Math: how things do stuff.

Clémence Chanavat

July 27, 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*

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.

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	$\neg C$		C	D	$C \wedge D$		C	D	$C \vee D$		C	D	$C \iff D$		C	D	$C \Rightarrow D$
0	1		0	0	0		0	0	0		0	0	1		0	0	1
0	0		0	1	0		0	1	1		0	1	0		0	1	1
			1	0	0		1	0	1		1	0	0		1	0	0
			1	1	1		1	1	1		1	1	1		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.

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

- :=

- prove implies + contrapositive

- prove iff

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 $x_1, \ldots, x_n$, 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 ϕ 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

$$f : X \to Y$$
$$x \mapsto f(x)$$

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.*

$$f : \mathbb{N} \to \mathbb{N}$$
$$x \mapsto 2x$$

- *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 id_X the function defined by

$$\text{id}_X : X \to X$$
$$x \mapsto x$$

. 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

$$f : \mathbb{N} \to \mathbb{N}$$
$$x \mapsto x + 1$$

and the function

$$f : \mathbb{N} \to \mathbb{Z}$$
$$x \mapsto x + 1$$

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, $g = g'$. $\qquad\square$

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.

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 $f(x) = x^2$.

The concept of bijection allows us to talk about finite sets, infinite sets, and cardinality. Let $n \in \mathbb{N}$ be a natural number. We write $[n]$ for the set $\{1, \cdots, n\}$, with convention that $[0] = \emptyset$.

The next lemma is very important. However, it does not really make sense to prove it formally, as we would need to make precise the foundations we are working with, but we did not. We are hence assuming it, and hope it makes sense intuitively.

Lemma 23 (Pigeonhole principle): Let $n, p \in \mathbb{N}$. Then

- There exists an injection $f : [n] \to [p]$ if and only if $n \leq p$.

- There exists a surjection $f : [n] \to [p]$ if and only if $p \leq n$.

- There exists a bijection $f : [n] \to [p]$ if anf only if $n = p$.

Definition 24: A set X is *finite* if there exists some $n \in \mathbb{N}$ such that X is in bijection with $[n]$. In that case, we say that X has cardinality n, we write $|X| = n$, and say that X has *cardinality* n. This is well defined according to Lemma 23, for if $f : X \to [n]$ is a bijection and $f' : X \to [p]$ is a bijection, then $f' \circ f^{-1} : [n] \to [p]$ is a bijection, so $n = p$. Otherwise, we say that X is *infinite*.

Example 25: Let X, Y be sets.

- If X is finite and there is a surjection $X \to Y$, then Y is finite.

- If X is infinite and there is an injection $X \to Y$, then Y is infinite.

- If there is a bijection $X \to Y$, then X is finite if and only if Y is finite, and moreover in that case, the cardinality of X is the one of Y.

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 26: 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 27: 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 $x \in X$, $x \sim x$.

$$\forall x, y, z \in X, (x \sim y \land y \sim z) \Rightarrow x \sim z.$$

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

Example 28: 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 29: 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 30: Let $(X, \sim)$ be a set with an equivalence relation. We have that $x \sim y$, if and only if $[x] = [y]$.

Proof. (**Lemma 30**) 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 31: 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 32: 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 $\bar{f}([x]) = f(x)$. This does not depends on the choice of representative, for if $[x] = [y]$, by Lemma 30, $x \sim y$, 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.

Equivalence relations on a set X are precisely partitions of X. A partition of a set is a way of dividing it into disjoint pieces.

Definition 33: Let X be a set. A partition of X is a collection of subsets $U_{i \in I}$ of X, such that $\bigcup_{i \in I} U_i = X$, and if $i \neq j$, $U_i \cap U_j = \emptyset$.

Proposition 34: Let X be a set. There is a bijection between the set of all equivalence relations on X, and the partition of X, given by the function that sends an equivalence relation to the set of all its equivalence classes.

Proof. (**Proposition 34**) Let $\sim$ be an equivalence relation on X. We let $\mathrm{cl}(X)$ be the set of equivalence classes of $\sim$, then $\bigcup_{C \in \mathrm{cl}(X)} C = X$, and moreover, suppose $[x] \neq [x']$, and assume we have an $y \in [x] \cap [x']$, then by definition $x \sim y$ and $x' \sim y$, so by symmetry and transitivity, $x \sim x'$, so by Lemma 30, $[x] = [x']$, contradiction so $[x] \cap [x'] = \emptyset$, hence the elements of $\mathrm{cl}(X)$ is a partition of X. Conversely, suppose $U_{i \in I}$ is a partition of X. Define $\sim$ by

$$x \sim y \iff \exists i \in I, x \in U_i \land y \in U_i.$$

Let $x \in X$, as $\bigcup_i U_i = X$, there exists some i such that $x \in U_i$, so $x \sim x$. The relation $\sim$ is also seen to be symmetric, and for transitivity, suppose $x \sim y$ and $y \sim z$, then there are some i, j such that $x, y \in U_i$ and $y, z \in U_j$. In particular $y \in U_i \cap U_j$, so $U_i \cap U_j \neq \emptyset$, hence by contrapositive, $i = j$, therefore $x, z \in U_i$ meaning $x \sim z$. $\square$

We give the following without prove (but it is an exercise to prove it, try first to do it for a two element partition).

Proposition 35: Let X be a finite set, and let $U_{i i \in I}$ be a partition of X. Then

$$|X| = \sum_{i \in I} |U_i|.$$

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

Theorem 36: 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 36**) 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 32. If $m([x]) = m([y])$, then $f(x) = f(y)$, so $x \sim y$, hence by Lemma 30, $[x] = [y]$, so m is injective. Then we have $m \circ p(x) = m([x]) = f(x)$. $\qquad \square$

4 Groups

Groups are mathematical structures that arise everywhere. Groups encode symmetries 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 $\{a, b\}$.

Before starting, we give a little bit of terminology that will be used throughout this chapter.

Definition 37: Let $f : X \to X$ be a function. We say that a subset $A \subseteq X$ is *closed* under f if whenever $a \in A$, $f(a) \in A$. Also, if we have $f : X \times X \to X$, and $A \subseteq X$, we say also that A is closed under f if for all $a, b \in A$, we have $f(a, b) \in A$.

4.1 Monoids

Definition 38: 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 39: 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 40: 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 41: 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 42: 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 43: 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 43**) 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 $e' = e$. $\square$

Definition 44: 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 45: 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 46: 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

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

a morphism of monoids?

Definition 47: 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 48: 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 49: 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 49**) 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. $\square$

Definition 50: 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.

Given a set X, how can we make it a monoid X^* such that elements of X are inside X^*? To see that, first suppose $X = \{x\}$, a set with an element. We construct a monoid X^*. As it is a monoid, it must have a neutral element, we call it e. We also want $x \in X^*$, so we put it there. So far our monoid X^* has elements e and x. But now, we can also consider $x \cdot x$, a priori, this element does not belong to X^*, but it should still exists, so we add it, and we call it xx for simplicity. Now our monoid has elements $\{e, x, xx\}$, and again we can consider $x \cdot (x \cdot x)$, or $(x \cdot x) \cdot x$. Those elements will have to be the same, so we add another element xxx to the monoid. And we continue forever. The end result will be that the elements of X^* are strings of x's, the monoid operation is concatenation, and the neutral element is the empty string. This indeed satisfies the axioms of monoid, as concatenating is associative, and concatenating the empty string to the left or the right of a word does not change it. Let us give a more general definition, when X is any set.

Definition 51: Let X be a set. We define X^* to be the monoid whose elements are finite strings $x_1 \ldots x_n$ with $x_i \in X$, whose law is concatenation, and whose neutral element is concatenation. This indeed defines a monoid, as concatenation is associative, and concatenating with the empty string does not change a string.

Lemma 52: Let X be any set, and $(M, \cdot, e_M)$ be a monoid. Then any set-theoretical function $f : X \to M$ gives rise to a morphism of monoid $f^* : X^* \to M$ by letting

$$f^*(x_1 x_2 \ldots x_n) = f(x_1) \cdot f(x_2) \ldots f(x_n),$$

where we allow $n = 0$, and we mean $f^*(e) = e_M$.

Proof. (**Lemma 52**) By definition, the map indeed maps the neutral element to the neutral element. If $x_1 \ldots x_n, y_1 \ldots y_m \in X^*$, then

$$f^*(x_1 \ldots x_n y_1 \ldots y_m) = f(x_1) \ldots f(x_n) f(y_1) \ldots f(x_m) = f^*(x_1 \ldots x_n) f^*(y_1 \ldots y_m).$$

$\square$

4.2 Groups

Monoids are interesting objects, but if we ask moreover that every element has an inverse, a whole new world appears, it is the one of groups.

4.2.1 General theory of groups

Definition 53: A *group* $(G, \cdot, e)$ is a monoid together with a function $-^{-1} : G \to G$ that sends $x \in G$ to x^{-1}, called the *inverse* of x, and such that

$$\forall x \in G, x \cdot x^{-1} = e = x^{-1} \cdot x.$$

A group is *abelian* if its underlying monoid is abelian, see Definition 44.

Remark 54: The Remark 45 also applies for groups, for instance we will often write $+$ for the law of an abelian group. Furthermore, we extend this notation to $-x$ to mean x^{-1} in the case where the group is abelian.

Example 55:

- $(\mathbb{Z}, +, 0, -)$ is an abelian group.

- $(\mathbb{R}^*, \times, 1, x \mapsto 1/x)$ is an abelian group.

- Let X be a set, call $\mathrm{Bij}(X)$ the set of all bijective function $f : X \to X$. This set is a (non-abelian) group with composition. What is the inverse of a function? What is the neutral element?

- We let $\mathbb{Z}_2$ to be the set $\{0, 1\}$, with the binary law being addition modulo 2, so for instance $0 + 1 = 1$, and $1 + 1 = 0$. This is a group in which each element is its own inverse.

- More generally, we let $\mathbb{Z}_n$ to be the set $\{0, \ldots, n-1\}$ with law being addition mod n, so to compute $p + q$, we first do it as in $\mathbb{Z}$, and then let $p + q$ be the reminder of this modulo n.

- Let $\mathbb{U}_n$ be the set of nth roots of unity, that is

$$\mathbb{U}_n = \{\exp(\frac{2\pi k}{n}) \mid k \in \{0, \ldots, n-1\}\},$$

  with law being multiplication. This is a group, which is in fact the same as $\mathbb{Z}_n$, more on this when we will do modular arithmetic.

- Dihedral groups are example of finite groups that are not abelian. The nth dihedral groups represent the rotational and mirrors symmetries of the regular $n$gone, so for instance the third dihedral groups is the symmetries of the equilateral triangle. It has 6 elements,

$$D_3 := \{r_0, r_1, r_2, s_0, s_1, s_2\},$$

  where r_i means *rotate the triangle by $i \times 120°$*, (so r_0 is the neutral element) and s_i means *reflect the triangle along the ith median*. The law of groups is *doing the symmetry one after another, from the rightmost to the leftmost*, so for instance $s_2 s_1 = r_1$, as if we take a triangle, reflect it along the first median, then the second median, it amounts to rotating it by $120°$. *TODO : add pictures, it would be better*. Check that this the group law is indeed not commutative.

- If you are interested in non-abelian finite groups, check out the classification of finite simple group. It consist of finding all finite group, that enjoy the property of being *simple* (it does not mean at all that the group is simple, but rather that its subgroups behave in some manageable way). It took humanity fifty years and tens of thousands of pages to prove that we found them all.

Remark 56: What we said previously about monoid, can also be extended to groups. In particular, neutral element is unique.

Lemma 57: Let G be a group, and let $x \in G$. Suppose we have $x' \in G$ such that $x' \cdot x = e$ or $x \cdot x' = e$, then $x' = x^{-1}$.

Proof. (**Lemma 57**) Suppose for instance $x' \cdot x = e$, then multiplying by x^{-1} both sides yields

$$x' \cdot x \cdot x^{-1} = e \cdot x^{-1},$$

which simplifies to $x' = x^{-1}$. □

Exercise 22: Let $(G, \cdot, e)$ bea group, and let $x, y \in G$, prove that we always have the following identities (and remember that they exists):

- $e^{-1} = e$,

- $(xy)^{-1} = y^{-1} x^{-1}$.

- $\left(x^{-1}\right)^{-1} = x$.

Definition 58: Let G be a group. A subgroup of G is a subset $H \subseteq G$ that is contains the neutral element, is closed under the group operation, and under taking inverses.

In fact, the definition of subgroups contains redundant element, to check that a subset is a subgroup, there is less work that we need to do.

Lemma 59: Let G be a group, and $H \subseteq G$. Then H is a subgroup if and only if it is non-empty, and whenever $x, y \in H$, we have $x \cdot y^{-1} \in H$.

Proof. (**Lemma 59**) Suppose H is a subgroup of $(G, \cdot, e)$, then it contains the neutral element, so is not empty. If $x, y \in H$, then by closure under taking the inverse $y^{-1} \in H$, and as H is closed under the group law, we get $x \cdot y^{-1} \in H$. Conversely, as H is non-empty, we can chose a $x \in H$, and by hypothesis, $x \cdot x^{-1} \in H$, that is $e \in H$. Now take any $x \in H$, we have $e \cdot x^{-1} \in H$, so $x^{-1} = e \cdot x^{-1} \in H$, so H is closed under taking inverses. Finally, let $x, y \in H$, we have by what we

just shown that $y^{-1} \in H$, now applying the hypothesis with x and y^{-1}, we get $x \cdot (y^{-1})^{-1} \in H$, that is, $x \cdot y \in H$. $\qquad\square$

Example 60: Subgroups are everywhere.

- Let $n \in \mathbb{Z}$, call $n\mathbb{Z}$ the set
$$n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\},$$
for instance $2\mathbb{Z}$ is the set of even integers. Then $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

- If n divides p, then $p\mathbb{Z}$ is a subgroup of $n\mathbb{Z}$ (thus generalizing the previous example, as $\mathbb{Z} = 1\mathbb{Z}$)

- The dihedral groups D_3 of Example 55 has $\mathbb{Z}_3$ as a subgroup, for instance $\{r_0, r_1, r_2\} \subseteq D_3$ is a subgroup that is isomorphic to $\mathbb{Z}_3$.

Exercise 23: Let G be a group, and let $(G_i)_{i \in I}$ be a family of subgroup of G, check that the intersection $\bigcap_{i \in I}$ is again a subgroup of G.

We now dive into the world of morphism of groups. We used the word *isomorphic* above, it means that two groups are the same, in a very precise and powerful way.

Definition 61: Let $f : G \to H$ be a function between two groups, we say that f is a *morphism of groups* if $f(e_G) = e_H$, for all $x, y \in G$, $f(xy) = f(x)f(y)$, and for all $x \in G$, $f(x^{-1}) = f(x)^{-1}$. That is, f is a function that respect the structure of a group, namely the neutral element, the multiplication, and taking the inverse.

Example 62:

- Let G be a group, let 0 be the group with one element. There is a unique morphism $0 \to G$, and a unique morphism $G \to 0$.

- Let G be a group and $H \subseteq G$ be a subgroup, then the function $\iota : H \to G$ that sends $x \in H$ to itself is a morphism of group.

- Let $f : \mathbb{Z} \to \mathbb{Z}_2$ be the function sending even elements to 0 and odd elements to 1. It is a morphism of group.

Remark 63: As morphism of group are in particular functions, it makes sense to say that a morphism of group is injective, surjective, or bijective. In the last case, we say that f is an *isomorphism*. So an isomorphism between two groups is a morphism of group that is bijective, i.e. that is both injective and surjective.

Like in the case for monoid, we define the kernel and the image. Notice that the definition is the same as Definition 48.

Definition 64: Let $f : G \to H$ be a morphism of group. The *kernel* of f is the set
$$\ker(f) := f^{-1}(\{e_H\}) = \{x \in X \mid f(x) = e_H\} \subseteq G$$
and the *image* of f to be the set
$$\operatorname{im}(f) := \{f(x) \mid x \in G\} \subseteq H.$$
(which is the same thing as the set-theoretical image of Definition 16).

Lemma 65: Let $f : G \to H$ be a morphism of groups. Then $\ker(f)$ is a subgroup of G, and $\operatorname{im}(f)$ is a subgroup of H.

Proof. (**Lemma 65**) We already know that $\ker(f)$ and $\operatorname{im}(f)$ are submonoids, according to Lemma 49. To check that it is a subgroup, it remains to see that they are closed under taking inverses. For that, let $x \in \ker(f)$, then $f(x^{-1}) = f(x)^{-1}$, because f is a morphism of groups, and by hypothesis, $f(x) = e_H$, therefore, $f(x^{-1}) = e_H^{-1} = e_H$. This proves $\ker(f)$ is a subgroup of G. Finally, take $y \in \operatorname{im}(f)$, that is $y = f(x)$ for some $x \in G$. We have $y^{-1} = f(x)^{-1} = f(x^{-1})$, meaning that $y^{-1} \in \operatorname{im}(f)$, so $\operatorname{im}(f)$ is a subgroup of H. $\qquad\square$

Images and kernels are very convenient object. Knowing them tells us when a morphism is injective, surjective, or an isomorphism.

Proposition 66: Let $f : G \to H$ be a morphism of groups. Then

- f is injective if and only if $\ker(f) = \{e_G\}$;

- f is surjective if and only if $\operatorname{im}(f) = H$;

- f is an isomorphism if and only if $\ker(f) = \{e_G\}$ and $\operatorname{im}(f) = H$.

Proof. (**Proposition 66**) Suppose f is injective, and let $x \in \ker(f)$, then $f(x) = e_H = f(e_G)$, so by injectivity, $x = e_G$. Conversely, suppose $\ker(f) = \{e_G\}$, and take $x, y \in G$ such that $f(x) = f(y)$. Multiplying by $f(y)^{-1}$ both sides, we get

$$e_H = f(y)f(y)^{-1} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}),$$

so $xy^{-1} \in \ker(f)$, and $\ker(f) = \{e_G\}$ by hypothesis, this means $xy^{-1} = e_G$, so multiplying by y, we find $xy^{-1}y = y$, i.e. $x = y$, and f is injective. Next, f surjective is by definition to say that $\operatorname{im}(f) = Y$, and finally, an isomorphism is a bijective group morphism, that is an injective and surjective group morphism. □

Example 67: Recall the examples of Example 62.

- Let G be a group. The map $0 \to G$ is injective, and the map $G \to 0$ is injective. If G is not the zero group, then the composition $G \to 0 \to G$ is neither injective, nor surjective.

- If $H \subseteq G$ is a subgroup, then the map $\iota : H \to G$ is injective.

- The map $f : \mathbb{Z} \to \mathbb{Z}_2$ of Example 62 is surjective.

Definition 68: Let G be a group, let $H \subseteq G$ be a subgroup, and $x \in G$. We define the *left coset* of H with x, to be the set

$$xH := \{x \cdot h \mid h \in H\}.$$

Similarly, the *right coset* of H with x is

$$Hx := \{h \cdot x \mid h \in H\}.$$

Definition 69: Let $x \in G$ be an element of a group. Let $n \in \mathbb{Z}$, we define by induction x^n. If $n = 0$, we let $x^0 = e$. Suppose x^n have been defined, we define x^{n+1} to be $x^n \cdot x$. Suppose $n < 0$, then we define $x^n = (x^{-n})^{-1}$.

Exercise 24: Check that this definition satisfies the usual laws of powers, that is

- $x^n x^m = x^{n+m}$

- $x^{-n} = (x^n)^{-1}$

Argue that defining x^n for some x is in fact the same thing as defining a morphism of group $\mathbb{Z} \to G$ that sends 1 to x.

Remark 70: If G is abelian, then according to Remark 54, we will often write $+$ for the group law, and in that case, we will write nx for x^n, with Exercise 24 giving for instance $nx + mx = (n+m)x$, as expected.

Definition 71: Let G be a group, and let $S \subseteq G$ be a subset. We let $\langle S \rangle$ be the smallest subgroup of G containing S.

Proposition 72: Let $\mathcal{S} := \{H \subseteq G \mid H \text{ subgroup and } S \subseteq H\}$, then

$$\langle S \rangle = \bigcap_{H \in \mathcal{S}} H.$$

Proof. (**Proposition 72**) We have $\langle S \rangle \subseteq \bigcap_{H \in \mathcal{S}} H$, as $\bigcap_{H \in \mathcal{S}} H$ is a subgroup of G (see Exercise 23) containing S, and $\langle S \rangle$ is the smallest of them all. Conversely, $\langle S \rangle \in \mathcal{S}$, so $\bigcap_{H \in \mathcal{S}} H \subseteq \langle S \rangle$. □

Definition 73: Let $x \in G$, we denote by $\langle x \rangle$ the subgroup $\langle \{x\} \rangle$, and we call it the *subgroup generated by x*.

4.2.2 Finite group theory

Armed with those definition, we are ready to specialize ourself to the one of finite groups.

Definition 74: A *finite group* is a group that is finite set. We call its cardinality the *order* of the group.

Exercise 25: For all $n \in \mathbb{N}$, the groups $\mathbb{Z}_n$ are finite groups of order n. The group with one element is the unique finite group of order 1. There are no group of order 0, as such a group would be empty, thus would not have a neutral element.

Definition 75: Let G be a group, we call the order of an element $x \in G$, if it exists, the smallest positive natural number such that $x^n = e$.

Lemma 76: In a finite group, the order of an element always exists.

Proof. (**Lemma 76**) Let G be a finite group, and $x \in G$. To take the minimal element of a set of natural numbers, we only need to make sure that it is non-empty. That is we want to find some $p \in \mathbb{N}^*$ (the set of natural number greater than 0), such that $x^p = e$. For that, consider the set

$$X := \{x^n \mid n \in \mathbb{N}^*\}.$$

It is included in G, so it has to be finite, therefore there exists some $n \neq m$ such that $x^n = x^m$ (otherwise the map $n \mapsto x^n$ would be an injection from $\mathbb{N}$ to X, meaning by Example 25 that X is infinite). Without loss of generality, suppose nm. Then, multiplying by $(x^n)^{-1}$ both sides, we get $e = x^m(x^n)^{-1} = x^{m-n}$ with $0 < m - n$. $\square$

Remark 77: Therefore, as the order of an element is always defined, we define the function

$$\mathrm{ord} : G \to \mathbb{N}$$
$$x \mapsto \mathrm{ord}(x)$$

that sends an element to its order, and we extend this notation to groups themselves by letting $\mathrm{ord}(G)$ be the order of the group G.

The order of an element of a group is related to the order of the group itself, we have that $\mathrm{ord}(x) \mid \mathrm{ord}(G)$ ($\mid$ means divides). In order to prove that, we will prove a more general theorem, that is the order of any subgroup of G divides the order of G. This is known as Lagrange's theorem.

Definition 78: Let $H \subseteq G$ be a finite group and a subgroup. We define $[G : H]$, the *index* of H in G to be the cardinality of the (finite) set

$$\{xH \mid x \in G\}.$$

That is, the index of a subgroup is its number of distinct left cosets.

Theorem 79: Let G be a finite group and and $H \subseteq G$ be a subgroup. We have

$$\mathrm{ord}(G) = [G : H]\,\mathrm{ord}(H).$$

In particular the order of H divides the order of G.

Proof. (**Theorem 79**) We define the binary relation $\sim$ on G by letting

$$x \sim y \iff y^{-1}x \in H.$$

We prove that it is an equivalence relation. It is reflexive, as $e = xx^{-1} \in H$. If $x \sim y$, then $xy^{-1} \in H$, so (H is a subgroup), $(y^{-1}x)^{-1} \in H$, that is, $yx^{-1} \in H$, meaning that $y \sim x$, hence the relation is symmetric. Finally, if $x \sim y$ and $y \sim z$, then $y^{-1}x \in H$ and $z^{-1}y \in H$, so $z^{-1}yy^{-1}x \in H$, that is $z^{-1}x \in H$, i.e. $x \sim z$. This proves $\sim$ is an equivalence relation. We denote by $[x]$ the

equivalence class of x under $\sim$. We prove that in fact $[x] = xH$. For that, let $y \in [x]$, then $x \sim y$, so $y \sim x$ that is $x^{-1}y \in H$, which is to say that there exists some $h \in H$ such that $x^{-1}y = h$, that we can rewrite to $y = xh$, so $y \in xH$. Conversely, if $y \in xH$, then $y = xh$ for some $h \in H$, so $x^{-1}y \in H$, i.e $y \in [x]$. The equivalence classes of $\sim$ are thus precisely the left cosets of H.

We now prove that all equivalence classes have the same cardinality, equal to the order of H. For that, we let $x \in G$, and by Example 25, it suffices to establish a bijection $H \to xH$. We construct such function f by sending $h \in H$ to $f(h) = xh$. We see that it is a bijection by considering $g : xH \to H$ sending any element $y \in xH$ to $x^{-1}y$. Then we compute $g \circ f(h) = x^{-1}xh = h$, so $g \circ f = \mathrm{id}_H$, and $f \circ g(y) = xx^{-1}y = y$, so $f \circ g = \mathrm{id}_{xH}$. We thus established $|[x]| = |xH| = \mathrm{ord}(H)$.

Now we let $\{x_1H, \ldots, x_kH\}$ the all the left cosets of H, by definition there are $[G : H]$ many of them, that is $k = [G : H]$. Recall that we proved that these cosets are exactly the equivalence classes of $\sim$, so we apply by the formula of Proposition 35:

$$\mathrm{ord}(G) = \sum_{i=1}^{k} |[x_i]| = \sum_{i=1}^{k} |H| = \left(\sum_{i=1}^{k} 1\right)|H| = k|H| = [G : H]\,\mathrm{ord}(H).$$

$\square$

Corollary 80: Let G be a finite group, and let $x \in G$, then $\mathrm{ord}(x) \mid \mathrm{ord}(G)$.

Proof. (**Corollary 80**) Let $\langle x \rangle$ be $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad$ $\square$