Terence Tao's Analysis 1

January 13, 2025

Contents

1 Logical basics

Here are some of the logical devices I will use in this text. I will not explain every piece of Syntax, as I hope that throughout the text it will be sufficiently clear, when the rules are explained.

1.1 Statements

I will introduce the notion of logical statements here. Logical statements are sentences that are either true or wrong. In logical syntax you would say ϕ is a sentence, and $\neg\phi$ is the same sentence but negated.
Meaning that if ϕ is true then $\neg\phi$ is false, and if ϕ is false then $\neg\phi$ is true.

Examples of statements in mathematics could be $3 + 4 = 7$ or $\mathbb{C} \subset \mathbb{R}$. The first statement is true and the second is false.

1.2 Logical Symbols

In logic you will use several Symbols to help connect Satements or to portray statements themselves.

The conjunction $\wedge$. This is used to display an "and"

The disjunction $\vee$. This is used to display an "or"

One way to memorize which one is which is the fact that there is an "n" in "and", and that the $\wedge$ symbol look like an "n".

The existential quantification $\exists$ is used to display that a property is true fro at least one object

The the universal quantification $\forall$ is used to display that a property is true for all objects

What does this mean? Basically you use these symbols in combination with statements to make statements that portray the truth of general statements. For example

$$\exists x, y \left(\frac{1}{x} + \frac{1}{y} = 1 \right) \tag{1.1}$$

shows that there exist two elements, x and y, that when inversely added make 1

$$\forall x \exists y, z \, (y = x - 1 \wedge z = x + 1) \tag{1.2}$$

shows that every number x has a number that follows it, and one that is before it. Here you can also see the conjunction.

The implication $\rightarrow, \Rightarrow, \leftarrow, \Leftarrow$. Is used to show that if one statement is true, then so is the other, but it isn't necessarily the case that the other way around is also true.

the equivalence $\leftrightarrow, \Leftrightarrow$ Is used to show that one thing implies the other, and also the other way around.

1.3 Logical rules

I will now list some rules. I will use the sign Γ to stand for an arbitrary assortment of statements, and I will use the sign $\vdash$ to signify that the right side can be constructed from the left side. Greek letters will stand for statements, and latin letters for variables.

Equality Rule - $\Gamma \vdash (t = t)$

Contradiction Rule - $\psi, \neg\psi \vdash \phi$

By Case Rule - $(\Gamma, \psi \vdash \phi) \wedge (\Gamma, \neg\psi \vdash \phi) \Rightarrow \Gamma \vdash \phi$

Implication rule - $(\Gamma, \phi \vdash \psi) \Rightarrow \Gamma \vdash (\phi \rightarrow \psi)$

Modus Ponens - $\phi, (\phi \rightarrow \psi) \vdash \psi$

Substitution Rule - $\phi(a, ..., c) \vdash \exists x ... \exists z \phi(x, ..., z)$

Implication reversal - $\Gamma \vdash (\phi \rightarrow \psi) \Rightarrow \Gamma, \phi \vdash \psi$

Contraposition - $(\phi \rightarrow \psi) \vdash (\neg\psi \rightarrow \neg\phi)$

Double negation - $\phi \vdash \neg\neg\phi$

Verum ex quodlibet (True Statements follow from anything) - $\psi \vdash (\phi \rightarrow \psi)$

Ex falso sequitur quodlibet (Anything follows from false statements) - $\neg\phi \vdash (\phi \rightarrow \psi)$

Falsum non ex verum (false statements don't follow from true statements) - $\phi, \neg\psi \vdash \neg(\phi \rightarrow \psi)$

Conjunction rule (Introduction) - $\phi, \psi \vdash \phi \wedge \psi$

Conjunction rule (Eradication) - $\phi \wedge \psi \vdash \phi$

Disjunction rule (Introduction) - $\psi \vdash \psi \vee \phi$

Disjunction rule (Eradication) - $(\phi \vee \psi), \neg\phi \vdash \psi$

Negation of universal quantification - $\neg\forall x \phi(x) = \exists x \neg\phi(x)$

Negation of existential quantification - $\neg\exists x \phi(x) = \forall x \neg\phi(x)$

These are many rules, but hopefully many of them will become obvious throughout the text.

2 The natural numbers

Principle of Mathematical Induction

Mathematical induction is a proof tactic that works for ordered sets like the Natural numbers. We take it here to be an Axiom.

Axiom of Mathematical Induction

Let $P(n)$ be a property of a number n. Suppose that $P(n)$ is true, and that $P(succ(n))$ is true, then $P(n)$ is true for all $N \geqslant n$.
In particular, if $P(0)$ is true and $P(succ(n))$ is true, then $P(n)$ is true for all natural numbers.

2.1 The Peano Axioms

1 0 is a natural number

2 If n is a natural number, then $succ(n)$ is also a natural number

3 0 is the successor of no other natural number. So, $\neg\exists x \in \mathbb{N}(x++ = 0)$

4 Different natural numbers have different successors. If $n \neq m$ then $succ(n) \neq suc(m)$. At the same time, if $succ(n) = succ(m)$ then $n = m$.

Proposition: 6 is not equal to 2

We know that $6 = succ(succ(4))$, $2 = succ(succ(0))$. So, for $6 = 2$ we would need $4 = 0$, however $4 = succ(3)$ and we know that $0 \neq succ(3)$, so we can infer that $6 \neq 2$.

Proving a Property $P(n)$ for all natural numbers

If we want to prove that a property $P(n)$ holds for all natural numbers, we can write a proof like the following:

Proof by induction: First, verify the base case $n = 0$, so we will prove $P(0)$. (Proof of $P(0)$). Now assume that $P(n)$ is true, now we prove that $P(succ(n))$ is also true. (Proof of $P(succ(n))$). As $P(n)$ is true for $n = 0$ and for all successors of 0, $P(n)$ is true for all natural numbers.

2.2 Addition

2.2.1 Definition of addition

Addition will be defined recursively. Firstly, we will define addition with 0 to be $0 + m = m$, and addition with $succ(n)$ will be $succ(n) + m = succ(n + m)$.

Remark on addition

You can see that this will define addition as a series of successions. For example

$$2 + n = succ(1 + n) = succ(succ(0 + n)) = succ(succ(n)). \tag{2.1}$$

Lemma: Commutativity of 0

For any number n, $n + 0 = n$.
Proof: We will use induction. The base case is n = 0. We calculate $0 + 0$. We know, by the Definition of Addition, that $0 + 0 = 0$. We will assume that we have proven this for n, so we will prove it for $n \to succ(n)$. So, $succ(n) + 0 = succ(n + 0)$ which we know by our Induction step is $succ(n)$. This closes our Induction and proves our Lemma.

Lemma: Invariance of Addition

For any numbers n and m, $n + succ(m) = succ(n + m)$. I call this invariance because it doesn't matter if we take the successor of the left or the right number.
Proof: We first prove this for the base case $n = 0$. Then $0 + succ(m) = succ(m)$ from the Definition of Addition, so $0 + succ(m) = succ(0 + m)$. We now assume that our Lemma is proven for n, now we prove it for $n \to succ(n)$. So we calculate, $succ(n) + succ(m) = succ(n + succ(m))$, which we know by our Induction step is $succ(succ(n + m))$, which proves our Lemma.

2.2.2 Theorem: Addition is Commutative

For any numbers n and m, $n + m = m + n$. This is known as the commutative property. *Proof:* We will use induction. The base case is $n = 0$. We calculate $0 + n = n$. From "Lemma: Commutativity of 0", we know that $n + 0 = n$. We assume this to be proven for n, and we prove $n \to succ(n)$. We know that $succ(n) + m = succ(n + m)$ and we also know from "Lemma: Invariance of Addition" that $m + succ(n) = succ(m + n)$. According to Peano Axiom 4 $succ(n + m) = succ(m + n)$ if $n + m = m + n$, which is our Induction step, and hence this proves our Theorem.

This is, then, our first important finding about the Natural numbers.

2.2.3 Theorem: Addition is Associative

For any numbers a, b and c, $(a + b) + c = a + (b + c)$. This is known as the commutative property. This will be proven in the exercise section.

2.2.4 Theorem: Cancellation Law

For any numbers a, b and c, if $a+c = b+c$ then $a = b$. This is our first example of a cancellation law, and will lead us to developing Subtraction, without having defined it yet.
Proof: We use induction on c. The base case is $c = 0$, so we have $a+0 = b+0$, which means that $a = b$, proving the base case. We assume this to be proven for n, and prove it for $n \to succ(c)$. We then have $a + succ(c) = b + succ(c)$, which means that $succ(a + c) = succ(b + c)$ which then means $a + c = b + c$ which we know to be true from our Induction step. Hence, proving the Theorem.

2.2.5 Definition of positive numbers

A natural number is called positive if and only if (short: iff) it is not equal to 0.

Lemma: Addition of positive numbers is positive

let a be a natural number and b a positive number, then $a + b$ is positive.
Proof: We use Induction with $a = 0$, so $0 + b = b$ which is positive, as b is positive. We now assume $a + b$ to be positive, and prove for $b \to succ(b)$. Then, $a + succ(b) = succ(a + b)$, and as we know $a + b$ to be positive, the successor is also positive. Proving this Lemma.

Lemma: Addition is 0

let a and b be natural numbers, then if $a + b = 0$ then $a = 0$ and $b = 0$.
Proof: We use a proof by contradiction, thus we assume that $a \neq 0$ or $b \neq 0$. First, say that $a \neq 0$, then $a + b$ is positive. The same argument is made in case of $b \neq 0$. This contradicts our assumption that $a + b = 0$, hence $a = 0$ and $b = 0$.

Lemma: All positive numbers

Let b be a positive number, then there exists a natural number a such that $succ(a) = b$.
This will be proven in the exercise section.

2.2.6 Definition: Ordering of natural numbers

Let m and n be natural numbers. We define n to be greater than or equal to m, $(n \geqslant m)$, if there is a natural number a such that $n = m + a$. We define n to be strictly greater than m, $(n > m)$, if there exists a positive number b such that $n = m + b$, or if $n \geqslant m$ and $n \neq m$.

Lemma: Properties of Orderings

Order is reflexive - $a \geqslant a$

Order is transitive - $a \geqslant b \wedge b \geqslant c \Rightarrow a \geqslant c$

Order is antisymmetric - $a \geqslant b \wedge b \geqslant a \Rightarrow a = b$

Addition preserves order - $a \geqslant b \Leftrightarrow a + c \geqslant b + c$

$a < b \Leftrightarrow succ(a) \leqslant b$

2.2.7 Theorem: Trichotomy of order for natural numbers

For any numbers a and b, a is either exactly larger, equal to, or smaller than b.
Proof: Firstly, prove that only one of the three is possible, and then that at least one of them is true.
Only one is possible: Let $a > b$, then by definition $a \neq b$. same for $b > a$. Now assume that $a > b$ and $b > a$, then by the antisymmetric property, $a = b$, but we just ruled this out, proving that only one of the three orderings is possible.
At least one is true: Use induction on a. Start with $a = 0$, then $b \geqslant 0$ so either $b = 0$ or $b > 0$, which proves the base case. We assume this to be proven for a, and now we prove $a \rightarrow succ(a)$. We take a by cases approach. Assume that $a > b$, then $succ(a) > b$.

This follows from. $a > b$ means there exists a $c \neq 0$ s.t. $a = b + c$, meaning that $succ(a) = succ(b + c) = b + succ(c)$ which means that $a > b$, as $succ(c) \neq 0$.
Assume now, that $a = b$, then $succ(a) > b$. This follows from the same argument, as $succ(a) = b + 1$ and $1 \neq 0$.
Assume now, that $a < b$, then $succ(a) \leqslant b$, following as a property of orderings. From this follows that $succ(a) = b$ or $succ(a) < b$, proving that At least one of the three properties is true.

As only one of the three cases can be true, and at least one must be true, only one of the three can be true. Proving the theorem.

2.2.8 Exercises

Theorem: Addition is associative

Proof: Proof by Induction over a. Base case, $a = 0$, then $(0 + b) + c = 0 + (b + c)$ and with the commutativity of 0 we know $(b) + c = (b + c)$ which is equivalent. So this is proven for the base case. We assume this to be true for a, and will now prove it for $a \rightarrow succ(a)$. Then $(succ(a) + b) + c = succ(a) + (b + c)$ which we know to be $(succ(a + b)) + c = succ(a + (b + c))$ and then $succ((a + b) + c) = succ(a + (b + c))$ which is true if $(a + b) + c = a + (b + c)$, which is our Induction step, so we know it to be true. This proves our Theorem.

Lemma: All positive numbers

Proof: We will prove this for all positive numbers by induction, so we start with $b = 1$, we find that there is a natural number for which $b = succ(a)$, namely $a = 0$. We assume our Lemma to be true for b, and prove it for $b \rightarrow succ(b)$. We know that $b = succ(a)$, we then take the successor of both elements, and have $succ(b) = succ(succ(a))$, then meaning that we have found our number, namely $succ(a)$. This closes the Induction and proves the lemma.

2.3 Multiplication

2.3.1 Definition of Multiplication

Just as with Addition, multiplication shall be defined recursively.
Let n, m be natural numbers. Define multiplication with 0 as $0 \times m = 0$. Then, define multiplication with $succ(n)$ as $succ(n) \times m = (n \times m) + m$.
For example, $2 \times m = 0 + m + m$.

2.3.2 Theorem: Multiplication is commutative

Let m, n be real numbers, then $m \times n = n \times m$.
The proof is in the exercise section.

2.3.3 Theorem: Natural numbers have no zero divisors

let n, m be natural numbers. Then $nm = 0$ iff $n = 0$ or $m = 0$, in particular if n and m are positive, then nm is positive.
The proof is in the exercise section.

2.3.4 Theorem: Distributive law

For any natural numbers a, b, c, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.
Proof: Only one of the two need to be proven because of commutativity. Use Induction on c. For the base case, $c = 0$ we calculate $a(b + 0) = a(b) = ab$ and $ab + a0 = ab$. Now assume $a(b+c) = ab+ac$ and prove the case for $c \to c++$, then we have $a(b+(c++)) = a(b+c)++ = a(b + c) + a$and $ab + a(c + +) = ab + ac + a$, so in total we have $a(b + c) + a = ab + ac + a$ which is true with our Induction step, proving our result.

2.3.5 Theorem: Multiplication is associative

For any natural numbers a, b, c, $a(bc) = (ab)c$
The proof is in the exercise section.

Lemma: Multiplication preserves Order

let a, b, c be natural numbers and $c \neq 0$. Then $a < b$ iff $ac < bc$.
`Proof:`
$\varepsilon \Rightarrow \varepsilon$: Suppose $a < b$, then we know there is a positive d s.t. $a + d = b$. Multiplying by c gives $(a + d)c = ac + dc = bc$ we know dc is positive as c, d are positive, meaning $ac < bc$.
$\varepsilon \Leftarrow \varepsilon$: Suppose $ac < bc$. Proof by contradiction, so suppose $a \geqslant b$. First case, $a > b$ then we know from $\varepsilon \Rightarrow \varepsilon$, that $ac > bc$, a contradiction. Second case, $a = b$, then $ac = bc$, also a contradiction. Therefore, $a < b$.
Proving the Lemma.

2.3.6 Theorem: Cancellation law of multiplication

Let a, b, c be natural numbers with $c \neq 0$, if $ac = bc$ then $a = b$
Proof: It was already proven that if $a = b$ then $ac = bc$, through preservation of Order. Now we prove that if $ac = bc$ then $a = b$. Proof by contradiction, suppose that $ac = bc$ and $a \neq b$, then either $a < b$ or $a > b$. Through order preservation, we can see that with $c \neq 0$ either $ac < bc$ or $bc < ac$, meaning that both cases can't be true. So, if $ac = bc$ then $a = b$.

2.3.7 Theorem: The Euclidean Algorithm

Let n be a natural number, and let q be a positive number. Then there exist natural numbers m, r such that $0 \leqslant r < q$ and $n = mq + r$
Proof: Induct on n, start with $n = 0$. Then, $0 = mq + r$, we find that $m = r = 0$. Now assume that there are m, r such that $n = mq + r$ for some n. now check for $succ(n)$, then $succ(n) = succ(mq + r)$. We now have the restriction that $0 \leqslant r < q$. This means, that in the event that $succ(r) = q$ (It can't be greater as that breaks our Induction Hypothesis) we will set $r = 0$ and $q \to succ(q)$. Otherwise $r \to succ(r)$. Then we have found q and r that fulfil our equation, closing the Induction and proving the theorem.

2.3.8 Definition of Exponentiation

Let m be a natural number. Raising m to the power of 0 is defined as $m^0 = 1$, then we will define exponentiation to the power of $n++$ as $m^{n++} = m^n \times m$

Binomial Fomula

$(a + b)^2 = a^2 + 2ab + b^2$.
Proof: We use Definitions. $(a+b)^2 = 1 \times (a+b) \times (a+b) = (a+b)(a+b) = a(a+b) + b(a+b) = aa + ab + ba + b = a^2 + ab + ab + b^2 = a^2 + 2ab + b^2$.

2.3.9 Exercises

Theorem: Multiplication is commutative

First, prove the Lemma $0 \times n = n \times 0$
Proof: Proof by Induction, we induct on n. With $n = 0$ we have $0 \times 0 = 0 \times 0$ which is true. Then we suppose to have proven this for n, and we will prove it for $n \to succ(n)$, so we have $\succ n \times 0 = 0 \times succ(n)$. We have $succ(n) \times 0 = n \times 0 + 0 = n \times 0$, which we know by our induction step is $0 \times n = 0$, which we know by Definition. We also know $succ(n) \times 0 = 0$ by definition, so both sides are equal. This closes the induction and proves that $0 \times n = n \times 0$.

Also, prove that $n \times succ(m) = n \times m + n$.
Proof: Proof by Induction, base case $n = 0$. Calculate $0 \times succ(m) = 0$ and $0 \times m + 0 = 0$, by definition of multiplication and addition. Then we assume the case to be true for n and prove $n \to succ(n)$. We start $succ(n) \times succ(m) = n \times succ(m) + succ(n)$ and then through our Induction step we know this is $n \times m + m + succ(n)$. We then evaluate $succ(n) \times m + succ(n)$ which we

know by definition is $n \times m + m + succ(n)$, which shows that both sides are equal. This closes the induction and proves $n \times succ(m) = n \times m + n$.

Now to prove our Theorem, that $n \times m = m \times n$

Proof: Proof by Induction, we induct on n, starting with $n = 0$. This case is already proven with our previous Lemma. Then we assume that $n \times m = m \times n$, and we prove $succ(n) \times m = m \times succ(n)$. From our previous Lemma we know that $m \times succ(n) = m \times n + m$ and by definition we know that $succ(n) \times m = n \times m + n$ we know with our induction step that these are equal, as $n \times m = m \times n$, and the additional n can be cancelled through our additive cancellation law.

Theorem: Natural numbers have no zero divisors

let n, m be natural nubers. Then $nm = 0$ iff $n = 0$ or $m = 0$, in particular, if n and m are positive, then nm is positive.

Proof:

$\varepsilon \Rightarrow \varepsilon$: Suppose $mn = 0$. Proof by contradiction, so assume $n \neq 0$ and $m \neq 0$. This means that m and n are positive, so there exist numbers a, b s.t. $succ(a) = n$ and $succ(b) = m$. We can then calculate $mn = succ(a)m = am + m$ which is positive, or $n \times succ(b) = nb + n$ which is also positive, so $nm \neq 0$, which contradicts our assumption that $nm = 0$, so either n or m must be 0.

$\varepsilon \Leftarrow \varepsilon$: Suppose $n = 0$ or $m = 0$. Firstly, suppose $n = 0$, then $nm = 0 \times m = 0$ by Definition, then suppose $m = 0$, then $nm = n \times 0 = 0$ by Definition.

Thus proving the equivalence.

Theorem: Multiplication is associative

For any natural numbers a, b, c, $a(bc) = (ab)c$.

Proof: Proof by Induction, induct on c. Start with $c = 0$. Then we calculate $a(b \times 0 = a \times 0 = 0$, and also $(ab) \times 0 = 0$. We then assume $a(bc) = (ab)c$ and prove for $c \rightarrow c++$. Then we calculate $a(b \times c++) = a(bc + b) = a(bc) + ab$, and $(ab) + (c++) = (ab)c + ab$, from the Induction Hypothesis this is true, proving the theorem.

3 Set Theory

3.1 Fundamentals

3.1.1 Axioms of Set Theory

1 (Sets are Objects). If A is a set then A Is also an Object. Given two sets A and B, it is meaningful to ask if A is in B.

2 (Empty Set) There exists a set $\emptyset$, the empty set, which contains no element, so for all elements x, $x \notin \emptyset$.

3 (Singleton sets) If a is an object, then there exists a set $\{a\}$ whose only element is a, so that $\forall x(x \in \{a\} \Leftrightarrow x = a)$.

4 (Pairwise union) Given two sets A, B, there exists a set $A \cup B$ such that its elements consist of all elements which belong to A or B, so $x \in A \cup B \Leftrightarrow (x \in A \vee x \in B)$.

5 (Specification) Let A be a set and for each $x \in A$ let $P(x)$ be a property of x, s.t. $P(x)$ is either true or false, then there exists a set such that $\{x \in A | P(x)\}$, whose elements are all elements of A for which $P(x)$ is true.

6 (Replacement) Let A be a set. For any object $x \in A$ and any object y, suppose we have a statement $P(x, y)$ such that for any x $P(x, y)$ is true for at most one y. Then there exists a set $\{y | P(x, y), x \in A\}$. Such that for any object z

$$z \in \{y | P(x, y) x \in A\} \Leftrightarrow P(x, z) \text{is true for some} x \in A.$$

7 (Infinity) There exists a set $\mathbb{N}$ whose elements are called natural numbers, in which there exists the object 0 and the object $n++$ for each element in $\mathbb{N}$, such that the Peano Axioms hold.

8 (Universal Specification) Suppose that for every object x there is a Property $P(x)$ that pertains to x. Then there exists a set $\{x | P(x)\}$, such that for every object y

$$y \in \{x | P(x)\} \Leftrightarrow P(y) \text{is true} \tag{3.1}$$

This can lead to Paradoxes, so the next Axiom is needed if this Axiom is introduced.

9 (Regularity) If A is a non-empty set, then there is at least one element x of A which is either not a set, or is disjoint from A.

3.1.2 Definition of Equality of Sets

Two sets A and B are Equal, $A = B$, iff every element of A is an element of B and the other way around.

Lemma of Single Choice

Let A be a non-empty set. Then there exists an object x such that $x \in A$.
Proof: Proof by Contradiction. Assume there is no Object with $x \in A$, meaning that $\forall x(x \notin A)$. Thus, from the Axiom of the Empty Set, $A = \emptyset$ as $x \in A \Leftrightarrow x \in \emptyset$. This contradicts that A is nonempty, as $\emptyset$ is empty. Proving the Lemma.

Example: The Empty set and the Set of the Empty set

The empty set $\emptyset$ and the set of the empty set $\{\emptyset\}$ are different sets.
Proof: Two sets are the same iff every element in A is an element of B. Per definition, for all x, $x \notin \emptyset$. As per the Single Choice Lemma, and that the set of the empty set is not empty, there is an $x \in \{\emptyset\}$. As there is an element in the set of the empty set, and there is no element in the empty set, the sets can't be equal.

Example: Substitution in Unions

Lemma: Let A, B, A' be sets and $A = A'$. Then $A \cup B = A' \cup B$.
Proof: Let $A = A'$, then for all x, $x \in A$ iff $x \in A'$. Let $x \in A \cup B$. Then x is either in B or A. Let x be in B. Then $x \in B$ and therefore $x \in A' \cup B$. Let x be in A. As $A = A'$, $x \in A'$, therefore $x \in A' \cup B$. Same reasoning the other way around.

Proving the Lemma.

Lemma: Unions are Commutative,Associative

Let A, B, C be sets. Then $A \cup B = B \cup A$, and $(A \cup B) \cup C = A \cup (B \cup C)$.
Associativity, Proof: let $x \in (A \cup B) \cup C$. Then $x \in (A \cup B)$ or $x \in C$. If $x \in C$ then $x \in (B \cup C)$. If $x \in (A \cup B)$ then $x \in A$ or $x \in B$. if $x \in B$ then $x \in (B \cup C)$. Thus, either $x \in A$ or $x \in (B \cup C)$ so $x \in A \cup (B \cup C)$. The opposite direction is proven by the same argument. This completes the proof.
Commutativity, Proof: let $x \in A \cup B$. Assume that $x \notin B \cup A$. Then $x \notin A \wedge x \notin B$. By our previous assumption, $x \in A$ or $x \in B$, however this leads to a contradiction. Then, $x \in B \cup A$. The opposite direction is proven by the same argument. This completes the proof.

Example: Triplet, Quadruplet sets

From our Axioms of singleton sets and Pairwise Union we can now define sets that are finitely large. This means we can define for example

$$\{a\} \cup \{b\} \cup \{c\} = \{a, b, c\} \tag{3.2}$$

3.1.3 Definition of Subsets

Let A, B be sets. A is a subset of B iff every element of A is also in B. We write

$$\text{for all } x,\ x \in A \rightarrow x \in B. \tag{3.3}$$

We use the notation $A \subseteq B$. We call A a proper subset of B if $A \subseteq B$ and $A \neq B$, then we use $A \subset B$.

Ordering of Sets

Sets are partiall ordered by set inclusion.
Let A, B, C be sets. If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$. If $A \subseteq B$ and $B \subseteq A$ then $A = B$. If $A \subset B$ and $B \subset C$ then $A \subset C$.
1, Proof: Let $A \subseteq B$ and $B \subseteq C$. Let x be arbitrary and let $x \in A$. As $x \in A$ and $A \subseteq B$ then $x \in B$. As $x \in B$ and $B \subset C$ then $x \in C$. Thus, $x \in A$ implies $x \in C$, so $A \subseteq C$.
2, Proof: Let $A \subseteq B$ and $B \subseteq A$. Then $\forall x(x \in A \Rightarrow x \in B \wedge x \in B \Rightarrow x \in A)$ which is $\forall x(x \in A \Leftrightarrow x \in B)$ which is $A = B$.
3, Proof: Let $A \subset B$ and $B \subset C$. We already know $A \subseteq C$ from (1). From our definitions we know that there is an $x \in B$ such that $x \notin A$ and $x \in C$. As $x \notin A$ and $x \in C$, $A \neq C$. Therefore, $A \subset C$.

3.1.4 Definition of Intersections

The Intersection $A \cap B$ is defined to be

$$A \cap B := \{x \in A | x \in B\} \tag{3.4}$$

So in other words

$$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B \tag{3.5}$$

3.1.5 Definition of Differences of Sets

The Difference of the sets A, B is defined as

$$A \backslash B := \{x \in A | x \notin B\} \tag{3.6}$$

Set connection laws

We can form set connection laws with the Union, Intersection and Difference of Sets. Let A, B, C be sets. let X be the set containing those sets.

a) (Minimal Element) $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$

b) (Maximal Element) $A \cup X = X$ and $A \cap X = A$

c) (Identity) $A \cap A = A$ and $A \cup A = A$

d) (Commutativity) $A \cap B = B \cap A$ and $A \cup B = B \cup A$

e) (Associativity) Unions and Intersections are Associative.

f) (Distributivity) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

g) (Partition) $A \cup (X \backslash A) = X$ and $A \cap (X \backslash A) = \emptyset$

h) (De Morgan) $X \backslash (A \cup B) = (X \backslash A) \cap (X \backslash B)$ and $X \backslash (A \cup B) = (X \backslash A) \cup (X \backslash B)$

Proofs:

a) $A \cup \emptyset = A$: Let $x \in A \cup \emptyset$ then either $x \in A$ or $x \in \emptyset$. We know from the empty set axiom that $x \notin \emptyset$, so that means $x \in A$.
Let $x \in A$. Assume $x \notin A \cup \emptyset$. Then $x \notin A$ and $x \notin \emptyset$. But $x \in A$. So this is a contradiction, so $x \in A \cup \emptyset$. Therefore $A \cup \emptyset = A$.

$A \cap \emptyset = \emptyset$: We use the definition of the intersection: $x \in A \cap \emptyset \Leftrightarrow (x \in A \text{and} x \in \emptyset)$. This statement is always false, so for an arbitrary x, $x \notin A \cap \emptyset$. This is the definition of the empty set, so $A \cap \emptyset = \emptyset$.

b) $A \cup X = X$: let $x \in A \cup X$. Then $x \in A$ or $x \in X$. Let $x \in A$, then because $A \subset X$, $x \in X$. Therefore, if $x \in A \cup X$ then $x \in X$.
let $x \in X$. Assume $x \notin A \cup X$, then $x \notin A$ and $x \notin X$, but $x \in X$, so we must have $x \in A \cup X$. Therefore $A \cup X = X$.

$A \cap X = A$: let $x \in A \cap X$. Then $x \in A$ and $x \in X$, so $x \in A$.
let $x \in A$ and assume $A \subset X$. Because $x \in A$ and $A \subset X$, $x \in X$. Because $x \in A$ and $x \in X$, $x \cap X$. Concluding: $A \cap X = A$.

c) $A \cap A = A$: Let $x \in A \cap A'$, assume $A = A'$. We have $x \in A$ and $x \in A'$. in either case $x \in A$, so $x \in A$.

$A \cup A$: Let $x \in A \cup A'$, assume $A = A'$. Assume $x \notin A$, then $x \in A'$, but $A = A'$, so $x \in A$ which is a contradiction. So $x \in A$.

d), e), f) From the commutativity, associativity and distributivity of the logical connectives.

g) $A \cup (X \backslash A) = X$: Assume $A \subset X$. let $x \in A \cup (X \backslash A)$: Then $x \in A$ or $x \in X \backslash A \Leftrightarrow (x \in X \wedge x \notin A)$. Assume $x \notin A$, then $x \in X \wedge x \notin A$, so $x \in X$.
Assume $x \notin X \backslash A$, then $x \in A$, and because $A \subset X$, $x \in X$.
Let $x \in X$
Proof by contradiction: assume that $x \notin A \cup (X \backslash A)$, then we have that $x \notin A \wedge (x \notin X \vee x \in A)$. As we have that $x \notin A$ and $\notin X \vee x \in A$, we know that $x \notin X$, however this contradicts that $x \in X$. Therefore, it must mean that $x \in X \cup (X \backslash A)$

$A \cap (X \backslash A) = \emptyset$: Assume $A \subset X$. Proof by contradiction, assume that there is an element in $A \cap (X \backslash A)$. So $x \in A \cap (X \backslash A)$, then $x \in A$ and $x \in X \backslash A$, which means that

$x \in X$ and $x \notin A$, so there is a contradiction that $x \in A$ and $x \notin A$, so we know that such an element does not exist. As there are no elements in $A \cap (X \setminus A)$ we know that it must be equivalent to $\emptyset$.

h) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$: Let $x \in X \setminus (A \cup B)$, then $x \in X$ and $x \notin A \cup B$, so that $x \notin A$ or $x \notin B$. Then we know that $x \in X$ and $x \notin A$ or $x \in X$ and $b \notin B$, which is $x \in (X \setminus A) \cap (X \setminus B)$.

The rest is proved by the same principle.

3.2 Functions

3.2.1 Definition of Functions

Let X, Y be sets, and let $P(x, y)$ be a property pertaining to $x \in X$ and $y \in Y$ such that for every x there is exactly one y for which the property is true. Then the function $f : X \to Y$ is the object which assigns every input x an output $f(x)$ defined such that $P(x, f(x))$ is true. So, for any x, y

$$y = f(x) \Leftrightarrow P(x, y) istrue$$

Functions are also referred to as maps or transformations, sometimes also morphisms.

3.2.2 Definition of equality of functions

Two functions $f : X \to Y$ and $g : X \to Y$ are equal, $f = g$ if and only if $f(x) = g(x)$ for all $x \in X$.

3.2.3 Definition of Composition of functions

Let $f : X \to Y$ and $g : Y \to Z$ be functions, then we define the composition $g \circ f : X \to Z$ to be the function which is defined by the formula

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

If the range of f and the domain of g are not equal, then the composition is undefined.

3.2.4 Lemma: Composition is Associative, but not Commutative

let $f : Z \to W$, $g : Y \to Z$ and $h : X \to Y$ be functions. Then $f \circ (g \circ h) = (f \circ g) \circ h$, but in general $f \circ g \neq g \circ f$.

Associativity, Proof: Both functions have the same range, that is $X \to W$. We have to see that the functions are equal for all $x \in X$. We use the definition of composition

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

3.2.5 Definition of One-to-one functions (Injectivity)

a function f is one-to-one if different elements map to different elements

$$x \neq x' \Rightarrow f(x) \neq f(x')$$

or equivalently, the contraposition

$$f(x) = f(x') \Rightarrow x = x'$$

3.2.6 Definition of onto functions (surjectivity)

a function f is onto if $f(X) = Y$. So, every element in Y comes from applying f to some element in X

$$\forall y \in Y \; \exists x \in X \; (f(x) = y)$$

3.2.7 Definition of Bijective functions

a function is bijective if it is surjective and injective.

3.2.8 Definition of inverse functions

If $f : X \to Y$ is bijective then there exists exactly one $x \in X$ for every $y \in Y$ such that $f(x) = y$. This value is denoted $x = f^{-1}(y)$. f^{-1} is called the inverse function and is a function from Y to X.

3.2.9 Exercises

1.

Show that the equality of functions is reflexive, symmetric and transitive.

- reflexivity: let f be a function and let x be arbitrary. Then $f(x) = f(x)$. As x is arbitrary it holds for all x, so $\forall x(f(x) = f(x))$. Thus equality is reflexive.
- symmetry: let f, g be functions and let $f = g$. Let x be arbitrary, then because $f(x) = g(x)$ we know that $g(x) = f(x)$. Because x is arbitrary, $\forall x(g(x) = f(x))$ which means $g = f$.
- transitivity: let f, g, h be functions. let $f = g$ and $g = h$. Let x be arbitrary, then $f(x) = g(x)$ and $g(x) = h(x)$. Then we have $f(x) = h(x)$ through the transitivity of the equality. As x is arbitrary we have $\forall x(f(x) = h(x)$, which means $f = h$.

Verify the substitution property of the composition
Proof: let $f, g, \tilde{f}, \tilde{g}$ be functions, and let $f = \tilde{f}$ and $g = \tilde{g}$.

$$(g \circ f)(x) = g(f(x)) = \tilde{g}(\tilde{f}(x)) = (\tilde{g} \circ \tilde{f})(x)$$

where the second equality holds because $\forall x(g(x) = \tilde{g}(x) \wedge f(x) = \tilde{f}(x))$

2.

Let $f : X \to Y$ and $g : Y \to Z$ be functions, show that if f and g are injective then so is $g \circ f$, as is the same for surjectivity.

- Injectivity: let f, g be injective. we then define the composition $g \circ f = g(f(x))$. We want to show that $g \circ f$ is injective. let $x, x' \in X$ be elements such that $x \neq x'$. Then we know that $f(x) \neq f(x')$, where $f(x), f(x') \in Y$. We also know that for two elements $y, y' \in Y$ with $y \neq y'$, $g(y) \neq g(y')$. Then, as we know that $f(x) \neq f(x')$ we know that $g(f(x)) \neq g(f(x'))$. This means that $x \neq x' \Rightarrow g(f(x)) \neq g(f(x'))$, which is the desired result.
- Surjectivity: let f, g be surjective. We define the composition $g \circ f = g(f(x))$. We will show that $\forall z \in Z \exists x \in X (g(f(x)) = z)$. We know that there exists some y such that $g(y) = z$, we also know that there exists some x such that $f(x) = y$, which means that there exists some x such that $g(f(x)) = z$, whis is the desired result

3.

When is the empty function injective, surjective, bijective?
idk what to say

4.

Let $f, \tilde{f} : X \to Y$ and $g, \tilde{g} : Y \to Z$ be functions. Show the cancellation laws for composition.

- Injective g: Let $g \circ f = g \circ \tilde{f}$ and let g be injective, show that $f = \tilde{f}$. We know that $\forall x (g(f(x)) = g(\tilde{f}(x)))$ Injectivity means that $g(y) = g(y') \Rightarrow y = y'$. As this is the case, we know that $\forall x (f(x) = \tilde{f}(x))$. If g is not injective, then there may exist two elements y, y' such that $g(y) = g(y')$ and $y \neq y'$. With this, we know that there could be an x such that $f(x) \neq \tilde{f}(x)$, which means that f and $\tilde{f}$ aren't equal. So in general, this only holds for injective g.
- Surjective f: Let $g \circ f = \tilde{g} \circ f$ and let f be surjective, show that $g = \tilde{g}$. We know that $\forall x (g(f(x)) = \tilde{g}(f(x)))$. Let $y \in Y$ be arbitrary. From f's surjectivity we know that there exists an $x \in X$ s.t. $f(x) = y$. Replace $f(x)$ with y in the previous equality, and we get $g(y) = \tilde{g}(y)$. As y is arbitrary, $\forall y \in Y (g(y) = \tilde{g}(y))$. So we have $g = \tilde{g}$.

5.

let $f : X \to Y$ and $g : Y \to Z$ be functions. Show that if $g \circ f$ is injective then f is injective.

Proof: let $g \circ f$ be injective, then $g(f(x)) = g(f(x')) \Rightarrow x = x$. Proof by contradiction, assume that f is not injective, so $\exists x, x' \left(x \neq x' \wedge f(x) = f(x')\right)$. From the definition of the function we know that $y = y' \Rightarrow g(y) = g(y')$. Inserting $f(x) = f(x') = y$ we get $g(f(x')) = g(f(x))$. Then, $x \neq x$, even though $g(f(x)) = g(f(x')) \Rightarrow x = x'$. So f must be injective.

Show that if $g \circ f$ is surjective then g is surjective.

Proof: let $g \circ f$ be injective, then $\forall z \exists x(g(f(x)) = z)$. Let z be arbitrary. We can find an x such that $g(f(x)) = z$. Evaluating $f(x) = y$ we get the desired result. As z is arbitrary, we have $\forall z \exists y(g(y) = z)$.

6.

Let $f : X \to Y$ be a bijective function and let $f^{-1} : Y \to X$ be its inverse.

Proof: For every $y \in Y$ value we have exactly one $x \in X$ such that $f(x) = y$ the value for x is then $f^{-1}(y)$. Then, we see that $f(f^{-1}(y)) = y$. Also knowing that $f(x) = y$ and that $f^{-1}(y) = x$ we see that $f^{-1}(f(x)) = x$.

3.3 Images and Inverse Images

3.3.1 Definition of Images of sets

Let $f : X \to Y$ be a function and $S \subset X$ then we define the set $f(S)$

$$f(S) := \{f(x) | x \in S\}$$

this set is a subset of Y. Then we say that S is the *Image* of S under f and $f(S)$ is the *forward image*.

Example

Take the map $f(x) = 2x$. Then we calculate

$$f(\{1, 2, 3\}) = \{2, 4, 6\}$$

Theorem

$$y \in f(S) \iff \exists x \in S(y = f(x))$$

3.3.2 Definition of Inverse images

If U is a subset of Y, then the set $f^{-1}(U)$ is defined as

$$f^{-1}(U) := \{x \in X | f(x) \in U\}$$

so $f^{-1}(U)$ is the set of all elements that map into U.

$$f(x) \in U \iff x \in f^{-1}(U)$$