# Algebra Notes

Trustin Nguyen

November 23, 2023

# Contents

# Chapter 1

# Set Theory and Categories

## 1.1 Naive Set Theory

**Definition 1.1.1**

**Equivalence Relation**

An equivalence relation on a set $S$ is any relation $\sim$ satisfying these three properties:

- *reflexivity:* $(\forall a \in S) a \sim a$;
- *symmetry:* $(\forall a \in S) a \sim b \implies b \sim a$;
- *transitivity*: $(\forall a \in S)(\forall b \in S)(\forall c \in S), (a \sim b \text{ and } b \sim c) \implies a \sim c$.

A partition of $S$ can be obtained through equivalence classes which are defined as

$$[a]_\sim := \{b \in S : b \sim a\}$$

This leads to the definition that shows that partitions of a set $S$:

**Definition 1.1.2**

**Quotient Set**

The *quotient* of the set $S$ with respect to the equivalence relation $\sim$ is the set

$$S/\sim := \mathcal{P}_\sim$$

of equivalence classes of elements of $S$ with respect to $\sim$.

**Example 1.1.1:** Take $S = \mathbb{Z}$, and let $\sim$ be the relation defined by

$$a \sim b \iff a - b \text{ is even}$$

Then $\mathbb{Z}/\sim$ consists of two equivalence classes:

$$\mathbb{Z}/\sim = \{[0]_\sim, [1]_\sim\}$$

**Problem Sets**

**Exercise 1**: Locate a discussion of Russell's paradox, and understand it.

*Answer.* Russell's paradox states that any set theory which contains the proposition that there exists a set for every proposition, that is

$$\forall p_1, p_2, \ldots, p_n \exists S \forall s (s \in S \iff \varphi(x, p_1, p_2, \ldots, p_n))$$

would contain a contradiction. Specifically, it was pointed out that the set of all sets that do not contain themselves was impossible to construct. If we follow from the definition, suppose that $R$ is the set of sets that do not contain themselves. We have two cases. If $R \notin R$, then we would observe that $R$ must contain itself so $R \in R$. Which is a contradiction. If we have the latter case that $R \in R$, then $R$ is in the set of sets that do not contain itself. Therefore, $R \notin R$ which is also a contradiction.

**Exercise 2**: Prove that if $\sim$ is a relation on a set $S$, then the corresponding family $\mathcal{P}_\sim$ is a partition of $S$: that is, its elements are nonempty, disjoint, and their union is $S$.

*Answer.* Since we define each equivalence to be reflexive, that means that for a given element $s \in S$, its equivalence class is nonempty as $s \sim s$. Now suppose that we have two equivalence classes:

$$s_1 \in [a], [b]$$

and that $[a] \neq [b]$. Suppose that $s_1 \in [b]$ also. We will show that $[a] \cap [b] = \emptyset$ otherwise, $[a] = [b]$. Since $s_1 \in [b]$, following from the definition of equivalence class:

$$[b] = s \in S : s \sim b$$

we find that $s_1 \sim b$. Now let $b_i \in [b]$ be arbitrary. Then $s_1 \sim b$, $b_i \sim b \implies b \sim b_i$. By transitivity, we have that $s_1 \sim b \sim b_i$. So an arbitrary element of $[b]$ must be in $[a]$: $[b] \subseteq [a]$. Since $[b] \neq \emptyset$ we have that some $b \in [b]$ is in $[a]$. But the same argument now, we conclude that $[a] = [b]$. Therefore, the equivalence classes are disjoint, otherwise they are the same. We can disregard these duplicates as $\mathcal{P}_\sim$ is a set. We can show that the equivalence classes partition $S$ since every element must belong to some equivalence class. Take an arbitrary $s \in S$. Then $s \in [s]$. We are done.

**Exercise 3**: Given a partition $\mathcal{P}$ on a set $S$, show how to define a relation $\sim$ on $S$ such that $\mathcal{P}$ is the corresponding partition.

*Answer.* Given a partition of a set $S$, we note that it is of the form $S = \bigcup_{i=1}^{n} S_i$ where $S_i \cap S_j = \emptyset$ for $i \neq j$. Now we say that $a \sim b \iff (a \in S_i \iff b \in S_i)$. This says that $a, b$ are related if only if they belong in the same set. This is an equivalence relation, which we will prove. Observe that in a partition, $a \in S_i \iff a \in S_i$. Therefore, $a \sim a$. It satisfies the reflexive property. As for the symmetric, we note that if $a \sim b$, then that means that $a \in S_i \iff b \in S_i$. But that means that $b \in S_i \iff a \in S_i$. Therefore, $b \sim a$ which is the symmetric property. Now for transitive, suppose that $a_1 \sim a_2 \wedge a_2 \sim a_3$. Then $a_1 \in S_i \iff a_2 \in S_i$ and $a_2 \in S_j \iff a_3 \in S_j$. By the fact that the partitions are disjoint, that means that if $a_1 \in S_i$, then $a_2 \in S_i$. But that means that $a_3 \in S_i$. And if $a_3 \in S_i$, then it follows that $a_1 \in S_i$ since we can argue the same backwards. So $a_1 \sim a_3$. We are done as this is a proper equivalence relation.

**Exercise 4**: How many different equivalence relations may be defined on the set $\{1, 2, 3\}$?

*Answer.* Given an equivalence class, observe that we can map it to a partition, as done in Exercise 2. In Exercise 3, we defined a partition that maps to an equivalence class. There is a clear bijection between the partitions of a set and the equivalence classes of a set, namely, we map a set of partitions

$$S_1, S_2, \ldots, S_n$$

to which we have $s_i \in S_i$ and we map $s_i \in [s_i]$. Observe that each partition gets mapped to an equivalence class. This mapping is injective and surjective. So the number of ways to partition a set is the number of equivalence classes there are. Therefore, since $\{1, 2, 3\}$ has partitions:

$$\{1\} \cup \{2\} \cup \{3\}, \{1, 2\} \cup \{3\}$$
$$\{1, 3\} \cup \{2\}, \{2, 3\} \cup \{3\}$$
$$\{1, 2, 3\}$$

which count to 5, there are 5 equivalence relations.

**Exercise 5**: Give an example of a relation that is reflexive and symmetric but not transitive. What happens if you attempt to use this relations to define a partition on a set?

*Answer.* When you do this, elements that are in the same equivalence class might not be related. For example, we might have that $a_1, a_2 \in [a]$:

$$[a] = \{s \in S : s \sim a\}$$

so we have that $a_1 \sim a$, $a_2 \sim a$ but not necessarily that $a_1 \sim a_2$. In fact, this may belong in a different equivalence class also. So our relation might not represent a partition of the set. We might define a relation such that $|a - b| < 2 \iff a \sim b$. Notice that $a \sim a$, if $a \sim b$, then $|a - b| < 2 \implies |b - a| < 2 \implies b \sim a$. As for the transitivity, we have that $4 \sim 3$, $3 \sim 2$, but $4 \nsim 2$ since $|4 - 2| \not< 2$.

**Exercise 6**: Define a relation $\sim$ on the set $\mathbb{R}$ of real numbers by setting $a \sim b \implies b - a \in \mathbb{Z}$. Prove that this is an equivalence relation, and find a 'compelling' description for $\mathbb{R}/\sim$. Do the same for the equivalence relation $\equiv$ on the plane $\mathbb{R} \times \mathbb{R}$ defined by declaring $(a_1, a_2) \equiv (b_1, b_2) \implies b_1 - a_1 \in \mathbb{Z}$ and $b_2 - a_2 \in \mathbb{Z}$.

*Answer.* (Part I) We just need to check the properties. Notice that $a - a = 0$ so $a \sim a$. Also, if $a - b = z \in \mathbb{Z}$, then we conclude that $b - a = -z \in \mathbb{Z}$. Therefore, the symmetry property is satisfied. Suppose that $a - b = z_1 \in \mathbb{Z}$ and that $b - c = z_2 \in \mathbb{Z}$. Then $a - c = z_1 + z_2 \in \mathbb{Z}$ showing the transitive property. The equivalence classes would look something like $[a]$ for $|a| < 1$ since elements that are related are ones that have the same decimal part.

(Part II) We will check the properties for this also. Notice that it is reflexive as $(a_1, a_2) - (a_1, a_2) = (0, 0) \in \mathbb{Z} \times \mathbb{Z}$. Now note that it is also symmetric since we would take the negative of both parts when reversing the relation which is also in $\mathbb{Z}$. To prove transitivity, suppose $(a_1, a_2) \approx (b_1, b_2)$ and $(b_1, b_2) \approx (c_1, c_2)$. Then we have that $b_1 - a_1 = z_1 \in \mathbb{Z} \wedge c_1 - b_1 = z_2 \in \mathbb{Z}$. This means that $c_1 - a_1 = z_2 + z_1 \in \mathbb{Z}$. The same argument works for the second component. Therefore, $(a_1, a_2) \approx (c_1, c_2)$.

## 1.2 Functions Between Sets

**Definition 1.2.1**

**Functions**

A function is one which takes an element from one set, mapping it to an element of another set. The definition will be based on the idea of a *graph* of $f$, our function:

$$\Gamma_f := \{(a, b) \in A \times B : b = f(a)\} A \times B$$

The restrictions on such a construction is that

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

So each element of $A$ is sent to one element in $B$. We also have the identity function, mapping every element to itself:

$$\mathrm{id}_A : A \to A$$

This naturally leads to the idea that if we have a subset of $A$, $S$, the identity would be sending every element of $s \in S$ to itself. If $S$ is a subset of $f$, then we have

$$f(S) := \{b \in B : (\exists a \in A)\, b = f(a)\}$$

This is the set of elements in the image of the mapping $f : S \to B$. In other words, this is a domain restriction which we denote by

$$(\forall s \in S) :\ f|_S\,(s) = f(s)$$

- Multisets: A multiset has multiple elements in one set. It can be defined by a function from a set to $\mathbb{N}_{>0}$ which maps an element to the number of occurrences of that element in that set.
- Indices: We can consider indices as functions also where if we consider $a_1, a_2, \ldots, a_n$, what we are meaning is a function

  $$a : \{1, \ldots, n\} \to \mathbb{Z} \ldots$$

  Where the RHS is where we have our elements of $a_i$. This means that we can have some $a_i = a_j$ or as $a_i$'s distinct.

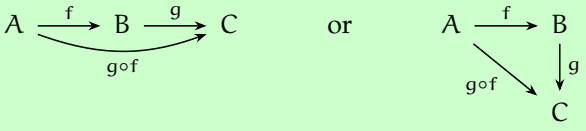
**Definition 1.2.2**

**Composition of functions**

Functions can be composed if $f : A \to B$ and $g : B \to C$ are functions. There are operations $f \circ g$ such as:

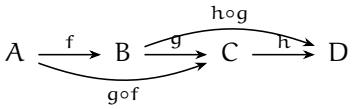
$$(\forall a \in A)\,(g \circ g)(a) := g(f(a))$$

that is, we use $f$ to go from $A$ to $B$ and then $g$ to go from $B$ to $C$. Here is a graphical representation:




We say that diagrams such as one drawn above commute if we start from $A$ and travel to $C$ in any of the two ways applying the functions along the way give rise to the same result.

Also note that composition is associative, where if we have $f : A \to B$, $g : B \to C$, and $h : c \to D$ which are functions, then $h \circ (g \circ f) = (h \circ g) \circ f$. This is the diagram:




which commutes. This diagram says that $(g \circ f) \circ h = f \circ g \circ h = f \circ (g \circ h)$.

The identity function has two representations with respect to composition. Let $f : A \to B$, then we have $\mathrm{id}_B \circ f = f$ and $f \circ \mathrm{id}_A = f$. This is represented by the diagrams:


which commute.

**Definition 1.2.3** **Injections, Surjections, Bijections**

We have special types of functions:

- A function $f : A \to B$ is *injective* if

$$a' \neq a'' \implies f(a') \neq f(a'')$$

  that is, $f$ sends different elements to different elements.

- A function $f : A \to B$ is *surjective* if

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

  of that $f$ covers the whole of $B$.

For injections, we draw $\hookrightarrow$ and for surjections, we draw $\twoheadrightarrow$.

If $f$ is both injective and surjective, we say that it is bijective and we write $f : A \tilde{\to} B$, or

$$A \cong B$$

and we say that $A, B$ are isomorphic sets.

This allows us to consider 'disjoint unions' which are the 'copies' $A', B'$ of the sets $A, B$, which we should consider as isomorphic sets to $A, B$. For example, we can take a copy defined by a bijective function:

$$f : A \to 0 \times A$$

defined by

$$(\forall a \in A)\, f(a) = (0, a)$$

**Definition 1.2.4** **Injections, Surjections, Bijections: Second Viewpoint**

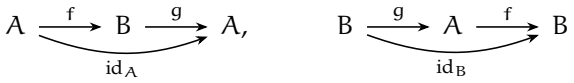
We can also note that if $f : A \to B$ is a bijection, we can flip the graph and define

$$g : B \to A$$

where we have $a = g(b)$ when $b = f(a)$. Since $f$ is injective, we guarantee that no element in $B$ gets mapped to two elements by $g$. Since the map is surjective, the

mapping given by $g$ is defined over the entire domain $B$. So $g$ is a function.

The graphical representation of $g$ is interesting:




which both commute, so we actually have bidirectional arrows and $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. The first identity shows that $g$ is a left-inverse of $f$ while the second shows that it is also a right-inverse. We way that it is the inverse of $f$ which is denoted as $f^{-1}$. Is the converse true? That if a function has an inverse that it is a bijection?

**Proposition 2.1**: *Assume* $A \neq \emptyset$, and let $f : A \to B$ be a function. Then

1. $f$ has a left-inverse if and only if it is injective.
2. $f$ has a right-inverse if and only if it is surjective.

*Proof.* (Part I) ($\to$) If $f : A \to B$ has a left-inverse, then there exists a $g : B \to A$ such that $g \circ f = \mathrm{id}_A$. Now suppose that $a' \neq a''$ are arbitrary different elements of $A$. Then

$$g(f(a')) = \mathrm{id}_A(a') = a' \neq a'' = \mathrm{id}_A(a'') = g(f(a''))$$

So as $g$ sends $f(a')$ and $f(a'')$ to different elements, $f(a') \neq f(a'')$.

($\leftarrow$) Now suppose that $f : A \to B$ is injective. The we construct a function $g : B \to A$ by assigning a unique value $g(b) \in A$ for each element $b \in B$. Choose a fixed element in $s \in A$

$$g(b) := \begin{cases} a & \text{if } b = f(a) \text{ for some } a \in A \\ s & \text{if } b \notin \mathfrak{I}f. \end{cases}$$

So if $b$ is the image of some element in $A$, then we send it back to that element. Otherwise, you send it to some fixed $A$. So every $b \in B$ is sent to a well-defined element in $A$. It can also be seen that $g$ is a left inverse of $g$. The proof of (2) is left as an exercise (Exercise 2.2). □

**Corollary 2.2**: A function $f : A \to B$ is a bijection if and only if it has a two-sided inverse.

A function that is injective will have many left-inverses and a function that is surjective will have many right-inverses. These are called sections.

The proposition shows something deep. The definition of injective and surjective maps looks at elements of sets, and how these functions are organized based on our sets. The definition of elements could be vague but ideas about injectivity and surjectivity could be deduced as properties of functions. They could be seen as a way of comparing sets.

One extra note on bijections, we denote the inverse of $f$ to be $f^{-1}$ where $f : A \to B$ and if $T \subseteq B$, then we write

$$f^{-1}(T) = \{a \in A : f(a) \in T\}$$

If $T = \{q\}$ is a singleton set, we can write $f^{-1}(T) = f^{-1}(q)$ which is called a *fiber* of $f$ over $q$. So a function $f : A \to B$ is a bijection if it has non-empty fibers over all elements of $B$ and that each of these fibers are singletons.

**Definition 1.2.5** **Monomorphism**

A function $f : A \to B$ is a *monomorphism* if the following holds:

$$\text{for all sets } Z \text{ and all functions } \alpha', \alpha'' : Z \to A$$
$$f \circ \alpha' = f \circ \alpha'' \implies \alpha' = \alpha''$$

We can look at this definition and notice that it looks like the injective requirement for a function.

**Proposition 2.3**: A function is injective if and only if it is a monomorphism.

*Proof.* ($\to$) If it is injective, it has a left inverse $g : B \to A$. Therefore, we have that

$$\begin{aligned} g \circ (f \circ \alpha') &= g \circ (f \circ \alpha'') \\ id_A \circ \alpha' &= id_A \circ \alpha'' \\ \alpha' &= \alpha'' \end{aligned}$$

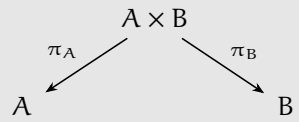
($\leftarrow$) Now suppose that $f$ is a monomorphism. To show injectivity, we only need to look at one element. So choosing $Z = p$, we have that

$$\begin{aligned} f \circ \alpha'(p) &= f \circ \alpha''(p) \\ \alpha'(p) &= \alpha''(p) \\ a' &= a'' \end{aligned}$$

which is by definition of an injective function. □

It is to be expected that there would be a definition as such for a surjective function. This is known as an *epimorphism* which will be proved in Exercise 2.5.

**Example 1.2.1:** If $A, B$ are sets, then the natural projections

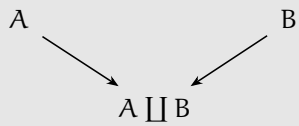



are defined by

$$\pi_A((a, b)) := a,\ \pi_B((a, b)) := b$$

for all $(a, b) \in A \times B$. These maps are definitely surjective.

**Example 1.2.2:** There are also injections from $A$ and $B$ to the disjoint union.




obtained by sending $a \in A$ to the element in the isomorphic copy in $A \coprod B$.

**Example 1.2.3:** If $\sim$ is an equivalence relation on a set $A$, there is a canonical projection

$$A \to A/\sim$$

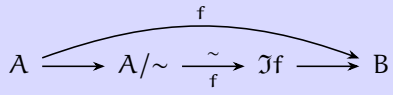
by sending the element $a$ to its equivalence class: $[a]$.

**Example 1.2.4:** Canonical decomposition. Injective and surjective functions allow us to construct any function. We note that every function $f : A \to B$ determines an equivalence relation: for all $a', a'' \in A$,

$$a' \sim a'' \iff f(a') = f(a'')$$

**Theorem 1.2.1** **First Isomorphism Theorem**

Let $f : A \to B$ be any function, and define $\sim$ as above. Then $f$ decomposes as follows




We have that the first function is the canonical projection $A \to A/\sim$. The third one is the identity from $Jf \subseteq B$. Out goal is to quotient out all the non-injective domain values, that is each equivalence class to one value in $b$. We represent each equivalence class by one member, and therefore, out middle mapping is defined by

$$\tilde{f}([a]_\sim) := f(a)$$

for all $a \in A$. Observe that this formula for $\tilde{f}$ is ambiguous, as we need to make sure that we get the same output for any representative of out equivalence class. We also need to prove that this formula is a function and defines a bijection.

*Proof.* Observe that by the defined equivalence class, for $a', a'' \in A$, we need to prove that to show that equivalence representatives do not matter

$$[a']_\sim = [a'']_\sim \implies f(a') = f(a'')$$

Since $[a']_\sim = [a'']_\sim$ means that $a' \sim a''$, we have that $f(a') = f(a'')$. Therefore, our choice of representatives does not matter.

Now we have to show that $\tilde{f}$ is a bijection: $\tilde{f} : A/\sim \to Jf$. For the injective part, we reason that if $\tilde{f}([a]) = \tilde{f}([b])$, then we must have that they are the same equivalence class. We note that $\tilde{f}([a])$ is just $f(a)$ and $\tilde{f}([b])$ is $f(b)$. Now using the equivalence relation we defined, we have that $a \sim b$. Therefore, $[a] = [b]$.

For surjectivity, we recall our function: $\tilde{f} : A/\sim \to Jf$. Let $b \in Jf$ be arbitrary. Notice that we only lose elements in $A/\sim$ which map to the same element. So we should in theory still have a surjective map that is 'minimal'. Namely, we note that $f(a) = b$. Therefore, we take $f([a]) = b \in Jf$. □

The proof is very interesting as it shows that we can define an equivalence relation on the elements in $A$ that map to the same element in $B$. And this actually gives us a bijection if we remove these elements. To conclude, we can decompose any function into one that is surjective function, a bijection, then an inclusion map/injection.

On a side note, notice that the definition of a disjoint union can have several choices for our copies of $A', B'$. This tells us that $A \coprod B$ is not will-defined, yet we will realize that $A \coprod B$ is well-defined up to isomorphism: Any two choices for $A', B'$ will lead to isomorphic candidates for $A \coprod B$. This applies to quotients and products.

**Problem Sets**

**Exercise 1**: How many different bijections are there between a set $S$ with $n$ elements and itself?

*Answer.* We start by labeling the elements $1, \ldots, n$. Then we have $n!$ choices.

**Exercise 2**: Prove statement (2) in Proposition 2.1, that is that $f : A \to B$ has a right-inverse if and only if it is surjective.

*Answer.* (Part I) Suppose that $f$ has a right-inverse, $f^{-1} : B \to A$. We take an arbitrary element of $B$, called $b$. Now observe that

$$\begin{aligned} f \circ f^{-1}(b) &= b \\ f(a) &= b \end{aligned}$$

Therefore, $f$ is surjective.

(Part II) Now suppose that $f$ is surjective. Consider the decomposition equivalence relation such that

$$a' \sim a'' \iff f(a') = f(a'')$$

Consider the mapping $f' : B \to A/\sim$ by:

$$f' := b \mapsto [a] : f(a) = b$$

Now we consider the mapping $f'' : A/\sim \to A$ by:

$$f'' := [a] \mapsto a$$

Notice that now, our function $f''f'$ is our $f^{-1}$ function. Take an arbitrary $b \in B$ where $f(a) = b$. Now plug in:

$$ff''f'(b) = ff''([a]) = f(a) = b$$

So it is the identity on $B$.

**Exercise 3**: Prove that the inverse of a bijection is a bijection and that the composition of two bijections is a bijection.

*Answer.* (Part I) We note that $f : A \to B$ is a bijection then it is both injective and surjective. What follows is that by definition, $f^{-1} : B \to A$ is such that $f \circ f^{-1} = \mathrm{id}_A$ and $f^{-1} \circ f = \mathrm{id}_B$. But by definition, $f^{-1}$ has a left and right inverse which is $f$. So $f^{-1}$ is a bijection.

(Part II) Suppose that we have two bijections $f, g$. A left-inverse for both exists so a left inverse of $f \circ g$ exists, namely $g^{-1} \circ f^{-1}$. The same for a right-inverse. And we're done.

**Exercise 4**: Prove that 'isomorphism' is an equivalence relation (on any set of sets).

*Answer.* This is asking that if we consider a set of sets, then two sets are considered isomorphic can define an equivalence relation. To do this, define the relation as

$$A \sim B \iff \exists f(f : A \to B \wedge \exists f^{-1}(f \circ f^{-1} = I \wedge f^{-1} \circ f = I))$$

So using this, we note that the relation is reflexive as a set is isomorphic to itself, take the identity function:

$$\mathrm{id}_A : A \to A$$
$$\mathrm{id}_A := a \mapsto a$$

Now suppose that we have $A \sim B$. We note that $B \sim A$ since the bijection going from $B \to A$ is the inverse. We proved previously that inverse of bijections were bijective. For the transitive property, we also proved that the composition of bijections were bijections. We are done.

**Exercise 5**: Formulate a notion of *epimorphism*, in the style of the notion of *monomorphism* seen in 2.6, and prove a result analogous to Proposition 2.3, for epimorphisms and surjections.

**Definition 1.2.6**

**Epimorphism**

A function $f : A \to B$ is an epimorphism if for all functions $a'' : Z \to B$, there exists a function $a' : Z \to A$ such that

$$f \circ a' = a''$$

**Proposition**: A function $f$ is surjective iff it is an epimorphism.

*Proof.* (Part I) Suppose that $f$ is a surjection. Then we have that for any $b \in B$, there exists an $a \in A$ such that $f(a) = b$. Notice that each function $a''$ is determined by individual mappings of $z_i \mapsto b_i$. We consider just one. We observe that there exists an $a_i$ such that $f(a_i) = b_i$. Therefore, we construct our $a'$ by the mapping of $z_i \mapsto a_i$.

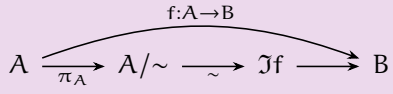
(Part II) Suppose that $f$ is an epimorphism. We take an arbitrary $a'' : Z \to B$. We know there exists a mapping $a' : Z \to A$. Consider a single mapping $z \mapsto b$ by $a''$. We know that $z \mapsto a_0$ since

$$a'' = f \circ a'$$

So that means that we must have $f(a_0) = z$. Therefore, our $f$ is surjective. □

**Exercise 6**: With notation as in Example 2.4, explain how any function $f : A \to B$ determines a section of $\pi_A$.

*Answer.* We have that the function can be decomposed into a surjective, then bijective, then injective map:




We note that $a' \sim a''$ if and only if $f(a') = f(a'')$. So we have that the equivalence classes are determined by the 'injectivity' of $f$.

**Exercise 7**: Let $f : A \to B$ be any function. Prove that the graph $\Gamma_f$ of $f$ is isomorphic to $A$.

*Answer.* Leave for later.

**Exercise 8**: Describe as explicitly as you can all terms in the canonical decomposition of the function $\mathbb{R} \to \mathbb{C}$ defined by $r \mapsto e^{2\pi i r}$.

*Answer.* Leave for later.

**Exercise 9**: Show that if $A' \cong A''$ and $B' \cong B''$, and further $A' \cap B' = \emptyset$ and $A'' \cap B'' = \emptyset$, then $A' \cup B' \cong A'' \cup B''$. Conclude that the operation $A \coprod B$ is well-defined up to isomorphism.

*Answer.* Leave for later.

**Exercise 10**: Show that if $A$ and $B$ are finite sets, then $|B^A| = |B|^{|A|}$.

*Answer.* Leave for later.

**Exercise 11**: In view of Exercise 2.10, it is not unreasonable to use $2^A$ to denote the set of functions from an arbitrary set $A$ to a set with 2 elements (say $\{0, 1\}$). Prove that there is a bijection between $2^A$ and the *power set* of $A$.

*Answer.* Leave for later.

## 1.3 Categories

A category is a collection of objects and the morphisms between them. Such a definition is vague to expand the number of objects that can be categories. For example, there is no such thing as a set of all sets which we found a counterexample to in Russell's paradox.

It is possible to define a universe which contains all categories and objects. What will be worked with is a class, which is a category and sometimes a set.

**Definition 1.3.1** **Category**

A category $C$ consists of

- a class $\mathrm{Obj}(C)$ of objects of the category, and
- for every two objects $A, B$ of $C$, a set $\mathrm{Hom}_C(A, B)$ of morphisms, with the properties listed below.

You can think of the objects as sets and the morphisms as functions. Here are the properties of morphisms:

- For every object $A$ of $C$, there exists a morphism $1_A \in \mathrm{Hom}_C(A, A)$, the identity on $A$.
- One can compose morphisms: two morphisms $f \in \mathrm{Hom}_C(A, B)$ and $g \in \mathrm{Hom}_C(B, C)$ determine a morphism $gf \in \mathrm{Hom}_C(A, C)$. So for every triple of objects $A, B, C$ of $C$ there is a function (of sets)

$$\mathrm{Hom}_C(A, B) \times \mathrm{Hom}_C(B, C) \to \mathrm{Hom}_C(A, C)$$

  and the image of the pair $(f, g)$ is denoted $gf$.
- This 'composition law' is associative: if $f \in \mathrm{Hom}_C(A, B)$, $g \in \mathrm{Hom}_C(B, C)$, and $h \in \mathrm{Hom}_C(C, D)$, then

$$(hg)f = h(gf)$$

- The identity morphisms are identities with respect to composition: that is for all $f \in \mathrm{Hom}_C(A, B)$ we have

$$f1_A = f,\ 1_B f = f$$

It is also required that $\mathrm{Hom}_C(A, B)$ and $\mathrm{Hom}_C(C, D)$ are disjoint unless $A = C, B = D$. We define an endomorphism to be $\mathrm{Hom}_C(A, A) = \mathrm{End}_C(A)$, the set of morphisms from an object to itself. This set is closed under composition.

A commutative diagram is that between morphisms such that any traversal direction of compositions will lead to the same result. A diagram is the set of objects of a category and the morphisms between these objects.

**Example 1.3.1:** To denote a category of sets, this notation will be used: Set

- $\mathrm{Obj}(\mathrm{Set})$ = the class of all sets;
- for $A, B$ in $\mathrm{Obj}(\mathrm{Set})$ (that is, for $A, B$ sets) $\mathrm{Hom}_{Set}(A, B) = B^A$.

**Example 1.3.2:** Another example is where $S$ is a set, $\sim$ is relation on $S$ which is reflexive and transitive. The category is defined as follows:

- *objects*: the elements of $S$;
- *morphisms*: if $a, b$ are objects (that is, if $a, b \in S$), then let $\mathrm{Hom}(a, b)$ be the set consisting of the element $(a, b) \in S \times S$ if $a \sim b$, and let $\mathrm{Hom}(a, b) = \emptyset$ otherwise.

In this category, there are not many morphism: one for any pair of objects and none for unrelated objects. We would then define a composition of morphisms and see if the conditions in Definition 1.3.1 are satisfied. We require that there is the identity morphism in every $\mathrm{End}_C(A)$ set, compositions exist in the category, the composition is associative, and that the identity works with composition:

- For the first condition, if $a \in S$ we require that
$$1_a \in \mathrm{Hom}(a, a).$$
But since $a \sim a$ as our relation is reflexive, this is satisfied, therefore, we conclude that
$$1_a = (a, a) \in \mathrm{Hom}(a, a)$$

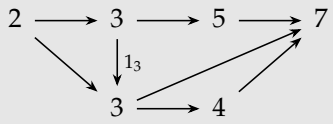
- Now for composition, we require that if we have
$$f \in \mathrm{Hom}(a, b),\ g \in \mathrm{Hom}(b, c);$$
then there is $gf \in \mathrm{Hom}(a, c)$. Since $f \in \mathrm{Hom}(a, b)$, the set $\mathrm{Hom}(a, b) \neq \emptyset$, therefore, $f = (a, b)$, and $g = (b, c)$. But looking at equivalence relations, we find that
$$a \sim b \wedge b \sim c \implies a \sim c$$
since we noted that $\sim$ was transitive. Therefore, $(a, c) \in \mathrm{Hom}(a, c)$ and
$$gf = (a, c) \in \mathrm{Hom}(a, c)$$

- We now check associativity, that is if $f \in \mathrm{Hom}(a, b), g \in \mathrm{Hom}(b, c)$, and $h \in \mathrm{Hom}(c, d)$, then
$$f = (a, b),\ g = (b, c),\ h = (c, d)$$
so we consider
$$f(gh) = (fg)h$$
which we solve for:
$$gh = (b, d),\ fg = (a, c)$$
and upon observation, our morphisms are indeed associative.

- To show that the identity morphisms are identities wrt composition, we suppose that $f \in \mathrm{Hom}(a, b)$ and that the identity morphisms are $1_a = (a, a), 1_b = (b, b)$:
$$1_b f := a \mapsto b \mapsto b$$
which goes the same for $1_a$.

One example of such a category is the equivalence relation $=$, where all morphisms are exactly the identity morphisms. Such categories are called *discrete*.

Another example is the relation $\leqslant$, to which we obtain



These categories are special in that all diagrams that are drawn from them are commutative. This is not often the case, such as in Set.

**Example 1.3.3:** Another category is where if $S$ be a set, the category $\hat{S}$:

- $\mathrm{Obj}(\hat{S}) = \mathcal{P}(S)$, the power set $S$
- for $A, B$ objects of $\hat{S}$ (that is, $A \subseteq S$ and $B \subseteq S$) let $\mathrm{Hom}_{\hat{S}}(A, B)$ be the pair $(A, B)$ if $A \subseteq B$, and let $\mathrm{Hom}_{\hat{S}}(A, B) = \emptyset$ otherwise.

The identity $1_A$ consists of the pair $(A, A)$, which is the only morphism from $A$ to $A$. We also have composition as the relation $\subseteq$ is transitive. The same goes for associative, as the order in which we view the subset relation does not change the subset relationship. Now let $1_B$ be $B \to B$ and $f \in \mathrm{Hom}_{\hat{S}}(A, B)$. We must have that $f = (A, B)$. So we look at

$$1_B f = A \to B \to B$$

which is just

$$A \to B = f$$

The same argument can be made for $1_A$.

**Example 1.3.4:** This example will be abstract but will recur a lot. Let $C$ be a category and let $A$ be an object of $C$. The category $C_A$ will have objects which are certain morphisms of $C$ and the morphisms are certain diagrams of $C$.

- $\mathrm{Obj}(C_A)$ = all morphisms form any object of $C$ to $A$. Therefore, any object of $C_A$ will be a morphism $f \in \mathrm{Hom}_C(Z, A)$ for some $Z \in C$. An object of $C_A$ is an arrow $Z \to A$ in $C$ which are draw top down.

$$\begin{array}{c} Z \\ \downarrow f \\ A \end{array}$$

What will the morphisms of $C_A$ look like? My idea: If we take two objects in $C_A$ and the other in $C_B$, then we have $f : Z_1 \to A$ and $g : Z_2 \to B$. If we want to map one to the other, it makes sense to have some morphism $m$ such that $m(f) = g$, where $m : A \to Z_2$. In actuality, the book takes into consideration simpler cases to deduce from there. In fact, my construction was incorrect because $C_A$ consists of objects that specifically send stuff to $A$, and not any other object in $C$. My option was close, but it lacked also the basic symmetry that the book presents:

- Let $f_1, f_2$ be objects of $C_A$, that is, two arrows

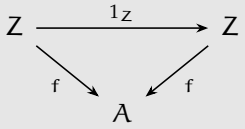
$$\begin{array}{cc} Z_1 & Z_2 \\ \downarrow f_1 & \downarrow f_2 \\ A & A \end{array}$$

  in $C$. Morphisms $f_1 \to f_2$ are defined to be *commutative diagrams*

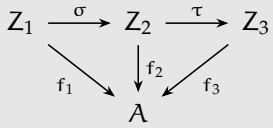
$$\begin{array}{ccc} Z_1 & \xrightarrow{\sigma} & Z_2 \\ & {\scriptstyle f_1}\searrow \quad \swarrow{\scriptstyle f_2} & \\ & A & \end{array}$$

  in the 'ambient' category $C$.

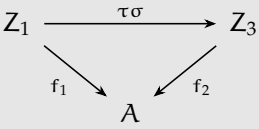
That is, morphisms $f \to g$ correspond precisely to those morphisms $\sigma : Z_1 \to Z_2$ in $C$ *such* that $f_1 = f_2\sigma$. Instead of thinking of these morphisms as a set, we think of these as a collection of diagrams that satisfy the commutative property. To check for the identity, we have the diagram which we get from $C$:



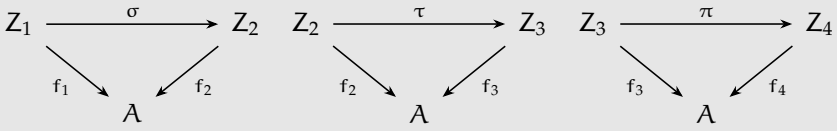

which commutes because C is a category. If we look at composition, $f_1 \to f_2 \to f_3$, we can put two diagrams side by side to get $f_1 \to f_3$:



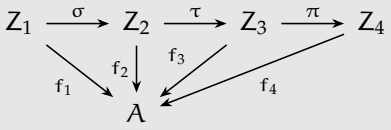

and then since C is a category, the diagram commutes, so we have




So the composition exists. To check associativity, we consider morphisms $\sigma, \tau, \pi$ defined as $Z_1 \to Z_2$, $Z_2 \to Z_3$, $Z_3 \to Z_4$ respectively and we draw a commutative diagram each:




Piecing this all together, we get




As this is a commutative diagram, we note that the grouping of the morphisms do not matter. Such a category is called a *slice category*.

**Example 1.3.5:** Let us apply this construction of a category to that in Example 3.3, where $S = \mathbb{Z}$ and $\sim$ is the relation $\leqslant$. Choose $A = 3$, an integer and the objects of $C_A$ are the morphisms in C which send stuff to 3. So we have the pairs $(n, 3)$ for $n \leqslant 3$. We have the morphism

$$(m, 3) \to (n, 3)$$

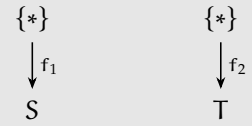
if and only if $m \leqslant n$. In this case, $C_A$ may be considered as the subcategory of integers $\leqslant 3$, with the 'the same' morphisms as in C.

**Example 1.3.6:** Another example are the morphisms obtained from morphisms in a category C which go from a fixed object A to any element in C. These are called *coslice categories*.

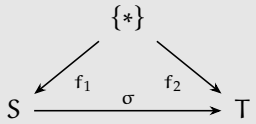
**Example 1.3.7:** A concrete example of a category for 3.7 is where C = Set and A = a fixed singleton $\{*\}$. Call the resulting category $\text{Set}^*$.

- an object of $\text{Set}^*$ is therefore a morphism $f : \{*\} \to S \in \text{Set}$. The object in Set must be nonempty and is the element $f(*)$. So the objects can be denoted as $(S, s)$ where S is the set and s is any object in S. Now a morphism between two objects $(S, s) \to (T, t)$ is a set-function $\sigma : S \to T$ such that $\sigma(s) = t$. Verify this:

The goal is to map a given morphism defined as $(S, s)$ to $(T, t)$. We also note that our singleton is fixed. So we have two given objects denoted as




So we require a morphism that maps $f_1 \mapsto f_2$ and considering the diagram, we attempt to construct a composition:

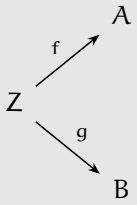



So following the commutative diagram, we have that the mapping is such that $\sigma$, as desired.

The objects of $\mathrm{Set}^*$ are called 'pointed sets'. One example is that a group $G$ has an identity $e_G$, and that the group homomorphisms will be functions which send identities to identities meaning that they are morphisms of pointed sets.

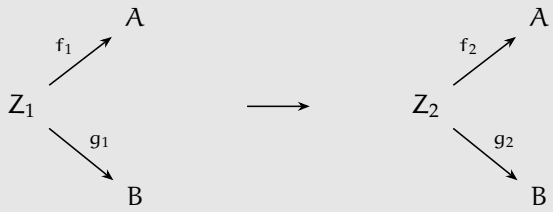
**Example 1.3.8:** We will define a new category given a category $C$, objects $A, B$ by

- $\mathrm{Obj}(C_{A,B})$ = diagrams

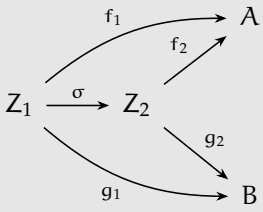



in $C$; and

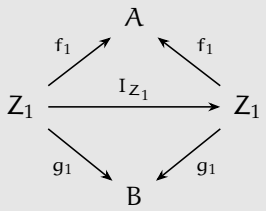
- morphisms



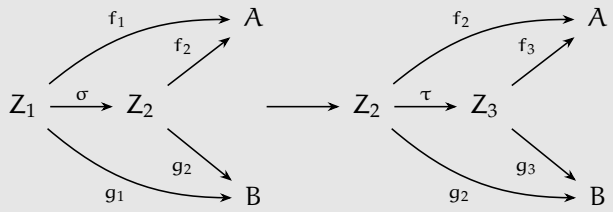

are commutative diagrams



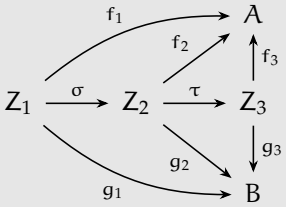

Observe that this is an application of $C_A$ and $C_B$ categories. Instead of considering singleton functions as objects, considering multiple gives us a diagram, and the morphisms are the commutative diagrams such that $\sigma$ satisfies the commutative condition. We first consider if an identity exists from a diagram to itself. This would be an identity on functions, and the morphism on sets that we desire is the identity from our category, namely, the identity diagram is



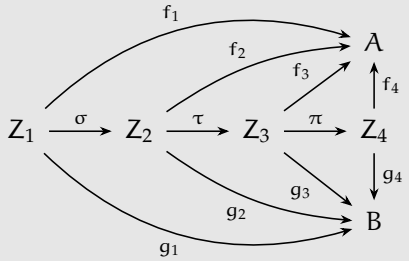

What would the composition of diagrams look like? Suppose we have one diagram such that $\sigma : f_2 \mapsto f_1$ and another such that $\tau : f_3 \mapsto f_2$, the same for $g_1$ and $g_2$:




So the composition of morphisms is now clear:




What does it mean to be associative? If we generalize this to a commutative diagram of three morphisms:




We can try to understand by traversing the diagram. Notice that our end goal is to get the mapping $f_1 : Z_1 \to A$. We follow the first two commutative diagrams, first by $\sigma$ then by $\tau$, and finally, with our input, $f_3$. So we have such that $f_3 \mapsto f_1$. Now if we do the innermost function, we have $\pi(f_4) = f_3$. So we get $(\sigma\tau)(\pi(f_4)) = f_1$. Notice that if we do the same the other direction, it works also.

It is clear that if we compose the identity diagram above, that we would get the same commutative diagram. We have verified that this is a category.

Cool note: if we flip the arrows on the diagrams, we would get the alternate *coslice diagram*. This is observed by how instead of the diagram requiring simultaneously that

$$f_1 = f_2\sigma \qquad\qquad g_1 = g_2\sigma$$

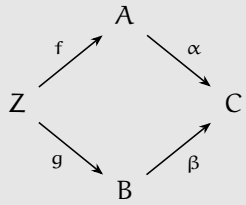
we instead reverse the composition to obtain

$$f_1 = \sigma f_2 \qquad\qquad g_1 = \sigma g_2$$

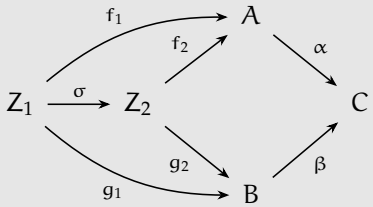
which is exactly as seen in the *coslice* example.

**Example 1.3.9:** We will consider the *fibered* version of $C_{A,B}$ and $C^{A,B}$. The ultimate test of understanding! Start with a given category C, and choose two fixed *morphisms* $\alpha : A \to C$, $\beta : B \to C$ with the same target C. We then consider a category $C_{\alpha,\beta}$ as follows:

- $\mathrm{Obj}(C_{\alpha,\beta})$ = *commutative diagrams*




- morphisms correspond to commutative diagrams

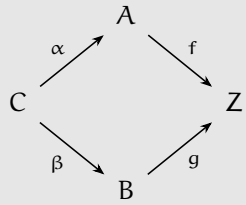



The identities and compositions of such a morphism should be considered. We observe that if there are two objects that are the same, the morphism between them that is the identity would just be a mapping of the identity on Z. In the composition of morphisms, we just extend leftward with another set $Z_0$ and write the outermost composition function $\tau$.

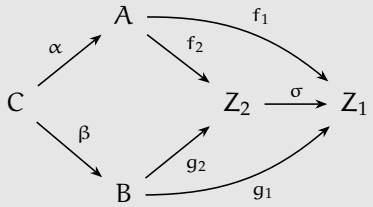
Now left to the reader is the construction of the mirror of this from two morphisms $\alpha : C \to A$, $\beta : C \to B$ with common source.

We define the fibered version of $C^{\alpha,\beta}$ as follows:

- $\mathrm{Obj}(C_{\alpha,\beta})$ =*commutative diagrams*




- morphisms correspond to commutative diagrams




This is essentially a reversing of the arrows on the previous fibered diagram.

**Problem Sets**

**Exercise 1**: Let $C$ be a category. Consider a structure $C^{op}$ with

- $\mathrm{Obj}(C^{op}) := \mathrm{Obj}(C)$;
- for $A, B$ objects of $C^{op}$ (hence objects of $C$), $\mathrm{Hom}_{C^{op}}(A, B) := \mathrm{Hom}_C(B, A)$.

Show how to make this into a category (that is, define composition of morphisms in $C^{op}$ and verify the properties listed in Definition 1.3.1).

*Answer.* If we have two morphisms $f \in \mathrm{Hom}_{C^{op}}(A, B)$, $f \in \mathrm{Hom}_{C^{op}}(B, C)$, then we note that $f \in \mathrm{Hom}_C(B, A)$ and $g \in \mathrm{Hom}_C(C, B)$. Therefore, we define the composition of morphisms to be

$$f \circ g : C \to A \in \mathrm{Hom}_{C^{op}}(A, C)$$

What happens with the identity morphisms? We know that $C$ is a category, so since $\mathrm{Hom}_{C^{op}}(A, A) := \mathrm{Hom}_C(A, A)$, the identity exists as the same identity from $C$. Note that the morphisms are associative as associativity is inherited from the associativity of $C$. Now to check that the identity is the identity with respect to composition, it is trivially inherited from $C$ also.

The category $C^{op}$ is essentially the category obtained by reversing the arrows on $C$. This tells us that $C$ is a category iff $C^{op}$ is.

**Exercise 2**: If $A$ is a finite set, how large is $\mathrm{End}_{\mathrm{Set}}(A)$?

*Answer.* If $A$ is finite, we simply have all the morphisms that go between $A$ and itself. So from one of the previous exercises, this is $|A|!$.

**Exercise 3**: Formulate precisely what it means to say that $1_a$ is an identity with respect to composition in Example 3.3, and prove this assertion.

*Proof.* For $1_a$ to be the identity, we require that for any morphism $f \in \mathrm{Hom}(a, b)$, we have that

$$f \circ 1_a = f$$

This is true as since $1_a$ is the identity, we have that $a \mapsto a$ and for $f$, this is also a singleton map $a \mapsto b$ as $a \sim b$ and $a \sim a$. We see that

$$f \circ 1_a = a \mapsto a \mapsto b = a \mapsto b = f$$

So it has been proven. □

**Exercise 4**: Can we define a category in the style of Example 3.3 using the relation $<$ on the set $\mathbb{Z}$?

*Answer.* Consider the category $C$ defined as follows:

- $\mathrm{Obj}(C)$ = elements in $\mathbb{Z}$,
- morphisms of $C$ are elements of $\mathrm{Hom}(a, b)$, $a, b \in \mathbb{Z}$. This is the set defined as $(a, b) \in \mathrm{Hom}(a, b) \iff a < b$, and $\mathrm{Hom}(a, b) = \emptyset$ otherwise.

But this does not work as it is not reflexive, that is, that $a \not< a$.

**Exercise 5**: Explain in what sense Example 3.4 is an instance of the categories considered in Example 3.3.

*Answer.* If we consider $\subseteq$ as the relation, we note that it is indeed reflexive and that it is transitive. There is also the fact that each $\mathrm{Hom}(A, B)$ group is of size either 1 or 0, with the same conditions as $\mathrm{Hom}(a, b)$.

**Exercise 6**: Define a category $V$ by taking $\mathrm{Obj}(V) = \mathbb{N}$. (We will leave the reader the task of making sense of a matrix with 0 rows or columns.) Use product of matrices to define composition. Does this category 'feel' familiar?

*Answer.* First, to consider matrices with 0 rows or columns, we define matrices in bijection with the set of linear operators from an $n$ dimensional space to that of a $m$ dimensional space. So to have 0 rows is to go to a zero dimensional space, which is the 0 mapping. To have 0 columns is to map from a 0 dimensional space which means that our function is defined solely by 0: $M(0) = 0$. This is also the 0 map.

The identity map is where we just take the matrix:

$$M = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

The identity map is indeed a identity with respect to composition. We already know that the composition exists in the category, and the composition is associative.

**Exercise 7**: Define carefully objects and morphisms in , and draw the diagram corresponding to composition.

*Answer.* Leave for later.

**Exercise 8**: A *subcategory* $C'$ of a category $C$ consists of a collection of objects of $C$, with morphisms $\mathrm{Hom}_{C'}(A, B) \subseteq \mathrm{Hom}_C(A, B)$ for all objects $A, B$ in $\mathrm{Obj}(C')$, such that identities and compositions in $C$ make $C'$ into a category. A subcategory $C'$ is *full* if $\mathrm{Hom}_{C'}(A, B) = \mathrm{Hom}_C(A, B)$ for all $A, B$ in $\mathrm{Obj}(C')$. Construct a category of *infinite sets* and explain how it may be viewed as a full subcategory of Set.

*Answer.* Define our category of infinite sets as follows:

- $\mathrm{Obj}(C')$ = Sets $S$ such that $|S| = \infty$,
- morphisms in the set, for any two sets $A, B$ in $C'$, $\mathrm{Hom}(A, B)$ such that $f : A \to B \iff f \in \mathrm{Hom}(A, B)$.

Notice that this is the same definition as defined in Set. So this means that if a morphism is in $\mathrm{Hom}_C(A, B)$, such that $A, B$ are infinite sets, then it is also in $\mathrm{Hom}_{C'}(A, B)$. We just need to check that this is a proper category. The identity is indeed inherited from $\mathrm{Hom}_C(A, A)$ for any infinite set $A$ as we just map every element to itself. Suppose that we have two morphisms from arbitrary infinite sets $X, Y, Z$: $f \in \mathrm{Hom}_{C'}(X, Y)$ and $\mathrm{Hom}_{C'}(Y, Z)$. Then it must be that $f : X \to Y$ and that $g : Y \to Z$. Our composition is defined as $g \circ f : X \to Y \to Z$, which exists in $\mathrm{Hom}_{C'}(X, Z)$ by definition. Associativity is inherited from $C$, and the identity property also. We are done.

**Exercise 9**: An alternative to the notion of *multiset* is obtained by considering sets endowed with equivalence relations; equivalent elements are taken to be multiple instances of elements 'of the same kind'. Define a notion of morphism between such enhanced sets, obtaining a category MSet containing (a 'copy' of) Set as a full subcategory. Which objects in MSetdetermine ordinary multisets as defined in 2.2 and how?

*Answer.* Leave for later.

**Exercise 10**: Since the objects of a category C are not (necessarily) sets, it is not clear how to make sense of a notion of 'subobject' in general. In some situations it does make sense to talk about subobjects, and the subobjects of any given objects $A$ in C are in one-to-one correspondence with the morphisms of $A \to \Omega$ for a fixed, special object $\Omega$ of C, called a *subobject classifier*. Show that Set has a subobject classifier.

*Answer.* Leave for later.

**Exercise 11**: Draw the relevant diagrams and define composition and identities for the category $C^{A,B}$ mentioned in Example 3.9. Do the same for the category $C^{\alpha\beta}$ mentioned in Example 3.10.

## 1.4 Morphisms

Just as in Set, we highlight certain types of function (injective, surjective, bijective), and we should do the same for morphisms. Note that defining morphisms by actions on 'elements' is not an option when we are looking at the general case, as objects of categories might not always have 'elements'.

**Definition 1.4.1**

**Isomorphisms**

A morphisms $f \in \mathrm{Hom}_C(A, B)$ is an *isomorphism* if it has a two sided inverse under composition, that is $\exists g \in \mathrm{Hom}_C(B, A)$ such that

$$gf = 1_A,\ fg = 1_B$$

Recall that when the inverse of of a function such as a left-sided inverse is not necessarily unique. Yet, we can guarantee uniqueness through the definition of an isomorphism.

**Proposition 4.2**: The inverse of an isomorphism is unique.

*Proof.* We must show that if we have two inverses $g_1$ and $g_2 : B \to A$, then $g_1 = g_2$. This is done by

$$g_1 = g_1 1_B = g_1(fg_2) = (g_1 f)g_2 = 1_A g_2 = g_2$$

as desired. □

This is needed so that there is no ambiguity of the left-sided inverse vs right-sided inverse when talking about $f^{-1}$.

**Proposition 4.3**: Based on the notation above,

- Each identity $1_A$ is an isomorphism and is its own inverse.
- If $f$ is an isomorphism, then $f^{-1}$ is an isomorphism and further $(f^{-1})^{-1} = f$.
- If $f \in \mathrm{Hom}_C(A, B)$, $g \in \mathrm{Hom}_C(B, C)$ are isomorphisms, then the composition $gf$ is an isomorphism and $(gf)^{-1} = f^{-1}g^{-1}$.

These are verification exercises.

We can create a definition that two objects $A, B$ in a category are isomorphic if they contain a bijection $f : A \to B$. This defines an equivalence relation.

**Example 1.4.1:** Notice that the isomorphisms in the category Set are the bijections.

**Example 1.4.2:** Identities are isomorphisms and they can be the only isomorphisms in a category. In the category C from the relation $\leqslant$ on $\mathbb{Z}$ in Example 1.3.2, we realize the only isomorphic objects are that when comparing the same object $a = a$. We require the morphism $f : a \to b$ and the morphism $g : b \to a$, which implies that $a = b$. So for such an isomorphism to exist, it must be the identity morphism: $1_a$.

**Example 1.4.3:** There are also categories where every morphism is an isomorphism, in which we call the categories *groupoids*.

An *automorphism* of an object $A$ of a category $C$ is an isomorphism from $A$ to itself.

The set of automorphisms of $A$ is denoted $\mathrm{Aut}_C(A)$, which is a subset of $\mathrm{End}_C(A)$. From proposition 4.3, there is structure to be talked about in $\mathrm{Aut}_C(A)$:

- the composition of two elements $f, g \in \mathrm{Aut}_C(A)$ is an element $gf \in \mathrm{Aut}_C(A)$,
- composition is associative,
- $\mathrm{Aut}_c(A)$ contains the element $1_A$, which is an identity for composition
- every element $f \in \mathrm{Aut}_C(A)$ has an inverse $f^{-1} \in \mathrm{Aut}_C(A)$.

This tells us that $\mathrm{Aut}_C(A)$ is a *group*, for all objects $A$ in any category $C$.

Since the objects in a category are varying, there is no way of talking about injectivity and surjectivity as we have previously as set-functions. The previous definitions required the concept of an element. So instead we define *monomorphisms* and *epimorphisms*:

**Monomorphism**

**Definition 1.4.2**

Let C be a category. A morphism $f \in \mathrm{Hom}_C(A, B)$ is a *monomorphism* if the following holds:

$$\textit{for all objects } Z \textit{ of } C \textit{ and all morphisms } \alpha', \alpha'' \in \mathit{Hom}_C(Z, A),$$
$$f \circ \alpha' = f \circ \alpha'' \implies \alpha' = \alpha''$$

and now for epimorphisms:

**Epimorphism**

**Definition 1.4.3**

Let C be a category. A morphism $f \in \mathrm{Hom}_c(A, B)$ is an *epimorphism* if the following holds:

$$\textit{for all objects } Z \textit{ of } C \textit{ and all morphisms } \beta', \beta'' \in \mathit{Hom}_C(B, Z),$$
$$\beta' \circ f = \beta'' \circ f \implies \beta' = \beta''$$

*Note*: My definition of epimorphism was incorrect in one of the homework problems. I can see why this definition of epimorphism is used. The idea of monomorphism was looking at 'injectivity' of the morphisms while looking at morphisms as elements. So for epimorphisms, a plausible idea is to flip this and look at injectivity the 'other way'. It refers to flipping the arrows on a commutative diagram to produce a *coslice category*.

**Example 1.4.4:** What was proven in Proposition 2.3 was that the monomorphisms are the injective functions. Now check that the epimorphisms are the surjective functions.

*Proof.* ($\rightarrow$) Suppose that $f$ is an epimorphism. Suppose that $f$ is not surjective for contradiction. Then there is some $b \in Z$ such that $f(a) \neq b$ for all $a \in B$. Now let the functions $\beta', \beta''$ be such that they map all elements in $\Im f$ to the same thing but $b$ to different things in $Z$. This gives us the contradiction that $f$ is an epimorphism.

($\leftarrow$) Since $f$ is surjective, we know that there is a left-inverse. Therefore, taking the left inverse of both sides shows that $f$ is an epimorphism. □

These definitions for morphisms work as the counterparts to injectivity and surjec-

tivity in categories.

**Example 1.4.5:** In the categories in Example 1.3.2, every morphism was a monomorphism and epimorphism. But there was at most one morphism between any two objects in the category, therefore, the condition for defining monomorphisms and epimorphisms was vacuous.

Consider Example 1.4.5. For example, in Set, the category which contains sets, an isomorphism is a morphism that is both surjective and injective, or is both a monomorphism and an epimorphism. In the category defined by $\leqslant$ on $\mathbb{Z}$, every morphism is both a monomorphism and an epimorphism. The only isomorphisms are identities (Example 1.4.2). This is a feature of Set, which might not be true in every category. It will not hold in the category of rings, but it will in every abelian category. In Set, a function is an epimorphism iff it has a right-inverse. This might not be true in general such as the category Grp of groups.

**Problem Sets**

**Exercise 4.1**: Composition is defined for *two* morphisms. If more than two morphisms are give, for example:

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \xrightarrow{i} E,$$

then one may compose them in several ways, for example:

$$(ih)(gh),\ (i(hg))f,\ i((hg)f),\ \text{etc}$$

so that every step one is only composing two morphisms. Prove that the result of any such nested composition is independent of the placement of the parentheses. (Hint: Use induction on $n$ to show that any such choice for $f_n f_{n-1} \cdots f_1$ equals

$$((\cdots((f_n f_{n-1})f_{n-2})\cdots)f_1)$$

Carefully working out the case $n = 5$ is helpful)

*Proof.* **Base Case**: We will consider the base case with the composition of three morphisms. The statement holds, as we just need to check that $((fg)h) = (f(gh))$ which is true as composition is associative.

**Inductive Case**: Suppose that we have $f_n f_{n-1} \cdots f_1$ such that $n > 3$. Consider the form:

$$((\cdots((f_n f_{n-1})f_{n-1})\cdots)f_1).$$

Notice that we can treat $f_n f_{n-1}$ as just one morphism $g_{n-1}$. But by the inductive hypothesis, we claim that we can rearrange the parentheses of this product to our liking. So we wrap $g_{n-1}$ with the morphism immediately to the right of it:

$$((\cdots((g_n f_{n-2})f_{n-2})\cdots)f_1)$$

And by the associative law, we now compose

$$((\cdots((f_n(f_{n-1}f_{n-2})))\cdots)f_1)$$

Notice that we can repeat this process however many times to get the innermost composition between any arbitrary $f_i f_{i-1}$. So since $(f_i f_{i-1})$ is just 1 morphism after composition, we have reduced it to the previous case. We are done. □

**Exercise 2**: In Example 1.3.2 we have seen how to construct a category from a set endowed with a relation, provided this latter is reflexive and transitive. For what types of relations is the corresponding category a groupoid (every morphism is an isomorphism)?

*Answer.* In the category with the set $\mathbb{Z}$ from which we draw the elements of $C$ and the morphisms defined by $\leqslant$, we notice that some morphisms were not necessarily isomorphisms, specifically the ones that are not identities. This is because our relation is not symmetric. That is, in general, we do not have

$$a \leqslant b \wedge b \leqslant a$$

So what happens if we include symmetry as a requirement? The we must have that $a \sim b$ and $b \sim a$. This tells us that any morphism $f$ is invertible. So $f$ is an isomorphism. We can probably also conclude the converse. Every set $\mathrm{Hom}_C(a, b)$, has either 1 or 0 elements. We will prove the contrapositive. Suppose that there exists a morphism that does not have an inverse. That must mean that if $f \in \mathrm{Hom}_C(a, b)$, the set $\mathrm{Hom}_C(b, a)$ must be empty. This means that $a \sim b$ but $b \nsim a$. So there exists two elements that do not have the symmetric property. So we have proven the contrapositive.

**Exercise 4.3**: Let $A, B$ be objects of a category $C$, and let $f \in \mathrm{Hom}_C(A, B)$ be a morphism.

- Prove that if $f$ has a right-inverse, then $f$ is an epimorphism.

  *Proof.* Suppose that $f \in \mathrm{Hom}_C(A, B)$ and consider arbitrary morphisms $a', a'' \in \mathrm{Hom}_C(Z, A)$. Now since $f$ has a right-inverse, we have

  $$\begin{aligned} a' \circ f &= a'' \circ f \\ a' \circ f \circ f^{-1} &= a'' \circ f \circ f^{-1} \\ a' \circ 1_B &= a'' \circ 1_B \\ a' &= a'' \end{aligned}$$

  as desired. □

- Show that the converse does not hold, by giving an explicit example of a category and an epimorphism without a right-inverse.

  *Answer.* We try finding one through a non symmetry equivalence relation that represents the morphisms of a category. Specifically, we have gone over the category with the morphisms corresponding to equivalence relations $\sim$ or $\leqslant$ on $\mathbb{Z}$. We take two arbitrary functions $a', a'' \in \mathrm{Hom}_C(b, z)$. Therefore, we have $f \in \mathrm{Hom}_C(a, b)$ for $a \neq b$. Now observe that indeed,

  $$a' \circ f = a'' \circ f \implies a' = a''$$

  which is vacuously true. But there is no right inverse for $f$ as $b \nleqslant a$. This concludes the proof.

**Exercise 4.4**: Prove that the composition of two monomorphisms is a monomorphism. Deduce that one can define a subcategory $C_{\mathrm{mono}}$ of a category $C$ by taking the same objects as in $C$ and defining $\mathrm{Hom}_{C_{\mathrm{mono}}}(A, B)$ to be the subset of $\mathrm{Hom}_C(A, B)$ consisting of monomorphisms, for all objects $A, B$. Do the same for epimorphisms. Can you define a subcategory $C_{\mathrm{nonmono}}$ of $C$ by restricting to morphisms that are *not* monomorphisms?

*Answer.* (Part I) Suppose that $f \in \mathrm{Hom}_C(B, C)$, $g \in \mathrm{Hom}_C(C, D)$ and that for arbitrary morphisms $a', a'' \in \mathrm{Hom}_C(A, B)$, $b', b'' \in \mathrm{Hom}_C(A, C)$ we have

$$f \circ a' = f \circ a'' \implies a' = a''$$
$$g \circ b' = g \circ b'' \implies b' = b''$$

So we now compose $g \circ f$ and verify:

$$(g \circ f) \circ a' = (g \circ f) \circ a'' \implies f \circ a' = f \circ a''$$
$$f \circ a' = f \circ a'' \implies a' = a''$$

So $g \circ f$ is a monomorphism. Interestingly, we can take all elements in C and define the subcategory consisting of the morphisms as only the monomorphisms of C, because composition of monomorphisms is possible and that the composition is also a monomorphism and is therefore a morphism in $C_{\mathrm{mono}}$. Identity is indeed a monomorphism. Identity with respect to composition is inherited from C.

(Part II) Suppose that $f \in \mathrm{Hom}_C(A, B)$, $g \in \mathrm{Hom}_C(B, C)$ and that for arbitrary morphisms $a', a'' \in \mathrm{Hom}_C(C, D)$, $b \in \mathrm{Hom}_C(B, D)$ we have

$$b' \circ f = b'' \circ f \implies b' = b''$$
$$a' \circ g = a'' \circ g \implies a' = a''$$

So we now compose $g \circ f$ and verify:

$$a' \circ (g \circ f) = a'' \circ (g \circ f) \implies a' \circ g = a'' \circ g$$
$$a' \circ g = a'' \circ g \implies a' = a''$$

This shows that $g \circ f$ is an epimorphism also. By the same reasoning in the previous part, we have justified the composition part. The identity is definitely an epimorphism. So this is indeed a subcategory $C_{\mathrm{epi}}$.

We cannot define such a category $C_{\mathrm{nonmono}}$ since the identity would not exist in it.

**Exercise 4.5**: Give a concrete description of monomorphisms and epimorphisms in the category MSet you constructed in Exercise 3.9. (You answer will depend on the notion of morphism you defined in that exercise!)

*Answer.* Leave for Later.

## 1.5 Universal Properties

Categories give us an overview to the reasons for the constructions in algebra. Upcoming are several important constructions satisfying universal properties. One will be how products and disjoint unions will have universal properties relating to $C^{A,B}$ and $C^{A,B}$ in Example 1.3.8.

The later definitions will contain an explicitly description followed by a description of its universal property. The 'explicit' description will help in computation and arguments, while the universal property will show the nature of the construction. The description will seem to depend on an arbitrary choice while the universal property will not be arbitrary.

Universal properties will help us view the relationship between concepts, such as how products and disjoint unions of sets are actually mirror constructions.

**Definition 1.5.1**

**Initial and Final Objects**

Let $C$ be a category. We say that an object $I$ of $C$ is *initial* in $C$ if for every object $A$ or $C$ there exists *exactly one* morphism $I \to A$ in $C$:

$$\forall A \in \mathrm{Obj}(C) : \mathrm{Hom}_C(I, A) \text{ is a singleton.}$$

We say that an object $F$ of $C$ is *final* in $C$ if for every object $A$ or $C$ there exists *exactly one morphism* $A \to F$ in $C$:

$$\forall A \in \mathrm{Obj}(C) : \mathrm{Hom}_C(A, F) \text{ is a singleton.}$$

You can also use *terminal* to denote either possibility, but in general, it is important to consider which 'end' of $C$ that is being considered. Categories do not need to have initial and final objects.

**Example 1.5.1:** The category obtained by endowing $\mathbb{Z}$ with the relation $\leqslant$ from Example 1.3.2 has no initial or final object. There is no such integer where $i \in \mathbb{Z}$ is $i \leqslant a$ for all integers $a$. Similarly, for a final object, we require an object larger than every integer in the set of integers which is impossible. In contrast, the category in Example 1.3.5 does have a final object which is the pair $(3, 3)$, but has no initial object. Initial and final objects might not be unique.

**Example 1.5.2:** In Set, the empty set $\emptyset$ is initial and is the unique set that is initial. For the final objects, there is the singleton set $\{p\}$ which is essentially the constant function. Although they may not be unique, we claim that they are unique up to *isomorphism*. This will be important so here is the proof.

**Proposition 5.4**: Let $C$ be a category.

- If $I_1, I_2$ are both initial objects in $C$, then $I_1 \cong I_2$.
- If $F_1, F_2$ are both final objects in $C$, then $F_1 \cong F_2$.

These isomorphisms are also uniquely determined.

*Proof.* Recall that for every object $A$ of $C$, there is at least one element in $\mathrm{Hom}_C(A, A)$, which is the identity $1_A$. If $I$ is initial, then there is a unique morphism $I \to I$, which is the identity $1_I$.

Now suppose that $I_1$ and $I_2$ are both initial. There there is a unique morphism $f : I_1 \to I_2$ in C and likewise, there is a unique morphism $g : I_2 \to I_1$. Consider $gf : I_1 \to I_1$. So we must have that $gf = 1_{I_1}$ by the top observation, and similarly, $fg = 1_{I_2}$. This shows that f is an isomorphism. □

The proposition shows that in fact, no initial or final object is more special than the other. Although it may seem like $\{\emptyset\}$ is a natural choice, it does not influence the nature of the interactions between the objects.

The notion of universal properties requires the understanding of functors, which will be introduced much later. So the current definition will suffice:

A construction satisfies a universal property when it can be seen as a terminal object of a category. We can say that it is the solution to a universal problem. In simple cases, it could be the statement such as $\emptyset$ is universal with respect tot he property of mapping to sets, which is also the assertion that $\emptyset$ is initial in the category of Set.

The situation is often more complicated, as being initial and final means that there is the existence and uniqueness of certain morphisms. So the explanation of universal follows that object X is universal with respect to the following property: for any Y such that ..., there exists a unique morphism $Y \to X$ such that ...

It is not uncommon to disregard part of the information about the solution to a universal problem, as this information can be implicitly in a given set-up.

**Definition 1.5.2** **Quotients**

Let $\sim$ be an equivalence relation defined on a set $A$. Consider the assertion

"The quotient $A/\sim$ is universal with respect to the property of mapping $A$ to a set in such a way that equivalent elements have the same image."

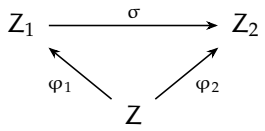
What does this mean? The assertion talks about functions so we can consider

$$\varphi : A \to Z$$

with Z any set that has the property

$$a' \sim a'' \implies \varphi(a') = \varphi(a'')$$

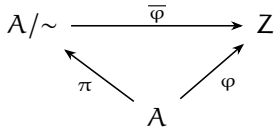
These morphisms are objects of a category similar to those defined in Example 1.3.6, so we can denote these objects like $(\varphi, Z)$. We should define morphisms $(\varphi_1, Z_1) \to (\varphi_2, Z_2)$ as commutative diagrams.




This is the same definition as in Example 1.3.6. Does this category have initial objects?

**Claim 5.5**: Denoting $\pi$ by 'canonical projection' defined in Example 1.2.3, the pair $(\pi, A/\sim)$ is an initial object of this category.

*Proof.* Consider any $(\varphi, Z)$. We have to prove that there exists a unique morphism $(\pi, A/\sim) \to (\varphi, Z)$ or a unique commutative diagram




Consider an arbitrary element of $A/\sim$. If the diagram is to commute, we require that

$$\overline{\varphi}([a]_\sim) = \varphi(a);$$

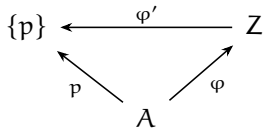
This means that $\overline{\varphi}$ is unique. We now have to check that $\overline{\varphi}$ is well-defined. That is, if $[a_1]_\sim = [a_2]_\sim$, then $\varphi(a_1) = \varphi(a_2)$. We have

$$[a_1]_\sim = [a_2]_\sim \implies a_1 \sim a_2 \implies \varphi(a_1) = \varphi(a_2)$$

This is the condition that morphisms of our category satisfy. □

In the assertion above, it does not tell us what category to consider, nor if we should look at the initial objects of the category. Also, the universal problem is not even $A/\sim$, it is actual $\pi : A \to A/\sim$. It is important to practice the skill of translating the loose assertions to precise statements.

The reason for the loose assertion is that there is no other morphism to be considered $A \to A/\sim$ other than the canonical projection, and additionally, the final object of the category is not interesting or of significance. Maybe the object $(p, A)$ with morphism $\varphi' : Z \to \{p\}$? For the commutative diagram:

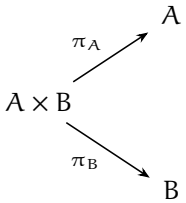



Since for any $Z$, there is only one mapping to the set $\{p\}$.

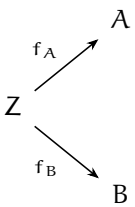
So what is to gain by viewing quotients in terms of their universal property? Suppose that $\sim$ is defined from a function $f : A \to B$. We will see that $\Im f$ also satisfies the universal property that is given above. This tells us that $A/\sim$ is isomorphic to $\Im f$. This shows an abstraction from the canonical decomposition that was done.

It is important to be able to see a universal property from a construction. Now is a good time to stop and consider the idea of a product of two sets and see if there is a universal property that jumps out.

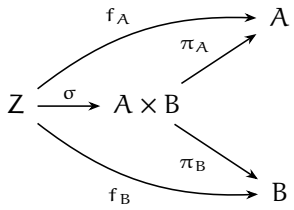
The universal property:




Where $A, B$ are sets with product $A \times B$ and the two natural projections. Then for every set $Z$ and morphisms



there exists a unique morphism $\sigma : A \times B$ such that the diagram




commutes, where we usually denote $\sigma$ by $f_A \times f_B$.

*Proof.* Define $\forall z \in Z$

$$\sigma(z) = (f_A(z), f_B(z))$$

This function makes the diagram commute because

$$\pi_A \sigma(z) = \alpha_A(f_A(z), f_B(z)) = f_A(z)$$

showing that $\pi_A \sigma = f_A$ and similarly, $\pi_B \sigma = f_B$. Since this definition is forced by the commutativity of the diagram, the morphism $\sigma$ is unique. □

Therefore, the product of sets with their natural projections are the final objects of the category $C_{A,B}$.

Why view the product as this? This allows us to say that this is a universal property in any category, but the definition only makes sense in the category Set. We say that a category C has finite products if for all objects A, B in C the category $C_{A,B}$ has final objects.

Note that the product does not always look like a product. Consider the category from $\leqslant$ on $\mathbb{Z}$. The objects of the category are $a, b \in \mathbb{Z}$ and call $a \times b$ a categorical product. The universal property now becomes *for all* $z \in \mathbb{Z}$ *such that* $z \leqslant a$ *and* $z \leqslant b$, *we have* $z \leqslant a \times b$.

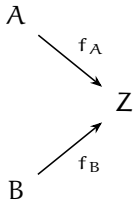
This universal problem does have a solution $\forall a, b$: it is not called $a \times b$ but rather $\min(a, b)$. We can see that $\min(a, b)$ satisfies this property, therefore, the category has products, and the products are a familiar operation on two integers.

There is a connection between the cartesian product of two sets and the minimum of two integers. Both are products taken from two different categories but they satisfy the same universal property in a different context.

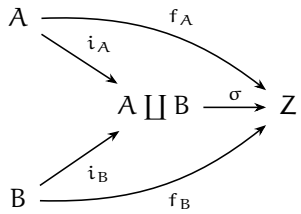
Overview is that what it means to be a universal property is that it holds for all morphisms in a category. That is to say that these morphisms are relations between the objects of a category.

Next are coproducts, and co- often means that there is a reversing of all the arrows. Where products are final objects in the categories $C_{A,B}$ by considering morphisms in C from a common source with targets A, B, coproducts are the initial objects in the categories $C^{A,B}$ with common target, who source from A, B. Dear reader, look away and spell this universal property out before we do.

Let A, B be objects of a category C. A coproduct $A \coprod B$ of A and B will be an object of C, endowed with two morphisms $i_A : A \to A \coprod B$, $i_B : B \to A \coprod B$ and satisfying the universal property such that for all objects Z and morphisms



there exists a unique morphism $\sigma : A \coprod B \to Z$ such that the diagram




commutes. There is symmetry with the universal property of products and we say that a category Ck has coproducts if this universal problem has a solution for all pairs of objects A and B. Here is a familiar coproduct:

**Proposition 5.6**: The disjoint union is a coproduct in Set.

*Proof.* Recall that the disjoint union $A \coprod B$ is defined to be the union of two disjoint isomorphic copies $A', B'$ of $A, B$, respectively. We may have $A' = \{0\} \times A, B' = \{1\} \times B$. Here, the functions $i_A, i_B$ are

$$i_A(a) = (0, a),\ i_B(b) = (1, b)$$

where we see these elements as elements of $(\{0\} \times A) \cup (\{1\} \times B)$.

Now let $f_A : A \to Z$, $f_B : B \to Z$ be arbitrary morphisms to a common target. Define

$$\sigma : A \coprod B = (\{0\} \times A) \cup (\{1\} \times B) \to Z$$

by

$$\sigma(c) = \begin{cases} f_A(a) & \text{if } c = (0, a) \in \{0\} \times A \\ f_B(b) & \text{if } c = (1, b) \in \{1\} \times B \end{cases}$$

this definition makes the diagram commute and it is forced on us, therefore, this morphism is unique. □

This shows that the category Set has coproducts and also shows us what disjoint unions are. For example, there were arbitrary choices to be made for a disjoint union, but any choice would lead to isomorphic relations. This is because terminal objects of a category are not unique but they are unique up to isomorphism.

There is also an unexpected symmetry between the products and disjoint unions between sets that becomes apparent when considering universal properties. The reader should also contemplate the notion of coproduct in other categories such as the one from $\leqslant$ on $\mathbb{Z}$, which does have coproducts. The coproduct of two objects $a, b$ is the maximum of them.

**Problem Sets**

**Exercise 1**: Prove that a final object in a category C is initial in the opposite category $C^{op}$.

*Proof.* Suppose that f is a final object of C. This means that for all other objects $g \in C$, we have that there is exactly one morphism in $\mathrm{Hom}_C(g, f)$. This means that if we consider the category $C^{op}$ with $\mathrm{Hom}_{C^{op}}(f, g) := \mathrm{Hom}_C(g, f)$, we have that for all $g \in C^{op}$, the set $\mathrm{Hom}_{C^{op}}(f, g)$ is a singleton. This says that f is initial in $C^{op}$. □

**Exercise 2**: Prove that $\emptyset$ is the *unique* initial object in Set.

*Proof.* We know that $\emptyset$ is an initial object in Set. This is because there is one

morphism from $\emptyset \to A$ for $A \in \mathrm{Set}$. We also know that initial objects are unique up to isomorphism. This means that $|\emptyset| = |I|$ for any initial object $I$ in $C$. But we know that $\emptyset$ is a subset of all sets. Therefore, $\emptyset \subseteq I$ and $|\emptyset| = |I|$ so $\emptyset = I$. □

**Exercise 3**: Prove that final objects are unique up to isomorphism.

*Proof.* Suppose that $F_1$ is a final object. This means that $|\mathrm{Hom}_C(F_1, F_1)| = 1$ and that implies that the element in the set must be $1_{F_1}$.

Suppose that $F_1, F_2$ are final objects. Then to prove isomorphism, we have to prove a bijection between them. By the fact that they are final objects, we have that there is one mapping $\varphi : F_1 \to F_2$ and another which is $\varphi' : F_2 \to F_1$. Now we compose them and observe that:

$$\varphi\varphi' \in \mathrm{Hom}_C(F_2)$$
$$\varphi'\varphi \in \mathrm{Hom}_C(F_1)$$

This means that either morphisms are both left-sided and right-sided inverses. Therefore, the mapping $\varphi$ is a bijection. We conclude that final objects are isomorphic. □

**Exercise 4**: What are initial and final objects in the category of 'pointed sets' (Example 1.3.7)? Are they unique?

*Proof.* For the initial objects in $\mathrm{Set}^*$, we note that the morphisms $\sigma$ of $\mathrm{Set}^*$ are such that $\sigma : S \to T$ with $\sigma(s) = t$ for objects $(S, s), (T, t)$. Note that the number of morphisms between two sets of size $m$ and $n$ is $n^m$ where $n$ is the cardinality of the codomain set.

$$n^m = 1$$
$$m = 0$$

Therefore, it is forced that the size of the initial object have cardinality 0 which is therefore $\emptyset$. This is the unique initial object. As for the final object, we do the same thing:

$$n^m = 1$$
$$n = 1$$

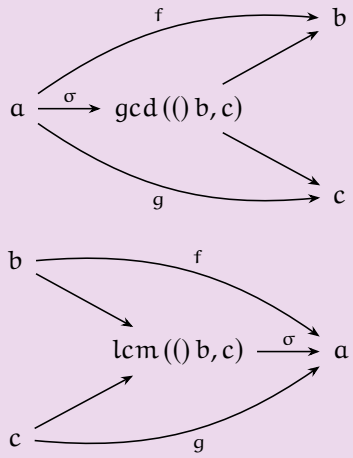
Which shows us that the final objects are singletons. These are not unique, but they are unique up to isomorphism. □

**Exercise 5**: What are the final objects in the category considered in 5.3?

*Proof.* What's 5.3? □

**Exercise 6**: Consider the category corresponding to endowing (as in Example 1.3.2) the set $\mathbb{Z}^+$ of positive integers with the *divisibility* relation. Thus there is exactly one morphism $d \to m$ in this category if and only if $d$ divides $m$ without remainder; there is no morphism between $d$ and $m$ otherwise. Show that this category has products and coproducts. What are their 'conventional' names?

*Proof.* The product and coproducts do exist in this category. For the product, we have that it is known by the lcm while for the coproduct, it is known as the gcd:




□

**Exercise 7**: Redo Exercise 2.9, this time using Proposition 5.4.

*Proof.* Later. □

**Exercise 8**: Show that in every category C the products $A \times B$ and $B \times A$ are isomorphic, if they exist.

*Proof.* Because they both satisfy the universal property for the product of $A, B$, we have that they are both final objects and are therefore isomorphic. □

**Exercise 10**: Let C be a category with products. Find a reasonable candidate for the universal property that the product $A \times B \times C$ of *three* objects of C ought to satisfy, and prove that both $(A \times B) \times C$ and $A \times (B \times C)$ satisfy this universal property. Deduce that $(A \times B) \times C$ and $A \times (B \times C)$ are necessarily isomorphic.

*Proof.* The product $A \times B \times C$ solves the universal problem of mappings from a set Z to three other sets $A, B, C$. Observe that the morphism that goes to our final object is determined uniquely by the elements $a_i, b_i, c_i$ such that $z_i \mapsto a_i, z_i \mapsto b_i, z_i \mapsto c_i$. This means that the structure of the sets $(A \times B) \times C$ and $A \times (B \times C)$ does not change the fact that they are both final objects and are therefore isomorphic. □

**Exercise 10**: Push the envelope a little further still, and define products and coproducts for *families*(i.e., indexed sets) of objects of a category.

1. Do these exist in Set?

   *Answer.* Try Later.

2. It is common to denote the product $\underbrace{A \times \cdots \times A}_{n \text{ times}}$ by $A^n$.

   *Answer.* Try Later.

**Exercise 11**: Let A, resp. B be the set, endowed with an equivalence relation $\sim_A$, resp. $\sim_B$. Define a relation $\sim$ on $A \times B$ by setting

$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 \sim_A a_2 \text{ and } b_1 \sim_B b_2$$

- Use the universal property for quotients in Definition 1.5.2 to establish that there are functions $(A \times B)/\sim \longrightarrow A/\sim_A$, $(A \times B)/\sim \longrightarrow B/\sim_B$.

*Proof.* We start off by declaring $\varphi_1$ to be the function such that:

$$a \sim a' \wedge b \sim b' \iff (a, b) \sim (a', b')$$

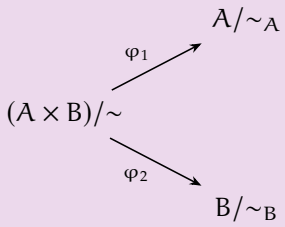
tells us that:

$$\varphi_1([a, b]) = [a] = \varphi_1([a', b'])$$

This mapping is well-defined, which we can tell by glancing. We define this analogously for the function $(A \times B)/{\sim} \longrightarrow B/{\sim_B}$. □

- Prove that $(A \times B)/{\sim}$, with these two functions, satisfies the universal property for the product of $A/{\sim_A}$ and $B/{\sim_B}$.

  *Proof.* What is to show is that the object:

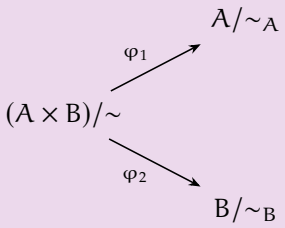
  
  

  is a final object. Suppose that we have an arbitrary set $Z$. We define the functions $\tau_1 : Z \to A/{\sim_A}$ and $\tau_2 : Z \to A/{\sim_B}$. Now we define a function $\sigma : Z \to (A \times B)/{\sim}$ by the following:

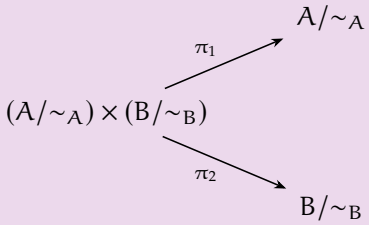
  $$\sigma(z_i) = [(a_i, b_i)]$$

  for $\tau_1(z_i) = [a_i]$ and $\tau_2(z_i) = [b_i]$. Observe that this function $\sigma$ is unique as it is forced by definition based on the $\varphi_1$ and $\varphi_2$ we defined. □

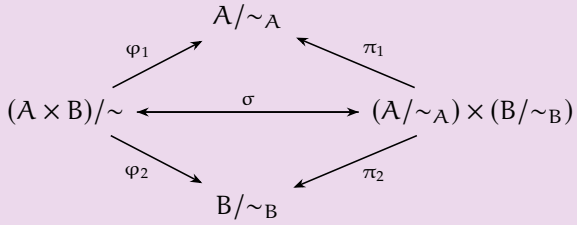
- Conclude (without further work) that $(A \times B)/{\sim} \cong (A/{\sim_A}) \times (B/{\sim_B})$. We conclude that the object:

  is a final object while

  is also a final object by the standard projection that we first used to identify products. Therefore, there is a commutative diagram to represent an isomorphism between them:




since there is a bijection $\sigma$ between the sets, that means that $(A \times B)/\sim \cong (A/\sim_A) \times (B/\sim_B)$.

**Exercise 12**: Define the notions of *fibered products* and *fibered coproducts*, as terminal objects of the categories $C_{\alpha,\beta}$, $C^{\alpha,\beta}$ considered in Example 1.3.9 by stating carefully the corresponding universal properties.

*Answer.* We define a fibered product as the object in $C_{\alpha,\beta}$ such that for any object $A$, commutative diagram in $C_{\alpha,\beta}$, there exists a unique morphism from $A$ to the fibered product to which

As it happens, Set has both fibered products and coproducts. Define these objects 'concretely', in terms of naive set theory.

# Chapter 2

# Groups, First Encounter

We will study the category Grp in which we look at monomorphisms and epimorphisms. We will also look at equivalence relations and quotients of a group and how the decomposition theorem works in Grp. For Chapter III, we will study rings and in Chapter IV, we will look at Sylow theorems, 'composition series', and the classification of finite abelian groups.

## 2.1 Definition of Group

**Joke 2.1.1** Definition: A group is a groupoid with a single object.

This is true in which we defined a groupoid in Example 1.4.3. Looking closely at the definition, this says that if $*$ is the single object of a groupoid $G$,

$$\mathrm{Hom}_G(*,*) = \mathrm{Aut}_G(*)$$

since $G$ is a groupoid. Call this set $G$. By the definition of a category, there is associativity in $G$, there is an identity, and for every $g \in G$, there is an inverse $g^{-1} \in G$. So this is the definition of a group:

**Definition 2.1.1** **Group**

Suppose that $G$ is a nonempty set with a binary operation, with a multiplication map:

$$\cdot : G \times G \to G$$

the notation is

$$\cdot(g,h) := g \cdot h$$

or simply

$$gh$$

Then $G$ is a group if

1. the operation $\cdot$ is *associative*:

$$(\forall g,h,k \in G) : (gh)k = g(hk)$$

2. there exists an *identity* element $e_G$ for $\cdot$:

$$(\exists e_G \in G)(\forall g \in G) : ge = g = eg$$

3. every element in G has an *inverse* with respect to $\cdot$:

$$(\forall g \in G)(\exists h \in G) : gh = e_G = hg$$

**Example 2.1.1:** Since G is nonempty, at the very least, we have $G = \{e\}$. This is the trivial group.

**Example 2.1.2:** It should be checked that $(\mathbb{Z}, +)$j, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are all groups. These examples are not very interesting as they are common and are to specialized. They are known as commutative groups.

**Example 2.1.3:** There is also a non-commutative group for the set of invertible $n \times n$ matrices for $n \geqslant 2$. The product of two matrices might not always commute.

We note that the identity is unique using the standard proof:

*Proof.* If $e_G$ and $h$ are identities:

$$h = eh = e$$

which concludes the proof. □

**Proposition 2.1.7**: Inverses are also unique. We use the same trick as the last proof:

*Proof.* Suppose that $h$ is in G and that $h^{-1}, g^{-1}$ are inverses:

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

therefore,

$$h^{-1}hg^{-1} = h^{-1} = eg^{-1} = g^{-1}$$

□

Elements of a group in general do not commute. They will commute if they are the same element:

$$g^n = \underbrace{g \cdots g}_{n \text{ times}}, \; g^{-n} = \underbrace{g^{-1} \cdots g^{-1}}_{n \text{ times}}$$

Cancellation holds in groups because of the existence of inverses. We can only cancel on same side however:

**Proposition 2.1.8**: Let G be a group. Then $\forall a, g, h \in G$:

$$ga = ha \implies g = h, \; ag = ah \implies g = h$$

the proof is left as an exercise for the reader.

Cancellation in general does not work in settings outside of groups, such as how the zero element in $\mathbb{R}$ does not have an inverse. To force a group, such as the multiplicative group on $\mathbb{R}$, we require:

$$\mathbb{R}^* := \mathbb{R} \backslash \{0\}$$

**Definition 2.1.2** — **Commutative Groups**

We say that a group is commutative if its binary operation is commutative:

$$gh = hg$$

Commutative groups arise in instances such as 'modules over the ring $\mathbb{Z}$'. These commutative groups are simply called abelian groups.

**Definition 2.1.3** — **Order of an Element**

An element $g \in G$ has finite order if $g^n = e$ for some positive integer $n$. The order is the smallest $n$.

**Lemma 2.1.10**: If $g^n = e$ for some positive integer $n$, then $\text{ord}(g) \mid n$.

We can use a proof by contradiction and division algorithm.

**Corollary 2.1.11**: Let $g$ be an element of finite order and $N \in \mathbb{Z}$. Then

$$g^N = e \iff N \text{ is a multiple of } \text{ord}(g)$$

this is an observation of the consequence of the proof in Lemma 2.1.10.

**Definition 2.1.4** — **Order of a Group**

If $G$ is a finite set, we write $|G|$ for the number of elements in $G$ and $|G| = \infty$ otherwise.

We note that the order of an element in $G$ cannot exceed $|G|$. Try proving this!

There is a stronger relation to be said between the order of an element and the group through Lagrange's Theorem. The elements of a group are not always predictable. We may have $f, g$ finite order but $\text{ord}(fg) = \infty$.

**Proposition 2.1.13**: Let $g \in G$ be an element of finite order. Then $g^m$ has finite order $\forall m \geqslant 0$, and also:

$$\text{ord}(g^m) = \frac{\text{lcm}\,(()\, m, \text{ord}(g))}{m} = \frac{|g|}{\text{gcd}\,(()\, m, \text{ord}(g))}$$

*Proof.* We first establish the equality on the RHS. This is true because of the fact that:

$$\frac{ab}{\text{gcd}\,(()\, a, b)} = \text{lcm}\,(()\, a, b)$$

Now to connect the equality to $\text{ord}(g^m)$, we note that if

$$g^a = e$$

We have that $m \mid a$, so what we really desire is the least common factor:

$$g^{\text{lcm}(()m,a)} = e$$

Which is almost there. We perform the decomposition:

$$(g^m)^{\frac{\text{lcm}(()a,m)}{m}} = e$$

and we're done.

We could also say that the order is the least $d$ such that:

$$g^{md} = e$$

Therefore, we have $m \cdot \text{ord}(g) = lcm\,((), m, \text{ord}(g))$. □

**Proposition 2.1.14**: If $gh = hg$, then $\text{ord}(gh)$ divides $lcm\,((), \text{ord}(g), \text{ord}(h))$.

*Proof.* Suppose that elements $g, h$ commute. If we take both to the power off $lcm\,((), \text{ord}(a), \text{ord}(b))$, we get:

$$gh^{lcm(()\text{ord}(a),\text{ord}(b))} = g^{lcm(()\text{ord}(a),\text{ord}(b))}h^{lcm(}$$

Therefore, the order divides this. □

**Problem Sets**

**Exercise 1**: Write a careful proof that every group is the group of isomorphisms of a groupoid. In particular, every group is the group of automorphisms of some object in some category.

*Proof.* Define the category with:

- The object is the set $G$.
- Morphisms in the group are in the set $\text{Hom}(G, G)$, which we call are the elements of $G$. These morphisms are defined as $f : G \to G$ where $f : g \in G \mapsto fg$.

This defines a category because the composition of morphisms is possible and associative. The identity function exists and so does the inverse, making every morphism an isomorphism. Therefore, the group is the collection of isomorphisms in this category. □

**Exercise 2**: Consider the 'sets of numbers' listed in 1.1 and decide which are made into groups by conventional operations such as $+$ and $\cdot$. Even if the answer is negative (such as $(\mathbb{R}, \cdot)$), see if variations on the definitions of these sets lead to groups (for example, $(\mathbb{R}^*, \cdot)$).

*Answer.* Leave for Later.

**Exercise 3**: Prove that $(gh)^{-1} = h^{-1}g^{-1}$ for all elements $g, h$ of a group $G$.

*Proof.* We are tasked with finding the inverse of $gh$. We denote that as $i$:

$$ghi = e \implies hi = g^{-1} \implies i = h^{-1}g^{-1}$$

So we are done. □

**Exercise 4**: Suppose that $g^2 = e$ for all elements $g$ of a group $G$; prove that $G$ is commutative.

*Proof.* If $g^2 = e$ for all elements, we consider $gh$ for $g, h \in G$. Notice that

$$(gh)^{-1} = h^{-1}g^{-1}$$

But since $g^2 = e$ for all elements, we have $gh = h^{-1}g^{-1}$ and therefore, $gh = hg$. □

**Exercise 5**: The 'multiplication table' of a group is an array compiling the results of all multiplications $gh$:

$$\begin{array}{ccccc} \cdot & e & \dots & h & \dots \\ e & e & \dots & h & \dots \\ \dots & \dots & \dots & \dots & \dots \\ g & g & \dots & gh & \dots \\ \dots & \dots & \dots & \dots & \dots \end{array}$$

Prove that every row and every column of the table contains all elements of the group exactly once.

*Proof.* Suppose that a given row for $g \in G$ contains duplicate elements $gh_1$ and $gh_2$. Then we have:

$$gh_1 = gh_2 \implies h_1 = h_2$$

This can be generalized to the columns also. □

**Exercise 6**: Prove that there is only one possible multiplication table for G if G has exactly 1, 2, or 3 elements. Analyze the possible multiplication tables for groups with exactly 4 elements, and show that there are two distinct tables, up to reordering the elements of G. Use these tables to prove that all groups with $\leqslant 4$ elements are commutative.

*Proof.* Not interested. □

**Exercise 7**: Prove Corollary 2.1.11.

*Proof.* Later. □

**Exercise 8**: Let G be a finite group with exactly one element $f$ of order 2. Prove that $\prod_{g \in G} g = f$.

*Proof.* We first note that since there is only one element of order 2, there can only be generating element of even order, for example, let $n$ be even and observe that if $g^n = e$ we have $g^{\frac{1}{2}=e}$. Now suppose we have the group $G \backslash \{g^{\frac{1}{2}}\}$. For all odd ordered elements $g$ and order $n$, we have

$$g, g^2, g^3, \dots, g^{n-1} \implies \prod_{i=1}^{n-1} g = g^{\frac{n(n-1)}{2}}$$

But since $n$ is odd, we must have $n-1$ even. Therefore, $n$ divides $\prod_{i=1}^{n-1} g$ which means that the product of this set of elements is just $e$. Now for the set generated by the element of even order:

$$g, g^2, \dots, g^{\frac{n}{2}-1}, g^{\frac{n}{2}+1}, \dots, g^{n-1}$$

To which we have the order as $g^{\frac{(n)(n-2)}{2}}$. Since $n-2$ is even we have that $n$ also divides this product of elements. Therefore,

$$\prod_{g \in G \backslash \{g^{\frac{n}{2}}\}} g = e$$

So if we add back in $f$, we have the result as desired. □

**Exercise 9**: Let G be a finite group, of order $n$, and let $m$ be the number of elements $g \in G$ of order exactly 2. Prove that $n - m$ is odd. Deduce that if $n$ is even, then $g$ necessarily contains elements of order 2.

*Proof.* (Part I) Consider the generating element $g$ of odd order $n$. Observe that this element contributes an even number of elements to the order of G:

$$g, g^2, \ldots, g^{n-1}$$

To which this list has $n-1-1+1$ or $n-1$ elements. Now consider the generating element $g$ of even order $n$.

$$g, g^2, \ldots, g^{n-1}$$

Each such element has one element of order 2. Suppose we have $m$ such elements. Notice that the list above has an odd number of elements, o Therefore, we have a contribution of an odd number of elements $o \cdot m$. This makes $n - m$ odd.

(Part II) From the first part that we concluded, observe that if there are no elements of order 2, then $n$ is odd. Therefore, by contrapositive, we have what we want. □

**Exercise 10**: Suppose that the order of $g$ is odd. What can you say about the order of $g^2$?

*Proof.* Recall that the order of $g^2$ is equal to the least common multiple of 2 and $g$ divided by 2. Therefore, we have $lcm\,(()\,n, 2) = 2n$ and

$$\frac{lcm\,(()\,n, 2)}{2} = n$$

□

**Exercise 11**: Prove that for all $g, h$ in a group G, $|gh| = |hg|$.

*Proof.* Suppose that $\text{ord}(gh) = n$. Then we have:

$$(gh)^n = e$$

or in expanded form:

$$\underbrace{gh \cdots gh}_{n \text{ times}} = e$$

Now if we take $hg$ to the power of $n + 1$, observe that we have:

$$h \cdot \underbrace{gh \cdots gh}_{n \text{ times}} \cdot g = hg$$

Therefore, we have

$$(hg)^{n+1} = hg$$

So the order of $gh$ divides the order of that of $hg$. We can show the same vice versa. Therefore, the orders are equal. *-We had to show that this $n$ was the least positive integer for $hg$. Apparently an alternate proof utilizes the hint: (Hint: Prove that $|aga^{-1}| = |g|$ for all $a, g$ in G). □

**Exercise 12**: In the group of invertible $2 \times 2$ matrices, consider

$$g = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \; h = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

Verify that $\text{ord}(g) = 4$, $\text{ord}(h) = 3$, and $\text{ord}(gh) = \infty$.

*Proof.* The first two problems are just verification. We check the last one:

$$gh = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Now we look at powers of this matrix:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$$

We notice that this might never reach the identity. The proof of this is a verification. □

**Exercise 13**: Give an example showing that $\text{ord}(gh)$ is not necessarily equal to $\text{lcm}(()\,\text{ord}(g), \text{ord}(h))$, even if $g$ and $h$ commute.

*Proof.* One example is if $\text{ord}(g) = 4$ and $h = g$. We have $gh = g^2$. But the order of $g^2$ is 2, which is not $\text{lcm}(()\,4, 4)$. □

**Exercise 14**: As a counter point to Exercise 1.13, prove that if $g$ and $h$ commute and $\gcd(()\,\text{ord}(g), \text{ord}(h)) = 1$, then $\text{ord}(gh) = \text{ord}(g)\text{ord}(h)$.

*Proof.* Suppose that $N$ is the order of $gh$. Then we have:

$$N = \text{lcm}(()\,|g|, |h|)$$

but by the fact that

$$\text{lcm}(()\,g, h) = \frac{gh}{\gcd(()\,g, h)}$$

we have that $N = |g||h|$ □

**Exercise 15**: Let $G$ be a commutative group, and let $g \in G$ be an element of maximal *finite* order, that is, such that if $h \in G$ has finite order, then $|h| \leqslant |g|$. Prove that in fact if $h$ has finite order in $G$, then $|h|$ *divides* $|g|$.

*Proof.* Consider for contradiction that we have

$$|g| = p^m r \qquad\qquad |h| = p^n s$$

with $m < n$, $p$ a prime integer, and $r, s$ relatively prime to $p$. We then seen that the order of $g^{p^m}$ is just $r$ as $(g^{p^m})^r$. We apply the same reasoning to see that the order of $h^s$ is $p^n$. Since $\gcd(()\,p^n, r) = 1$, we can conclude that the order of $g^{p^m}h^s$ is the product of $|g^{p^m}||h^s| = p^n r$. But this is a contradiction because we have found and element with greater order than $g$ as $n > m$. □

## 2.2 Examples of Groups

We have already seen that every object $A$ of every category $C$ determines a group called $\text{Aut}_C(A)$ which is the group of automorphisms of $A$. We will see that groups arise from these automorphisms in what will be discussed as group actions.

**Symmetric Group**

The symmetric group is the group of permutations denoted $S_A$ is the group $\mathrm{Aut}_{\mathrm{Set}}(A)$. The group of permutations of the set $\{1, \ldots, n\}$ is denoted $S_n$.

The group of automorphisms of $A$ is just the set of bijections between $A$ and itself. We have already shown that $|S_n| = n!$. Elements of $S_A$ are functions and therefore, the binary action should be the composition of functions. It is important to know the elements of $S_n$ for small $n$. In $S_3$, notice that the elements are not commutative.

**Definition 2.2.2**

**Dihedral Groups**

The dihedral groups can be thought of as the symmetries on a 2d regular polygon of $n$ sides. We denote this group as $D_{2n}$. These group elements consists of rotation and reflection. The precise definition of this group is:

$$D_{2n} = \{r^a s^b : rsr^{-1} = s^{-1} \wedge r^2 = e \wedge s^n = e\}$$

Notice that $D_6 \cong S_3$. We can show this through a group homomorphism which is a morphism between groups that preserves the structure of composition of group elements.

**Definition 2.2.3**

**Cyclic Groups and Modular Arithmetic**

Let $n$ be a positive integer and consider the equivalence relation on $\mathbb{Z}$ defined by

$$(\forall a, b \in \mathbb{Z}) : a \equiv b \mod n \iff n \mid (b - a).$$

This is called congruence modulo $n$. We have seen this relation in Example 1.1.1. The set of equivalence classes $\mathbb{Z}/\sim$ is called $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$.

These groups are also called cyclic groups with the notation $C_n$ where we say that the group $C_n$ is generated by one element $x$ where $x^n = e$. For $\mathbb{Z}/n\mathbb{Z}$, the element $[1]$ generates the group.

It should be checked that $\mathbb{Z}/n\mathbb{Z}$ consists of exactly $n$ elements:

$$[0]_n, [1]_n, \ldots, [n-1]$$

This is an abelian group with respect to addition:

$$[a] + [b] := [a + b]$$

which we have to check is well defined.

**Proposition 2.2.3**: The order of $[m]$ in $\mathbb{Z}/n\mathbb{Z}$ is 1 if $n \mid m$ and more generally,

$$|[m]_n| = \frac{n}{\gcd(()\, m, n)}$$

*Proof.* We see that if $n \mid m$, then $[m] = [0]$. For the general statement, we see that $[m] = [1]^m$. Applying the past proposition, we have that

$$|[m]_n| = \frac{n}{\gcd(()\, m, n)}$$

□

The proof shows that the order of every element of a cyclic group divides the order of the group.

**Corollary 2.2.5**: The class $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(()\, m, n) = 1$.

This leads to the fact that any group $\mathbb{Z}/p\mathbb{Z}$ where $p$ is prime is generated by all of its elements except for 0.

Also note that it should be checked that we have multiplication defined in the group. The operation:

$$[a] \cdot [b] := [ab]$$

is also well-defined but does not have a group structure unless we modify it:

$$(\mathbb{Z}/n\mathbb{Z})^* := \{[m] \in \mathbb{Z}/n\mathbb{Z} : \gcd(() m, n) = 1\}$$

This subset is well-defined.

**Proposition 2.2.6**: Multiplication makes $(\mathbb{Z}/n\mathbb{Z})^*$ into a group.

*Proof.* We observe that the group is closed under multiplication as if $\gcd(() m_1, n) = 1$ and $\gcd(() m_2, n) = 1$, we have that $\gcd(() m_1 m_2, n) = 1$. We have associativity as a property of multiplication. The identity exists because $\gcd(() m, n) = 1$ therefore, we have that $[m]$ generates the additive group and so $[1]$ must be in there:

$$[m][a] = [1]$$

Therefore, multiplicative inverses exist. To verify that $\gcd(() a, n) = 1$, we make the observation that if $[a][m] = [1]$, we have that $[am] = [1]$ and therefore, $am = bn + 1$. If $r \mid a$, we must have that $r \mid bn+1$. But if $r$ divides $bn+1$, it cannot divide $bn$, otherwise, we have $r \mid 1$. So $r$ is 1. Therefore, $\gcd(() a, n) = 1$. □

For $n = p$ where $p$ is a positive prime, the group $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$ has order $p - 1$.

**Problem Sets**

**Exercise 1**: One can associate an $n \times n$ matrix $M_\sigma$ with a permutation $\sigma \in S_n$ by letting the entry at $(i, \sigma(i))$ be 1 and letting all other entries be 0. For example, the matrix corresponding to the permutation

$$\sigma = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \in S_3$$

would be

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Prove that, with this notation,

$$M_{\sigma\tau} = M_\sigma M_\tau$$

for all $\sigma, \tau \in S_n$, where the product on the right is the ordinary product of matrices.

*Proof.* Leave for Later. □

**Exercise 2**: Prove that if $d \leqslant n$, then $S_n$ contains elements of order $d$.

*Answer.* We just need

$$(1 \ldots d)$$

**Exercise 3**: For every positive integer $n$ find an element of order $n$ in $S_n$.

*Answer.* We just need

$$(1 \ldots n)$$

**Exercise 4**: Define a homomorphism $D_8 \to S_4$ by labeling vertices of a square, as we did for a triangle in 2.2. List the 8 permutations in the image of this homomorphism.

*Answer.* We just label the vertices of the square by 1, 2, 3, 4 and use an identity map.

**Exercise 5**: Describe generators and relations for all dihedral groups $D_{2n}$.

*Proof.* The generators of the group are of the form $s, r, sr, s^2r, \ldots, s^{n-1}r$. We can say that two permutations are related if you can reach them by a number of rotations. □

**Exercise 6**: For every positive integer $n$ construct a group containing two elements $g, h$ such that $|g| = 2$, $|h| = 2$, and $|gh| = n$.

*Proof.* We can use $D_{2n}$ where $r$ has order 2 and $sr$ also has order 2. □

**Exercise 7**: Find all elements of $D_{2n}$ that commute with every other element.

*Proof.* Notice that the elements that commute with every other element. If $n$ is even, we have that $s^{\frac{n}{2}}$ commutes with all other elements:

$$s^{\frac{n}{2}} r s^j = s^{\frac{n}{2}} s^{-j} r = s^{\frac{n}{2}-j} r$$
$$r s^j s^{\frac{n}{2}} = r s^{\frac{n}{2}+j} = s^{\frac{n}{2}-j} r$$

We also have that $rs^{\frac{n}{2}}$ commutes with every element. There are no other elements that commute with every other element. Notice that this only works when $n$ is even. □

**Exercise 8**: Find the orders of the groups of symmetries of the five 'platonic solids'.

*Proof.* The order of the symmetries group on the tetrahedron is the number of unique morphisms that are generated by those that fix one element and rotate the rest. So it is generated by

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

The order of this group would be 12. For the cube, we have rotation across the three axes, along with reflection across three planes. So the group of symmetries is generated by the set:

$$S = \{\, (1\,2\,3\,4)(5\,6\,7\,8), (1\,2\,6\,5)(3\,4\,8\,7), (2\,3\,7\,6)(1\,4\,8\,5), (1\,5)(2\,6)(3\,7)(4\,8), \\ (1\,2)(5\,6)(3\,4)(7\,8), (2\,3)(6\,7)(1\,4)(5\,8) \,\}$$

□

**Exercise 9**: Verify carefully that 'congruence mod $n$' is an equivalence relation.

*Proof.* Consider the relation where two elements are related if and only if $a \equiv b \pmod{n}$. We definitely have that $a \sim a$, since $n \mid a - a$. Also, we have that if $n \mid a - b$, then also, $n \mid -(a - b)$ or $n \mid b - a$. Therefore, the relation is symmetric. Finally, for transitivity, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, Then we have $n \mid a - b$ and $n \mid b - c$, therefore, $n \mid (a - b) + (b - c) = a - c$. Therefore, the relation is transitive and this means that it is an equivalence relation. □

**Exercise 10**: Prove that $\mathbb{Z}/n\mathbb{Z}$ consists of precisely $n$ elements.

*Proof.* We have that $\mathbb{Z}/n\mathbb{Z}$ is the set of equivalence classes of $Z$ based on our equivalence relation. Observe that the number of unique remainders that we can have lies between $0, \ldots, n-1$. Therefore, we have $n$ elements in $\mathbb{Z}/n\mathbb{Z}$. □

**Exercise 11**: Prove that the square of every odd integer is congruent to 1 modulo 8.

*Proof.* We just have to check the equivalence classes with odd representatives, because mod 8, the square of odd numbers are odd and therefore, odd - even = odd:

$$\mathbb{Z}/8\mathbb{Z} = \{[0], [1], [2], [3], [4], [5], [6], [7]\}.$$

So we have to just square the odd ones:

$$[1]^2 = [1],\ [3]^2 \equiv [1],\ [5]^2 \equiv [1],\ [7]^2 \equiv [1]$$

which concludes the proof. □

**Exercise 12**: Prove that there are no integers $a, b, c$ such that $a^2 + b^2 = 3c^2$.

*Proof.* We can try working in mod 3 so that the RHS cancels to just 0:

$$\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$$

So now we square all elements:

$$\{[0], [1]\}$$

So all possible sums of two square remainders are:

$$\{[0], [1]\}$$

This means that both $a, b$ must have either remainder 0. But this is impossible since the LHS is divisible by an even number of 3's but the RHS is divisible by an odd number of 3's. □

**Exercise 13**: Prove that if $\gcd(() m, n) = 1$, then there exists integers $a$ and $b$ such that

$$am + bn = 1$$

*Proof.* Observe that if $n = 1$, we have that $m = 1$, to which we use $a = 0$, $b = 1$. Now suppose that $n > 1$. Then we have by modding both sides:

$$am \equiv 1 \pmod{n}$$

Now observe that the order of the element $1^m$ in $\mathbb{Z}/n\mathbb{Z}$ is just

$$\frac{\operatorname{lcm}(() m, n)}{m} = \frac{n}{\gcd(() m, n)} = n$$

Therefore, $[1]^{ma} = [1]$ for some $a$. So $m$ has an inverse, we call $a$. This concludes the proof. □

**Exercise 14**: State and prove an analog of Lemma 2.2, showing that the multiplication on $\mathbb{Z}/n\mathbb{Z}$ is a well-defined operation.

*Proof.* Hell no □

**Exercise 15**: Let $n > 0$ be an odd integer.

- Prove that if $\gcd(() m, n) = 1$, then $\gcd(() 2m + n, 2n) = 1$.

*Proof.* If we have what is above, due to the properties of the gcd, we have $\gcd(()\, m, n) = 1 \implies \gcd(()\, 2m, 2n) = 2$. Since $n$ is odd, we have that $2m + n$ does not have a factor of 2. Furthermore, the factors of $2m + n$ cannot divide those of $n$ because $\gcd(()\, 2m, n) = 1$. Therefore, we have $\gcd(()\, 2m + n, 2n) = 1$ □

- Prove that if $\gcd(()\, r, 2n) = 1$, then $\gcd(()\, \frac{r+n}{2}, n) = 1$.

  *Proof.* Leave for Later. □

- Conclude that the function $[m]_n \to [2m + n]_{2n}$ is a bijection between $(\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/2n\mathbb{Z})^*$.

The number $\varphi(n)$ of elements of $(\mathbb{Z}/n\mathbb{Z})^*$ is *Euler's φ-function*. The reader has just proved that if $n$ is odd, then $\Phi(2n) = \varphi(n)$. Much more general formulas will be given later on.

**Exercise 16**: Find the last digit of $1238237^{18238456}$ by working in $\mathbb{Z}/10\mathbb{Z}$.

*Proof.* Too much work. □

**Exercise 17**: Show that if $m \equiv m' \bmod n$, then $\gcd(()\, m, n) = 1$ if and only if $\gcd(()\, m', n) = 1$.

*Proof.* This follows trivially from the proof on the last proposition in the section. □

**Exercise 18**: For $d \leqslant n$, define an injective function $\mathbb{Z}/d\mathbb{Z} \to S_n$ preserving the operation, that is, such that the sum of equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ corresponds to the product of the corresponding permutations.

*Proof.* Just use an element of order $d$ in $S_n$:

$$(1\, 2 \ldots d)$$

This is injective, we just name this element $g$ and we do the mapping such that:

$$[i] \mapsto g^i$$

□

**Exercise 19**: Both $(\mathbb{Z}/5\mathbb{Z})^*$ and $(\mathbb{Z}/12\mathbb{Z})^*$ consist of 4 elements. Write their multiplication tables, and prove that no re-ordering of the elements will make them match.

*Proof.* The elements of both groups are:

$$(\mathbb{Z}/5\mathbb{Z})^* = \{[1], [2], [3], [4]\} \text{ and } (\mathbb{Z}/12\mathbb{Z})^* = \{[1], [5], [7], [11]\}$$

and multiplication tables:

| | [1] | [2] | [3] | [4] |
|---|---|---|---|---|
| [1] | [1] | [2] | [3] | [4] |
| [2] | [2] | [4] | [1] | [3] |
| [3] | [3] | [1] | [4] | [2] |
| [4] | [4] | [3] | [2] | [1] |

| | [1] | [5] | [7] | [11] |
|---|---|---|---|---|
| [1] | [1] | [5] | [7] | [11] |
| [5] | [5] | [1] | [11] | [7] |
| [7] | [7] | [11] | [1] | [5] |
| [11] | [11] | [7] | [5] | [1] |

All elements in $(\mathbb{Z}/12\mathbb{Z})^*$ are of order 2. This is not true for the elements of $(\mathbb{Z}/5\mathbb{Z})^*$ □

## 2.3 The Category Grp

A group has two types of information. One is the set and the other, the binary operation:

$$m_G : G \times G \to G$$

satisfying certain properties. For two groups, a group homomorphism is:

$$\varphi : (G, m_G) \to (H, m_H)$$

which is a function between sets. But we must incorporate the information of the binary operation in this somehow. We also have that the function $\varphi$ determines:

$$(\varphi \times \varphi) : G \times G \to H \times H$$

and using the universal property of products. Or we could just define the function using what we already know about sets:

$$(\forall (a, b) \in G \times G) : (\varphi \times \varphi)(a, b) = (\varphi(a), \varphi(b))$$

with respect to the group operations $m_G, m_H$ on the groups $G, H$, we can define a diagram that incorporates all this information:

$$\begin{array}{ccc} G \times G & \xrightarrow{\varphi \times \varphi} & H \times H \\ \downarrow{\scriptstyle m_G} & & \downarrow{\scriptstyle m_H} \\ G & \xrightarrow[\varphi]{} & H \end{array}$$

a very natural requirement would make this diagram commute.

**Definition 2.3.1**

**Group Homomorphism**

A function $\varphi : G \to H$ is a group homomorphism if the diagram above commutes. This reveals a simple property. What commutativity means is that we can travel the diagram in equal ways:

$$\begin{array}{ccc} (a, b) & \dashrightarrow & \\ \downarrow & & \vdots \\ a \cdot b & \longmapsto & \varphi(a \cdot b) \end{array} \qquad \begin{array}{ccc} (a, b) & \longmapsto & (\varphi(a), \varphi(b)) \\ \vdots & & \downarrow \\ & \dashrightarrow & \varphi(a) \cdot \varphi(b) \end{array}$$

So we have that the order of operations does not matter where we can take $\varphi$ first then do the binary operation or take the binary operation then the $\varphi$. That is to say:

$$\varphi(ab) = \varphi(a)\varphi(b)$$

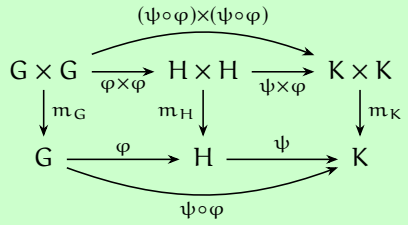
which means that $\varphi$ 'preserves the structure'.

**Homomorphisms of Grp**

For $G, H$ groups, we define

$$\mathrm{Hom}_{\mathrm{Grp}}(G, H)$$

to be the set of group homomorphisms $G \to H$. If $G, H, K$ are groups and $\varphi : G \to H$, $\psi : H \to K$ are group homomorphisms, we have that the composition is a group homomorphism with $\psi \circ \varphi : G \to K$:




We check that the outer rectangles commute:

$$\begin{aligned}(\psi \circ \varphi)(a \cdot b) &= \psi(\varphi(a \cdot b)) = \psi(\varphi(a) \cdot \varphi(b)) = \psi(\varphi(a)) \cdot \psi(\varphi(b)) \\ &= (\psi \circ \varphi)(a) \cdot (\psi \circ \varphi)(b)\end{aligned}$$

Since $\mathrm{id}_G : G \to G$ is a group homomorphism, we have that Grp is a category.

One additional thing to consider is the fact that a group keeps track of the existence of inverses and the identity element. This means that the morphisms of Grp should keep track of this data. This is automatic in what we found out about the structure of a group homomorphism however:

**Proposition 2.3.2**: Let $\varphi : G \to H$ be a *group homomorphism*. Then

- $\varphi(e_G) = e_H$;
- $\forall g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$

In referencing a diagram, we get:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ {\scriptstyle \mathrm{id}_G}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_H} \\ G & \xrightarrow[\varphi]{} & H \end{array}$$

must commute.

*Proof.* (Part I) Since $e_H e_H = e_H$:

$$e_H \cdot \varphi(e_G) = \varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G)$$

which means that $e_G = \varphi(e_G)$.

(Part II) For the second part, we have:

$$\varphi(g^{-1}) \cdot \varphi(g) = \varphi(g^{-1} \cdot g) = \varphi(e_G) = e_H = \varphi(g)^{-1} \cdot \varphi(g)$$

which shows that $\varphi(g^{-1}) = \varphi(g)^{-1}$. □

The categories Grp and Set look very similar, but there is the additional information about the binary operation in a group. Another difference is that Set has a unique initial object $\emptyset$ which are not the same as final objects which are the singletons.

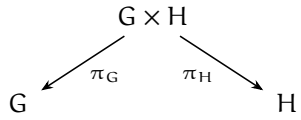
**Proposition 2.3.3**: *Trivial groups* are both initial and final in Grp. This means that trivial groups are zero objects of the category Grp.

*Proof.* The trivial groups are final object because they contain one element and by the same reasoning as made in Set. To show that they are initial, we note that the homomorphisms of Grp are group homomorphisms and that the identity must map to the identity. Therefore, this is the trivial map also. So the trivial group is a zero object. □

Grp also has products and the product of two groups $G, H$ would be the based on $G \times H$. We would define multiplication component-wise $\forall g_1, g_2 \in G, \forall h_1, h_2 \in H$:

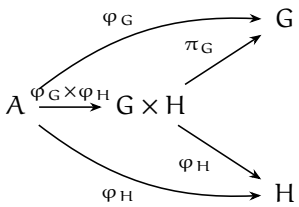
$$(g_1, h_1) \cdot (g_2, h_2) := (g_1, g_2, h_1, h_2)$$

This defines a group structure on $G \times H$. The group $G \times H$ is called the *direct product* of the groups $G$ and $H$. We also have the projections as group homomorphisms:




**Proposition 2.3.4**: With the operation defined component-wise, $G \times H$ is a product in Grp.

*Proof.* To be a product means to solve the universal problem that for any $\varphi_G : A \to G$, $\varphi_H : A \to H$, there is a unique homomorphism $\varphi_G \times \varphi_H$ which makes:




commute. We know that it commutes because it is the same as the product of $G, H$ in Set. Now we check that $\varphi_G \times \varphi_H$ is a group homomorphism and exists in Grp:

$$\begin{aligned}\varphi_G \times \varphi_H(ab) &= (\varphi_G(ab), \varphi_H(ab)) = (\varphi_G(a)\varphi_G(b), \varphi_H(a)\varphi_H(b)) \\ &= (\varphi_G(a), \varphi_H(a))(\varphi_G(b), \varphi_H(b)) = (\varphi_G \times \varphi_H(a))(\varphi_G \times \varphi_H(b))\end{aligned}$$

□

Coproducts also exist in Grp, but their construction will be more challenging to see. These will show up in Exercise 3.8, 5.6, 5.7. Free groups are cases of coproducts. For now, it is sufficient to know that coproducts can be constructed with the disjoint union in Set, which we cannot do in Grp because there is no group structure we have for disjoint union. The coproduct of $G$ and $H$ is called the free product of $G$ and $H$ which is $G * H$.

The category Ab have objects as abelian groups with morphisms as group homomorphisms. These will be more important than the ones in Grp. Ab is also a nicer category than Grp. Interestingly, the products in Ab are also the coproducts. When working with coproducts, the product $G \times H$ of abelian groups is often called the direct sum or denoted as $G \oplus H$.

Notice that even if $G$ and $H$ are commutative, they may not solve the universal problem that makes $G \times H$ into a coproduct.

**Problem Sets**

**Exercise 1**: Let $\varphi : G \to H$ be a morphism in a category $C$ with products. Explain why there is a unique morphism

$$(\varphi \times \varphi) : G \times G \to H \times H.$$

(This morphism is defined explicitly for $C = \text{Set}$ in 3.1)

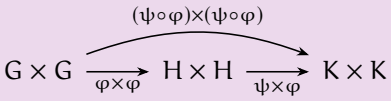
**Exercise 2**: Let $\varphi : G \to H$, $\psi : H \to K$ be morphisms in a category with products, and consider morphisms between the product $G \times G$, $H \times H$, $K \times K$ as in Exercise 3.1.

Prove that

$$(\psi\varphi) \times (\psi\varphi) = (\psi \times \psi)(\varphi \times \varphi)$$

(This is part of the commutativity of the diagram displayed in 3.2).

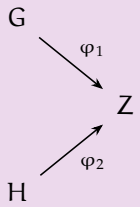
*Proof.* From the commutative diagram, we get that:



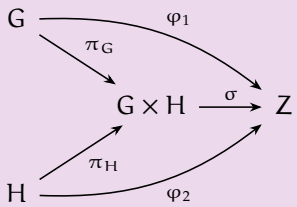

The top arrow is equal to the composition of the both two arrows. This concludes the proof. □

**Exercise 3**: Show that if G, H are abelian groups, then $G \times H$ satisfies the universal property for coproducts in Ab.

*Proof.* We start by supposing that there is a problem to solve, the mapping from two groups to a group by a homomorphism:




Now if we take the product, we can take two sensible mappings to the product to be the projection mappings:




To find $\sigma$, we observe that it has to be a group homomorphism. So we observe what the action of $\varphi_1, \varphi_2$ does on two elements from both G and H:

$$\pi_H(h_1) = (e, h_1)$$
$$\varphi_2(h_1) = z_1$$

This means that we have $(e, h_1) \mapsto \varphi_2(h_1)$ for all $h \in H$. We denote this as $\sigma : \{(e, h) : h \in H\} \to Z$ to be $\sigma(e, h) := \varphi_2(e)\varphi_2(h) = \varphi_2(h)$. Likewise, we show the same for $\varphi_1$ on elements in G. Therefore, we get the forced mapping:

$$\sigma : G \times H \to Z \qquad \sigma(g, h) := \varphi_1(g)\varphi_2(h)$$

Is this a homomorphism? Suppose that we have elements of $G \times H$ called $(g_1, h_1), (g_2, h_2)$, which map to $z_1, z_2$ respectively. Then we have:

$$\begin{aligned}\sigma((g_1, h_1)(g_2, h_2)) &= \sigma((g_1g_2, h_1h_2)) \\ &= \varphi_1(g_1g_2)\varphi_2(h_1h_2) \\ &= \varphi_1(g_1)\varphi_1(g_2)\varphi_2(h_1)\varphi_2(h_2)\end{aligned}$$

But since $Z$ is commutative, $\varphi_1(g_2)$ and $\varphi_2(h_1)$ commute! So:

$$\begin{aligned}\sigma((g_1,h_1)(g_2,h_2)) &= \varphi_1(g_1)\varphi_2(h_1)\varphi_1(g_2)\varphi_2(h_2)\\ &= \sigma((g_1,h_1))\sigma((g_2,h_2))\end{aligned}$$

□

**Exercise 4**: Let $G$, $H$ be groups, and assume that $G \cong H \times G$. Can you concludes that $H$ is trivial?

*Proof.* Later. □

**Exercise 5**: Prove that $\mathbb{Q}$ is not the direct product of two nontrivial groups.

**Exercise 6**: Consider the product of the cyclic groups $C_2, C_3 : C_2 \times C_3$. By Exercise 3.3, this group is a coproduct of $C_2$ and $C_3$ in Ab. Show that it is *not* a coproduct of $C_2$ and $C_3$ in Grp as follows:

- find injective homomorphisms $C_2 \to S_3, C_3 \to S_3$:

  *Proof.* We have the inclusion maps from $C_2$ to $S_3$ and $C_3$ to $S_3$:

  $$\begin{aligned}\iota_{C_2} &: C_2 \to S_3\\ \iota_{C_3} &: C_3 \to S_3\end{aligned}$$

  □

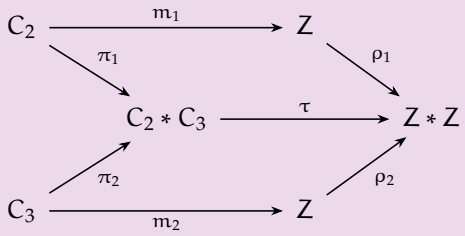
- arguing by contradiction, assume that $C_2 \times C_3$ is a coproduct of $C_2, C_3$ and deduce that there would be a group homomorphism $C_2 \times C_3 \to S_3$ with certain properties;

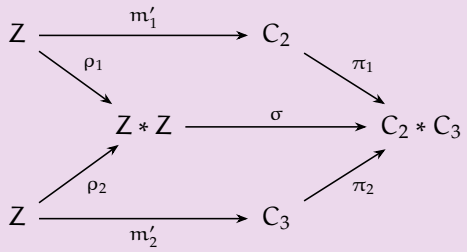
  *Proof.* Now suppose that $C_2 \times C_3$ is a coproduct of $S_3$ and we have a group homomorphism $\sigma : C_2 \times C_3 \to S_3$. Note that the homomorphism is from a product of abelian groups. Therefore, the product $C_2 \times C_3$ is abelian also. Now note that we have that $(1\,2) \mapsto (1\,2)$ and $(1\,2\,3) \mapsto (1\,2\,3)$. But since the elements of $C_2 \times C_3$ commute, we must have that $(1\,2)(1\,2\,3) = (1\,2\,3)(1\,2)$ which is false. □

- show that there is no such homomorphism.

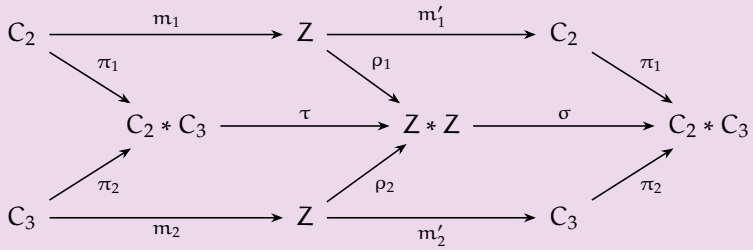
**Exercise 7**: Show that there is a *surjective* homomorphism $\mathbb{Z} * \mathbb{Z} \to C_2 * C_3$ (* denotes coproduct in Grp)

*Proof.* We can draw two commutative diagrams to see the relationship between these objects:

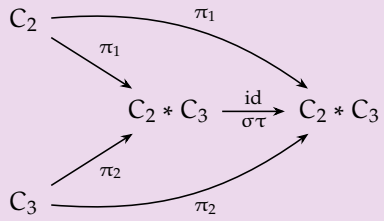





Notice that $\sigma$ has a right inverse however which can be seen by putting the diagrams together:




Notice that there is a surjective mapping for $m_1', m_2'$ because $|\mathbb{Z}| > |C_3| > |C_2|$. So there is a right inverse, $m_1, m_2$ for the morphisms respectively with respect to the commutative diagram above. But if we traverse the mappings, we get $\sigma\tau\pi_1 = \pi_1 m_1' m_1$ and $\sigma\tau\pi_2 = \pi_2 m_2' m_2$. Or simply, $\sigma\tau\pi_1 = \pi_1$ and $\sigma\tau\pi_2 = \pi_2$. But because $\sigma$ and $\tau$ are unique, $\sigma\tau$ is the unique morphism such that the diagram commutes. But we know that the morphism from an initial object to itself is the identity. So that means that $\sigma\tau$ is the identity and that $\tau$ is surjective. To clarify, we have:




□

**Exercise 8**: Define a group G with two generators $x, y$, subject (only) to the relations $x^2 = e_G, y^3 = e_G$. Prove that G is a co-product of $C_2$ and $C_3$ in Grp. (The reader will obtain an even more concrete description for $C_2 * C_3$ in Exercise 9.14; it is called the modular group)

**Exercise 9**: Show that *fiber* products and coproducts exist in Ab.

## 2.4 Group Homomorphisms

**Example 2.4.1:** For any two groups $G, H$, the set $\mathrm{Hom}_{\mathrm{Grp}}(G, H)$ is not empty. We define a homomorphism by sending all elements in the group G to the identity. Therefore, $\mathrm{Hom}_{\mathrm{Grp}}(G, H)$ is a pointed set.

Notice that Grp has zero-objects which are both final and initial objects $\{*\}$, so there are unique morphisms:

$$G \to \{*\},\ \{*\} \to H$$

The composition of these mappings is the identity element of $\mathrm{Hom}_{\mathrm{Grp}}(G, H)$.

Recall the example of the homomorphism $D_6 \to S_3$ which we defined as a group homomorphism. Other examples will consider group actions, which is the action from a group $G$ to an object $A$ of a category $C$:

$$G \to \mathrm{Aut}_C(A);$$

For example, if the category is $C = \mathrm{Set}$, then the group actions will determine the permutations of the sets in $C$. One example is the set of vertices and the action of $D_6$ on them.

Another example is the exponential function from $(\mathbb{R}, +)$ to the group $(\mathbb{R}^{>0}, \cdot)$ where we have $e^{a+b} = e^a e^b$. Another example is where we let $G$ be any group and $g \in G$ be the element of $G$. We have the exponential map as $\varepsilon_g : \mathbb{Z} \to G$

$$(\forall a \in \mathbb{Z}) : \varepsilon_g(a) := g^a$$

We note that this is a group homomorphism and that $g$ generates $G$ if and only if the mapping is surjective.

Another example of a homomorphism are the quotient functions:

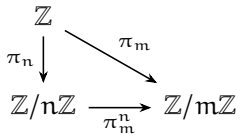
$$a \mapsto a \cdot [1]_n = [a]_n :$$

with the notation introduced above, this is $\varepsilon_{[1]_n}$. The function is surjective so $[a]_n$ generates $\mathbb{Z}/n\mathbb{Z}$. We already noted that $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(() m, n) = 1$.

If $m \mid n$, there is a homomorphism

$$\pi_m^n : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

by making the diagram




commute or basically:

$$\pi_m^n([a]_n) = [a]_m$$

It should be checked that this is well-defined. Furthermore, if $m_1$ and $m_2$ are divisors of $n$, then there are homomorphisms $\pi_{m_1}^n$ and $\pi_{m_2}^n$ from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m_1\mathbb{Z}$ and $\mathbb{Z}/m_2\mathbb{Z}$ and therefore to their direct product. For instance, we have the homomorphisms:

$$\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

which we have by:

$$\begin{array}{lll} [0]_6 \mapsto ([0]_2, [0]_3), & [1]_6 \mapsto ([1]_2, [1]_3), & [2]_6 \mapsto ([0]_2, [2]_3), \\ [3]_6 \mapsto ([1]_2, [0]_3), & [4]_6 \mapsto ([0]_2, [1]_3), & [5]_6 \mapsto ([1]_2, [2]_3) \end{array}$$

This is an isomorphism and we see that the $C_6 \cong C_2 \times C_3$. We can define a homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ if $n \mid m$. But what about when $m \nmid n$? Try to deduce a proof before it is shown.

*Proof.* The only homomorphism from $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is the trivial homomorphism. Observe that all homomorphisms are of the form $\varphi : n \mapsto an$ for some $0 \leqslant a \leqslant m$. This is because all morphisms are determined by what the generator maps to. Then we must have that $n \mapsto an$ and $0 \mapsto 0$. But observe that $an \in \mathbb{Z}/m\mathbb{Z}$ is not 0. This is because $n \nmid m$ so $an \neq m$ for any $a \in \mathbb{Z}$. □

Considering that group homomorphisms must preserve the identity and the order, it must be that elements of finite order are sent to those of finite order also. So we have that

$$\varphi(g)^n = \varphi(g^n) = \varphi(e_G) = e_H$$

which gives us a more precise statement:

**Proposition 2.4.1**: Let $\varphi : G \to H$ be a group homomorphism, and let $g \in G$ be an element of finite order. Then $|\varphi(g)|$ divides $|g|$.

*Proof.* We observed that $\varphi(g)^{|g|} = e_H$. So we know that the order of $\varphi(g)$ divides the exponent. □

**Example 2.4.2:** There are no nontrivial homomorphisms $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$. The image of every element of $\mathbb{Z}/n\mathbb{Z}$ must have finite order and the only element of finite order in $(\mathbb{Z}, +)$ is 0.

There are also no nontrivial homomorphisms $\varphi : C_4 \to C_7$. The orders of the elements in $C_4$ divide 4 and the orders of the elements in $C_7$ divide 7. Therefore, the order of each $\varphi(g)$ divides both 4 and 7 which means that $|\varphi(g)| = 1$.

The order is not preserved in general such as $1 \in \mathbb{Z}$ while $[1]_n \in \mathbb{Z}/n\mathbb{Z}$ has finite order. Order is, however, preserved through isomorphism.

An isomorphism of groups $\varphi : G \to H$ is an isomorphism in Grp which is a group homomorphism with an inverse:

$$\varphi^{-1} : H \to G$$

which is a group homomorphism. If we look at Set, if a homomorphism is an isomorphism, then it must be a bijection between the sets. So the converse holds:

**Proposition 2.4.3**: Let $\varphi : G \to H$ be a group homomorphism. Then $\varphi$ is an isomorphism of groups if and only if it is a bijection.

*Proof.* The first implication is immediate. Now suppose that $\varphi : G \to H$ is a bijective homomorphism. Then since it is a bijection, it has an inverse $\varphi$ in Set.

$$\varphi^{-1} : H \to G$$

is this a group homomorphism? Suppose that $h_1, h_2$ are elements of $H$, then we have $g_1 = \varphi^{-1}(h_1), g_2 = \varphi^{-1}(h_2)$ as the elements of $G$. Now we check:

$$\varphi^{-1}(h_1h_2) = \varphi^{-1}(\varphi(g_1)\varphi(g_2)) = \varphi^{-1}(\varphi(g_1g_2)) = g_1g_2 = \varphi^{-1}(h_1)\varphi^{-1}(h_2)$$

as desired. □

**Example 2.4.3:** The function $D_6 \to S_3$ is an isomorphism of groups since it is a bijective homomorphism. The exponential function $(\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)$ is also an isomorphism. If the exponential function $\varepsilon_g : \mathbb{Z} \to G$ is determined by an element

$g \in G$ is an isomorphism, we say that G is an infinite cyclic group.

The function $\pi_2^6 \times \pi_3^6 : C_6 \to C_2 \times C_3$ is an isomorphism.

**Definition 2.4.1**

**Isomorphic Groups**

Two groups $G, H$ are isomorphic if they are isomorphic in Grp or in other words, if there is a bijective group homomorphism $G \to H$.

We note that the isomorphic condition is an equivalence relation. We write that $G \cong H$ if G and H are isomorphic. Automorphisms of a group G are isomorphisms $G \to G$. These form a group $\mathrm{Aut}_{\mathrm{Grp}}(G)$ or $\mathrm{Aut}(G)$.

**Example 2.4.4:** The concept of isomorphisms allow us to give a formal definition of cyclic groups that we last discussed in Definition 2.2.3.

**Cyclic Group**

A group G is cyclic if it is isomorphic to $\mathbb{Z}$ or to $C_n = \mathbb{Z}/n\mathbb{Z}$ for some $n$.

We have that $C_2 \times C_3$ is cyclic because it is isomorphic to $C_6$. In general $C_m \times C_n$ is cyclic if $\gcd(() m, n) = 1$.

We know that $D_6$ and $S_3$ are isomorphic, but what about $C_6$ and $S_3$? We will look at this soon.

We can also see that if p is prime, the group $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$ is cyclic. This is a deep fact and we see that $(\mathbb{Z}/12\mathbb{Z})^*$ is not cyclic. What it means to be cyclic is that there is an $a$ where every non-multiple of p is congruent to a power of $a$. The usual proofs are not constructive. There is also a connection between the order of an element of a cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$ which are called 'cyclotomic polynomials' which will be introduced after some field theory.

Isomorphic objects should be indistinguishable in a category so they share the same group structure.

**Proposition 2.4.8**: Let $\varphi : G \to H$ be an isomorphism.

- $(\forall g \in G) : |\varphi(g)| = |g|$;
- G is commutative if and only if H is commutative.

*Proof.* (Part I) The first part we get from the fact that the order of $\varphi(g)$ divides that of g. If we take the inverse, the order of g which is $\varphi^{-1}(\varphi(g))$ divides that of $\varphi(g)$. So the orders are equal.

(Part II) The second part is left to the reader. □

**Example 2.4.5:** $C_6 \ncong S_3$ since one is commutative and the other is not. We can also say that the number of distinct orders in $C_6$ does not match that of $S_3$, so the groups are not isomorphic.

*Note*: Two finite commutative groups are isomorphic if and only if they have the same number of elements of any given order. This will be proved in the next chapter. The general statement for non-commutative groups is not true.

We will look at homomorphisms in abelian groups because in general, those in Ab are more well-behaved. We note that $\mathrm{Hom}_{\mathrm{Grp}}(G, H)$ is a pointed set for any two groups $G, H$, but in Ab, $\mathrm{Hom}_{\mathrm{Ab}}(G, H)$ is a group.

The operation in $\mathrm{Hom}_{\mathrm{Ab}}(G, H)$ is inherited from the operation in $H$ and if $\varphi, \psi : G \to H$ are group homomorphisms, let $\varphi + \psi$ be the function:

$$(\forall a \in G) : (\varphi + \psi)(a) := \varphi(a) + \psi(a).$$

Would $\varphi + \psi$ be a group homomorphism? For all $a, b \in G$:

$$\begin{aligned}(\varphi + \psi)(a + b) &= \varphi(a + b) + \psi(a + b) = (\varphi(a) + \varphi(b)) + (\psi(a) + \psi(b))) \\ &= (\varphi(a) + \psi(a)) + (\varphi(b) + \psi(b)) = (\varphi + \psi)(a) + (\varphi + \psi)(b).\end{aligned}$$

The + signs are used to denote commutative operations in this book. The operation makes $\mathrm{Hom}_{\mathrm{Ab}}(G, H)$ into a group. The properties of + we get from a homomorphism such as associativity, identity, and inverses are defined as:

$$(\forall a \in G) : (-\varphi)(a) = -\varphi(a).$$

Note that these conclusions only require that $H$, the codomain is commutative. We can also say that $H^A = \mathrm{Hom}_{\mathrm{Set}}(A, H)$ is a group for all sets $A$, which is a group that will be studied later.

**Problem Sets**

**Exercise 4.1**: Check that the function $\pi_m^n$ defined in 4.1 is well-defined and makes the diagram commute. Verify that it is a group homomorphism. Why is the hypothesis $m \mid n$ necessary?

*Proof.* Suppose that $[a]_n = [b]_n$. We must show that $\pi_m^n([a]_n) = \pi_m^n([b]_n)$. Since $[a]_n = [b]_n$, we have that $a - b = cn$ for some $c \in \mathbb{Z}$. But since $m \mid n$, we must have that $c'm = n$. Therefore, $a - b = cc'm$. Therefore, we have as desired. □

**Exercise 4.2**: Show that the homomorphism $\pi_2^4 \times \pi_2^4 : C_4 \to C_2 \times C_2$ is not an isomorphism. In fact, is there any nontrivial isomorphism $C_4 \to C_2 \times C_2$?

*Proof.* It is not an isomorphism because it is not injective. We have

$$\begin{aligned}0 &\mapsto (0, 0) \\ 1 &\mapsto (1, 1) \\ 2 &\mapsto (0, 0) \\ 3 &\mapsto (1, 1)\end{aligned}$$

There are no isomorphisms because the number of order 2 and 4 elements in $C_4$ do not match with the number of 2 and order 4 elements in $C_2 \times C_2$ respectively. □

**Exercise 4.3**: Prove that a group of order $n$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ if and only if it contains an element of order $n$.

*Proof.* ($\to$) Suppose that $G$ is a group of order $n$ with an element of order $n$

called $g$. Then we can list out all the elements of G as $g^k$ for some $k$. Therefore, the group is cyclic and has order $n$. Therefore, $G \cong \mathbb{Z}/n\mathbb{Z}$.

($\leftarrow$) Suppose that $G \cong \mathbb{Z}/n\mathbb{Z}$. Since isomorphisms preserve order, we must have an element of order $n$. □

**Exercise 4.4**: Prove that no two of the groups $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ are isomorphic to one another. Can you decide whether $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are isomorphic to one another?

*Proof.* Notice that all homomorphisms from $\mathbb{Z}$ to any other group must be of the form

$$\varphi := n \mapsto an$$

for some $a$ in the codomain. So we must have for $\varphi : \mathbb{Z} \to \mathbb{Q}$ as:

$$0 \mapsto 0 \qquad 1 \mapsto a$$

But observe that $\frac{a}{2} \notin \mathfrak{I}\varphi$. We can show this by induction on the positive integers. So the homomorphism is not surjective, and therefore not bijective. So it is not an isomorphism. We just need to prove that $\mathbb{R} \ncong \mathbb{Q}$. We do this by noting that $|\mathbb{Z}| = |\mathbb{Q}|$. So we are done. The cardinalities do not match up. We cannot decide whether $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are isomorphic because we do not know how to compare their cardinalities, nor do we know what a homomorphism would look like. □

**Exercise 4.5**: Prove that the groups $(\mathbb{R}\backslash\{0\}, \cdot)$ and $(\mathbb{C}\backslash\{0\}, \cdot)$ are not isomorphic.

*Proof.* We have that the only elements of finite order in $\mathbb{R}$ are $1, -1$ which have order 1 and 2 respectively. But in $\mathbb{C}\backslash\{0\}$, there are elements $i, -i$ which both have order 4. Since isomorphism preserves order, the groups are not isomorphic. □

**Exercise 4.6**: We have seen that $(\mathbb{R}, +)$ and $(\mathbb{R}^{>0}, \cdot)$ are isomorphic in Example 2.4.3. Are there groups $(\mathbb{Q}, +)$ and $(\mathbb{Q}^{>0}, \cdot)$ isomorphic?

*Proof.* Yes the groups are isomorphic. We can define a homomorphism $\varphi : q \mapsto x^q$, for some variable $x$. This is a group homomorphism which can be checked. Additionally, the map is both injective and surjective, when we take $x$ to be $> 0$. If $\varphi(q_1) = \varphi(q_2)$, we have $\frac{\varphi(q_1)}{\varphi(q_2)} = x^0$. Therefore, we have that $q_1 - q_2 = 0$ and $q_1 = q_2$. The mapping is surjective as it is essentially an identity function. □

**Exercise 4.7**: Let G be a group. Prove that the function $G \to G$ defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian. Prove that $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

*Proof.* (Part I)($\rightarrow$) Suppose that $\varphi : G \to G$ and that $\varphi := g \mapsto g^{-1}$. Then we have that for arbitrary $g_1, g_2$:

$$\varphi(g_1 g_2) = g_2^{-1} g_1^{-1} = g_1^{-1} g_2^{-1} = \varphi(g_1)\varphi(g_2)$$

We can rearrange terms to show that the elements commute:

$$g_2^{-1} g_1^{-1} = g_1^{-1} g_2^{-1} \implies g_1 g_2 = g_2 g_1$$

($\leftarrow$) Suppose that G is abelian. Then we can check with two elements that it is a homomorphism using the abelian property. This can be seen in the first part of the proof.

(Part II)($\rightarrow$) Suppose that $\varphi : G \to G$ is a homomorphism such that $\varphi := g \mapsto g^2$. Again with the verification:

$$\varphi(g_1 g_2) = g_1 g_2 g_1 g_2 = g_1 g_1 g_2 g_2 = \varphi(g_1)\varphi(g_2)$$

By taking inverses of both sides, we get:

$$g_1g_2g_1g_2 = g_1g_1g_2g_2 \implies g_1g_2 = g_2g_1$$

($\leftarrow$) The other way can be seen by how the previous part was done. □

**Exercise 4.8**: Let G be a group, and let $g \in G$. Prove that the function $\gamma_g : G \to G$ defined by $(\forall a \in G) : \gamma_g(a) = gag^{-1}$ is an automorphism of G. (The automorphisms $\gamma_g$ are called 'inner' automorphisms of G). Prove that the function $G \to \mathrm{Aut}(G)$ defined by $g \mapsto \gamma_g$ is a homomorphism. Prove that this homomorphism is trivial if and only if G is abelian.

*Proof.* (Part I) This function is a group homomorphism because if we have $g_1, g_2$:

$$\gamma_g(g_1g_2) = gg_1g_2g^{-1} = gg_1g^{-1}gg_2g^{-1} = \gamma_g(g_1)\gamma_g(g_2)$$

Also, it has an inverse homomorphism which we have as $\gamma_{g^{-1}}(a) := g^{-1}ag$.

(Part II) The second part is a verification. Let $\sigma : G \to \mathrm{Aut}(G)$ be defined as $\sigma(g) := g \mapsto \gamma_g$. Then we have for two elements in G:

$$\sigma(g_1g_2)(a) = \gamma_{g_1g_2}(a) = g_1g_2ag_2^{-1}g_1 = \gamma_{g_1}\gamma_{g_2}(a) = \sigma(g_1)\sigma(g_2)(a)$$

Now if the group is abelian, we have that $\gamma_g := g \mapsto gag^{-1} = agg^{-1} = a$. Therefore, the function $\gamma_g = eae^{-1}$, so the morphism $\sigma : G \to \mathrm{Aut}(G)$ is a trivial homomorphism. □

**Exercise 4.9**: Prove that if $m, n$ are positive integers such that $\gcd(()\, m, n) = 1$, then $C_{mn} \cong C_m \times C_n$.

*Proof.* Let $\varphi : C_{mn} \to C_m \times C_n$ be the morphism such that $\varphi := z \to ([z]_m, [z]_n)$. We prove that it is a homomorphism:

$$\varphi(g_1g_2) = ([g_1g_2]_m, [g_1g_2]_n) = ([g_1]_m, [g_1]_m)([g_2]_n, [g_2]_n) = \varphi(g_1)\varphi(g_2)$$

Now to prove surjectivity, we require that for arbitrary $z_1, z_2$, we have a $z$ such that:

$$\varphi(z) = ([z_1]_m, [z_2]_n)$$

So we require that

$$z \equiv z_1 \pmod{m} \qquad z \equiv z_2 \pmod{n}$$

So this comes down to the Chinese Remainder Theorem:

$$z \equiv 1 \pmod{m} \qquad z \equiv 0 \pmod{m}$$
$$z \equiv 0 \pmod{n} \qquad z \equiv 1 \pmod{n}$$

Since we know that $\gcd(()\, n, m) = 1$, $n$ is a generator in $\mathbb{Z}/m\mathbb{Z}$. We can pick an $0 \leqslant a_1 < m$ such that $a_1n \equiv 1 \pmod{m}$ and simultaneously, $a_1n \equiv 0 \pmod{n}$. Furthermore, the same can be said for the RHS system of equations. Therefore, we have $z_1a_1n + z_2a_2m \equiv z_1 \pmod{m}$ and $z_1a_1n + z_2a_2m \equiv z_2 \pmod{n}$. Therefore, the mapping is surjective. Since the cardinalities of the groups are equal, it is bijective and therefore, an isomorphism. □

**Exercise 4.10**: Let $p \neq q$ be odd prime integers; show that $(\mathbb{Z}/pq\mathbb{Z})^*$ is not cyclic.

*Proof.* We can start by looking at an example of the group $(\mathbb{Z}/15\mathbb{Z})^*$:

$$(\mathbb{Z}/15\mathbb{Z})^* = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$$

Notice that we remove all multiples of 3 and 5. In other words, we consider the order of the groups $(\mathbb{Z}/3\mathbb{Z})^*$ and $(\mathbb{Z}/5\mathbb{Z})^*$ to see how many multiples we remove:

$$(\mathbb{Z}/3\mathbb{Z})^* = \{[1], [2]\}$$
$$(\mathbb{Z}/5\mathbb{Z})^* = \{[1], [2], [3], [4]\}$$

Notice that we can remove exactly $|(\mathbb{Z}/3\mathbb{Z})^*|$ multiples of 5 and $|(\mathbb{Z}/5\mathbb{Z})^*|$ multiples of 3 in the set

$$\{[1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14]\}$$

This gives us the formula for the cardinality of $(\mathbb{Z}/15\mathbb{Z})^*$ or $(\mathbb{Z}/pq\mathbb{Z})^*$ in general:

$$|(\mathbb{Z}/pq\mathbb{Z})^*| = (\mathbb{Z}/pq\mathbb{Z})^+ - 1 - |(\mathbb{Z}/p\mathbb{Z})^*| - |(\mathbb{Z}/q\mathbb{Z})^*|$$

We know that both $(\mathbb{Z}/p\mathbb{Z})^*$ and $(\mathbb{Z}/q\mathbb{Z})^*$ are cyclic because $p, q$ are prime. Therefore, their orders are $p-1$ and $q-1$ respectively. So this gives:

$$\begin{aligned} |(\mathbb{Z}/pq\mathbb{Z})^*| &= pq - 1 - (p-1) - (q-1) \\ &= pq - 1 - p + 1 - q + 1 \\ &= (p-1)(q-1) \end{aligned}$$

Now that we have found the order of $(\mathbb{Z}/pq\mathbb{Z})^*$, we can prove that it is not cyclic by showing that no element in it has order $(p-1)(q-1)$. Consider the fact that the order of an element $g$ divides the order of the group. Therefore, we have $\text{ord}(g) \mid (p-1)(q-1)$. Now suppose that we did have an element with order $(p-1)(q-1)$:

$$g^{(p-1)(q-1)} = e$$

Notice that this is actually impossible. We note that $\gcd(() g, p) = 1$ and $\gcd(() g, q) = 1$. This gives us:

$$g^{(p-1)} \equiv e \pmod{p}$$
$$g^{(q-1)} \equiv e \pmod{q}$$

Therefore, we choose the lcm of $(p-1)$, $(q-1)$, since then we will have both factors: $\gcd(() g^{\text{lcm}((()(p-1),(q-1))}, pq) = 1$! But since $p-1$ and $q-1$ are even, as both $p, q$ are odd, they share a factor of 2. So

$$\text{lcm}(() (p-1), (q-1)) \neq (p-1)(q-1)$$

□

**Exercise 4.11**: In due time we will prove the easy fact that if $p$ is a prime integer, then the equation $x^d = 1$ can have at most $d$ solutions in $\mathbb{Z}/p\mathbb{Z}$. Assume this fact, and prove that the multiplicative group $G = (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

*Proof.* Suppose that we have an element of maximal order $g$ with order $|g|$. Since multiplication is commutative, our group $(\mathbb{Z}/p\mathbb{Z})^*$ is commutative. This means that for all $h \in G$, $h^{|g|} = e$. Using the fact that the equation $x^d = 1$ has at most $d$ solutions in $\mathbb{Z}/p\mathbb{Z}$, we conclude that $|g| \geqslant |G|$. We also know that the order of $g$ cannot be greater than $|G|$ because if we consider the chain:

$$g, g^2, g^3, \ldots, g^{|G|}, g^{|G|+1}$$

the number of unique elements of this listing cannot exceed the order of the group or $|G|$. Therefore, we have $|g| \leqslant |G|$ also. Thus, $|g| = |G|$ and we can conclude that the group is isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z}$ □

**Exercise 4.12**: Compute the order of $[9]_{31}$ in the group $(\mathbb{Z}/31\mathbb{Z})^*$. Does the equation $x^3 - 9 = 0$ have solutions in $\mathbb{Z}/31\mathbb{Z}$?

*Proof.* (Part I) We know that 31 is prime. Therefore, the order of $[9]_{31}$ is a factor of 30, the order of the group. So the order is $2, 3, 5, 6, 10$, or 15:

$$9^2 = 81 \cong 19$$
$$19 * 9 = 171 \cong 16$$

So the order is not 2 or 3. For 6, we take $16^2 = 256 \cong 8$, so it cannot be 5 either. Now for $10, 15$:

$$16 * 9 = 144 \cong 20$$
$$20 * 9 = 180 \cong 25$$
$$25^2 = 625 \cong 5$$
$$25 * 5 = 125 \cong 1$$

The second line calculates $9^5$, the third, $9^{10}$, the fourth $9^{15}$. Therefore, the order is 15.

(Part II) To solve the equation we rewrite it to

$$x^3 = 9$$

Then we see that $x^3$ has order 15. But we know that the order of $x^3$ is the lcm of the order of $|x|$ and 3. Therefore, we have $15 = \frac{lcm(()3,d)}{3}$, where $d$ is the order of $x$. This means that $d = 45$, which is impossible. □

**Exercise 4.13**: Prove that $\mathrm{Aut}_{\mathrm{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$.

*Proof.* Consider the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ represented as the set:

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{e, r, s, rs\}$$

where $r, s$ have order 2 and $rs = sr$. Notice that if we consider the set $\{r, s, rs\}$, we have that the product of any two elements is equal to the third element. This can be checked by casework. Now if we consider the bijections between this set and itself, we would like to consider specifically the homomorphisms, so it is required that:

$$e \mapsto e$$

Now the other mappings are determined by what two elements map to. For $r$ and $s$, choose an arbitrary but different mapping from $r$ and $s$ to something in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This will be a homomorphism. We must show that for any $g_1, g_2$ in the set, we have:

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$$

Certainly, this is true. Since $g_1 \neq g_2$, we can say that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$ where $h_1 \neq h_2$. Since $g_1 g_2 \neq g_1 \vee g_2$, we have that it must be the third element of the set $g_3$. This means that $g_3$ must be sent to $\varphi(h_3)$. Now we consider what $h_1 h_2$ is. It is just $h_3$ because as we have established from the group, it cannot be equal to $h_1 \vee h_2$ nor can it be the identity since $h_1 \neq h_2$. We have a way to find all homomorphisms. Since these are also bijective, we have the isomorphisms and therefore the elements of $\mathrm{Aut}_{\mathrm{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. Notice that this shows the isomorphism to $S_3$. The identity is fixed, and we find all ways to permute the mappings of the three elements to themselves. So we can label each element of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as $1, 2, 3$ and consider it as the permutations of these three. Since the orders of the sets are equal and there is an injective mapping, it must be a bijection. In fact, we have established that this is an isomorphism because of the similar nature of the construction. □

**Exercise 4.14**: Prove that the order of the group of automorphisms of a cyclic group $C_n$ is the number of positive integers $r < n$ that are relatively prime to $n$. (This is called Euler's $\varphi-$ function).

*Proof.* Suppose that we have a cyclic group $C_n$ denoted as:

$$C_n = \{0, 1, 2, 3, \ldots, n-1\}$$

Notice now that all homomorphisms are determined by what the 1 element is sent to, as it generates the group. So therefore, we have $n$ options. Clearly, we cannot have $1 \mapsto 0$, as we must have $0 \mapsto 0$ and this would not form a bijection. Suppose we have $1 \mapsto p$ where $\gcd(()p, n) \neq 1$. Then we observe that the equation:

$$pp' \cong 1 \pmod{n}$$

has no solution because of Bezout's Theorem. This means that the range of our homomorphism does not contain 1. Therefore, it cannot be a bijection. Now what about when $\gcd(()k, n) = 1$? Observe that by Bezout's Theorem, there is an inverse $m$ such that:

$$mk \cong 1 \pmod{n}$$

So we do in fact have a surjective mapping. Is it injective? Since the size of the sets are equal, it must be bijective. It is also a homomorphism. We need to verify that for $g_1, g_2 \in C_n$, we have that $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$. We first note that $1 \mapsto k$. So We have:

$$\varphi(g_1 g_2) = (g_1 + g_2)k = g_1 k + g_2 k = \varphi(g_1)\varphi(g_2)$$

Therefore, we have an isomorphism, as desired. □

**Exercise 4.15**: Compute the group of automorphisms of $(\mathbb{Z}, +)$. Prove that if $p$ is prime, then $\mathrm{Aut}_{\mathrm{Grp}}(C_p) \cong C_{p-1}$.

*Proof.* We must have $0 \mapsto 0$. Now we must have all automorphisms of the form:

$$a \mapsto an$$

for some $n \in Z$. We consider the fact that every automorphism has a positive smallest element in the codomain. We let this be $n$ as seen above. If not all morphisms are not of that form, we must have some $a \mapsto an + r$ where $0 < r \leqslant n - 1$. We can perform the division algorithm because we have inverses. But then we must have that $r$ is in the codomain. This leads to a contradiction. □

**Exercise 4.16**: Prove *Wilson's theorem*: a positive integer $p$ is prime if and only if

$$(p-1)! \equiv -1 \pmod{p}.$$

**Exercise 4.17**: For a few small (but not too small) primes $p$, find a generator of $(\mathbb{Z}/p\mathbb{Z})^*$.

**Exercise 4.18**: Prove the second part of Proposition 2.4.8.

## 2.5 Free Groups