# Math: how things do stuff.

Clémence Chanavat

July 25, 2023

## Contents



# 1 Introduction

Mathematics is about things, and how they do stuff. What is a thing, what can they do, and what it means to do is the subject of this class. We will start with discovering the underlying language of mathematics, the one that will allows us to discuss with it. It is called *logic*. It will be needed to understand what is a mathematical thing, what is a mathematical stuff, and how mathematics do things. Once this will be done, we will move on to the basics building blocs of mathematics, the one that are everywhere and that are useful to construct all sorts of other things that will do all sort of amazing stuff. Those are sets and functions. A function is the most general instance of a mathematical thing, even worse, math is in fact the study of functions.

**Definition 1:** A function is a thing that do stuff.

That is it, that is math. We could stop here, but so far, it would not be very useful to do anything. Rather, what we will do is specify finer and finer behavior to our functions, and to the thing they produce so that we can say meaningful stuff about it. *TODO*

- prove something is unique
- prove forall
- prove exists

# 2 Logic

## 2.1 Connective

Mathematics is a language made of sentences. In this section, we learn the basics of its grammar, and how to make well formed sentences. Then, given a well formed sentence, we see a general procedure to see wether a given sentence is true or false. We start with a few list of symbols, that constitute the basic alphabet of mathematics. It is primordial to know them, they are called *connectives*. We have

1. The *and*, noted $\wedge$.

2. The *or*, noted $\vee$.

3. The *not*, noted $\neg$.

4. The *implies*, noted $\Rightarrow$.

5. The *equivalent*, noted $\iff$.

As in any language, these symbols have a meaning, that somewhat correspond to the intuition. To understand it, let us abbreviate with the letter $C$, the sentence *the cat is orange*, and with $D$ the sentence *the dog has three legs*. Then, we write

$$C \wedge D$$

to mean that both the cat is eating *and* the dog is sleeping. Then whenever I see the cat, it is orange, and whenever I see the dog, it has three leg.

Next is the or. It is a little bit different than what we are used to in the English language. We write

$$C \vee D$$

to mean that the cat is orange, *or* the dog has three leg. This means that at least one of the three following statements is true:

1. The cat is orange,

2. The dog has three legs,

3. The cat is orange, and the dog has three legs.

In math, the or connective need to to be exclusive. In $C \vee D$, both $C$ and $D$ can be true. It means that after seeing the cat and the dog, I am guarantee that at least the cat will be orange, or the dog will have three legs, at least one of the two statements will be true.

The next connective of interest is not. We write

$$\neg D$$

to mean that the dog has *not* three legs, that is whenever I will see the dog, it will have some number of legs and I am guarantee that this number is not three. It can be one, it can be four, it can be something else, but it will not be three.

**Exercise 1:** Argue that $\neg(C \wedge D)$ says the same thing as $\neg C \vee \neg D$.

We move on to equivalence. We write

$$C \iff D$$

to mean that knowing that the cat is orange is the same thing as knowing that the dog has three leg. It means that if I go first see the cat to see it orange, then I do not need to go to the dog to see it has three leg. I already know it. Conversely, if I go first see the dog, and it has three legs, then I am sure that the cat is orange.

**Exercise 2:** Argue that $C \iff D$ says the same thing as $D \iff C$.

Finally, we have the implication. It is the most used of them all. We write

$$C \Rightarrow D$$

to mean that *if* the cat is orange, *then* the dog has three legs. It says that if I go see the cat and constate it is orange, then I am guarantee that the dog will have three legs. However, and this is very important, if I do not see that the cat is orange, then I *cannot* say anything at all about the dog.

**Exercise 3:** Argue that $(C \Rightarrow D) \wedge (D \Rightarrow C)$ says the same thing as $C \iff D$. Is $C \Rightarrow D$ saying the same thing as $D \Rightarrow C$?

Notice that when we will do math later, we will freely employ the symbol themselves, or their equivalent English terminology. In particular, we write "if $X$ then $Y$" more often than "$X \Rightarrow Y$", but keep in mind that they are the same thing. We summarize these constructions with truth tables, you should refer to these when in doubt on what a sentence mean. Here is how to read it. The number 1 means True, the number 0 means False. In the table for $\vee$, on a given row, a column gives a particular truth value to $C$, to $D$, and to the resulting $C \vee D$. For instance, if $C$ is true, $D$ is false, we see that $C \vee D$ is true.

| $C$ | $\neg C$ |
|---|---|
| 0 | 1 |
| 0 | 0 |

,

| $C$ | $D$ | $C \wedge D$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

,

| $C$ | $D$ | $C \vee D$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |

,

| $C$ | $D$ | $C \iff D$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

,

| $C$ | $D$ | $C \Rightarrow D$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

## 2.2 Quantifiers

So far, we cannot really say much. We need to introduce two new symbols:

$$\forall, \exists.$$

They will allow us to quantify, to say that all things in a big thing share the same property, or that there is some thing in a big thing that has a property. However, there is some subtleties that comes with those symbols, we need to use free variables. Earlier, I said $D$ means that the dog has three legs. There is no room in this formula, everything is fixed. Allow me to do something, and replace three with the letter $n$, that will I declare to be an unspecified natural number. Now, I write

$$D(n)$$

to mean that the dog has $n$ legs, for some number $n$, that I deliberately *not* specify. This $n$ is called a free variable, it can potentially be any natural number, and it is good to think of it as being *all* the natural number at the same time. Now, if I take a natural number, say 7, then I will write $D(7)$ to specify the unknown number $n$ with 7, and $D(7)$ means that the dog has seven leg. Notice that our previous sentence $D$ is now the same thing as $D(3)$.

Is the sentence $D(n)$ true or false? It does not make sense to ask this question. We cannot ask for the truth value of a sentence with free variables, we first need to specify a behavior for our free variable, and this is done with the quantifier. We write

$$\exists n, D(n)$$

to mean that there *exists* at least a value of $n$ (like 4, 9, or seven billion) such that the dog has $n$ legs. For instance, I know $\exists n, D(n)$ is true because when I will look at my dog, I will count its number of legs, and see that there is $n = 4$. We say that 4 is a *witness* of $\exists n, D(n)$.

Next, we write

$$\forall n, D(n)$$

to mean that *for all* choice of number $n$, my dog will have precisely this number of legs. Here, this is quite absurd, because my dog has one and only one number of leg. But consider the following:

$$\forall n, (5 \leq n \Rightarrow \neg D(n)).$$

It means that for all number $n$, if the number $n$ is greater or equal to 5, then my dog has not $n$ legs. This feels more true, as I know indeed that my dog has four legs.

**Exercise 4:** Is $\exists n, \neg D(n)$ true? Can you rewrite $\neg \exists n, \neg D(n)$ with something with less symbols?

## 2.3 Practical sentences, and how to do proofs

This was only the tip of the iceberg, and logic is a very powerful language to talk with math. Ultimately, we will also want to do proofs. This section is a practical place that you are invited to reread every time you do not know how to start a proof, or do an exercise.

*TODO*

- forall proof
- exists prove
- prove unique
- :=

# 3 Sets and functions

We arrive to our first objects of interest, sets and functions. We cannot really give a precise definition of what a set is, it is a very far reaching question, and we will content ourselves (that will be enough for our applications), of a very intuitive definition. I am saying here that we will base the entire building of mathematics on something that we do not define precisely. This is crazy, but in fact, this is also what is happening in general. However, we try to reduce the part that we leave to intuition to a smaller and more specific chunk that we then build around, and we can study further. Here, we will be shaky, and treat sets as primitive objects with given sets of rule and syntax, that we will familiarize with.

## 3.1 Sets

**Definition 2:** A *set* $X$ is something. The syntax

$$x \in X$$

means that we took something, named $x$, inside the set $X$. We call $x$ an *element* of $X$. If there is a bunch of things $x_1, \dots, x_n$, and I want to make a set out of them, we use the syntax:

$$\{x_1, \cdots, x_n\}.$$

We will see later more advanced construction to make better sets.

We can create sets of almost (and this "almost" might be the most important "almost" of math) anything. For instance, here are a bunch of classical sets, that can be defined more precisely from smaller sets, but again, we do not have time to enter into such details.

**Example 3:** Here are some examples of sets:

- $\emptyset$ is the *empty set*, the set with nothing in it.
- $\mathbb{N}$ is the set of *natural numbers*, inside it are the numbers $0, 1, 2, \cdots$.
- $\mathbb{Z}$ is the set of *integers*, inside it are the numbers $\cdots, -2, -1, 0, 1, 2, \cdots$.
- $\{a, b\}$ is the set with two elements, called for the occasion $a$ and $b$.

**Exercise 5:** Argue that for all $x \in \emptyset$, $x = 0$, and that for all $x \in \emptyset$, $x = 1$. What is happening here, did we just prove $0 = 1$?

**Definition 4:** Let $X$ and $Y$ be two sets. We say that that $X$ is *included* in $Y$, and write $X \subseteq Y$ if

$$\forall x \in X, x \in Y.$$

We that that $X$ and $Y$ are equal if $X \subseteq Y$ and $Y \subseteq X$.

**Exercise 6:** Argue that two sets $X$ and $Y$ are equal is to say

$$\forall x, x \in X \iff x \in Y.$$

**Exercise 7:** Prove that $\mathbb{N} \subseteq \mathbb{Z}$.

Let us see a very useful way to build sets from other. It goes formally by the name of *replacement* axiom, and is one of the foundational tool of mathematics. We present it a little bit informally here.

**Definition 5:** Let $X$ be a set, and $\phi(x)$ a formula that depends on a parameter $x$ allowed to vary in $X$. Then we define the set

$$\{x \in X \mid \phi(x)\}$$

to be the subset of $X$ whose elements are precisely those of $X$ that makes $\phi$ true.

**Example 6:** We can use the formula $\phi(n) := n \geq 0$ to define the natural from the integer, indeed:

$$\mathbb{N} = \{n \in \mathbb{Z} \mid n \geq 0\}.$$

**Exercise 8:** Using replacement, define the set of even number from the set of natural numbers.

There are very important operations that we can do with sets. First, we have union, intersection, and complement. They are analogous to the logical operation we saw previously.

**Definition 7:** Let $X, Y$ be two sets. We define the *intersection* of $X$ and $Y$ by

$$X \cap Y := \{x \mid x \in X \text{ and } x \in Y\}.$$

We define the *union* of $X$ and $Y$ by

$$X \cap Y := \{x \mid x \in X \text{ or } x \in Y\}.$$

Let $A \subseteq X$. We define the *complement* of $A$ in $X$ to be the set

$$X \backslash A := \{x \in X \mid x \notin A\}.$$

The syntax $x \notin A$ is just a shorthand for $\neg(x \in A)$, the same way $x \neq y$ is shorthand for $\neq (x = y)$.

**Exercise 9:** Prove that, for all sets $X, Y, Z$, we have

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

Prove that for all $A, B \subseteq X$, we have

$$X \backslash (A \cup B) = (X \backslash A) \cap (X \backslash B).$$

Does it remind you of something?

Next, we have the product of sets. It is axiomatic in the theory, so we cannot define it from smaller primitive.

**Definition 8:** Let $X, Y$ be sets. The *product* of $X$ and $Y$ is the set

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

constituted of all the pairs $(x, y)$ for $x \in X$ and $y \in Y$.

**Example 9:** We have the following products:

- $\{0, 1\} \times \{a, b, c\} = \{(0, a), (0, b), (0, c), (1, a), (1, b), (1, c)\}$.
- For all set $X$, $X \times \emptyset = \emptyset$.

**Exercise 10:** If $X$ has $n$ elements, and $Y$ has $m$ elements, how many elements has $X \times Y$?

Another primitive of sets is the power set. The power set of a set is another set that contains all the subset of the set with started with.

**Definition 10:** Let $X$ be a set. We define the set $2^X$ (also written $\mathcal{P}(X)$) to be the set

$$2^X := \{A \mid A \subseteq X\}.$$

**Example 11:** We have the following power sets.

- $2^{\{}0, 1\} = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.
- $2^{\emptyset} = \{\emptyset\}$.

Notice that $\emptyset$ is very different from $\{\emptyset\}$. The former has zero elements, while the latter has one.

**Exercise 11:** If $X$ has $n$ elements, how many elements has $2^X$?

## 3.2 Functions

Function are the most fundamental objects of mathematics. A function can describe all sorts of thing, it is something that takes an input and produces an output. It is very convenient to declare inputs and outputs to be sets. Then the function will take anything from the input set, and give something in the output set.

**Definition 12:** Let $X, Y$ be two sets. A function $f$ between $X$ and $Y$ is a thing that, for all $x \in X$, gives an element $f(x) \in Y$. We write

$$f : X \to Y.$$

$X$ is called the *domain* of $f$, and $Y$ is called the *codomain*. If we want to specify further the behavior of the function, we can use the following syntax

$$\begin{aligned} f : X &\to Y \\ x &\mapsto f(x) \end{aligned}$$

Note that a function is an asymmetric notion, the domain and the codomain are highly non-interchangeable.

**Example 13:** Here are a bunch of functions, and some various way of syntactically defining them (which are all equivalent, we often use the one that is more convenient).

- *A function that doubles its input.*

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N} \\ x &\mapsto 2x \end{aligned}$$

- *A function that says if something is true.* Let $f : \mathbb{N} \to \{\text{true}, \text{false}\}$ be the function such that $f(x) = \text{true}$ if $x = 57$, and $f(x) = \text{false}$ else.
- *The function that does nothing.* Let $f : X \to X$ be the function sending $x$ to itself.

The last example is so fundamental that it deserves its own definition.

**Definition 14:** Let $X$ be a set, we call $\mathrm{id}_X$ the function defined by

$$\begin{aligned} \mathrm{id}_X : X &\to X \\ x &\mapsto x \end{aligned}$$

. We call it the *identity* on $X$.

**Definition 15:** Let $f, g : X \to Y$ be two functions, we say that $f = g$ if for all $x \in X$, we have $f(x) = g(x)$. This principle is called *extensionnality*.

Beware that the domain and the codomain are part of the data of a function, that is the function

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N} \\ x &\mapsto x + 1 \end{aligned}$$

and the function

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{Z} \\ x &\mapsto x + 1 \end{aligned}$$

are not the same, even though they have the same behavior and produce the same outputs.

We now define some important data associated to a function.

**Definition 16:** Let $f : X \to Y$ be a function. Let $A \subseteq X$, the *image* of $A$ through $f$ is the subset of $Y$ defined by

$$f(A) := \{y \in Y \mid \exists x \in A, f(x) = y\}.$$

Let $B \subseteq Y$, the *preimage* of $B$ through $f$ is the subset of $X$ defined by

$$f^{-1}(B) := \{x \in X \mid f(x) \in B\}.$$

Be careful that we overload the notation $f(-)$ with, in place of element of the sets, sets themselves, therefore if $x \in X$ and $A \subseteq X$, then writing $f(x)$ and $f(A)$ is two very distinct things.

**Exercise 12:** Let $f : \mathbb{N} \to \mathbb{N}$ be the function defined by $f(x) = 2x$. What is the set $f(\mathbb{N})$? Let $\mathcal{O}$ be the subset of $\mathbb{N}$ constituted of odd numbers. What is the set $f^{-1}(\mathcal{O})$?

**Exercise 13:** Let $f : X \to Y$ be a function, let $A, A' \subseteq X$ and $B, B' \subseteq Y$. Prove some of the following identities (they are very useful to know, or at least remember they exist).

- $f(A \cup A') = f(A) \cup f(A)$.
- $f(A \cap A') \subseteq f(A) \cap f(A')$.
- $f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$.
- $f^{-1}(B \cap B') \subseteq f^{-1}(B) \cap f^{-1}(B')$.
- $f^{-1}(f(X)) = X$.
- $f^{-1}(f(A)) \supseteq A$.
- $f(f^{-1}(Y)) = f(X)$.
- $f(f^{-1}(B)) \subseteq B$.

It is even a better exercise to try to come up with a example where the full equality fails, for instance provide a function where we do not have $f(A \cap B) = f(A) \cap f(B)$. For a more exhaustive list of these relations, see this Wikipedia page.

We can serialize function, that is if we have a function $f : X \to Y$, and a function $g : Y \to Z$, we can consider the function that does $f$, then $g$.

**Definition 17:** Let $f : X \to Y$ and $g : Y \to Z$ be function such that the codomain of $f$ is the domain of $g$. We define the function $g \circ f$ to be $g \circ f(x) := g(f(x))$. We call it the *composition* of $f$ and $g$.

**Definition 18:** Let $f : X \to Y$ be a function. An *inverse* to $f$ is a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$.

Composition is what we call a partial operation, not all functions can be composed: the output of the first one needs to match the input of the second one.

**Example 19:** Let $f : \mathbb{N} \to \mathbb{N}$ be the function defined by $f(x) = 2x$, and $g : \mathbb{N} \to \mathbb{N}$ be the function defined by $g(x) = x + 1$. Compute the functions $g \circ f$ and $f \circ g$.

**Lemma 20:** If $f : X \to Y$ has an inverse, then it is unique.

*Proof.* (**Lemma 20**) Let $f : X \to Y$ be a function, and suppose we have two inverses $g, g' : Y \to X$. Let $y \in Y$, we have by definition $y = f \circ g(y)$, thus applying $g'$ both sides gives

$$g'(y) = g' \circ f \circ g(y),$$

and thus, as $g' \circ f = \mathrm{id}_X$, we have

$$g'(y) = g' \circ f \circ g(y) = g(y).$$

We conclude that for all $y \in Y$, $g(y) = g'(y)$, thus by extensionality, $g = g'$. $\square$

Therefore, Lemma 20 allows us to use the notation $f^{-1}$ for *the* unique inverse of $f$, when it exists. Be careful that $f^{-1}$ might not always exists, and is in conflict with the notation $f^{-1}(B)$ (which is always well defined), and both do not mean the same thing.

**Exercise 14:** Provide a function that has an inverse, and a function that does not have an inverse.

**Exercise 15 (Conflict of notation):** Let $f : X \to Y$ be a function that admits an inverse, and let $B \subseteq Y$. Prove that

$$f^{-1}(B) = f^{-1}(B),$$

where the $f^{-1}(B)$ on the left is the preimage of $B$ through $f$, and $f^{-1}(B)$ on the right the the image of $B$ through the function $f^{-1}$.

We conclude this section on functions by three very important notions.

**Definition 21:** Let $f : X \to Y$ be a function. We say that:

- $f$ is *injective* if
$$\forall x, y \in X, f(x) = f(y) \Rightarrow x = y.$$
- $f$ is *surjective* if
$$\forall y \in Y, \exists x \in X, f(x) = y.$$
- $f$ is *bijective* if it is both injective and surjective.

**Exercise 16:** Prove that the function from $\mathbb{N}$ to $\mathbb{N}$ that adds 1 to a number is injective. Is it surjective? Prove that the function from $\mathbb{Z}$ to $\mathbb{Z}$ that add one to a number is bijective.

**Exercise 17:** Let $f : X \to Y$ be a function. Let $f' : X \to f(X)$ defined by letting $f'(x) = f(x)$. Prove that $f'$ is surjective.

In fact (under the axiom of choice), being bijective is equivalent to having an inverse.

**Proposition 22:** Let $f : X \to Y$ be a function with $X \neq \emptyset$. We have

- $f$ is injective if and only if there exists $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$.
- $f$ is surjective if and only if there exists $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$.
- $f$ is bijective if and only if it admits an inverse.

*Proof.* (**Proposition 22**) Suppose $f : X \to Y$ is injective. As $X \neq \emptyset$, select any $x_0 \in X$. To define $g : Y \to X$, take $y \in Y$, if there is some $x \in X$ such that $f(x) = y$, define $g(y) := x$, else define $g(y) := x_0$. By construction, for all $x \in X$, $g(f(x)) = x'$, where $x'$ is such that $f(x') = f(x)$, by injectivity, this means $x = x'$, thus $g(f(x)) = x$. Conversely, suppose $f$ has a left inverse $g$, and suppose $f(x) = f(y)$, then applying $g$ both sides yields $g(f(x)) = g(f(y))$, that is $x = y$, so $f$ is injective.

Next, suppose $f$ is surjective. We construct $g : Y \to X$ as follow. For all $y \in Y$, we pick any element $x \in f^{-1}(\{y\})$, and we let $g(y) = x$. We can always pick such an element, as being surjective means precisely that for all $y \in Y$, the set

$$f^{-1}(\{y\}) = \{x \in X \mid f(x) = y\}$$

is non empty, so we can choose an element inside. (This last affirmation is quite subtle, to see that, Google "axiom of choice"). We then have, by construction, $f(g(y)) = y$, as $g(y) \in f^{-1}(\{y\})$. Conversely, if $f$ admits a right inverse $g$, then for all $y \in Y$, $f(g(y)) = y$, so the element $g(y) \in X$ witness the existential quantifier for surjectivity.

Last, suppose $f$ is bijective, then is is both surjective and injective, so by what we juts proved, there is a function $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$, and a function $g' : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ (they need not to be the same so far). Let $y \in Y$, we have

$$g'(y) = g'(f \circ g(y)) = (g' \circ f)(g(y)) = g(y),$$

so $g = g'$, and thus $f$ has an inverse. Conversely, suppose $f$ has an inverse, then it is in particular a left inverse, so $f$ is injective, and it is also a right inverse, so $f$ is surjective, hence $f$ is bijective. $\square$

The following exercise emphasizes that the domain and codomain are *really* part of the data of a function.

**Exercise 18:** Determine if the following functions are injective, surjective, bijective, or none. WE call $\mathbb{R}^+$ the set of real numbers greater or equal to 0.

- $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x^2$.
- $f : \mathbb{R}^+ \to \mathbb{R}$ such that $f(x) = x^2$.
- $f : \mathbb{R} \to \mathbb{R}^+$ such that $f(x) = x^2$.
- $f : \mathbb{R}^+ \to \mathbb{R}^+$ such that $f(x) = x^2$.

### 3.3 Equivalence relations

Sometimes we have a set, and we would like to make things inside it *more* equal to each other. For instance, let us take the set $\mathbb{N}$. So far, if we take $n, m \in \mathbb{N}$, then $m = n$ if they are the same number. We would like to say that all even number are equal to each other, while all odd numbers are also equal to each other. The resulting set would then be a set with two elements, for each parity. One element would represent all the even numbers, and the other one all the odd number. There is a very general way to do that called equivalence relation. We introduce it here because equivalence relations are pervasive in mathematics, and we will see them many times during this class. They are a little bit weird to talk about, and to define functions on them can be counter intuitive.

**Definition 23:** Let $X$ be a set. A *binary relation* $\sim$ on $X$ is a subset of $X \times X$. If $(x, y) \in \sim$, we simply write

$$x \sim y.$$

**Definition 24:** Let $X$ be a set, and $\sim$ a binary relation on $X$. We say that

- $\sim$ is *reflexive* if
$$\forall x \in X, x \sim x.$$
- $\sim$ is *symmetric* if
$$\forall x, y \in X, x \sim y \Rightarrow y \sim x.$$
- $\sim$ is *reflexive* if for all $x \in X$, $x \sim x$.
$$\forall x, y, z \in X, (x \sim y \wedge y \sim z) \Rightarrow x \sim z.$$

A reflexive, symmetric, transitive relation is called an *equivalence relation*.

**Example 25:** The most famous equivalence relation of them all is simply the relation $=$. Indeed, $x = x$, if $x = y$, then $y = x$, and if $x = y$ and $y = z$, then $x = z$. It is good to think of equivalence relations as extended equality.

**Definition 26:** Let $(X, \sim)$ be a set with an equivalence relation. We define the *equivalence class* of $x$, written $[x]$, or $\mathrm{cl}(x)$, to be the set

$$[x] := \{y \in X \mid x \sim y\}.$$

If $y \in [x]$, we say that $y$ is a *representative* of $[x]$. Of course, $x$ is a representative of $[x]$.

**Lemma 27:** Let $(X, \sim)$ be a set with an equivalence relation. We have that $x \sim y$, if and only if $[x] = [y]$.

*Proof.* (Lemma 27) Suppose $x \sim y$. Take any $z \in [x]$, then by definition $x \sim z$. By symmetry, also $y \sim x$, so by transitivity, $y \sim z$, hence $z \in [y]$. We proved $[x] \subseteq [y]$. Conversely, take $z \in [y]$, then $y \sim z$, and as $x \sim y$, by transitivity $x \sim z$ so $z \in [x]$, hence $[y] \subseteq [x]$, proving $[x] = [y]$. Conversely, if $[x] = [y]$, then as $y \in [y]$, also $y \in [x]$, so $x \sim y$. $\square$

**Definition 28:** Let $(X, \sim)$ be a set with an equivalence relation. We define the *quotient* of $X$ by $\sim$, written $X/\sim$, to be the set

$$X/\sim := \{[x] \mid x \in X\}.$$

We have a function $p : X \to X/\sim$, called the *canonical projection*, that sends $x$ to $[x]$.

**Remark 29:** Suppose $f : X \to Y$ is a function such that for all $x, y \in X$, if $x \sim y$, then $f(x) = f(y)$. Then $f$ defines a function $\bar{f} : (X/\sim) \to Y$ defined by $f([x]) = f(x)$. This does not depends on the choice of representative, for if $[x] = [y]$, by Lemma 27, $x \sim y$, so we have $f(x) = f(y)$, hence $\bar{f}([x]) = \bar{f}([y])$.

**Exercise 19:** Define $\sim$ on the natural number by letting $n \sim m$ if and only if $m$ and $n$ have same parity. Show that this is an equivalence relation, and that the set $\mathbb{N}/\sim$ has two elements. Show that the canonical projection $\mathbb{N} \to \{[0], [1]\}$ acts as the "mod 2" function, by seeing $[0]$ as 0, and $[1]$ as 1. This idea will be further generalized in the lesson on modular arithmetic.

We conclude by a canonical result that will appear here and there under similar forms during this course.

**Theorem 30:** Let $f : X \to Y$ be a function. There exists two (unique) functions $m, p$ such that $p$ is surjective, $m$ is injective, and $f = m \circ p$.

*Proof.* (**Theorem 30**) Let $\sim$ be the equivalence relation on $X$ defined by $x \sim y$ iff $f(x) = f(y)$. We let $p : X \to X/\sim$ be the canonical projection, it is indeed surjective, and we let $m : (X/\sim) \to Y$ to be $\bar{f}$ as in Remark 29. If $m([x]) = m([y])$, then $f(x) = f(y)$, so $x \sim y$, hence by Lemma 27, $[x] = [y]$, so $m$ is injective. Then we have $m \circ p(x) = m([x]) = f(x)$. $\square$

# 4 Groups

Groups are mathematical structure that arise everywhere. Groups encode symmetry in structures, and symmetries are prevalent in math. As this class is computer-science oriented, we will first introduce monoids, that are object slightly more general than groups, and that anyone in computer science already encounter. Typically, when we consider the regular expression $(ab)^*$, we are considering the free monoid on the alphabet $\{a, b\}$.

## 4.1 Monoids

**Definition 31:** Let $X$ be a set. A *binary operation* $\cdot$ on $X$ is a function $\cdot : X \times X \to X$. Instead of writing $\cdot(x, y)$ for the application of $\cdot$ to $(x, y)$, we typically write $x \cdot y$.

**Example 32:** This definition should not be new for you, it is just the abstract version of things we already know.

- The function $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is a binary operation.
- The function $\times : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is a binary operation.
- etc.

**Definition 33:** Let $(X, \cdot)$ be a set with a binary operation. We say that $(X, \cdot)$ is a monoid if

1. There exists a particular element $e \in X$, called the *neutral element*, such that:

$$\forall x \in X, e \cdot x = x = x \cdot e.$$

2. The binary operation is *associative*, that is:

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

In that case, we are allowed to write $x \cdot y \cdot z$ to mean either $x \cdot (y \cdot z)$ or $(x \cdot y) \cdot z$, as they are equal.

**Example 34:** Prove that $(\mathbb{N}, +)$ is a monoid. Is $(\mathbb{R}, \times)$ a monoid? Prove that $(\mathbb{R}^*, \times)$ is a monoid, where by $\mathbb{R}^*$, we mean the set of real number with 0 removed. What is its neutral element?

**Example 35:** A very important monoid is the set with one element $\{e\}$. The binary law is (necessarily) defined by $e \cdot e = e$, and the neutral element is (necessarily) $e$. Check that this is indeed a monoid.

**Lemma 36:** Neutral elements are unique, that is in a monoid $(X, \cdot, e)$, if there is an element $e' \in X$ such that

$$\forall x \in X, e' \cdot x = x = x \cdot e',$$

we have $e = e'$.

*Proof.* (**Lemma 36**) Suppose $e'$ is another neutral element for all $x$ we have

$$e' \cdot x = x,$$

so in particular letting $x = e$, we get $e' \cdot e = e$. Now, $e$ is also neutral element, so for all $x$, we have $x \cdot e = x$, hence with $x = e'$, we get $e' = e' \cdot e$, so $e' = e$. □

**Definition 37:** Let $(X, \cdot, e)$ be a monoid with binary operation $\cdot$ and neutral element $e$. We say that $X$ is *commutative* if

$$\forall x, y \in X, x \cdot y = y \cdot x.$$

**Remark 38:** Here are some common abuse of notation that we do in group theory. We say that *$X$ is a monoid*, where we are supposed to say $(X, \cdot, e)$ is a monoid, the data of the binary law and the neutral element being part of the definition. As they are often explicit from the context, we tend to avoid it, and say simply that $X$ is a monoid.
More often than not, when the monoid is commutative, we write its law $+$, and 0 its neutral element. Beware that these $+$ and 0 have a priori nothing to do with the $+$ and 0 of the natural numbers. It is just that this notation helps us remember that the monoid is commutative, as is the monoid $(\mathbb{N}, +, 0)$.
Also, when $(X, \cdot, e)$ is a monoid, we also like to write $xy$ for $x \cdot y$, like we often write $st$ for $s \times t$.

**Definition 39:** Let $(X, \cdot, e_X), (Y, \cdot, e_Y)$ be monoids, a function $f : X \to Y$ is a *morphism of monoids* if

$$\forall x, y, f(x \cdot y) = f(x) \cdot f(y),$$

and

$$f(e_X) = e_Y,$$

that is $f$ preserves the monoid laws, and it sends the neutral element to the neutral element.

**Exercise 20:** Prove that the exponential function $\exp : (\mathbb{R}, +) \to (\mathbb{R}^*, \times)$ is a morphism of monoids. Is the function

$$\begin{aligned} f : (\mathbb{N}, +, 0) &\to (\mathbb{N}, +, 0) \\ x &\mapsto x + 1 \end{aligned}$$

a morphism of monoids?

**Definition 40:** Let $X$ be a monoid, and let $A \subseteq X$. We say that $A$ is a *submonoid* if it contains the neutral element and is closed under the monoid law, that is $e \in A$, and for all $x, y \in A$, $xy \in A$.

**Definition 41:** Let $f : X \to Y$ be a morphism of monoids. We define the *kernel* of $f$ to be the set

$$\ker(f) := f^{-1}(\{e_Y\}) = \{x \in X \mid f(x) = e_Y\} \subseteq X$$

and the *image* of $f$ to be the set

$$\operatorname{im}(f) := \{f(x) \mid x \in X\} \subseteq Y.$$

(which is the same thing as the set-theoretical image of Definition 16).

The kernel and the image have in fact a structure of monoid, so when one is given with a morphism of monoid, one get two submonoids for free.

**Lemma 42:** Let $f : X \to Y$ be a morphism of monoid. Then $\ker(f)$ is a submonoid of $X$, and $\operatorname{im}(f)$ is a submonoid of $Y$.

*Proof.* (**Lemma 42**) By definition of a morphism of monoid, $f(e_X) = e_Y$, this means $e_X \in \ker(f)$. If $x, y \in \ker(f)$, then

$$f(xy) = f(x)f(y) = e_Y e_Y = e_Y,$$

so $xy \in \ker(f)$. This proves $\ker(f)$ is a submonoid of $X$.

Now for the image, again $f(e_X) = e_Y$, so $e_Y \in f(X) = \operatorname{im}(f)$. If $y, y' \in \operatorname{im}(f)$, then by definition there exist $x, x' \in X$ such that $f(x) = y$ and $f(x') = y'$, so $yy' = f(x)f(x') = f(xx')$, meaning that $yy' \in \operatorname{im}(f)$. This proves that $\operatorname{im}(f)$ is a submonoid of $Y$. □

**Definition 43:** Let $X, Y$ be monoids. We define the product of $X, Y$ to be the monoid whose underlying set is $X \times Y$, the neutral element is the couple $(e_X, e_Y)$, and the law is defined pointwise, that is

$$(x, y) \cdot (x', y') := (x \cdot x', y \cdot y').$$

More generally, if $(X_i)_{i \in I}$ is a family of monoids, we define the product $\prod_{i \in I} X_i$ to be the monoid whose underlying set is $\prod_{i \in I} X_i$, whose neutral element is $(e_{X_i})_{i \in I}$, and whose law is defined pointwise with

$$(x_i)_{i \in I} \cdot (x'_i)_{i \in Y} := (x_i \cdot x'_i)_{i \in I}.$$

**Exercise 21:** Prove that if $(X_i)_{i \in I}$ is a family of monoids, indeed $\prod_{i \in I} X_i$ is a monoid.