical

Exercise II.12. Recall that a function has limit $+\infty$ at $+\infty$ if

$$\forall A \in \mathbb{R}, \exists M \in R, \forall x \in \mathbb{R}, x > M \Rightarrow f(x) > A$$

1. Prove that the identity function $f(x) = x$ has limit $+\infty$ at $+\infty$.
2. Prove that the sinus fuction $g(x) = \sin x$ does not have limit $+\infty$ at $+\infty$.

(S) **Exercise II.13.** Recall the following definitions, already met in Exercise II.13:

- A function $f : \mathbb{R} \to \mathbb{R}$ is continuous at $a \in \mathbb{R}$ if:

$$\forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

- A function is continuous on $\mathbb{R}$ if it is continuous at every $a \in \mathbb{R}$.

- A real function f is uniformly continuous on $\mathbb{R}$ if:

$$\forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, \forall y \in \mathbb{R}, |y - x| < \delta \Rightarrow |f(y) - f(x)| < \varepsilon.$$

1. Prove that if a function f is uniformly continuous, then f is continuous.

2. Prove that the function $x \mapsto cx + d$ is uniformly continuous on $\mathbb{R}$.

   [Hint: if $c = 0$, this is trivial. If $c \neq 0$, then $\delta = \frac{\varepsilon}{|c|}$ is clearly a good idea.]

3. Prove that the square function $x \mapsto x^2$ is continuous on $\mathbb{R}$.

   [Hint: Assume a fixed. When ε is given, use (for example)

$$\delta = \min\left(\sqrt{\frac{\varepsilon}{2}}, \frac{\varepsilon}{4|a| + 1}\right).$$

   You may admit that the implication of inequalities will hold for this value of δ, but you must write properly all the rest of the argument.]

4. Prove that the square function $x \mapsto x^2$ is *not* uniformly continuous on $\mathbb{R}$.

   [Hint: in fact each ε will eventually fail if you let the variables go far enough from 0. Have a look at large (but close) values for x and y.]

3 Induction Proofs

(S) **Exercise II.14.** Prove that

$$\forall n \in \mathbb{N}, \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

(S) **Exercise II.15.** Prove that

$$\forall n \in \mathbb{N}, \quad \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

(S) **Exercise II.16.** Read the following argument.

"We prove by induction that in a parterre of roses, if one is red then all are red. So for each $n \in \mathbb{N}$, let $P(n)$ be the property:

If one among n roses is red, then all n roses are red.

- Initialization. It is clear that if 1 among 1 rose is red, then the whole parterre is red. So $P(1)$ holds.

- Heredity. We assume $P(n)$ and prove $P(n+1)$. So let A be a parterre of $n+1$ roses $r_1, \dots, r_{n+1}$. Assume that one of these roses is red. For convenience we may assume it is r_1. Now consider the sub-parterre $B = \{r_1, \dots r_n\}$. (This notation means that B is the set of elements $r_1, \dots, r_n$.) of n roses, one of which is red. By the inductive hypothesis, all roses in B are red. So we now consider $C = \{r_2, \dots, r_{n+1}\}$, another (sub-)parterre of n roses, one of which is red. By the inductive hypothesis again, all roses in C are red. Since B and C cover A, all roses in A are red, hence $P(n+1)$ holds. Therefore $P(n) \Rightarrow P(n+1)$, and this is true for any $n \in \mathbb{N}$.

By induction, etc."

What went wrong ?

Exercise II.17. Let q be a real number not equal to 1. Prove that

$$\forall n \in \mathbb{N}, \sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}.$$

Chapter III

Set Theory

Aus dem Paradies, das Cantor uns geschaffen,
soll uns niemand vertreiben können.

We know how to state and prove statements. It is time to start exploring the realm of mathematics. A unified description of this world may be done in terms of sets. Discussing sets will also give us many concrete examples of interesting properties requiring clear proofs.

Main goals: Write formal proofs involving sets

- Know how to prove that $A \subseteq B$
- Know how to prove that $A = B$.
- Understand set notation and abstract definitions of sets
- Know how to handle infinite intersections and unions.

Notions. Membership and inclusion. Intersection, Union, Difference. Power set. Cartesian Product. Partition.

LECTURE 16 (SETS AND ELEMENTS. ALGEBRA WITH SETS)

III.1 Sets and membership

III.1.1 Notations; first examples

A *set* is something that has *elements*. (We do not pretend to give a definition.)

Actually a set is entirely determined by its elements.

Axiom III.1.1 (Extensionality Principle)**.** *Two sets are equal if and only if they have the same elements.*

Notation III.1.2. For a set A and an object x, we write $x \in A$ if x is an element of A. If $x \in A$ does not hold, we write $x \notin A$.

Caution! The membership symbol $\in$ is *not* an epsilon ε.

Remark III.1.3. It is customary (and following this custom is advised) to denote sets by capital letters, as opposed to their elements.

Remark III.1.4 (Alternate Expressions)**.**

"x is a member of A", "x lies in A", "x belongs to A"
- all mean "x is an element of A".

Caution!

- $x \in A$ may *not* be written $A \ni x$.
- It may *not* be read "A contains x", nor "x is contained in A".
- It may *not* be read "x is included in A".

Example III.1.5. Here are some fairly common sets:

- the set of natural numbers $\mathbb{N}$; $1 \in \mathbb{N}$.
- the set of (possibly negative) intgers $\mathbb{Z}$; $-1 \in \mathbb{Z}$ but $-1 \notin \mathbb{N}$.
- the set of rational numbers $\mathbb{Q}$; $\frac{1}{2} \in \mathbb{Q}$ but $\frac{1}{2} \notin \mathbb{Z}$.
- the set of real numbers $\mathbb{R}$; $\sqrt{2} \in \mathbb{R}$ but $\sqrt{2} \notin \mathbb{Q}$.
- Of course we can go beyond. If you know about complex numbers, $i \in \mathbb{C}$ but $i \notin \mathbb{R}$. On the other hand we need not involve such technology. Let f be the sinus function. It is a mathematical object, so it certainly is an element of some set. But it is not a real number, that is $f \notin \mathbb{R}$.

III.1.2 Inclusion of sets

In Example III.1.5, sets were going bigger. This motivates a definition.

Definition III.1.6 (subset, inclusion)**.** Let A and B be two sets. A is a subset of B (written $A \subseteq B$) if every element of A lies in B. One also says that A is included in B.

Hence, $A \subseteq B$ is equivalent to "$\forall x \in A, x \in B$".

Definition III.1.7 (proper subset)**.** If $A \subseteq B$ and $A \neq B$, we say that A is a proper subset of B and write $A \subsetneq B$.

Caution!

- $A \subsetneq B$ means that A is a *proper* subset of B.
- But $A \not\subseteq B$ means that A is *not* a subset of B!

Remark III.1.8. For any set A, it is the case that $A \subseteq A$.

Method to prove $\mathbf{A \subseteq B}$.

- Pick any $x \in A$.
- Prove $x \in B$.
- Conclude that $A \subseteq B$.

This suggests a method to prove the equality of two sets.

Method to prove that two sets A and B are equal.

- Prove $A \subseteq B$:
  - Pick any $x \in A$.
  - Prove $x \in B$.
  - Conclude that $A \subseteq B$.
- Prove $B \subseteq A$:
  - Pick any $x \in B$.
  - Prove $x \in A$.
  - Conclude that $B \subseteq A$.
- Conclude that $A = B$.

Properties III.1.9. *Let A, B, C be sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

The proof is an exercise. Exercise III.8

III.1.3 A special set

Before we go any further we introduce a very important set.

Definition III.1.10. The *empty set* $\emptyset$ is the set with no elements.

Remark III.1.11.

- The empty set is unique: if O is a set with no elements either, then since $\emptyset$ and O have exactly the same elements, they are equal by the extensionality principle, Axiom III.1.1.
- The empty set is a subset of every set.

Properties III.1.12. *Let P be a proposition in the variable x. Then :*

- *"$\forall x \in \emptyset, P(x)$" is* true.
- *"$\exists x \in \emptyset, P(x)$" is* false.

Example III.1.13.

- "$\forall x \in \emptyset, x \neq x$" is *true*.
- "$\forall x \in \emptyset, 1 + 1 = 2$" is *true*.
- "$\exists x \in \emptyset, 1 + 1 = 2$" is *false*.

Caution!

- "$\forall x \in \emptyset, P(x)$" is *true* because there are no possible counter-examples, since there are no elements at all in the empty set.
- On the other hand, "$\exists x \in \emptyset, P(x)$" is *false* because you will never find anything in the empty set (by definition of the empty set).

Remark III.1.14. As a consequence, the proposition

$$[\forall x \in A, P(x)] \Rightarrow [\exists x \in A, P(x)]$$

does not hold when $A = \emptyset$. But it does for any non-empty set A.

This flaw made our quantifiers suspect. And indeed, they are as irrelevant as our notion of implication, and as useful. Some people suggested that "for any x in A" should assume that A is non-empty; it did not make things any clearer; we shall stick to our convention, which is the only natural one.

III.1.4 Brace notation

Sometimes, and especially when dealing with finite sets, it is useful to define a set by giving its elements. This is done with braces.

Notation III.1.15. The ordering of elements between braces does not matter. Repeted elements are counted only once.

Example III.1.16.

- $\{1, 5\}$ is the set that has as only elements 1 and 5.
- $\{1, 2, 1\} = \{1, 2\} = \{2, 1\}$.
- $\{0, \sin\}$ is the set that has elements the number 0 and the function sin.
- Let A be any set. Then $\{A\}$ is the set that has A as its only element.

Exercises III.1, III.2

III.2 Naive operations with sets

We now describe the most elementary constructions with sets. They should be well-known. Always bear in mind the analogy with connectives.

III.2.1 Intersection

Definition III.2.1 (intersection)**.** Let A and B be two sets. The intersection of A and B (write $A \cap B$, pronounce "A and B" or "A intersected with B") is the set of elements of A that also lie in B.

Example III.2.2. $\mathbb{N} \cap \{-1, 1\} = \{1\}$. Exercise III.6

Properties III.2.3. *For all sets A, B, and C:*

(i). $A \cap B \subseteq A$.

(ii). $A \cap A = A$.

(iii). $\emptyset \cap A = \emptyset$.

(iv). $A \cap B = B \cap A$.

(v). $A \cap B = A$ *if and only if* $A \subseteq B$.

(vi). $A \cap (B \cap C) = (A \cap B) \cap C$.

Before we start the proof, remember the following methods.

- To prove an inclusion of sets $E \subseteq F$, take any x in E ("Let $x \in E$."), and prove $x \in F$.
- To prove an equality of sets $E = F$, prove two inclusions, namely $E \subseteq F$ and $F \subseteq E$.

Proof.

(i). Let us prove that $A \cap B \subseteq A$.

Let $x \in A \cap B$. Then $x \in A$ and $x \in B$; so $x \in A$. Since this is true regardless of $x \in A \cap B$, we have proved $A \cap B \subseteq B$.

(ii). Let us prove that $A \cap A = A$. [In order to do that, we prove two inclusions.]

By (i), it is the case that $A \cap A \subseteq A$.

So it remains to prove that $A \subseteq A \cap A$. Let $x \in A$. It is the case that $x \in A$ and $x \in A$, so $x \in A \cap A$. Since this is true regardless of $x \in A$, we have proved that $A \subseteq A \cap A$.

Because $A \cap A \subseteq A$ and $A \subseteq A \cap A$, we have $A \cap A = A$.

(iii). Let us prove that $\emptyset \cap A = \emptyset$.

We know that the empty set is a subset of any set, hence $\emptyset \subseteq \emptyset \cap A$ holds.

On the other hand, by (i), we have that $\emptyset \cap A \subseteq \emptyset$.

As a conclusion, we find that $\emptyset \cap A = \emptyset$.

(iv). Let us prove that $A \cap B = B \cap A$. [We have to prove two inclusions: we prove one, and conclude by symmetry!]

Let us prove that $A \cap B \subseteq B \cap A$. Let $x \in A \cap B$. Then $x \in A$ and $x \in B$; so $x \in B$ and $x \in A$. This means that $x \in B \cap A$. Since this is true regardless of $x \in A \cap B$, we have proved that $A \cap B \subseteq B \cap A$.

Now exchanging A and B we find $B \cap A \subseteq A \cap B$.

We thus have $A \cap B \subseteq B \cap A$ and $B \cap A \subseteq A \cap B$; therefore $A \cap B = B \cap A$.

(v). Let us prove that $A \cap B = A$ if and only if $A \subseteq B$. [We want to prove an equivalence, so we prove two implications.]

Let us assume that $A \cap B = A$ and let us prove that $A \subseteq B$. So let $x \in A$. Since $A = A \cap B$, we get that $x \in A \cap B$. In particular, $x \in B$. Since this is true regardless of $x \in A$, we have proved that $A \subseteq B$.

Now let us assume that $A \subseteq B$, we shall prove that $A \cap B = A$. [We have to prove two inclusions.]

By (i), it is always the case that $A \cap B \subseteq A$. So all it remains to prove is $A \subseteq A \cap B$ [using our assumption "$A \subseteq B$", of course.] Let $x \in A$. Since $A \subseteq B$, we find $x \in B$. Thus $x \in A$ and $x \in B$, which means $x \in A \cap B$. Since this is true regardless of $x \in A$, we have proved $A \subseteq A \cap B$. The converse inclusion has already been noticed, so $A = A \cap B$.

We proved both implications; hence $A \cap B = A$ is equivalent to $A \subseteq B$.

(vi). Let us prove that $A \cap (B \cap C) = (A \cap B) \cap C$. [Two inclusions.]

Let $x \in A \cap (B \cap C)$. Then $x \in A$, and $x \in B \cap C$. This means that $x \in A$, and $x \in B$, and $x \in C$. Therefore $x \in A \cap B$ and $x \in C$, which means $x \in (A \cap B) \cap C$. Since this is true regardless of $x \in A \cap (B \cap C)$, we deduce that $A \cap (B \cap C) \subseteq (A \cap B) \cap C$.

Instead of proving the converse inclusion, let us apply the part we have proved to C, B, A. We get $C \cap (B \cap A) \subseteq (C \cap B) \cap A$. Applying (iv) a couple of times, this implies $(A \cap B) \cap C \subseteq A \cap (B \cap C)$, so the other inclusion is proved too. [If you don't understand, just write a proof like that of the previous paragraph.]

Both inclusions hold, therefore $A \cap (B \cap C) = (A \cap B) \cap C$. QED

Remark III.2.4. (vi) enables us to write $A \cap B \cap C$ without parentheses.

Definition III.2.5 (disjoint)**.** Call two sets A and B *disjoint* if $A \cap B = \emptyset$.

III.2.2 Union

Definition III.2.6 (union)**.** Let A and B be two sets. The union of A and B (write $A \cup B$, pronounce "A union B") is the set made of elements of A together with elements of B.

Properties III.2.7. *For all sets A, B and C:*

(i). $A \subseteq A \cup B$.

(ii). $A \cup A = A$.

(iii). $A \cup \emptyset = A$.

(iv). $A \cup B = B \cup A$.

(v). $A \cup B = B$ *if and only if* $A \subseteq B$.

(vi). $A \cup (B \cup C) = (A \cup B) \cup C$.

The proof is an exercise. Exercise III.7

Properties III.2.8 (dsitributivity)**.** *Let A, B, C be sets. Then:*

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

The proof is an exercise. Exercise III.9

Caution! There is no convention on priority between $\cap$ and $\cup$. In particular $A \cap B \cup C$ makes no sense, and you *must* add parentheses somewhere

Remark III.2.9 (analogy with connectives)**.**

- Notice the analogy between $\wedge$ and $\cap$, and the analogy between $\vee$ and $\cup$.
- Contrarily to the case of propositions in which $P \Rightarrow Q$ was a proposition, there is no such thing here. The natural translation of $P \Rightarrow Q$ would be $P \subseteq Q$ - but this is a statement, not a set.
- $\neg$ has no analogous, because instead of defining the "absolute" complement of a set, we shall consider only differences of sets (Definition III.2.10).

III.2.3 Difference of sets

Definition III.2.10 (set difference)**.** Let A and B be two sets. The set difference $A \setminus B$ (pronounce "A minus B", or "A without B") is the set made of elements of A that do not lie in B.

Remark III.2.11. The notation $A - B$ also exists, but is not recommended.

Example III.2.12.

- $\mathbb{Z} \setminus \mathbb{N}$ is the set of non-positive integers.
- $\mathbb{N} \setminus \mathbb{Z} = \emptyset$.

Properties III.2.13. *For all sets A, B, C,*

(i). $A \setminus A = \emptyset$.

(ii). $A \setminus \emptyset = A$.

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

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

The proof is an exercise.

Caution! Do not try to make up other rules with the $\setminus$ operation. Always check what you affirm. For example, set difference is *not* commutative (like substraction): it is not the case that $A \setminus B = B \setminus A$. Think of a counter-example. Exercises III.10 to III.15

End of Lecture 16.

Lecture 17 (Not so naive operations on sets)

III.3 Not so naive operations with sets

III.3.1 Taking subsets

We have defined in §III.1.2 what a subset of a given set is. We now introduce further notation.

Notation III.3.1. Let A be a set and $P(x)$ a proposition depending on x. Then $\{x \in A : P(x)\}$ (pronounce "the set of elements of A satisfying P") is the subset of A made of the elements of A that satisfy P.

Remark III.3.2 (Alternate Expressions)**.**

"the set of x in A such that $P(x)$ holds", "the set of members of A s.t. $P(x)$" - all mean "the set of elements of A satisfying P".

Remark III.3.3. You might also find the following notations:

- $\{x \in A \mid P(x)\}$
- $\{x \in A,\ P(x)\}$

Example III.3.4.

- $A \setminus B = \{a \in A : a \notin B\}$.
- $\{n \in \mathbb{N} : \exists k \in N, n = 2k\}$ is the set of even natural numbers.
- $\{x \in \mathbb{R} : \sin x \leq 1\} = \mathbb{R}$. (Prove it!)
- $\{x \in \mathbb{R} : x \geq 0\} = \{x \in \mathbb{R} : \exists y \in \mathbb{R}, x = y^2\}$.

III.3.2 A special case: subsets of the real line

Definition III.3.5. Let $a \leq b$ be real numbers. We define the following sets:

- $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$ (the *closed interval* from a to b)
- $(a, b) = \{x \in \mathbb{R} : a < x < b\}$ (the *open interval* from a to b)
- $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$ (the *interval* closed at a, open at b)
- $(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$ (the *interval* open at a, closed at b)

Similarly, we define:

- $[a, +\infty) = \{x \in \mathbb{R} : a \leq x\}$ (the *closed ray* from a)
- $(a, +\infty) = \{x \in \mathbb{R} : a < x\}$ (the *open ray* from a)
- $(-\infty, a] = \{x \in \mathbb{R} : x \leq a\}$ (the *closed ray* to a)
- $(-\infty, a) = \{x \in \mathbb{R} : x < a\}$ (the *open ray* to a)

Remark III.3.6.

- $(-\infty, +\infty) = \mathbb{R}$.
- ∞ is never used with a bracket (because ∞ is not a real number).
- If $a > b$, $[a, b]$ (and others) makes no sense, and we avoid writing it.

Exercises III.20, III.22

III.3.3 The image of a set

In the following, a functional relation just means an F such that whenever a is determined, so is $F(a)$.

Definition III.3.7. Let A be a set and let F be a functional relation. Then $\{F(a) : a \in A\}$ (pronounce "the set of all $F(a)$'s, where a ranges over A") is the set of all objects of the form $F(a)$ where $a \in A$.

Remark III.3.8. Like for subsets, there are alternate notations: $\{F(a)|a \in A\}$ and $\{F(a), a \in A\}$.

Example III.3.9.

- $\{x + 1 : x \in \{1, 2\}\} = \{2, 3\}$.
- $\{x^2 : x \in \{-1, 0, 1\}\} = \{0, 1\}$.
- $\{x + 1 : x \in \mathbb{R}\} = \mathbb{R}$.
- $\{2k : k \in \mathbb{N}\}$ is the set of even numbers.

Exercise III.26

III.3.4 The power set

Definition III.3.10 (power set)**.** Let A be a set. The power set of A, written $P(A)$, is the set whose elements are all subsets of A.

Caution!

- $B \in P(A)$ iff B is a subset of A iff $B \subseteq A$. (Pay attention to $\in$ and $\subseteq$).
- For any set A, $\emptyset \in P(A)$. So $P(A)$ is *never empty*.

Example III.3.11.

- $P(\emptyset) = \{\emptyset\}$.
- $P(\{1\}) = \{\emptyset, \{1\}\}$.
- $P(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.
- In general, if A has n elements, then $P(A)$ has 2^n elements.

Exercises III.3 to III.5

Example III.3.12. We determine $P(\{\emptyset, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}, \{\{\emptyset\}\}\})$.

[I am looking for $P(E)$ where $E = \{\emptyset, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}, \{\{\emptyset\}\}\}$.

Since E has three elements, I am supposed to find 8 subsets. Let $a = \emptyset$, $b = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$, and $c = \{\{\emptyset\}\}$. The eight subsets of $\{a, b, c\}$ are: $\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$.]

We find:

$$P(E) = \left\{ \emptyset, \underbrace{\{\emptyset\}}_{\{a\}}, \underbrace{\{\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}\}}_{\{b\}}, \underbrace{\{\{\{\emptyset\}\}\}}_{\{c\}}, \underbrace{\{\emptyset, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}\}}_{\{a,b\}}, \right.$$
$$\left. \underbrace{\{\emptyset, \{\{\emptyset\}\}\}}_{\{a,c\}}, \underbrace{\{\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}, \{\{\emptyset\}\}\}}_{\{b,c\}}, \underbrace{\{\emptyset, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}, \{\{\emptyset\}\}\}}_{\{a,b,c\}=E} \right\}$$

Exercises III.16 to III.19

III.3.5 Union of sets

Definition III.3.13 (union of a family)**.** Let I be a set (this set provides "indices") and for each $i \in I$, let A_i be a set. The union of the A_i's when i ranges over I (denoted $\bigcup_{i \in I} A_i$, read "the union for i in I of A_i") is the set of all elements that lie in some A_i for some $i \in I$.

So actually, our naive union of two sets is a special case (when I, the set of indices, is made of only two elements).

Example III.3.14.

- For any set A,
$$A = \bigcup_{a \in A} \{a\}.$$
- $$\bigcup_{n \in \mathbb{N}} \{x \in \mathbb{R} : |x| = n\} = \mathbb{Z} \setminus \{0\}.$$
- $$\bigcup_{i \in \emptyset} A_i = \emptyset.$$

III.3.6 Intersection of sets

Definition III.3.15 (intersection of a *non-empty* family)**.** Let I be a *non-empty* set and for each $i \in I$, let A_i be a set. The intersection of the A_i's when i ranges over I (denoted $\bigcap_{i \in I} A_i$, read "the intersection for i in I of A_i") is the set of all elements that lie in all A_i's for all $i \in I$.

Exercise III.23

Caution! The intersection over the empty set is *not* defined.

End of Lecture 17.

Lecture 18 (Cartesian products and Function sets)

III.3.7 Cartesian Products

Notation III.3.16. (a, b) denotes the *ordered* pair "a, then b". It is not the same as (b, a) (unless of course if $a = b$).

Remark III.3.17. We could easily define (a, b) to be $\{a, \{a, b\}\}$); this technicality does not interest us and we take the existence of ordered pairs for granted.

Definition III.3.18 (Cartesian product)**.** Let A and B be two sets. The Cartesian product of A and B ($A \times B$, read "A times B") is the set of all pairs of the form (a, b), where $a \in A$ and $b \in B$.

Example III.3.19. Draw pictures of the following:

- $[0, 1] \times [0, 1]$
- $\mathbb{R} \times [0, 1)$
- $\{(x, y) \in \mathbb{R} \times \mathbb{R} : x < y\}$
- $\mathbb{N} \times \{x \in \mathbb{R} : x < 0 \vee x > 1\}$. Exercise III.24

Remark III.3.20. If A and B are finite sets, then so is $A \times B$, and its number of elements is: the number of elements in A times the number of elements in B.

Notation III.3.21. We write A^2 for $A \times A$. Similarly we write A^3 for the set of triples (a, a', a'') of elements of A, etc. Exercise III.27

Caution! A^2 is *bigger* than the set of all pairs (a, a) where $a \in A$. It is actually the set of all pairs (a, a') where a and a' are in A (not necessarily equal!).

We now explain how Cartesian products can simplify notation when working with quantifiers.

Properties III.3.22. *Let A, B be sets and $P(x, y)$ be a proposition depending on x and y. Then:*

- $\forall x \in A, \forall y \in B, P(x, y)$ *is equivalent to* $\forall (x, y) \in A \times B, P(x, y)$.
- $\exists x \in A, \exists y \in B, P(x, y)$ *is equivalent to* $\exists (x, y) \in A \times B, P(x, y)$.

If you feel comfortable with quantifiers, you may even adopt the following simplification of notation.

Notation III.3.23. Let A be a set.

- Instead of "$\forall (x, y) \in A^2$", we may write "$\forall x, y \in A$", implicitely understanding that both x and y freely range over A.
- Similarly, instead of $\exists (x, y) \in A^2$, we may write "$\exists x, y \in A$", implicitely understanding that both x and y are found in A.

At your own risk!

III.3.8 Function sets

Definition III.3.24 (function set)**.** Let A, B be sets. The set of functions from A to B is denoted B^A ("B to the A").

Remark III.3.25. If A and B are finite, then so is B^A, and its number of elements is the number of elements in B to the number of elements in A.

End of Lecture 18.

Lecture 19 (Partitions)

III.3.9 Partitions

Definition III.3.26 (partition)**.** Let E be a set. A partition of E is a family $\Pi = \{A_i : i \in I\}$ of subsets $A_i \subseteq E$ (indexed by I) such that:

- $\emptyset \notin \Pi$ (no A_i is empty)
- $i \neq j \Rightarrow A_i \cap A_j = \emptyset$ (the A_i's are pairwise disjoint)
- $\bigcup_{i \in I} A_i = E$ (the A_i's cover E)

Partitioning a set is very much like cutting a cake: no slice is empty, no two (different) slices overlap, and all the cake is cut.

Example III.3.27.

- The sets $[n, n+1)$ for $n \in \mathbb{Z}$ form a partition of $\mathbb{R}$.
- The sets $[n, n+1]$ for $n \in \mathbb{Z}$ *do not* form a partition of $\mathbb{R}$: because the intervals are not pairwise disjoint. For example, $[1, 2] \cap 52, 3] \neq \emptyset$.
- The sets $(n, n+1)$ for $n \in \mathbb{Z}$ *do not* form a partition of $\mathbb{R}$: because covering fails. Indeed, 1 is no set of the form $(n, n+1)$ for $n \in \mathbb{Z}$.

Caution! The clause "$A_i \cap A_j$ is empty whenever $i \neq j$" is *much stronger* than "the intersection of the A_i's is empty".

Counter-example III.3.28. Let $A_1 = \{2, 3\}$, $A_2 = \{1, 3\}$, and $A_3 = \{1, 2\}$. Then $A_1 \cap A_2 \cap A_3 = \emptyset$, but any intersection of two of them is non-empty.

Exercises III.32 to III.34

III.4 Remarks and Exercises

Perhaps some of you have imagined, or heard about the set of all sets. From the mathematical point of view, assuming that the collection of all mathematical sets is a mathematical set leads to Russell's well-known paradox.

> Let E be the set of all sets. We will find a contradiction (without having made an hypothesis, which is a flaw in the theory).
>
> Let $F = \{x \in E : x \notin x\}$. Aassuming that E is an ordinary, mathematical set, the set F makes good sense too.
>
> We wonder if F is an element of F. Let us start a case divsion.
>
> - If F is an element of F, then by definition of F, F satisfies the formula $x \notin x$. In particular, $F \notin F$, so F is not an element of F: this is a contradiction.
> - If F is not an element of F, then by definition of F, F does not satisfy the formula $x \notin x$. In particular, $F \in F$, so F is an element of F: this is a contradiction again.
>
> In either case, we have a contradiction!

Something must have gone wrong. Actually inspection of the proof reveals no trouble. Only the very first line relies on a common "pun" in logic: using the same word with two different meanings ("set" as the intuitive notion of collection, and "set" as the formal notion of mathematical set).

The proof relies on taking a special subset of E; this is possible if E is a mathematical set. So, assuming E is a mathematical set does lead to the contradiction. As a conclusion:

> Russell's argument only proves that the intuitive collection E of all sets is not a mathematical set itself.

End of Lecture 19.

Lecture 20 (Review)

End of Lecture 20.

Lecture 21 (ME2)

End of Lecture 21.

Exercises on Chapter III.

1 Very easy exercises

1.1 Finite sets

Exercise III.1. How many elements does $\{\emptyset, \{\emptyset, \{\emptyset\}\}\}$ have?

(S) **Exercise III.2.** Give all elements of the following sets:

1. $\{1, \{2\}, \{\{3\}, 4\}\}$
2. $P(\{a, b, c\}) \setminus (P(\{a, b\}) \cup P(\{a, c\}))$
3. $\{\emptyset, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}, \{\{\{\emptyset\}\}\}\}$

(S) **Exercise III.3.** Simplify the following sets:

1. $(\{a, \{a, b\}, b\} \cup \{a, \{a\}\}) \setminus \{\{b\}\}$.
2. $\{a, \{a, b\}\} \cap (\{a, b\} \cup P(\{a\}))$.
3. $P(\{a\}) \cup P(\{b\})$.
4. $P(\{a, b\}) \setminus P(\{b\})$.

Exercise III.4. Let $A = \{a, \{a, b\}, \{b, c\}\}$. How many elements are there in the set $P(P(A) \cup \{a, \{a, b\}\})$?

(S) **Exercise III.5.**

1. What is $P(P(\emptyset))$?
2. What is $P(P(\{\emptyset\}))$?
3. How many elements are there in $P(P(P(P(\emptyset))))$?
4. How many elements are there in $P(P(P(\{\emptyset\})))$?

1.2 The algebra of sets

Exercise III.6. Let A denote the set of all real numbers a that can be written $a = \sqrt{2} + n$ for some natural number n. Prove that $\mathbb{N} \cap A = \emptyset$.

Exercise III.7. Prove that for all sets A, B and C:

1. $A \subseteq A \cup B$.
2. $A \cup A = A$.
3. $A \cup \emptyset = A$.
4. $A \cup B = B \cup A$.
5. $A \cup B = B$ if and only if $A \subseteq B$.
6. $A \cup (B \cup C) = (A \cup B) \cup C$.

(S) **Exercise III.8.** Let A, B, C be sets. Show that if $A \subseteq B$ and $B \subseteq C$, $A \subseteq C$.

(S) **Exercise III.9.** Let A, B, C be sets. Prove that:

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(S) **Exercise III.10.** Let A, B be sets. Find a proposition (which does not involve the $\setminus$ operation) equivalent to $A \setminus B = A$. Prove this equivalence.

(S) **Exercise III.11.** Let A, B, C be sets. Give counter-examples (pictures are allowed) to the following wrong propositions:

1. $A \subseteq C \Rightarrow A \subseteq B \subseteq C$.
2. $A \setminus (B \cup C) = (A \setminus B) \cup (A \setminus C)$.

Exercise III.12. Let A, B be sets. Prove that $A \cap B = A \cup B \Rightarrow A = B$.

Exercise III.13. Let A, B, C be sets. Assume $A \cap B = A \cap C$ and $A \cup B = A \cup C$. Prove that $B = C$.

Exercise III.14. Let A, B be sets such that for any set C, $A \subseteq C \Rightarrow B \subseteq C$. Show $B \subseteq A$.

(S) **Exercise III.15.** We define the *symmetric difference* of two sets A, B to be $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

1. Make a picture.
2. Prove that $A \triangle B = B \triangle A$.
3. Prove that $(A \cap B) \cap (A \triangle B) = \emptyset$.
4. Prove that $(A \cap B) \cup (A \triangle B) = A \cup B$.
5. Prove that $A \triangle B = \emptyset$ if and only if $A = B$.
6. Prove that $A \triangle B \subseteq A$ if and only if $B \subseteq A$.
7. Prove that $A \subseteq A \triangle B$ if and only if $A \cap B = \emptyset$.
8. Prove that $A \triangle B = A$ if and only if $B = \emptyset$.

1.3 The power set operation

(S) **Exercise III.16.** Let A and B be sets.

1. Prove that $P(A \cap B) = P(A) \cap P(B)$.
2. Prove that $P(A) \cup P(B) \subseteq P(A \cup B)$.
3. Find a case in which $P(A) \cup P(B) \subsetneq P(A \cup B))$ (recall Definition III.1.7).

(S) **Exercise III.17.** Let A, B be sets. Show that $A = B \Leftrightarrow P(A) = P(B)$.

(S) **Exercise III.18.**

1. Find a set A such that $A \cap P(A) \neq \emptyset$.
2. Find a set B such that $B \cap P(B)$ has at least two elements.
3. Find a set C such that $C \cap P(C)$ is infinite.

(S) **Exercise III.19.** Prove *by induction* that if a set A has n elements, then $P(A)$ has 2^n elements.

2 Understanding set notation

(S) **Exercise III.20.** Find a shorter description (in symbols) of the following sets
.

1. $(\mathbb{N} \cap \mathbb{Z}) \cup (\mathbb{Q} \cap \mathbb{R})$.
2. $\{x \in \mathbb{R} : x^2 = 2\} \cap \mathbb{Q}$.
3. $\{n \in \mathbb{Z}, n^2 \in \mathbb{N}\} \cap \mathbb{Q}$.
4. $[0, 1] \cap [\frac{1}{2}, 2)$.
5. $[0, 1] \cup [\frac{1}{2}, 2)$.
6. $\{1, \{1, 2\}, 2, \{1\}\} \cap \{1, 2, \{3\}\}$.
7. $(\mathbb{Z} \setminus \mathbb{R}) \cup (\mathbb{Q} \setminus \mathbb{N})$.
8. $(\mathbb{Q} \cap \{\sqrt{2}, \{1, -1\}, 2, -2\}) \setminus \mathbb{N}$.

(S) **Exercise III.21.** Same question.

1. $\{x \in \mathbb{R} : x^2 = 2\} \cap \mathbb{Q}$.
2. $\{x \in \mathbb{R} : x^2 = -1\}$.
3. $[0, 1] \cap [\frac{1}{2}, 2)$.
4. $[0, 1] \cup [\frac{1}{2}, 2)$.
5. $\{x^2 : x \in \mathbb{R}\} \cap \{x^3 : x \in \mathbb{R}\}$.
6. $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : xy = 1\}$.
7. $\bigcup_{x>0}(-x, x]$.
8. $\bigcap_{x>0}(-x, x)$.
9. $\{x + 1 : x \in \{y \in \mathbb{R} : \exists z \in \mathbb{R} : z = 0\}\}$.
10. $\bigcup_{x>0}(-x, x] \setminus (0, x)$.

(S) **Exercise III.22.** Same question.

1. $\{x \in \mathbb{R} : x^2 = 1\} \cup \{x^2 : x \in \mathbb{R}\}$.
2. $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : xy = 2\}$.
3. $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : y = 0\}$.
4. $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : x = 0\}$.
5. $\{n \in \mathbb{N} : \exists q \in \mathbb{Q} : n = q\}$
6. $\{q \in \mathbb{Q} : \exists n \in \mathbb{N} : n = q\}$

(S) **Exercise III.23.** Same question.

1. $$\bigcap_{n\in\mathbb{N}}[-n, +\infty)$$
2. $$\bigcap_{n\in\mathbb{N}}[n, +\infty)$$
3. $$\bigcup_{n\in\mathbb{N}}\{x \in \mathbb{R} : n \leq x < n + 1\}$$
4. $$\bigcup_{x\in\mathbb{R}}\bigcap_{y\in\mathbb{R}}\{z \in \mathbb{R} : z = y\}$$
5. $$\bigcup_{0<a<1}(-a, a)$$
6. $$\bigcap_{a>1}(-a, a)$$

(S) **Exercise III.24.** Same question.

1. $$\bigcup_{0<x<1} (0, x)$$

2. $$\bigcup_{0<x<1} [0, x]$$

3. $$\bigcap_{0<x<1} (0, x)$$

4. $$\bigcap_{0<x<1} [0, x]$$

5. $$(\{0,1\} \times \{0,1\}) \setminus (\{(a,a) : a \in \{0,1\}\})$$

6. $$\mathbb{R} \times \mathbb{R} \setminus (\ (\mathbb{R}_{\geq 0} \times \mathbb{R}_{<0}) \cup (\mathbb{R}_{<0} \times \mathbb{R}_{<0}) \cup (\mathbb{R}_{<0} \times \mathbb{R}_{\geq 0})\ )$$

7. $$\{x \in \mathbb{R} : \forall y \in [0,1] : x > y\}$$

8. $$\{x \in \mathbb{R} : \exists y \in [0,1] : x > y\}$$

9. $$\{x \in \emptyset : x \in \mathbb{R}\}$$

10. $$\{x \in \{\emptyset\} : x \in \mathbb{R}\}$$

(S) **Exercise III.25.** Same question.

1. $P(P(\emptyset)) \setminus P(\emptyset)$
2. $$\bigcup_{x \in [-1,1]} (-|x|, x)$$
3. $$\bigcup_{n \in \mathbb{N}} (-n, 0)$$
4. $$\bigcap_{q \in \mathbb{Q}} [-|q|, 0]$$
5. $\{x \in \mathbb{R} : \forall y \in \mathbb{R} : x > y\}$
6. $\{x \in \mathbb{R} : \forall y \in \mathbb{R} : x > |y|\}$
7. $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : x > |y|\}$
8. $\{x \in \mathbb{R} : x > 0 \vee x < 0\}$
9. $\cos([0, \pi])$
10. $\{x : x \in \{y \in \mathbb{R} : y^2 = 1\}\}$
11. $\{x^2 : x \in \{y \in R : y = 1\}\}$
12. $$\bigcup_{q \in \{x \in \mathbb{Q} : x > 0\}} (-q, q)$$
13. $$\bigcup_{q \in \mathbb{Q}} (q - 1, q + 1)$$
14. $$\bigcup_{n \in 2\mathbb{Z}} (n - 1, n + 1)$$

(S) **Exercise III.26.** For any integer n, let $n\mathbb{Z}$ be the set $\{kn : k \in \mathbb{Z}\}$.

1. Rewrite the definition in English.
2. What is $2\mathbb{Z} \cup 4\mathbb{Z}$?
3. What is $2\mathbb{Z} \cap 4\mathbb{Z}$?
4. What is $2\mathbb{Z} \cap 3\mathbb{Z}$?

Exercise III.27. Let:

$A_1 = \{(x, y) \in \mathbb{R}^2 : x + y < 1\}$

$A_2 = \{(x, y) \in \mathbb{R}^2 : |x + y| < 1\}$

$A_3 = \{(x, y) \in \mathbb{R}^2 : |x| + |y| < 1\}$

$A_4 = \{(x, y) \in \mathbb{R}^2 : x + y > -1\}$

$A_5 = \{(x, y) \in \mathbb{R}^2 : |x - y| < 1\}$

1. Draw these sets.
2. Deduce a geometric proof of the following:

$$(|x + y| < 1 \wedge |x - y| < 1) \Leftrightarrow |x| + |y| < 1.$$

Exercise III.28. What are the following sets equal to?

1. $$\bigcap_{n\in\mathbb{N}} \left[n - \frac{1}{n}, n + \frac{1}{n}\right]$$

2. $$\bigcup_{k\in\mathbb{N}} \bigcap_{n\in\mathbb{N}} \left[k - \frac{1}{n}, k + \frac{1}{n}\right]$$

3 Infinite operations and partitions

3.1 Infinite operations

Exercise III.29. Let I be a set and $(A_i)_{i\in I}$ be a family of sets. Let B be a set. Prove the following:

1. $$B \cup \bigcup_{i\in I} A_i = \bigcup_{i\in I} (B \cup A_i)$$

2. $$B \cup \bigcap_{i\in I} A_i = \bigcap_{i\in I} (B \cup A_i)$$

3. $$B \cap \bigcup_{i\in I} A_i = \bigcup_{i\in I} (B \cap A_i)$$

4. $$B \cap \bigcap_{i\in I} A_i = \bigcap_{i\in I} (B \cap A_i)$$

Exercise III.30. Let $\{A_n, n \in \mathbb{N}\}$ and $\{B_n, n \in \mathbb{N}\}$ be two families of sets indexed by $\mathbb{N}$.

1. Assume: $\forall n \in \mathbb{N}, A_n \subseteq B_n \subseteq A_{n+1}$. Show that $\bigcup_{n\in\mathbb{N}} A_n = \bigcup_{n\in\mathbb{N}} B_n$.
2. Assume: $\forall n \in \mathbb{N}, A_n \supseteq B_n \supseteq A_{n+1}$. Show that $\bigcap_{n\in\mathbb{N}} A_n = \bigcap_{n\in\mathbb{N}} B_n$.

(S) **Exercise III.31.** Let I, J be two non-empty sets with $I \subseteq J$. For each $j \in J$, let A_j be a set.

1. Prove the following:

   (a)
   $$\bigcup_{i \in I} A_i \subseteq \bigcup_{j \in J} A_j$$
   (b)
   $$\bigcap_{j \in J} A_j \subseteq \bigcap_{i \in I} A_j$$

2. Find an example of sets I, J, and A_j such that:

   (a)
   $$I \subsetneq J, \qquad \bigcup_{i \in I} A_i \subsetneq \bigcup_{j \in J} A_j, \qquad \bigcap_{j \in J} A_j = \bigcap_{i \in I} A_j$$

   (b)
   $$I \subsetneq J, \qquad \bigcup_{i \in I} A_i = \bigcup_{j \in J} A_j, \qquad \bigcap_{j \in J} A_j \subsetneq \bigcap_{i \in I} A_j$$

   No justification required.

3.2 Partitions

(S) **Exercise III.32.** Let $A = \{a, b, c, d, e\}$. Give two partitions of A into three sets that have an odd number of elements. (No justification required.)

(S) **Exercise III.33.** Let X be the set of finite, non-empty subsets of $\mathbb{N}$. For each natural number n, let X_n be the set of subsets of $\mathbb{N}$ that have exactly n elements. Show that $\{X_n, n \in \mathbb{N}\}$ is a partition of X.

(S) **Exercise III.34.** Let A, I be non-empty sets and $\Pi = \{A_i : i \in I\}$ a partition of A. Let $B \subseteq A$ be non-empty and $J = \{j \in I : B \cap A_j \neq \emptyset\}$. Show that $\{B \cap A_j : j \in J\}$ is a partition of B.

4 Very conceptual

(S) **Exercise III.35.** We define the *finite Von Neumann ordinals* inductively:

1. $N_0 = \emptyset$
2. for each $n \in \mathbb{N} \cup \{0\}$, $N_{n+1} = N_n \cup \{N_n\}$.

This means $N_0 = \emptyset$, $N_1 = \{\emptyset\}$, $N_2 = \{\emptyset, \{\emptyset\}\}$, $N_3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, etc.

1. Give N_4 (no justification required).
2. Prove that for all $n \in \mathbb{N} \cup \{0\}$, $N_n \subseteq N_{n+1}$.
3. Prove that for all $n \in \mathbb{N} \cup \{0\}$, $N_n \subseteq P(N_n)$.

4. Prove that for all $n \in \mathbb{N} \cup \{0\}$, $N_n \notin N_n$.
5. Prove that for all $n \in \mathbb{N} \cup \{0\}$, N_n has exactly n elements.
6. Prove that for all $n \in \mathbb{N} \cup \{0\}$,
$$N_n = \bigcup_{k \leq n} N_k.$$
7. Prove that $\forall n \in \mathbb{N} \cup \{0\}, \forall m \in \mathbb{N} \cup \{0\}$, $n \leq m \Rightarrow N_n \in P(N_m)$.
8. Prove that $\forall n \in \mathbb{N} \cup \{0\}, \forall m \in \mathbb{N} \cup \{0\}$, $n < m \Leftrightarrow N_n \in N_m$.
9. If you want to think: consider the union over $\mathbb{N}$ of all N_n's; let N_ω be this union; consider $N_{\omega+1} = N_\omega \cup \{N_\omega\}$; resume process till you reach two times the infinity; resume process; resume process; etc.; enjoy.

Make your proofs as short as possible. Avoid $P(n)$ since this letter is already over-used in set theory.

Chapter IV

Functions

> *Lorsque des quantités variables sont tellement liées entre elles que, les valeurs de quelques-unes étant données, on puisse en conclure celles de toutes les autres, on conçoit ces diverses quantités exprimées au moyen de plusieurs d'entre elles, qui prennent alors le nom de* variables indépendantes*; et les quantités restantes, exprimées au moyen des variables indépendantes, sont ce qu'on appelle des* fonctions *de ces mêmes variables.*

With the language and framework of set theory at hand we shall now formalize the well-known concept of a function, which is the central notion of abstract mathematics. This chapter is a slippery bridge to advanced mathematics.

Main goals: Work with abstract functions and related notions

- Understand what a function is.
- Be able to show that a function is injective, or surjective.
- Compute reciprocal bijections.
- Compute image and preimage sets.

Notions. Function, Composition. Injection, Surjection. Bijection, Reciprocal Bijection. Image Set, Preimage.

LECTURE 22 (GRAPHS. THE VERTICAL LINE TEST. COMPOSITION.)

IV.1 Functions and Composition

A few words, not to define functions (which we shall do shortly), but to give an intuition of what will be going on. Suppose that you know what a function is;

take one (eg. the sinus function). Draw a picture. Draw a picture of the cos function.

We make the following observation.

> Any vertical line meets the curve once and once only. This means that each element x is mapped to a unique element.

Informally, when x is given, then $f(x)$ is understood with no ambiguity. We now are ready for the definition.

IV.1.1 Function graphs

Definition IV.1.1 (function graph)**.** Let A and B be sets. The graph of a function from A to B is a subset $\Gamma_f \subseteq A \times B$ such that the following two conditions are satisfied:

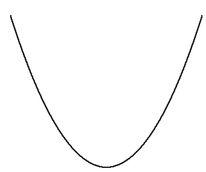
- $\forall a \in A, \exists b \in B, (a, b) \in \Gamma_f$
- $\forall (a, b, b') \in A \times B^2, (a, b) \in \Gamma_f \wedge (a, b') \in \Gamma_f \Rightarrow b = b'$.

In other words, a subset $\Gamma_f \subseteq A \times B$ is the graph of a function if and only if

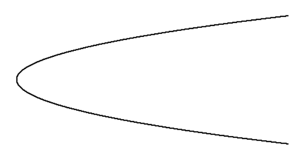
$$\forall a \in A, \exists! b \in B, (a, b) \in \Gamma_f.$$

Remark IV.1.2 (vertical line test)**.** For a given curve to be the graph of a function, it is necessary and sufficient to have the following property: every vertical line meets the curve exactly once.

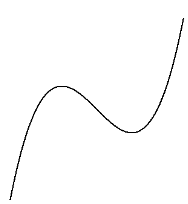
Example IV.1.3.

- 

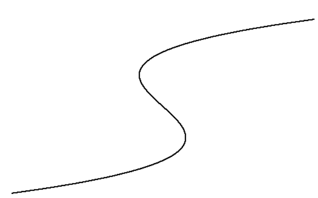
  This is the graph of a function (it could be the square function).

- 

  This is not a function graph: a vertical line will meet the curve twice.

- 

  This is the graph of a function (for instance, $x^3 - x$ would do).

- 

  Not a function graph: central vertical lines meet the curve three times.

IV.1.2 Functions and function notation

Definition IV.1.4 (function)**.** A function is a triple (A, B, Γ_f), where Γ_f is the graph of a function from A to B.

We then say that f is a function from A to B, and write

$$f : A \to B$$

Definition IV.1.5 (domain, codomain)**.** Let f be a function from A to B. A is the domain of f, denoted $\operatorname{dom} A$. B is the codomain of f, denoted $\operatorname{cod} f$.

Caution! A function is not a mapping. It consists of a domain, a codomain, and a mapping. Domain and codomain *must* be specified.

Example IV.1.6. Though they have exactly the same graph, the function f from $\mathbb{R}$ to $\mathbb{R}$ that maps x to x^2, and the function g from $\mathbb{R}$ to $\mathbb{R}_{\geq 0}$ that maps x to x^2 *are not* the same mathematical object (as they have different codomains):

$$\operatorname{cod} f = \mathbb{R} \quad \text{but} \quad \operatorname{cod} g = \mathbb{R}_{\geq 0}$$

Exercise IV.1

Notation IV.1.7 (function notation)**.** Given a function $f : A \to B$, we know that for each $x \in A$ there is a unique $y \in B$ associated to it. We say that f sends/maps x to y; in particular, writing $y = f(x)$ makes sense. Hence "f is the function from A to B that sends/maps x to f of x" is denoted:

$$\begin{array}{rccc} f: & A & \to & B \\ & x & \mapsto & f(x). \end{array}$$

Caution! $\to$ indicates domain and codomain, but $\mapsto$ denotes the assignment.

Definition IV.1.8 (identity function)**.** Let A be a set. The identity function of A is the function Id_A defined by

$$\begin{array}{rccc} \mathrm{Id}_A: & A & \to & A \\ & x & \mapsto & x \end{array}$$

Example IV.1.9. We shall use the following functions as running examples. Let $\mathcal{F}$ be the set of functions from $[0, 1]$ to $\mathbb{R}$ that can be derivated arbitrarily many times (technically, $\mathcal{F} = \mathcal{C}^\infty([0, 1], \mathbb{R})$; informally, it is the set of "smooth" functions, functions with a very "smooth" graph).

- Let $\mathcal{D}$ be the derivation operation:

$$\begin{array}{rccc} \mathcal{D}: & \mathcal{F} & \to & \mathcal{F} \\ & f & \mapsto & f' \end{array}$$

(It is the case that if $f \in \mathcal{F}$, then $f' \in \mathcal{F}$ too.)

- "Mapping a function to its primitive" is ambiguous, as there are infinitely many primitives. (Technically, $\int f$ denotes the *set* of primitives of f.)
- Let $\mathcal{P}$ map a function to its *unique* primitive which vanishes at 0:

$$\begin{array}{rccc} \mathcal{P}: & \mathcal{F} & \to & \mathcal{F} \\ & f & \mapsto & \int_0^x f(t)\mathrm{dt} \end{array}$$

  (Again, if $f \in \mathcal{F}$, then $\int_0^x f(t)\mathrm{dt}$ is in $\mathcal{F}$ too.)

Example IV.1.10. We take the notations of Example IV.1.9. exp denotes the exponential function from $[0,1]$ to $\mathbb{R}$.

- $\mathcal{D}(\exp)$ is the derivative of exp, hence $\mathcal{D}(\exp) = \exp$.
- $\mathcal{P}(\exp)$ is the primitive of exp which vanishes at 0. We know that exp is a primitive of itself, but $\exp(0) = 1$. So the primitive of exp which vanishes at 0 is the function mapping x to $\exp(x) - 1$, that is $\mathcal{P}(\exp) = \exp - 1$.
- $[\mathcal{D}(\exp)](0) = \exp(0) = 1$ and $[\mathcal{P}(\exp)](0) = (\exp - 1)(0) = e^0 - 1 = 0$.
- For any function $f \in \mathcal{F}$, one has

$$[\mathcal{P}(f)]\,(1) = \left(\int_0^x f(t)\mathrm{dt}\right)(1) = \int_0^1 f(t)\mathrm{dt}$$

IV.1.3 Composition of functions

Definition IV.1.11 (composition)**.** Let $f : A \to B$ and $g : B \to C$ be functions. The composition $g \circ f$ is the function from A to C which maps x to $g(f(x))$.

In symbols,

$$\mathrm{dom}(g \circ f) = \mathrm{dom}\, f; \quad \mathrm{cod}(g \circ f) = \mathrm{cod}\, g; \quad g \circ f(x) = g(f(x))$$

Caution!

- Apply f first, then g! The closest to x must be executed first!
- $f \circ g$ makes no sense (unless of course if $A = B$)

Example IV.1.12.

- $\sin \circ \cos$ is the function from $\mathbb{R}$ to $\mathbb{R}$ which maps x to $\sin(\cos(x))$.
- Let $f : \{1,2,3\} \to \{a,b,c\}$ be such that $f(1) = b$, $f(2) = c$, $f(3) = a$, and let $g : \{a,b,c\} \to \{\alpha,\beta,\gamma\}$ be such that $g(a) = \alpha$, $g(b) = \gamma$, $g(c) = \beta$. Then $(g \circ f)(1) = \alpha$, $(g \circ f)(2) = \beta$, $(g \circ f)(3) = \gamma$

Properties IV.1.13 (associativity of $\circ$)**.** *Let $f : A \to B$, $g : B \to C$, $h : C \to D$ be functions. Then*

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

Proof. We check that the functions $h\circ(g\circ f)$ and $(h\circ g)\circ f$ have same domain, same codomain, and define the same mapping.

$$\operatorname{dom}(h\circ(g\circ f)) = \operatorname{dom}(g\circ f) = \operatorname{dom} f = \operatorname{dom}((h\circ g)\circ f)$$

so domains agree.

$$\operatorname{cod}(h\circ(g\circ f)) = \operatorname{cod} h = \operatorname{cod}(h\circ g) = \operatorname{cod}((h\circ g)\circ f)$$

so codomains agree.

Let $x \in A$, then

$$\begin{array}{rcl}(h\circ(g\circ f))(x) & = & h((g\circ f)(x)) = h(g(f(x))) = ((h\circ g)(f(x))) \\ & = & ((h\circ g)\circ f)(x)\end{array}$$

So domains and codomains agree, and they define the same mapping. The functions $h\circ(g\circ f)$ and $(h\circ g)\circ f$ are therefore equal. QED

Properties IV.1.14. *Let $f : A \to B$ be a function. Then*

$$f \circ Id_A = f = Id_B \circ f$$

Example IV.1.15. We take the notations of Example IV.1.9 again.

- We claim that $\mathcal{D}\circ\mathcal{P} = \mathrm{Id}_{\mathbb{F}}$.

  Indeed, $\operatorname{dom}(\mathcal{D}\circ\mathcal{P}) = \operatorname{dom}(\mathcal{P}) = \mathcal{F}$, and $\operatorname{cod}(\mathcal{D}\circ\mathcal{P}) \operatorname{cod}\mathcal{D} = \mathcal{F}$ again. So $\mathcal{D}\circ\mathcal{P}$ is from $\mathcal{F}$ to $\mathcal{F}$.

  Now for any $f \in \mathcal{F}$, one has

  $$(\mathcal{D}\circ\mathcal{P})(f) = \mathcal{D}(\mathcal{P}(f)) = \mathcal{D}\left(\int_0^x f(t)\mathrm{dt}\right) = \left(\int_0^x f(t)\mathrm{dt}\right)' = f(x)$$

- We claim that $\mathcal{P}\circ\mathcal{D}$ is the following:

  $$\begin{array}{rccc}\mathcal{P}\circ\mathcal{D}: & \mathcal{F} & \to & \mathcal{F} \\ & f & \mapsto & \left(\begin{array}{cccc}\hat{f}: & [0,1] & \to & \mathbb{R} \\ & x & \mapsto & f(x)-f(0)\end{array}\right)\end{array}$$

  It is easy to see that $\mathcal{P}\circ\mathcal{D}$ is from $\mathcal{F}$ to $\mathcal{F}$. Now for $f \in \mathcal{F}$,

  $$(\mathcal{P}\circ\mathcal{D})(f) = \mathcal{P}(f') = \int_0^x f'(t)\mathrm{dt} = f(x) - f(0)$$

  so $\mathcal{P}\circ\mathcal{D}$ does map f to $\hat{f}$.

End of Lecture 22.

Lecture 23 (Injectivity and Surjectivity)

IV.2 Injectivity, Surjectivity, Bijectivity

IV.2.1 Injective functions

Definition IV.2.1 (injection)**.** Let $f : A \to B$ be a function. f is injective if:

$$\forall (a, a') \in A^2, f(a) = f(a') \Rightarrow a = a'.$$

Remark IV.2.2. Old-fashioned authors sometimes say that f is *one-one*. This terminology is *extremely confusing*, hence forbidden.

Remark IV.2.3. Contraposing, injectivity is equivalent to

$$\forall (a, a') \in A^2, a \neq a' \Rightarrow f(a) \neq f(a')$$

meaning that distinct elements cannot be mapped to the same element.

Caution! This is where students drown by number. Remember:

- "$\forall (a, a') \in A^2, a = a' \Rightarrow f(a) = f(a')$" means that the notation $f(a)$ makes sense, i.e. that when a is given, $f(a)$ is uniquely determined.
- Injectivity is "$\forall (a, a') \in A^2, f(a) = f(a') \Rightarrow a = a'$".

Remark IV.2.4 (Horizontal line test)**.** $f : A \to B$ is injective if and only if for all $b \in B$, there is *at most* one solution to the equation $f(x) = b$, $x \in A$. In other words, when you draw the graph, f is injective iff an horizontal line intersects the curve *at most* once.

Example IV.2.5.

- Let A be any set. Then Id_A is injective.
- $\sin : \mathbb{R} \to [-1, 1]$ is not injective (for instance, $\sin(0) = \sin(\pi)$).
- If A has only one element, then any function from A is injective.
- If A has more than one element, no constant function from A is injective.
- $\ln : \mathbb{R}_{>0} \to \mathbb{R}$, $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ are injective (draw the graphs).

Caution! Injectivity strongly depends on the domain!

Example IV.2.6.

- The square function $\mathbb{R} \to \mathbb{R}$ is *not* injective, as $(-1)^2 = 1 = 1^2$.
- The square function $\mathbb{R} \to \mathbb{R}_{\geq 0}$ is *not* injective, as $(-1)^2 = 1 = 1^2$.
- The square function $\mathbb{R}_{\geq 0} \to \mathbb{R}$ is injective.
- The square function $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is injective.

Proposition IV.2.7. *Let $f : A \to B$ and $g : B \to C$ be functions.*

(i). *If f and g are injective, then so is $g \circ f$.*

(ii). *If $g \circ f$ is injective, then so is f.*

Proof.

(i). We assume that f and g are injective, and we prove that $g \circ f$ is. So we let $a, a' \in A$ be such that $(g \circ f)(a) = (g \circ f)(a')$, and we prove $a = a'$. Our assumption means $g(f(a)) = g(f(a'))$. By injectivity of g, this implies $f(a) = f(a')$. By injectivity of f, this implies $a = a'$. So $g \circ f$ is injective.

(ii). We now assume that $g \circ f$ is injective, and we prove that f is. So let $a, a' \in A$ be such that $f(a) = f(a')$; we want to prove that $a = a'$. Applying g to our hypothesis, we get $(g \circ f)(a) = g(f(a)) = g(f(a')) = (g \circ f)(a')$. But by injectivity of $g \circ f$, this implies $a = a'$. QED

Caution! If $g \circ f$ is injective, there is no reason why g should be.

Counter-example IV.2.8. Let $f : \{1\} \to \{1, 2\}$ map 1 to 1, and let $g : \{1, 2\} \to \{1\}$ map 1 and 2 to 1. Notice that g is not injective. However, $g \circ f : \{1\} \to \{1\}$ is injective. Exercise IV.2

IV.2.2 Surjective functions

Definition IV.2.9 (surjection)**.** Let $f : A \to B$ be a function. f is surjective if

$$\forall b \in B, \exists a \in A, f(a) = b.$$

Remark IV.2.10. Old-fashioned authors sometimes say that f is *onto* B.

Remark IV.2.11. $f : A \to B$ is surjective if and only if $\forall b \in B$, there is *at least* one solution to the equation $f(x) = b$, $x \in A$. In other words, when you draw the graph of f, then an horizontal line intersects the curve *at least* once.

Example IV.2.12.

- Let A be any set. Then Id_A is surjective.
- $\sin : \mathbb{R} \to [-1, 1]$ is surjective.
- If A has only one element, then any function to A is surjective.
- $\ln : \mathbb{R}_{>0} \to \mathbb{R}$, $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ are surjective. Exercises IV.3, IV.4

Caution! Surjectivity strongly depends on the domain and codomain!

Example IV.2.13. We consider the same functions as in Example IV.2.6.

- The square function $\mathbb{R} \to \mathbb{R}$ is *not* surjective, as (-1) has no square root.

- The square function $\mathbb{R} \to \mathbb{R}_{\geq 0}$ is surjective.
- The square function $\mathbb{R}_{\geq 0} \to \mathbb{R}$ is *not* surjective.
- The square function $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is surjective.

Proposition IV.2.14. *Let $f : A \to B$ and $g : B \to C$ be functions.*

(i). *If f and g are surjective, then so is $g \circ f$.*

(ii). *If $g \circ f$ is surjective, then so is g.*

Proof.

(i). We assume that f and g are surjective, and we prove that $g \circ f$ is. So we let $c \in C$, and find $a \in A$ such that $(g \circ f)(a) = c$. By surjectivity of g, there is $b \in B$ such that $g(b) = c$. By surjectivity of f, there is $a \in A$ such that $f(a) = b$. Then $(g \circ f)(a) = c$.

(ii). We now assume that $g \circ f$ is surjective, and we prove that g is. So we let $c \in C$, and find $b \in B$ such that $g(b) = c$. By surjectivity of $g \circ f$, there is $a \in A$ such that $(g \circ f)(a) = c$. Let $b = f(a) \in B$. Then $g(b) = c$. QED

Caution! If $g \circ f$ is surjective, there is no reason why f should be.

Counter-example IV.2.15. We consider the same functions as in Counter-example IV.2.8. Let $f : \{1\} \to \{1, 2\}$ map 1 to 1, and let $g : \{1, 2\} \to \{1\}$ map 1 and 2 to 1. Notice that f is not surjective. However, $g \circ f : \{1\} \to \{1\}$ is surjective.

Exercise IV.8

End of Lecture 23.

Lecture 24 (Bijections and Reciprocal Bijections)

IV.2.3 Bijective Functions

It turns out that the case where a function is both injective and surjective is extremely interesting.

Definition IV.2.16 (bijection)**.** Let $f : A \to B$ be a function. f is bijective if it is both injective and surjective; in other words f is bijective iff

$$\forall b \in B, \exists! a \in A, f(a) = b.$$

Remark IV.2.17. Old-fashioned authors sometimes say that f is a *one-to-one correspondence*. This terminology is *extremely confusing*, hence forbidden.

Remark IV.2.18. $f : A \to B$ is bijective if and only if $\forall b \in B$, there is *exactly* one solution to the equation $f(x) = b$, $x \in A$. In other words, when you draw the graph of f, then an horizontal line intersects the curve *exactly* once.

Example IV.2.19.

- Let A be a set. Then Id_A is a bijection.
- $\ln : \mathbb{R}_{>0} \to \mathbb{R}$, $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ are bijections.
- The cube function $\mathbb{R} \to \mathbb{R}$ is a bijection.
- The absolute value $\mathbb{R} \to \mathbb{R}_{\geq 0}$ is not a bijection.

Caution! Bijectivity strongly depends on the domain and codomain!

Example IV.2.20. Same functions as in Examples IV.2.6 and IV.2.13.

- The square function $\mathbb{R} \to \mathbb{R}$ is *not* bijective, as it is not surjective.
- The square function $\mathbb{R} \to \mathbb{R}_{\geq 0}$ is *not* bijective, as it is not injective.
- The square function $\mathbb{R}_{\geq 0} \to \mathbb{R}$ is *not* bijective, as it is not surjective.
- The square function $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ *is* bijective.

Proposition IV.2.21. *Let $f : A \to B$, $g : B \to C$ be functions.*

(i). *If f and g are bijective, then so is $g \circ f$.*

(ii). *If $g \circ f$ is bijective, then f is injective, and g is surjective.*

Proof. Obvious from Propositions IV.2.7 and IV.2.14. QED

Caution! If $g \circ f$ is bijective, there is no reason why f nor g should be.

Counter-example IV.2.22. We consider the same functions as in Counter-examples IV.2.8 and IV.2.15. Let $f : \{1\} \to \{1, 2\}$ map 1 to 1, and let $g : \{1, 2\} \to \{1\}$ map 1 and 2 to 1. Neither f nor g is bijective. However, $g \circ f : \{1\} \to \{1\}$ is bijective.

Exercises IV.9, IV.10

IV.2.4 Reciprocal Bijections

A bijection is a "perfect" correspondence which can serve as a dictionary. You may also view it as an operation with no loss of information. What a bijection does, another bijection undoes. This "reverse" operation is actually unique.

Proposition IV.2.23. *Let $f : A \to B$ be a bijection. Then there is a unique function $g : B \to A$ such that*

$$g \circ f = Id_A \text{ and } f \circ g = \mathrm{Id}_B\,.$$

Besides, g is bijective.

Definition IV.2.24 (reciprocal bijection)**.** g is the reciprocal bijection of f, denoted f^{-1} (read: "f reciprocal")

Caution! There is no such thing if f is not a bijection!

Proof of Proposition IV.2.23.

- We first define g. Let $b \in B$. Then by bijectitivy of f, there is exactly one $a_b \in A$ such that $f(a_b) = b$ (of course, a_b depends on b). We let $g(b) = a_b$. Notice that since a_b is unique, this is well-defined. Hence g does define a function from B to A.

  Next we compute $g \circ f$. Notice that the domain and the codomain are A. Let $a \in A$. Then $g(f(a))$ is by definition the unique $\alpha \in A$ such that $f(\alpha) = f(a)$. Since f is injective, we get $\alpha = a$. So $g(f(a)) = a$, and since this is true regardless of $a \in A$, we have $g \circ f = \mathrm{Id}_A$.

  We now compute $f \circ g$. Notice that the domain and the codomain are B. Let $b \in B$. By bijectivity of f, there is exactly one element $a_b \in A$ such that $f(a_b) = b$. Then the definition of g says that $g(b) = a_b$. So $f(g(b)) = f(a_b) = b$. Since this is true regardless of $b \in B$, we find $f \circ g = \mathrm{Id}_B$.

  Hence there is a function g such that $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$. It remains to show bijectivity and uniqueness.

- Since $g \circ f = \mathrm{Id}_A$ is surjective, so is g (Proposition IV.2.14). Since $f \circ g = \mathrm{Id}_B$ is injective, so is g (Proposition IV.2.7). Hence g is bijective.

- We eventually show uniqueness. Suppose that there is another function, say h, from B to A and such that $h \circ f = \mathrm{Id}_A$ and $f \circ h = \mathrm{Id}_B$. We show $h = g$.

  Indeed, $h = h \circ Id_B = h \circ (f \circ g) = (h \circ f) \circ g = \mathrm{Id}_A \circ g = g$. QED

Properties IV.2.25. *Let $f : A \to B$, $g : B \to C$ be bijections. Then:*

(i). $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

(ii). $(f^{-1})^{-1} = f$.

Caution! $g^{-1} \circ f^{-1}$ is meaningless. You put your socks on, and then your shoes on. But you take off your shoes first, and then your socks!

Exercises IV.5, IV.6

End of Lecture 24.

Lecture 25 (Images and Preimages)

IV.3 Images and preimages

IV.3.1 Images

Definition IV.3.1 (image set)**.** Let $f : A \to B$ be a function, and let $E \subseteq A$ be a subset of A. The image of E under f is $f(E) = \{f(e) : e \in E\}$.

When $f : A \to B$, we say that $f(A)$ is the *image of* f.

Example IV.3.2. Let f denote the square function from $\mathbb{R}$ to $\mathbb{R}$.

- $f(\mathbb{R}) = f(\mathbb{R}_{\geq 0}) = f(\mathbb{R}_{\leq 0}) = \mathbb{R}_{\geq 0}$
- $f([-1,1]) = f([0,1]) = f([-1,0]) = [0,1]$

Properties IV.3.3. *Let $f : A \to B$ be a function, and let $E, F \subseteq A$ be subsets of A. Then:*

(i). $f(E \cap F) \subseteq f(E) \cap f(F)$.

(ii). $f(E \cup F) = f(E) \cup f(F)$.

Proof.

(i). Let $y \in f(E \cap F)$; we show $y \in f(E) \cap f(F)$. By definition, there is $x \in E \cap F$ such that $y = f(x)$. Since $x \in E$, one has $y \in f(E)$. Since $x \in F$, one also has $y \in f(F)$. This proves $f(E \cap F) \subseteq f(E \cap F)$.

(ii). Let $y \in f(E \cup F)$; we show $y \in f(E) \cup f(F)$. By definition, there is $x \in E \cup F$ such that $y = f(x)$. If $x \in E$, one has $y \in f(E) \subseteq f(E) \cup f(F)$. If $x \in F$, one has $y \in f(F) \subseteq f(E) \cup f(F)$. So in either case, $y \in f(E) \cup f(F)$. This proves $f(E \cup F) \subseteq f(E \cup F)$.

Now let $y \in f(E) \cup f(F)$; we show $y \in f(E \cup F)$. If $y \in f(E)$, then there is $x \in E$ such that $y = f(x)$. So $x \in E \cup F$ and $y \in f(E \cup F)$. If $y \in f(F)$, we show $y \in f(E \cup F)$ similarly. This proves $f(E) \cup f(F) \subseteq f(E \cup F)$. QED

Caution! In general $f(E \cap F) \subsetneq f(E) \cap f(F)$.

Example IV.3.4. Let $f : \mathbb{R} \to \mathbb{R}$ be the square function. Then one has $f(\mathbb{R}_{>0}) = \mathbb{R}_{>0} = f(\mathbb{R}_{<0})$, so $f(\mathbb{R}_{>0}) \cap f(\mathbb{R}_{<0}) = \mathbb{R}_{>0}$. But since $\mathbb{R}_{<0} \cap \mathbb{R}_{>0} = \emptyset$, one also $f(\mathbb{R}_{<0} \cap \mathbb{R}_{>0}) = \emptyset$.

IV.3.2 Preimages

Definition IV.3.5 (preimage)**.** Let $f : A \to B$ be a function, and let $F \subseteq B$ be a subset of B. The preimage of F under f is $f^{\langle -1 \rangle}(F) = \{a \in A : f(a) \in F\}$.

Caution! $f^{\langle -1 \rangle}$ is not defined as a function from B to A. Expressions like $f^{\langle -1 \rangle}(b)$ are meaningless. The argument of $f^{\langle -1 \rangle}$ must be a *subset* of B.

Example IV.3.6. Let f be the square function $\mathbb{R} \to \mathbb{R}$.

- $f^{\langle -1 \rangle}(\mathbb{R}) = \mathbb{R}$.
- $f^{\langle -1 \rangle}([0,1]) = [-1,1]$.
- $f^{\langle -1 \rangle}([-2,-1]) = \emptyset$.

Exercises IV.11, IV.12

Properties IV.3.7. *Let $f : A \to B$ be a function, and let $E, F \subseteq B$ be subsets of B. Then:*

(i). $f^{\langle -1 \rangle}(E \cap F) = f^{\langle -1 \rangle}(E) \cap f^{\langle -1 \rangle}(F)$.

(ii). $f^{\langle -1 \rangle}(E \cup F) = f^{\langle -1 \rangle}(E) \cup f^{\langle -1 \rangle}(F)$.

Proof.

(i). Let $x \in f^{\langle -1 \rangle}(E \cap F)$; we show $x \in f^{\langle -1 \rangle}(E) \cap f^{\langle -1 \rangle}(F)$. By definition, $f(x) \in E \cap F$. Since $f(x) \in E$, one has $x \in f^{\langle -1 \rangle}(E)$. Since $f(x) \in F$, one also has $x \in f^{\langle -1 \rangle}(F)$. This proves $f^{\langle -1 \rangle}(E \cap F) \subseteq f^{\langle -1 \rangle}(E \cap F)$.

Now let $x \in f^{\langle -1 \rangle}(E) \cap f^{\langle -1 \rangle}(F)$; we show $x \in f^{\langle -1 \rangle}(E \cap F)$. Since $x \in f^{\langle -1 \rangle}(E)$, one has $f(x) \in E$. Since $x \in f^{\langle -1 \rangle}(F)$, one also has $f(x) \in F$. Hence $f(x) \in E \cap F$. So $x \in f^{\langle -1 \rangle}(E \cap F)$. This proves $f^{\langle -1 \rangle}(E) \cap f^{\langle -1 \rangle}(F) \subseteq f^{\langle -1 \rangle}(E \cap F)$.

(ii). Let $x \in f^{\langle -1 \rangle}(E \cup F)$; we show $x \in f^{\langle -1 \rangle}(E) \cup f^{\langle -1 \rangle}(F)$. By definition, $f(x) \in E \cup F$. If $f(x) \in E$, one has $f(x) \in E \cup F$, whence $x \in f^{\langle -1 \rangle}(E \cup F)$. If $f(x) \in F$, one has $x \in f^{\langle -1 \rangle}(E \cup F)$ similarly. This proves $f^{\langle -1 \rangle}(E \cup F) \subseteq f^{\langle -1 \rangle}(E) \cup f^{\langle -1 \rangle}(F)$.

Now let $x \in f^{\langle -1 \rangle}(E) \cup f^{\langle -1 \rangle}(F)$; we show $x \in f^{\langle -1 \rangle}(E \cup F)$. If $x \in f^{\langle -1 \rangle}(E)$, one has $f(x) \in E \subseteq E \cup F$, so $x \in f^{\langle -1 \rangle}(E \cup F)$. If $x \in f^{\langle -1 \rangle}(F)$, one has $x \in f^{\langle -1 \rangle}(E \cup F)$ similarly. This proves $f^{\langle -1 \rangle}(E) \cup f^{\langle -1 \rangle}(F) \subseteq f^{\langle -1 \rangle}(E \cup F)$. QED

Exercises IV.13 to IV.16

Remark IV.3.8. If $f : A \to B$ is bijective and $E \subseteq B$, then

$$\underbrace{f^{-1}(E)}_{\substack{\text{image under} \\ \text{the function } f^{-1}}} = \underbrace{f^{\langle -1 \rangle}(E)}_{\substack{\text{preimage under} \\ \text{the function } f}}$$

IV.4 Remarks and Exercises

It is possible to define "partially reciprocal" functions under conditions weaker than bijectivity.

Proposition IV.4.1. *Let $f : A \to B$ be an injective function. Then there is a unique function $g : f(A) \to A$ such that*

$$g \circ f = Id_A \text{ and } f \circ g = \mathrm{Id}_{f(A)}\,.$$

Besides, g (as a function from $f(A)$ to A) is bijective.

Caution!

- If $f(A) \subsetneq B$, then g is not defined on B, but only on $f(A)$.

- There is no reason why $f \circ g$ should be Id_B.

Example IV.4.2. Let $A = \{1\}$, $B = \{1, 2\}$. Then the map $A \to B$ which maps 1 to 1 is injective but not surjective. The partial reciprocal function is the function $\{1\} \to \{1\}$. The composition $f \circ g$ is the constant function 1, which is not equal to Id_B.

Proposition IV.4.3. *Let $f : A \to B$ be a surjective function. Then there is a (not necessarily) unique function $g : B \to A$ such that*

$$f \circ g = \mathrm{Id}_B \,.$$

Besides, any such g (as a function from B to A) is injective.

Caution!

- In general, g is not unique.
- There is no reason why $g \circ f$ should be Id_A.

Example IV.4.4. Let $f : \{1, 2\} \to \{1\}$ be the constant function 1. Then there are two possible choices for g, namely $g_1 : 1 \mapsto 1$ and $g_2 : 1 \mapsto 2$. However, $g_1 \circ f$ is the constant function 1 and $g_2 \circ f$ is the constant function 2: neither equals Id_A.

Example IV.4.5. Let $A = \{1\}$, $B = \{1, 2\}$. Then $\iota_{A,B}$ is injective but not surjective. The partial reciprocal function is the function $\{1\} \to \{1\}$.

Proof of Proposition IV.4.3. Since f is surjective, for each $b \in B$, there is $a_b \in A$ such that $f(a_b) = b$. For each $b \in B$, fix such a_b. This might involve performing infinitely many choices (one choice for each a_b, that is as many choices as elements of B), and a specific axiom is required. Now define a function $g : B \to A$ by $g(b) = a_b$. Since for any $b \in B$, a_b is uniquely defined, g is well-defined. It is straightforward that $f \circ g = \mathrm{Id}_B$. QED

End of Lecture 25.

Exercises on Chapter IV.

1 Warm-up exercises

(S) **Exercise IV.1.** Do the following constructions define functions? If yes, find the biggest possible domain on which they make sense.

1. Send any real number x to its square.
2. Send any real number to one of its real square roots.

3. Send any non-negative real number to one of its real square roots.

4. Send any real number to the biggest integer not greater than it.

5. Send any real number to the integer that is closest to it.

6. Send x to $\sin(\sqrt{(}-x^2))$.

(S) **Exercise IV.2.** Are the functions $\mathcal{D}$, $\mathcal{P}$ of Example IV.1.9 injective?

(S) **Exercise IV.3.** Are the functions $\mathcal{D}$, $\mathcal{P}$ of Example IV.1.9 surjective?

Exercise IV.4.

1. Determine all injections $\{1,2\} \to \{1,2,3,4\}$ (you should find 12 of these).

2. Determine all surjections $\{1,2,3,4\} \to \{1,2\}$ (you should find 14 of these).

Exercise IV.5. Let $f, g : \{1,2,3,4\} \to \{1,2,3,4\}$ be the following bijections:

$$f : \begin{cases} 1 & \mapsto & 2 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 4 \\ 4 & \mapsto & 3 \end{cases}, \qquad g : \begin{cases} 1 & \mapsto & 2 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 1 \\ 4 & \mapsto & 4 \end{cases}$$

1. Check that $f \circ g \neq g \circ f$.

2. Compute f^{-1} (the reciprocal bijection), g^{-1}.

3. Check that $f^{-1} = f$ and $g^{-1} = g \circ g$.

4. Find a bijection $h : \{1,2,3,4\} \to \{1,2,3,4\}$ such that $h^{-1} = h \circ h \circ h$.

Exercise IV.6. Let $a \in \mathbb{R} \setminus \{0\}$ and $b \in \mathbb{R}$. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = ax + b$.

1. Prove that f is a bijection.
2. Determine f^{-1}.

Exercise IV.7. Define $f : \mathbb{Z} \times \mathbb{Z} \setminus \{0\} \to \mathbb{Q}$ by:

$$f((p,q)) = \frac{p}{q}.$$

1. Is f injective? If so, prove it. If not, provide a counter-example.

2. Find $f^{\langle -1 \rangle}(\{\frac{1}{2}\})$.

2 Injections, Surjections, Bijections

Exercise IV.8. Suppose that $A_0, ..., A_n$ are sets and for each $i = 1, ..., n$, $f_i : A_{i-1} \to A_i$ is a surjective function. Prove by induction that:

$$f_n \circ f_{n-1} \circ \cdots \circ f_1 : A_0 \to A_n$$

is also surjective.

(S) **Exercise IV.9.** Let E be a set. For any subset $A \subseteq E$, the *characteristic function* of A in E is:

$$\begin{array}{rccl} \chi_A : & E & \to & \{0,1\} \\ & x & \mapsto & \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases} \end{array} .$$

1. Draw the characteristic function of $[0,1]$ in $\mathbb{R}$.
2. Draw the characteristic function of $\mathbb{Q}$ in $\mathbb{R}$.
3. Let 2^E be the set of functions $E \to \{0,1\}$. Let

$$\begin{array}{rccc} \Phi : & P(E) & \to & 2^E \\ & A & \mapsto & \chi_A \end{array} .$$

   Prove that Φ is injective.
4. Prove that Φ is surjective.
5. Deduce that if E is finite and has n elements, then $P(E)$ has 2^n elements.

(S) **Exercise IV.10.** This exercise is entirely trivial, but highly abstract.
Let $\mathbb{F}$ be the set of functions from $\mathbb{R}$ to $\mathbb{R}$.

1. [Constant functions] For any $a \in \mathbb{R}$, let $C_a \in \mathbb{F}$ be defined as follows:

$$\begin{array}{rccc} C_a : & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & a \end{array}$$

   Let

$$\begin{array}{rccc} \mathcal{C} : & \mathbb{R} & \to & \mathbb{F} \\ & a & \mapsto & C_a \end{array}$$

   Prove that $\mathcal{C}$ is injective.
2. Prove that $\mathcal{C}$ is not surjective.
3. [Evaluation functionals] For any $a \in \mathbb{R}$, let ev_a be the following function:

$$\begin{array}{rccc} ev_a : & \mathbb{F} & \to & \mathbb{R} \\ & f & \mapsto & f(a) \end{array}$$

   So by definition, for all $f \in \mathbb{F}$, $a \in \mathbb{R}$, one has $ev_a(f) = f(a)$.

   Find a function $f \in \mathbb{F}$ such that $ev_0(f) = ev_1(f) = 1$.

4. [The space canonically embeds into its bidual] Let $\mathbb{F}'$ be the set of all functions $\mathbb{F} \to \mathbb{R}$ (getting conceptual!). For instance, for any $a \in \mathbb{R}$, we have $ev_a \in \mathbb{F}'$.

   Let

   $$\begin{array}{rccc} \Phi: & \mathbb{R} & \to & \mathbb{F}' \\ & a & \mapsto & ev_a \end{array}$$

   Prove that Φ is injective.

5. Prove that Φ is not surjective.

   [This question is not hard: find something that assigns to each function a number, in such a way that this assignment is not an evaluation map.]

6. For any $f \in \mathbb{F}$, let εv_f be the following map $\mathbb{F}' \to \mathbb{R}$:

   $$\begin{array}{rccc} \varepsilon v_f: & \mathbb{F}' & \to & \mathbb{R} \\ & \psi & \mapsto & \psi(f) \end{array}$$

   Hence for all $\psi \in \mathbb{F}'$, $f \in \mathbb{F}$, one has $\varepsilon v_f(\psi) = F(\psi)$.

   Show that for all $a \in \mathbb{R}$, for all $f \in \mathbb{F}$, one has $\varepsilon v_f(ev_a) = f(a)$.

3 Images and preimages

(S) **Exercise IV.11.** Let f be the following function:

$$\begin{array}{rccc} f: & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & x^4 \end{array}$$

Determine the following sets:

1. $f(\mathbb{R})$, $f(\mathbb{R}_{\geq 0})$, $f(\mathbb{R}_{\leq 0})$, $f([0,1])$, $f([-1,1])$

2. $f^{\langle -1 \rangle}(\mathbb{R})$, $f^{\langle -1 \rangle}(\mathbb{R}_{\geq 0})$, $f^{\langle -1 \rangle}(\mathbb{R}_{\leq 0})$, $f^{\langle -1 \rangle}([0,1])$, $f^{\langle -1 \rangle}([-1,1])$.

(S) **Exercise IV.12.** Let f be the function from $P(\mathbb{N}) \setminus \{\emptyset\}$ to $\mathbb{N}$ taking any non-empty subset of $\mathbb{N}$ to its least element.

1. Let A be the set of all infinite sets of $\mathbb{N}$. Determine $f(A)$.

   Let B be the set of all finite, non-empty sets of $\mathbb{N}$. Determine $f(B)$.

2. Determine $f^{\langle -1 \rangle}(\{1\}), f^{\langle -1 \rangle}(\{2\}), f^{\langle -1 \rangle}(\{1,2\})$.

3.1 Getting abstract

Exercise IV.13. Let $f : A \to B$ be a function.

1. Suppose that f is injective. Let E, F be subsets of A. Show that $f(E \cap F) = f(E) \cap f(F)$.
2. Prove the converse: suppose that for all be subsets E, F of A, $f(E \cap F) = f(E) \cap f(F)$, and show that f is injective.

(S) **Exercise IV.14.** Let $f : A \to B$ be a function.

1. Let $E \subseteq A$ be a subset of A. Prove that $E \subseteq f^{\langle -1 \rangle}(f(E))$.
2. Find an example of a function f and a subset $E \subseteq \operatorname{dom} f$ such that $E \subsetneq f^{\langle -1 \rangle}(f(E))$.
3. Let $F \subseteq B$ be a subset of B. Prove that $f(f^{\langle -1 \rangle}(F)) \subseteq F$.
4. Find an example of a function f and a subset $F \subseteq \operatorname{cod} f$ such that $f(f^{\langle -1 \rangle}(F)) \subsetneq F$.
5. Suppose f injective. Show that for any $E \subseteq \operatorname{dom} f$, $E = f^{\langle -1 \rangle}(f(E))$.
6. Prove the converse: suppose that for any $E \subseteq \operatorname{dom} f$, $E = f^{\langle -1 \rangle}(f(E))$, and show that f is injective.

(S) **Exercise IV.15.** Let $f : A \to B$ be a function, and define the function

$$g : \begin{array}{ccc} P(A) & \to & P(B) \\ E & \mapsto & f(E) \end{array}$$

1. Prove that f is injective if and only if g is.
2. Prove that f is surjective if and only if g is.

Notice that for any subset $E \subseteq A$, one has $f(E) = g(E)$.

Exercise IV.16. Let $f : A \to B$ be a function, and define the function

$$h : \begin{array}{ccc} P(B) & \to & P(A) \\ E & \mapsto & f^{\langle -1 \rangle}(E) \end{array}$$

1. Prove that f is injective if and only if h is surjective.
2. Prove that f is surjective if and only if h is injectve.

Solutions to Some Exercises

Exercises of Chapter I

I.1 Basic exercises

I.1.1 Propositions

Solution of Exercise I.1.

1. "Hello!" is not a proposition. This should be clear.
2. "How are you?" is a question, not a statement. It is not a proposition.
3. "I am fine." is not a proposition, as the meaning of "I" is fuzzy.
4. "Paul (SSN 142-19-6471) is fine." is a proposition, because one exactly knows who Paul is (through his SSN), and what "fine" means.
5. "This number is positive." is not a proposition: which number?
6. "-1 is positive." is a proposition. The meaning is clear (though false).
7. "There are no free lunches." is a general statement whose meaning is clear. (We won't discuss its truth.)
8. "When it rains, π is a circle." is a proposition. It is false, as it sometimes rains but π is never a circle.

I.1.2 Truth tables

Solution of Exercise I.4. To compute the truth table of a complex proposition, auxiliary columns may be useful. This is what we do (the auxiliary columns are not part of the answer).

The requested truth tables are:

1.

P	Q	R	$P \wedge \neg Q$	$\neg R$	$(P \wedge \neg Q) \wedge \neg R$
F	F	F	F	T	F
F	F	T	F	F	F
F	T	F	F	T	F
F	T	T	F	F	F
T	F	F	T	T	T
T	F	T	T	F	F
T	T	F	F	T	F
T	T	T	F	F	F

2.

P	Q	R	$\neg P \vee Q$	$\neg Q \vee R$	$(\neg P \vee Q) \wedge (\neg Q \vee R)$
F	F	F	T	T	T
F	F	T	T	T	T
F	T	F	T	F	F
F	T	T	T	T	T
T	F	F	F	T	F
T	F	T	F	T	F
T	T	F	T	F	F
T	T	T	T	T	T

Solution of Exercise I.6. The requested truth tables are:

1.

P	Q	$(P \vee Q) \Rightarrow (P \wedge Q)$
F	F	T
F	T	F
T	F	F
T	T	T

2.

P	Q	R	$(\neg P \wedge Q) \Rightarrow (Q \wedge R)$
F	F	F	T
F	F	T	T
F	T	F	F
F	T	T	T
T	F	F	T
T	F	T	T
T	T	F	T
T	T	T	T

3.

P	Q	R	$P \Rightarrow (Q \Rightarrow R)$
F	F	F	T
F	F	T	T
F	T	F	T
F	T	T	T
T	F	F	T
T	F	T	T
T	T	F	F
T	T	T	T

4.

P	Q	R	$P \Leftrightarrow (Q \Leftrightarrow R)$
F	F	F	F
F	F	T	T
F	T	F	T
F	T	T	F
T	F	F	T
T	F	T	F
T	T	F	F
T	T	T	T

Solution of Exercise I.8. Some interpretation of the problem can help. Let us comment on this table: notice the requested expression is true when P, or Q, *but not both* is. So we get an intuition that $P \wedge Q \wedge \neg(P \wedge Q)$ should fit. It is the case (as one should check):

P	Q	$P \wedge Q \wedge \neg(P \wedge Q)$
F	F	F
F	T	T
T	F	T
T	T	F

Remark.

- this form corresponds to the English "either P or Q". It is called *exclusive or* (as opposed to the mathematical "inclusive" or).
- $\neg(P \Leftrightarrow Q)$ is another possible answer.

I.1.3 Translations

Solution of Exercise I.9.

1. $$\text{(I think)} \wedge \text{(I am)}$$

   Do not be surprised. The original sentence is about a specific argument (shall we say a proof?). It would have been translated by "$\Rightarrow$" had it been of the form: "Whoever thinks, is."

2. "If it rains and I am home, then I play the piano or listen to the radio." is of the form:

   $$[\text{(It rains)} \wedge \text{(I am home)}] \Rightarrow [\text{(I play the piano)} \vee \text{(I listen to the radio)}]$$

3. "Paul was neither silly nor stupid, but George was a fool and so was Ringo." is of the form:

   $$\neg PS_1 \cap \neg PS_2 \cap GF \cap RF$$

4. $$\neg K \Rightarrow [L \wedge (\neg P \Rightarrow S)]$$

5. $$\neg \text{ I have a car} \wedge \text{I take the subway}$$

   Same observation as for 1. It is not a general statement, but a mere a conjunction of arguments. The implication would be used for "Who has no car must take the subway".

6. $$(P \vee Q) \wedge \neg(P \wedge Q)$$

Solution of Exercise I.12. Some possible solutions:

1. "John is the best but if Paul is the best, John is not the best."
2. "I lay eggs or watch TV; by the way I watch TV exactly when I am too tired to do anything else."

I.1.4 Negations

Solution of Exercise I.14.

1. Let us be extremely wordy on the first one.

   $(P \wedge Q) \vee (P \vee Q)$ is a disjunction (namely, the disjunction of $P \wedge Q$ and of $P \vee Q$). We know that the negation of a disjunction of a disjunction is the conjunction of negations, so the desired negation will be equivalent to

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

   We are not done. We have to work on smaller terms: $\neg(P \wedge Q)$ is the negation of a conjunction, hence the disjunction of negations. So $\neg(P \wedge Q)$ is equivalent to $\neg P \vee \neg Q$. Now $\neg(P \vee Q)$ is the negation of a disjunction, hence the conjunction of negations, so it is equivalent to $(\neg P \wedge \neg Q)$.

   Putting this together, we find that $\neg\left[(P \wedge Q) \vee (P \vee Q)\right]$ is equivalent to $(\neg P \vee \neg Q) \wedge (\neg P \wedge \neg Q)$.

2. Let us be a little less wordy.

   The negation of $(P \wedge Q) \wedge (P \vee Q)$ is equivalent to $\neg(P \wedge Q) \vee \neg(P \vee Q)$, which is equivalent to $(\neg P \vee \neg Q) \vee (\neg P \wedge \neg Q)$, which we may rewrite as $\neg P \vee \neg Q \vee (\neg P \wedge \neg Q)$.

3. The negation of $(P \wedge Q) \vee (R \wedge S)$ is $(\neg P \vee \neg Q) \wedge (\neg R \vee \neg S)$.
4. The negation of $(P \vee \neg Q) \wedge (\neg R \vee S)$ is $(\neg P \wedge Q) \vee (R \wedge \neg S)$.

Solution of Exercise I.15.

1. Let us compute the negation of $(P \wedge Q) \Rightarrow R$. This is the negation of an implication, and we know that the negation of $A \Rightarrow B$ is equivalent to $A \wedge \neg B$. So the desired negation is equivalent to $P \wedge Q \wedge \neg R$.
2. $\neg\left[(P \Rightarrow Q) \vee R\right]$ is equivalent to $\neg(P \Rightarrow Q) \wedge \neg R$, which is equivalent to $(P \wedge \neg Q) \wedge \neg R$, which may be rewritten $P \wedge \neg Q \wedge \neg R$.
3. The negation of $P \Rightarrow (Q \Leftrightarrow R)$ is $P \wedge \left[(Q \wedge \neg R) \vee (R \wedge \neg Q)\right]$.

Solution of Exercise I.17.

1. We first translate into symbols, manipulate the symbolic expressions, and translate back into English. The sentence "When it rains or snow, I avoid kangaroos and read Lewis Carroll" can be written $(R \vee S) \Rightarrow (AK \wedge RLC)$.

   Now we compute the negation - it is the negation of an implication, and we remember that $\neg((R \vee S) \Rightarrow (AK \wedge RLC))$ is equivalent to $(R \vee S) \wedge \neg(AK \wedge RLC)$.

   We simplify using De Morgan's laws: $(R \vee S) \wedge \neg(AK \wedge RLC)$ is equivalent to $(R \vee S) \wedge (\neg AK \vee \neg RLC)$. We are pleased with this formula which runs in English:

   > "It rains or snow, but I don't avoid kangaroos or don't read Lewis Carroll."

2. The negation of "Tarski shaves Gödel if and only if Gödel shaves Tarski." is "Tarski shaves Gödel but Gödel doesn't shave Tarski, [mark a pause here] or Gödel shaves Tarski but Tarski doesn't shave Gödel".

   You may use "and" instead of "but" since we are writing in English.

I.1.5 Misc manipulations

Solution of Exercise I.19. The answers are:

prop.	$P \Rightarrow (Q \Rightarrow R)$	$(P \Rightarrow Q) \Rightarrow R$	$(P \Rightarrow Q) \Rightarrow (R \Rightarrow S)$
negation	$P \wedge \neg(Q \Rightarrow R)$	$(P \Rightarrow Q) \wedge \neg R$	$(P \Rightarrow Q) \wedge \neg(R \Rightarrow S)$
converse	$(Q \Rightarrow R) \Rightarrow P$	$R \Rightarrow (P \Rightarrow Q)$	$(R \Rightarrow S) \Rightarrow (P \Rightarrow Q)$
contrap.	$\neg(Q \Rightarrow R) \Rightarrow \neg P$	$\neg R \Rightarrow \neg(P \Rightarrow Q)$	$\neg(R \Rightarrow S) \Rightarrow \neg(P \Rightarrow Q)$

Solution of Exercise I.20. The propositions in question are precisely the negations, converses, and contrapositives of the expressions of Exercise I.19.

The answers are

1. $\neg P \vee \neg Q \vee R$
2. $(P \wedge \neg Q) \vee R$
3. $(P \wedge \neg Q) \vee \neg R \vee S$
4. $P \wedge Q \wedge \neg R$
5. $(\neg P \wedge \neg R) \vee (Q \wedge \neg R)$
6. $(\neg P \wedge R \wedge \neg S) \vee (Q \wedge R \wedge \neg S)$
7. $(Q \wedge \neg R) \vee P$
8. $\neg R \vee \neg P \vee Q$
9. $(R \wedge \neg S) \vee \neg P \vee Q$
10. $\neg Q \vee R \vee \neg P$
11. $R \vee (P \wedge \neg Q)$
12. $\neg R \vee S \vee (P \wedge \neg Q)$

Let us explain a non-trivial one, say $(P \Rightarrow Q) \wedge \neg R$.

We know that $P \Rightarrow Q$ is equivalent to $\neg P \vee Q$. Hence $(P \Rightarrow Q) \wedge \neg R$ is equivalent to $(\neg P \vee Q) \wedge \neg R$. The latter is not of the required form, so we use distributivity, and therefore $(P \Rightarrow Q) \wedge \neg R$ is equivalent to $(\neg P \wedge \neg R) \vee (Q \wedge \neg R)$.

Solution of Exercise I.22.

1. $(P \vee Q) \Rightarrow \neg R$ is successively equivalent to its contrapositive (Properties I.2.36) $R \Rightarrow \neg(P \vee Q)$, then using De Morgan's law (Properties I.2.23) to $R \Rightarrow (\neg P \wedge \neg Q)$.

2. $\neg[P \vee \neg(Q \Rightarrow R)]$ is successively equivalent to $\neg P \wedge (Q \Rightarrow R)$, then by definition of an implication to $\neg P \wedge (\neg Q \vee R)$, then to $(\neg P \wedge \neg Q) \vee (\neg P \wedge R)$ by distributivity.

I.2 Exercises involving quantifiers

I.2.1 Easy translations

Solution of Exercise I.24.

1. $\forall x \in \mathbb{R}, \exists n \in \mathbb{N}, \forall y \in \mathbb{R}, |y| > n \Rightarrow |y| > |x|$ reads in English:

   > "For any x in R, there exists n in N **such that** for all y in R, if the absolute value of y is greater than n then the absolute value of y is greater than the absolute value of x."

2. $\exists n \in \mathbb{N}, \forall k \in \mathbb{N}, \exists \ell \in \mathbb{N}, k = n \cdot \ell$ reads:

   > "There is a natural number n **such that** for any natural number k there is a natural number ℓ **satisfying** k equals n times ℓ."

   $n = 1$ has the desired property (and is actually the only such number).

3. $\exists n \in \mathbb{Z}, \forall x \in \mathbb{R}, |x| < n \Rightarrow \exists y \in \mathbb{R}, 0 = 1$ reads:

   > "There is an integer n **such that** for any real x, if the absolute value of x is less than n then there is a real y **with** $0 = 1$."

   If $n = 0$, for instance, then $|x|$ cannot be less than n. So the implication "$|x| < n \Rightarrow \exists y \in \mathbb{R}, 0 = 1$" holds, regardless of $x \in \mathbb{R}$.

Solution of Exercise I.25.

1. This is worth remembering. A number is called *even* if 2 divides it, *odd* otherwise. A number is odd if and only if it is an even integer plus 1. Hence we have the propositions expressing respectively that n is even/odd:

   $$\begin{array}{ll} E(n): & \text{“}\exists k \in \mathbb{N}, n = 2k\text{”}, \\ O(n): & \text{“}\exists k \in \mathbb{N}, n = 2k+1\text{”} \end{array}$$

   The translation would then be:

   $$(\exists n \in \mathbb{N}, \exists k \in \mathbb{N}, n = 2k) \wedge (\exists n \in \mathbb{N}, \exists k \in \mathbb{N}, n = 2k+1)\,.$$

   Though this makes sense, it is not very wise to write it that way. If we wanted to make one sentence, with four quantifiers (quantifiy once and for all, and then state properties), we would get a conflict between the names. Hence we should prefer:

$$\exists n \in \mathbb{N}, \exists m \in \mathbb{N}, \exists k \in \mathbb{N}, \exists \ell \in \mathbb{N}, n = 2k \wedge m = 2\ell + 1.$$

Remark. Another formulation might be:

$$O(n) : \text{“}\neg(\exists k \in \mathbb{N}, n = 2k)\text{”}.$$

As one may not keep negations in front of quantifiers, we rewrite it as

$$\forall k \in \mathbb{N}, n \neq 2k.$$

Hence the translation (after suitable renaming) would be:

$$\exists n \in \mathbb{N}, \exists m \in \mathbb{N}, [(\exists k \in \mathbb{N}, n = 2k) \wedge (\forall k \in \mathbb{N}, m \neq 2k)]$$

2. $\forall x \in \mathbb{R}, \exists n \in \mathbb{N}, n > x$.
3. The translation might seem straightforward: $\exists x \in \mathbb{R}, \neg(\exists y \in \mathbb{R}, x = y^2)$.

   As mentioned above, it is customary not to keep negations in front of quantifiers. Hence the answer should be: $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x \neq y^2$.

   Caution! Insanities such as $\nexists \sqrt{x}$ are meaningless. If $\sqrt{x}$ does not exist, how come you mention it? Furthermore, $\nexists$ is strictly forbidden.

Solution of Exercise I.26.

1. The sentence may go in English:

   > “For all positive ε [pronounce “epsilon”], there exists an integer n_0 such that for any integer n, if n is greater than or equal to n_0 then the absolute value of u_n minus ℓ is smaller than ε.”

   Remark. Using “If. . . then” instead of “implies” after long quantifications is recommended.

2. The negation of the proposed expression is:

$$\exists \varepsilon > 0, \forall n_0 \in \mathbb{N}, \exists n \in \mathbb{N}, n \geq n_0 \wedge |u_n - \ell| \geq \varepsilon.$$

3. A translation into English of the latter is:

   > “There exists a positive real number ε such that for any integer n_0, there exists an integer n such that n is greater than or equal to n_0 but the absolute value of u_n minus ℓ is greater than or equal to ε.”

Solution of Exercise I.28.

1. The negation of the suggested property is:

$$\exists \varepsilon > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0, |u_n - \ell| \geq \varepsilon,$$

   which goes in English:

   > "There exist a positive real number epsilon and an integer n_0 such that for any integer n greater than or equal to n_0, the absolute value of u_n minus ℓ is smaller than epsilon."
   > [Or: "...such that for any integer n, if n is greater than or equal to n_0 then the absolute value..."]

2. In English, our property reads:

   > "For any positive real number epsilon and any integer n_0, there exists an integer n greater than or equal to n_0 such that the absolute value of u_n minus ℓ is smaller than epsilon",

   the negation of which is:

   > "There exist a positive real number epsilon and an integer n_0 such that all integers n greater than or equal to n_0 satisfy that the absolute value of u_n minus ℓ is greater than or equal to epsilon."

   Check consistency!

I.2.2 Abstract translations

Solution of Exercise I.29. $\exists! x \in A, P(x)$ stands for

$$\exists x \in A, (P(x) \wedge \forall y \in A, P(y) \Rightarrow x = y)$$

So the negation is successively equivalent to

$$\begin{array}{lcccccc}
\neg\exists x \in A, & (P(x) & \wedge & \forall y \in A, & P(y) & \Rightarrow & x = y) \\
\forall x \in A, & \neg(P(x) & \wedge & \forall y \in A, & P(y) & \Rightarrow & x = y) \\
\forall x \in A, & (\neg P(x) & \vee & \neg\forall y \in A, & P(y) & \Rightarrow & x = y) \\
\forall x \in A, & (\neg P(x) & \vee & \exists y \in A, & \neg(P(y) & \Rightarrow & x = y)) \\
\forall x \in A, & (\neg P(x) & \vee & \exists y \in A, & \neg P(y) & \wedge & x \neq y)
\end{array}$$

which is the desired negation.

Remark. Another approach is possible. The proposition $\exists! x \in A, P(x)$ means that there is a unique x satisfying P. It can fail for two reasons: if there are no x at all satisfying P, or if there are at least two. The first is written "$\forall x \in A, \neg P(x)$", and the second "$\exists x \in A, \exists y \in A, P(x) \wedge P(y) \wedge x \neq y$". So the negation of $\exists! x \in A, P(x)$ may also be written:

$$(\forall x \in A, \neg P(x)) \vee (\exists x \in A, \exists y \in A, P(x) \wedge P(y) \wedge x \neq y)$$

As an exercise, check that the two answers we provided are equivalent.

Solution of Exercise I.30. We just adapt from what "$\exists!$" stands for. Check that the following meets our requirements:

$$\exists x \in A, \exists y \in A, \{P(x) \wedge P(y) \wedge x \neq y \wedge \forall z \in A, [P(z) \Rightarrow (z = x \vee z = y)]\}.$$

Caution! Do not forget to claim that x and y are not the same!

I.2.3 Around functions

Solution of Exercise I.33.

1. "f has a limit at a" goes:

$$\exists \ell \in \mathbb{R}, \forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - \ell| < \varepsilon.$$

2. "f has a limit everywhere" goes:

$$\forall a \in \mathbb{R}, \exists \ell \in \mathbb{R}, \forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - \ell| < \varepsilon.$$

Solution of Exercise I.34.

1.
   - f is continuous at a if:

     for any positive epsilon there exists a positive delta such that for any real number x, if the absolute value of x minus a is smaller than delta, then the absolute value of f of x minus f of a is smaller than epsilon.

   - f is uniformly continuous on $\mathbb{R}$ if:

     for any positive epsilon there exists a positive delta such that for any real numbers x and y, if the absolute value of x minus y is smaller than delta, then the absolute value of f of x minus f of y is smaller than epsilon.

2. "f is continuous on $\mathbb{R}$" may be written:

$$\forall a \in \mathbb{R}, \forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

3.
   - The negation of "f is continuous at a" is:

$$\exists \varepsilon > 0, \forall \delta > 0, \exists x \in \mathbb{R}, |x - a| < \delta \wedge |f(x) - f(a)| \geq \varepsilon.$$

   - The negation of "f is continuous on $\mathbb{R}$" is:

$$\exists a \in \mathbb{R}, \exists \varepsilon > 0, \forall \delta > 0, \exists x \in \mathbb{R}, |x - a| < \delta \wedge |f(x) - f(a)| \geq \varepsilon.$$

- The negation of "f is uniformly continuous on $\mathbb{R}$" is:

$$\exists \varepsilon > 0, \forall \delta > 0, \exists x \in \mathbb{R}, \exists y \in \mathbb{R}, |x - y| < \delta \wedge |f(x) - f(y)| \geq \varepsilon.$$

4. - Hence "f is *not* continuous at a" goes:

   > there exists a positive epsilon such that for any positive delta, there exists a real number x such that the absolute value of x minus a is less than delta but the absolute value of f of x minus f of a is greater than or equal to epsilon.

   - "f is *not* continuous on $\mathbb{R}$" goes:

   > there exists a real number a and a positive real number epsilon such that for any positive delta, there exists a real number x such that the absolute value of x minus a is less than delta but the absolute value of f of x minus f of a is greater than or equal to epsilon.

   - "f is *not* uniformly continuous on $\mathbb{R}$" goes:

   > there exists a positive epsilon such that for any positive delta, there exist reals number x and y such that the absolute value of x minus y is less than delta but the absolute value of f of x minus f of y is greater than or equal to epsilon.

Solution of Exercise I.35.

1. The function f is differentiable at a if:

$$\exists \ell \in \mathbb{R}, \forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R} \setminus \{a\}, |x - a| < \delta \Rightarrow |\tau_{f,a}(x) - \ell| < \varepsilon.$$

   [$\mathbb{R} \setminus \{a\}$ stands for the set of all real numbers but a. Indeed, $\tau_{f,a}(x)$ was not defined for the value $x = a$. This is just for the sake of rigor, and was not the point of the exercise. You may read $\mathbb{R}$ if you prefer.]

   This reads in English:

   > "There exists a real number ℓ such that for any positive real number epsilon, there is a positive number delta such that for any real x different from a, if the absolute value of x minus a is less than delta, then the absolute value of tau f a of x minus ℓ is less than epsilon."

2. The function f is differentiable on $\mathbb{R}$ if:

$$\forall a \in \mathbb{R}, \exists \ell \in \mathbb{R}, \forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R} \setminus \{a\}, |x - a| < \delta \Rightarrow |\tau_{f,a}(x) - \ell| < \varepsilon,$$

   which stands for:

> "For any real number a, there exists a real number ℓ such that for any positive real number epsilon, there is a positive number delta such that for any real x different from a, if the absolute value of x minus a is less than delta, then the absolute value of tau f a of x minus ℓ is less than epsilon."

3. The function is *not* differentiable on $\mathbb{R}$ if:

   $$\exists a \in \mathbb{R}.\forall \ell \in \mathbb{R}, \exists \varepsilon > 0, \forall \delta > 0, \exists x \in \mathbb{R} \setminus \{a\}, |x - a| < \delta \wedge |\tau_{f,a}(x) - \ell| \geq \varepsilon,$$

   and this reads:

   > "There is real number a such that for any real number ℓ, there exists a positive epsilon such that for any positive delta, there is a real number x different from a and such that the absolute value of x minus a is less than delta *but* the absolute value of tau f a of x minus ℓ is greater than or equal to epsilon."

Solution of Exercise I.36.

1. "f is a constant function" may be written: "$\exists c \in \mathbb{R}, \forall x \in \mathbb{R}, f(x) = c$", which reads

   > "there exists a real c such that for any x in R, f of x equals c."

2. Hence "f is not a constant function" may go: "$\forall c \in \mathbb{R}, \exists x \in \mathbb{R}, f(x) \neq c$", which reads

   > "for any real c, there exists x in R such that f of x is not c."

   Caution! "$\neg(\exists c \in \mathbb{R}, \forall x \in \mathbb{R}, f(x) = c)$" is *not* an answer, since we have to move negations after the quantifiers.

3. "f is increasing" is expressed by: "$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x \leq y \Rightarrow f(x) \leq f(y)$", which reads:

   > "for any real numbers x and y, if x is less than or equal to y, then f of x is less than or equal to f of y".

   Caution! Perhaps f is not differentiable, so mentioning f' is irrelevant.

4. "f is not increasing" may go: "$\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x \leq y \wedge f(x) > f(y)$", which could be read:

   > "there exist real numbers x and y with x less than or equal to y but f of x bigger than f of y".

   Caution! "decreasing" is not the negation of "increasing".

   $\sin x$, for instance, is neither increasing nor decreasing!

5. "f is increasing or decreasing" goes:

$$\begin{array}{ll} & (\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x \leq y \Rightarrow f(x) \leq f(y)) \\ \vee & (\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x \leq y \Rightarrow f(x) \geq f(y)) \end{array}$$

   which reads:

   > EITHER for any real numbers x and y, if x is less than or equal to y, then f of x is less than or equal to f of y, OR for any real numbers x and y, if x is less than or equal to y, then f of x is greater than or equal to f of y."

   Here "either" serves as a mere delimiter for long disjunctions.

   Caution! The proposition

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, [(x \leq y \Rightarrow f(x) \leq f(y)) \vee (x \leq y \Rightarrow f(x) \geq f(y))]$$

   is *always true*; it is *not* the answer.

6. "f is bounded above" if $\exists M \in \mathbb{R}, \forall x \in \mathbb{R}, f(x) < M$, which reads

   > "there is a real number M such that for any real number x, f of x is smaller than M".

Exercises of Chapter II

II.1 Basic proofs

Solution of Exercise II.1.

1. Let us prove $P \Rightarrow P \vee Q$. The statement is an implication; we assume the first term and prove the second. Assume P. Then P holds, and so does $P \vee Q$. Hence P implies $P \vee Q$. We have proved $P \Rightarrow P \vee Q$.

2. Let us prove $P \wedge Q \Rightarrow P$. Assume $P \wedge Q$. Then P holds. In particular, $P \wedge Q \Rightarrow P$ is true.

3. Let us prove $[(P \Rightarrow Q) \wedge P] \Rightarrow Q$. Assume $(P \Rightarrow Q) \wedge P$. Then P holds, and so does $P \Rightarrow Q$. It follows that Q holds. Assuming $(P \Rightarrow Q) \wedge P$ we could prove Q. Hence $[(P \Rightarrow Q) \wedge P] \Rightarrow Q$ is proved.

4. Let us prove $(P \Rightarrow \neg P) \Rightarrow \neg P$. Assume $P \Rightarrow \neg P$; we want to prove $\neg P$. There are two cases. If P is true, then as by assumption $P \Rightarrow \neg P$, we deduce $\neg P$, and the conclusion is proved in the first case. The second case is when P is false, i.e. $\neg P$ is true, and the second case is trivial. So in either case $\neg P$ is true. Hence $P \Rightarrow \neg P$ does imply $\neg P$. We have therefore proved $(P \Rightarrow \neg P) \Rightarrow \neg P$.

Solution of Exercise II.2. We assume that $\sqrt{3}$ is rational, and prove a contradiction. If $\sqrt{3}$ is rational, then it can be written $\sqrt{3} = \frac{a}{b}$, where a and b are coprime integers.

Raising to the square and multiplying, we find $a^2 = 2b^2$. In particular, 3 divides a^2. But this implies that 3 divides a. Hence 9 divides $a^2 = 3b^2$, and therefore 3 divides b^2. Now this implies that 3 divides b. So we have found that 3 divides both a and b, which can't be coprime. This is a contradiction.

Hence $\sqrt{3}$ is not a rational number.

Solution of Exercise II.3. We assume that $\sqrt[3]{5}$ is rational, and prove a contradiction. If $\sqrt[3]{5}$ is rational, then it can be written $\sqrt[3]{5} = \frac{a}{b}$, where a and b are coprime integers.

Raising to the cube and multiplying, we find $a^3 = 5b^3$. In particular, 5 divides a^3. But this implies that 5 divides a. Hence 125 divides $a^3 = 5b^3$, and therefore 25 divides b^3. Now this implies that 5 divides b. So we have found that 5 divides both a and b, which can't be coprime. This is a contradiction.

Hence $\sqrt[3]{5}$ is not a rational number.

II.2 Proofs involving quantifiers

II.2.1 Baby proofs

Solution of Exercise II.4.

1. In order to prove a conjunction, we prove each term. In order to prove an existentially quantified proposition, it is a good idea to provide an example. So all we have to do is find an example of an even number, and an example of an odd number. So our proof may be:

   > "Let $n = 2$, $k = 1$, $m = 3$, and $\ell = 1$. It is clear that these numbers meet our conditions." QED

2. In order to prove a universally quantified formula $\forall x \in A, P(x)$, we pick any element a in A and prove that $P(a)$ holds, regardless of any extra assumption on a. So we must start with some $a \in \mathbb{R}$ (but since we are not allowed to chose which, we certainly can't tell which it is, and must call it a, x, or y, or whatever). This is done with the ritual words: "Let $a \in \mathbb{R}$."

   Now we have our a (don't feel confused if you don't know which it is ; we will work with it anyway), and we want to prove $P(a)$, that is we aim at proving $\exists n \in \mathbb{N}, n > a$. This is an existential formula.

   In order to prove this existential formula we need a suitable n. Here we can't build a concrete example (since a is unknown), but all we have to do is find a natural number greater than a. If a is negative, this is easily done. If not, then we can think of the integer part of a (often denoted $\lfloor a \rfloor$). This is the biggest integer smaller than or equal to a. So it is clear that $\lfloor a \rfloor + 1$ is bigger than a. We now write our proof:

> "Let $a \in \mathbb{R}$. If a is negative, then $1 > a$. If a is non-negative, then $\lfloor a \rfloor + 1 \in \mathbb{N}$ and $\lfloor a \rfloor + 1 > a$. So in either case we have proved that there is $n \in \mathbb{N}$ such that $n > a$. Since this is true for any real number a, we are done." QED

3. We must prove an existential formula, an example is a good idea. Of course -1 will be a correct example, but you must convince the reader that it has no square root. In order to do this, you must pick any $y \in \mathbb{R}$, and prove that y^2 can't be 1. A proof may be:

   > "Consider $x = -1$. Let $y \in \mathbb{R}$. Then $y^2 \geq 0$, and hence $y^2 \neq -1$. This is true for any real number y, so -1 satisfies $\forall y \in \mathbb{R}, x \neq y^2$. Hence we have proved $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x \neq y^2$." QED

Solution of Exercise II.5. Let m and n be integers. We assume that m is odd and n is even, and we prove that $m+n$ is odd. Since m is odd, there is an integer k such that $m = 2k + 1$. On the other hand, since n is even, there is an integer ℓ such that $n = 2\ell$. Hence we have that $m + n = (2k + 1) + 2\ell = 2(k + \ell) + 1$, and therefore $m + n$ is odd.

Solution of Exercise II.6.

1. (a) An English translation of P is:

   For any real number x, there is a real number y such that x equals y plus 1.

   (b) We prove P. Let x be a real number. Let $y = x - 1$. Since $x = y + 1$, we have proved $\exists y \in \mathbb{R}, x = y + 1$. This is true regardless of x, and therefore $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x = y + 1$ holds.

2. (a) An English translation of Q is:

   For all real numbers y, there is a real number x such that x equals y plus 1.

   (b) We prove that the negation of Q is true. We observe that $\neg Q$ is equivalent to $\forall y \in \mathbb{R}, \exists x \in R, x \neq y + 1$. We prove the latter.

   Let $y \in \mathbb{R}$. We prove that $\exists x \in R, x \neq y + 1$. Indeed, let $x = y$. Then $x \neq y + 1$. So we have found an x meeting our requirements, that is $\exists x \in R, x \neq y + 1$. Now this is true for al real numbers y, and therefore $\forall y \in \mathbb{R}, \exists x \in R, x \neq y + 1$ holds. Hence $\neg Q$ is true, and Q is false.

Solution of Exercise II.7.

1. We prove that between two distinct integers there is always a real number.

   Let m be an integer, and let n be an integer distinct from m. Let $x = \frac{m+n}{2}$. It is clear that the real number x lies between m and n. So such a number exists. Since this is true regardless of m and n provided they are distinct, we have proved the statement.

2. This is still true with real numbers, and the same proof works. It is an interesting property of the real line: between two distinct points there is always one point. (The same is true with rational numbers.)

II.2.2 Abstract proofs

Solution of Exercise II.9.

1. We prove $[\exists x \in A, \forall y \in A, R(x,y)] \Rightarrow [\forall y \in A, \exists x \in A, R(x,y)]$.

   In order to do that, we assume $[\exists x \in A, \forall y \in A, R(x,y)]$ and we prove $[\forall y \in A, \exists x \in A, R(x,y)]$. By assumption, there is $x \in A$ such that $\forall y \in A, R(x,y)$; let x_0 be such an element, that is let $x_0 \in A$ be such that:

   $$\forall y \in A, R(x_0, y).$$

   We now prove $\forall y \in A, \exists x \in A, R(x,y)$. Let $y \in A$. We show that $\exists x \in A, R(x,y)$. Let $x = x_0$. Then $R(x_0, y)$ holds, and in particular there is an x such that $R(x,y)$. So we have proved $\exists x \in A, R(x,y)$. This being true for any y in A, we have proved $\forall y \in A, \exists x \in A, R(x,y)$.

   Assuming $[\exists x \in A, \forall y \in A, R(x,y)]$, we proved $[\forall y \in A, \exists x \in A, R(x,y)]$. Hence $[\exists x \in A, \forall y \in A, R(x,y)] \Rightarrow [\forall y \in A, \exists x \in A, R(x,y)]$ holds.

2. The converse of S is:

   $$[\forall y \in A, \exists x \in A, R(x,y)] \Rightarrow [\exists x \in A, \forall y \in A, R(x,y)].$$

3. The converse of S does not always hold: indeed, consider $A = \mathbb{R}$, and $R(x,y)$ be "$x = y+1$". Clearly the assumption of the converse of S holds, but the conclusion does not. Hence the converse of S does not hold.

4. A special case in which the converse of S holds anyway is when A is a set with only one element, say a.

   In this case, "$\forall y \in A, \exists x \in A, R(x,y)$" is equivalent to "$R(a,a)$", and "$\forall y \in A, \exists x \in A, R(x,y)$" is equivalent to "$R(a,a)$".

   In particular, both S and its converse are true in this case.

Solution of Exercise II.10.

1. A translation is:

   $$\exists x \in A, [S(x) \Rightarrow (\forall y \in A, S(y))].$$

2. There are two cases. Either everyone smokes in the classroom, or somebody does not. In the first case, then the conclusion $\forall y \in A, S(y)$ will be true. In the second, we shall just take an x such that the hypothesis $S(x)$ does not hold. So we have our proof, which runs:

We first assume $\forall y \in A, S(y)$. We then pick any $a \in A$. Since $\forall y \in A, S(y)$, it is the case that $S(a) \Rightarrow (\forall y \in A, S(y))$. Hence a meets our requirements, so $\exists x \in A, [S(x) \Rightarrow (\forall y \in A, S(y))]$.

We now assume the negation, that is $\exists y \in A, \neg S(y)$. We let a be such a y. Then $S(a)$ does not hold, so the implication $S(a) \Rightarrow (\forall y \in A, S(y))$ is true. Hence a meets our requirements, and we have proved $\exists x \in A, [S(x) \Rightarrow (\forall y \in A, S(y))]$ again.

As both cases have been dealt with, we are done.

3. It is no longer true when A is the empty set. Indeed, a formula that is existentially quantified over the empty set cannot be true.

II.2.3 More technical

Solution of Exercise II.13.

Caution! The solution of this exercise has been detailed to its maximum clumsiness. It might seem long, but it is actually shorter. Not all intermediate explainations are required in order to provide a convincing proof, but this is what you should write if you are not an expert.

Remark. Notice that before stating anything with symbols, we use a couple of words to say if it is a proposition that we have already proved/that we assume/that we are trying to prove. You should do that in order not to get confused when reading your scratchwork.

1. Let f be a real function. We assume that f is uniformly continuous on $\mathbb{R}$, and we prove that it is continuous on $\mathbb{R}$.

   In order to do that, we prove that f is continuous at every $a \in \mathbb{R}$. So let $a \in \mathbb{R}$, and we prove continuity of f at a.

   Let $\varepsilon > 0$, we look for δ such that

   $$\forall x \in \mathbb{R}, |x-a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

   Since f is uniformly continuous on $\mathbb{R}$, we know that

   $$\exists \delta > 0, \forall x \in \mathbb{R}, \forall y \in \mathbb{R}, |x-y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon.$$

   We take such a δ. Now since $a \in \mathbb{R}$, we have that

   $$\forall x \in \mathbb{R}, |x-a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon,$$

   so δ has the desired property. Hence

   $$\exists \delta > 0, \forall x \in \mathbb{R}, |x-a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon,$$

   and since we have made no assumption on ε, we have actually proved

   $$\forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, |x-a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon,$$

   which is the definition of continuity at a.

2. Let $f(x) = cx + d$, we prove that f is uniformly continuous on $\mathbb{R}$.

   - We first assume that $c = 0$. Then $\forall x \in \mathbb{R}, f(x) = d$, so f is a constant function. Let $\varepsilon > 0$, and take any positive δ, for example $\delta = 1$. Let x and y be real numbers. If $|x-y| < \delta$, then $|f(x)-f(y)| = |d-d| = 0 < \varepsilon$. Hence such a δ exists, and we have proved that

     $$\exists \delta > 0, \forall x \in \mathbb{R}, \forall y \in \mathbb{R}, |y - x| < \delta \Rightarrow |f(y) - f(x)| < \varepsilon.$$

     Since our proof does not depend on ε, we have shown:

     $$\forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, \forall y \in \mathbb{R}, |y - x| < \delta \Rightarrow |f(y) - f(x)| < \varepsilon,$$

     hence f is uniformly continuous on $\mathbb{R}$, this ends the first case.

   - We now assume that $c \neq 0$.
     Let $\varepsilon > 0$; we are looking for $\delta > 0$ such that:

     $$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, |y - x| < \delta \Rightarrow |f(y) - f(x)| < \varepsilon.$$

     Let $\delta = \frac{\varepsilon}{|c|}$. Whenever x and y are real numbers such that $|x-y| < \delta$, it is clear that $f(x) - f(y)| = |cx - cy| < c\delta = \varepsilon$. So far we have proved that

     $$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, |y - x| < \delta \Rightarrow |f(y) - f(x)| < \varepsilon,$$

     hence our δ meets the requirements. So it the case that

     $$\exists \delta > 0, \forall x \in \mathbb{R}, \forall y \in \mathbb{R}, |y - x| < \delta \Rightarrow |f(y) - f(x)| < \varepsilon.$$

     Since this is true for any positive ε, we have even:

     $$\forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, \forall y \in \mathbb{R}, |y - x| < \delta \Rightarrow |f(y) - f(x)| < \varepsilon,$$

     hence f is uniformly continuous on $\mathbb{R}$, and this ends the second case.

   Since these two cases represent all possibilities, we are done and we may conclude that f is uniformly continuous.

3. We prove that the function $x \mapsto x^2$ is continuous on $\mathbb{R}$, that is we prove:

   $$\forall a \in \mathbb{R}, \forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

   For this we let $a \in \mathbb{R}$ and $\varepsilon > 0$. Let $\delta = \min\left(\sqrt{\frac{\varepsilon}{2}}, \frac{\varepsilon}{4|a|+1}\right)$.

   Now whenever x is a real number satisfying $|x - a| < \delta$, we have that $|x^2 - a^2| < \varepsilon$ [if you don't see why, admit it].

   Hence we have proved

   $$\forall x \in \mathbb{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon,$$

so our δ fulfils the condition, and this means that

$$\exists\delta > 0, \forall x \in \mathbb{R}, |x-a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

Since this is true for any positive ε, we conclude that

$$\forall\varepsilon > 0, \exists\delta > 0, \forall x \in \mathbb{R}, |x-a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

Now the latter is true for any real number a, hence

$$\forall a \in \mathbb{R}, \forall\varepsilon > 0, \exists\delta > 0, \forall x \in \mathbb{R}, |x-a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon,$$

and this is the definition of the fact that f is continuous on $\mathbb{R}$.

4. We now prove that the function $x \mapsto x^2$ is *not* uniformly continuous on $\mathbb{R}$, that is we prove:

$$\exists\varepsilon > 0, \forall\delta > 0, \exists x \in \mathbb{R}, \exists y \in \mathbb{R}, |x-y| < \delta \wedge |f(x) - f(y)| \geq \varepsilon.$$

[We have to find some ε in $\mathbb{R}_+^*$ such that

$$\forall\delta > 0, \exists x \in \mathbb{R}, \exists y \in \mathbb{R}, |x-y| < \delta \wedge |f(x) - f(y)| \geq \varepsilon$$

Intuition is required. The condition means that how close x and y may be, this does not ensure that $f(x) - f(y)$ is smaller than ε. Indeed when x and y are very close but very large, the difference $y^2 - x^2$ can be big.]

We let $\varepsilon = 1$ and we prove that it is suitable. Indeed, let δ be any positive real number. Since if δ is not small there is not much to do, we may assume that $0 < \delta < 1$.

We now let $x = \frac{1}{\delta}$ and $y = \frac{1}{\delta} + \frac{\delta}{2}$. It is then the case that $|x-y| < \delta$. On the other hand, one finds that

$$|x^2 - y^2| = (y-x).(y+x) \geq \frac{\delta}{2}.2x = x \geq 1 = \varepsilon.$$

Hence x and y fulfill our requirements, and we have proved that:

$$\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, |x-y| < \delta \wedge |f(x) - f(y)| \geq \varepsilon.$$

Now our proof works for any $\delta > 0$, and therefore we have that:

$$\forall\delta > 0, \exists x \in \mathbb{R}, \exists y \in \mathbb{R}, |x-y| < \delta \wedge |f(x) - f(y)| \geq \varepsilon.$$

Our ε fits to the condition, therefore

$$\exists\varepsilon > 0, \forall\delta > 0, \exists x \in \mathbb{R}, \exists y \in \mathbb{R}, |x-y| < \delta \wedge |f(x) - f(y)| \geq \varepsilon.$$

This is the statement that f is *not* uniformly continuous.

II.3 Exercises on Induction Proofs

Solution of Exercise II.14. For any integer n, let $P(n)$ be the property:

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

We prove by induction: $\forall n \in \mathbb{N}, P(n)$.

- Basic step/Initialization: We prove that $P(1)$ holds. Indeed, when $n = 1$,

  $$\sum_{k=1}^{1} k^2 = 1 = \frac{1(1+1)(2 \cdot 1 + 1)}{6},$$

  so $P(1)$ is true.

- Inductive step/Heredity: We now prove the inductive step. Let $n \in \mathbb{N}$. We assume $P(n)$, and we prove $P(n+1)$.

  We have

  $$\sum_{k=1}^{n+1} k^2 = \left(\sum_{k=1}^{n} k^2\right) + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2$$

  because of $P(n)$, and therefore

  $$\sum_{k=1}^{n+1} k^2 = (n+1) \cdot \left(\frac{n(2n+1)}{6} + (n+1)\right) = (n+1) \cdot \frac{2n^2+7n+6}{6}.$$

  Now we can factor $2n^2+7n+6$ as $(n+2)(2n+3)$ [either compute roots and factor, or bluff because this is what you have to find eventually]. Therefore

  $$\begin{aligned} \sum_{k=1}^{n+1} k^2 &= (n+1) \cdot \frac{2n^2+7n+6}{6} = (n+1) \cdot \frac{(n+2)(2n+3)}{6} \\ &= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}, \end{aligned}$$

  hence $P(n+1)$ is true.

  So we have proved that $P(n) \Rightarrow P(n+1)$, and since this is true for any n, we have thus proved $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$. This concludes the heredity step.

We have established that $P(1)$ holds, and that for any $n \in \mathbb{N}$, $P(n) \Rightarrow P(n+1)$. By induction, we have proved that for any $n \in \mathbb{N}$, $P(n)$ holds.

Caution! $P(n)$ is a proposition, not a number!

Solution of Exercise II.15. For any integer n, let $P(n)$ be the property:

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

We prove by induction: $\forall n \in \mathbb{N}, P(n)$.

- Basic step/Initialization: We prove that $P(1)$ holds. Indeed, when $n = 1$,

  $$\sum_{k=1}^{1} k^3 = 1 = \left(\frac{1(1+1)}{2}\right)^2,$$

  so $P(1)$ is true.

- Inductive step/Heredity: We now prove the inductive step. Let $n \in \mathbb{N}$. We assume $P(n)$, and we prove $P(n+1)$.

  We have that

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

  because of $P(n)$, and therefore

  $$\sum_{k=1}^{n+1} k^3 = (n+1)^2.\left(\frac{n^2}{4} + (n+1)\right) = (n+1)^2.\frac{n^2+4n+4}{4}.$$

  Now we can factorize $n^2 + 4n + 4$ as $(n+2)^2)$, and we get

  $$\sum_{k=1}^{n+1} k^3 = (n+1)^2.\frac{n^2+4n+4}{4} = (n+1)^2.\frac{(n+2)^2}{4},$$

  hence $P(n+1)$ is true.

  So we have proved that $P(n) \Rightarrow P(n+1)$, and since this is true for any n, we have thus proved $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$. This concludes the heredity step.

We have established that $P(1)$ holds, and that for any $n \in \mathbb{N}$, $P(n) \Rightarrow P(n+1)$. By induction, we have proved that for any $n \in \mathbb{N}$, $P(n)$ holds.

Solution of Exercise II.16. Obviously something has gone wrong. The initial step is clearly correct, and the use of induction seems appropriate. So the problem must come from the inductive step.

So, assuming that the property does hold for n roses, we take a parterre of $n+1$ roses one of which is red, and we read the proof. It is the case indeed that we can assume r_1 to be red, no trick red. As a consequence, all the first

n roses (of the sub-parterre $B = \{r_1, \ldots, r_n\}$) *are* red. This is the inductive hypothesis, and *we cannot refute it* since it is the methodology of an induction proof to assume it. No trap this far.

Now we turn to the subparterre $C = \{r_2, \ldots, r_{n+1}\}$. Since we have assumed $P(n)$, it is the case that if one of the n roses of C is red, then all roses in C are red. But on the other hand, nothing proves that one of the roses in C is actually red! Of course is n is large, it is intuitive that B and C must meet, but it is *not the case if* $n = 2$!

Hence when $n = 2$, there is no reason to affirm that there is a red rose in C. And therefore, though it is the case that

$$\forall n \geq 2, P(n) \Rightarrow P(n+1),$$

it is not true that $P(1) \Rightarrow P(2)$. This missing inductive step ruins the proof.

Exercises of Chapter III

III.1 Very easy exercises

III.1.1 Finite sets

Solution of Exercise III.2.

1. The three elements of $\{1, \{2\}, \{\{3\}, 4\}\}$ are:

   the number 1, the set with one element $\{2\}$, and the set with two elements $\{\{3\}, 4\}$.

2. $P(\{a, b, c\}) \setminus (P(\{a, b\}) \cup P(\{a, c\})) = \{\{a, b, c\}\}$

3. The three elements of $\{\emptyset, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}, \{\{\{\emptyset\}\}\}\}$ are:

   the empty set $\emptyset$, the set with three elements $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$, and the set with one element $\{\{\{\emptyset\}\}\}$.

Solution of Exercise III.3.

1. $(\{a, \{a, b\}, b\} \cup \{a, \{a\}\}) \setminus \{\{b\}\} = \{a, b, \{a\}, \{a, b\}\}$.

2. $\{a, b\} \cup P(\{a\}) = \{a, b, \emptyset, \{a\}\}$, so $\{a, \{a, b\}\} \cap (\{a, b\} \cup P(\{a\})) = \{a\}$.

3. $P(\{a\}) \cup P(\{b\}) = \{\emptyset, \{a\}, \{b\}\}$.

4. $P(\{a, b\}) \setminus P(\{b\}) = \{\{a\}, \{a, b\}\}$.

Solution of Exercise III.5.

1. $P(P(\emptyset)) = P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.
2. $P(P(\{\emptyset\})) = P(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$.
3. We use that if A has n elements, then $P(A)$ has 2^n elements. This yields that $P(P(P(P(\emptyset))))$ has 16 elements.
4. $P(P(P(\{\emptyset\})))$ has 16 elements.

III.1.2 The algebra of sets

Solution of Exercise III.8. We assume $A \subseteq B$ and $B \subseteq C$, and we prove $A \subseteq C$. So let $x \in A$; we must prove $x \in C$. Since $x \in A$ and $A \subseteq B$, we get $x \in B$. But since $B \subseteq C$, we deduce $x \in C$. Because this is true regardless of $x \in A$, we have proved $A \subseteq C$.

Solution of Exercise III.9.

1. Let us prove the equality of sets $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; in order to do that, we prove two inclusions.

    - Let $x \in A \cap (B \cup C)$, we must prove $x \in (A \cap B) \cup (A \cap C)$. Since $x \in A \cap (B \cup C)$, we have $x \in A$ and also $x \in B \cup C$. There are two cases:

        - If $x \in B$, then we have $x \in A \cap B \subseteq (A \cap B) \cup (A \cup C)$ because of the properties of union. So $x \in (A \cap B) \cup (A \cup C)$.
        - If $x \in C$, we argue similarly.

      So in both cases, $x \in (A \cap B) \cup (A \cup C)$. Now this is true for all $x \in A \cap (B \cup C)$, and therefore $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

    - We now prove the converse inclusion. Let $x \in (A \cap B) \cup (A \cap C)$; we must prove $x \in A \cap (B \cup C)$. Since $x \in (A \cap B) \cup (A \cap C)$, we have $x \in A \cap B$ or $x \in A \cap C$. Again there are two cases.

        - If $x \in A \cap B$, then $x \in A$ and $x \in B \subseteq B \cup C$, so $x \in A \cap (B \cup C)$.
        - If $x \in A \cap C$, we argue similarly.

      So in both cases, $x \in A \cap (B \cup C)$. Now this is true for all $x \in (A \cap B) \cup (A \cap C)$, and therefore $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

    Both inclusions being proved, equality holds.

2. Very much alike (hence pretty annoying).

Solution of Exercise III.10. Let A, B be sets. We are looking for a property equivalent to $A \setminus B = A$. A picture suggests that $A \setminus B$ doesn't remove anything from A when A and B are disjoint. So we conjecture:

$$A \setminus B = A \Leftrightarrow A \cap B = \emptyset.$$

Let us prove this.

Assume $A \setminus B = A$. We want to prove that $A \cap B = \emptyset$. So let $x \in A \cap B$. Since $x \in A$ and $A = A \setminus B$, we find $x \in A \setminus B$. On the other hand, $x \in B$, and this is impossible. Therefore there is no such x, that is $A \cap B = \emptyset$.

Now assume $A \cap B = \emptyset$, and let us prove that $A \setminus B = A$. The inclusion $A \setminus B \subseteq A$ always hold, so it only remains to prove that $A \subseteq A \setminus B$. So let $x \in A$. Since $A \cap B = \emptyset$, it follows that $x \notin B$. In particular, $x \in A \setminus B$. Because this does not depend on $x \in A$, we have $A \subseteq A \setminus B$, whence equality.

The equivalence is now proved.

Solution of Exercise III.11.

1. Let $A = C = \emptyset$ and B be any non-empty set. Then we have $A \subseteq C$ but it is not the case that ($A \subseteq B$ and $B \subseteq C$).

2. Let $A = \{1, 2\}$, $B = \{1\}$, and $C = \{2\}$. Then $B \cup C = A$, whence $A \setminus (B \cup C) = \emptyset$. But $A \setminus B \neq \emptyset$, so $(A \setminus B) \cup (A \setminus C) \neq \emptyset$.

Solution of Exercise III.15.

1. The picture is left to the reader.

2. Let us prove that $A \triangle B = B \triangle A$.

   By definition, $A \triangle B = (A \setminus B) \cup (B \setminus A)$ which by the commutativity of union is equal to $(B \setminus A) \cup (A \setminus B) = B \triangle A$.

3. Let us prove that $(A \cap B) \cap (A \triangle B) = \emptyset$.

   Let $x \in (A \cap B) \cap (A \triangle B)$. Then $x_i n A \cap B$ and $x \in A \triangle B$. By definition, $A \triangle B = (A \setminus B) \cup (B \setminus A)$, so there are two cases.

   (a) If $x \in A \setminus B$, then we have $x \in A \cap B \subseteq B$, whence $x \in B$, and also $x \in A \setminus B$, whence $x \notin B$. This is impossible.
   (b) If $x \in B \setminus A$, we argue similarly.

   A contradiction is reached in both cases. Hence $(A \cap B) \cap (A \triangle B) = \emptyset$.

4. Let us prove that $(A \cap B) \cup (A \triangle B) = A \cup B$.

   We first prove $(A \cap B) \cup (A \triangle B) \subseteq A \cup B$. We already know that $A \cap B \subseteq A \subseteq A \cup B$. Now from the definition it is obvious that $A \triangle B \subseteq A \cup B$. So $(A \cap B) \cup (A \triangle B) \subseteq A \cup B$.

   We now prove that $A \cup B \subseteq (A \cap B) \cup (A \triangle B)$. Let $x \in A \cup B$. There are three cases.

   - If $x \in A \cap B$, then $x \in (A \cap B) \cup (A \triangle B)$.
   - If $x \in A \setminus B$, then $x \in A \triangle B \subseteq (A \cap B) \cup (A \triangle B)$.
   - If $x \in B \setminus A$, we argue as in the second case.

These three cases cover all possibilities; therefore $A \cup B \subseteq (A \cap B) \cup (A \triangle B)$. Equality is proved.

5. Let us prove that $A \triangle B = \emptyset$ if and only if $A = B$.

   Assume that $A \triangle B = \emptyset$, and let us prove that $A = B$. So let $x \in A$; we shall prove that $x \in B$. If $x \notin B$, then $x \in A \setminus B \subseteq A \triangle B$ which is empty; this is impossible. Therefore $x \in B$. So far we have proved $A \subseteq B$; the other inclusion is obtained similarly. So $A = B$.

   Now assume that $A = B$, and let us prove that $A \triangle B = \emptyset$. This is obvious from the definition.

6. Let us prove that $A \triangle B \subseteq A$ if and only if $B \subseteq A$.

   Assume that $A \triangle B \subseteq A$, and let us prove $B \subseteq A$. So let $x \in B$; we shall prove $x \in A$. If not, then $x \in B \setminus A$, whence $x \in A \triangle B \subseteq A$. We then get $x \in A$, which is a contradiction. So $x \in A$ after all. This proves $B \subseteq A$.

   Now assume that $B \subseteq A$, and let us prove that $A \triangle B \subseteq A$. This is easily seen from the definition.

7. Let us prove that $A \subseteq A \triangle B$ if and only if $A \cap B = \emptyset$.

   Assume that $A \subseteq A \triangle B$, and let us prove that $A \cap B = \emptyset$. So let $x \in A \cap B$. Then $x \in A \subseteq A \triangle B$; in particular $x \in (A \cap B) \cap (A \triangle B)$. Question 3. implies $x \in \emptyset$, that is there is no such x. This proves $A \cap B = \emptyset$.

   Assume now that $A \cap B = \emptyset$, and let us prove that $A \subseteq A \triangle B$. Question (iv) tells us that $(A \cap B) \cup (A \triangle B) = A \cup B$. Here $A \cap B = \emptyset$, so $A \cup B = (A \cap B) \cup (A \triangle B) = A \triangle B$. Now we get $A \subseteq A \cup B = A \triangle B$.

8. Questions 6. and 7. together with properties of intersection imply the equivalence $A \triangle B = A \Leftrightarrow B = \emptyset$.

III.1.3 The power set operation

Solution of Exercise III.16. Let A and B be sets.

1. Let us prove that $P(A \cap B) = P(A) \cap P(B)$.

   Let $E \in P(A \cap B)$. By definition, $E \subseteq A \cap B$. Since $A \cap B \subseteq A$, we find $E \subseteq A$, that is $E \in P(A)$. We obtain $E \in P(B)$ similarly. Hence $E \in P(A) \cap P(B)$; and this shows $P(A \cap B) \subseteq P(A) \cap P(B)$.

   Now let $E \in P(A) \cap P(B)$. This means $E \subseteq A$ and $E \subseteq B$. So $E \subseteq A \cap B$, that is $E \in P(A \cap B)$.

   This concludes the proof.

2. Let us prove that $P(A) \cup P(B) \subseteq P(A \cup B)$.

   Let $E \in P(A) \cup P(B)$. So $E \in P(A)$, or $E \in P(B)$. We assume we are in the first case, the other is similar. So we assume $E \in P(A)$, that is $E \subseteq A$. Since $A \subseteq A \cup B$, we have $E \subseteq A \cup B$, that is $E \in P(A \cup B)$.

3. In general, $P(A) \cup P(B) \subsetneq P(A \cup B)$. Consider any two sets A and B such that none is a subset of the other. Then $A \cup B \in P(A \cup B)$, but $A \cup B \notin P(A)$, and $A \cup B \notin P(B)$!

Solution of Exercise III.17. First assume $A \subseteq B$; let $E \in P(A)$. This means $E \subseteq A$, and since $A \subseteq B$ we get $E \subseteq B$, that is $E \in P(B)$. Hence $P(A) \subseteq P(B)$.

We now prove the converse; assume $P(A) \subseteq P(B)$. Since $A \subseteq A$, we have $A \in P(A) \subseteq P(B)$, so $A \in P(B)$, which means $A \subseteq B$. The other implication is proved. QED

Solution of Exercise III.18.

1. With sets of numbers, this clearly can't work. So we think with sets of sets. For example, $A = \{\emptyset\}$ has as unique element $\emptyset$, which is of course a subset of it!

2. We need to think a bit more. But making guesses in the same direction, we end up with $B = \{\emptyset, \{\emptyset\}\}$. This set has two elements, namely $\emptyset$ and $\{\emptyset\}$. Now $P(B) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$ so clearly $B \subseteq P(B)$, and we are done.

3. We can think of iterating the process. So we consider for each $n \in \mathbb{N}$ the set A_n with 1 element : $A_n = \underbrace{\{\ldots\{}_{n \text{ times}}\emptyset\underbrace{\}\ldots\}}_{n \text{ times}}$.

   Now for any $n \in \mathbb{N}$ we define a set E_n having $n+1$ elements : $E_n = \{A_0 \ldots, A_n\}$. Let E be the union of all sets E_n for $n \in \mathbb{N}$. Check that for any $n \in \mathbb{N}$, $A_n \in E \cap P(E)$.

Solution of Exercise III.19. For any non-negative integer n, let $P(n)$ be the property:

> whenever a set A has n elements, then $P(A)$ has 2^n elements.

Let us prove by induction: $\forall n \in \mathbb{N} \cup \{0\}, P(n)$.

- $P(0)$ holds because $\emptyset$ is the only set with 0 elements and $P(\emptyset) = \{\emptyset\}$ has exactly $1 = 2^0$ elements.

- Now fix $n \in \mathbb{N} \cup \{0\}$; assume $P(n)$; let's prove $P(n+1)$. So we let A be a set having $n+1$ elements. Let $a \in A$ be some fixed element, and let $B = A \setminus \{a\}$. So $\{a\}$ and B form a partition of A.

  Subsets of A divide into two categories:

  – Subsets not having a as an element. These are just subsets of B, so there are 2^n of them (by our inductive hypothesis).

  – Subsets having a as an element. Any such subset C is entirely defined by $C \setminus \{a\}$, that is by a subset of B again. So there are 2^n of them (by induction again).

So we have $2^n + 2^n = 2^{n+1}$ subsets of A. Our set A with 2^{n+1} elements is arbitrary; this proves $P(n+1)$.

- By induction, we have $\forall n \in \mathbb{N} \cup \{0\}, P(n)$.

III.2 Understanding set notation

Solution of Exercise III.20.

1. $(\mathbb{N} \cap \mathbb{Z}) \cup (\mathbb{Q} \cap \mathbb{R}) = \mathbb{Q}$.
2. $\{x \in \mathbb{R} : x^2 = 2\} \cap \mathbb{Q}$.
3. $\{n \in \mathbb{Z}, n^2 \in \mathbb{N}\} \cap \mathbb{Q}\}$.
4. $[0,1] \cap [\frac{1}{2}, 2)$.
5. $[0,1] \cup [\frac{1}{2}, 2)$.
6. $\{1,2\}$.
7. $(\mathbb{Z} \setminus \mathbb{R}) \cup (\mathbb{Q} \setminus \mathbb{N}) = \mathbb{Q} \setminus \mathbb{N}$.
8. $(\mathbb{Q} \cap \{\sqrt{2}, \{1,-1\}, 2, -2\}) \setminus \mathbb{N}$ $= \{-2\}$.

Solution of Exercise III.21.

1. $\{x \in \mathbb{R} : x^2 = 2\} \cap \mathbb{Q} = \emptyset$.
2. $\{x \in \mathbb{R} : x^2 = -1\} = \emptyset$.
3. $[0,1] \cap [\frac{1}{2}, 2) = [\frac{1}{2}, 1]$.
4. $[0,1] \cup [\frac{1}{2}, 2) = [0, 2)$.
5. $\{x \in \mathbb{R} : x \geq 0\}$.
6. $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : xy = 1\} = \mathbb{R}\setminus\{0\}$.
7. $$\bigcup_{x>0} (-x, x] = \mathbb{R}.$$
8. $$\bigcap_{x>0} (-x, x) = \mathbb{R}.$$
9. $\mathbb{R}$.
10. $$\bigcup_{x>0} (-x, x] \setminus (0, x) = \mathbb{R}.$$

Solution of Exercise III.22.

1. $\{x \in \mathbb{R} : x^2 = 1\} \cup \{x^2 : x \in \mathbb{R}\} = \mathbb{R}_{\geq 0} \cup \{-1\}$.
2. $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : xy = 2\} = \mathbb{R} \setminus \{0\}$.
3. $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : y = 0\} = \mathbb{R}$.
4. $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : x = 0\} = \{0\}$.
5. $\{n \in \mathbb{N} : \exists q \in \mathbb{Q} : n = q\} = \mathbb{N}$
6. $\{q \in \mathbb{Q} : \exists n \in \mathbb{N} : n = q\} = \mathbb{N}$

Solution of Exercise III.23.

1.
$$\bigcap_{n\in\mathbb{N}}[-n,+\infty)=[-1,+\infty)$$

2.
$$\bigcap_{n\in\mathbb{N}}[n,+\infty)=\emptyset$$

3.
$$\bigcup_{n\in\mathbb{N}}\{x\in\mathbb{R}:n\leq x<n+1\}=[1,\infty)$$

4.
$$\bigcup_{x\in\mathbb{R}}\bigcap_{y\in\mathbb{R}}\{z\in\mathbb{R}:z=y\}=\bigcup_{x\in\mathbb{R}}\bigcap_{y\in\mathbb{R}}\{y\}=\bigcup_{x\in\mathbb{R}}\emptyset=\emptyset$$

5.
$$\bigcup_{0<a<1}(-a,a)=(-1,1)$$

6.
$$\bigcap_{a>1}(-a,a)=[-1,1]$$

Solution of Exercise III.24.

1.
$$\bigcup_{0<x<1}(0,x)=(0,1)$$

3.
$$\bigcap_{0<x<1}(0,x)=\emptyset$$

2.
$$\bigcup_{0<x<1}[0,x]=[0,1)$$

4.
$$\bigcap_{0<x<1}[0,x]=\{0\}$$

5.
$$(\{0,1\}\times\{0,1\})\setminus(\{(a,a):a\in\{0,1\}\})=\{(0,1),(1,0)\}$$

6.
$$\mathbb{R}\times\mathbb{R}\setminus(\ (\mathbb{R}_{\geq 0}\times\mathbb{R}_{<0})\cup(\mathbb{R}_{<0}\times\mathbb{R}_{<0})\cup(\mathbb{R}_{<0}\times\mathbb{R}_{\geq 0})\ )=\mathbb{R}_{\geq 0}\times\mathbb{R}_{\geq 0}$$

7.
$$\{x\in\mathbb{R}:\forall y\in[0,1]:x>y\}=(1,\infty)$$

8.
$$\{x\in\mathbb{R}:\exists y\in[0,1]:x>y\}=(0,\infty)$$

9.
$$\{x\in\emptyset:x\in\mathbb{R}\}=\emptyset$$

10.
$$\{x\in\{\emptyset\}:x\in\mathbb{R}\}=\emptyset$$

Solution of Exercise III.25.

1. $P(P(\emptyset)) \setminus P(\emptyset) = \{\{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$
2. $$\bigcup_{x\in[-1,1]} (-|x|, x) = (-1, 1)$$
3. $$\bigcup_{n\in N} (-n, 0) = (-\infty, 0)$$
4. $$\bigcap_{q\in\mathbb{Q}} [-|q|, 0] = \{0\}$$
5. $\{x \in \mathbb{R} : \forall y \in \mathbb{R} : x > y\} = \emptyset$
6. $\{x \in \mathbb{R} : \forall y \in \mathbb{R} : x > |y|\} = \emptyset$
7. $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : x > |y|\} = (0, \infty)$
8. $\{x \in \mathbb{R} : x > 0 \vee x < 0\} = \mathbb{R} \setminus \{0\}$
9. $\cos([0, \pi]) = [-1, 1]$
10. $\{x : x \in \{y \in \mathbb{R} : y^2 = 1\}\} = \{-1, 1\}$
11. $\{x^2 : x \in \{y \in R : y = 1\}\} = \{1\}$
12. $$\bigcup_{q\in\{x\in\mathbb{Q}:x>0\}} (-q, q) = \mathbb{R}$$
13. $$\bigcup_{q\in\mathbb{Q}} (q - 1, q + 1) = \mathbb{R}$$
14. $$\bigcup_{n\in 2\mathbb{Z}} (n - 1, n + 1) = \mathbb{R} \setminus \{k \in \mathbb{Z} : k \text{ is odd}\}$$

Solution of Exercise III.26.

1. The definition reads: "the set of all products k times n, where k ranges over $\mathbb{Z}$", or anything having the same meaning.
2. Since $4\mathbb{Z} \subseteq 2\mathbb{Z}$, we find $2\mathbb{Z} \cup 4\mathbb{Z} = 2\mathbb{Z}$.
3. Similarly, $2\mathbb{Z} \cap 4\mathbb{Z} = 4\mathbb{Z}$.
4. $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ is clear.

If you want to think: define the sum of two sets A and B as $\{a + b : (a, b) \in A \times B\}$. Then $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$. Actually (and this is called Bézout's theorem), whenever $m, n \in \mathbb{Z}$, one has $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ where d is the greatest common divisor of m and n.

This means that the notion of common divisor does not require a prime factorization result to have a meaning.

III.3 Infinite operations and partitions

III.3.1 Infinite operations

Solution of Exercise III.31.

1. (a) Let us prove that
$$\bigcup_{i\in I} A_i \subseteq \bigcup_{j\in J} A_j.$$
Let $x \in \bigcup_{i\in I} A_i$. By definition, there is an $i \in I$ such that $x \in A_i$. Since $I \subseteq J$, we have $i \in J$. This means that $x \in \bigcup_{j\in J} A_j$.

   (b) Let us prove that
$$\bigcap_{j\in J} A_j \subseteq \bigcap_{i\in I} A_j.$$
Let $x \in \bigcap_{j\in J} A_j$; we want to prove that $x \in \bigcap_{i\in I} A_i$. Let $i \in I$. Since $I \subseteq J$, we have $i \in J$. So by definition, $x \in A_i$. Since this is true regardless of $i \in I$, we find $x \in \bigcap_{i\in I} A_i$.

2. Let $I = \{1\}$, and $J = \{1, 2\}$.

   Let $A_1 = \{\pi\}$, $A_2 = \{\pi, \sqrt{2}\}$. Then $A_1 \cap A_2 = A_1$ but $A_1 \subsetneq A_1 \cup A_2 = A_2$.

   Now let $A_1 = \{\pi\}$ and $A_2 = \emptyset$. Then $A_1 \cup A_2 = A_1$ but $A_1 \cap A_2 = \emptyset \subsetneq A_1$.

III.3.2 Partititions

Solution of Exercise III.32. Let $A = \{a, b, c, d, e\}$.

- Let $A_1 = \{a\}$, $A_2 = \{b\}$, $A_3 = \{c, d, e\}$. The family $\{A_i : i \in \{1, 2, 3\}\}$ is a partition of A into three sets that have an odd number of elements.
- Now consider $B_1 = \{b\}$, $A_2 = \{c\}$, $A_3 = \{a, d, e\}$. The family $\{B_i : i \in \{1, 2, 3\}\}$ is another partition of A into three sets that have an odd number of elements.

Solution of Exercise III.33.

1. Let n, m be distinct non-negative integers; let us check that $X_n \cap X_m$ is empty. Indeed, no set A_i can have at the same time n and m elements. This proves $n \neq m \Rightarrow X_n \cap X_m = \emptyset$, i.e. the "pairwise disjoint" clause.
2. Now let $i \in I$ and let's check A_i is in some of the X_n. Let n be the number of elements of A_i. Then it is clear that $A_i \in X_n$. This proves the "covering" clause. We are done.

Solution of Exercise III.34. Let $\Sigma = \{B \cap A_j, j \in J\}$.

- First notice that by definition of J, no $B \cap A_j$ is empty for $j \in J$. Hence Σ is a collection of non-empty subsets of B.
- We prove covering. Let $b \in B$. As $B \subseteq A$, we know $b \in A$. As Π is a partition of A, there is $i \in I$ such that $b \in A_i$. It follows that $B \cap A_i \neq \emptyset$. In particular $i \in J$ and $b \in B \cap A_i$ with $B \cap A_i \in \Sigma$, so elements of Σ do cover B.

- We prove disjunction. Let $j, k \in J$ be distinct. Then $(B \cap A_j) \cap (B \cap A_k) \subseteq A_j \cap A_k = \emptyset$. Hence elements of Σ are disjoint.

By definition, Σ is a partition of B.

III.4 Very conceptual

Solution of Exercise III.35.

1. We find $N_4 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$.

2. If you don't see why this is true, I am sorry for you.

3. Let's prove by induction that for all $n \in \mathbb{N} \cup \{0\}$, $N_n \subseteq P(N_n)$.

   This clearly holds for 0, because $N_0 = \emptyset$. So assume it holds for some fixed n and let's prove it for $n+1$. Let $x \in N_{n+1}$; we want to prove $x \subseteq N_{n+1}$. The assumption $x \in N_{n+1}$ and the definition $N_{n+1} = N_n \cup \{N_n\}$ lead to two cases:

   - If $x \in N_n$, then by our inductive assumption we have $x \subseteq N_n$.
   - If $x \in \{N_n\}$, we have $x = N_n$.

   In either case $x \subseteq N_n$, which by the previous question is a subset of N_{n+1}. So $x \subset N_{n+1}$; this is true regardless of $x \in N_{n+1}$ so $N_{n+1} \subseteq P(N_{n+1}$. This concludes the heredity step; by induction, we are done.

4. Let's prove by induction that $\forall n \in \mathbb{N} \cup \{0\}, N_n \notin N_n$.

   This clearly holds for $n = 0$ since $N_0 = \emptyset$. Now let's assume it holds for a certain n and prove it for $n+1$. Assume $N_{n+1} \in N_{n+1}$; let's prove a contradiction. Since $N_{n+1} = N_n \cup \{N_n\}$ by definition, $N_{n+1} \in N_{n+1}$ can hold in only two cases:

   - $N_{n+1} \in N_n$, which since $N_n \subseteq P(N_n)$ (previous question) implies $N_{n+1} \subseteq N_n$. In particular, $N_n \in N_{n+1}$ yields $N_n \in N_n$, against our inductive assumption.
   - $N_{n+1} \in \{N_n\}$, which means $N_{n+1} = N_n$. Now $N_{n+1} \in N_{n+1}$ but $N_n \notin N_n$ by our inductive assumption; this is a contradiction again.

   In either case we have reached a contradiction; this means that $N_{n+1} \in N_{n+1}$ cannot hold; i.e. $N_{n+1} \notin N_{n+1}$ is true. This concludes the heredity step, and by induction we are done.

5. Let us prove by induction that for all $n \in \mathbb{N} \cup \{0\}$, N_n has exactly n elements.

   This clearly holds for 0. Assume it does for some n; let's prove it for $n+1$. Since $N_{n+1} = N_n \cup \{N_n\}$, all we have to do is prove that N_n is not an element of N_n; we already did that. So N_{n+1} has $n+1$ elements indeed; etc.

6. Since $N_n \subseteq N_{n+1}$ always holds, a quick induction shows that

$$\forall n \in \mathbb{N} \cup \{0\}, \forall k \leq n, N_k \subseteq N_n.$$

In particular,

$$\bigcup_{k \leq n} N_k = N_n.$$

7. We want to prove

$$\forall n \in \mathbb{N} \cup \{0\}, \forall m \in \mathbb{N} \cup \{0\}, n \leq m \Rightarrow N_n \in P(N_m).$$

This is equivalent to

$$\forall m \in \mathbb{N} \cup \{0\}, \forall n \in \mathbb{N} \cup \{0\}, n \leq m \Rightarrow N_n \in P(N_m).$$

For any $m \in \mathbb{N} \cup \{0\}$, let $Q(m)$ be the property:

$$\forall n \in \mathbb{N} \cup \{0\}, n \leq m \Rightarrow N_n \in P(N_m).$$

Let us prove by induction on m that $Q(m)$ holds on $\mathbb{N} \cup \{0\}$.

- $Q(0)$ is the statement:

  $$\forall n \in \mathbb{N} \cup \{0\}, n \leq 0 \Rightarrow N_n \in P(\emptyset).$$

  Because of the restriction $n \leq 0$, this reduces to $\emptyset \in P(\emptyset)$, which is true. So $Q(0)$ holds.
- Let $m \in \mathbb{N} \cup \{0\}$ be such that $Q(m)$ holds; we want to prove $Q(m+1)$, i.e. we want to prove:

  $$\forall n \in \mathbb{N} \cup \{0\}, n \leq m+1 \Rightarrow N_n \in P(N_{m+1}).$$

  So we let $n \leq m+1$, and we prove $N_n \subseteq N_{m+1}$. There are two cases.
  - If $n \leq m$, then because $P(m)$ holds, we have $N_n \subseteq N_m$, which is itself a subset of N_{m+1}. So $N_n \subseteq N_{m+1}$.
  - If $n = m+1$, then there is not much to prove...

  So in either case, $N_n \subseteq N_{m+1}$ holds. This being true regardless of $n \leq m+1$, we find

  $$\forall n \in \mathbb{N} \cup \{0\}, n \leq m+1 \Rightarrow N_n \in P(N_{m+1}),$$

  that is $Q(m+1)$. This concludes the heredity step.
- By induction, we have proved that $Q(m)$ always holds, that is

  $$\forall n \in \mathbb{N} \cup \{0\}, \forall m \in \mathbb{N} \cup \{0\}, n \leq m \Rightarrow N_n \in P(N_m).$$

8. If you could understand the previous proof, you may want to try to adapt its techniques to the last question. Hope you enjoyed this exercise.

Exercises of Chapter IV

IV.1 Warm-up Exercises

Solution of Exercise IV.1.

1. Sending a real number x to its square does define a function from $\mathbb{R}$ to (for instance) $\mathbb{R}$.
2. Sending a real number to one of its real square roots is ambiguous, as positive real numbers have two *distinct* square roots. It does not define a function.
3. Sending a non-negative real number to one of its real square roots has the same problem. It does not define a function.
4. Sending any real number to the biggest integer not greater than it is a well-defined, unambiguous construction. It defines a function $\mathbb{R} \to \mathbb{Z}$.
5. Sending a real number x to the closest integer is non-ambiguous, except when there are *two* such integers, namely when x is of the form $k + \frac{1}{2}$ for $k \in \mathbb{Z}$. The construction defines a function $\mathbb{R} \setminus (\mathbb{Z} + \frac{1}{2}) \to \mathbb{Z}$.
6. Sending x to $\sin(\sqrt{(}-x^2))$ makes sense only for $x = 0$ (in which case it assumes the value 0). So it actually defines a function from $\{0\}$ to $\{0\}$.

Solution of Exercise IV.2.

1. The function $\mathcal{D}$ is *not* injective, as two distinct functions may have the same derivative. For instance, $\mathcal{D}(0) = 0 = \mathcal{D}(1)$, where 0 and 1 denote the constant functions equal to 0 (resp. 1).
2. The function $\mathcal{P}$ is injective. Let $f, g \in \mathcal{F}$ be two functions such that $\mathcal{P}(f) = \mathcal{P}(g)$. We want to show that $f = g$.

   By assumption,

   $$\mathcal{P}(f) = \int_0^x f(t)\mathrm{d}t = \mathcal{P}(g) = \int_0^x g(t)\mathrm{d}t$$

   Derivating, we find $f(x) = g(x)$ for all $x \in [0, 1]$, so $f = g$ as functions.

Remark. We know from Example IV.1.15 that $\mathcal{D} \circ \mathcal{P} = \mathrm{Id}_{\mathcal{F}}$, which is injective. So by Proposition IV.2.7, $\mathcal{P}$ must be injective.

Solution of Exercise IV.3.

1. The function $\mathcal{D}$ is surjective. Let $g \in \mathcal{F}$; we let f be any primitive of g ($\mathcal{P}(g)$ would do!). Then clearly $\mathcal{D}(f) = g$, so $\mathcal{D}$ is surjective.
2. The function $\mathcal{P}$ is not surjective: by definition, a function $\mathcal{P}(f)$ is a primitive vanishing at 0, and therefore $\mathcal{P}(f)(0) = 0$ for any f. So a function g not vanishing at 0 cannot be of the form $\mathcal{P}(f)$; for instance there is no $f \in \mathcal{F}$ such that $\mathcal{P}(f) = 1$ (the constant function 1).

Remark. We know from Example IV.1.15 that $\mathcal{D} \circ \mathcal{P} = \mathrm{Id}_{\mathcal{F}}$, which is surjective. So by Proposition IV.2.14, $\mathcal{D}$ must be surjective.

IV.2 Injections, Surjections and Bijections

Solution of Exercise IV.9.

1. Easy.
2. Both $\mathbb{Q}$ and $\mathbb{R} \setminus \mathbb{Q}$ are dense in $\mathbb{R}$, meaning that:
   - between any two real numbers, there is a rationnal number;
   - between any two real numbers, there is an irrationnal number.

   So if you want to draw $\chi_{\mathbb{Q}}$, it might look like two parallel lines.
3. Let us prove that $\Phi : P(E) \to 2^E$ is injective. So let $A, A' \in P(E)$ be such that $\Phi(A) = \Phi(A')$, and let us prove that $A = A'$.

   In order to prove $A \subseteq A'$, let $x \in A$. Using the characteristic function χ_A, we have by definition $\chi_A(x) = 1$. Now our assumption is $\Phi(A) = \Phi(A')$, that is $\chi_A = \chi_{A'}$. In particular, $\chi_{A'}(x) = 1$ too, meaning by definition $x \in A'$. Hence $A \subseteq A'$, and the other inclusion is similar. Therefore $A = A'$.
4. This one is not more difficult, but requires attention.

   Let us prove that $\Phi : P(E) \to 2^E$, that is, let us prove:

   $$\forall f \in 2^E, \exists A \in P(E), \Phi(A) = f.$$

   [Of course if you called your function f something like χ_A, you just cheated. What one has to prove is that any f is of the form χ_A indeed.]

   Let $f \in 2^E$, that is, let f be a function $E \to \{0, 1\}$. We try to find a subset $A \subseteq E$ such that $\Phi(A) = f$, that is $\chi_A = f$. Thinking ten minutes about the meaning of characteristic functions, you may come up with the following idea.

   Let $A = \{x \in E : f(x) = 1\} = f^{\langle -1 \rangle}(\{1\})$. Then $A \in P(E)$ and clearly, $\chi_A = f$. (If you think this is not obviously proved, prove it).

   So $\Phi(A) = f$, and Φ is surjective.
5. In particular, if E is finite with n elements, then there is a bijection between $P(E)$ and the set 2^E which has 2^n elements. This means that $P(E)$ has 2^n elements.

Solution of Exercise IV.10.

1. Let us prove that $\mathcal{C} : \mathbb{R} \to E'$ is injective; that is, let $a, a' \in \mathbb{R}$ be such that $\mathcal{C}(a) = \mathcal{C}(a')$, and let us prove $a = a'$.

   By definition, $\mathcal{C}(a) = C_a$ is the constant function $\mathbb{R} \to \mathbb{R}$ mapping any x to a.

   Our assumption is $C_a = C_{a'}$. Applying this real function to $0 \in \mathbb{R}$, we get $C_a(0) = a = C_{a'}(0) = a'$.

2. Proving that $\mathcal{C} : \mathbb{R} \to E'$ is not surjective amounts to proving that not all functions $\mathbb{R} \to \mathbb{R}$ are constant, something rather obvious.

3. You knew how to do this one. For example, C_1 is as required.

4. Let $\Phi : \mathbb{R} \to E''$ map a to ev_a. We want to prove that Φ is injective. So let $a, a' \in \mathbb{R}$ be such that $\Phi(a) = \Phi(a')$, and let us prove that $a = a'$.

   Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = (x - a)$. Then $f(a) = 0$, meaning $ev_a(f) = 0$. But our assumption $\Phi(a) = \Phi(a')$ reands $ev_a = ev_{a'}$, in particular $ev_{a'}(f) = ev_a(f) = 0$. So $f(a') = a' - a = 0$, and $a = a'$.

   [You could also do a contradiction proof using a function g not taking the same value at a and a' assuming they were distinct.]

5. Let us prove that Φ is not surjective, meaning that not all elements of E'' are evaluation maps. So we are trying to find some $F : E' \to \mathbb{R}$ such that $\forall a \in \mathbb{R}, F \neq ev_a$. Let for example

$$\mathbb{F} : \begin{array}{ccc} E' & \to & \mathbb{R} \\ f & \mapsto & f(0) + f(1) \end{array}.$$

   (So $F = ev_0 + ev_1$!)

   We want to prove that F is not in $\Phi(\mathbb{R})$. Let $a \in \mathbb{R}$. Let C_1 be as above. Then $F(C_1) = C_1(0) + C_1(1) = 1 + 1 = 2$, but $ev_a(C_1) = C_1(a) = 1$. So F and ev_a don't map C_1 to the same element of $\mathbb{R}$. In particular, $F \neq ev_a$.

   This is true for any $a \in \mathbb{R}$, proving that F can't be in $\Phi(\mathbb{R})$. Hence Φ is not surjective.

6. Abstract and easy (these adjectives do go along very well).

IV.3 Images and Preimages

Solution of Exercise IV.11.

1. $f(\mathbb{R}) = [0, \infty) = f(\mathbb{R}_{\geq 0}) = f(\mathbb{R}_{\leq 0})$; $\quad f([0, 1]) = [-1, 1] = f([-1, 1])$.

2. $f^{\langle -1 \rangle}(\mathbb{R}) = \mathbb{R} = f^{\langle -1 \rangle}(\mathbb{R}_{\geq 0})$; $\quad f^{\langle -1 \rangle}(\mathbb{R}_{\leq 0}) = f^{-1}(\{0\}) = \{0\}$,
   $f^{\langle -1 \rangle}([0, 1]) = f^{\langle -1 \rangle}([-1, 1]) = [-1, 1]$.

Solution of Exercise IV.12. Let f be the function from $P(\mathbb{N}) \setminus \{\emptyset\}$ to $\mathbb{N}$ taking any non-empty subset of $\mathbb{N}$ to its least element.

1. Let A be the set of all infinite sets of $\mathbb{N}$. Let B be the set of all finite, non-empty sets of $\mathbb{N}$. It is clear that $f(A) = f(B) = \mathbb{N}$.

2. $f^{\langle -1 \rangle}(\{1\}) = \{E \in P(N) : 1 \in E\}$.
   $f^{\langle -1 \rangle}(\{2\}) = \{E \in P(N) : 1 \notin E \wedge 2 \in E\}$.
   $f^{\langle -1 \rangle}(\{1, 2\}) = \{E \in P(N) : 1 \in E \vee 2 \in E\}$.

Solution of Exercise IV.14. Let $f : A \to B$ be a function.

1. Let $E \subseteq A$ be a subset of A. Let us prove that $E \subseteq f^{\langle -1 \rangle}(f(E))$.

   Let $e \in E$. We want to show that $e \in f^{\langle -1 \rangle}(f(E))$. By definition, this amounts to proving that $f(e) \in f(E)$, which is obvious since $e \in E$.

2. Here is an example of a function f and a subset $E \subseteq \operatorname{dom} f$ such that $E \subsetneq f^{\langle -1 \rangle}(f(E))$: consider the square function $f : \mathbb{R} \to \mathbb{R}$, and let $E = [0, 1]$. Then $f(E) = [0, 1]$, but $f^{\langle -1 \rangle}(f(E)) = [-1, 1]$ is bigger than E.

3. Let $F \subseteq B$ be a subset of B. Let us prove that $f(f^{\langle -1 \rangle}(F)) \subseteq F$.

   Let $y \in f(f^{\langle -1 \rangle}(F))$; we want to prove that $y \in F$. We know that $y \in f(f^{\langle -1 \rangle}(F))$, that is we know that there is $a \in f^{\langle -1 \rangle}(F)$ such that $y = f(a)$. Now since $a \in f^{\langle -1 \rangle}(F)$, we have $y = f(a) \in F$, which we wanted to prove.

4. Here is an example of a function f and a subset $F \subseteq \operatorname{cod} f$ such that $f(f^{\langle -1 \rangle}(F)) \subsetneq F$: consider the square function $f : \mathbb{R} \to \mathbb{R}$, and let $F = [-1, 1]$. Then $f^{\langle -1 \rangle}(F) = [-1, 1]$, but $f(f^{\langle -1 \rangle}(F)) = [0, 1]$ is smaller than F.

5. Let us prove that if f is injective, then for any $E \subseteq \operatorname{dom} f$, one has $E = f^{-1}(f(E))$.

   Assume f injective; by (1) all we have to do is prove that $f^{\langle -1 \rangle}(f(E)) \subseteq E$. So let $x \in f^{\langle -1 \rangle}(f(E))$; we want to prove that $x \in E$.

   Since $x \in f^{\langle -1 \rangle}(f(E))$, we know $f(x) \in f(E)$. This by definition means that there is $e \in E$ such that $f(x) = f(e)$. Now f being injective, we find $x = e \in E$.

6. Let us prove that if for any $E \subseteq \operatorname{dom} f$, one has $E = f^{\langle -1 \rangle}(f(E))$, then f is injective.

   Indeed, assume towards a contradiction that there are $x \neq x'$ in E such that $f(x) = f(x')$. Let $E = \{x\}$. Then $f(E) = \{f(x)\}$, and this implies $x' \in f^{\langle -1 \rangle}(f(E))$. This is a contradiction to $f^{\langle -1 \rangle}(f(E)) = E = \{x\}$.

   Hence we have proved that f is injective.

Solution of Exercise IV.15. Notice that for any subset $E \subseteq A$, $g(E) = f(E)$, where

- $g(E)$ means: the image of E *as an element of* $P(A)$ through the function g (that takes sets as arguments), and
- $f(E)$ means: the *image-set* of E as a subset of A through the function f.

1. Let us prove that f is injective if and only if g is.

   We first assume that f is injective, and prove that g is. Let $E, F \in P(A)$ be such that $E \neq F$; we prove that $g(E) \neq g(F)$. We may assume that there is $x \in E \setminus F$ (the other case will be similar). Since $x \in E$, we have $f(x) \in f(E)$. We assume towards a contradiction that $f(x) \in f(F)$. Then by definition, there is an element $x' \in F$ such that $f(x) = f(x')$. Now since f is injective, we get $x = x' \in F$, a contradiction to the definition of x. This proves that $f(x) \notin f(F)$. Since $f(x) \in f(E)$, we have shown that $f(E) \neq f(F)$.

Let us now assume that g is injective, and prove that f is. Let $a, a' \in A$ be distinct. Then the sets $\{a\}$ and $\{a'\}$ are distinct; in particular, $\{f(a\} = g(\{a\}) \neq g(\{a'\}) = \{f(a')\}$. So $\{f(a)\} \neq \{f(a')\}$, and this proves $f(a) \neq f(a')$.

2. Let us prove that f is surjective if and only if g is.

   We first assume that f is surjective, and prove that g is. Let $F \in P(B)$ be a subset of B. Let $E = \{x \in A : f(x) \in F\}$. Clearly $E \in P(A)$. By definition, if $x \in E$, then $f(x) \in F$; this means $g(E) = f(E) \subseteq F$. On the other hand, let $y \in F$. Since f is surjective, there is $x \in A$ such that $y = f(x)$. As $y \in F$, by definition $x \in E$. So $F \subseteq f(E) = g(E)$. This proves $F = g(E)$. So g is surjective.

   Let us now assume that g is surjective, and prove that f is. Let $y \in B$. Since g is surjective, there exists $E \in P(A)$ such that $g(E) = \{y\}$. Since $\{y\}$ is not empty, $E \neq \emptyset$. So let $x \in E$. By definition, $f(x) \in g(E) = \{y\}$, hence $f(x) = y$, and f is surjective.

Index of Notions

List of Lectures