A first course on linear algebra

Ricardo Souza

September 5, 2019

Contents

1 Basic set theory **2**
1.1 Naive set theory 2
1.1.1 Axioms and you 2
1.1.2 Russell's Paradox 4
1.2 Basic results and properties of sets 5
1.2.1 Equality always 5
1.2.2 United we stand, intersected we... Fall? 11
1.3 Time to do some actual set theory, none of this introductory bullshit 18
1.3.1 How does this function 18
1.3.2 Bijection is the new equality 24
1.3.3 The A and Ω of sets 31
1.3.4 Multiplying sets 34
1.3.5 Adding sets? 42
1.3.6 Everything is a set! 48
1.3.7 Relations are hard, sometimes they leave you broken up inside 55
1.3.8 Second order thinking 65

2 Real Linear Algebra **73**
2.1 Introduction 73
2.1.1 First notions and definitions 73
2.1.2 Real vector fields 80

Chapter 1

Basic set theory

1.1 Naive set theory

1.1.1 Axioms and you

Most, if not all, concepts in mathematics are phrased in the language of set theory: Geometric figures are just collections of points, transformations between two different objects are the collections of all the transitional states inbetween etc.

Hence, it makes sense to give some more formal foothold when studying any area of maths by beginning with some basic set theory.

But then, why *naive*?

Well, formal mathematics (that is, all contemporary and modern mathematics for more than a hundred years) is based on what we like to call *axioms* - you can think of them as the "rules of the game", in some sense.

Let me give you all an example of a well-accepted axiom of Euclidean geometry:

axiom

Given any two distinct points, there is one, and only one, line through them.

Some people say it's "something that you can't prove", but it's not exactly that - axioms are either things that you don't *want* to prove, and just want to assume as truth (maybe because it is, indeed, impossible to prove it) or things that are, in some vague sense, "natural" or "self-evident".

Either way, the correct mindset to approach axioms is to think of them as the building blocks with which you build maths - just like atoms are the building blocks of matter -: by combining different axioms in different ways you get different results - the so called "theorems".

That's what maths is all about: Working with axioms and already proven theorems to prove new theorems. It's kinda like a game of scrabble, where the axioms are not only the blocks you (and everyone else) has in their hands, but also the rules of the game and the game board, and the theorems are the words you can make - subject to the rules of the game, the pieces and the board.

Hence, *naive* set theory is called so not because it is a theory of naive sets, but because it's a theory that's not properly formalized, and relies heavily on intuition and common sense.

In proper, axiomatic, set theory you'd have to define what is, and what isn't, a set. In naive set theory, however, we can just hand-wave it and say

naive axiom(?)

Any collection of things is a set.

Now, as to *why* this isn't formal, it's due to the fact that it leads to a logical contradiction - a paradox. We're gonna show this contradiction in what follows, but if it doesn't interest you (you filthy, you) you can just skip the next section. It's fine, I won't judge you (actually, I will).

1.1.2 Russell's Paradox

Imagine that every random collection of random things is a set. Then it is only natural to consider the collection of all sets. But, since it is a collection (duh) it is also a set. But since it is the collection of all sets, it is an element of itself.

That's weird, ok? Try thinking of any sets - I'll give you plenty of time, don't worry - that are like that: they contain themselves as elements. You can't, right?

While that's not a contradiction, per se, it *really is weird*.

So let us consider N the collection of all non-weird sets - that is, the collection of all sets that do not contain themselves as elements.

Now, one naturally asks the question: Is N itself a weird set? That is, $N \in N$?

Well, I don't know. But if it was, then, by definition, all elements of N are non-weird sets, so N, being an element of N, would have to be a non-weird set - that is, $N \notin N$. So... If we assume that $N \in N$ we can logically infer that $N \notin N$...

Okay, maybe we made a mistake all along by assuming that $N \in N$! Yeah, that must be the case! Clearly, N can't be a weird set!... But then, since N isn't weird, it must be an element of N (since N contains *all* non-weird sets)... That is, $N \in N$. So if we assume $N \notin N$ we can logically deduce that $N \in N$.

We have just proven that $N \in N$ and $N \notin N$ are *logically equivalent*. But by the **Principle of Non-Contradiction** (something can't be simultaneously both true and false) those two can't be equivalent!

So, by assuming that there is a set containing all sets we can logically derive a contradiction - that, my friends, is the definition of a paradox.

This is the famous **Russell's Paradox** and it applies in broader contexts - it basically means that, from a logical POV, self-references are *kinda weird and you shouldn't actually do that*.

For instance, if you put as an axiom that "anything that can be stated can be proven", then you could ask "can I prove that there is something that cannot be proven?" and the answer would have to be *yes*, since you said (by axiom) that everything had to be provable. But that's a contradiction - by forcing everything to have a proof you have proven that you cannot prove everything.

This was proposed by philosopher-mathematician Bertrand Russell to show that maths really does need a formal framework to work with - otherwise we might be working in a system where contradictions arise (as we have seen).

There is, however, a solution to this. We have a set of axioms for set theory called the Zermello-Frankel axioms, which are a list of axioms that do not generate that kind of contradiction. It is, however, *impossible* to prove whether it does or doesn't generate *any* paradox (this is due to a bunch of hard maths/philosophy that is waaaaay out of the scope of this text).

Just know that if you ever see ZFC anywhere you can rest safe because you're working with a (relatively) safe set of axioms.

1.2 Basic results and properties of sets

1.2.1 Equality always

As we have previously stated, a *set* is a collection of objects. We will usually denote a set by a capital letter (not always), such as X, A or B.

Since we cannot (as seen in the previous section) consider "the set of all sets", fix any set X. Now, X might be any set - numbers, birds, colours, the numerous of ways you can insult someone's mum etc.

When we have an object that is in that set we say that it is an **element** of that set, and usually denote it by a non-capital letter (once again, not always). In symbols, if we want to say that a is an element of X we would write that as $a \in X$ - which should be read as "a is an element of X", "a is in X" or even "X contains a as an element".

Example(s)

Let E be the collection of all even integers. So $2 \in E$ and $28 \in E$, but $5 \notin E$ ("5 isn't in E", or "5 isn't an even integer") and *dog* $\notin E$ (because *dog* is **not** an even integer). Actually, you can see this as a formal proof of the well known fact that all dogs are *odd*.

You can, however, take all the elements of a set and ask if they satisfy a certain condition.

Example(s)

Following up on the previous example, let ϕ denote the proposition "*can be written in english with only three letters*". Now we can consider the *subset* of E formed by all elements of E that also satisfy ϕ (if $x \in E$ is such an element, we simply write $\phi(x)$ to denote "x satifies ϕ"). This is written as follows:

$$E_\phi := \{x \in E \mid \phi(x)\}.$$

Let us break this down bit-by-bit:

- The symbol E_ϕ is non-standard notation that we're introducing here to mean "*the set E subject to the condition ϕ*";

- The symbol := means "*equals, by definition*". This can be used in two distinct ways: During a logical regression, we can use this symbol to justify one step by saying "this thing that I'm claiming is true, is actually true by definition"; or we can use it to define new terms - we're basically saying "the LHS is a new symbol whose meaning I'm defining to be the RHS" - kinda like attributing a value to a variable.

  In this text we're **always** going to use this symbol with the second meaning - so in the preceding expression the := means "I'm defining E_ϕ to mean $\{x \in E \mid \phi(x)\}$".

- The brackets, in mathematics, almost always denote a *set*, and always are presented with the following structure: $\{A \mid B\}$.

The A part is *what kind of elements does this set have*. In the example above, $x \in E$ means that the elements we're working with are even integers.

The B part is *which condition these elements are subject to*. In the example above, $\phi(x)$ means that the elements of this set must satisfy ϕ.

Now that that's out of the way, what is E_ϕ? What are *the even integers that can be written in english using only three letters*? There are only three such numbers: **two**, **six** and **ten**. So we write $E_\phi = \{2, 6, 10\}$.

Definition 1.2.1.1. *Two sets A and B are said to be **equal** if they have the same elements. This means that every element of A is an element of B, and every element of B is an element of A.*

In this case we write $A = B$.

Let us give some examples of equalities.

Example(s)

- Let A be the set of all animals that are wooly, fluffy and go *baa*, and let B be the set of all sheep. Clearly $A = B$.
- Let A be the set of roots of the polynomial $x^2 - x$ and let $B = \{0, 1\}$. It is an easy exercise to see that these two sets are the same.
- However, $A = \mathbb{N}$ the set of all natural numbers, and $B = \mathbb{Z}^{\geq 0}$ the set of non-negative integers, are **not** equal sets. You can see this in any proper course of number/set theory, but the elements of $\mathbb{Z}$ are always signed: -2, $+6$, $+1$ etc. (aside from 0), whereas the elements of $\mathbb{N}$ are **not** signed: 1, 6 etc. So $1 \notin \mathbb{Z}$ and $+1 \notin \mathbb{N}$, and therefore $A \neq B$.

Remark 1.2.1.2

In mathematics, a *definition* is the term we use to "assign" a new value to a certain term. In the definition above, we assigned a meaning to the phrase "two sets are equal".
Please be aware that this text will be filled with definitions of this kind, so take your time to get accostumed to them.

Notice, however, that we can sort of "relax" the conditions of the preceding definition. For instance, consider the following case:

Example(s)

Let $A = \mathbb{N}$ the set of all natural numbers and $B = E$ the set of all even natural numbers. Notice that $A \neq B$ - for instance, 3 is in A, but not in B - so they can't be equal.
On the other hand, notice that it is impossible to produce such a counterexample starting from B: No matter which element you choose in B it will always be a natural number, of course, and therefore it will also be an element of A.

So these two sets, although not-equal, are not *entirely* different.

Definition 1.2.1.3. *Let A and B be two sets such that every element of B is also an element of A. In this case, we say that A **contains** B **as a subset** - or more simply that B **is a subset of** A, which we'll denote in symbols by $B \subseteq A$.*

Example(s)

- In the preceding example, we see that $B \subseteq A$.
- Take any set A, and let $B = A$. We then ask the question: Is B a subset of A? Well, by definition, $B \subseteq A$ if, and only if, every element of B is also an element of A... But this is trivially true - since $B = A$!

  This gives us some insight on our first result:

Proposition 1.2.1.4. *For any set A we have that $A \subseteq A$.*

Proof

We want to show that every element $a \in A$ is also an element of A. But that's trivial. The result follows. □

Remark 1.2.1.5

In mathematics, a *proof* of a proposition/lemma/theorem/corolary is nothing more than a logical reasoning explaining why what we said is true. Proofs are to mathematics as scientific experiments are to sciences. This is what mathematicians do and work with all their lives. One could argue that maths is the science of reasoning and arguing.

Now we have our first non-trivial result:

Proposition 1.2.1.6. *Let A and B be two sets. Then $A = B$ if, and only if, $A \subseteq B$ and $B \subseteq A$.*

Proof

Assume that $A = B$. We want to show that $A \subseteq B$ and $B \subseteq A$, but this is trivial in light of the preceding proposition.

Assume now that $A \subseteq B$ and $B \subseteq A$. We want to show that $A = B$ - that is, every element of A is an element of B, and every element of B is an element of A.
Notice, however, that the phrase "every element of A is an element of B" is the definition of the symbol $A \subseteq B$, and the phrase "every element of B is an element of A" is the definition of the symbol $B \subseteq A$ - both of which we are assuming to be true.
Therefore, we have just proven that $A = B$, as stated, which finishes the proof. □

Remark 1.2.1.7

In mathematics, an *if, and only if,* statement is the equivalent of a logical equivalence. Basically, whenever we say "*this* holds if, and only if, *that* holds" what that means is that *this* and *that* are equivalent: *this* is true precisely when *that* is true, and *this* is false precisely when *that* is also false.
Without going too much into propositional logic, we usually write "a if, and only if, b" in symbols as $a \iff b$, which is logically equivalent to saying that "a being true is sufficient for us to prove that b is also true" and "b being true is sufficient for us to prove that a is also true". In symbols we would write these, respectively, as $a \implies b$ and $b \implies a$ - which should be read as "a implies b" and "b implies a", respectively.
That's what we did in the preceding proposition: If a="$A = B$" and b="$A \subseteq B$ and $B \subseteq A$", we proved that assuming a we can conclude b, and that assuming b we can conclude a - that is, we proved that a implies b and b implies a - which is logically equivalent to proving that a and b are equivalent.

This proposition is the most common tool used by mathematicians to prove that two sets are equal: We simply prove that each one contains the other - therefore, they must be equal.

Example(s)

Let A be the set of roots of the polynomial $x^2 - x$ - that is, the set of numbers r such that $r^2 - r = 0$ - and $B = \{0, 1\}$. We claim that $A = B$.
First, let us show that $B \subseteq A$ - that is, both 0 and 1 are roots of $x^2 - x$. This is done by a simple verification:

$$0^2 - 0 = 0 - 0 = 0 \qquad \text{and} \qquad 1^2 - 1 = 1 - 1 = 0$$

so they are, indeed, roots of $x^2 - x$ - and therefore, $B \subseteq A$.
Now, to prove that $A \subseteq B$ we need to show that those are the only two possible roots.
To do that, let r be any root of $x^2 - x$ - that is, $r^2 - r = 0$. But then, $r^2 = r$, by adding r on both sides, and we see that $r = 0$ is indeed a solution to this equation ($0^2 = 0$). So if we assume that $r \neq 0$ we can divide both sides by r and get $\frac{r^2}{r} = \frac{r}{r}$ which is the same as $r = 1$, which was a unique solution being $r = 1$.
Hence we have proven that any root r of $x^2 - x$ is either 0 or 1, and therefore $A \subseteq B$.
Finally, since $A \subseteq B$ and $B \subseteq A$ we can finally say that $A = B$, as we had previously stated.

Definition 1.2.1.8. *We say that A is a **proper subset** of B if A is a subset of B, but B isn't a subset of A. In this case we use the symbol $A \subset B$.*

Example(s)

Consider $A = \mathbb{N}$ the set of natural numbers, and $B = E$ the set of even natural numbers. We clearly have $B \subseteq A$ and $A \nsubseteq B$, so we can see that B is a *proper* subset of A - that is,

$B \subset A$.

Finally, we can use all that we've done so far to construct a very special set - the empty set.

Example(s)

Let $\mathbb{N}$ be the set of natural numbers and let ϕ be the proposition "is not a natural number". For instance, $\phi(\text{car})$ is just "car is not a natural number", which is true.
Now we can do just as we did before and consider

$$\mathbb{N}_\phi := \{n \in \mathbb{N} \mid \phi(n)\}$$

that is, the set of all natural numbers which are not natural numbers.
What **is** this set? Is there any natural number that isn't a natural number? Of course not!
So this is a set *which has no elements*.
Take now $\mathbb{Z}$ the set of all integers and let ψ be the proposition "is not an integer". We can then define, once more,

$$\mathbb{Z}_\psi := \{n \in \mathbb{Z} \mid \psi(n)\}$$

that is, the set of all integers which aren't integers.
This set is, once again, empty.
This begets the question: $\mathbb{N}_\phi = \mathbb{Z}_\psi$ - that is, are two empty sets always equal?

Definition 1.2.1.9. *Given any set X we call the* ***empty set defined by*** *X to be the set of all elements of X which aren't elements of X, denoted by $\varnothing_X$.*

Theorem 1.2.1.10. *Given any two sets A and B, then $\varnothing_A = \varnothing_B$.*

Proof

If they were different, then there would either be some element of $\varnothing_A$ which is not in $\varnothing_B$, or some element of $\varnothing_B$ which is not in $\varnothing_A$. But both of these are impossible, since both sets are empty.
So they can't be different, and, therefore, $\varnothing_A = \varnothing_B$ $\square$

Corollary 1.2.1.11. *For any set A, its empty set $\varnothing_A$ is uniquely determined.*

Corollary 1.2.1.12. *There a unique empty set.*

Remark 1.2.1.13

In mathematics, a *corolary* is a result that follows immediately from something that came before it - sometimes even foregoing a proof because of how immediate this conclusion is.

Definition 1.2.1.14. *We're going to define the* ***unique empty set*** *to be the empty set of any set, which will be denoted in symbols by $\varnothing$.*

Proposition 1.2.1.15. *For any set A we have that $\varnothing \subseteq A$. Furthermore, we have that $A \subseteq \varnothing$ if, and only if, $A = \varnothing$.*

Proof

If $\varnothing \not\subseteq A$, then there'd be some element in $\varnothing$ that was not in A. But $\varnothing$ is empty, therefore $\varnothing \not\subseteq A$ is false, and hence $\varnothing \subseteq A$.

For the second statement, we clearly have $A \subseteq \varnothing$ if $A = \varnothing$, by definition of set equality. But if we assume that $A \subseteq \varnothing$, we can now use the first statement of this proof, which proves that $\varnothing \subseteq A$, to conclude, by definition of set equality, that $A = \varnothing$, and this finishes the proof. $\square$

1.2.2 United we stand, intersected we... Fall?

Now that we have a basic understanding of sets and subsets, we're going to build new sets from existing ones.

Definition 1.2.2.1. *Let A and B be two sets. The* ***union*** *of A and B is another set - denoted by $A \cup B$ defined by the following properties:*

(a) $A \cup B$ contains both A and B as subsets;

(b) Any other set C that contains both A and B as subsets also contains $A \cup B$ as a subset.

First things first, let us show that this definition makes sense - that is, that given two sets, their union is a unique set:

Lemma 1.2.2.2. *Let A and B be two sets, and C and D be two sets satisfying the above definition. Then $C = D$.*

Proof

Since C and D are unions of A and B, they contain both of them as subsets (item (a)). Now, since C satisfies (a) and D satisfies (b), we get that $D \subseteq C$. Similarly, since D satisfies (a) and C satisfies (b), we get that $C \subseteq D$.
It follows that $C = D$, and so the union of two sets is indeed well-defined, $\square$

With that out of the way, let us show some examples to build some intuition:

Example(s)

Let A be the set of all dogs and B be the set of all cats. Let C be the set of all animals. We ask: $C = A \cup B$?
Certainly, C satisfies (a) (since all dogs and all cats are animals), but does it satisfy (b)?
Well, certainly not! Because the set D of all mammals also contains A and B, but it clearly doesn't contain C (because not every animal is a mammal - for instance, there are birds).
Now we ask: Ok, since C is not the union of A and B, maybe D is?
Well, no, because we can consider E - the set of all mammal quadrupeds - and see that it contains both A and B as susbets, but not D.
And so on, and so forth...

How can we make sure that we don't get an endless regression - that is, we're always inching closer to the result, but never truly getting there?

Well, in formal set theory, for instance ZFC, you can always use your axioms to guarantee the existence of such a set. Here, however, we're going to have to appeal to intuition:

Proposition 1.2.2.3. *Given two sets A and B and any set C containing both A and B, their union is precisely the subset of C given by the proposition $\phi =$ "is in any one of the sets A or B".*

Proof

First, we'll show that $A \subset C_\phi$ and $B \subseteq C_\phi$.
To do that we'll just use the definition: Take $a \in A$ (resp. $b \in B$). Since $A \subseteq C$ (resp. $B \subseteq C$) we have that $a \in C$ (resp. $b \in C$). We then ask: is $\phi(a)$ (resp. $\phi(b)$) true? Well, it trivially is - $\phi(x)$ is true if, and only if x is in A or B - and a (resp. b) certainly is. Therefore, for any $a \in A$ (resp. $b \in B$) we can conclude $\phi(a)$ (resp. $\phi(b)$) - and therefore, $a \in C_\phi$ (resp. $b \in C_\phi$). This shows that $A \subseteq C_\phi$ (resp. $B \subseteq C_\phi$) - and therefore, C_ϕ satifies item (a) of the definition of set union.
Now, take any set D such that D contains both A and B as subsets. If we show that D also contains C_ϕ as a subset, we'll have shown that C_ϕ satisfies the definition of union - and therefore it must be the union.
To do that, take any $x \in C_\phi$. Then, by definition, $\phi(x)$ is true - that is, $x \in A$ or $x \in B$. But since both $A \subseteq D$ and $B \subseteq D$ hold, it doesn't matter if $x \in A$ or $x \in B$ is true - as long as one of them is true, we can conclude that $x \in D$. And since this holds for any $x \in C_\phi$, we have just shown that $C_\phi \subseteq D$.
Since the D we chose was general, the result follows. $\square$

This is important: We now have a way to construct the union of two sets - just take any set containing both of them and restrict it to be only the elements from the original sets.

That, however, requires the existence of some set containing both of them - and that's where ZFC comes in: There's an axiom that states that there always exists a set containing any amount of other sets.

Since we're foregoing axioms here, we're going to provide a "construction" that should be enough for most purposes:

Example(s)

Following up on the previous example, we can now see that $A \cup B$ is any one of "the set of all animals which are cats or dogs", "the set of all mammals which are cats or dogs" or "the set of all mammal quadrupeds which are cats or dogs" - any one of those work, by what we've already proven.
We could, however, give a more explicit construction: $A \cup B$ is just the set of all cats and dogs.

Example(s)

Another, even more constructive example: Let $A = \{a, b, c\}$ and $B = \{c, d, e, f\}$. Then $A \cup B = \{a, b, c, d, e, f\}$ (prove it using the definition if you're not convinced).

Finally, let's end our discussions on the union with the following alternative characterization of it:

Lemma 1.2.2.4. *Let A and B be sets. Then $x \in A \cup B$ if, and only if, $x \in A$ or $x \in B$.*

Proof

One side of this proof is trivial and follows from the definition of set union.
Let us prove then that $x \in A \cup B$ implies $x \in A$ or $x \in B$.
Define $N = \{x \in A \cup B \mid x \notin A \text{ and } x \notin B\}$ the collection of all elements of $A \cup B$ which are in neither A nor B - which is, by definition, a subset of $A \cup B$.
We can now define $U = \{x \in A \cup B \mid x \notin N\}$ the collection of all elements of $A \cup B$ which are not in N - which is, by definition, a subset of $A \cup B$.
We claim that U contains A and B as subsets. This is easy to see: Take y in either A or B (doesn't matter which). Since $A \cup B$ contains both of them, $y \in A \cup B$. But since y came from either A or B, it cannot be in N (by definition of N) - so it must be in U (by definition of U). It follows that both A and B are contained in U.
But this is a conundrum, because $A \cup B$ is *contained* in every set that contains A and B (by definition of set union) - in particular, since U contains A and B this means that U *also contains* $A \cup B$.
This shows that $U = A \cup B$, and therefore $N = \varnothing$.
Finally, to show that $x \in A \cup B$ implies $x \in A$ or $x \in B$, take any $x \in A \cup B$ and notice, by what we've done, that this is the same as saying that $x \in U$. But, then again, this is the same as saying that $x \notin N$ - that is x is in A or B, just as stated. This finishes the proof. $\square$

Going in the opposite direction of unions, there is the concept of intersections. If unions take two sets to build a bigger one, interceptions take two sets to build a smaller one:

Definition 1.2.2.5. *Let A and B be two sets. The **intersection** of A and B is another set - denoted by $A \cap B$ defined by the following properties:*

(a) $A \cap B$ is contained in both A and B as a subset;

(b) Any other set C that is contained both A and B as a subset is also contained $A \cap B$ as a subset.

Remark 1.2.2.6

Notice that the two definitions are basically the same, just changing, in some sense, the "order" of the inclusions $\subseteq$.

Now, let us proceed to prove essentially the same results for intersections as we did for unions:

Lemma 1.2.2.7. *Let A and B be two sets, and C and D be two sets satisfying the above definition. Then $C = D$.*

Proof

Since C and D are intersections of A and B, they are contained in both of them as subsets (item (a)). Now, since C satisfies (a) and D satisfies (b), we get that $C \subseteq D$. Similarly, since D satisfies (a) and C satisfies (b), we get that $D \subseteq C$.
It follows that $C = D$, and so the intersection of two sets is indeed well-defined, $\square$

Contrary to unions, however, we cannot refine intersections. We can, however, still give a construction of the intersection:

Lemma 1.2.2.8. *Let A and B be sets. Then $x \in A \cap B$ if, and only if, $x \in A$ and $x \in B$.*

Proof

One side of this proof is trivial and follows from the definition of set intersection.
Let us prove then that $x \in A$ and $x \in B$ implies $x \in A \cap B$.
Define $N = \{x \in A \text{ and } x \in B \mid x \notin A \cap B\}$ the collection of all elements which are, at once, in both A and B, but not in $A \cap B$ - which is, by definition, a subset of both A and B.
We can now define $I = \{x \in A \text{ and } x \in B \mid x \notin N\}$ the collection of all elements of both A and B which are not in N - which is, by definition, a subset of both A and B. This implies, by definition of set intersection, that $I \subseteq A \cap B$.
We claim now that I contains $A \cap B$ as a subset. This is easy to see: Take any $y \in A \cap B$. Since $A \cap B \subseteq A$ and $A \cap B \subseteq B$, we see that $y \in A$ and $y \in B$. So this y is an element of both A and B which is in $A \cap B$ - which is the definition of an element of I. This shows that $y \in I$.
But this is a conundrum, because $A \cap B$ *contains* every set that is contained in both A and B (by definition of set intersection).
This shows that $I = A \cap B$, and therefore $N = \varnothing$.
Finally, to show that $x \in A$ and $x \in B$ implies $x \in A \cap B$, take any $x \in A$ and $x \in B$ and notice, by what we've done, that this is the same as saying that $x \notin N$ (since it is empty). But, then again, this is the same as saying that $x \in I$ - that is x is in $A \cap B$, just as stated.
This finishes the proof. $\square$

Finally, let's do some examples:

Example(s)

- Let $A = \{1, 2, 3, 4\}$ and $B = \{1, 3, 5, 7, 9\}$. Then, $A \cap B = \{1, 3\}$.
- If A is the set of all even integers, and B is the set of all odd integers, then $A \cap B = \varnothing$.
- If A is the set of all cats and B is the set of all brown animals, then $A \cap B$ is the set of all brown cats.

As a final topic on this section, let us consider another construction.

Definition 1.2.2.9. *Given any set X we denote the* ***set of all subsets of*** *X by $\mathcal{P}(X)$ (or 2^X) and call it the* ***power set*** *of X.*

Remark 1.2.2.10

Note that, at this point, we have not defined products and sums of sets - even less exponents. So, for now, the symbol 2^X is just that - a symbol. It has no meaning resembling the powering

of real numbers.
We will, however, as this text progresses, show two reasons why this notation makes sense, and we'll expand it to be able to take any set to the power of any other set.

Okay, before anything else, let us do some examples:

Example(s)

Let $A = \{1, 2, 3\}$. What is $\mathcal{P}(A)$? Well, by definition it is the set of all subsets of A. Well then - what are the subsets of A?
We can list a few: $\varnothing$, A, $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 2\}$, $\{1, 3\}$ and $\{2, 3\}$. But are there any others?
Well, assume $B \subseteq A$. Then we can ask if B has any elements or not. If it doesn't, great!, because $B = \varnothing$, which we've already accounted for.
If it does, we can ask if it contains 1. And then, we can ask if it contains 2 and 3. And depending on those answers we can pinpoint B exactly, and see that it is, indeed, in the list above (e.g., if it contains 1 and 2, but not 3, then $B = \{1, 2\}$, which is on the list above).
At this point, it is easy to see that

$$\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}.$$

The preceding reasoning, however, gives us our first insight into how to understand the symbol 2^A: Making a subset of A is the same as asking each element of A if it is, or not, in there.
Imagine the elements of A are cards in a deck and you want to make a hand. Making a hand is the same as going through the deck, card by card, and choosing which cards you want to keep, or not.
Since every card has two options (to be, or not to be), the amount of hands is precisely 2 to the number of cards.
Note that in this particular example, $2^A = \mathcal{P}(A)$ has precisely $2^3 = 8$ elements, while A has precisely 3 elements.

Now that we're talking about power sets, we can define one of the most important concepts of set theory:

Definition 1.2.2.11. *Let X be a set and 2^X its power set. Given any $A \in 2^X$, we define its* ***complement*** *to be the set denoted by $X \setminus A$, which is given by*

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

That is, the complement of a set is the collection of all elements that *do not* belong to that set.

Example(s)

Following up on the previous example, let $B = \{1\}$. Then what is $A \setminus B$? Well, by definition, it's the collection of all elements of A that are not in B - that is, 2 and 3, so $A \setminus B = \{2, 3\}$.
Call $C = A \setminus B$. What is, then, $A \setminus C$? Once again, by definition, it's the set of all elements

of A which are not in C - that is, 1, so $A \setminus C = B$.

And finally, just before wrapping up this section, let us give one final definition and example:

Definition 1.2.2.12. *Let A and B be any two sets. We define $A \setminus B$ to be equal to $(A \cup B) \setminus B$ - that is, $A \setminus B$ is the complement of B in $A \cup B$.*

Example(s)

Let $A = \{a, b, c, d, e, f, g, h, i, j\}$ and $B = \{a, e, i, o, u\}$. Then $A \setminus B$ is, by definition, the set of all elements of $A \cup B$ which are not in B. So writing $A \cup B = \{a, b, c, d, e, f, g, h, i, j, o, u\}$ we see that $A \setminus B$ is just $\{b, c, d, f, g, h, j\}$.
Similarly, $B \setminus A$ is the set of all elements of $A \cup B$ which are not in A - that is, $B \setminus A = \{o, u\}$.

To really wrap up this section, then, we're gonna make a list of properties for the things we've just described. You're welcome to try to prove them, although most of them are really trivial (that is, they follow immediately from the definitions or a quick observation).

Proposition 1.2.2.13. *Let A, B, C be any three subsets of a given, fixed, set X. Then the following properties always hold:*

(1) $A \cup B = B \cup A$;

(2) $A \cup (B \cup C) = (A \cup B) \cup C$;

(3) $A \cup \varnothing = A$;

(4) $A \cup X = X$;

(5) $A \cup A = A$;

(6) $A \cap B = B \cap A$;

(7) $A \cap (B \cap C) = (A \cap B) \cap C$;

(8) $A \cap \varnothing = \varnothing$;

(9) $A \cap X = A$;

(10) $A \cap A = A$;

(11) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;

(12) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;

(13) $A \cup B = A$ *if, and only if,* $B \subseteq A$;

(14) $A \cap B = B$ *if, and only if,* $B \subseteq A$;

(15) $A \subseteq B$ *implies* $A \setminus B = \varnothing$;

(16) $A \cap B = \varnothing$ *implies* $A \setminus B = A$ *and* $B \setminus A = B$;

(17) $X = (X \setminus A) \cup A$;

(18) $(A \setminus B) \cup (B \setminus A) \cup (A \cap B) = A \cup B$;

(19) $(A \setminus B) \cap (B \setminus A) = \varnothing$;

(20) $X \setminus A \in 2^X$;

(21) $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$;

(22) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$;

(23) $A \setminus (A \setminus B) = B$;

(24) $A \setminus (A \cap B) = A \setminus B$.

Remark 1.2.2.14

In the preceding proposition, as well as in maths as a whole, we usually save the parenthesis to mean "this should be done first". For instance, $A \cup (B \cup C)$ means "the union of A and the union of B and C", whereas $(A \cup B) \cup C$ means "the union of the union of A and B and C".

1.3 Time to do some actual set theory, none of this introductory bullshit

1.3.1 How does this function

Understanding functions is, basically, the most important thing in all of mathematics - and that's not an overstatement. Even if you forego set theory, the concept of a function still makes sense and it's still at the center of any mathematical discussion.

Since this is a naive introduction to set theory, we're not gonna bother with certain technicalities and simply define:

Definition 1.3.1.1. *Let A and B be two sets. A formula ϕ is said to be of* ***function type*** *(or a* ***function****) from A to B if for any $a \in A$ there's a unique $b \in B$ such that $\phi(a, b)$.*

In that case, we will write that as $\phi(a) = b$ and say that b ***is the image of*** *a* ***under*** *ϕ.*

Example(s)

Let $A = B = \mathbb{N}$ the set of natural numbers, and let $\phi(x, y) =$ "y is the square of x". Then ϕ is clearly a function: for any $a \in A$, there is a unique $b \in B$ such that $\phi(a, b)$, and that b is precisely a^2. So we write this as $\phi(a) = a^2$.
Now, define $\psi(x, y) = \phi(y, x)$. Is ψ also a function? The answer is no: Indeed, for any $a \in A$, there exists, at most, one $b \in B$ such that $\psi(a, b)$. But the thing is - there are some a for which there is no b! For instance, for $a = 3$, there is no b such that $\psi(3, b)$. So ψ can't be a function.

Definition 1.3.1.2. *Let A, B be sets and ϕ be a function from A to B. We will call A the* ***domain*** *of the function and B its* ***codomain****, somtimes written as $A = \mathrm{Dom}(\phi)$ and $B = \mathrm{Cod}(\phi)$.*

In this case, we wil also use the notation $\phi : A \to B$ or $A \xrightarrow{\phi} B$ to say that "ϕ is a function whose domain is A and whose codomain is B".

Definition 1.3.1.3. *Two functions $f, g : A \to B$ between the same two sets are said to be* ***equal*** *if $f(a) = g(a)$ for all $a \in A$. That is, $f(a, g(a))$ and $g(a, f(a))$ hold for all $a \in A$.*

Example(s)

Let $A = B = \mathbb{R}$ the set of real numbers, and let $f, g : A \to B$ be functions defined by $f(x) = \sqrt{x^2}$ and $g(x) = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{otherwise.} \end{cases}$
We claim that $f = g$.
To see that, take any real number, $x \in \mathbb{R}$. Now, if $x \geq 0$, then $g(x) = x$. Furthermore, $f(x) = \sqrt{x^2} = x$, so $f(x) = g(x)$. On the other hand, if $x < 0$, we have $g(x) = -x$ and $f(x) = \sqrt{x^2} = \sqrt{(-x)^2}$ and since $x < 0$, $-x$ must be greater than 0, so $f(x)$ is simply $-x$.
Therefore, $f(x) = g(x)$ for all $x \in \mathbb{R}$ (since any real number is either negative or non-

negative), and we see that $f = g$, as stated.

Definition 1.3.1.4. *If $f : A \to B$ is a function such that $f(a) = b$ for some $a \in A$ and $b \in B$, we then say that f **takes** a **to** b, which will be written as $a \mapsto b$.*

Example(s)

The functions f, g of the previous example can be rewritten as

$$\begin{aligned} f : A &\to B \\ a &\mapsto \sqrt{a^2} \end{aligned}$$

and

$$\begin{aligned} g : A &\to B \\ a &\mapsto \begin{cases} a, & \text{if } a \geq 0 \\ -a, & \text{otherwise.} \end{cases} \end{aligned}$$

Before we move forward, a couple of important definitions:

Definition 1.3.1.5. *Given any function $f : A \to B$, the set of all elements of B which are image of some element of A under f will be called the **image of** A **under** f (or just the image of f) and denoted by $f(A)$ (or $\mathrm{Im}(f)$).*

*Analogously, given any $X \subseteq A$, we denote the set of all elements of B which are image of some element of X under f by **image of** f **when restricted to** X, and denote it by $f(X)$.*

Proposition 1.3.1.6. *For any function $f : A \to B$, and any $X \subseteq A$, $f(X) \subseteq B$.*

Proof

Trivial, by the definition of image of a function. □

Definition 1.3.1.7. *Given any function $f : A \to B$ and any point $b \in f(A)$, we define the **inverse image of** b **under** f to be the set $f^{-1}(b) := \{a \in A \mid f(a) = b\}$ of all points in A whose image under f is precisely b.*

*Analogously, given any $Y \subseteq f(A)$, we define the **inverse image of** Y **under** f to be the set $f^{-1}(X) := \{a \in A \mid f(a) \in Y\}$ of all points in A whose image under f is in Y.*

Proposition 1.3.1.8. *For any function $f : A \to B$, and any $Y \in f(A)$, $f^{-1}(Y) \subseteq A$.*

Proof

Trivial, by the definition of inverse image of a function. □

Finally we can start working with some very important classes of functions: Injections, surjections and bijections.

Definition 1.3.1.9. *A function $f : A \to B$ is called an* ***injection*** *if $f(a) = f(a')$ implies $a = a'$.*

Remark 1.3.1.10

This is logically equivalent to saying that a function is an injection if diferent points of the domain have different images in the codomain.

Example(s)

Let $f, g : \{1, 2, 3\} \to \{a, b, c, d\}$ be defined by: $f(1) = a, f(2) = b, f(3) = c$ and $g(1) = g(2) = g(3) = d$. Then f is injective and g is clearly not injective.

Let, now, $h : \mathbb{R} \to \mathbb{R}$ be defined by $h(x) = x^2$. Is h injective?
Well, suppose x and x' are such that $h(x) = h(x')$. This means that $x^2 = x'^2$. Taking square roots on both sides we get that $|x| = |x'|$ - which can be further simplified to mean $x = \pm x'$. In other words, we see that if two points have the same square, then they must differ only by a sign. That's good and all, but also shows us that two numbers that differ by a sign have the same image under h - and therefore h cannot be injective.
For instance, $2 \neq -2$, but $h(2) = h(-2) = 4$.

Definition 1.3.1.11. *A function $f : A \to B$ is called a* ***surjection*** *if for any $b \in B$ there is some $a \in A$ such that $f(a) = b$.*

Example(s)

Following up on the previous example, neither f nor g are surjections: $d \in \{a, b, c, d\}$ isn't in the image of any point over both f and g.
Let us then define $f' : \{a, b, c, d\} \to \{1, 2, 3\}$ by putting $f'(a) = 1, f'(b) = 2, f'(c) = 3, f'(d) = 3$. Now, f' is indeed a surjection.

Notice that h too isn't a surjection: -1 isn't the image of any real number under h. However, if we define $h' : \mathbb{R} \to \mathbb{R}^{\geq 0}$, where $\mathbb{R}^{\geq 0}$ is the set of all non-negative real numbers, by putting $h'(x) := h(x)$, we see that h' is, now, a surjection.

Remark 1.3.1.12

Note that, in the example above, we defined h' by putting $h'(x) := h(x)$. Does that mean that $h' = h$?
The answer is **no**: By the definition of function equality, for two functions to be equal they must have the same domain and codomain.
This is a very important distinction, and one that most mathematicians and students rarely pay attenttion to.

Finally, we can define:

Definition 1.3.1.13. *A function $f : A \to B$ is called a* ***bijection*** *if it is both an injection and a surjection.*

Example(s)

None of the previous examples are bijections, so we have to come up with new examples.
Let $f : \{a, b, c\} \to \{1, 2, 3\}$ be defined by $f(a) = 1, f(b) = 2, f(c) = 3$. Then f is both injective and surjective, and, therefore, a bijection by definition.

Let $g : \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ be defined by $g(x) = x^2$. Then g is both injective (since there's only one sign on the domain) and surjective (since that are no negatives on the codomain), and, therefore, bijective by definition.

Let $h : \{a, b, c\} \to \{a, b, c\}$ be defined by $h(a) = a, h(b) = c, h(c) = b$. Is h a bijection? Well, it clearly is both injective and surjective, so it has to be by definition.
Notice that bijections don't have to abide by our expectations (such is life).

Lemma 1.3.1.14. *If $f : A \to B$ is injective, then there is a bijection $g : A \to f(A)$.*

Proof

Let $g : A \to f(A)$ be defined by $g(a) := f(a)$ for all $a \in A$.

- g is injective:

  To see that, take $a, a' \in A$ such that $g(a) = g(a')$. Then, by definition, this implies $f(a) = f(a')$, and since f is injective, this in turn implies $a = a'$, so g is injective.

- g is surjective:

  To see that, take any $b \in f(A)$. By definition of image, there exists some $a \in A$ such that $b = f(a)$. But now, by defintion of g, this means that $b = g(a)$.

  We have just shown that every point in the codomain of g is the image of some point in the domain of g under g - this means that g is surjective.

Since g is both injective and surjective, it is, by definition, a bijection, which ends the proof. $\square$

We can use this lemma to easily determine whether a function is, or isn't, an injection.

Example(s)

Let $f : \{a, b, c\} \to \{1, 2\}$ be defined by $f(a) = 1, f(b) = 2, f(c) = 1$. Is f injective?
Well, f takes two different points (a and c) to the same point (1), so it can't be injective.

Actually - is it possible for there to be an injective function from $\{a, b, c\}$ to $\{1, 2\}$?
Let's try making one: First, we choose an image for a - it can be either 1 or 2 - doesn't

matter which. Now, to choose an image for b we can't choose the same point as we chose for a - otherwise f won't be injective. So b's image is now uniquely determined: the only point left in $\{1, 2\}$ after we take out $f(a)$. Finally, when we try to choose an image for c, it can't be $f(a)$, nor can in be $f(b)$ (otherwise, f wouldn't be injective). But $\{1, 2\} = \{f(a), f(b)\}$ - that is, if $f(c)$ can't be $f(a)$ and it can't be $f(b)$, then there's **nothing** that it can be!
But, on the other hand, since f is a function, we **have to** take c somewhere. This means that we **have to** repeat either $f(a)$ or $f(b)$.
This shows that there are no injective functions from $\{a, b, c\}$ to $\{1, 2\}$.

Lemma 1.3.1.15. *If $f : A \to B$ is surjective, then there is a bijection $g : f(A) \to B$.*

Proof

Let $g : f(A) \to B$ be defined by $g(b) := b$ for all $b \in f(A)$.

- g is surjective:

  To see that, take any $b \in B$. Since f is surjective, for each point in B there is at least one point in A which is its inverse image under f - in particular, there is some $a \in A$ such that $f(a) = b$. But this means that $b \in f(A)$, by definition of image of f. Now, since $b \in f(A)$, we see that $g(b) = b$ and, therefore, g is surjective.

- g is injective:

  To see that, take any two points $b, b' \in f(A)$ such that $g(b) = g(b')$. But, by definition of g, this is the same as saying $g = g'$ - therefore g is injective.

Since g is both injective and surjective, it is, by definition, a bijection, which ends the proof. $\square$

Analogously to injections, this lemma gives us a clear cut method for distinguishing surjections:

Example(s)

Let $f : \{1, 2\} \to \{a, b, c\}$ be given by $f(1) = a$ and $f(2) = b$. Clearly, then, f isn't surjective, because there is one point in its codomain (c) which is not the image of any point of the domain under f.

And then we ask: Can there ever be a surjective function from $\{1, 2\}$ to $\{a, b, c\}$?
Once again, let's try building one: First, we choose $f(1)$. It can be anything, so choose anything. Now to choose $f(2)$, there's also no restrictions, but remember that we're trying to make a function that "covers" $\{a, b, c\}$ with guys from $\{1, 2\}$, so even though we could put $f(2) := f(1)$, it makes sense to choose $f(2)$ to be anything aside from $f(1)$... And we're done.
Notice, however, that no matter **how** we do that choice, there'll always be some point left in $\{a, b, c\}$. Therefore, there can be no surjections from $\{1, 2\}$ to $\{a, b, c\}$.

These last two examples give us a nice intuition of what injections and surjections measure: Injections measure how much "smaller" the domain is, when compared to the codomain, and surjections measure how much "bigger" the codomain is, when compared to the domain.

This allows us to consider one final example:

Example(s)

Let $f : \{a, b, c\} \to \{1, 2, 3\}$ be a function. Can f be a bijection?
Let's try: First, we choose any of $\{1, 2, 3\}$ to be $f(a)$. Now, since we want f to be a bijection, it needs to be injective and surjective, so we can't choose $f(b) = f(a)$, so choose $f(b)$ to be any of $\{1, 2, 3\} \setminus \{f(a)\}$. Again, by the same reasoning, choose $f(c)$ to be any of $\{1, 2, 3\} \setminus \{f(a), f(b)\}$ - which isn't really a choice, since there's only one point left.
And we're done! By construction, $f(a) \neq f(b)$, $f(a) \neq f(c)$ and $f(b) \neq f(c)$ (so f is injective) and all of $\{1, 2, 3\}$ have inverse images.
This is a strong intuition that we want to build at this point:
Bijections between two sets tell us if they have the same amount of points. In many ways, then, bijections can be thought of as a relabeling of your set - or even, in some cases, as the *definitive and improved* notion of set equality.
And it makes sense - why should the sets $\{a, b, c\}$ and $\{1, 2, 3\}$ be treated as being different? You might argue that $1 + 2 = 3$, but $a + b$ doesn't even make sense - but the point here is that even $1 + 2$ doesn't make sense. There's no operations being taken into consideration, nothing. Just sets with elements. The only information we have is that "$\{a, b, c\}$ is a set with three distinct things inside it" and that "$\{1, 2, 3\}$ is a set with three distinct things inside it". *What* those things are doesn't really matter to us from a set-theoretical POV. What matters is that there are some things.

To expand in that idea - that bijections are the new equality - we're gonna start a more technical subsection.

The reader is encouraged to **not** skip this section, although I don't own you, so you do you. This subsection will have many proofs, so it's good for practicing your proofs, but not only that - the reasoning employed here is central to understanding what's behind many of the most intricate results in linear algebra.

1.3.2 Bijection is the new equality

Definition 1.3.2.1. *Given any two functions $f : A \to B$ and $g : B \to C$, we call the function $g \circ f : A \to C$ defined by $(g \circ f)(a) := g(f(a))$ the* ***composition*** *of f and g.*

Definition 1.3.2.2. *Given any set X, we call the function $\mathrm{id}_X : X \to X$ defined by $\mathrm{id}_X(x) := x$ the* ***identity function*** *of X.*

Definition 1.3.2.3. *Given a function $f : A \to B$, we say that f* ***is an isomorphism*** *if there is some function $g : B \to A$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$. In this case, we say that g is an* ***inverse*** *for f.*

Proposition 1.3.2.4. *Function composition is associative - that is, if $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, then $h \circ (g \circ f) = (h \circ g) \circ f$.*

Proof

Take $a \in A$. Then,

$$\begin{aligned}(h \circ (g \circ f))(a) &= h((g \circ f)(a)) \\ &= h(g(f(a))) \\ &= (h \circ g)(f(a)) = ((h \circ g) \circ f)(a)\end{aligned}$$

and therefore $(h \circ (g \circ f))(a) = ((h \circ g) \circ f)(a)$ for any $a \in A$ which, by the definition of function equality, implies that $h \circ (g \circ f) = (h \circ g) \circ f$. $\square$

Proposition 1.3.2.5. *Given any function $f : A \to B$, we have that $f = \mathrm{id}_B \circ f = f \circ \mathrm{id}_A$.*

Proof

Take any $a \in A$. Then:

$$(\mathrm{id}_B \circ f)(a) = \mathrm{id}_B(f(a)) = f(a) = f(\mathrm{id}(a)) = (f \circ \mathrm{id}_A)(a)$$

which implies, by the definition of function equality, that $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$. $\square$

Proposition 1.3.2.6. *Let $f : A \to B$ be an isomorphism, and let $g, h : B \to A$ be two inverses for f. Then $g = h$.*

Proof

This follows from the two preceding propositions and the definition of isomorphism:

$$g = g \circ \mathrm{id}_B = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_A \circ h = h.$$

$\square$

Definition 1.3.2.7. *Given an isomorphism f, we will denote its (unique!) inverse by f^{-1}.*

Definition 1.3.2.8. *A function $f : A \to B$ is called a **monomorphism** if given any other two functions $g, h : C \to A$, we have that $f \circ g = f \circ h$ implies $g = h$.*

Example(s)

Let $f : \{1, 2, 3\} \to \{a, b, c, d\}$ be defined by $f(1) = a, f(2) = b, f(3) = c$. We claim that f is a monomorphism.
To see that, take any $g, h : C \to \{1, 2, 3\}$ such that $f \circ g = f \circ h$. In particular, for any $x \in C$ we have that $f(g(x)) = f(h(x))$. Well, this means that $f(g(x))$ is either a, b or c. In either case, we know precisely who $g(x)$ is (for instance, if $f(g(x))) = b$, then $g(x) = 2$, since 2 is the only point which is taken to b via f).
But since $f(g(x)) = f(h(x))$, there's a unique $u \in \{1, 2, 3\}$ such that $y = g(x) = h(x)$. In particular, $g(x) = h(x)$.
This shows that $g = h$, and, therefore, f is a monomorphism.

Theorem 1.3.2.9. *A function is a monomorphism if, and only if, it is an injection.*

Proof

Assume that $f : A \to B$ is injective. Then given $g, h : C \to A$ such that $f \circ g = f \circ h$ we want to show that $g = h$. Since f is injective, $f(g(c)) = f(h(c))$ implies $g(c) = h(c)$, for all $c \in C$. It follows, then, that $g = h$ and f is monic.

Conversely, if $f : A \to B$ is monic, define $g, h : \{c\} \to A$ by putting $g(c) = a$ and $h(c) = a'$ for two $a \neq a' \in A$ fixed. Now, since f is monic, by assumption, and since $g \neq h$, we have that $f \circ g \neq f \circ h$ (otherwise we would have f monic, $f \circ g = f \circ h$ and $g \neq h$ all being true, which is impossible). But then:

$$f(a') = f(h(c)) = f \circ h(c) \neq f \circ g(c) = f(g(c)) = f(a)$$

that is, $a \neq a'$ assures us that $f(a) \neq f(a')$, and so f is injective.
Notice that we used the fact that there are two distinct points in A: a and a'. If, however, A has only one point it is even simpler: Any function from a set with a single point has to be injective - in particular, monomorphisms whose domain are a single point are injective.
This finishes the proof. $\square$

Lemma 1.3.2.10. *Every isomorphism is a monomorphism.*

Proof

Let $f : A \to B$ be an isomorphism and $g, h : C \to A$ any two functions such that $f \circ g = f \circ h$. Then, since f is an isomorphism, there is a unique inverse $f^{-1} : B \to A$ such that $\mathrm{id}_A = f^{-1} \circ f$

and $\text{id}_B = f \circ f^{-1}$. Therefore:

$$g = \text{id}_A \circ g = (f^{-1} \circ f) \circ g = f^{-1} \circ (f \circ g) = f^{-1} \circ (f \circ h) = (f^{-1} \circ f) \circ h = \text{id}_A \circ h = h$$

and we see that f is monic. $\square$

Definition 1.3.2.11. *A function $f : A \to B$ is called an **epimorphism** if given any other two functions $g, h : B \to C$, we have that $g \circ f = h \circ f$ implies $g = h$.*

Example(s)

Let $f : \{a, b, c\} \to \{1, 2\}$ be defined by $f(a) = f(b) = 1$ and $f(c) = 2$. We claim that f is epic.
To see that, take any two functions $g, h : \{1, 2\} \to C$ such that $g \circ f = h \circ f$. We want to show that $g = h$ - that is, for any $x \in \{1, 2\}$, we have that $g(x) = h(x)$.
But since f is surjective (check!), there is some $y \in \{a, b, c\}$ such that, then $x = f(y)$, so

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

and therefore we see that $g = h$, which proves that f is indeed an epimorphism.

Theorem 1.3.2.12. *A function $f : A \to B$ is an epimorphism if, and only if, it is a surjection.*

Proof

First, let us assume that $f : A \to B$ is surjective. Then, given $g, h : B \to C$ such that$g \circ f = h \circ f$ we wish to show that $g = h$. We can just proceed as above: Proving that $g = h$ is the same as proving that for all $x \in B$, we have that $g(x) = h(x)$, but since f is surjective, by assumption, we have that there is some $y \in A$ such that $x = f(y)$. It follows then that

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

and therefore $h = g$, which shows that f is epic.
Conversely, assume that f is epic, and let $C = \{c, c'\}$. Now pick a point $b \in B$ and define $g, h : B \to C$ by putting $g(x) = c$ for all $x \in B$, $h(b) = c'$ and $h(x) = c$ if $x \neq b$.
Now, $g(b) \neq h(b)$, so $g \neq h$. Since f is epic, we must then have that $g \circ f \neq h \circ f$, by definition of epimorphism. This means that there is some $a \in A$ such that $g(f(ay)) \neq h(f(a))$.
Since g takes everyone to c, the only possible value of $h(f(a))$ that could be different from that is is $h(f(a)) = c'$, but the only element of B that is taken to c' by h is b - this means that $f(a) = b$.
We have just proven that given any $b \in B$ there is some $a \in A$ such that $f(a) = b$ - that is, f is surjective, which finishes the proof. $\square$

Lemma 1.3.2.13. *Every isomorphism is an epimorphism.*

Proof

Let $f : A \to B$ be an isomorphism and $g, h : B \to C$ two functions such that $g \circ f = h \circ f$. Since f is an isomorphism, it has an inverse $f^{-1} : B \to A$. Therefore:

$$g = g \circ \mathrm{id}_B = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = (h \circ f) \circ f^{-1} = h \circ (f \circ f^{-1}) = h \circ \mathrm{id}_B = h$$

and we see that $g = h$, which proves that f is an epimorphism. □

Definition 1.3.2.14. *A function $f : A \to B$ is called a **bimorphism** if it is a mono-epimorphism.*

Clearly, by what we've already shown, bijections and bimorphisms are the same thing. However, we can do one better than that:

Lemma 1.3.2.15. *Every monomorphism $f : A \to B$ has a left-inverse, that is, a function $g : B \to A$ such that $\mathrm{id}_A = g \circ f$, and every function which has a left-inverse is a monomorphism.*

Proof

Let $f : A \to B$ be a monomorphism and consider $f(A)$. Since f is monic, by theorem 1.3.2.9 we see that f is injective, which means that for all $b \in f(A)$ we have that $f^{-1}(b)$ is a single point in A.
We then define $g : B \to A$ by

$$g(b) = \begin{cases} f^{-1}(b), & \text{if } b \in f(A) \\ a, & \text{otherwise,} \end{cases}$$

where $a \in A$ is any (literally any) element of A.
We claim that this g is a left-inverse for f. Indeed, for any $x \in A$ we have

$$(g \circ f)(x) = g(f(x)) = f^{-1}(f(x)) = x = \mathrm{id}_A(x)$$

since $f(x) \in f(A)$ for all $x \in A$. Therefore, we have shown that for all x we have $(g \circ f)(x) = x = \mathrm{id}_A(x)$ - which implies, by the definition of function equality, that $g \circ f = \mathrm{id}_A$.

Take now $f : A \to B$ a function that has a left-inverse $g : B \to A$ - that is, $\mathrm{id}_A = g \circ f$. Now take two functions $h, j : C \to A$ such that $f \circ h = f \circ j$. We want to show that $h = j$ (and therefore, f is monic).
Since $f \circ h = f \circ j$, we can compose g on the left on both sides of the equation to obtain $g \circ (f \circ h) = g \circ (f \circ j)$, which, by proposition 1.3.2.4, is the same as $(g \circ f) \circ h = (g \circ f) \circ j$, and since g is a left-inverse to f, we can further affirm that this is the same as $\mathrm{id}_A \circ h = \mathrm{id}_A \circ j$. Finally, by the definition of id_A, we see that this implies $h = j$ - and therefore f is monic, as stated.
This finishes the proof. □

Lemma 1.3.2.16. *Every epimorphism $f : A \to B$ has a right-inverse, that is, a function $g : B \to A$ such that $\mathrm{id}_B = f \circ g$, and every function which has a right-inverse is an epimorphism.*

Proof

Let $f : A \to B$ be an epimorphism, and consider $f(A)$ its image. By theorem 1.3.2.12, we know that g is a surjection. Since g is a surjection, then, for every $b \in B$ the set $f^{-1}(b)$ is well defined (by definition of surjection).
Now, choose $a_b \in f^{-1}(b)$ for each $b \in B$ (here the index is simply so we know where it came from), and consider the function $g : B \to A$ taking each b to the a_b we chose above.
This is clearly a function (check!), and so we can do, for evrey $b \in B$:

$$(f \circ g)(b) = f(g(b)) = f(a_b) = b = \mathrm{id}_B(b)$$

and therefore $f \circ g$ and id_B are equal in every point - which means that they're equal, and g is a right-inverse for f, as stated.

Take now $f : A \to B$ a function with a right-inverse $g : B \to A$ - that is, $f \circ g = \mathrm{id}_B$. Now take two functions $h, j : B \to C$ such that $h \circ f = j \circ f$. We want to show that $h = j$ (and, therefore, f is epic).
Since $h \circ f = j \circ f$, we can compose g on the right on both sides of the equation to obtain $(h \circ f) \circ g = (j \circ f) \circ g$, which, by proposition 1.3.2.4, is the same as $h \circ (f \circ g) = j \circ (f \circ g)$, and since g is a right-inverse to f, we can further affirm that this is the same as $h \circ \mathrm{id}_B = j \circ \mathrm{id}_B$. Finally, by the definition of id_B, we see that this implies $h = j$ - and therefore f is epic, as stated.
This finishes the proof. $\square$

Lemma 1.3.2.17. *If a function $f : A \to B$ is such that $g, h : B \to A$ are a left- and a right-inverse, respectively, then $g = h$, f is an isomorphism and g is its inverse.*

Proof

It follows trivially by the following computation:

$$g = g \circ \mathrm{id}_B = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_A \circ h = h,$$

which shows at once that $g = h$. This means that $\mathrm{id}_A = g \circ f$ and $\mathrm{id}_B = f \circ g$ - and therefore g is an inverse to f, which shows that f is an isomorphism, as stated. $\square$

Theorem 1.3.2.18. *A function f is an isomorphism if, and only if, it is a bimorphism.*

Proof

In light of lemmas 1.3.2.10 and 1.3.2.13, we see that every isomorphism is monic and epic and, therefore, a bimorphism.
Conversely, by lemmas 1.3.2.15 and 1.3.2.16 we see that any bimorphism has both a left- and a right-inverse. But now, lemma 1.3.2.17 shows us that since every bimorphism has a left- and a right-inverse, it must be an isomorphism, which ends the proof. □

Corollary 1.3.2.19. *Every bijection has a unique inverse.*

And now, finally, to end this section, some technical results that appear all the time in mathematics.

Lemma 1.3.2.20. $A \xrightarrow{f} B \xrightarrow{g} C$ *be two functions. Then the following hold:*

(a) If both f and g are monic, then so is $g \circ f$;

(b) If both f and g are epic, then so is $g \circ f$;

(c) If both f and g are iso, then so is $g \circ f$;

(d) If $g \circ f$ is monic, then so is f;

(e) If $g \circ f$ is epic, then so is g;

(f) If $g \circ f$ and f are iso, then so is g;

(g) If $g \circ f$ and g are iso, then so is f.

Proof

(a) Assume both f and g are monic, and let $f' : B \to A$ and $g' : C \to B$ be their respective left-inverses. We claim that $f' \circ g'$ is a left-inverse to $g \circ f$. Indeed:

$$(f' \circ g') \circ (g \circ f) = f' \circ (g' \circ g) \circ f = f' \circ \mathrm{id}_B \circ f = f' \circ f = \mathrm{id}_A$$

so $g \circ f$ is monic.

(b) Assume both f and g are epic, and let $f' : B \to A$ and $g' : C \to B$ be their respective right-inverses. We claim that $f' \circ g'$ is a right-inverse to $g \circ f$. Indeed:

$$(g \circ f) \circ (f' \circ g') = g \circ (f \circ f') \circ g' = g \circ \mathrm{id}_B \circ g' = g \circ g' = \mathrm{id}_C$$

so $g \circ f$ is epic.

(c) Follows immediately from (a) and (b).

(d) If $g \circ f$ is monic, by lemma 1.3.2.15 we see that there is some function $h : C \to A$ that is a left-inverse to $g \circ f$ - that is, $\mathrm{id}_A = h \circ (g \circ f)$. But now, by proposition 1.3.2.4, we see that $h \circ (g \circ f) = (h \circ g) \circ f$ and, therefore, $\mathrm{id}_A = (h \circ g) \circ f$ and we see that $h \circ g$ is a left-inverse for f. Now the converse of lemma 1.3.2.15 tells us that since f has a left-inverse, it must be monic.

(e) If $g \circ f$ is epic, by lemma 1.3.2.16 we see that there is some function $h : B \to C$ that is a right-inverse to $g \circ f$ - that is, $\mathrm{id}_B = (g \circ f) \circ h$. But now, by proposition 1.3.2.4, we see that $(g \circ f) \circ h = g \circ (f \circ h)$ and, therefore, $\mathrm{id}_B = g \circ (f \circ h)$ and we see that $f \circ h$ is a right-inverse to g. Now, the converse of lemma 1.3.2.16 tells us that since g has a right-inverse, it must be epic.

(f) If f is iso, then so is f^{-1} (its inverse is precisely f). Therefore, the equality $g \circ f = g \circ f$ yields the equality $(g \circ f) \circ f^{-1} = g$ by composing f^{-1} to the right on both sides of the equality. Now we use item (c) to conclude that since g is the composition of two isomorphisms, it is also an isomorphism.

(g) If g is iso, then so is g^{-1} (its inverse is precisely g). Therefore, the equality $g \circ f = g \circ f$ yields the equality $g^{-1} \circ (g \circ f) = f$ by composing g^{-1} to the left on both sides of the equality. Now we use item (c) to conclude that since f is the composition of two isomorphisms, it is also an isomorphism.

This ends the proof. $\square$

And finally we end this section with a definition.

Definition 1.3.2.21. *Two sets are said to have* ***the same cardinality*** *if they are isomorphic - that is, if there is an isomorphism between them. If A and B have the same cardinality, we will represent that in symbols by $\#A = \#B$.*

Remark 1.3.2.22

Notice that for finite sets, $\#A$ is precisely the formalization of the intuitive notion of "number of elements of A".

1.3.3 The A and Ω of sets

Now that we have dealt with functions and their properties, we can use them to define new sets.

Before that, though, let's have a quick talk about *universal properties*.

A *universal property* is a way of defining something by saying it's somewhat singular in the universe. For instance, when defining the union and intersection of two sets, we didn't use the classical definition, but, instead, used a universal property to define those sets.

Here's the advantage of working with universal properties:

Definition 1.3.3.1. *We say that a set X is* ***initial*** *if there is a unique function from X to any other set.*

Similarly, we say that X is ***terminal*** *if there is a unique function from any other set to X.*

Meta-theorem

All universal properties can be coded in terms of initial/terminal objects on a specific class of sets.

For instance, the union of A and B is the *initial* set in the class of all sets containing A and B. Analogously, the intersection of A and B is the *terminal* set in the class of all sets contained in A and B.

Meta-theorem

All sets defined by universal properties are uniquely defined (up to isomorphism).

This means that if X is initial/terminal regarding a certain class of sets, then it is the unique set in that class that is initial/terminal (not counting sets that are isomorphic to X).

Proof

Let X and Y be two sets which are initial regarding a certain class of sets. Since X is initial, there's a unique function $!_Y : X \to Y$. Since Y is initial, there's a unique function $!_X : X \to Y$. This gives us, by composition, a function $!_X \circ !_Y : X \to X$ and a function $!_Y \circ !_X : Y \to Y$.

Now remember that for any set, there's always its identity map. So we have $\mathrm{id}_X : X \to X$ and $\mathrm{id}_Y : Y \to Y$.

But since X is initial, there's a unique function from X to itself. Since there's always an identity function, that function must be the unique map. But we've just shown that $!_X \circ !_Y$ is also a map from X to itself. It follows then that $\mathrm{id}_X = !_X \circ !_Y$.

Arguing similarly for Y we can show that $\mathrm{id}_Y = !_Y \circ !_X$, and, therefore, $!_Y$ is an inverse for $!_X$, and hence they are isomorphisms.

The proof for the terminal case is identical and left as an exercise to the reader. $\square$

This is another reason why isomorphism is a better notion of set equality - because sets defined by universal properties are unique, up to isomorphism.

Finally, before defining new sets using universal properties, let us prove a couple of interesting results:

Lemma 1.3.3.2. *The set $\varnothing$ is the initial set of all sets.*

Proof

There clearly is only one function from $\varnothing$ to any other set.
To see this, think of what would have to go wrong for there to be two different functions, f and g: We'd have to have one element x of $\varnothing$ such that $f(x) \neq g(x)$. But $\varnothing$ doesn't have any elements, so any two functions defined on it must be equal. $\square$

Lemma 1.3.3.3. *The set $\{a\}$ is the terminal set of all sets.*

Proof

There clearly is only one function from any set to $\{a\}$: The function sending all elements of your domain to a. $\square$

Corollary 1.3.3.4. *There is only one function from any singleton (i.e. a set with a single element) to $\{a\}$.*

Proof

Follows trivially by the preceding lemma. $\square$

Corollary 1.3.3.5. *Any two singletons are isomorphic.*

Proof

It is also trivial to prove that any other singleton is also a terminal object. Therefore, it must be isomorphic to $\{a\}$.
Take, then, two singletons $*$ and $\bullet$, and do:

$$* \leftrightarrow \{a\} \leftrightarrow \bullet,$$

where the $\leftrightarrow$ denote the unique isomorphism between the two sets. This is a composition of isomorphisms and, therefore, an isomorphism. $\square$

Corollary 1.3.3.6. *All terminal objects are singletons.*

Proof

Take T any terminal object.
By the preceding lemma, it must be isomorphic to a singleton $\{a\}$. This means that there is a bijection $f : \{a\} \to T$. This means, by lemma 1.3.1.14 and lemma 1.3.1.15, that the image of this isomorphism is isomorphic to $\{a\}$ (since isomorphisms are injective), and the image is also equal to T (since isomorphisms are surjective).
But since the image is a singleton ($\operatorname{Im} f = \{f(a)\}$), we have that T is a singleton as well, which ends the proof. $\square$

Remark 1.3.3.7

For reasons that will become clearer further ahead, for here onwards we're gonna denote the unique initial set by 0 and the unique terminal set by 1 (sometimes by $*$ to avoid misconceptions and misunderstandings).

1.3.4 Multiplying sets

Now that this is done, let us define new sets using universal properties:

Definition 1.3.4.1. *Let X and Y be two sets. We define the **product of** X **and** Y to be the set $X \prod Y$ which is terminal in the class of sets with functions to both X and Y - this means that:*

i. There are functions $\pi_X : X \prod Y \to X$ and $\pi_Y : X \prod Y \to Y$;

ii. If Z is some set with functions $p_X : Z \to X$ and $p_Y : Z \to Y$, then there is a unique function $p : Z \to X \prod Y$ such that $p_X = \pi_X \circ p$ and $p_Y = \pi_Y \circ p$.

We usually denote this saying that the following diagram commutes:

$$\begin{tikzcd}
 & Z \arrow[d, dashed, "\exists! p"] \arrow[ddl, bend right, "p_X"'] \arrow[ddr, bend left, "p_Y"] & \\
 & X \prod Y \arrow[dl, "\pi_X"] \arrow[dr, "\pi_Y"'] & \\
X & & Y
\end{tikzcd}$$

This means that no matter which path we take on the diagram, the end result should be the same.

Now, this may seem very abstract and weird at first. But I assure you that you already know what that is.

Definition 1.3.4.2. *Let X and Y be two sets. We define the **cartesian product of** X **and** Y to be the set $X \times Y$ of all ordered pairs (x, y) such that $x \in X$ and $y \in Y$.*

This is a well-known definition.

Example(s)

Let $A = \{a, b, c\}$ and $B = \{1, 2\}$. Then $A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$ is the cartesian product of A and B.
Let $C = \{$yellow pants, brown pants, shorts$\}$ and $D = \{$crop top, black shirt, sweater, jacket$\}$. Then $C \times D$ is the set of all possible combinations of pants types (C) and shirt types (D) in your closet.

Now, since the two previous definitions have such similar names they must be related in some way, right? Well...

Proposition 1.3.4.3. *For any two sets X and Y, their cartesian product $X \times Y$ is the product $X \prod Y$.*

Proof

We have to show two things: (i.) There are functions $\pi_X : X \times Y \to X$ and $\pi_Y : X \times Y \to Y$ and; (ii.) It is terminal with that property.

To show (i.), let us define π_X and π_Y as follows: $\pi_X(x, y) := x$ and $\pi_Y(x, y) := y$ for all $(x, y) \in X \times Y$. These are clearly functions from $X \times Y$ to both X and Y, so (i.) is done.

Now take any other set Z with functions $p_X : Z \to X$ and $p_Y : Z \to Y$. We want to build a function $p : Z \to X \times Y$ such that $p_X = \pi_X \circ p$ and $p_Y = \pi_Y \circ p$, and show that it is the unique function with that property.
Well, take $z \in Z$ and follow it around: If we apply p_X to z we get $p_X(z) \in X$, and, similarly, applying p_Y we get $p_Y(z) \in Y$. Since $p_X(z)$ is in X and $p_Y(z)$ is in Y, by definition of cartesian product we have that $(p_X(z), p_Y(z))$ is in $X \times Y$.
Now, clearly we have that $\pi_X(p_X(z), p_Y(z)) = p_X(z)$ and $\pi_Y(p_X(z), p_Y(z)) = p_Y(z)$ (this is precisely how we defined π_X and π_Y above). So it is obvious what we must define $p : Z \to X \times Y$ to be:

$$p(z) := (p_X(z), p_Y(z))$$

for all $z \in Z$.
This is clearly a function from Z to $X \times Y$ and, by definition, $p_X = \pi_X \circ p$ and $p_Y = \pi_Y \circ p$.

To finish this, we need to show that this p is unique. Well, suppose there is another function, $q : Z \to X \times Y$ such that $p_X = \pi_X \circ q$ and $p_Y = \pi_Y \circ q$. But then, for every $z \in Z$ we'd have that $p_X(z) = \pi_X(q(z))$ and $p_Y(z) = \pi_Y(q(z))$.
This means that $q(z)$ is a point in $X \times Y$ whose X-coordinate is $p_X(z)$ (this is what the equation $p_X(z) = \pi_X(q(z))$ tells us), and whose Y-coordinate is p_Y (this is what the equation $p_Y(z) = \pi_Y(q(z))$ tells us).
Therefore, $q(z) = (p_X(z), p_Y(z))$ and the RHS is just $p(z)$, by definition. So we have $q(z) = p(z)$ for all $z \in Z$ - which implies, by the definition of function equality, that $q = p$.
It follows then that the p we've defined is the unique function with that property, so $X \times Y$ is indeed the product of X and Y, which ends the proof. $\square$

What's the advantage of defining via universal property instead of just outright using the classical definition? Well...

It's easy to prove that, using the classical definition, we can take any finite number of sets $\{A_i\}_{i \leq n}$ and take their product $A_1 \times A_2 \times \cdots \times A_n$ to be the iterated product:

A_1 and A_2 are well-defined, so $A_1 \times A_2$ is well-defined.
But now, $A_1 \times A_2$ and A_3 are well-defined, so $(A_1 \times A_2) \times A_3$ is well-defined.
And so on, up to A_n.

But try doing that for infinitely many sets. Heck, try doing that for an uncountable amount of sets.

It's not easy to see how to even *define* such an operation if the set of indices isn't, say, ordered.

However, using the universal property, we can define the product of *any* amount of sets:

Definition 1.3.4.4. *Let $\{A_i\}_{i\in I}$ be a collection of sets indexed by another set I (which can be infinite or finite, countable or uncountable, doesn't matter, as long as it's a set). We define $\prod_{i\in I} A_i$ to be the set given by:*

i. There is a function $\pi_n : \prod_{i\in I} A_i \to A_n$ for each $n \in I$;

ii. If Z is a set with a function $p_n : Z \to A_n$ for each $n \in I$, then there's a unique function $p : Z \to \prod_{i\in I} A_i$ such that $p_n = \pi_n \circ p$ for each $n \in I$.

Which is just the *same* definition we used for the product of two sets, but generalized for *any* amount of sets.

This is another great reason to prefer definitions via universal properties instead of explicit ones.

Definition 1.3.4.5. *Given three sets A, B and C with functions $f : A \to B$ and $g : A \to C$, the unique function from A to $B \times C$ induced by the definition of product will be called the* ***product map of** f **and** g* *and denoted by $f \times g : A \to B \times C$.*

By definition, $(f \times g)(a) := (f(a), g(a))$ for any $a \in A$.

Example(s)

Let $\mathbb{R}$ be the set of real numbers, $f, g : \mathbb{R} \to \mathbb{R}$ be defined by $f := \mathrm{id}_{\mathbb{R}}$ and $g(x) := x^2$ for any $x \in \mathbb{R}$. Then the product map $f \times g : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ is the map $x \mapsto (x, x^2)$ for any $x \in \mathbb{R}$.

Definition 1.3.4.6. *The product map of id_X and id_X, for any set X will be called the* ***diagonal map of** X* *and denoted by $\Delta_X : X \to X \times X$.*

It is, as in the above definition, the unique map commuting the diagram

$$\begin{tikzcd}
& X \arrow[d, "\exists!\Delta_X"] \arrow[ddl, bend right, "\mathrm{id}_X"'] \arrow[ddr, bend left, "\mathrm{id}_X"] & \\
& X \times X \arrow[dl, "\pi^1_X"] \arrow[dr, "\pi^2_X"'] & \\
X & & X.
\end{tikzcd}$$

Example(s)

Let $A = \{a, b, c\}$. Let's calculate Δ_A.
By definition, we must have $\mathrm{id}_A = \pi^1_A \circ \Delta_A$ and $\mathrm{id}_A = \pi^1_A \circ \Delta_A$. So take any $a \in A$.
We know that, from the first equation, we must have $a = (\pi^1_A \circ \Delta_A)(a) = \pi^1_A(\Delta_A(a))$, so the first coordinate of $\Delta_A(a)$ must be a.
Similarly, the second equation gives us $a = (\pi^2_A \circ \Delta_A)(a) = \pi^2_A(\Delta_A(a))$ and so, the second coordinate of $\Delta_A(a)$ must also be a.

Since $\Delta_A(a) = (\pi_A^1(\Delta_A(a)), \pi_A^2(\Delta_A(a)))$, we get that $\Delta_A(a) = (a, a)$ for any $a \in A$. This is why it's called the *diagonal* map.

Remark 1.3.4.7

From here onwards, the symbol $\cong$ will mean "is isomorphic to" - so $A \cong B$ should be read as "A is isomorphic to B".

Let us then prove some nice properties of products:

Lemma 1.3.4.8. *For any three sets A, B and C the following hold:*

(a) $A \times B \cong B \times A$ *(but not equal);*

(b) $A \times (B \times C) \cong (A \times B) \times C$ *(but not equal);*

(c) $A \times 0 = 0$*;*

(d) $A \times 1 \cong A$ *(but not equal).*

Proof

(a) Since $A \times B$ is the product of A and B, there are functions $\pi_A : A \times B \to A$ and $\pi_B : A \times B \to B$. Similarly, since $B \times A$ is the product of B and A, there are functions $\pi'_B : B \times A \to B$ and $\pi'_A : B \times A \to A$.

Now, $A \times B$ has a function to B and a function to A, so, by definition of product, there's a unique function $\phi : A \times B \to B \times A$ such that $\pi_A = \pi'_A \circ \phi$ and $\pi_B = \pi'_B \circ \phi$. Analogously, since $B \times A$ has functions to A and B, there's a unique function $\psi : B \times A \to A \times B$ such that $\pi'_A = \pi_A \circ \psi$ and $\pi'_B = \pi_B \circ \psi$.

As done previously, we can consider the functions $\mathrm{id}_{A \times B}$ and $\psi \circ \phi$, both from $A \times B$ to itself. Notice that $\pi_A = \pi_A \circ \mathrm{id}_{A \times B}$ and $\pi_B = \pi_B \circ \mathrm{id}_{A \times B}$. Notice also that

$$\pi_A = \pi'_A \circ \phi = (\pi_A \circ \psi) \circ \phi = \pi_A \circ (\psi \circ \phi)$$

and

$$\pi_B = \pi'_B \circ \phi = (\pi_B \circ \psi) \circ \phi = \pi_B \circ (\psi \circ \phi),$$

so both $\mathrm{id}_{A \times B}$ and $\psi \circ \phi$ commute the diagram

$$\begin{tikzcd}
 & A \times B \arrow[d, shift right, "\psi\circ\phi"'] \arrow[d, shift left, "\mathrm{id}_{A\times B}"] \arrow[ddl, bend right, "\pi_A"'] \arrow[ddr, bend left, "\pi_B"] & \\
 & A \times B \arrow[dl, "\pi_A"] \arrow[dr, "\pi_B"'] & \\
A & & B.
\end{tikzcd}$$

But by definition of product, there's a unique function from any set (including $A \times B$ itself) to $A \times B$ for which that holds. Hence, these two functions must be the same - that is, $\psi \circ \phi = \mathrm{id}_{A\times B}$.

Arguing analogously, we can prove that $\mathrm{id}_{B\times A}$ and $\phi \circ \psi$ are two functions from $B \times A$ to itself which commute the corresponding diagram and, once again, by definition of product, they must be the same - that is, $\phi \circ \psi = \mathrm{id}_{B\times A}$.

Hence, ϕ and ψ are inverses and, therefore, isomorphisms.

(b) We'll show that both $A \times (B \times C)$ and $(A \times B) \times C$ are isomorphic to $A \times B \times C$, so they must be isomorphic (since composition of isomorphisms is isomorphism).

Actually, we'll only show one of these and leave the other one as an exercise to you, reader.

Let

$$\begin{tikzcd}
 & A \times (B \times C) \arrow[dl, "\pi_A"'] \arrow[dr, "\pi_{B,C}"] & & \\
 & & B \times C \arrow[dl, "\pi_B"] \arrow[dr, "\pi_C"'] & \\
A & B & & C
\end{tikzcd}$$

be the functions from $A \times (B \times C)$ to each one of A, B and C (which exist by definition of all the products involved).

Similarly, let

$$\begin{tikzcd}
 & A \times B \times C \arrow[dl, "\pi'_A"'] \arrow[d, "\pi'_B"] \arrow[dr, "\pi'_C"] & \\
A & B & C
\end{tikzcd}$$

be the functions from $A \times B \times C$ to each one of A, B and C (which exist by definition of product).

Now, by definition of $A \times B \times C$, there's a unique $\phi : A \times (B \times C) \to A \times B \times C$ such that $\pi_A = \pi'_A \circ \phi$, $\pi_B \circ \pi_{B,C} = \pi'_B \circ \phi$ and $\pi_C \circ \pi_{B,C} = \pi'_C \circ \phi$.

But, by definition of $B \times C$, there's a unique $\psi_{B,C} : A \times B \times C \to B \times C$ such that $\pi'_B = \pi_B \circ \psi_{B,C}$ and $\pi'_C = \pi_C \circ \psi_{B,C}$.

Finally, by definition of $A \times (B \times C)$, the above $\psi_{B,C}$ together with π'_A show that there's a unique $\psi : A \times B \times C \to A \times (B \times C)$ such that $\pi'_A = \pi_A \circ \psi$ and $\psi_{B,C} = \pi_{B,C} \circ \psi$.

Now, it's easy to see that using all of the equations above we get that

$$\begin{aligned}
\pi'_A \circ (\phi \circ \psi) &= (\pi'_A \circ \phi) \circ \psi \\
&= \pi_A \circ \psi = \pi'_A
\end{aligned}$$

$$
\begin{aligned}
\pi'_B \circ (\phi \circ \psi) &= (\pi'_B \circ \phi) \circ \psi \\
&= (\pi_B \circ \pi_{B,C}) \circ \psi \\
&= \pi_B \circ (\pi_{B,C} \circ \psi) = \pi_B \circ \psi_{B,C} = \pi'_B
\end{aligned}
$$

$$
\begin{aligned}
\pi'_C \circ (\phi \circ \psi) &= (\pi'_C \circ \phi) \circ \psi \\
&= (\pi_C \circ \pi_{B,C}) \circ \psi \\
&= \pi_C \circ (\pi_{B,C} \circ \psi) = \pi_C \circ \psi_{B,C} = \pi'_C
\end{aligned}
$$

and, like before, this shows that $\phi \circ \psi = \mathrm{id}_{A\times B\times C}$ - since $\mathrm{id}_{A\times B\times C}$ is the unique function satisfying those three equalities.

Similarly:

$$
\begin{aligned}
\pi_A \circ (\psi \circ \phi) &= (\pi_A \circ \psi) \circ \phi \\
&= \pi'_A \circ \phi = \pi_A
\end{aligned}
$$

$$
\begin{aligned}
(\pi_B \circ \pi_{B,C}) \circ (\psi \circ \phi) &= \pi_B \circ (\pi_{B,C} \circ (\psi \circ \phi)) \\
&= \pi_B \circ ((\pi_{B,C} \circ \psi) \circ \phi) \\
&= \pi_B \circ (\psi_{B,C} \circ \phi) \\
&= (\pi_B \circ \psi_{B,C}) \circ \phi \\
&= \pi'_B \circ \phi = \pi_B \circ \pi_{B,C}
\end{aligned}
$$

$$
\begin{aligned}
(\pi_C \circ \pi_{B,C}) \circ (\psi \circ \phi) &= \pi_C \circ (\pi_{B,C} \circ (\psi \circ \phi)) \\
&= \pi_C \circ ((\pi_{B,C} \circ \psi) \circ \phi) \\
&= \pi_C \circ (\psi_{B,C} \circ \phi) \\
&= (\pi_C \circ \psi_{B,C}) \circ \phi \\
&= \pi'_C \circ \phi = \pi_C \circ \pi_{B,C}
\end{aligned}
$$

and now the last two equalities show that since $\pi_{B,C}$ and $\pi_{B,C} \circ \psi \circ \phi$ are two maps from $A \times (B \times C)$ to $B \times C$ commuting the diagram

$$
\begin{tikzcd}
 & A \times (B \times C) \arrow[d, shift right, "\pi_{B,C}\circ\psi\circ\psi"'] \arrow[d, shift left, "\pi_{B,C}"] \arrow[ddl, bend right, "\pi_B\circ\pi_{B,C}"'] \arrow[ddr, bend left, "\pi_C\circ\pi_{B,C}"] & \\
 & B \times C \arrow[dl, "\pi_B"] \arrow[dr, "\pi_C"'] & \\
B & & C
\end{tikzcd}
$$

and since, by definition of product, that map must be unique, it follows that $\pi_{B,C} = \pi_{B,C} \circ \psi \circ \phi$.

But this, on the other hand, shows that both $\mathrm{id}_{A\times(B\times C)}$ and $\psi\circ\psi$ commute the diagram

$$\begin{tikzcd}
 & A\times(B\times C) \arrow[dl, bend right, "\pi_A"'] \arrow[d, shift right, "\psi\circ\psi"'] \arrow[d, shift left, "\mathrm{id}_{A\times(B\times C)}"] \arrow[dr, bend left, "\pi_{B,C}"] & \\
 & A\times(B\times C) \arrow[dl, "\pi_A"] \arrow[dr, "\pi_{B,C}"'] & \\
A & & B\times C
\end{tikzcd}$$

which, once again, implies that $\psi\circ\phi = \mathrm{id}_{A\times(B\times C)}$, by definition of product.

This shows that ψ and ϕ are mutually inverse and, therefore, isomorphisms.

(c) This is equivalent to proving that if there is a function between some set Z and 0, then $Z = 0$.

To see this, consider such a function $f : Z \to 0$. If $Z \neq 0$, then there's at least one point $z \in Z$ - and, therefore, $f(z) \in \mathrm{Im}(f) \subseteq 0$. But 0 is empty, so it has no elements, but we've just showed that if $Z \neq 0$, then $f(z) \in 0$, which is a contradiction. It follows that $Z \neq 0$ is false, and, so, $Z = 0$.

Now, we're going to prove that 0 is the product of A and 0 using the definition:

First, see that since 0 is initial, there's a unique function $!_A : 0 \to A$ and a unique function $!_0 : 0 \to 0$, but since id_0 always exists, we must have $!_0 = \mathrm{id}_0$.

Now let B be a set with functions $f : B \to A$ and $g : B \to 0$. Then $B = 0$ (since g is a function to 0). It follows, then, that $f =!_A$ and $g =!_0$. Clearly, then, the function $!_0 : 0 \to 0$ commutes the diagram

$$\begin{tikzcd}
 & 0 \arrow[dl, bend right, "!_A"'] \arrow[d, "!_0"] \arrow[dr, bend left, "!_0"] & \\
 & 0 \arrow[dl, "!_A"] \arrow[dr, "!_0"'] & \\
A & & 0
\end{tikzcd}$$

for $!_A$ and $!_A\circ!_0$ are two functions from 0 to A, so they must be equal (since 0 is initial), and similarly for $!_0\circ!_0$ and $!_0$.

We have just proven that 0 satisfies the universal property defining $A \times 0$, so we must have $0 \cong A \times 0$, but the only set isomorphic to 0 is 0, so we get $0 = A \times 0$.

(d) Similarly, to prove this result we'll use that A satisfies the definition of product of A and 1:

First, notice that there's a function $\mathrm{id}_A : A \to A$ and a unique function $!^A : A \to 1$ (since 1 is terminal).

Now, suppose B is a set with functions $f : B \to A$ and $g : B \to 1$. Since 1 is terminal, $g :=!^B$ the unique function from B to 1.

It is now easy to see that $f : B \to A$ commutes the diagram

$$\begin{tikzcd} & B \arrow[dl, bend right, "f"'] \arrow[d, "f"] \arrow[dr, bend left, "!^B"] & \\ & A \arrow[dl, "\mathrm{id}_A"] \arrow[dr, "!^A"'] & \\ A & & 1 \end{tikzcd}$$

for $f = \mathrm{id}_A \circ f$, trivially, and $!^B$ and $!^A \circ f$ are two functions from B to 1, so they must be equal (since 1 is terminal).

We've just shown that A satisfies the universal property which defines $A \times 1$, so, since universal properties define sets uniquely up to isomorphism, we get $A \cong A \times 1$.

□

Remark 1.3.4.9

From here onwards, whenever we multiply a set by itself, we'll take inspiration on numbers and denote the product of n copies of any set A by A^n. Note that this makes sense because of the item (b) above.

If you think about it, there's no immediate reason why these four statements should be true. Yet, the fact that they are true makes it way more reasonable for our naming it the "product" of two sets: Because it looks just like number multiplication.

1.3.5 Adding sets?

Well, now that we have multiplication, you know what to do next, right?

Definition 1.3.5.1. *Let X and Y be two sets. We define the **coproduct of** X **and** Y to be the set $X \coprod Y$ which is initial in the class of sets with functions from both X and Y - this means that:*

i. There are functions $\iota_X : X \to X \coprod Y$ and $\iota_Y : Y \to X \coprod Y$;

ii. If Z is some set with functions $i_X : X \to Z$ and $i_Y : Y \to Z$, then there is a unique function $i : X \coprod Y \to Z$ such that $i_X = i \circ \iota_X$ and $i_Y = i \circ \iota_Y$.

We usually denote this saying that the following diagram commutes:

$$\begin{tikzcd}
X \arrow[dr, "\iota_X"] \arrow[ddr, bend right, "i_Z"'] & & Y \arrow[dl, "\iota_Y"'] \arrow[ddl, bend left, "i_Y"] \\
& X \coprod Y \arrow[d, dashed, "\exists! i"] & \\
& Z &
\end{tikzcd}$$

Once again, this all sounds too abstract. What's this so called "coproduct"? Well, it might not seem obvious at first...

Definition 1.3.5.2. *Let A and B be two sets. We define the **disjoin union** of A and B to be the set $A \sqcup B$ of all elements in either A or B, but disregarding equalities.*

This is till too abstract, so lets give an example:

Example(s)

Consider the sets $A = \{a, b\}$ and $B = \{1, 2, 3\}$. Now, since $A \cap B = \varnothing$, we see that the set $A \cup B$ is just taking all elements of A and B, and putting them all in the same box: $A \cup B = \{a, b, 1, 2, 3\}$.
If, however, we take the sets $C = \{a, b, c, d, e\}$ and $D = \{a, e, i, o, u\}$, we see that $C \cup D = \{a, b, c, d, e, i, o, u\}$ which is **not** the same as just taking every element in C and D and putting them all in the same box. That happens because, contrary to the first case where $A \cap B = \varnothing$, in this case we have $C \cap D = \{a, e\} \neq \varnothing$.
In other words, there is at least one $x \in C$ and one $y \in D$ such that $x = y$.
We can, however, fix that problem by "coloring" the elements.

Imagine that C was a large blue paint can, and D was a giant red paint can. Now, putting the elements from C and D together, we can see that the a and the e that came from C are blue, whereas the corresponding elements from D are red.
This is the idea behind disjoint unions:
C, as a set, is clearly isomorphic to the set $C_C := \{a_C, b_C, c_C, d_C, e_C\}$, which has "the same elements, but painted in the color C". Similarly, the set D is clearly isomorphic to the set

$D_D := \{a_D, e_D, i_D, o_D, u_D\}$, which has "the same elements, but painted in the color D".
Now, instead of computing $C \cup D$, we compute

$$C_C \cup D_D = \{a_C, b_C, c_C, d_C, e_C, a_D, e_D, i_D, o_D, u_D\},$$

which is precisely what we would get by taking all elements of C and D and putting them in a box, disregarding equalities.
So we put $C \sqcup D := C_C \cup D_D$, and call it the **disjoint union of C and D**.

This final argument in the example suggests the following result:

Lemma 1.3.5.3. *For any two sets X and Y we have that $X \sqcup Y \cong (X \times \{0\}) \cup (Y \times \{1\})$.*

Proof

It follows directly from the example above and from the fact that we can denote any element in $X \times \{0\}$ (which is of the form $(x, 0)$, by definition) as x_0, just as a shorthand notation (and similarly for $Y \times \{1\}$), so we can just write $X_0 := X \times \{0\}$ and $Y_1 := Y \times \{1\}$..

Define $f : X \sqcup Y \to X_0 \cup Y_1$ by putting

$$f(a) := \begin{cases} a_0, & \text{if } a \in X \\ a_1, & \text{if } a \in Y. \end{cases}$$

- **f is injective:**

  Take $a, b \in X \sqcup Y$ such that $f(a) = f(b)$. We have four different possibilities:

  1. If $a \in X$ and $b \in X$, we see that $a_0 = f(a) = f(b) = b_0$ and hence $a = b$.
  2. If $a \in X$ and $b \in Y$, we see that $a_0 = f(a) = f(b) = b_1$, which is absurd because the second coordinate of b_1 is 1, and the second coordinate of a_X is 0, and $0 \neq 1$, so $b_1 \neq a_0$. So this case cannot happen.
  3. Similarly, if $a \in Y$ and $b \in X$ we'd get that same contradiction, so this case also cannot happen.
  4. Finally, if $a \in Y$ and $b \in Y$, just like the first case we can see that $a_1 = b_1$, and hence $a = b$.

  Since in all cases, the only possible situation which doesn't lead to a contradiction is $a = b$, we see that f is injective.

- **f is surjective:**

  Take $c \in X_0 \cup Y_1$. We want to show that there's some $a \in X \sqcup Y$ such that $f(a) = c$.

  Since $X_0 \cap Y_1 = \varnothing$, c must lie in either X_0 or Y_1 - that is, either $c = x_0$ for some $a \in X$ or $c = y_1$ for some $y \in Y$. But this means that c is either $f(x)$, for some $x \in X$ or $f(y)$, for some $y \in Y$.

No matter which one of these hold, there's always one $a \in X \sqcup Y$ such that $f(a) = c$, for any $c \in X_0 \cup Y_1$. This proves that f is surjective.

Since f is both injective and surjective, it is a bijection and, therefore, an isomorphism. This ends the proof. $\square$

Now, an important question at this point is *WHY?*. I mean, why do we need this new notion of union, when the old one suited us just fine? Well, let me present you some results to convince you on that:

Proposition 1.3.5.4. *For any two sets X and Y, their disjoint union $X \sqcup Y$ is the coproduct $X \coprod Y$.*

Proof

We have to show two things:

(i.) There are functions $\iota_X : X \to X \sqcup Y$ and $\iota_Y : Y \to X \sqcup Y$.

This can easily be seen by considering the lemma 1.3.5.3, and so we can put $\iota_X(x) := x_0$ and $\iota_Y(y) := y_1$ for any $x \in X$ and any $y \in Y$.

(ii.) Let Z be any set with functions $i_X : X \to Z$ and $i_Y : Y \to Z$. We want to show that there's a unique function $i : X \sqcup Y \to Z$ such that $i_X = i \circ \iota_X$ and $i_Y = i \circ \iota_Y$.

This is easy: Define $i : X \sqcup Y \to Z$ by putting

$$i(a) := \begin{cases} i_X(x), & \text{if } a = x_0 \\ i_Y(y), & \text{if } a = y_1. \end{cases}$$

Clearly then we have:

$$(i \circ \iota_X)(x) = i(x_0) = i_X(x)$$

and

$$(i \circ \iota_Y)(y) = i(y_1) = i_Y(y),$$

so our i satisfies the equalities.

Now to prove that it is unique: Suppose there's some $j : X \sqcup Y \to Z$ that also satisfies the equalities. In particular, we have that $(j \circ \iota_X)(x) = (i \circ \iota_X)(x)$ and $(j \circ \iota_Y)(y) = (i \circ \iota_Y)(y)$.

But the RHS of the first equation evaluates to $i(x_0)$, by definition, and the RHS of the second equation evaluates to $i(y_1)$, also by definition.

But, on the other hand, the LHS evaluates to $j(x_0)$ and $j(y_1)$, respectively, again by definition.

Finally, since every element of $X \sqcup Y$ is either in X_0 or in Y_1, it follows that the functions j and i are equal for all elements of X_0 and Y_1 - and, therefore, equal for all of $X \sqcup Y$ - which implies, by definition of equality, $j = i$. This shows that there's a unique function satisfying the equalities

Finally, (i.) and (ii.) together show that $X \sqcup Y$ satisfies the universal property defining the coproduct of X and Y. This finishes the proof. □

Just like with products, we can use coproducts to generalize disjoint unions to infinitely many sets:

Definition 1.3.5.5. *Let $\{A_i\}_{i\in I}$ be a collection of sets indexed by another set I (which can be infinite or finite, countable or uncountable, doesn't matter, as long as it's a set). We define $\coprod_{i\in I} A_i$ to be the set given by:*

i. There is a function $\iota_n : A_n \to \coprod_{i\in I} A_i$ for each $n \in I$;

ii. If Z is a set with a function $i_n : A_n \to Z$ for each $n \in I$, then there's a unique function $i : \coprod_{i\in I} A_i \to Z$ such that $i_n = i \circ \iota_n$ for each $n \in I$.

And we can also get a similar concept to the diagonal map:

Definition 1.3.5.6. *Given three sets A, B and C with functions $f : A \to C$ and $g : B \to C$, the unique function from $A \sqcup B$ to C induced by the definition of coproduct will be called the* ***coproduct map of f and g*** *and denoted by $f \sqcup g : A \sqcup B \to C$.*

By definition, $(f \sqcup g)(x) := \begin{cases} f(x), & \text{if } x \in A \\ g(x), & \text{if } x \in B. \end{cases}$

Example(s)

Let $\mathbb{R}$ be the set of real numbers, $f, g : \mathbb{R} \to \mathbb{R}$ be defined by $f := \mathrm{id}_{\mathbb{R}}$ and $g(x) := x^2$ for any $x \in \mathbb{R}$. Then the coproduct map $f \sqcup g : \mathbb{R} \sqcup \mathbb{R} \to \mathbb{R}$ is the map $x \mapsto \begin{cases} x, & \text{if } x \in \mathbb{R}_0 \\ x^2, & \text{if } x \in \mathbb{R}_1 \end{cases}$ for any $x \in \mathbb{R} \sqcup \mathbb{R}$.

Definition 1.3.5.7. *The coproduct map of id_X and id_X, for any set X will be called the* ***fold map of X*** *and denoted by $\nabla_X : X \sqcup X \to X$.*

It is, as in the above definition, the unique map commuting the diagram

$$\begin{tikzcd}
X \arrow[dr, "\iota_0"] \arrow[ddr, bend right, "\mathrm{id}_X"'] & & X \arrow[dl, "\iota_1"'] \arrow[ddl, bend left, "\mathrm{id}_X"] \\
& X \sqcup X \arrow[d, "\exists!\nabla_X"] & \\
& X &
\end{tikzcd}$$

Example(s)

Let $A = \{a, b, c\}$. Let's calculate ∇_A.
By definition, we must have $\mathrm{id}_A = \nabla_A \circ \iota_0$ and $\mathrm{id}_A = \nabla_A \circ \iota_1$. So take any $a \in A$.
We know that, from the first equation, we must have $a = (\nabla_A \circ \iota_0)(a) = \nabla_A(\iota_0(a)) = \nabla_A(a_0)$.
Similarly, the second equation gives us $a = (\nabla_A \circ \iota_1)(a) = \nabla_A(\iota_1(a)) = \nabla_A(a_1)$.
So ∇_A is the function that ignores color. It's basically the colorblind function - in its eyes, x_0 and x_1 are just x.
It is, in some sense, folding x_0 and x_1 on top of eachother - gluing them together. Hence why it's called the *fold* map.

Now, finally, we'll state similar results to the ones in the product section:

Lemma 1.3.5.8. *For any three sets A, B and C the following hold:*

(a) $A \sqcup B \cong B \sqcup A$ *(but not equal);*

(b) $A \sqcup (B \sqcup C) \cong (A \sqcup B) \sqcup C$ *(but not equal);*

(c) $A \sqcup 0 \cong A$ *(but not equal).*

Proof

(a) It is basically the same proof as in the case of products, so we'll leave it to the reader.

(b) This follows from the fact that union is associative, from $X \sqcup Y \cong X_0 \cup Y_1$ and from the fact that all sigletons are isomorphic.

Specifically, write $A \sqcup (B \sqcup C)$ as $A_0 \cup (B \sqcup C)_1$, and writing $B \sqcup C \cong B_0 \cup C_1$, we can further rewrite $A \sqcup (B \sqcup C)$ as $A_0 \cup B_{0,1} \cup C_{1,1}$ - which, upon closer inspection, is just $A_0 \cup B_1 \cup C_2$.

Similarly, we can write $(A \sqcup B) \sqcup C$ as $(A \sqcup B)_0 \cup C_1$, and writing $A \sqcup B \cong A_0 \cup B_1$, we can further rewrite $(A \sqcup B) \sqcup C$ as $A_{0,0} \cup B_{1,0} \cup C_1$ - which, upon closer inspection, is just $A_0 \cup B_1 \cup C_2$.

The result now follows trivially.

(c) This is proven by showing that A satisfies the universal property defining $A \sqcup 0$ - and is, therefore, isomorphic to it.

First, notice that there are functions $\mathrm{id}_A : A \to A$ and $!_A : 0 \to A$.

Now, let B be a set with functions $f : A \to B$ and $g : 0 \to B$. Since 0 is initial, $g = !_B$ the unique function from 0 to B. So it's easy to see that $f : A \to B$ makes it so that the following diagram commutes

$$\begin{tikzcd}
A \arrow[dr, "\mathrm{id}_A"] \arrow[ddr, bend right, "f"'] & & 0 \arrow[dl, "!_A"'] \arrow[ddl, bend left, "!_B"] \\
& A \arrow[d, "f"] & \\
& B &
\end{tikzcd}$$

so A satisfies the universal property defining $A \sqcup 0$ and is, therefore, isomorphic to it, just as stated.

An alternative proof could be given:

Since $A \sqcup 0 \cong A_0 \cup 0_1$, we can use lemma 1.3.4.8(c) to see that 0_1, which is just fancy notation for $0 \times \{1\}$, is just 0 (since it is 0 times a set). So $A \sqcup 0 \cong A_0 \cup 0$, and we can now use proposition 1.2.2.13(3) and see that $A_0 \cup 0 = A_0$, which is clearly isomorphic to A. This shows that $A \sqcup 0 \cong A$, as stated.

This proves the result. $\square$

If you think about it, there's no immediate reason why these three statements should be true. Yet, the fact that they are true makes it way more reasonable for our naming it the "coproduct" of two sets: Because it looks just like number addition.

The next subsection will be all about that: How to deal with sets as numbers, and numbers as sets.

1.3.6 Everything is a set!

The motivation for this section couldn't be simpler and more direct: We want to give a proper, formal definition of *numbers*.

The reasoning for this is simple: What is a number? What is the number 2, for instance, and why does it not equal, say, 4?

Through the history of mathematics, this has been tried to solve in many ways. For instance, Bertrand Russell (the same one from Russell's Paradox) proposed that the number 2, for instance, should be defined as being the collection of all collections with two elements. Of course, the way I put it here isn't very proper, or formal, but the general ideal is there: You take all collections in the universe, and group them together into mini-collections following a simple rule: Two collections belong in the same mini-collection if, and only if, they have the same amount of elements. And then you say that a *number* is each one of those mini-collections.

Now, we can agree or disagree that this is a good definition, but it sure as hell is a very interesting definition, at least. Think about it - if you go to any dictionary, it'll say that a number is a descriptive of quantity, and a quantity is the number of elements - which is a circular definition. Russell managed to sidestep that problem using the clever idea of grouping all collections with the same amount of elements together.

But then, we can ask: How can you count elements in a set without using numbers? Or, maybe a simpler problem: How to know if two sets have the same amount of elements without using numbers?

What Russell proposed as a solution to that problem is precisely what we're going to use: Bijections.

For Russell, two sets would be said to have the same amount of elements if you could make pairings of elements on both sets such that every element on the first set had a unique match on the second set, and that there was no elements left on either set after this process.

This idea is so simple, yet so brilliant, that even though it's not what we usually think of as numbers today, as mathematicians, it's still a very rich idea on the concept of numbers - so much so that it has been used as an alternative to the classic teaching method for introducing the concept of numbers to small children.

What we're going to do, however, is a tad different. We're going to use the so called **Peano's Axioms**, which is a list of axioms (which will be three in this text) that is widely accepted in mathematics as being the "best formalization of the set of natural numbers".

One of the reasons, and I could argue the *best* reason, why it is considered as such, comes from the fact that it is *categorical*, that is, it admits a unique model (up to isomorphisms, of course).

Basically, what that means is: Suppose I give you a list of axioms. What guarantee is there that there is something that is able to satisfy all those axioms at the same time? For instance, the list

- All of its elements are sets;
- Every set is in there;
- There are no sets in there.

admits no *model* - that is, there's nothing in the universe that satisfies all these three properties at the same time (you can actually take any two of these and it would work, but with all three at once, it's impossible).

Hence the name model - it's a way of *modelling* your list of conditions - taking it from something abstract and *modelling* it as something concrete.

Now, it's a known fact in mathematical logic that Peano's Axioms (which we're going to present) do admit a model (which we're going to construct), and that it is the *only* model (up to set isomorphism) for those axioms.

Without further ado, then, here we go.

Definition 1.3.6.1 (Peano's Axioms)**.** *Let N be a set satisfying*

(PA1) *There is a point $0 \in N$ called* zero*.*

(PA2) *There is an injective function $s : N \to N$ called* successor *such that $0 \notin \mathrm{Im}(s)$;*

(PA3) *If $X \subseteq N$ is a set containing 0 such that for every $x \in X$ we have that $s(x) \in X$, then $X = N$.*

Then N is called the ***set of natural numbers****.*

Now, there is no way, at first glance, to tell if these axioms do, or do not, induce a paradox.

The best way to do that is to produce a model for it - for if a list of axioms can be modelled, then it is consistent (i.e., it has no paradoxes).

So, we're going to do just that: Produce a model for it.

Definition 1.3.6.2 (Zero)**.** *We'll call the set $\varnothing$ the* ***zero set*** *and denote it as 0.*

Definition 1.3.6.3 (Successor)**.** *For any set X we define it's* ***successor*** *to be the set $s(X) := X \cup \{X\}$.*

Now, let's see what is this successor all about.

Example(s)

Let $A = \{a, b\}$. What is $s(A)$? Well, by definition, $s(A) = A \cup \{A\} = \{a, b, \{a, b\}\}$.
Similarly, if $B = \{1, 2, 3, 4\}$, then $s(B) = \{1, 2, 3, 4, \{1, 2, 3, 4\}\}$.
Notice that in both of these cases, the successor of a set has exactly one more element than the set itself - just like in the naturals, the successor of n is precisely $n + 1$.

What is then $s(0)$? Well, once again, by definition, $s(0) = 0 \cup \{0\}$, but we know that $0 \cup A = A$ for any set A! So $s(0) = \{0\}$ - a singleton!
Let's call $1 := s(0) = \{0\}$.
Now we can ask what is $s(1)$, and it will be $1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$.
Let's call $2 := s(1) = \{0, 1\}$...
You can see where we're going with this, right?

Definition 1.3.6.4. *Let S denote any set containing 0 and closed under taking successors (that is, $x \in S$ implies $s(x) \in S$). We define $\mathbb{N}$ to be the set given by*

$$\mathbb{N} := \bigcap_{N \in \mathcal{N}} N$$

where $\mathcal{N} := \{X \in \mathcal{P}(S) \mid x \in X \implies s(x) \in X\}$.

In some sense, $\mathbb{N}$, as defined above, is "the smallest set containing zero and all its successors". We can finally model Peano's Axioms:

Theorem 1.3.6.5. *The set $\mathbb{N}$ satisfies all of (PA1), (PA2) and (PA3).*

Proof

By definition, $\mathbb{N}$ satisfies (PA1) and (PA2).
To prove (PA3), first notice that if we take $X \subseteq \mathbb{N}$ containing 0 and closed by successors, then, by definition of $\mathbb{N}$, we see that $\mathbb{N} \subseteq X$ (since $\mathbb{N}$ is the smallest set with those properties). Since we have both $X \subseteq \mathbb{N}$ and $\mathbb{N} \subseteq X$, we can conclude that $X = \mathbb{N}$, and so (PA3) holds. This shows that $\mathbb{N}$ is a model for Peano's Axioms, as we wanted. $\square$

With this, we see that Peano's Axioms are consistent (i.e., don't derive any logical contradictions) and, therefore, we can work with them.

So, from now on, every natural number n should be thought of as the set $\{0, 1, 2, 3, \cdots, n-1\}$.

Since, however, our main goal here is to get to Linear Algebra, we're not going to spend time defining the addition, subtraction, multiplication and division operations on $\mathbb{N}$, and we're going to assume that the reader is sufficiently familiar with them.

We're also not going to construct the integers, rationals or real numbers, not because it would be unfeasible, but because it doesn't suit the text.

Now that we have numbers, we can finally begin our study on cardinality, which will be central to our studies when we eventually get to linear algebra.

Definition 1.3.6.6. *Let X be a set. We say that X is* ***finite*** *if there is some $n \in \mathbb{N}$ such that $X \cong n$. In this case, we say that X* ***has n elements****, and denote it with the symbol $\#X = n$.*

Example(s)

Consider $A = \{a, b\}$. Then A is finite, because $A \cong 2$. To see that, consider the function $f : A \to 2$ taking $a \mapsto 0$ and $b \mapsto 1$. It clearly is bijective, by definition, so it is an isomorphism.

Conversely, the set $\mathbb{N}$ isn't finite. To see that, suppose it was - that is, there is some $n \in \mathbb{N}$ such that $n \cong \mathbb{N}$. This would imply that n satisfies Peano's Axioms - in particular, n would be closed by successors.
But $n = \{0, 1, 2, 3, \cdots, n-1\}$, and, clearly, for all $x \in n$, aside from $x = n - 1$, we see that

$s(x) \in n$. But if $n \cong \mathbb{N}$, we would have to have that $s(n-1) \in n$. But $s(n-1) = n$. So we would be saying that $n \in n$, which, by our previous discussion on Russell's Paradox, **cannot** happen.
Therefore, if $\mathbb{N} \cong n$, for some $n \in \mathbb{N}$, we would get a paradox akin to Russell's Paradox. Since we don't want that, we can't have $\mathbb{N} \cong n$, no matter which $n \in \mathbb{N}$ we choose.
It follows that $\mathbb{N}$ is not finite.

Proposition 1.3.6.7. *For all $n \in \mathbb{N}$, if $f : n \to n$ is injective, then it is automatically surjective.*

Proof

If $n = 0$, it is true (since the only function between 0 and 0 is the identity, which is a bijection).
Suppose it is true for some $n \in \mathbb{N}$. We will prove that it holds true also for $n+1$.
Let $f : n+1 \to n+1$ be an injective function, and consider $f^{-1}(n)$.

- If there is no $x \in n$ such that $f(x) = n$, we can define $f' : n \to n$ by putting $f'(x) := f(x)$ and see that f' is injective:

  If $f'(x) = f'(y)$ for some $x, y \in n$, then, by definition, $f(x) = f'(x) = f'(y) = f(y)$ and therefore $f(x) = f(y)$, but since f is injective, we have that this implies $x = y$.

  Now, we have that $f' : n \to n$ is injective and, therefore, by our assumption that the result holds for any injection from n to n, we see that f' is surjective.

  Now we ask: Can $f(n)$ be in n? Well, if it was, there'd be some $m \in n$ such that $f'(m) = f(n)$, since f' is injective. But $f'(m) = f(m)$, by definition of f'. So we would have $f(m) = f'(m) = f(n)$ which would imply, since f is injective by hypothesis, that $m = n$ - which is absurd, because $m \in n$ and we've shown many times before that $X \notin X$ for any set X.

  This means that $f(n) \notin n$ and, therefore, $f(n)$ must be the only element left in $n+1$ - that is n, from which it follows that f is surjective.

- If, however, there is some $x \in n$ such that $f(x) = n$, then we know that this x is unique since f is injective. Let's call this element k, so $f(k) = n$. This allows us, then, to define a new function $g : n+1 \to n+1$ as such: $g(k) := f(n)$, $g(n) := f(k)$, $g(m) := f(m)$ for all $m \in n$.

  Now g is an injection for which there's no $x \in n$ such that $g(x) = n$ (by construction). But now g is just as in the previous case, so it must be surjective. But then, f must also be surjective, since they have the same images.

So we've shown that the set of all n such that the proposition holds is a subset of $\mathbb{N}$ which contains 0 and is closed under taking successors. It follows from (PA3) that this set is the whole $\mathbb{N}$, so the proposition follows. $\square$

Proposition 1.3.6.8. *For all $n \in \mathbb{N}$, if $f : n \to n$ is surjective, then it is automatically injective.*

Proof

If $f : n \to n$ is surjective, it has a right-inverse $g : n \to n$ such that $\mathrm{id}_n = f \circ g$.
Since id_n is an isomorphism, we see that g is injective. But now, the preceding proposition tells us that g is also an isomorphism.
Finally, lemma 1.3.2.20(f) tells us that since $\mathrm{id}_n = f \circ g$ and both id_n and g are iso, we have that f is also iso - and hence, injective.
This finishes the proof. $\square$

Corollary 1.3.6.9. *For any $f : X \to X$ with X finite, the following are equivalent:*

1. *f is injective;*

2. *f is surjective;*

3. *f is bijective.*

Corollary 1.3.6.10. *For all $n, m \in \mathbb{N}$, we have that $n \in m$ if, and only if, there's an injection $f : n \to m$ which is not a surjection.*

Proof

If $n \in m$, the function $i_n : n \to m$ defined by $i_n(x) := x$ for all $x \in n$ is clearly injective (by definition), but it is not surjective: $n \in m$, but $n \notin \mathrm{Im}(f)$.

Conversely, assume that $n \notin m$. Then either $m \in n$ or $n = m$ (by definition of $\mathbb{N}$).

- If $m \in n$, then, by the first case, we see that there's an injection $g : m \to n$ that is not surjective.

  Now, if there was an injection $f : n \to m$, then their composite $g \circ f : n \to n$ would be an injection too and so, by the preceding lemma, $g \circ f$ would be a bijection, which, by lemma 1.3.2.20, implies that g would be a surjection, which is a contradiction.

  This shows that there cannot be such an f.

- If $m = n$, then every injection is surjective, by the preceding proposition.

This finishes the proof. $\square$

Corollary 1.3.6.11. *For all $n, m \in \mathbb{N}$, we have that $n \in m$ if, and only if, there's a surjection $f : m \to n$ which is not an injection.*

Lemma 1.3.6.12. *For any $n \in \mathbb{N}$, we have that $\mathbb{N} \cong \mathbb{N} \setminus \{n\}$.*

Proof

Consider the function:

$$f : \mathbb{N} \to \mathbb{N} \setminus \{n\}$$

$$f(x) := \begin{cases} x, & \text{if } x \in n \\ x+1, & \text{otherwise.} \end{cases}$$

- f is surjective:

  Take any $x \in \mathbb{N} \setminus \{n\}$. If $x \in n$, then clearly $x = f(x)$. If $x \notin n$, then x is the successor of some y, and, clearly, $x = f(y)$.

  Either way, we see that $x \in \mathrm{Im}(f)$, so f is surjective.

- f is injective:

  Take $x, y \in \mathbb{N}$ such that $f(x) = f(y)$.

  If $f(x) \in n$, then, by definition, $x \in n$ and, therefore, $x = f(x) = f(y) = y$.

  If $f(x) \notin n$, then, by definition, $x \notin n$ and, therefore, $x + 1 = f(x) = f(y) = y + 1$ and since s is injective, by (PA2), we have that $s(x) = x + 1 = y + 1 = s(y)$ implies $x = y$.

  These two together show that f is indeed injective.

Since f is injective and surjective, it is bijective, as we wished to show. □

Proposition 1.3.6.13. *A set is finite if, and only if, there's no surjection from it to* $\mathbb{N}$*.*

Proof

Let X be finite. For all intents and purposes we can consider that, up to isomorphism, $X = n$, for some $n \in \mathbb{N}$.

- If $n = 0$, there's clearly no surjection from n to $\mathbb{N}$.

- Assume the result is true for some $n \in \mathbb{N}$ - that is, there's no surjection from n to $\mathbb{N}$. We're gonna prove the result for $n + 1$.

  Let $f : n+1 \to \mathbb{N}$ be a surjection. In that case, we get a surjection $f' : n \to \mathbb{N} \setminus \{f(n)\}$ by putting $f'(x) := f(x)$ for all $x \in n$.

  But the preceding lemma tells us that $\mathbb{N} \cong \mathbb{N} \setminus \{f(n)\}$, so f' is a surjection from n to $\mathbb{N}$ - which is absurd, by hypothesis.

  It follows then that f cannot be a surjection, just as we wished to show.

We have just shown that "the set of all $n \in \mathbb{N}$ for which there's no surjection to $\mathbb{N}$" contains 0 and is closed by successors, so, by (AP3), it must be $\mathbb{N}$ itself.

Conversely, suppose X is not finite, that is, for all $n \in \mathbb{N}$ we have $X \ncong n$.

Now, for each $Y \subseteq X$, choose an element $x_Y \in Y$.
We define $f : \mathbb{N} \to X$ by putting

$$f(n) := \begin{cases} x_X, & \text{if } n = 0; \\ x_{X \setminus \{f(0), f(1), \cdots, f(n-1)\}}, & \text{otherwise.} \end{cases}$$

Clearly, for all n, we have that $X \setminus \{f(0), f(1), \cdots, f(n-1)\} \neq \varnothing$ because, otherwise, X would be finite.
This function is then clearly injective by definition (since, for each $n \in \mathbb{N}$, $f(n)$ is chosen from a set that doesn't contain any of $f(0)$ up to $f(n-1)$). Therefore, it has a left-inverse $g : X \to \mathbb{N}$ such that $\mathrm{id}_{\mathbb{N}} = g \circ f$.
But $\mathrm{id}_{\mathbb{N}}$ is clearly a bijection - and hence a surjection. It follows that g is also a surjection from X to $\mathbb{N}$, just as we wanted.

This ends the proof. $\square$

Corollary 1.3.6.14. *A set is finite if, and only if, there's no injection from* $\mathbb{N}$ *to it.*

Definition 1.3.6.15. *A set is **infinite** if it is not finite.*

Corollary 1.3.6.16. *Every infinite set contains a subset that is isomorphic to* $\mathbb{N}$.

1.3.7 Relations are hard, sometimes they leave you broken up inside

The next sections should be way less technical, so that's a plus.

It would be great to have a way to describe when two sets are related in mathematical terms.

Example(s)

Let $A = \{1, 2\}$ and $B = \{2, 4\}$. Then all elements of B are precisely the double of some element of A. So A and B are related by the following relation: "B contains the doubles of the elements of A".
But if you think about it, there are other relations you could make using those two sets: "B contains one of the elements of A", "B contains the quadruple of an element of A", "B contains some element of A added with 3", "the elements of B are greater than the elements of A".
You can literally make as many relations as you want to.

Definition 1.3.7.1. *Let A and B be sets. We define the* ***set of (binary) relations between*** *A* ***and*** *B to be the set $\mathcal{P}(A \times B)$.*

In other words, a ***(binary) relation between*** *A* ***and*** *B is just a subset of $A \times B$.*

Example(s)

Continuing the example above, we have the following relations, in order:

- $R_1 := \{(1, 2), (2, 4)\} \subseteq A \times B$;
- $R_2 := \{(2, 2)\} \subseteq A \times B$;
- $R_3 := \{(1, 4)\} \subseteq A \times B$;
- $R_4 := \{(1, 4)\} \subseteq A \times B$;
- $R_5 := \{(1, 2), (1, 4), (2, 4)\} \subseteq A \times B$.

And we can see that relations R_3 and R_4 are the same relation, just phrased differently.

Definition 1.3.7.2. *Given a relation $R \subseteq A \times B$, we say that $a \in A$* ***is related to*** *$b \in B$* ***via*** *R if $(a, b) \in R$.*

In symbols, we write that as $a \mathrel{\mathrm{R}} b$.

Example(s)

Still on that example, take for instance R_1. Then we have $1 \mathrel{\mathrm{R}_1} 2$ (this means "2 is the double of 1", or "1 is related to 2 via R_1") and $2 \mathrel{\mathrm{R}_1} 4$.
Similarly, we have $1 \mathrel{\mathrm{R}_5} 2$ (this means "5 is greater than 1", or "1 is related to 5 via R_5"), $1 \mathrel{\mathrm{R}_5} 4$ and $2 \mathrel{\mathrm{R}_5} 4$ on R_5.

Proposition 1.3.7.3. *A function $f : A \to B$ is just a relation $R := \{(a, b) \in A \times B \mid b = f(a)\}$.*

Proposition 1.3.7.4. *A relation $R \subseteq A \times B$ is a function if, and only if, for each $a \in A$ there's a unique $b \in B$ such that $a \, \mathrm{R} \, b$.*

These two propositions follow trivially from the definition of function and relation.

Example(s)

Let $\mathbb{N}$ be the set of natural numbers. Remember that this set has a natural order $\leq$ given by "$n \leq m$ if, and only if, $n \in m$ or $n = m$", which is just the usual order we're used to: $0 \leq 1 \leq 2 \leq 3 \leq 4 \leq \cdots$.
Notice that this order is a *relation* on $\mathbb{N} \times \mathbb{N}$: We can think of the symbol $n \leq m$ as meaning "n is related to m via $\leq$".
In other words, we can think of $\leq$ as being the set

$$\leq \, = \{(0,0), (0,1), (0,2), \cdots, (1,1), (1,2), (1,3), \cdots, (2,2), (2,3), \cdots\}$$

or equivalently, but more specifically, the set

$$\leq \, = \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid n \in m \text{ or } n = m\}.$$

Now this relation is special: You can check that it satisfies three special conditions:

- (Reflexivity) For all $n \in \mathbb{N}$ we have that $n \leq n$;
- (Antisymmetry) If both of $n \leq m$ and $m \leq n$ hold, for some $n, m \in \mathbb{N}$, then $n = m$;
- (Transitivity) If $n \leq m$ and $m \leq l$, for some $n, m, l \in \mathbb{N}$, then $n \leq l$.

Let's check:

- It is clearly reflexive, since, by definition, $n \leq m$ includes the case $n = m$;
- Assume $n \leq m$ and $m \leq n$ both hold at once, for some $n, m \in \mathbb{N}$. Now, we have four cases to consider:

  1. $n \in m$ and $m \in n$.
     This case cannot happen, because we would have injections $f : n \to m$ and $g : m \to n$, whose compositions $f \circ g : m \to m$ and $g \circ f : n \to n$ would be injections from m to itself, and from n to itself, but we've already seen that those are always bijective.
     Hence, we'd get that both g and f are also bijective, which is absurd, because we'd be able to show that $n = m$ while $n \in m$, and we know this cannot be true (a set cannot be an element of itself);
  2. $n \in m$ and $n = m$.
     This case also cannot happen, by what we've just said;

3. $n = m$ and $m \in n$.

   Same as the previous case;

4. $n = m$ and $m = n$.

Since the only case that doesn't let to a contradiction is (4), we have that the only possible way that we can have both of $n \leq m$ and $m \leq n$ at once is if $n = m$. This shows that $\leq$ is antisymmetric.

- If $n \leq m$ and $m \leq l$, for some $n, m, l \in \mathbb{N}$, we have, once again, four cases to consider:

1. $n \in m$ and $m \in l$.

   This is fine, since $m \in l$ implies $m \subseteq l$, by definition. This, coupled with $n \in m$ shows us that $n \in m \subseteq l$ and hence $n \in l$, so $n \leq l$;

2. $n \in m$ and $m = l$.

   Again this is fine, since $n \in m = l$ implies $n \in l$, and hence $n \leq l$;

3. $n = m$ and $m \in l$.

   Once again, fine: $n = m \in l$ implies $n \in l$, and thus $n \leq l$;

4. $n = m$ and $m = l$.

   The simplest one: $n = m = l$, so $n = l$, and thus $n \leq l$

In each of the four cases, the only logical conclusion is $n \leq l$, so we have that $\leq$ is transitive.

Definition 1.3.7.5. *Let A be any set with a relation $R \subseteq A \times A$. We say that R is a* ***partial order*** *if R is reflexive, antisymmetric and transitive.*

Now we will justify the terminology *partial*:

Example(s)

Let X be any set, and consider $\mathcal{P}(X)$ its power set.
We claim that the relation $Y \subseteq Z$ is a partial order on $\mathcal{P}(X)$.

- Clearly, for all $Y \in \mathcal{P}(X)$ we have that $Y \subseteq Y$, since Y is a set, so $\subseteq$ is reflexive;
- Assume that for some $Y, Z \in \mathcal{P}(X)$ we have both $Y \subseteq Z$ and $Z \subseteq Y$. Then, by definition of set equality, $Y = Z$, so $\subseteq$ is antisymmetric;
- Assume that for some $Y, Z, W \in \mathcal{P}(X)$ we have both $Y \subseteq Z$ and $Z \subseteq W$. Then every element of Y is an element of Z (by the first part) and every element of Z is an element of W (by the second part). This implies that every element of Y is an element of W, and, therefore, $Y \subseteq W$, and we see that $\subseteq$ is transitive.

This is all pretty standard.

Consider, then, $X = \{a, b, c\}$. Then $\mathcal{P}(X) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, X\}$.
We ask: is $\{b\}$ related to $\{a, b\}$ via $\subseteq$? It clearly is!
Now, is $\{b\}$ related to $\{a, c\}$ via $\subseteq$? It clearly **isn't**!
So contrary to the order $\leq$ in $\mathbb{N}$, the order $\subseteq$ in $\mathcal{P}(X)$ doesn't allow us to compare any two elements. This is why it's called a *partial* order.

Definition 1.3.7.6. *Let A be a set with a partial order $\leq$. We call the ordered pair $(A, \leq)$ a* ***poset*** *(**p**artially-**o**rdered **set**).*

Sometimes, we consider the order to be implicit and simply say that A is a poset.

Definition 1.3.7.7. *Let $(A, \leq)$ be a poset. We say that $\leq$ is a* ***total order*** *or a* ***linear order*** *if for all $a, b \in A$ we have that either or both of $a \leq b$ and $b \leq a$ hold.*

Lemma 1.3.7.8. *The set $\mathbb{N}$ with the usual order is a totally-ordered set.*

Definition 1.3.7.9. *Let $(A, \leq)$ be a poset and $X \subseteq A$. We define the following symbols:*

- *We say that x* ***is the maximum of*** *X if every other element of X is smaller than x, that is,*
$$\max X := \{x \in X \mid \forall y \in X, y \leq x\};$$
- *We say that x* ***is the minimum of*** *X if x is smaller than every other element of X, that is,*
$$\min X := \{x \in X \mid \forall y \in X, x \leq y\};$$
- *We say that x* ***is a maximal element of*** *X if x is not smaller than any other element of X;*
- *We say that x* ***is a minimal element of*** *X if there is no element of X which is smaller than x.*

Example(s)

Let X be as in the previous example, and consider $\mathcal{P}(X)$ ordered by set inclusion.
Then $\mathcal{P}(X)$ has a maximum: X; and a minimum: $\varnothing$.
Notice that they are also respectively maximal and minimal elements.
Consider however $\mathcal{P}(X) \setminus \varnothing, X$, that is, $\{\{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}\}$.
Does this set have a minimum or a maximum? Well, suppose $\{a\}$ was a minimum. Then it'd have to be smaller than everyone - including $\{b, c\}$. But $\{a\} \not\subseteq \{b, c\}$, so $\{a\}$ cannot be a minimum (and $\{b, c\}$ cannot be a maximum). Similarly, we can show that this set doesn't have a minimum or a maximum.
However, it *does* have minimals and maximals: For instance, $\{a\}$ is minimal - since there's no element that's smaller than $\{a\}$. Similarly, $\{b, c\}$ is maximal, since there's no element that's greater than it.

Lemma 1.3.7.10. *If X is a poset with maximum (resp. minimum), then that maximum (resp. minimum) is also maximal (resp. minimal).*

Proof

Let $x = \max X$. Then for all other $y \in X$ we have $y \leq x$. In particular, if $y \neq x$ we have that $x \nleq y$, so x is a maximal element of X. $\square$

Definition 1.3.7.11. *Given a set A, an order $\leq$ in A is said to be a **well-order** if for every non-empty $X \subseteq A$ we have that $\min X$ exists.*

*In this case, we say that A is a **well-ordered** set.*

Theorem 1.3.7.12 (Well-ordering Principle)**.** *The set $\mathbb{N}$ with the usual order is well-ordered.*

Proof

Assume there is some set $B \subset \mathbb{N}$ which doesn't have a minimum. Consider $B' := \mathbb{N} \setminus B$.

- $0 \in B'$.

  This is trivial, cause, otherwise $0 \in B$, but then $0 = \min B$. Since we're assuming B doesn't have a minimum, then $0 \notin B$ and therefore $0 \in B'$.

- Assume $m \in B'$ for all $m \leq n$. We're going to show that $n + 1 \in B'$.

  If $n + 1$ was in B, then, since every $m \leq n$ is not in B, by assumption, we'd have that $n+1$ is a minimum of B. But B doesn't have a minimum, so $n+1 \notin B$ and, therefore, $n + 1 \in B'$.

But then B' is a subset of $\mathbb{N}$ which contains 0 and all its successors - therefore it must be $\mathbb{N}$ (by (PA3)).
But $B' = \mathbb{N} \setminus B$. So $B = \mathbb{N} \setminus B' = \mathbb{N} \setminus \mathbb{N} = \varnothing$ and, therefore, the only subset of $\mathbb{N}$ which doesn't have a minimum is $\varnothing$ - this proves that $\mathbb{N}$ is well-ordered, as we wished to show. $\square$

Let us now present a new kind of relation:

Proposition 1.3.7.13. *For any set X, "$x \sim y$ if, and only if, $x = y$" is a relation.*

Example(s)

Take X any set, and consider the relation above: $x \sim y$ if, and only if, $x = y$.

- First, we see that $x \sim x$ for all $x \in X$, since every element equals itself.

- Now, assume that $x \sim y$ for some $x, y \in X$. But this means that $x = y$, and therefore $y = x$, so $y \sim x$.

- Finally, if $x \sim y$ and $y \sim z$ for some $x, y, z \in X$, then this means that $x = y$ and $y = z$, so $x = y = z$ implies $x = z$. This means that $x \sim z$.

The first and the last items above say that $\sim$ is reflexive and transitive, respectively. The second one, however, is a new property - one that orders, in general, don't satisfy. It's called *symmetry*.

Definition 1.3.7.14. *Given a set X with a relation R, we say that R* ***is symmetric*** *if $x \mathrel{\mathrm{R}} y$ if, and only if, $y \mathrel{\mathrm{R}} x$.*

So, in other words, a relation is symmetric if it doesn't care about order.

Example(s)

The relation "a is a son of b" is **not** symmetric: a being b's son doesn't imply that b is a's son.
However, the relation "a is in the same class as b" is symmetric: a being in the same class as b is the same as b being in the same class as a.
Similarly, the relation "X has the same amount of elements as Y" is symmetric.

Definition 1.3.7.15. *Given a set X, a relation $\sim$ is said to be an* ***equivalence*** *if it is reflexive, symmetric and transitive.*

Lemma 1.3.7.16. *In any set X, element equality is an equivalence relation on X.*

Lemma 1.3.7.17. *Given any set X, the relation "$Y \sim Z$ if, and only if, $Y \cong Z$" is an equivalence relation on $\mathcal{P}(X)$.*

Proof

- $\sim$ is reflexive:

  Clearly, any $Y \in \mathcal{P}(X)$ is isomorphic to itself via the identity function $\mathrm{id}_Y : Y \to Y$;

- $\sim$ is symmetric:

  Let $Y \sim Z$ - that is, there is a bijection $f : Y \to Z$. But we know that bijections are isomorphisms, so there is an inverse $f^{-1} : Z \to Y$ which is also an isomorphism - and hence a bijection. So there is a bijection from Z to Y, and so $Z \sim Y$;

- $\sim$ is transitive:

  This follows trivially from the fact that composition of isomorphisms is, again, an isomorphism.

Since $\sim$ is reflexive, symmetric and transitive it is, by definition, an equivalence.
This ends the proof. $\square$

This is the final, and best reason why we should think of isomorphisms as being the true idea of set equality: Because it is an equivalence relation that tells us much more interesting information than set equality does.

Finally, to end this section we will use relations to build new sets.

Example(s)

Let $\mathbb{Z}$ be the set of integers, and define the following relation:

$$x \sim y \iff \exists k \in \mathbb{Z} \text{ such that } x - y = 2k.$$

Let us show that this is an equivalence:

- $\sim$ is reflexive:

  For all $x \in \mathbb{Z}$, $x - x = 0 = 2 \cdot 0$ and $0 \in \mathbb{Z}$, so $x \sim x$ and $\sim$ is reflexive.

- $\sim$ is symmetric:

  Let $x \sim y$ for some $x, y \in \mathbb{Z}$. Then there exists some $k \in \mathbb{Z}$ such that $x - y = 2k$, by definition of $\sim$. But then,

  $$y - x = -(x - y) = -(2k) = 2(-k),$$

  and since $k \in \mathbb{Z}$ we get that $-k \in \mathbb{Z}$, so $y \sim x$ and $\sim$ is symmetric.

- $\sim$ is transitive:

  Let $x \sim y$ and $y \sim z$, for some $x, y, z \in \mathbb{Z}$. Then, by definition of $\sim$, there exist some $k, l \in \mathbb{Z}$ such that $x - y = 2k$ and $y - z = 2l$.

  But then,
  $$x - z = x - y + y - z = 2k - 2l = 2(k - l)$$
  and since $k, l \in \mathbb{Z}$, we see that $k - l \in \mathbb{Z}$, so $x - z = 2(k - l)$ tells us that $x \sim z$, so $\sim$ is transitive.

So we see that $\sim$ is indeed an equivalence relation on $\mathbb{Z}$.
Now, this is our first weird equivalence. Let's see who is equivalent to whom in this new "equality":
For instance, who is equivalent to 1? Well, if $x \sim 1$, then $x - 1 = 2k$ for some $k \in \mathbb{Z}$, and so $x = 2k + 1$. But this means that x is *odd* (this is the definition of an odd number: one more than a multiple of 2).
Conversely, if $x = 2l + 1$ for some $l \in \mathbb{Z}$ is an odd number, we see that $x - 1 = (2l + 1) - 1 = 2l$ and so $x \sim 1$.
So if we denote by [1] the **class of every element in $\mathbb{Z}$ which is $\sim$-equivalent to 1**, we see that
$$[1] = \{x \in \mathbb{Z} \mid x \text{ is odd}\}.$$

But since we've proven that $\sim$ is an equivalence, if we take any other odd number - say, 3, we see that $[3] = [1]$, for the following reasoning:

- 3 is odd, so $3 \sim 1$.
- If $x \sim 3$, for some x, then since $\sim$ is transitive this implies $x \sim 1$.

- This, in turn, implies that x is odd.

Conversely - if x is odd, then $x \sim 1$, and since $3 \sim 1$ and $\sim$ is transitive, we get $x \sim 3$.
So everyone who is $\sim$-equivalent to 3 is also $\sim$-equivalent to 1, and vice-versa.
This means that we don't need to check any more odd numbers to fully understand $\sim$.

Let us check then the even numbers. For instance, 0. What's $[0]$ - that is, who is $\sim$-equivalent to 0?
Well, if $x \sim 0$, then $x - 0 = 2k$ for some $k \in \mathbb{Z}$, but $x - 0 = x$, so we get that $x = 2k$. This means that x is even.
Conversely, if x is even, then $x = 2l$ for some $l \in \mathbb{Z}$ (this is the definition of an even number: it is a multiple of 2). So $x - 0$ is just $2l - 0$ which is simply $2l$, so all even numbers are $\sim$-equivalent to 0.
This means that

$$[0] = \{x \in \mathbb{Z} \mid x \text{ is even}\}.$$

And doing the same reasoning we did above, we can see that $[2k] = [0]$ for any $l \in \mathbb{Z}$.
Therefore, under this new sense of "equality", there are only two different elements in $\mathbb{Z}$: 0 and 1. Everyone else is either $\sim$-equal to 0 or 1.

Definition 1.3.7.18. *Given any set X with an equivalence $\sim$, we define the* ***quotient set of*** *X* ***over*** *$\sim$ to be the set $X/\sim$ of all equivalence classes of elements of X under the equivalence $\sim$.*

Example(s)

Continuing the previous example, $\mathbb{Z}/\sim$ is just the set $\{[0], [1]\}$.

To finish this section, we'll prove two important results.

Theorem 1.3.7.19 (Cantor-Bernstein-Schroeder)**.** *If $f : A \to B$ and $g : B \to A$ are both injective, then there's an isomorphism $\phi : A \to B$.*

Proof

For each $x \in A \sqcup B$ define:

- $s_0^x := x$;
- $s_{n+1}^x := (f \sqcup g)(s_n^x)$;
- $s_{-(n+1)}^x := (f \sqcup g)^{-1}(s_{-n}^x)$, if s_{-n}^x is well-defined.

Note that for each $x \in A \sqcup B$ we know nothing about s_n^x being well-defined for negative n.
So, for each $x \in A \sqcup B$, we can create a new set:

$$S^x := \{y \in A \sqcup B \mid y = s_n^x \text{for some } n \in \mathbb{Z}\}$$

that is, S^x is the collection of all s_n^x that are well-defined.
Now, it's easy to see that every element of $A \sqcup B$ is in some S^x - so we get

$$A \sqcup B = \bigcup_{x \in A \sqcup B} S^x$$

(we're not claiming that this union is disjoint, there could be $x \neq y$ but such that $S^x = S^y$. We're not excluding that possibility).
Indeed, assume that's the case - that there's some $x \neq y$ such that $s_n^x = s_m^y$, for some $n, m \in \mathbb{Z}$. Then, clearly, $s_{n+l}^x = s_{m+l}^y$ for all $l \in \mathbb{Z}$, so $S^y = S^x$.
So now the proof consists of showing not that $A \cong B$, but that for each $x \in A \sqcup B$, we have $(S^x \cap A) \cong (S^x \cap B)$ - that is, the parts of A and B inside each of S^x are isomorphic. This suffices, because we can then extend this isomorphism to the whole A and B.

- If s_n^x is well-defined for all $n \in \mathbb{Z}$, then this means that $f' : S^x \cap A \to S^x \cap B$ is surjective, and therefore a bijection (since it's already injective).
- If $s_n^x \in A$ is the smallest well-defined, then, once again, $f' : S^x \cap A \to S^x \cap B$ is surjective, and therefore a bijection (since it's already injective).
- If $s_n^x \in B$ is the smallest well-defined, then $g' : S^x \cap B \to S^x \cap A$ is surjective, and, therefore, a bijection (since it's already injective).

Either way, we see that for all $x \in A \sqcup B$ we have $(S^x \cap A) \cong (S^x \cap B)$, so $A \cong B$, and the result follows. □

Theorem 1.3.7.20. *Let X be a set. Then the relation "$Y \leq Z$ if, and only if, there is an injection $f : Y \to Z$" is an order in $\mathcal{P}(X)/\cong$.*

Proof

- $\leq$ is reflexive:

  Let $Y \in \mathcal{P}(X)$. Then the identity map is injective, so $Y \leq Y$, and $\leq$ is reflexive.

- $\leq$ is antisymmetric:

  Let $Y \leq Z$ and $Z \leq Y$, for some $Y, Z \in \mathcal{P}(X)$. Then, by definition of $\leq$, there are injections $f : Y \to Z$ and $g : Z \to Y$. Now, by theorem 1.3.7.20, we see that $Y \cong Z$, and so $\leq$ is antisymmetric.

- $\leq$ is transitive:

  If $Y \leq Z$ and $Z \leq W$, for some $Y, Z, W \in \mathcal{P}(X)$, then there are injections $f : Y \to Z$ and $g : Z \to W$. But since composition of injections is, again, an injection, we see that $g \circ f : Y \to W$ is injective, and, therefore, $Y \leq W$, so $\leq$ is transitive.

Since $\leq$ is reflexive, antisymmetric and transitive, it is an order, by definition. This ends the proof. $\square$

Corollary 1.3.7.21. *Let X be a set. Then $Y \leq Z$ in $\mathcal{P}(X)/\cong$ if, and only if, there is a surjection $g : Z \to Y$.*

Proof

Follows trivially from the previous theorem and the fact that every injection has a left-inverse which is surjective. $\square$

We can finally proceed to the final section.

1.3.8 Second order thinking

Now, to finish up our brief talk on set theory, we're gonna talk about sets of functions.

Definition 1.3.8.1. *Let A and B be two sets. We denote the* ***set of functions from*** A ***to*** B *by* $\mathrm{Hom}(A, B)$.

Example(s)

Let $A = \{1, 2\}$ and $B = \{a, b, c\}$. Then, the only possible functions $A \to B$ are:

- $f_1 = \{(1, a), (2, a)\}$
- $f_2 = \{(1, a), (2, b)\}$
- $f_3 = \{(1, a), (2, c)\}$
- $f_4 = \{(1, b), (2, a)\}$
- $f_5 = \{(1, b), (2, b)\}$
- $f_6 = \{(1, b), (2, c)\}$
- $f_7 = \{(1, c), (2, a)\}$
- $f_8 = \{(1, c), (2, b)\}$
- $f_9 = \{(1, c), (2, c)\}$

so $\mathrm{Hom}(A, B) \cong 9$.
Notice that $A \cong 2$ and $B \cong 3$.

Analogously, the only possible functions $B \to A$ are:

- $g_1 = \{(a, 1), (b, 1), (c, 1)\}$
- $g_2 = \{(a, 1), (b, 1), (c, 2)\}$
- $g_3 = \{(a, 1), (b, 2), (c, 1)\}$
- $g_4 = \{(a, 1), (b, 2), (c, 2)\}$
- $g_5 = \{(a, 2), (b, 1), (c, 1)\}$
- $g_6 = \{(a, 2), (b, 1), (c, 2)\}$
- $g_7 = \{(a, 2), (b, 2), (c, 1)\}$
- $g_8 = \{(a, 2), (b, 2), (c, 2)\}$

so $\mathrm{Hom}(B, A) \cong 8$.
We can readily see that $\mathrm{Hom}(A, B) \cong \#B^{\#A}$ and $\mathrm{Hom}(B, A) \cong \#A^{\#B}$.

Lemma 1.3.8.2. *For any set X, we have that $\mathcal{P}(X) \cong \mathrm{Hom}(X, 2)$.*

Proof

Let $Y \in \mathcal{P}(X)$ and consider the function $f_Y : X \to 2$ defined by

$$f_Y(x) := \begin{cases} 1 & \text{if } x \in Y \\ 0, & \text{otherwise.} \end{cases}$$

This defines a unique function $f : \mathcal{P}(X) \to \mathrm{Hom}(X, 2)$ given by $f(Y) := f_Y$.

- f is injective:

  Let $Y, Z \in \mathcal{P}(X)$ be such that $f(Y) = f(Z)$. But this means that the functions $f_Y, f_Z : X \to 2$ are the same. But by definition of function equality, this means that $f_Y(x) = f_Z(x)$ for all $x \in X$.

In particular, $1 = f_Y(y)$. But this implies $1 = f_Y(y) = f_Z(y)$, so $y \in Z$ (by definition of f_Z). This shows that every element of Y is also an element of Z - that is, $Y \subseteq Z$.

Analogously, for all $z \in Z$ we have $f_Z(z) = 1$ and so $f_Y(z) = f_Z(z) = 1$ which implies that $z \in Y$ (by definition of f_Y), and hence every element of Z is also an element of Y - that is, $Z \subseteq Y$.

These two together imply that $Y = Z$ and so f is injective.

- f is surjective:

  Let $g : X \to 2$ be a function. Then, $g^{-1}(1) \subseteq X$. Call it X'. We claim that $f(X') = g$.

  Indeed, given any $x \in X$ we want to show that $f_{X'}(x) = g(x)$.

  If $x \in X'$, then:
  $$f_{X'}(x) = 1 = g(x)$$
  where the first equality holds by definition of $f_{X'}$ and the second equality holds by definition of X' (i.e., it's the inverse image of 1 under g - which means that if we apply g to X' we always get 1).

  If $x \notin X'$, the:
  $$f_{X'}(x) = 0 = g(x)$$
  where the two equalities hold by exactly the same reason as above.

  This shows that $f_{X'} = g$, and so $g \in \mathrm{Im}(f)$, which means that f is surjective.

Since f is both injective and surjective, we see that it is bijective - and hence an isomorphism. This ends the proof. □

Definition 1.3.8.3. *Given A and B, we're going to denote the set* $\mathrm{Hom}(A, B)$ *by* B^A *and call it the* ***exponential set****.*

Remark 1.3.8.4

This finally justifies the notation 2^X for the power set of X. It is, as we've shown, a set of functions: Any subset of X can be seen as a function which takes all its elements to 1, and everyone else to 0.

Theorem 1.3.8.5. *For any set X there is a bijection* $\mathrm{Hom}(1, X) \cong X$.

Proof

Define $f : \mathrm{Hom}(1, X) \to X$ like this: Given any $g : 1 \to X$, since 1 is a singleton, $g(0) \in X$ is also a singleton. So we define $f(g) := g(0) \in X$.

- f is injective:

Take two functions $g, h : 1 \to X$ such that $f(g) = f(h)$. But this means, by definition of f that $g(0) = h(0)$, and since $1 = \{0\}$ this means that g and h are equal for all elements of 1 - the definition of function equality.

This shows that $g = h$ and so f is injective.

- f is surjective:

  Take any element $x \in X$. Define the function $g_x : 1 \to X$ by putting $g_x(0) := x$. Then clearly, $f(g_x) = x$, by definition of both f and g_x.

  This shows that f is surjective.

Since f is both injective and surjective, it is a bijection, which ends the proof. □

Remark 1.3.8.6

This is one remarkable result: It tells us that if, somehow, we could define functions without knowing what elements are, we would be able to completely recover the elements of any set simply by looking at functions from 1 to that set.

Now we can do arithmetic with finite sets:

Lemma 1.3.8.7. *For any $n, m \in \mathbb{N}$ the following hold:*

- $n \sqcup m \cong n + m$;
- $n \times m \cong nm$;
- $\mathrm{Hom}(m, n) \cong n^m$.

Theorem 1.3.8.8 (Sets are cartesian-closed)**.** *Let X, Y, Z be sets. Then we have the following set isomorphism:*

$$\mathrm{Hom}(X \times Y, Z) \cong \mathrm{Hom}(X, \mathrm{Hom}(Y, Z)).$$

Proof

Fix, first and foremost, X, Y, Z to be any sets.
Now we define $f : \mathrm{Hom}(X \times Y, Z) \to \mathrm{Hom}(X, \mathrm{Hom}(Y, Z))$ as such: For any function $g : X \times Y \to Z$ we define $f(g)$ to be the function that takes any $x \in X$ to the function $(f(g))(x)$ that takes any $y \in Y$ to $((f(g))(x))(y) := g(x, y)$.
Define, now, $f' : \mathrm{Hom}(X, \mathrm{Hom}(Y, Z)) \to \mathrm{Hom}(X \times Y, Z)$ as such: For any function $g : X \to \mathrm{Hom}(Y, Z)$, we define $f'(g)$ to be the function that takes any $(x, y) \in X \times Y$ to $(f'(g))(x, y) := (g(x))(y)$.
We claim that $f' = f^{-1}$ and, thus, that f is an isomorphism.
Take any $g : X \to \mathrm{Hom}(Y, Z)$, any $x \in X$ and any $y \in Y$. We can see that

$$\begin{aligned}
(((f \circ f')(g))(x))(y) &= (f(f'(g))(x))(y) \\
&= (f'(g))(x, y) && \text{(by definition of } f) \\
&= g(x)(y) && \text{(by definition of } f'),
\end{aligned}$$

so, as functions, $((f \circ f')(g))(x) = g(x)$ (since they are equal for every $y \in Y$), and so $(f \circ f')(g) = g$ (since they are equal for every $x \in X$), and so $f \circ f' = \mathrm{id}_{\mathrm{Hom}(X,\mathrm{Hom}(Y,Z))}$ (since they are equal for every $g \in \mathrm{Hom}(X, \mathrm{Hom}(Y, Z))$).

Conversely, we have, for any $g : X \times Y \to Z$ and any $(x, y) \in X \times Y$ that

$$\begin{aligned}
((f' \circ f)(g))(x, y) &= (f'(f(g)))(x, y) \\
&= ((f(g))(x))(y) && \text{(by definition of } f') \\
&= g(x, y) && \text{(by definition of } f)
\end{aligned}$$

so, as functions, $(f' \circ f)(g) = g$ (since they are equal for every $(x, y) \in X \times Y$), and so $f' \circ f = \mathrm{id}_{\mathrm{Hom}(X \times Y,Z)}$ (since they are equal for every $g \in \mathrm{Hom}(X \times Y \to Z)$).

This shows that $f' = f^{-1}$ and hence f is an isomorphism.
The proves the result. □

Remark 1.3.8.9

This result is basically saying that there's a one-to-one correspondence between functions with two inputs and functions with one input whose input is another function with one input.

We will show, at some point, that an equivalent result also holds for linear transformations - and that will be of much use for us further ahead.

Proposition 1.3.8.10. *Any function $f : X \to Y$ induces unique functions from $\mathrm{Hom}(A, X)$ to $\mathrm{Hom}(A, Y)$ and from $\mathrm{Hom}(Y, A)$ to $\mathrm{Hom}(X, A)$ for any set A.*

Proof

Define $\phi_f : \mathrm{Hom}(A, X) \to \mathrm{Hom}(A, Y)$ by putting $\phi_f(g) := f \circ g$ for any $g \in \mathrm{Hom}(A, X)$ and $\psi^f : \mathrm{Hom}(Y, A) \to \mathrm{Hom}(X, A)$ by putting $\psi^f(h) := h \circ f$.
Clearly ϕ and ψ are functions, so the result follows. □

Definition 1.3.8.11. *Given any set A and any function $f : X \to Y$, the unique functions induced by f will be denoted by $\mathrm{Hom}(A, f) : \mathrm{Hom}(A, X) \to \mathrm{Hom}(A, Y)$ and $\mathrm{Hom}(f, A) : \mathrm{Hom}(Y, A) \to \mathrm{Hom}(X, A)$.*

Lemma 1.3.8.12. *If $X \xrightarrow{f} Y \xrightarrow{g} Z$, then, for any A we have that $\mathrm{Hom}(A, g \circ f) = \mathrm{Hom}(A, g) \circ \mathrm{Hom}(A, f)$ and $\mathrm{Hom}(g \circ f, A) = \mathrm{Hom}(f, A) \circ \mathrm{Hom}(g, A)$.*

Proof

Take any $h \in \mathrm{Hom}(A, X)$. Then:

$$\begin{aligned}
\mathrm{Hom}(A, g \circ f)(h) &= (g \circ f) \circ h \\
&= g \circ (f \circ h) \\
&= \mathrm{Hom}(A, g)(f \circ h) \\
&= \mathrm{Hom}(A, g)(\mathrm{Hom}(A, f)(h)) = (\mathrm{Hom}(A, g) \circ \mathrm{Hom}(A, f))(h),
\end{aligned}$$

and so $\mathrm{Hom}(A, g \circ f) = \mathrm{Hom}(A, g) \circ \mathrm{Hom}(A, f)$.
Similarly, given any $h \in \mathrm{Hom}(Z, A)$ we have:

$$\begin{aligned}
\mathrm{Hom}(g \circ f, A)(h) &= h \circ (g \circ f) \\
&= (h \circ g) \circ f \\
&= \mathrm{Hom}(f, A)(h \circ g) \\
&= \mathrm{Hom}(f, A)(\mathrm{Hom}(g, A)(h)) = (\mathrm{Hom}(f, A) \circ \mathrm{Hom}(g, A))(h),
\end{aligned}$$

and so $\mathrm{Hom}(g \circ f, A) = \mathrm{Hom}(f, A) \circ \mathrm{Hom}(g, A)$. $\square$

Lemma 1.3.8.13. *For any sets A, B, we have that $\mathrm{Hom}(A, \mathrm{id}_B) = \mathrm{id}_{\mathrm{Hom}(A,B)} = \mathrm{Hom}(\mathrm{id}_A, B)$.*

Proof

This follows trivially by inspection:

$$\mathrm{Hom}(A, id_B)(g) = \mathrm{id}_B \circ g = g \circ \mathrm{id}_A = \mathrm{Hom}(\mathrm{id}_A, B)(g)$$

for all $g \in \mathrm{Hom}(A, B)$. $\square$

Finally, the last result of this section - the Yoneda Lemma:

Definition 1.3.8.14. *Let X, Y be sets. A **natural transformation** $\phi : \mathrm{Hom}(-, X) \to \mathrm{Hom}(-, Y)$ is a family of functions $\phi := \{\phi_A : \mathrm{Hom}(A, X) \to \mathrm{Hom}(A, Y)\}_A$, where A ranges over all sets, such that*

$$\begin{tikzcd}
\mathrm{Hom}(B, X) \arrow[r, "\phi_B"] \arrow[d, "\mathrm{Hom}(g,X)"'] & \mathrm{Hom}(B, Y) \arrow[d, "\mathrm{Hom}(g,Y)"] \\
\mathrm{Hom}(A, X) \arrow[r, "\phi_A"'] & \mathrm{Hom}(A, Y)
\end{tikzcd}$$

commutes for all $g : A \to B$.

*If each ϕ_A in the family is an isomorphism, then we say that ϕ is a **natural isomorphism**.*

Theorem 1.3.8.15 (Yoneda's Lemma)**.** *Let X and Y be any sets. Then there is a bijective correspondence between natural transformations $\phi : \mathrm{Hom}(-, X) \to \mathrm{Hom}(-, Y)$, and functions $f : X \to Y$.*

Proof

Take $g : A \to B$ any function.
Since the diagram commutes, by hypothesis, $\mathrm{Hom}(g, Y) \circ \phi_B = \phi_A \circ \mathrm{Hom}(g, X)$ holds for any choice of A, B and g.
So if we take $g : A \to X$, by applying the equality above to id_X we see that

$$(\mathrm{Hom}(g, Y) \circ \phi_X)(\mathrm{id}_X) = \mathrm{Hom}(g, Y)(\phi_X(\mathrm{id}_X)) = (\phi_X(\mathrm{id}_X)) \circ g$$

and

$$(\phi_A \circ \mathrm{Hom}(g, X))(\mathrm{id}_X) = \phi_A(\mathrm{Hom}(g, X)(\mathrm{id}_X)) = \phi_A(\mathrm{id}_X \circ g) = \phi_A(g)$$

must be equal - in other words, $\phi_X(\mathrm{id}_X) \circ g = \phi_A(g)$.
But this shows us that $\phi_A : \mathrm{Hom}(A, X) \to \mathrm{Hom}(A, Y)$ is uniquely defined by $\phi_A = \mathrm{Hom}(A, \phi_X(\mathrm{id}_X))$.
In other words, the correspondence

$$\{\phi_A : \mathrm{Hom}(A, X) \to \mathrm{Hom}(A, Y)\}_A \mapsto (\phi_X(\mathrm{id}_X) : X \to Y)$$

$$(f : X \to Y) \mapsto \{\mathrm{Hom}(A, f) : \mathrm{Hom}(A, X) \to \mathrm{Hom}(A, Y)\}_A$$

is bijective.
This finishes the proof. □

Definition 1.3.8.16. *Let X, Y be sets. A **natural transformation** $\phi : \mathrm{Hom}(X, -) \to \mathrm{Hom}(Y, -)$ is a family of functions $\phi := \{\phi_A : \mathrm{Hom}(X, A) \to \mathrm{Hom}(Y, A)\}_A$, where A ranges over all sets, such that*

$$\begin{tikzcd}
\mathrm{Hom}(X, A) \arrow[r, "\phi_A"] \arrow[d, "\mathrm{Hom}(X,g)"'] & \mathrm{Hom}(Y, A) \arrow[d, "\mathrm{Hom}(Y,g)"] \\
\mathrm{Hom}(X, B) \arrow[r, "\phi_B"'] & \mathrm{Hom}(Y, B)
\end{tikzcd}$$

commutes for all $g : A \to B$.

*If each ϕ_A in the family is an isomorphism, then we say that ϕ is a **natural isomorphism**.*

Corollary 1.3.8.17 (Yoneda's Lemma)**.** *Let X and Y be any sets. Then there is a bijective correspondence between natural transformations $\psi : \mathrm{Hom}(X, -) \to \mathrm{Hom}(Y, -)$, and functions $f : Y \to X$.*

Proof

It's essentially the same proof as the theorem's, so it'll be left as an exercise to the reader. □

Corollary 1.3.8.18. *For any pair of sets X, Y the following are equivalent:*

(i.) There is a natural isomorphism $\phi : \mathrm{Hom}(-, X) \to \mathrm{Hom}(-, Y)$;

(ii.) There is a natural isomorphism $\psi : \mathrm{Hom}(Y, -) \to \mathrm{Hom}(X, -)$*;*

(iii.) $X \cong Y$*.*

Proof

We will only prove (i.) if, and only if, (iii.). The case (ii.) if, and only if, (iii.) is similar and will be left as an exercise to the reader.

Let $\phi := \{\phi_A : \mathrm{Hom}(A, X) \to \mathrm{Hom}(A, Y)\}_A$ be a natural isomorphism. Analogously, let $\phi^{-1} := \{\phi_A^{-1} : \mathrm{Hom}(A, Y) \to \mathrm{Hom}(A, X)\}_A$ be the inverse natural isomorphism.
In light of Yoneda's Lemma, we see that ϕ and ϕ^{-1} determine unique functions $f_\phi : X \to Y$ and $f_{\phi^{-1}} : Y \to X$ given by $f_\phi := \phi_X(\mathrm{id}_X)$ and $f_{\phi^{-1}} := \phi_Y^{-1}(\mathrm{id}_Y)$, respectively, such that $\phi_A = \mathrm{Hom}(A, f_\phi)$ and $\phi_A^{-1} = \mathrm{Hom}(A, f_{\phi^{-1}})$ for every set A.
We claim that they are mutually inverse and, therefore, $X \cong Y$.
To see this, let us compute:

$$\begin{aligned}\mathrm{Hom}(X, \mathrm{id}_X) &= \mathrm{id}_{\mathrm{Hom}(X,X)} \\ &= \phi_X^{-1} \circ \phi_X \\ &= \mathrm{Hom}(X, f_{\phi^{-1}}) \circ \mathrm{Hom}(X, f_\phi) \\ &= \mathrm{Hom}(X, f_{\phi^{-1}} \circ f_\phi)\end{aligned}$$

and

$$\begin{aligned}\mathrm{Hom}(Y, \mathrm{id}_Y) &= \mathrm{id}_{\mathrm{Hom}(Y,Y)} \\ &= \phi_Y \circ \phi_Y^{-1} \\ &= \mathrm{Hom}(Y, f_\phi) \circ \mathrm{Hom}(Y, f_{\phi^{-1}}) \\ &= \mathrm{Hom}(Y, f_\phi \circ f_{\phi^{-1}})\end{aligned}$$

together tells us that f_ϕ and $f_{\phi^{-1}}$ are mutually inverse and, therefore, isomorphisms.
This proves $X \cong Y$.

Conversely, if $f : X \to Y$ is an isomorphism, then clearly $\phi := \{\phi_A := \mathrm{Hom}(A, f)\}_A$ is a natural isomorphism.
We have thus shown that (i.) if, and only if, (iii.), which ends the proof. □

Summing it all up, what Yoneda's Lemma tells us is that the only possible natural transformations are of the form $\mathrm{Hom}(-, f) : \mathrm{Hom}(-, X) \to \mathrm{Hom}(-, Y)$ or $\mathrm{Hom}(f, -) : \mathrm{Hom}(Y, -) \to \mathrm{Hom}(X, -)$, for some $f : X \to Y$.

This is very useful in Linear Algebra where we use that two vector spaces are isomorphic if, and only if, there is a natural isomorphism of sets of linear transformations - basically the preceding corollary, but applied to vector spaces.

Theorem 1.3.8.19. *The isomorphism in theorem 1.3.8.8 is natural for all three entries - that is, we have three natural isomorphisms:*

$$\phi_{X,Z} : \mathrm{Hom}(X \times -, Z) \to \mathrm{Hom}(X, \mathrm{Hom}(-, Z))$$

$$\phi_X^Y : \mathrm{Hom}(X \times Y, -) \to \mathrm{Hom}(X, \mathrm{Hom}(Y, -))$$
$$\phi_Z^Y : \mathrm{Hom}(- \times Y, Z) \to \mathrm{Hom}(-, \mathrm{Hom}(Y, Z))$$

We will not prove this result, since it follows trivially by inspection. We will, once more, leave it as an exercise to the reader.

With this, we have proven most of the stuff that we'll need to study Linear Algebra.
So, without further ado, let us begin.

Chapter 2

Real Linear Algebra

2.1 Introduction

2.1.1 First notions and definitions

To start working with vector spaces we first need to understand that the perspective is going to change a bit from the previous chapter. We're leaving the domain of **set theory** and jumping right in the domain of **algebra**.

Algebra is the domain of mathematics that deals with operations and their properties.

Definition 2.1.1.1. *Given any set X, a* ***(binary) operation*** *on X is a function $f : X \times X \to X$.*

Example(s)

Let $\mathbb{N}$ be the set of natural numbers, as before. We have a few operations here:

$$f, g, h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

$$(n, m) \mapsto f(n, m) := n + m$$
$$(n, m) \mapsto g(n, m) := nm$$
$$(n, m) \mapsto h(n, m) := n^m$$

and some of these operations have some properties that the others don't.
For instance, all three functions satisfy the following property:

- Let ϕ be an operation on X. There is some $n_e \in X$ such that $\phi(n, n_e) = n$ for all $n \in X$.

In the case of f, if we choose $n_e := 0$, we see that $f(n, 0) = n + 0 = n$, no matter which $n \in \mathbb{N}$ we chose, so f satisfies the property above.
In the case of g, if we choose $n_e := 1$, we see that $g(n, 1) = n \cdot 1 = n$, no matter which $n \in \mathbb{N}$ we chose, so g satisfies the property above.

Finally, in the case of h, if we choose $n_e := 1$, we see that $h(n, 1) = n^1 = n$, no matter which $n \in \mathbb{N}$ we chose, so h satisfies the property above.

Next up is the property:

- Let ϕ be an operation on X. There is some $n_e \in X$ such that $\phi(n_e, n) = n$ for all $n \in X$.

What can we say about f, g, h in this case? Well, it's easy to see that for f and g it still holds true - and it does so for the same value of n_e as before.
However, for h it fails. For instance, is there some number $x \in \mathbb{N}$ such that $h(x, 2) = 2$? Well, by definition of h we would need to have $x^2 = 2$ and so $x = \sqrt{2}$ which is not in $\mathbb{N}$ - this tells us that there's no such $x \in \mathbb{N}$. It follows that this property fails for h.

Summing up all of these together, we get the following property:

- (Identity element) Let ϕ be an operation on X. There is some $n_e \in X$ such that $\phi(n, n_e) = n = \phi(n_e, n)$ for all $n \in X$.

And we see that f and g have what's called an *identity element* - it's an element n_e such that if you fix it in any input of your operation, then your operation is just the identity function.

Consider now the following property:

- (Associativity) Let ϕ be an operation on X. Then, for all $n, m, l \in X$ we have that $\phi(\phi(n, m), l) = \phi(n, \phi(m, l))$.

In the case of f we can check

$$f(f(n, m), l) = f(n + m, l) = (n + m) + l = n + (m + l) = f(n, m + l) = f(n, f(m, l))$$

and see that f is associative.
In the case of g we can check

$$g(g(n, m), l) = g(nm, l) = (nm)l = n(ml) = g(n, ml) = g(n, g(m, l))$$

and see that g is associative.
However, for h, once again, this property fails: For instance, let us compare $h(h(2, 2), 3)$ and $h(2, h(2, 3))$:

$$h(h(2, 2), 3) = h(2^2, 3) = (2^2)^3 = 4^3 = 64$$

$$h(2, h(2, 3)) = h(2, 2^3) = 2^{(2^3)} = 2^8 = 256$$

so they are clearly different, and h is not associative.

One more:

- (Commutativity) Let ϕ be an operation on X. Then, for all $n, m \in X$ we have that $\phi(n,m) = \phi(m,n)$.

In the case of f we can easily see that $f(n,m) = n+m = m+n = f(m,n)$.
Similarly for g, we see that $g(n,m) = nm = mn = g(m,n)$.
But, once again, $h(2,3) = 8 \neq 9 = h(3,2)$, so h is not commutative.

These are the most common operations in $\mathbb{N}$ and some of their properties. Now, let us show something that is **not** an operation:
Consider the functions

$$f', g' : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

$$(n,m) \mapsto f'(n,m) := n - m$$

$$(n,m) \mapsto g'(n,m) := n/m.$$

Notice that I've just lied to you - these are **not** functions. To see that, take f' and apply it on $(3,1)$. By definition of function, $f'(3,1)$ should lie on $\mathbb{N}$, the codomain of f'. But, by definition of f', we see that $f'(3,1) = 3 - 1 = -2$, which is **not** in $\mathbb{N}$.
Similarly, g' isn't a function for the same reason: It should take, for instance, $(1,2)$ to a natural number - but it doesn't. It takes $(1,2)$ to $g'(1,2) = 1/2$ which, once more, is not a natural number.
However, for *some* specific values of the input, f' and g' really have outputs in $\mathbb{N}$. For that reason, they are called **partial operations** and, sadly, won't be studied in this text, since we're mostly concerned with proper operations.
If, however, you'd like to learn more about partial operations, you should click here or Google for "groupoid" - which is precisely the mathematical notion of a set with an associative partial operation.

Definition 2.1.1.2. *Given an operation $\phi : X \times X \to X$ we will say that*

- *(Identity element) ϕ admits an **identity element** if there is some $e \in X$ such that $\phi(x,e) = x = \phi(e,x)$ for all $x \in X$. In this case, e is called an **identity element**;*
- *(Associativity) ϕ is **associative** if $\phi(x, \phi(y,z)) = \phi(\phi(x,y), z)$ for all $x, y, z \in X$;*
- *(Commutative) ϕ is **commutative** if $\phi(x,y) = \phi(y,x)$ for all $x, y \in X$;*
- *(Inverse element) ϕ admits **inverse elements** if for all $x \in X$ there is some $y \in X$ such that $\phi(x,y) = e = \phi(y,x)$ for some identity element $e \in X$.*

Definition 2.1.1.3. *Let X be a set with two operations, $f, g : X \times X \to X$. We say that f **distributes over** g **on the left** (resp. **on the right**) if*

$$f(x, g(y,z)) = g(f(x,y), f(x,z))$$

(resp.

$$f(g(x,y), z) = g(f(x,z), f(y,z)))$$

for all $x, y, z \in X$.

*If f distributes over g on both sides, we simply say that f **distributes over** g.*

Example(s)

Following up on the previous example, we see that g (the multiplication) distributes over f (the addition):

$$g(n, f(m, l)) = g(n, m + l) = n(m + l) = nm + nl = f(nm, nl) = f(g(n, m), g(n, l))$$

$$g(f(n, m), l) = g(n + m, l) = (n + m)l = nl + ml = f(nl, ml) = f(g(n, l), g(m, l))$$

but f doesn't distribute (on either side!) over g:

$$1 + (1 \cdot 1) = 1 + 1 = 2 \neq 4 = 2 \cdot 2 = (1 + 1) \cdot (1 + 1)$$

$$(1 \cdot 1) + 1 = 1 + 1 = 2 \neq 4 = 2 \cdot 2 = (1 + 1) \cdot (1 + 1)$$

All this talk now brings us to a very specific definition:

Definition 2.1.1.4. *Let X be a set with two operatios $A, M : X \times X \to X$. We will say that (X, A, M) is a **field** if*

(1) A is associative;

(2) A is commutative;

(3) A has an identity element;

(4) A has inverses;

(5) M is associative;

(6) M is commutative;

(7) M has an identity element;

(8) M has inverses (excluding the additive identities);

(9) M distributes over A.

*In this case, we call A and M, respectively, the field's **addition** and **multiplication** operations, and denote them simply by $x + y := A(x, y)$ and $xy := M(x, y)$ for all $(x, y) \in X \times X$.*

Proposition 2.1.1.5. *The set $\mathbb{R}$ of real numbers with the usual addition and multiplication is a field.*

Proof

This is immediate, since for every $x, y, z \in \mathbb{R}$ we have:

(1) $x + (y + z) = (x + y) + z$;

(2) $x + y = y + x$;

(3) $x + 0 = 0 + x = x$;

(4) $x + (-x) = (-x) + x = 0$;

(5) $x(yz) = (xy)z$;

(6) $xy = yx$;

(7) $x \cdot 1 = 1 \cdot x = x$;

(8) $xx^{-1} = x^{-1}x = 1$ if $x \neq 0$;

(9) $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$.

$\square$

Example(s)

Notice, however, that the sets $\mathbb{N}$ and $\mathbb{Z}$, of the naturals and integers, respectively, are **not** fields: $\mathbb{N}$ doesn't have either additive or multiplicative inverses (so it fails properties (4) and (8)), and $\mathbb{N}$ doesn't have multiplicative inverses (so it fails property (8)).
On the other hand, it's easy to see that $\mathbb{Q}$, the set of rational numbers, is indeed a field. It is actually constructed to be, in some sense, "the smallest field which extends $\mathbb{Z}/\mathbb{N}$".
Finally, the set $\mathbb{C}$ of complex numbers is also a field if you define the inverse of $z = x + iy$ to be $z^{-1} := \dfrac{x - iy}{x^2 + y^2}$. Indeed:

$$zz^{-1} = (x + iy)\left(\frac{x - iy}{x^2 + y^2}\right) = \frac{x^2 + y^2}{x^2 + y^2} = 1$$

so it is indeed an inverse for z.

Let us show some properties of fields:

Lemma 2.1.1.6. *Let $(k, +, \cdot)$ be a field. Then the following hold:*

(a) There's a unique additive identity;

(b) For each $x \in k$, there's a unique additive inverse;

(c) There's a unique multiplicative identity;

(d) For each $x \in k$, there's a unique multiplicative inverse;

(e) Let 0 be an additive identity of k. Then $0x = 0$ for all $x \in k$.

(f) Let 1 be a multiplicative identity of k. Then $-x = (-1)x$, where $(-1) + 1 = 0$.

Proof

(a) Let 0 and $0'$ be two additive identities of k. Then

$$0 = 0 + 0' = 0'$$

where the leftmost equality holds since $0'$ is additive identity, and the rightmost equality holds since 0 is additive identity, and so $0 = 0'$.

(b) Given $x \in k$, let x' and x'' be two additive inverses to x. Then

$$x' = x' + 0 = x' + (x + x'') = (x' + x) + x'' = 0 + x'' = x''$$

and so $x' = x''$.

(c) Let 1 and $1'$ be two multiplicative identities of k. Then

$$1 = 1 \cdot 1' = 1'$$

where the leftmost equality holds since $1'$ is a multiplicative identity, and the rightmost equality holds since 1 is a multiplicative identity, so $1 = 1'$.

(d) Given $x \in k$, let x'' and x'' be two multiplicative inverses to x. Then

$$x' = x' \cdot 1 = x'(xx'') = (x'x)x'' = 1 \cdot x'' = x''$$

and so $x' = x''$.

(e) Given $x \in k$, we have that

$$0x = (0+0)x = 0x + 0x$$

since k is a field and 0 is the additive identity. Let $y \in k$ be the additive inverse of $0x$.

Then, since the above is true, we can see that $(0x) + y = (0x + 0x) + y$ is also true. But the LHS is just 0, since y is the additive inverse of $0x$, and the RHS is just $(0x+0x)+y = 0x + (0x + y) = 0x + 0 = 0x$, so the above equation evaluates to $0 = 0x$.

(f) Given $x \in k$, we have that $0x = (1 + (-1))x$ since $1 + (-1) = 0$. But now, by the distributive property of fields we see that $0x = (1 + (-1))x = (1)x + (-1)x$.

But $0x = 0$ and $1x = x$, so this is just $0 = x + (-1)x$. Since additive inverses are unique, we see that $(-1)x = -x$.

□

This result basically tells us that every field is "similar" to $\mathbb{R}$, in some sense.

Remark 2.1.1.7

The reason why we require that the multiplication has inverses for all elements *except for 0* is precisely because of item (e) above. Since $0x = 0$ for all x, if we could have some 0^{-1}, then $0 = 00^{-1} = 1$ so we would have $0 = 1$.
But since $1x = x$ for all x, this would imply that $x = 1x = 0x = 0$, so **every element of the field would have to be 0 for it to be consistent**.
In other words, the only set that satisfies all the properties of a field and also has a multiplicative inverse to 0 is the set $\{0\}$.
In fact:

Proposition 2.1.1.8. *The set* $1 = \{0\}$ *with addition and multiplication being equal and given by* $0 + 0 = 0 \cdot 0 = 0$ *is a field. Its multiplicative and additive identities are* 0*, who is also the inverse of* 0.

Proof

There's literally nothing to prove. □

Finally, to end this section, let us give some examples of fields that aren't 1, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.

Example(s)

Let $p \in \mathbb{N}$ be a prime number (that is, there are only two ways to write $p = nm$: $n = p, m = 1$ and $n = 1, m = p$). Consider the set $p \in \mathbb{N}$ - that is, $p = \{0, 1, 2, \cdots, p-1\}$. We will give a field structure to p as follows:
For any $x, y \in p$, define:

- $x + y$ is the remainder of the division of $x + y$ in $\mathbb{N}$ by p;
- xy is the remainder of the division of xy in $\mathbb{N}$ by p.

We claim that p with those two operations is a field, which will be denoted by either $\mathbb{Z}_p$, $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{F}_p$.
For instance, let us do some computations with $p = 3$.
In this case, $p = \{0, 1, 2\}$, and so we have the following tables of operations:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

and

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

It is, then, readily seen that 0 and 1 are, respectively, the additive and multiplicative identities of $\mathbb{F}_3$.
We can also see that $1 + 2 = 0$ so 1 and 2 are additive inverses to each other. Similarly, we see that $1 \cdot 1 = 1 = 2 \cdot 2$ so both 1 and 2 are multiplicative inverses to themselves.
This shows that $\mathbb{F}_3$ is a field.
Building similar tables of operations we can prove that any $\mathbb{F}_p$ is a field.
Let us now show the necessity of p being a prime.

Let $4 = \{0, 1, 2, 3\}$. Let's try building the same operations:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

and

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

but this shows that 2 doesn't have any multiplicative inverses: $2 \cdot 0 = 0$, $2 \cdot 1 = 2$, $2 \cdot 2 = 0$ and $2 \cdot 3 = 2$.
But by definition of a field, the only element that has no multiplicative inverse is 0. But clearly $2 \neq 0$ (since $1 + 2 \neq 1$), so $\mathbb{Z}/4\mathbb{Z}$ cannot be a field.
This happens precisely because 4 can be written as $4 = nm$ in *three* different ways: $4 = 4 \cdot 1 = 1 \cdot 4 = 2 \cdot 2$.
Since this isn't supposed to be a course on field theory, we won't go into much detail on how to prove that $\mathbb{Z}/n\mathbb{Z}$ is a field if, and only if, n is prime.

2.1.2 Real vector fields

Let us start this section with the set that will be the focus of most, if not all, of this chapter: $\mathbb{R}^2$.

By definition, $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is the set of ordered pairs of real numbers.

Definition 2.1.2.1. *We're going to define the* ***addition*** $A : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$ *to be given by* $A((x, y), (z, w)) := (x + z, y + w)$ *for any* $(x, y), (z, w) \in \mathbb{R}^2$.

Proposition 2.1.2.2. *The addition A we've just defined satisfies the following properties:*

(i.) *A is associative;*

(ii.) *A is commutative;*

(iii.) *A admits an identity element;*

(iv.) *A admits inverses.*

Proof

Choose any three elements $(a, b), (c, d), (e, f) \in \mathbb{R}^2$. Then:

(i.)

$$\begin{aligned} A\left(A\left((a,b),(c,d)\right),(e,f)\right) &= A((a+c, b+d),(e,f)) \\ &= ((a+c)+e, (b+d)+f) \\ &= (a+(c+e), b+(d+f)) \\ &= A((a,b),(c+e,d+f)) = A((a,b), A((c,d),(e,f))), \end{aligned}$$

so A is associative;

(ii.)

$$A((a,b),(c,d)) = (a+c, b+d) = (c+a, d+b) = A((c,d),(a,b))$$

so A is commutative;

(iii.) $A((a,b),(0,0)) = (a+0, b+0) = (a,b) = (0+a, 0+b) = A((0,0),(a,b))$ so A has identity $(0,0)$;

(iv.) $A((a,b),(-a,-b)) = (a-a, b-b) = (0,0) = (-a+a, -b+b) = A((-a,-b),(a,b))$ so A has inverses.

□