Mathematical Writing

Adrien Deloro

Fall 2023

Chapter I — Stating Things

In this chapter we learn how to write and read formal mathematical statements. Always bear in mind that *symbols are for stating, not for proving.*

Chapter Goals. Learn mathematical language:

- Determine if a sentence is a proposition or not.
- Translate from English to symbols and back.
- Find the truth table of a (non-quantified) proposition.
- Determine whether two propositions are equivalent.
- Manipulate quantified propositions.
- Compute the negation of a given proposition.

Main Notions. Proposition, Truth value, Truth table, Connective, Equivalence, Quantifier.

We first discuss *propositions* and *truth values* (§ 1). Using the *propositional connectives* $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ (§ 2), we can build *compound propositions* (§ 3); some are *equivalent.* Another step in complexity, where real mathematics begin, is by adding the *quantifiers* $\exists, \forall$ (§ 4); the method of truth tables no longer applies. Quantified propositions beg for special rules and manipulations (§ 5).

1 Propositions

One has to start somewhere and our notion of a proposition will remain non-formal. (A second course in mathematical logic would return to the topic, which is not our current business.)

1.1 Informal discussion

Not every sentence* is subject to logical treatment. Let us consider a few examples. phrase, énoncé

1.1.1. Example.

Sentence	Context-independent meaning?	True/False?
$0 = 0$	Y	T
I am here.	N	/
$0 = 1$.	Y	F
Cats lay eggs.	Y	F
$x = 0$	N	/
Hence $2 > 0$.	N	/

A sentence with a precise meaning is the same as a statement* which is either true or false, not depending on any context. affirmation

1.1.2. Remark.

- Though 'I am here' sounds true to any person saying it, its contents depend on the person saying it. So this sentence does not have a precise meaning.
- Of course $0 \neq 1$. But the sentence '$0 = 1$' makes good sense, even though we know it is false. We understand the meaning of the statement.
- '$x = 0$' is not a proposition. Who is x? The meaning depends on something undefined. (Later it will be called a 'proposition depending on a variable'.)
- The sentence starting with 'Hence' is obviously part of something else (maybe a proof), but it is not a *statement*.

The sentences that sound relevant for our purposes are those whose meaning is precise. They are the sentences one could describe as either 'true' or 'false'.

1.2 Informal definition

1.2.1. Definition (proposition, truth value)**.** A proposition is a sentence which is either true or false. 'True' or 'False' is the truth value* of the proposition. valeur de vérité

('False' is a truth value.)

1.2.2. Notation.

- Any of the following stands for *true*: T, 1, $\top$†. \top
- Any of the following stands for *false* : F, 0, $\bot$†. \bot

1.2.3. Remark (a digression)**.** Consider the sentence:

'Every even number is a sum of two prime numbers.'

This is a proposition as it has a precise meaning. It also has a truth value. But nobody knows if it is true or false. (This famous statement is known as the *Goldbach Conjecture*. More in general, a *conjecture* is a mathematical proposition whose truth value we do not know, viz. an open problem.)

Hence our (informal) definition of a proposition actually relies on something very hard to determine in practice, its truth value. Which is also why there is still research in mathematics, but that is another story. . .

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.

1.2.4. Remark. For the sake of pedagogy I sometimes use sentences which are not propositions, but which provide striking, easily remembered examples.

1.2.5. Remark (alternative phrases)**.** Let P be a proposition (take for example $0 = 0$, or take $0 = 1$; it does not matter).

- Phrases* meaning that P is true: expression(s)

  • 'P'; • 'P is true'; • 'P holds'; • 'it is the case that P'; • 'we have P'.

- Phrases meaning that P is false:

  • 'P is not true'; • 'P is false'; • 'P does not hold'; • 'it is not the case that P'.

Notice that in mathematics, to say '$0 = 0$' is the same as saying 'it is true that $0 = 0$'. So be careful with what you say.

1.2.6. Example.
— *Does the proposition 'cats lay eggs' hold?*
— *No, it is not the case that cats lay eggs.*
Pay attention to quotation marks*. guillemets

2 Connectives

We usually assemble basic propositions using words such as 'and' or 'or'. This is done in mathematics too.

We shall introduce five connectives : not (§ 2.1), and (§ 2.2), or (§ 2.3), implies (§ 2.4), if and only if (§ 2.5). The first three are easily understood. You may have to pay special attention to the last two.

2.1 Negation

2.1.1. Definition (negation)**.** Let P be a proposition. Then 'not-P' is a proposition, called the *negation* of P and denoted by $\neg P$†. \neg

2.1.2. Remark. Old-fashioned* notation (forbidden): $\sim P$. Bad notation (forbidden): $\not P$. Démodé(e)

2.1.3. Example. Let x and y be real numbers.

- The negation of '$x + 0 = y$' is '$x + 0 \neq y$'.
- The negation of '$x > y$' is '$x \leqslant y$'.

We know that not-P is true if P is false, and false if P is true. It is convenient to summarize this in a *truth table**. This is just an array giving the truth value of a proposition, depending on the truth values of its components. table de vérité

Truth table of $\neg P$:	P	$\neg P$
	F	T
	T	F

2.1.4. Remark. P and $\neg\neg P$ always have the same truth value. This is an indication that they essentially have the same meaning (§ 3.2).

(The idea that 'same truth value = same meaning' was disputed at the beginning of the XX$^{\text{th}}$ century, which led to an interesting theoretical developement, and a philosophical debate.)

2.2 Conjunction

2.2.1. Definition (conjunction)**.** Let P and Q be propositions. Then 'P-and-Q' is a proposition, called the *conjunction* of P and Q, and denoted by $P \wedge Q$[†]. \wedge

2.2.2. Remark. Old-fashioned notation (forbidden): P & Q.

2.2.3. Remark. Before we write the truth table of $\wedge$, we adopt a natural convention. In order to write truth tables with several variables (below, P and Q are our two variables), it is convenient to use *always the same* enumeration of the truth entries.

Replace 'True' by 1 and 'False' by 0. Then the natural way to enumerate all possibilities is 00, 01, 10, 11, in increasing order. So the natural way to enumerate truth values in two variables is FF, FT, TF, TT.

$P \wedge Q$ is true if both P and Q are true, false otherwise.

Truth table of $P \wedge Q$:	P	Q	$P \wedge Q$
	F	F	F
	F	T	F
	T	F	F
	T	T	T

Thus $P \wedge T$ always has the same truth value as P, while $P \wedge F$ is always false.

2.2.4. Remark. In English (in French as well), there are two ways to use 'and':

- *connective and*, for connecting sentences, as in '2 is even and 4 is even': we use $\wedge$;
- *enumerative and*, for listing things, as in '2 and 4 are even': here it is *absolutely forbidden* to use $\wedge$.

In mathematics *we only have the connective*. So 'Let a and b be two numbers', *may not* be written 'Let $a \wedge b \ldots$'.

Likewise, '4 is greater than 1 and 2' writes as '$(4 > 1) \wedge (4 > 2)$'.

2.2.5. Remark. Mathematical language is poor. The English 'but' would be translated by 'and', losing the nuance of opposition in it.

2.2.6. Example. Let us complicate things and introduce three propositions.

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

Hence $(P \wedge Q) \wedge R$ and $P \wedge (Q \wedge R)$ always have the same truth value.

End of lecture 1

2.3 Disjunction

2.3.1. Definition (disjunction)**.** Let P and Q be propositions. Then 'P-or-Q' is a proposition, called the *disjunction* of P and Q, and denoted by $P \vee Q$†. \vee

Since $P \vee Q$ is true as soon as one of P or Q is true, we get the following truth table.

Truth table of $P \vee Q$:

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

Thus $P \vee T$ is always true, while $P \vee F$ always has the same truth value as P.

2.3.2. Remark (no symbol for '*enumerative* or')**.** 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', viz. $(x = 1 \vee x = 2)$. Never write '$x = 1 \vee 2$'.

2.3.3. Remark (mathematical 'or' is *inclusive*)**.** The mathematical 'or' is inclusive, viz. it always means 'P or Q *or both*'.

In English (in French as well), 'or' is often implicitly means 'or. . . , *but not both*'. For instance, 'will you come on Monday or on Tuesday?'* does not expect 'both' as an answer. « fromage ou dessert »

Should you want to specify 'not both', use 'either. . . or. . . '*. Mathematics does not have a universal symbol for this 'exclusive or'. ou bien. . . ou bien

2.3.4. Remark (continued)**.** In symbols, 'either P or Q' writes $(P \wedge \neg Q) \vee (\neg P \wedge Q)$. (Alternative, less clear options, are $(P \vee Q) \wedge \neg(P \wedge Q)$, or $\neg(P \Leftrightarrow Q)$ to be seen later.)

2.3.5. Examples.

- Using truth tables, one sees that:

[Hamlet's Principle:] $P \vee \neg P$ is always true.

In mathematics, 'to be or not to be' is no question: it is simply true.

- Classical mathematical joke: — *'Is it a boy or a girl?'* — *'Yes.'*

2.4 Implication

The fourth connective is generally misunderstood and deserves extra attention.

2.4.1. Definition (implication)**.** Let P and Q be propositions. Then 'if-P-then-Q' is a proposition, called the *implication from P to Q* and denoted by $P \Rightarrow Q^{\dagger}$. \Rightarrow

Implication says nothing about the cases in which P does not hold. So the truth table is as follows.

Truth table of $P \Rightarrow Q$:

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

2.4.2. Remarks (arrow shapes)**.**

- One may also use the simple arrow $P \to Q^{\dagger}$. \rightarrow, \to
- No backwards arrows. '$\Leftarrow$' and '$\leftarrow$' are absolutely forbidden.

2.4.3. Remark. $P \Rightarrow Q$ does not mean 'P has Q as an arguable consequence'. It means that if P holds, then so does Q. In particular:

False implies anything. — *Anything implies True.*

2.4.4. Example.

- 'If $1 = 0$, then cats lay eggs' is *true.*
- 'If cats lay eggs, then $1 + 1 = 2$' is *true.*
- 'If $1 + 1 = 2$, then cats lay eggs' is *false.*
- 'If hens lay eggs, then $0 = 0$' is *true.*

2.4.5. Remark (alternative phrases)**.** Here are various readings of $P \Rightarrow Q$:

• 'P implies Q; • 'if P, then Q'; • 'P is a sufficient condition for Q to hold'.

2.4.6. Remark (unrecommended alternative phrases)**.**

- The English 'Q if P' is grammatically correct and means $P \Rightarrow Q$, but is a bad idea as it suggests writing the (forbidden) $Q \Leftarrow P$.
- Likewise, 'Q is a necessary condition for P to hold' is correct and does mean $P \Rightarrow Q$ (one cannot have P without having Q, viz. $P \Rightarrow Q$), but again suggests writing backwards.

- The English ‘P only if* Q’ means exactly $P \Rightarrow Q$. seulement si

  Example: ‘You’re allowed to board this plane only if you have a boarding pass’. People aboard the plane will have a boarding pass. *But* someone with a boarding pass could be late and miss the plane. So really, the sentence is ‘allowed $\Rightarrow$ has pass’, not the other way around.

  I cannot recommend this phrase. First, even I have to think in order to understand which implies which. Second, the hasty listener could hear ‘if and only if’, which is something else (§ 2.5).

2.4.7. Remark (common mistakes)**.** Here are two common mistakes.

- $P \Rightarrow Q$ may not be read ‘P then Q’.

  Here ‘then’ would mean ‘later’, which is not what you mean. *If you want to use ‘then’, then you must use ‘if’.*

- ‘$P \Rightarrow Q$ may not be read ‘P, hence Q’ (nor ‘P, therefore Q’, etc.).

  Let us elaborate on this. Consider the two sentences:

  – ‘If cats lay eggs, then $0 = 1$’—a true proposition;
  – ‘Cats lay eggs, hence $0 = 1$’—an incorrect proof.

  Beginners tend to mistake 1. ‘P implies Q’ (a proposition) with 2. ‘P, which implies* Q’ (a part of a proof). In case 1. you say nothing about P or Q, simply about their relationship. In case 2. you claim both. ce qui implique

  It may be simpler to remember that *there is no symbol for ‘hence’, because there is no symbol for deduction.*

We define two notions related to implication.

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

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

2.5 Equivalence

This is arguably more of an abbreviation than a connective. It is less useful than beginners think.

2.5.1. Definition (equivalence)**.** Let P and Q be propositions. Then ‘P-if-and-only-if-Q’ is a proposition, called the *equivalence of P and Q* and denoted by $P \Leftrightarrow Q$†. \Leftrightarrow

Of course, $P \leftrightarrow Q$† is allowed as well. \leftrightarrow

Truth table of $P \Leftrightarrow Q$:

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

2.5.2. Remark (alternative phrases)**.** Here are various readings of $P \Leftrightarrow Q$:

> • 'P if and only if Q'; • 'P is a necessary and sufficient condition for Q to hold'; • 'Q is a necessary and sufficient condition for P to hold'.

Of course the last is usually a bad idea as it reverts the order.

One may also say 'P is equivalent to Q', for a reason explained in § 3.2.

3 Complex propositions

With the five propositional connectives one obtains compound* propositions. composé(es)

3.1 Parentheses

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 an expression is well-formed or not.

3.1.1. Example.

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

If we keep assembling compound propositions, we should use parentheses. Now if we want to drop some of the parentheses, we need a convention, because the meaning of $\neg P \vee Q$ is not clear at first sight; it could be either $(\neg P) \vee Q$ or $\neg(P \vee Q)$.

Pre-eminence is given to $\vee$*, then to* $\wedge$*, then to* $\neg$*.*

3.1.2. Example.

$$\begin{array}{rcl} \neg\neg\neg P & \text{stands for} & \neg(\neg(\neg(P))) \\ \neg P \vee Q & \text{stands for} & (\neg P) \vee Q \\ \neg P \vee Q \wedge R & \text{stands for} & (\neg P) \vee (Q \wedge R). \end{array}$$

But the golden rule is clarity:

Better too many parentheses than relying on conventions.

3.2 Equivalent Propositions

3.2.1. Definition. Two propositions P, Q are called *equivalent* if they always have the same truth value.

We shall see examples shortly. For the moment, a provocative comment.

3.2.2. Remark. There is *no symbol* to denote that two propositions are equivalent. (The symbol $\Leftrightarrow$ actually means something else; § 2.5.)

The following properties are essential when computing negations.

3.2.3. Properties (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.'

3.2.4. Example.

- 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)'. If it were, its meaning would become clear: 'No stopping *and* no standing'. ne pas s'arrêter ou stationner

Now, using truth tables, we show how the connectives relate to each other.

3.2.5. Remark. $P \Rightarrow Q$ is equivalent to $\neg P \vee Q$.
Indeed, '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.

3.2.6. Remark (negation of implication)**.**

$\neg(P \Rightarrow Q)$ is equivalent to $P \wedge \neg Q$.

- 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 seen to be equivalent to $P \wedge \neg Q$.
- $P \Rightarrow Q$ means 'whenever P is true, also Q is true'. Negating it amounts to *refuting* the implication. This is done by giving a *counter-example*, that is something that satisfies P, but not Q. This explains intuitively why $\neg(P \Rightarrow Q)$ is equivalent to $P \wedge \neg Q$.

3.2.7. Remark. In Definition 2.5.1, we defined the 'if and only if' *connective*. In Definition 3.2.1, we defined equivalence as a *property* of two propositions. This is *not* at all the same, but the relationship is expressed as follows:

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

The *symbol* '$\Leftrightarrow$' is used only as a connective. When asked to prove that two propositions P and Q are equivalent, one may prove that the compound proposition $P \Leftrightarrow Q$ is true. This is not literally the same question, but it is an equivalent question.

3.2.8. Remark (continued)**.** The compound proposition 'P is equivalent to Q' is, as a proposition, equivalent to the proposition 'P implies Q and Q implies P'. Therefore:

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

End of lecture 2

3.3 Some Classical Equivalences

Every equivalence below must be understood, known, and always ready for use. The last column gives the common name of the property.

$\neg\neg P$	is equiv. to	P	'double-negation'
$P \wedge (Q \wedge R)$	" "	$(P \wedge Q) \wedge R$	'associativity of $\wedge$'
$P \vee (Q \vee R)$	" "	$(P \vee Q) \vee R$	'associativity of $\vee'$
$Q \wedge P$	" "	$P \wedge Q$	'commutativity of $\wedge$'
$Q \vee P$	" "	$P \vee Q$	'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'
$P \Rightarrow Q$	" "	$\neg P \vee Q$	'material implication'
$\neg(P \Rightarrow Q)$	" "	$P \wedge \neg Q$	'counter-example'

One must recognize them when P and Q are compound themselves.

One should practice a little with truth tables and rewriting compound propositions. But one should quickly move on as mathematics becomes interesting with *quantification* (which is no longer explained by truth tables).

End of lecture 3

4 Quantifiers

Quantifying a proposition P is building another proposition that says how many 'things' satisfy P. The following are quantified propositions:

- 'For any real number x, one has $x^2 \geqslant 0$.'
- 'There is a real number x that satisfies the equation $x^5 + x - 2 = 0$.'

For common mathematical purposes, the two phrases 'all things satisfy P' and 'there exists (at least one) a thing satisfying P' suffice. So there will be only two quantifiers*, $\forall$ and $\exists$. (A useful abbreviation, $\exists!$, is also introduced.) quantificateur(s)

Notice that *truth tables cannot explain quantification*.

4.1 Preliminaries

It is interesting to quantify in a sentence P only if P depends on something. For example the expression '$x > 0$' is meaningless as long as we do not know who x is. We call such a sentence a *proposition depending on a variable* (here x), that is an expression that becomes a proposition as soon as we assign a meaning to its variables.

4.1.1. Example.

- '$x + y = y + x$' 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 does not state anything.

If a proposition depending on x, say $P(x)$, becomes a true proposition when we assign to x a certain value, say x_0, we say that x_0 *satisfies* P*. satisfaire *à*

4.1.2. Example.

- 2 satisfies 'n is even'.
- 0 as x and 1 as y satisfy '$x + y = y + x$'.

We also need some notation before proceeding.

4.1.3. Notation. We use throughout the following symbols:

- $\in$† denotes membership. Given two mathematical objects x and A, '$x \in A$' reads 'x is in A', or 'x is an element of A', or 'x belongs to A'. In context, 'belong*ing*'* can be more correct than 'belongs'. Really, 'in' is shortest and clearest. \in appartenant

  You *may not* use expressions like 'A contains x' or 'x is included in A' (which mean something else).

- In English, 'positive'* means > 0. This creates many confusions and requires some care. strictement positif

  For $\geqslant 0$, one uses 'non-negative'*. positif

- $\mathbb{N}$† denotes the set of all natural numbers, that is $\mathbb{N} = \{0, 1, 2, 3, \dots\}$. So '$x \in \mathbb{N}$' reads: '$x$ is in N', or 'x is a natural number', or 'x is a non-negative integer'. \mathbb{N}

- $\mathbb{R}$† denotes the set of all real numbers, that is the numbers on the line. So '$x \in \mathbb{R}$' reads: 'x is in R', or 'x is a real number'. \mathbb{R}

- To denote all positive real numbers, one writes $\mathbb{R}_{>0}$.† (French-style notation $\mathbb{R}_+^*$ is inconvenient and non-universal; hence forbidden.) \mathbb{R}_{>0}

  For non-negative real numbers, use $\mathbb{R}_{\geqslant 0}$.† \mathbb{R}_{\geq 0}

4.2 For all

4.2.1. Definition (universal quantification)**.** Let A be a set and $P(x)$ be a proposition depending on a variable x. Then 'for all x in A, P of x' is a proposition, called *the universal quantification of* $P(x)$ *over* $x \in A$ and denoted by $\forall x \in A, P(x)$.

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

4.2.2. Remarks.

- Good, though infrequent, practice prefers $(\forall x \in A)(P(x))$.
- The comma ',' after the quantification '$\forall x \in A$' is here for clarity, and entirely optional. One may wish to read it 'one has'.

4.2.3. Example.

- '$\forall x \in \mathbb{R}, x^2 \geqslant 0$' ('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.)

4.2.4. Remark. In some books the set A does not appear. Though technically correct (as opposed to the present exposition…), it is pedagogically speaking not a very good idea, because so far x is just a 'thing', and one could too easily forget what we are talking about. This is why we prefer to relativise (or *bound**) the quantifier to the set A. borner

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 why beginners should avoid such sentences and use only bounded quantifiers.

4.2.5. Remark (alternative phrases)**.** $\forall x \in A$ may be read:

> • 'for all x in A'; • 'for any element x of A'; • 'for each x belonging to A'; • 'for every x in the set A;

or any variation on these.

One may freely add 'one has'; or not.

4.2.6. Remark (classical sets)**.** An important special case is when dealing with common sets like $\mathbb{N}$ or $\mathbb{R}$. Instead of set-theoretic terminology 'x in N', one often describes x by a mass noun, as in:

> • 'for any positive integer x'; • 'for every natural number x'; • 'for all reals x'; etc.

4.2.7. Example. 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?

4.2.8. Remark (quantifying twice)**.** We know that for any two real numbers x and y, one has $x + y = y + x$. This writes '$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y = y + x$', and reads:

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

This sounds long. If confident, one will simply say:

> 'For any real numbers x and y, x plus y equals y plus x'.

Similarly, '$\forall x \in \mathbb{R}, \forall n \in \mathbb{N}, \ldots$' may read:

> 'for any real number x and any positive integer n…'

However this enumerative 'and' *may not* be written as a connective. So '$\forall x \wedge y$' is *absolutely forbidden.*

4.3 There exists

4.3.1. Definition (existential quantification)**.** Let A be a set and $P(x)$ be a proposition depending on a variable x. Then 'there is x in A *such that* P of x' is a proposition, called *the existential quantification of* $P(x)$ *over* $x \in A$ and denoted by $\exists x \in A, P(x)$.

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

4.3.2. Remark ('such that')**.**

- After 'there exists', never forget to say 'such that'* (or something similar) — if you do not, your sentence is grammatically incorrect. tel que
- This confuses beginners, since after 'for all', one does *not* add 'such that'.
- This is why you might like to put commas. When you find a comma after a $\exists$, read 'such that'. When you find a comma after $\forall$, do not read it; or possibly read it 'one has'.
- French-style / to mean 'such that' is neither universal nor rigorous; hence forbidden.
- Mathematics is a symmetric language; but English and French are not. Do not make rules; simply follow your knowledge of grammar.

4.3.3. Example.

- '$\exists x \in \mathbb{R}, x^2 = 2$' ('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.)

4.3.4. Remark (alternative phrases)**.** $\exists x \in A$ may be read:

> • 'there exists an x in A *such that*'; • 'there is an element x of A *satisfying**'; • 'there is an x in A *with the property that*'; • 'there is some x belonging to A *for which**'; etc. vérifiant pour lequel

And of course, when dealing with known sets:

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

4.3.5. Remark (unrecommended alternative phrase)**.** There also is the possibility to say 'for some x in A', but I cannot recommend this. The hasty listener will hear 'for' and guess 'for all', viz. $\forall$; which is not what you meant.

4.3.6. Example. Read the following aloud:

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

Which are true?

4.3.7. Remark. 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'.

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 are natural numbers k and ℓ such that …'

However this is an instance of 'enumerative and' and $\wedge$ is forbidden here.

End of lecture 4

5 Manipulating quantifiers

Quantified propositions are more interesting than non-quantified ones, but also deserve more attention. In § 5.1 we discuss *renaming*; then we give rules for quantifiers in § 5.2. § 5.3 introduces the abbreviation $\exists!$, which is *not* a quantifier. We finish with negating quantified sentences in § 5.4.

5.1 Renaming, and an independent digression

5.1.1. Remark (renaming is important)**.** Let us write in symbols:

> 'there exists a natural number which is even, and there exists a natural number which is odd'.

- The first half may be written: $\exists n \in \mathbb{N}, \exists k \in \mathbb{N}, n = 2k$.
- The second half may in turn be written: $\exists n \in \mathbb{N}, \exists k \in \mathbb{N}, n = 2k + 1$.
- Combining, we get a jam. Letters n and k each play two different roles. (Calling all your children 'Jessie' would lead to confusions.) So it is reasonable to rename. Hence we write for instance:

  $$(\exists n_1 \in \mathbb{N}, \exists k_1 \in \mathbb{N}, n_1 = 2k_1) \wedge (\exists n_2 \in \mathbb{N}, \exists k_2 \in \mathbb{N}, n_2 = 2k_2 + 1).,$$

  and everything is clear again.

This is quite the same as the treatment of the mute* variable in $\int_a^b f(x)dx = \int_a^b f(y)dy$. muette

5.1.2. Notation (a liberty with notation)**.** An important set in mathematics is the set $\mathbb{R}_{>0}$ of all positive real numbers. As it is sometimes boring to write $x \in \mathbb{R}_{>0}$, we adopt the following convention:

'$\forall x > 0$'	stands for	'$\forall x \in \mathbb{R}_{>0}$',
'$\exists x > 0$'	stands for	'$\exists x \in \mathbb{R}_{>0}$'.

5.1.3. Example. '$\forall \varepsilon > 0, \exists \delta > 0, \delta < \varepsilon$' 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'.

5.2 Quantifiers rules

5.2.1. Properties.

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

Proof. Since truth values are no longer relevant for quantification, we shall give a *proof* of these properties in Chapter II. $\square$

So consecutive 'quantification blocks' *of the same nature* may be freely exchanged. It is not the case with different quantifiers; *never switch a* $\forall$ *with a* $\exists$.

5.2.2. Counter-example. 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?

5.2.3. Example. 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.*

5.3 A useful abbreviation

Here is a useful abbreviation, which is not strictly speaking a quantifier.

5.3.1. Notation. 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 a unique 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, but also that any other y in A satisfying P has to be equal to x. Hence *x is the only element of A satisfying P.*

5.3.2. Remark (alternative phrases)**.** $\exists! x \in A, P(x)$ may read:

• 'there is exactly one x in A *such that*'; • 'there is a unique x in A *satisfying*'; etc.

5.3.3. Example. 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?

5.3.4. Remark. Notice how we say 'unique' in mathematics: 'if there are two, they are the same'. So $\exists!$ really means 'exists and is unique'.

5.3.5. Remark. '$\exists!$' is *not* a quantifier, but an abbreviation. Therefore you should make no rules but always return to the definition.

5.3.6. Counter-example.

- 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 $y_0 \in \mathbb{R}$, but there are many such. So the proposition is *false*.

5.4 Computing negations

As an application, we may now compute negations of all propositions.

5.4.1. Remark. $\not\forall$ and $\nexists$ are absolutely forbidden.

Consider the following proposition:

$$P: \quad \text{‘}\forall x \in \mathbb{R}, \exists n \in \mathbb{N}, \forall y \in \mathbb{R}, |y| > n \Rightarrow |y| > |x|\text{’}.$$

$\neg P$ is successively equivalent to:

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

5.4.2. Remark. Be careful that the negation of '$\exists x > 0, P(x)$' is *not* '$\forall x \leqslant 0, \neg P(x)$'.

Remember that '$\exists x > 0$' actually stands for '$\exists x \in \mathbb{R}_{>0}$'. Hence the negation of '$\exists x > 0, P(x)$' is '$\forall x > 0, \neg P(x)$'.

End of lecture 5

Check-up and Exercises

- Words used (check that you understand their meaning):
  - proposition (Definition 1.2.1)
  - connective: negation (Definition 2.1.1), conjunction (2.2.1), disjunction (2.3.1), implication (2.4.1), equivalence (2.5.1)
  - converse (Definition 2.4.8), contrapositive (Definition 2.4.9)
  - equivalence of two propositions (Definition 3.2.1)
  - quantification: universal (Definition 4.2.1), existential (4.3.1)
- Truth tables are useless. We teach them for two reasons:
  - they make students feel confident;
  - they help us convince you that sentences like 'If hens have teeth, then I am Santa Claus' are *true*.

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

Basic exercises (no quantifiers)

Propositions

I.1. *Which of the following are propositions? 1. How are you? 2. I am fine. 3. Socrates is dead. 4. This number is positive. 5.* -1 *is positive. 6. When it rains,* π *is a circle.*

I.2. *Determine if the following are propositions. When they are, try to find their truth values. 1.* $1^2 = 1$. *2.* $\sin^2 x + \cos^2 x = \tan^2 x$. *3.* $\forall n \in \mathbb{N}, n \in \mathbb{R}$. *4.* $\forall x \wedge y \in \mathbb{R}, x + y = y + x$. *5. Every triangle is a square. 6. There are only two real numbers the square of which equal themselves.*

Truth tables

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

Let P, Q, R denote propositions.

I.4. *Give the truth tables of: 1.* $(P \wedge \neg Q) \wedge \neg R$ *2.* $(\neg P \vee Q) \wedge (\neg Q \vee R)$

I.5. *Write truth tables for the following: 1.* $P \Rightarrow \neg Q$ *2.* $\neg P \Rightarrow Q$ *3.* $\neg P \Rightarrow \neg Q$

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.* $P \Leftrightarrow (Q \Leftrightarrow R)$

I.7. *Same exercise with: 1.* $(P \wedge Q) \vee (P \vee Q)$ *2.* $(P \wedge Q) \wedge (P \vee Q)$ *3.* $(P \wedge Q) \Rightarrow R$ *4.* $(P \Rightarrow Q) \vee R$

I.8. *Find a proposition whose truth table is:*

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

Translations

I.9. *Write the following sentences as compound propositions, using symbolic connectives (and parentheses):*

1. *'If it rains and I am home, then I play the piano or listen to the radio.'*

2. *'Paul was neither silly nor stupid, but George was a fool and so was Ringo.'*

3. *'Whenever I do not see cats around, I turn off the light; if in addition there is no party around, I sleep pacefully.'*

4. *'Either you come or I go and get you.'*

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 do not know how to drive.'*

4. *'You're allowed to drive only if you have a license.'*

5. *'I want salt and pepper but no sauce.'*

6. *'Mike turns off the light exactly when he wants to sleep.'*

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.'*

I.12. *Make up English sentences whose translations into symbols would be the following: 1. $P \wedge (Q \Rightarrow \neg P)$ 2. $(P \vee Q) \wedge (Q \Leftrightarrow R)$*

I.13. *Write ten compound propositions and find English sentences having their logical structures.*

Negations

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.* $(P \vee \neg Q) \wedge (\neg R \vee S)$

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* $\wedge$*.*

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.* $(P \Rightarrow Q) \Rightarrow (Q \Rightarrow R)$

I.17. *What are the negations of:*

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

I.18. *Without writing intermediate steps, give the negations of:*

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

Miscallenea manipulations

I.19. *Provide the negation, converse, and contrapositive of the following: 1.* $P \Rightarrow (Q \Rightarrow R)$ *2.* $(P \Rightarrow Q) \Rightarrow R$ *3.* $(P \Rightarrow Q) \Rightarrow (R \Rightarrow S)$.

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

> *give them 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,

$$\begin{array}{lll} P \Rightarrow (Q \Rightarrow R) & \textit{becomes} & \neg P \vee \neg Q \vee R, \\ (P \Rightarrow Q) \Rightarrow R & \textit{becomes} & (P \wedge \neg Q) \vee R, \\ (P \Rightarrow Q) \Rightarrow (R \Rightarrow S) & \textit{becomes} & (P \wedge \neg Q) \vee \neg R \vee S. \end{array}$$

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

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

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

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* $(\neg P \wedge \neg Q) \vee (\neg P \wedge R)$

Exercises involving quantifiers

Easy translations

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

Which are true?

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.

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 without a real square root.*

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

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

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

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

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

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

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:

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

You may use it or not.

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:*

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

Take the negation of the property, then translate the negation into English. Remark. The notation is quick-and-dirty for : $\exists n \in \mathbb{N}, n \geqslant n_0 \wedge |u_n - \ell| < \varepsilon$.

Abstract translations

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

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.*

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.*

Around functions

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.*

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 $\mathbb{R}$).*

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.*

I.35.

- *Recall 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 $x \in \mathbb{R}\backslash\{a\}$:*

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

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.*

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 — Proving Things

We know how to *state* propositions and turn to learning how to *prove* them. Proofs are arguments that establish mathematical statements and must be written *in English only.* (Symbolic language is *only for statements.*)

Chapter Goals. Write mathematical proofs:

- Prove easy propositions.
- Be able to follow a contradiction proof.
- Write induction proofs.

Main Notions. Proof, Contradiction proof, Induction proof.

The golden rule of proof writing is quite simple.

Be precise. Be concise. Prefer short sentences.

6 General ideas

The notion of a *proof* is central in mathematics. The criterion of acceptability of a new proposition is: 'does it have a proof?'. A formal definition would not help here, and one learns through practice.

Certainly you understand the difference between a position and a movement. By analogy, statements are positions, and proofs are movements. Only statements may be written using formal symbols. In particular, there is no symbol for *deduction*, as opposed to *implication* for which there is a symbol. (Symbol $\therefore$ is non-universal, ancient, and forbidden.)

So in a proof, you will often use the following phrases:

• so; • therefore; • thus; • hence; • whence; • as a result,

all expressing *deduction.* (These cannot be abbreviated by '$\Rightarrow$', which states an *implication.* One should be careful with 'then', which can also express deduction if alone; as opposed to 'if... then...', which expresses implication.)

6.1 Proofs, refutations, contradiction

6.1.1. Remark (how to start a proof)**.** In general, beginners should: 1. state what they will prove, 2. prove it, and then 3. tell that they have proved it. This looks redundant, but it shows the logical structure of your paper.

In particular, in 1., it is perfectly fine to write 'I/We want to prove that ...'.

6.1.2. Remark (how to continue a proof)**.** In a proof you may freely use:

- Propositions known to be true (e.g. usual equivalences).
- Your *current* assumptions*. hypothèse(s)
- Things you have already proved *under the same assumptions*.
- Classical results (eg. the fact that for real x one has $\sin^2 x + \cos^2 x = 1$).

The level of detail in a proof depends on contextual factors: whom you write for, how well-trained you are, etc. For that reason I will not always follow the guidelines below.

6.1.3. Remark (how to finish a proof)**.** To celebrate your final victory, there are several options.

- If you announced what you wanted to prove, you may say 'as wanted'* as a conclusion. comme voulu
- Snobbish variant: use QED*, which stands for the Latin: CQFD

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

- Mathematicians are keen on the $\square$ symbol (which reads 'QED' or 'end of proof'). In many books, proofs end like this.
- One occasionally sees $\dashv$ (not recommended).

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

*To disprove** is a synonym of *to refute*. [n'a pas d'équivalent]

6.1.5. Definition. A *contradiction** is any of the following: absurdité

- a proposition which 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 your current assumptions;
- something contradicting classical results.

6.2 How to know what to prove

There are three layers of increasing difficulty.

1. If an exercise asks to prove P (or if it asks to refute P) one knows what to do.
2. If an exercise asks to (prove P or refute P), this is already harder as one has to understand *which* is true before writing. This is where intuition gets into play. A proof of P and a proof of $\neg P$ do not even start similarly.
3. Research is even harder: one first has to decide which proposition P one wants to prove. The problem being to determine, through intuition (and not through wishful thinking*), a proposition P which is both true and interesting. le fait de prendre ses désirs pour des réalités

7 Propositional methods

We shall sketch a couple of techniques to prove propositions. Notice how the techniques one uses depend on the shape of what one has to prove.

7.1 How to prove $\neg P$; also, contradiction proof

In order to prove $\neg P$, prove that P cannot hold.

Proof of ¬P:

- Assume P.
- Prove a contradiction.
- Conclude that you have proved $\neg P$.

7.1.1. Example (important)**.** Let us prove $\sqrt{2} \notin \mathbb{Q}$[†]. \sqrt{2} \notin \mathbb{Q}, or \sqrt2\notin\mathbbQ (not recommended)

> 'Suppose that $\sqrt{2}$ is rational. [We prove a contradiction] Then there are integers $a, b \neq 0$ with $\sqrt{2} = \frac{a}{b}$. We may assume that a and b are coprime*. copremiers, premiers entre eux
>
> 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 2 divides both a and b, a contradiction to coprimality.
>
> Hence $\sqrt{2}$ is not a rational number.'

This example had historical significance and must be learnt.

Variation: contradiction proof. Since P and $\neg\neg P$ are equivalent, this gives rise to the powerful *contradiction proof**. It creates an assumption 'from nothing' by negating what you want to prove. dém. par l'absurde

Contradiction Proof of P:

- Assume $\neg P$.
- Prove a contradiction.
- Conclude that $\neg P$ cannot hold, and therefore P does hold.

It is slightly better not to give a contradiction proof if it can be avoided, for two reasons:

- some philosophers have disputed the validity of contradiction proofs (technically, they prove $\neg\neg P$, not P);
- contradiction proofs are more challenging for the mind as it must focus on something *false*.

7.2 How to prove $P \wedge Q$

This is simple.

Proof of P ∧ Q:

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

7.3 How to prove $P \vee Q$

The method is *not* to prove P or prove Q. First, which should you choose? Second, to prove P is much stronger than to prove $P \vee Q$ (since $P \Rightarrow P \vee Q$ but the converse does not always hold). Typically one can use a contradiction proof here.

Contradiction proof of P ∨ Q:

- Assume $\neg P \wedge \neg Q$.
- Prove a contradiction.
- Conclude that you have proved $P \vee Q$.

But one seldom does this, and relies on of the following variations instead.

Variation 1 for P ∨ Q:

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

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

Variation 2 for P ∨ Q:

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

7.3.1. Example. 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. Hence 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.'

7.4 How to prove $P \Rightarrow Q$; also, case division

We turn to implications.

Direct proof of P ⇒ Q:

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

Do not forget the conclusion.

7.4.1. Example. 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 $\sin x = 1 \Rightarrow \cos x = 0$.'

Sometimes the contrapositive (§ 2.4) is easier to prove.

Contraposition Proof of P ⇒ Q:

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

7.4.2. Example. 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 $\cos x \neq 0 \Rightarrow \sin x \neq 1$.'

Return to $P \Rightarrow Q$. Even assuming P, one may have trouble proving Q. In that case a contradiction proof is always possible.

Contradiction proof of P ⇒ Q:

- Assume $P \wedge \neg Q$.
- Prove a contradiction.
- Conclude $P \Rightarrow Q$.

Notice that a contradiction proof of the contrapositive is essentially the same.

Case division. A case division proof of P consists in separating different cases and proving P in each. The underlying principle is the following: P is equivalent to $(Q \Rightarrow P) \wedge (\neg Q \Rightarrow P)$. (Check you still see why by a direct computation.) One may introduce more than two cases.

Case division proof of P:

- Introduce cases $Q_1, \ldots, Q_n$ and prove that $Q_1 \vee \cdots \vee Q_n$ is true.
- Prove each implication $Q_i \Rightarrow P$.
- Say that you have proved P in each case Q_i, and that the various cases cover all possibilities. Conclude that you have proved P.

7.4.3. Example. 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.'

7.4.4. Remark. Always make sure that the disjunction of the Q_i's is true. (Cases *may* overlap, but they *must* cover all possibilities.)

7.5 How to prove $P \Leftrightarrow Q$

'If and only if' statements are actually abbreviations for two implications, which explains the following method.

Proof of P $\Leftrightarrow$ Q:

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

7.5.1. Remarks.

- The backwards arrow '$\Leftarrow$' is forbidden.
- In practice, series of $\Leftrightarrow$ almost never work.

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

7.5.3. Remark. In Example 7.5.2, between the two parts we have 'cleared assumptions'. This is expressed implicitly by '*Now* assume...'.

End of lecture 6

8 Proofs involving quantifiers

8.1 How to prove $\forall x \in A, P(x)$

To prove such a statement one must prove $P(x)$ for any x in A. This is done by taking x arbitrary in A, with no extra assumptions. (It goes without saying that mathematics does not recognize 'proof by example'.)

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

- Take any x in A.

  (This is expressed by: 'Let* $x \in A$.') Soit

- Prove that $P(x)$ holds, without assuming anything special on x.
- Conclude that for any x in A, $P(x)$ holds.

8.1.1. Example. 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:

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

8.1.2. Remark ('general let'). In the above proof, 'Let $n \in \mathbb{N}$' means 'Let us take any $n \in \mathbb{N}$, without making any further assumptions on it'. We call it *general let*.

8.2 How to prove $\exists x \in A, P(x)$

Unlike proofs of universal propositions, 'existential proofs' might rely on intuition. You need to find an example, and this requires deep understanding of the problem.

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: 'Let* x be' [its definition]). Soit, ici encore

- Prove that *for this special* x, $P(x)$ holds.
- Conclude that there exists an x in A such that $P(x)$ holds.

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

[We must think before we start writing. We are looking for a real number x such that for any real number y, y squared is not x. In other words, we am looking for a real number that does not have a real square root. Now intuition suggests that -1 will do. We briefly check that it works, and then start writing the proof.]

'**Let** $\mathbf{x} = -1$. Let $y \in \mathbb{R}$. Since $y^2 \geqslant 0$, 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** $\exists \mathbf{x} \in \mathbb{R}, \forall \mathbf{y} \in \mathbb{R}, \mathbf{x} \neq \mathbf{y^2}$ '

8.2.2. Remark ('particular let')**.** In the proof above, 'Let $x = -1$' means 'We define x to be -1.' This we call *particular let*, which is very different from the *general let* of 'Let $y \in \mathbb{R}$'.

Hence in English, 'let' has two very different meanings:* [même problème en français]

- *General let*, as in 'let n be an integer'. This is used in proofs of $\forall$-statements.
- *Particular let*, as in 'let $n = 2$'. This one is used in definitions, and in proofs of $\exists$-statements.

8.3 Contradiction and quantifiers

It is sometimes useful to apply the 'Contradiction Proof' technique to universal statements. The following relies on the fact that $\neg\forall x \in A, P(x)$ is equivalent to $\exists x \in A, \neg P(x)$ (§ 5.2; we return to it in § 8.4).

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.

8.3.1. Remark. This is an abstract proof, because one does not have the slightest idea what x is being used (in particular because one is actually proving there is no such x). In general, contradiction proofs require the mind to focus on something false.

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.

8.3.2. Remark. This is an existence proof of x yielding no suitable x. It is called a *non-constructive* proof (and is one of the reasons contradiction proofs are disputed by some).

8.4 Application: proving the quantifier rules

In § 5.2 we stated the following, which we now prove.

8.4.1. Properties.

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

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

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

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

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

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

Proof.

(i) We prove:
$$(\forall x \in A, P(x)) \Rightarrow (\forall y \in A, P(y)).$$
Suppose $\forall x \in A, P(x)$; we prove $\forall y \in A, P(y)$. Let $y \in A$. By assumption, we have $P(y)$. This holds for any $y \in A$, and therefore one has $\forall y \in A, P(y)$.

Therefore $(\forall x \in A, P(x)) \Rightarrow (\forall y \in A, P(y))$. We conclude by symmetry.

(ii) Essentially the same; exercise.

(iii) We prove:
$$(\forall x \in A, \forall y \in B, P(x,y)) \Rightarrow (\forall y \in B, \forall x \in A, P(x,y)).$$
Suppose $\forall x \in A, \forall y \in B, P(x,y)$; we prove $\forall y \in B, \forall x \in A, P(x,y)$. Let $y \in B$. Let $x \in A$. By assumption, $P(x,y)$. Therefore $\forall x \in A, P(x,y)$. This proves $\forall y \in B, \forall x \in A, P(x,y)$. So we have $(\forall x \in A, \forall y \in B, P(x,y)) \Rightarrow (\forall y \in B, \forall x \in A, P(x,y))$. We conclude by symmetry.

(iv) Essentially the same; exercise.

(v) We first prove $(\neg\exists x \in A, P(x)) \Rightarrow (\forall x \in A, \neg P(x))$. Suppose $\neg\exists x \in A, P(x)$; we prove $\forall x \in A, \neg P(x)$. Let $x \in A$. If $P(x)$ holds then $\exists x \in A, P(x)$. This is a contradiction; so $\neg P(x)$ holds. This is true of any $x \in A$, and therefore $\forall x \in A, \neg P(x)$. This proves the first implication.

We now prove the converse, viz. $(\forall x \in A, \neg P(x)) \Rightarrow (\neg\exists x \in A, P(x))$. Suppose $\forall x \in A, \neg P(x)$; we prove $\neg\exists x \in A, P(x)$. Suppose $\exists x \in A, P(x)$. Let x_0 be one witness, so that* $P(x_0)$ holds. This contradicts the assumption, so actually $\neg\exists x \in A, P(x)$. This proves the converse implication, and we find the equivalence. de telle sorte que

(vi) Could be treated applying negations, but is an excellent independent exercise. □

End of lecture 7

8.5 Our First Example (Tutorial)

8.5.1. Example. A real function $f\colon \mathbb{R} \to \mathbb{R}$ is *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 [*Caution: '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

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

□

End of tutorial. Half of lecture 8 was devoted to ∃!

9 'Induction proof'

Mathematical induction* is *not* a proof method, but a property of the integers. It is usually classified as a proof method and my colleagues certainly expect the present skill course to cover this aspect; I may not disappoint them.

récurrence

9.1 Induction principle

9.1.1. Theorem (induction principle)**.** *Let $P(n)$ be a proposition depending on an integer n. Suppose:*

- $P(0)$*;*
- $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$.

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

9.2 Proofs using 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 very efficient if you feel that proving $P(n)$ is easier when already established for smaller values than n.

Caution. n has to be a positive integer!

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

- Prove that $P(0)$ holds.
- 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 *induction hypothesis**.)

hypothèse de récurrence

- Conclude. This is done as follows:

  '**We have proved $\mathbf{P}(\mathbf{0})$ and $\forall \mathbf{n} \in \mathbb{N},\ \mathbf{P}(\mathbf{n}) \Rightarrow \mathbf{P}(\mathbf{n}+\mathbf{1})$.**
  By induction, we have proved $\forall \mathbf{n} \in \mathbb{N},\ \mathbf{P}(\mathbf{n})$.'

9.2.1. Remark. Induction is extremely easy for two reasons:

- All you need is remember the model of the proof, then 'fill up the form'.
- The answer is given in the exercise, you need not discover anything.

9.2.2. Example.

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

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}.$$

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

- We prove $P(0)$. Indeed, $\sum_{k=0}^{0} k = 0 = \frac{0(0+1)}{2}$, so $P(0)$ is true.
  [To be honest, here 'Clearly, $P(0)$ holds' would suffice.]
- Let $n \in \mathbb{N}$. We assume $P(n)$, and prove $P(n+1)$. We have:

  $$\sum_{k=0}^{n+1} k = \left(\sum_{k=0}^{n} k\right) + (n+1) = \frac{n(n+1)}{2} + (n+1)$$

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

  $$\sum_{k=0}^{n+1} k = (n+1)\left(\frac{n}{2}+1\right) = (n+1)\frac{n+2}{2} = \frac{(n+1)((n+1)+1)}{2}.$$

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

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

- We proved $P(0)$ and $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$. By induction, we have proved $\forall n \in \mathbb{N},\ P(n)$.

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

Write

$$\begin{array}{ccccccc} S & = & 1 & + & \ldots & + & n \\ & = & n & + & \ldots & + & 1 \end{array}$$

and hence

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

9.3 Variation: induction not starting from 0

9.3.1. Notation. '$\forall n \geqslant 2,\ P(n)$' (read: 'for all n greater than or equal to 2, P of n') stands for '$\forall n \in \mathbb{N},\ n \geqslant 2 \Rightarrow P(n)$'.

9.3.2. Remarks.

- It is implicit that n should be an integer, since the set $\mathbb{N}$ is not actually present in the notation. This is because habit dictates that n denotes an integer.
- Likewise, '$\exists n \geqslant 2, P(n)$' (read: 'there is an n greater than or equal to n such that P of n') stands for '$\exists n \in \mathbb{N}, n \geqslant 2 \wedge P(n)$'.
- In contrast, '$\forall x > -\pi, P(x)$' (read: 'for all x greater than minus π, P of x') stands for '$\forall x \in \mathbb{R}, x > -\pi \Rightarrow P(x)$', because here one guesses from context that x stands for a real number.
- Last, '$\exists x > -\pi, P(x)$' (read: 'there is an x greater than $-\pi$ such that P of x') stands for '$\exists x \in \mathbb{R}, x > -\pi \wedge P(x)$'. And 'let $x > -\pi$' means 'let $x \in \mathbb{R}$ be greater than π'.

The following exemple shows how it is possible to do induction from a value greater than 0.

9.3.3. Example. We prove $\forall n \geqslant 4, n^2 - 3n \geqslant 4$.

> 'We do induction on $n \geqslant 4$. For a natural number $n \geqslant 4$, let $P(n)$ be the property: $n^2 - 3n \geqslant 4$.
>
> - Since $4^2 - 3.4 = 16 - 12 = 4 \geqslant 4$, $P(4)$ holds.
> - We show $\forall n \geqslant 4, P(n) \Rightarrow P(n+1)$. Let $n \geqslant 4$. We assume $P(n)$, and we prove $P(n+1)$.
>   Using the induction hypothesis, one has:
> $$(n+1)^2 - 3(n+1) = n^2 - 2n - 2 \geqslant n + 2$$
>   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 $n \geqslant 4$, we have $\forall n \geqslant 4, P(n) \Rightarrow P(n+1)$.
> - We have proved $P(4)$ and $\forall n \geqslant 4, P(n) \Rightarrow P(n+1)$. By induction, we have $\forall n \geqslant 4, P(n)$. '

9.3.4. Remark. Here is another proof of Example 9.3.3. Induction proofs are always a bit clumsy, so a direct proof is likely to be more elegant.

> 'We have to prove $\forall n \geqslant 4, n^2 - 3n \geqslant 4$, in other words, we prove $\forall n \geqslant 4, n^2 - 3n - 4 \geqslant 0$.
>
> Notice how for $x \in \mathbb{R}$, one has $x^2 - 3x - 4 = (x+1)(x-4)$. The graph of the real function $f(x) = x^2 - 3x - 4$ is therefore a convex parabola meeting the horizontal axis at $x = -1$ and $x = 4$. Therefore, $f(x)$ is non-negative when $x \geqslant 4$. This remains true when we restrict to integers, so $\forall n \in \mathbb{N}, n \geqslant 4 \Rightarrow n^2 - 3n - 4 \geqslant 0$.'

End of lecture 8

Check-up and Exercises

Words used (check that you understand their meaning):

- proof; refutation;
- contradiction; contradiction proof;
- proof by contrapositive;
- case division;
- induction proof.

Basic proofs

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. $(P \Rightarrow \neg P) \Rightarrow \neg P$.

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

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

Proofs involving quantifiers

Easy proofs

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 greater than it.*
3. *There is a real number that doesn't have a real square root.*

II.5. *Here is a proof of:*

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

> *'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.'*

Write a proof of:

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

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 $m = 2k + 1$.

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.*

II.7.

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

Abstract proofs

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 $\exists y \in B, \exists x \in A, P(x, y)$.*

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

$$S\colon \text{‘}[\exists x \in A, \forall y \in A, R(x, y)] \Rightarrow [\forall y \in A, \exists x \in A, R(x, y)]\text{’.}$$

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.*

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?*

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

More technical

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 $+\infty$.*

II.13. *Recall the following definitions:*

- *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.]

Induction proofs

II.14. *Prove that*

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

II.15. *Prove that*

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

II.16. *Let q be a real number not equal to 1. Prove that*

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

II.17. *Read the following argument.*

> *'We prove by induction that in a non-empty basket of fruits, if one is an apple then all are apples. So for each $n \in \mathbb{N}$, let $P(n)$ be the property:*
>
> *If one among n fruits is an apple, then all n fruits are apples.*
>
> - *It is clear that if 1 among 0 fruits is an apple, then the whole basket consists of apples. So $P(0)$ holds.*
> - *We assume $P(n)$ and prove $P(n+1)$. So let B be a basket of $n+1$ fruits $f_1, \ldots, f_{n+1}$. Assume that one of these fruits is an apple. For convenience we may assume it is f_1. Now consider the sub-basket $B' = \{f_1, \ldots f_n\}$. (This notation means that B' is the set of elements $f_1, \ldots, f_n$.) of n fruits, one of which is an apple. By the inductive hypothesis, all fruits in B' are apples. So we now consider $B'' = \{f_2, \ldots, f_{n+1}\}$, another (sub-)basket of n fruits, one of which is an apple. By the inductive hypothesis again, all fruits in B'' are apples. Since B' and C'' cover B, all fruits in B are apples. 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 ?

Chapter III — Using Sets

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 given in terms of sets. (Occasionally this complicates matters instead of simplifying them.) Discussing sets will also give us many concrete examples of properties requiring proofs.

Chapter 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
- Handle arbitrary intersections and unions.

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

10 Sets and membership

10.1 Notation; some common sets

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

10.1.1. Notation. 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 $x \notin A$.

10.1.2. Remark. It is customary (and good practice) to denote sets by capital letters, as opposed to their elements.

10.1.3. Remark (alternative phrases)**.** $x \in A$ may read:

- 'x is a member of A'; • 'x lies in A'; • 'x belongs to A'.

10.1.4. Remark (continued)**.**

- $x \in A$ 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'.
- I once heard 'x *exists* in A', but this is completely inappropriate.

Actually a set is entirely determined by its elements.

10.1.5. Properties (extensionality axiom)**.** * *Two sets are equal if and only if they have the same elements.* *extensionnalité*

10.2 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.

10.2.1. Notation. The ordering of elements between braces does not matter. Repeated elements are counted only once.

10.2.2. Example.

- $\{1, 5\}$ is the set that has as only elements 1 and 5.
- $\{1, 2, 1\} = \{1, 2\} = \{2, 1\}$. It has exactly two elements.
- $\{0, \sin\}$ 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. In oral form one says *singleton* A for $\{A\}$.

10.3 The empty set

10.3.1. Definition. The *empty set* $\varnothing^{\dagger}$ is the set with no elements. \emptyset

'The' is legitimate as the empty set will be proved to be unique.

10.3.2. Remark. Let P be a proposition in the variable x. Then:

- '$\forall x \in \varnothing, P(x)$' is *true*, and
- '$\exists x \in \varnothing, P(x)$' is *false*.

10.3.3. Example. Let me insist on the following:

- '$\forall x \in \varnothing, 1 + 1 = 3$' is *true*;
- '$\exists x \in \varnothing, 1 + 1 = 2$' is *false*.

Indeed, whenever you give me x in the empty set, $1 + 1$ will be 3: because you cannot give me such an x. Also, you cannot give me x in the empty set, so you cannot give me one satisfying the extra (true) requirement that $1 + 1$ is 2.

10.3.4. Remark. As a consequence, the proposition

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

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

This once made quantification suspect. Some ill-advised people suggest that 'for any x in A' should assume that A is non-empty; methodologically, this is a serious mistake

10.4 Subsets, inclusion

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

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

10.4.2. Remark. The English 'contained' is very ambiguous; mathematical English uses only 'belongs' (for $\in$) and 'included' (for $\subseteq$).

10.4.3. Definition (proper subset)**.** If $A \subseteq B$ and $A \neq B$, we say that A is a *proper* subset of B and write $A \subsetneq B^{\dagger}$. \subsetneq

10.4.4. Remark. Pay attention to the following difference in notation:

- $A \subsetneq B$ means that A is a *proper* subset of B;

  [I do not recommend $\subset$, which looks too much like C, at least when writing.]

- $A \not\subseteq B^{\dagger}$ means that A is *not* a subset of B. \not\subseteq

For instance, $\{1\} \subsetneq \{1, 2\}$ while $\{1\} \not\subseteq \{0, 2\}$.
(If in real numbers we used $3 \lneq 4$ for $3 < 4$, the analogy would be clear.)

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

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

10.4.5. Properties. *Let A, B, C be sets. Then:*

(i) if $A \subseteq B$ and $B \subseteq A$ then $A = B$;

(ii) $\varnothing \subseteq A$;

(iii) the empty set is unique: if O is another empty set, then $O = \varnothing$;

(iv) $A \subseteq A$;

(v) if $A \subseteq B \subseteq C$, then $A \subseteq C$.

Proof.

(i) Suppose $A \subseteq B \subseteq A$. For any x, one has $x \in A \Rightarrow x \in B$ and $x \in B \Rightarrow x \in A$. So A and B have the same elements. By 'extensionality', $A = B$.

(ii) There is nothing to check since $\varnothing$ has no elements.

(iii) If O has no elements either, then $\varnothing \subseteq O$ and $O \subseteq \varnothing$, which we know implies $O = \varnothing$.

(iv) Let $x \in A$. Then $x \in A$. Thus, $A \subseteq A$.

(v) Suppose $A \subseteq B \subseteq C$. Let $x \in A$. Since $A \subseteq B$, one has $x \in B$. Since $B \subseteq C$, one has $x \in C$. Therefore $A \subseteq C$. □

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

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

- Prove $A \subseteq B$.
- Prove $B \subseteq A$.
- Conclude that $A = B$.

End of lecture 9

11 Very 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.

11.1 Intersection

11.1.1. Definition (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. \cap

Thus, for any x one has: $(x \in A \cap B) \Leftrightarrow (x \in A \wedge x \in B)$. Later we shall return to intersections, allowing arbitrarily many terms.

11.1.2. Example. $\mathbb{N} \cap \{-1, 1\} = \{1\}$.

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

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

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

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

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

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

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

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 $\varnothing \cap A = \varnothing$.

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

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

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

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

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

11.1.5. Definition (disjoint)**.** Call two sets A and B *disjoint* if $A \cap B = \varnothing$.

11.2 Union

11.2.1. Definition (union)**.** Let A and B be two sets. The union of A and B (write $A \cup B^{\dagger}$, pronounce 'A union B') is the set made of elements of A together with elements of B. \cup

Thus, for any x one has: $(x \in A \cup B) \Leftrightarrow (x \in A \vee x \in B)$.

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

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

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

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

(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.

11.2.3. Properties (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.

11.2.4. Remark. We give no convention on priority between $\cap$ and $\cup$. In particular $A \cap B \cup C$ makes no sense, and one must add parentheses somewhere.

11.3 Difference of sets

11.3.1. Definition (set difference)**.** Let A and B be two sets. The set difference $A \backslash B^{\dagger}$ (pronounce 'A minus B') is the set made of those elements of A that are not in B. \setminus; avoid \backslash

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

11.3.3. Example.

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

11.3.4. Properties. *For all sets A, B, C,*

(i). $A \backslash A = \varnothing$.

(ii). $A \backslash \varnothing = A$.

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

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

The proof is an exercise.

11.3.5. Remark. Do not try to make up or remember rules with the $\backslash$ operation. It is safer to redraw a small Venn diagram each time.

End of lecture 10

12 Naive operations with sets

12.1 Taking subsets

We have defined in § 10.4 what a subset of a given set is. We now introduce further notation.

12.1.1. Notation. 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 those elements of A which satisfy P.

It is absolutely necessary to say 'such that' (or a synonym) for the colon*. deux points

12.1.2. Remark (alternative phrases)**.** This is equally pronounced:

• 'the set of x in A such that $P(x)$ holds'; • 'the set of members of A with $P(x)$'; etc.

12.1.3. Remark (unrecommended other notation)**.**

- One occasionally finds the notation $\{x \in A \mid P(x)\}$. It may conflict with using $|$ as divisibility or asbolute value.
- I cannot recommend $\{x \in A,\ P(x)\}$, because a comma between braces looks too much like a list.
- 'French-style' / is forbidden because / means something completely different.

12.1.4. Example.

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

12.2 The power set

12.2.1. Definition (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.

12.2.2. Remark.

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

12.2.3. Example.

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

12.2.4. Example. We determine $P(\{\varnothing, \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}, \{\{\varnothing\}\}\})$.

[I am looking for $P(E)$ where $E = \{\varnothing, \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}, \{\{\varnothing\}\}\}$.
Since E has three elements, I am supposed to find 8 subsets. Let $a = \varnothing$, $b = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$, and $c = \{\{\varnothing\}\}$. The eight subsets of $\{a,b,c\}$ are: $\varnothing, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}$.]

We find:

$$P(E) = \left\{ \begin{array}{l} \varnothing, \underbrace{\{\varnothing\}}_{\{a\}}, \underbrace{\{\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}\}}_{\{b\}}, \underbrace{\{\{\{\varnothing\}\}\}}_{\{c\}}, \\ \underbrace{\{\varnothing, \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}\}}_{\{a,b\}}, \underbrace{\{\varnothing, \{\{\varnothing\}\}\}}_{\{a,c\}}, \\ \underbrace{\{\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}, \{\{\varnothing\}\}\}}_{\{b,c\}}, \\ \underbrace{\{\varnothing, \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}, \{\{\varnothing\}\}\}}_{\{a,b,c\}=E} \end{array} \right\}$$

12.3 Unions and intersections of families

The proper definition of a family would require that of a function, which comes only later. Fortunately it is intuitive enough.

Union.

12.3.1. Definition (union of a family)**.** Let I be a set (this set provides 'indices' and is called the 'indexing/index set') 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 $\bigcup_{i \in I} A_i{}^{\dagger}$, read 'the union for i in I of A_i') is the set of all elements that lie in some A_i for some $i \in I$. \bigcup_{i\in I} A_i

In retrospect, the union of two sets is a special case (when the index set I has only two elements).

12.3.2. Example.

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

Intersection

12.3.3. Definition (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 $i \in I$.

12.3.4. Remark. The intersection over the empty set is *not* defined. (It would lead to the 'classical paradoxes' of naive set theory.)

12.3.5. Example.
$$\bigcap_{\varepsilon \in \mathbb{R}_{>0}} (-\varepsilon, \varepsilon) = \{0\}.$$

12.4 Cartesian Products

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

12.4.2. Remark. 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.

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

12.4.4. Example. Draw pictures of the following:

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

12.4.5. Remark. 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.

12.4.6. Notation. We write A^2 for $A \times A$.

12.4.7. Remark. 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 (but not necessarily equal).

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

12.4.8. Properties. *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* $\exists (x, y) \in A \times B, P(x, y)$.

12.5 Functions

12.5.1. Definition. Let A, B be sets. A *function graph* is a subset $\Gamma \subseteq A \times B$ such that:

$$(\forall a \in A)(\exists! b \in B)((a, b) \in \Gamma).$$

One should refrain from using $\exists!$. So this rewrites:

$$\begin{aligned} &(\forall a \in A)(\exists b \in B)((a, b) \in \Gamma) \\ \wedge &(\forall a \in A)(\forall b_1 \in B)(\forall b_2 \in B)\left[((a, b_1) \in \Gamma \wedge (a, b_2) \in \Gamma) \Rightarrow b_1 = b_2\right]. \end{aligned}$$

The first line means: 'every a has at least one image'; the second line means 'every a has at most one image'.

12.5.2. Remark (function notation)**.** Given a function graph $\Gamma \subseteq A \times B$, we know that for each a there is a unique b with $(a, b) \in \Gamma$. We may then use function notation, and write $b = \Gamma(a)$ for the unique b.

Of course f is often a good name for a function.

Check-up and Exercises

Words used (check that you understand their meaning):

- set, subset; membership, inclusion;
- union, intersection; complement;
- powerset, infinitary union, infinitary intersection;
- function.

Very easy exercises

Finite sets

III.1. *How many elements does* $\{\varnothing, \{\varnothing, \{\varnothing\}\}\}$ *have?*

III.2. *Give all elements of the following sets:*

(i). $\{1, \{2\}, \{\{3\}, 4\}\}$

(ii). $P(\{a,b,c\})\backslash(P(\{a,b\}) \cup P(\{a,c\}))$

(iii). $\{\varnothing, \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}, \{\{\{\varnothing\}\}\}\}$

III.3. *Simplify the following sets:*

(i). $(\{a, \{a,b\}, b\} \cup \{a, \{a\}\})\backslash\{\{b\}\}$.

(ii). $\{a, \{a,b\}\} \cap (\{a,b\} \cup P(\{a\}))$.

(iii). $P(\{a\}) \cup P(\{b\})$.

(iv). $P(\{a,b\})\backslash P(\{b\})$.

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

III.5.

(i). *What is* $P(P(\varnothing))$*?*

(ii). *What is* $P(P(\{\varnothing\}))$*?*

(iii). *How many elements are there in* $P(P(P(P(\varnothing))))$*?*

(iv). *How many elements are there in* $P(P(P(\{\varnothing\})))$*?*

The algebra of sets

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* $\mathbb{N} \cap A = \varnothing$.

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

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

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

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

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

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

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

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

III.9. *Let* A, B, C *be sets. Prove that:*

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

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

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

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

(i). $A \subseteq C \Rightarrow A \subseteq B \subseteq C$.

(ii). $A \backslash (B \cup C) = (A \backslash B) \cup (A \backslash C)$.

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

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

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

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

(i). *Make a picture.*

(ii). *Prove that $A \triangle B = B \triangle A$.*

(iii). *Prove that $(A \cap B) \cap (A \triangle B) = \varnothing$.*

(iv). *Prove that $(A \cap B) \cup (A \triangle B) = A \cup B$.*

(v). *Prove that $A \triangle B = \varnothing$ if and only if $A = B$.*

(vi). *Prove that $A \triangle B \subseteq A$ if and only if $B \subseteq A$.*

(vii). *Prove that $A \subseteq A \triangle B$ if and only if $A \cap B = \varnothing$.*

(viii). *Prove that $A \triangle B = A$ if and only if $B = \varnothing$.*

The power set operation

III.16. *Let A and B be sets.*

(i). *Prove that $P(A \cap B) = P(A) \cap P(B)$.*

(ii). *Prove that $P(A) \cup P(B) \subseteq P(A \cup B)$.*

(iii). *Find a case in which $P(A) \cup P(B) \subsetneq P(A \cup B)$) (recall Definition 10.4.3).*

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

III.18.

(i). *Find a set A such that $A \cap P(A) \neq \varnothing$.*

(ii). *Find a set B such that $B \cap P(B)$ has at least two elements.*

(iii). *Find a set C such that $C \cap P(C)$ is infinite.*

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

Understanding set notation

III.20. *Find a shorter description (in symbols) of the following sets. (i).* $(\mathbb{N} \cap \mathbb{Z}) \cup (\mathbb{Q} \cap \mathbb{R})$. *(ii).* $\{x \in \mathbb{R} : x^2 = 2\} \cap \mathbb{Q}$. *(iii).* $\{n \in \mathbb{Z}, n^2 \in \mathbb{N}\} \cap \mathbb{Q}$. *(iv).* $[0,1] \cap [\frac{1}{2}, 2)$. *(v).* $[0,1] \cup [\frac{1}{2}, 2)$. *(vi).* $\{1, \{1,2\}, 2, \{1\}\} \cap \{1, 2, \{3\}\}$. *(vii).* $(\mathbb{Z} \backslash \mathbb{R}) \cup (\mathbb{Q} \backslash \mathbb{N})$. *(viii).* $(\mathbb{Q} \cap \{\sqrt{2}, \{1,-1\}, 2, -2\}) \backslash \mathbb{N}$.

III.21. *Same question. (i).* $\{x \in \mathbb{R} : x^2 = 2\} \cap \mathbb{Q}$. *(ii).* $\{x \in \mathbb{R} : x^2 = -1\}$. *(iii).* $[0,1] \cap [\frac{1}{2}, 2)$. *(iv).* $[0,1] \cup [\frac{1}{2}, 2)$. *(v).* $\{x^2 : x \in \mathbb{R}\} \cap \{x^3 : x \in \mathbb{R}\}$. *(vi).* $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : xy = 1\}$. *(vii).* $\bigcup_{x>0}(-x, x]$. *(viii).* $\bigcap_{x>0}(-x, x)$. *(ix).* $\{x + 1 : x \in \{y \in \mathbb{R} : \exists z \in \mathbb{R} : z = 0\}\}$. *(x).* $\bigcup_{x>0}(-x, x] \backslash (0, x)$.

III.22. *Same question.*

(i). $\{x \in \mathbb{R} : x^2 = 1\} \cup \{x^2 : x \in \mathbb{R}\}$.

(ii). $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : xy = 2\}$.

(iii). $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : y = 0\}$.

(iv). $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : x = 0\}$.

(v). $\{n \in \mathbb{N} : \exists q \in \mathbb{Q} : n = q\}$

(vi). $\{q \in \mathbb{Q} : \exists n \in \mathbb{N} : n = q\}$

III.23. *Same question.*

(i). $\bigcap_{n\in\mathbb{N}}[-n, +\infty)$

(ii). $\bigcap_{n\in\mathbb{N}}[n, +\infty)$

(iii). $\bigcup_{n\in\mathbb{N}}\{x \in \mathbb{R} : n \leqslant x < n + 1\}$

(iv). $\bigcup_{x\in\mathbb{R}} \bigcap_{y\in\mathbb{R}}\{z \in \mathbb{R} : z = y\}$

(v). $\bigcup_{0<a<1}(-a, a)$

(vi). $\bigcap_{a>1}(-a, a)$

III.24. *Same question.*

(i). $\bigcup_{0<x<1}(0, x)$

(ii). $\bigcup_{0<x<1}[0, x]$

(iii). $\bigcap_{0<x<1}(0, x)$

(iv). $\bigcap_{0<x<1}[0, x]$

(v). $(\{0,1\} \times \{0,1\}) \setminus (\{(a,a) : a \in \{0,1\}\})$

(vi). $\mathbb{R} \times \mathbb{R} \backslash (\ (\mathbb{R}_{\geqslant 0} \times \mathbb{R}_{<0}) \cup (\mathbb{R}_{<0} \times \mathbb{R}_{<0}) \cup (\mathbb{R}_{<0} \times \mathbb{R}_{\geqslant 0})\ )$

(vii). $\{x \in \mathbb{R} : \forall y \in [0,1] : x > y\}$

(viii). $\{x \in \mathbb{R} : \exists y \in [0,1] : x > y\}$

(ix). $\{x \in \varnothing : x \in \mathbb{R}\}$

(x). $\{x \in \{\varnothing\} : x \in \mathbb{R}\}$

III.25. *Same question.*

(i). $P(P(\varnothing))\backslash P(\varnothing)$

(ii). $\bigcup_{x\in[-1,1]}(-|x|, x)$

(iii). $\bigcup_{n\in\mathbb{N}}(-n, 0)$

(iv). $\bigcap_{q\in\mathbb{Q}}[-|q|, 0]$

(v). $\{x \in \mathbb{R} : \forall y \in \mathbb{R} : x > y\}$

(vi). $\{x \in \mathbb{R} : \forall y \in \mathbb{R} : x > |y|\}$

(vii). $\{x \in \mathbb{R} : \exists y \in \mathbb{R} : x > |y|\}$

(viii). $\{x \in \mathbb{R} : x > 0 \vee x < 0\}$

(ix). $\cos([0, \pi])$

(x). $\{x : x \in \{y \in \mathbb{R} : y^2 = 1\}\}$

(xi). $\{x^2 : x \in \{y \in R : y = 1\}\}$

(xii).

$$\bigcup_{q\in\{x\in\mathbb{Q}:x>0\}}(-q, q)$$

(xiii).

$$\bigcup_{q\in\mathbb{Q}}(q-1, q+1)$$

(xiv).

$$\bigcup_{n\in2\mathbb{Z}}(n-1, n+1)$$

III.26. *For any integer n, let $n\mathbb{Z}$ be the set $\{kn : k \in \mathbb{Z}\}$.*

(i). *Rewrite the definition in English.*

(ii). *What is $2\mathbb{Z} \cup 4\mathbb{Z}$?*

(iii). *What is $2\mathbb{Z} \cap 4\mathbb{Z}$?*

(iv). *What is $2\mathbb{Z} \cap 3\mathbb{Z}$?*

III.27. *Let:*

$A_1 = \{(x, y) \in \mathbb{R}^2 : x + y < 1\}$

$A_2 = \{(x, y) \in \mathbb{R}^2 : |x + y| < 1\}$

$A_3 = \{(x, y) \in \mathbb{R}^2 : |x| + |y| < 1\}$

$A_4 = \{(x, y) \in \mathbb{R}^2 : x + y > -1\}$

$A_5 = \{(x, y) \in \mathbb{R}^2 : |x - y| < 1\}$

(i). Draw these sets.

(ii). Deduce a geometric proof of the following:

$$(|x+y|<1 \wedge |x-y|<1) \Leftrightarrow |x|+|y|<1.$$

III.28. *What are the following sets equal to?*

(i).

$$\bigcap_{n\in\mathbb{N}}\left[n-\frac{1}{n}, n+\frac{1}{n}\right]$$

(ii).

$$\bigcup_{k\in\mathbb{N}}\bigcap_{n\in\mathbb{N}}\left[k-\frac{1}{n}, k+\frac{1}{n}\right]$$

Infinite operations

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:*

(i).

$$B \cup \bigcup_{i\in I} A_i = \bigcup_{i\in I}(B \cup A_i)$$

(ii).

$$B \cup \bigcap_{i\in I} A_i = \bigcap_{i\in I}(B \cup A_i)$$

(iii).

$$B \cap \bigcup_{i\in I} A_i = \bigcup_{i\in I}(B \cap A_i)$$

(iv).

$$B \cap \bigcap_{i\in I} A_i = \bigcap_{i\in I}(B \cap A_i)$$

III.30. *Let $\{A_n, n\in\mathbb{N}\}$ and $\{B_n, n\in\mathbb{N}\}$ be two families of sets indexed by $\mathbb{N}$.*

(i). Assume: $\forall n\in\mathbb{N}, A_n \subseteq B_n \subseteq A_{n+1}$. Show that $\bigcup_{n\in\mathbb{N}} A_n = \bigcup_{n\in\mathbb{N}} B_n$.

(ii). Assume: $\forall n\in\mathbb{N}, A_n \supseteq B_n \supseteq A_{n+1}$. Show that $\bigcap_{n\in\mathbb{N}} A_n = \bigcap_{n\in\mathbb{N}} B_n$.

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.*

(i). Prove the following:

(a)

$$\bigcup_{i\in I} A_i \subseteq \bigcup_{j\in J} A_j$$

(b)

$$\bigcap_{j\in J} A_j \subseteq \bigcap_{i\in I} A_j$$

(ii).

(a) Find an example of sets I, J, and A_j such that:

$$(I \subsetneq J) \quad \wedge \quad \left(\bigcup_{i \in I} A_i \subsetneq \bigcup_{j \in J} A_j \right) \quad \wedge \quad \left(\bigcap_{j \in J} A_j = \bigcap_{i \in I} A_j \right).$$

(b) Find an example of sets I, J, and A_j such that:

$$(I \subsetneq J) \quad \wedge \quad \left(\bigcup_{i \in I} A_i = \bigcup_{j \in J} A_j \right) \quad \wedge \quad \left(\bigcap_{j \in J} A_j \subsetneq \bigcap_{i \in I} A_j \right).$$

No justification required.

Chapter IV — Using Functions

We use set formalism to discuss functions properly. We do not introduce a distinction between 'functions' and 'applications' (which has little interest if any at all).

Chapter Goals. Work with abstract functions and related notions:

- understand what a function is;
- compute image and preimage sets;
- be able to show that a function is injective, or surjective.

Main Notions. Function, composition. Injection, surjection, bijection. Image set, preimage.

13 Functions and Composition

13.1 Function graphs

13.1.1. Definition (function graph)**.** Let A and B be sets. A function graph $A \to B$ is a subset $\Gamma_f \subseteq A \times B$ such that the following two conditions are satisfied:

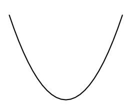
- $\forall a \in A, \exists b \in B, (a, b) \in \Gamma_f$
- $\forall (a, b, b') \in A \times B^2, (a, b) \in \Gamma_f \wedge (a, b') \in \Gamma_f \Rightarrow b = b'$.

Thus, a subset $\Gamma_f \subseteq A \times B$ is the graph of a function if and only if:

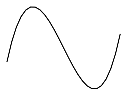
$$(\forall a \in A)(\exists! b \in B)((a, b) \in \Gamma_f).$$

13.1.2. Remark (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.

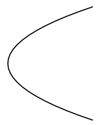
13.1.3. Example.

- 

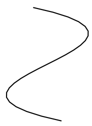
  This is the graph of a function (it could be the square function).

- 

  This is the graph of a function (for instance, $x^3 - x$ would do).

- 

  Not the graph of a function: some vertical lines meet the curve twice.

- 

  Not a function graph: some vertical lines meet the curve twice (or more).

13.2 Functions and function notation

13.2.1. Definition (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

$$f\colon A \to B.$$

13.2.2. Remark. A function is not a mapping. It consists of a 'domain' A, a 'codomain' B, and a mapping. Domain and codomain *must* be specified.

13.2.3. Example. 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 $\mathbb{R}_{\geqslant 0}$ that maps x to x^2 *are not* the same mathematical object.

13.2.4. Notation (function notation)**.** Given a function $f\colon A \to B$, 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:

$$\begin{array}{rccc} f\colon & A & \to & B \\ & x & \mapsto & f(x). \end{array}$$

13.2.5. Remark. $\to^{\dagger}$ indicates the domain A and the codomain B, but $\mapsto^{\dagger}$ \to
denotes the assignment. \mapsto

13.3 Composition of functions

13.3.1. Definition (composition)**.** Let $f\colon A \to B$ 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,
$$(g \circ f)(a) = g(f(a)).$$

13.3.2. Remark (the graph of the composition)**.** In graph notation, let $\Gamma_f \subseteq A \times B$ be the graph of f and $\Gamma_g \subseteq B \times C$ be the graph of g. Then:

$$\Gamma_{g\circ f} = \{(a, c) \in A \times C : (\exists b \in B)((a, b) \in \Gamma_f \wedge (b, c) \in \Gamma_g)\}.$$

13.3.3. Remark.

- Apply f first, then g. The closest to x must be executed first.
- $f \circ g$ makes no sense (unless of course if $A = B$).

13.3.4. Example.

- $\sin \circ \cos$ is the function from $\mathbb{R}$ to $\mathbb{R}$ which maps x to $\sin(\cos(x))$.
- Let $f\colon \{1, 2, 3\} \to \{a, b, c\}$ 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 $(g \circ f)(1) = \alpha$, $(g \circ f)(2) = \beta$, $(g \circ f)(3) = \gamma$

13.3.5. Properties (associativity of $\circ$)**.** *Let $f\colon A \to B$, $g : B \to C$, $h : C \to D$ be functions. Then:*
$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Proof. Exercise. □

14 Images and preimages

14.1 Images

14.1.1. Definition (image set)**.** Let $f\colon A \to B$ 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 $f\colon A \to B$, we say that $f(A)$ is the *image of f*.

14.1.2. Example. Let f denote the square function from $\mathbb{R}$ to $\mathbb{R}$.

- $f(\mathbb{R}) = f(\mathbb{R}_{\geqslant 0}) = f(\mathbb{R}_{\leqslant 0}) = \mathbb{R}_{\geqslant 0}$.
- $f([-1, 1]) = f([0, 1]) = f([-1, 0]) = [0, 1]$.

14.1.3. Properties. *Let $f\colon A \to B$ 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 $f(E) \cup f(F) \subseteq f(E \cup F)$. ☐

14.1.4. Remark. In general $f(E \cap F) \subsetneq f(E) \cap f(F)$.

Let $f\colon \mathbb{R} \to \mathbb{R}$ 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 $\mathbb{R}_{<0} \cap \mathbb{R}_{>0} = \varnothing$, one also $f(\mathbb{R}_{<0} \cap \mathbb{R}_{>0}) = \varnothing$.

14.2 Preimages

14.2.1. Definition (preimage)**.** Let $f\colon A \to B$ be a function, and let $F \subseteq B$ be a subset of B. The preimage of F under f is $f^{-1}(F) = \{a \in A : f(a) \in F\}$.

As opposed to an image set, this has the form $\{x \in A : P(x)\}$, viz. a subset obtained through 'separation'.

14.2.2. Remark. f^{-1} is not defined as a function from B to A. Expressions like $f^{-1}(b)$ are meaningless. The argument of f^{-1} must be a *subset* of B.

14.2.3. Example. Let f be the square function $\mathbb{R} \to \mathbb{R}$.

- $f^{-1}(\mathbb{R}) = \mathbb{R}$.
- $f^{-1}([0, 1]) = [-1, 1]$.
- $f^{-1}([-2, -1]) = \varnothing$.

14.2.4. Properties. *Let $f\colon A \to B$ be a function, and let $E, F \subseteq B$ be subsets of B. Then:*

(i). $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$.

(ii). $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$.

Proof.

(i). Let $x \in f^{-1}(E \cap F)$; we show $x \in f^{-1}(E) \cap f^{-1}(F)$. By definition, $f(x) \in E \cap F$. Since $f(x) \in E$, one has $x \in f^{-1}(E)$. Since $f(x) \in F$, one also has $x \in f^{-1}(F)$. This proves $f^{-1}(E \cap F) \subseteq f^{-1}(E \cap F)$.

Now let $x \in f^{-1}(E) \cap f^{-1}(F)$; we show $x \in f^{-1}(E \cap F)$. Since $x \in$

$f^{-1}(E)$, one has $f(x) \in E$. Since $x \in f^{-1}(F)$, one also has $f(x) \in F$. Hence $f(x) \in E \cap F$. So $x \in f^{-1}(E \cap F)$. This proves $f^{-1}(E) \cap f^{-1}(F) \subseteq f^{-1}(E \cap F)$.

(ii). Let $x \in f^{-1}(E \cup F)$; we show $x \in f^{-1}(E) \cup f^{-1}(F)$. By definition, $f(x) \in E \cup F$. If $f(x) \in E$, one has $f(x) \in E \cup F$, whence $x \in f^{-1}(E \cup F)$. If $f(x) \in F$, one has $x \in f^{-1}(E \cup F)$ similarly. This proves $f^{-1}(E \cup F) \subseteq f^{-1}(E) \cup f^{-1}(F)$.

Now let $x \in f^{-1}(E) \cup f^{-1}(F)$; we show $x \in f^{-1}(E \cup F)$. If $x \in f^{-1}(E)$, one has $f(x) \in E \subseteq E \cup F$, so $x \in f^{-1}(E \cup F)$. If $x \in f^{-1}(F)$, one has $x \in f^{-1}(E \cup F)$ similarly. This proves $f^{-1}(E) \cup f^{-1}(F) \subseteq f^{-1}(E \cup F)$. □

15 Injectivity, surjectivity, bijectivity

15.1 Injectivity

15.1.1. Definition (injection)**.** Let $f\colon A \to B$ be a function. f is injective if:

$$\forall (a, a') \in A^2, f(a) = f(a') \Rightarrow a = a'.$$

15.1.2. Remark. Old-fashioned, forbidden terminology: 'one-one'. This may create confusion with bijections.

15.1.3. Remark. 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.

15.1.4. Remark. Distinguish carefully between:

- '$\forall (a, a') \in A^2, a = a' \Rightarrow f(a) = f(a')$', which means that the notation $f(a)$ makes sense, i.e. that when a is given, $f(a)$ is uniquely determined;
- '$\forall (a, a') \in A^2, f(a) = f(a') \Rightarrow a = a'$', viz. injectivity.

15.1.5. Remark (horizontal line test)**.** $f\colon A \to B$ 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.

15.1.6. Example.

- 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!

15.1.7. Example.

- The square function $\mathbb{R} \to \mathbb{R}$ is *not* injective, as $(-1)^2 = 1 = 1^2$.
- The square function $\mathbb{R} \to \mathbb{R}_{\geqslant 0}$ is *not* injective, as $(-1)^2 = 1 = 1^2$.
- The square function $\mathbb{R}_{\geqslant 0} \to \mathbb{R}$ is injective.
- The square function $\mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ is injective.

15.1.8. Proposition. *Let $f\colon A \to B$ 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 $a = a'$. $\square$

15.1.9. Remark. If $g \circ f$ is injective, there is no reason why g should be.

Let $f\colon \{1\} \to \{1, 2\}$ map 1 to 1, and let $g : \{1, 2\} \to \{1\}$ map 1 and 2 to 1. Notice that g is not injective. However, $g \circ f\colon \{1\} \to \{1\}$ is injective.

15.2 Surjectivity

15.2.1. Definition (surjection)**.** Let $f\colon A \to B$ be a function. f is surjective if

$$\forall b \in B, \exists a \in A, f(a) = b.$$

15.2.2. Remark. Old-fashioned, unrecommended terminology: 'onto'. (Harmless, but not recommended.)

15.2.3. Remark. $f\colon A \to B$ 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.

15.2.4. Example.

- 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.

Caution. Surjectivity strongly depends on the domain and codomain!

15.2.5. Example. We consider the same functions as in Example 15.1.7.

- The square function $\mathbb{R} \to \mathbb{R}$ is *not* surjective, as (-1) has no square root.
- The square function $\mathbb{R} \to \mathbb{R}_{\geqslant 0}$ is surjective.
- The square function $\mathbb{R}_{\geqslant 0} \to \mathbb{R}$ is *not* surjective.
- The square function $\mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ is surjective.

15.2.6. Proposition. *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 $g(b) = c$. $\square$

15.2.7. Remark. If $g \circ f$ is surjective, there is no reason why f should be.

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.

15.3 Bijectivity

It turns out that the case where a function is both injective and surjective is extremely interesting.

15.3.1. Definition (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:

$$\forall b \in B, \exists! a \in A, f(a) = b.$$

15.3.2. Remark. Old-fashioned, forbidden terminology: *one-to-one correspondence.* The risk of confusion with ‘one-one’ is huge.

15.3.3. Remark. $f: A \to B$ 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.

15.3.4. Example.

- 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 $\mathbb{R} \to \mathbb{R}_{\geqslant 0}$ is not a bijection.

Caution. Bijectivity strongly depends on the domain and codomain!

15.3.5. Example. Same functions as in Examples 15.1.7 and 15.2.5.

- The square function $\mathbb{R} \to \mathbb{R}$ is *not* bijective, as it is not surjective.
- The square function $\mathbb{R} \to \mathbb{R}_{\geqslant 0}$ is *not* bijective, as it is not injective.
- The square function $\mathbb{R}_{\geqslant 0} \to \mathbb{R}$ is *not* bijective, as it is not surjective.
- The square function $\mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ *is* bijective.

15.3.6. Proposition. *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 15.1.8 and 15.2.6. □

15.3.7. Remark. If $g \circ f$ is bijective, there is no reason why f nor g should be.
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.

Check-up and Exercises

Warm-up exercises

IV.1. *Do the following constructions define functions? If yes, find the biggest possible domain on which they make sense.*

(i). Map any real number x to its square.

(ii). Map any real number to one of its real square roots.

(iii). Map any non-negative real number to one of its real square roots.

(iv). Map any real number to the biggest integer not greater than it.

(v). Map any real number to the integer that is closest to it.

(vi). Map x to $\sin(\sqrt{(}-x^2))$.

IV.2. *Let $\mathcal{F}$ be the set of polynomials with real coefficients.*

- *Let $\mathcal{D}$ be the derivation operation:*

$$\begin{array}{rccc} \mathcal{D} : & \mathcal{F} & \to & \mathcal{F} \\ & f & \mapsto & f' \end{array}$$

- *Let $\mathcal{P}$ map a polynomial to its* unique *primitive which vanishes at* 0*:*

$$\begin{array}{rccc} \mathcal{P}: & \mathcal{F} & \to & \mathcal{F} \\ & f & \mapsto & \int_0^x f(t)\mathrm{dt} \end{array}$$

(i). Are the functions $\mathcal{D}$, $\mathcal{P}$ injective?

(ii). Are the functions $\mathcal{D}$, $\mathcal{P}$ surjective?

IV.3.

(i). Determine all injections $\{1,2\} \to \{1,2,3,4\}$ *(you should find* 12 *of these).*

(ii). Determine all surjections $\{1,2,3,4\} \to \{1,2\}$ *(you should find* 14 *of these).*

IV.4. *Define* $f\colon \mathbb{Z} \times \mathbb{Z}\backslash\{0\} \to \mathbb{Q}$ *by:*

$$f((p,q)) = \frac{p}{q}.$$

(i). Is f injective? If so, prove it. If not, provide a counter-example.

(ii). Find $f^{-1}(\{\frac{1}{2}\})$.

Injections, Surjections, Bijections

IV.5. *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.

IV.6. *Let E be a set. For any subset $A \subseteq E$, the* characteristic function *of A in E is:*

$$\begin{array}{rccl} \chi_A: & E & \to & \{0,1\} \\ & x & \mapsto & \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases} \end{array}.$$

(i). Draw the characteristic function of $[0,1]$ *in* $\mathbb{R}$.

(ii). Draw the characteristic function of $\mathbb{Q}$ *in* $\mathbb{R}$.

(iii). 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.

(iv). Prove that Φ is surjective.

(v). Deduce that if E is finite and has n elements, then $P(E)$ has 2^n elements.

Images and preimages

IV.7. *Let f be the following function:*

$$\begin{array}{rccc} f\colon & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & x^4 \end{array}$$

Determine the following sets:

(i). $f(\mathbb{R})$, $f(\mathbb{R}_{\geqslant 0})$, $f(\mathbb{R}_{\leqslant 0})$, $f([0,1])$, $f([-1,1])$

(ii). $f^{-1}(\mathbb{R})$, $f^{-1}(\mathbb{R}_{\geqslant 0})$, $f^{-1}(\mathbb{R}_{\leqslant 0})$, $f^{-1}([0,1])$, $f^{-1}([-1,1])$.

IV.8. *Let f be the function from $P(\mathbb{N})\backslash\{\varnothing\}$ to $\mathbb{N}$ taking any non-empty subset of $\mathbb{N}$ to its least element.*

(i). *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 $f(B)$.

(ii). *Determine $f^{-1}(\{1\}), f^{-1}(\{2\}), f^{-1}(\{1,2\})$.*