# Algebraic Structures
MST20010

# Contents

# Chapter 0

# Sets and functions

In this chapter we quickly recall some basic notions and notation about sets and functions. It is there for reference only and is not part of the course: You should have seen it in first year, you will not be asked anything about it, but we will use the notation all the time.

The following resource:

`http://www.ucd.ie/msc/mathematicsresources/settheory/`

contains some very similar material, you might like it better.

## 0.1 Sets

For us, a set is simply be a collection of objects. These objects can be anything and are called the elements of the set. (This is a very intuitive notion of set, that will be sufficient for us. A precise study of the notion of set is beyond the scope of this course and is rather non-trivial. If you feel so inclined you may try to look up something called Russell's paradox.)

There are two main notations used for defining sets. In the first one, a set is given by listing all its elements, and in the second one the set is given by describing its elements:

**(1) Set given by listing its elements**

This is done for instance as follows:

$$\{1, -\pi, \star\},\ \{1, 2, 3, 4\}, \{\text{the colour blue}, -1, \text{the planet Mars}\}.$$

The ellipsis $(\ldots)$ can be used to indicate that the list of elements goes on "in the obvious way", for instance:

$$\{1, 2, 3, 4, \ldots\}$$

denotes the set of all positive integers (also denoted by $\mathbb{N}$).

**Set given by describing its elements**

This is usually done by giving a property that characterizes the elements of the set. For instance

$$\{n \mid n \text{ is a positive integer, and 3 divides n}\}$$

denotes the set $\{3, 6, 9, 12, \ldots\}$ (and reads "the set of all $n$ such that $n$ is a positive integer and 3 divides $n$"). . More generaly, this is done by indicating a letter that will be used in the property, and then indicating the property: The notation

$$\{x \mid \text{some property involving } x\}$$

means "the set of all elements (which we call $x$ in the following property) such that the given property is true for $x$".

---

In this case, if we want to know if some object (any kind of object) is in the set, we temporarilly call it $x$ and check if the property is true for this value of $x$. If it is, the element belongs to the set, if it is not, the element does not belong to the set.

**Example 0.1.** *1.* $\mathbb{N} = \{1, 2, 3, \ldots\}$ *the set of all positive integers.*

*2.* $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ *the set of all integers.*

*3.* $\mathbb{Q} = \{a/b \mid a, b \text{ are integers}, b \neq 0\}$*, the set of all rational numbers.*

*4.* $\mathbb{R}$ *denotes the set of all real numbers (it is more complicated to give a precise description of it).*

Some variations on the above notation are common and are usualy clear, for instance

$$\{x^2 \mid x \in \mathbb{R} \text{ and } x > 3\}$$

denotes the set of all squares of elements of $\mathbb{R}$ that are greater than 3 (it is equal to $(9, \infty)$).

**Remark 0.2.** *An important feature of sets is that a set is completely determined by the elements that it contains. In other words, if two sets contain the same elements, they are equal:*

$$\{1, 2\} = \{1, 2, 2, 2\} = \{2, 1\}, \ \{1, 2, 3\} \neq \{1, 2, 3, 4\}.$$

*As you can see, it means in particular that:*

1. *Repeating an element does not change the set;*
2. *The order in which the elements are listed does not matter.*

**Definition 0.3.** *The empty set is the set that does not contain any element. Using the notation introduced above, it can be written* $\{\}$*, but the most common notation for it is* $\emptyset$ *(an "O" with a diagonal bar).*

The notation $\boldsymbol{a \in B}$ means that $B$ is a set, and that $a$ is an element of $B$. We write $a \notin B$ to denote that $a$ is not an element of $B$. So, for instance:

$$3 \in \mathbb{N},\ -1 \notin \mathbb{N},\ 4 \notin \{-10, \star, \pi\}.$$

If $S$ and $T$ are both sets, the notation $\boldsymbol{S \subseteq T}$ (also written $\boldsymbol{S \subset T}$) means that every element of $S$ is also in $T$, and we say that $S$ **is contained in** $T$, or that $S$ **is a subset of** $T$. Similarly, the notation $S \not\subseteq T$ means that $S$ is not a subset of $T$, i.e. that there is at least one element of $S$ that is not in $T$. For instance

$$\{1,2\} \subseteq \{1,2,3\},\ \{1,2\} \subseteq \{1,2\},\ \mathbb{N} \subseteq \mathbb{Q},$$

but

$$\{-1,2\} \not\subseteq \mathbb{N},\ \mathbb{Q} \not\subseteq \{1,2,3\}.$$

**Remark 0.4.** *Observe that if $A$ is any set, then the empty set is a subset of $A$. Why? Because if it were not the case, then there would be an element in the empty set that is not in $A$ (by definition of being a subset). But the empty set does not contain any element, so it is not possible.*

We say that $S$ is a **proper subset** of $T$ if $S \subseteq T$ and $S \neq T$ (i.e. every element of $S$ is in $T$, and there is at least one element of $T$ that is not in $S$). This is denoted by $S \subsetneq T$ or $S \subsetneqq T$.

Finaly, if $S$ is a finite set, we denote by $|S|$ the number of elements in $S$. If $S$ is infinite, we write $|S| = \infty$. This number $|S|$ is called **the cardinality of S**.

## 0.2 Union and intersection

If $S$ and $T$ are two sets, we can build:

1. The **union** of $S$ and $T$, denoted $\boldsymbol{S \cup T}$. It is the set that consists of all the elements of $S$ together with all the elements of $T$:

   $$S \cup T = \{x \mid x \in S \text{ or } x \in T\}.$$

   For instance

   $$\{-3,4\} \cup \mathbb{N} = \{-3,1,2,3,4,5,\ldots\},$$
   $$\{1,2\} \cup \{\star,-6\} = \{1,2,\star,-6\}.$$

2. The **intersection** of $S$ and $T$, denoted $\boldsymbol{S \cap T}$. It is the set that consists of all the elements that are in both $S$ and $T$:

   $$S \cap T = \{x \mid x \in S \text{ and } x \in T\}.$$

   For instance

   $$\{-3,4\} \cap \mathbb{N} = \{4\},$$
   $$\{1,2\} \cap \{\star,-6\} = \emptyset.$$

## 0.3 Functions

Given two sets $S$ and $T$, a function (also called a map) from $S$ to $T$ is "something" that associates an element of $T$ to each element of $S$. If the function is called $f$, we denote this by $f : S \to T$, and the element from $T$ associated to an element $a$ from $S$ is denoted by $f(a)$ (and is called the image of $a$ by $f$).

This "something" can be anything that associates an element of $T$ to each element of $S$: A formula, a procedure explicitely described, or something completely arbitrary. A common compact notation for indicating how $f$ is defined is:

$$f : S \to T,\ x \mapsto \text{"how to get } f(x) \text{ out of } x\text{"},$$

see examples below.

**Examples 0.5.** *1. $f : \mathbb{N} \to \mathbb{N}$ given by $f(n) = n + 1$. The compact notation is $f : \mathbb{N} \to \mathbb{N},\ n \mapsto n + 1$.*

*2. $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = \sin(x) + x^2 - 1$. The compact notation is $g : \mathbb{R} \to \mathbb{R},\ x \mapsto \sin(x) + x^2 - 1$.*

*3. $f : \mathbb{Z} \to \mathbb{N}$ given by $f(-1) = 3$, $f(12) = 1$ and $f(x) = |x|$ if $x$ is different from $-1$ and $12$. The "compact" notation would be $f : \mathbb{Z} \to \mathbb{N},\ -1 \mapsto 3,\ 12 \mapsto 1,\ x \mapsto |x|$ if $x$ is not $-1$ or $12$, but would be rather cumbersome here.*

*4. $\varphi : \{-1, \star\} \to \mathbb{R}$ given by $\varphi(-1) = \pi$ and $\varphi(\star) = 0$.*

*5. $f : \mathbb{R} \to \mathbb{R},\ x \mapsto \sqrt{x}$ is not a map, because it is not defined for every element of $\mathbb{R}$ (only for the non-negative ones), but $f : [0, \infty) \to \mathbb{R},\ x \mapsto \sqrt{x}$ is a map.*

*6. If $S$ is a set, the map $S \to S,\ x \mapsto x$ is called **the identity map** (on $S$) and is denoted by $\mathrm{Id}_S$ (or simply $\mathrm{Id}$ if the set $S$ is clear from the context).*

**Definition 0.6.** *If $f : S \to T$ is a function, the set $S$ is called the* **domain** *of $f$ and the set $T$ its* **codomain**. *The set of all the images of elements of $S$ is called the* **image of** *$f$ and is denoted by $f(S)$:*

$$f(S) = \{f(x) \mid x \in S\}.$$

**Definition 0.7.** *Let $f$ and $g$ be two functions. We say that $f$ and $g$ are equal (and write $f = g$) if:*

*1. They have the same domain and codomain;*

*2. They agree on each element of the domain, i.e. if the domain is $S$: $f(x) = g(x)$ for every $x \in S$.*

Two properties of maps are particularly important:

**Definition 0.8.** *Let $f : S \to T$ be a function.*

*1. We say that $f$ is* **injective** *if for every $x, y \in S$ with $x \neq y$ we have $f(x) \neq f(y)$.*
*It is equivalent to saying that for all $x, y \in S$, if $f(x) = f(y)$, then $x = y$.*

2. *We say that $f$ is* **surjective** *if every element of $T$ can be obtained as $f(x)$ for some $x \in S$. In other words, if $f(S) = T$.*

3. *A function that is both injective and surjective is called* **bijective**. *We also say that it is a* **bijection**.

You may encounter the terminology "one to one" for injective and "onto" for surjective, but we will avoid using it.

**Example 0.9.** 1. *$f : \mathbb{R} \to \mathbb{R},\ x \mapsto x + 1$ is injective, since $f(x) = f(y)$ implies $x = y$. It is also surjective, since every element of $\mathbb{R}$ is in the image of $f$.*

2. *$f : \mathbb{R} \to [0, \infty),\ x \mapsto x^2$ is not injective (since different elements of $\mathbb{R}$ can have the same image) and is surjective. However, $g : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$ is not surjective. Observe that the maps $f$ and $g$ are different (they do not have the same codomain).*

**Lemma 0.10.** *Let $f : S \to T$ be an injective map. Then $|S| = |f(S)|$.*

*Proof.* We first consider the case where $S$ is finite, so $S = \{x_1, \ldots, x_n\}$ where the $x_i$ are all different. By definition $f(S) = \{f(x_1), \ldots, f(x_n)\}$, so $|f(S)| \leq n$. We now check that $f(x_1), \ldots, f(x_n)$ are all different: If it where not the case, we would have $f(x_i) = f(x_j)$ for some $x_i \neq x_j$, but it is impossible since $f$ is injective. Therefore $f(S)$ has $n$ elements.

If $S$ is infinite: Let $T$ be a subset of $S$ with $n$ elements (where $n \in \mathbb{N}$). Then by the argument above $f(T)$ has $n$ elements. But $f(T) \subseteq f(S)$, so $f(S)$ has at least $n$ elements, for every $n \in \mathbb{N}$, i.e. $|f(S)| = \infty$. □

**Corollary 0.11.** *Let $f : S \to T$ be a map where $S$ and $T$ are finite with the same number of elements. Then $f$ injective is equivalent to $f$ surjective.*

*Proof.* If $f$ is injective: By the previous lemma we know that $|f(S)| = |S|$. Since $|S| = |T|$ we get $|f(S)| = |T|$. So $f(S) \subseteq T$ and both have the same finite number of elements, which shows that $f(S) = T$, i.e. that $f$ is surjective.

If $f$ is surjective. Write $S = \{x_1, \ldots, x_n\}$, with the $x_i$ all different. Then $f(S) = \{f(x_1), \ldots, f(x_n)\}$. Since $f(S) = T$ and $|T| = |S| = n$, we have $|f(S)| = n$, so the $f(x_i)$ must be all different, i.e. $f$ is injective. □

**Definition 0.12.** *Let $f : S \to T$ and $g : T \to W$ be maps. The* **composition** *of $f$ with $g$, denoted $g \circ f$ is the map*

$$g \circ f : S \to W,\ x \mapsto g(f(x)).$$

**Definition 0.13.** *Let $f : S \to T$. A map $g : T \to S$ is called the* **inverse** *of $f$ if $f \circ g = \mathrm{Id}_T$ and $g \circ f = \mathrm{Id}_S$.*
*(In other words: $f(g(x)) = x$ for every $x \in T$ and $g(f(y)) = y$ for every $y \in S$.) The map $g$ is denoted by $f^{-1}$.*

*We say that $f$ is* **invertible** *if it has an inverse.*

**Remark 0.14.** *In the previous definition, we called $g$* the *inverse of $f$. We can do this because it is not very hard to check that if $f$ is invertible, then it has only one inverse: If both $g$ and $g'$ are inverses of $f$, then we must have $g = g'$. This is left as an exercise (use that $g(f(y)) = y$ and that $f$ is surjective).*

**Proposition 0.15.** *1. Let $f$ and be a map. Then $f$ has an inverse if and only if $f$ is bijective.*

*2. Let $f : S \to T$ and $g : T \to U$ be bijective maps. Then $g \circ f$ is bijective and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$*

# Chapter 1

# $\mathbb{Z}/n\mathbb{Z}$, the integers modulo $n$, aka clock arithmetic

## 1.1 The clock example

Imagine a standard clock with numbers from 1 to 12. Adding 3 hours to 11 o'clock gives 2 o'clock, so $11 + 3 = 2$. Similarly, adding 30 hours to 2 o'clock gives 8 o'clock, so $30 + 2 = 8$. Again similarly: $17 = 5$, $2 - 5 = 9$, etc.

What is happening here? We simply identify 12 with 0, which means that all multiples of 12 "disappear". In other words, if we look at a number, we discard all multiples of 12, so that, for instance: $17 = 1 \times 12 + 5$, so $17 = 5$. Also: $2 - 5 = 9$ because $2 - 5 = 12 + 2 - 5 = 9$, $-2 = 12 + (-2) = 10$, $27 = 2 \times 12 + 3 = 3$.

This could be done in exactly the same way if we had $n$ numbers on the clock (where $n$ is any integer) instead of 12. We will do this next, except that we will write:
– in the case of a normal clock: 0 instead of 12 (it is more convenient), so that the numbers will be $0, 1, 2, \ldots, 11$
– in the case of a clock with $n$ numbers: 0 instead of $n$, so that the numbers will be $0, 1, \ldots, n - 1$.

## 1.2 $\mathbb{Z}/n\mathbb{Z}$

Recall the following:

**Division of integers**

Let $m \in \mathbb{Z}$ and $n \in \mathbb{N}$. There are $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n - 1\}$ such that

$$m = nq + r.$$

$q$ is called the quotient in the division of $m$ by $n$, and $r$ the remainder. The element $r$ is denoted $m \bmod n$ (we read $m$ modulo $n$).

**Example 1.1.** *Following the clock example above:* $26 \bmod 12 = 2$ *(because* $26 = 12 \times 2 + 2$*. If we use a clock with numbers from 1 to 10:* $26 \bmod 10 = 6$ *(*$26 = 10 \times 2 + 6$*).*

**What does it mean?**

If we look at the previous example, it gives us that:

- 26 is the same as 2 on a 12-hour clock, because the difference between them is a multiple of 12.
- 26 is the same as 6 on a 10-hour clock, because the difference between them is a multiple of 10.

So: If we divide $m$ by $n$, the remainder $r$ tells us that $m$ will be the same as $r$ on a clock with $n$ numbers.

The notation "mod $n$" is also used to indicate that two integers have the same remainder in the division by $n$:
If $a, b \in \mathbb{Z}$, we say that $a$ and $b$ are equal modulo $n$, and write $a = b \bmod n$, if $a$ and $b$ have the same remainder modulo $n$ (in other words: they are the same on a clock with $n$ numbers). For instance:

$$26 = 2 \bmod 12, \quad 26 = 6 \bmod 10$$

$$1 = 3 \bmod 2, \quad 7 = 11 \bmod 4.$$

**Definition 1.2.** *For* $n \in \mathbb{N}$*, we denote by* $\mathbb{Z}/n\mathbb{Z}$ *the set of all remainders in the division of integers by* $n$*, so:*

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}.$$

We also define a sum $+_n$ and a product $\cdot_n$ of elements of $\mathbb{Z}$ with value in $\mathbb{Z}/n\mathbb{Z}$ as follows:

- $a +_n b = (a + b) \bmod n$,
  i.e. compute the usual sum $a + b$ then take the remainder in the division by $n$.
- $a \cdot_n b = (a \cdot b) \bmod n$,
  i.e. compute the usual product $a \cdot b$ then take the remainder in the division by $n$.

**This is exactly what would happen on a clock with numbers from 0 to** $n - 1$**.**

**Examples 1.3.** *This sum and product can be used to compute sum and product of elements of* $\mathbb{Z}/n\mathbb{Z}$ *and get results in* $\mathbb{Z}/n\mathbb{Z}$ *again (we will come back to this later):*

1. *Take $n = 4$. Then $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$. The table of the operation $+_4$ is*

| $+_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

*and the table of the product is*

| $\cdot_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

2. *Take $n = 5$. Then $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ and $3 + 4 = 2$, $3 \cdot 4 = 2$, $4 \cdot 4 = 1$.*
3. *Take $n = 8$. Then $\mathbb{Z}/8\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and $3 + 4 = 7$, $3 \cdot 4 = 4$, $4 \cdot 4 = 0$.*

We will often drop the index $n$ and simply write $+$ and $\cdot$ instead of $+_n$ and $\cdot_n$ when the context is clear enough.

We finish with some very important properties of the sum and product in $\mathbb{Z}/nZ$.

**Proposition 1.4.** *Let $a, b \in \mathbb{Z}$. Then the following equalities are true in $\mathbb{Z}/n\mathbb{Z}$:*

$$a +_n b = (a \bmod n) +_n (b \bmod n) = (a \bmod n) +_n b = a +_n (b \bmod n),$$

$$a \cdot_n b = (a \bmod n) \cdot_n (b \bmod n) = (a \bmod n) \cdot_n b = a \cdot_n (b \bmod n).$$

**What does it mean?**

It means that at any stage in a computation modulo $n$, you can replace any integer $x$ by $x \bmod n$ (recall that is is the remainder in the division of $x$ by $n$. It is usually a smaller number, so should simplify the computation).

*Proof.* We only check $a +_n b = (a \bmod n) +_n b$, the others are similar. This equality means that the integers $a+b$ and $(a \bmod n)+b$ have the same remainder modulo $n$. Write $a = xn+r$ and $b = yn+s$ with $x, y \in \mathbb{Z}$ and $r, s \in \{0, 1, \ldots, n-1\}$ the remainders of $a, b$ modulo $n$.

Then $a+b = (x+y)n+(r+s)$ and $(a \bmod n)+b = r+yn+s = yn+(r+s)$. We do the division of $r+s$ by $n$ and obtain $r+s = kn+t$ with $t \in \{0, 1, \ldots, n-1\}$ so

$$a + b = (x + y + k)n + t, \quad \text{and } (a \bmod n) + b = (y + k)n + t,$$

so $a + b$ and $(a \bmod n) + b$ have the same remainder modulo $n$. □

We now list of few rather obvious properties of sum and product modulo $n$. We do this mostly for future reference.

**Proposition 1.5.** *Let $a, b, c \in \mathbb{Z}/n\mathbb{Z}$ (or in $\mathbb{Z}$). The following equalities hold:*

1. *Properties involving only the sum:*

$$a +_n b = b +_n a,$$
$$(a +_n b) +_n c = a +_n (b +_n c),$$
$$a +_n 0 = a,$$
$$a +_n (-a) = 0.$$

2. *Properties involving only the product:*

$$a \cdot_n b = b \cdot_n a,$$
$$(a \cdot_n b) \cdot_n c = a \cdot_n (b \cdot_n c),$$
$$a \cdot_n 1 = a,$$

3. *Multiplication distributes over addition:*

$$a \cdot_n (b +_n c) = a \cdot_n b +_n a \cdot_n c.$$

*Proof.* All properties are either trivial (for instance $a +_n 0 = a$) or are easily checked using Proposition 1.4. As an example we check $(a +_n b) +_n c = a +_n (b +_n c)$. By definition:

$$\begin{aligned}(a +_n b) +_n c &= [(a + b) \bmod n] + c \bmod n \quad \text{by definition of } +_n \\ &= ((a + b) + c) \bmod n \quad \text{by Proposition 1.4} \\ &= (a + (b + c)) \bmod n \\ &= a + [(b + c) \bmod n] \bmod n \quad \text{by Proposition 1.4} \\ &= a +_n (b +_n c).\end{aligned}$$

□

**Example 1.6.**

- *We compute $(5 + 12) \cdot 62$ in $\mathbb{Z}/3\mathbb{Z}$:*

  $5 = 2$, $12 = 0$, $62 = 2$. *So* $(5 + 12) \cdot 62 = 2 \cdot 2 = 4 = 1$.

- *We compute $56^{34}$ in $\mathbb{Z}/3\mathbb{Z}$:*

  $56 = 2$, *so* $56^{34} = 2^{34}$. *We look now at the powers of* 2 *in* $\mathbb{Z}/3Z$:

$$2,\ 2^2 = 4 = 1,\ 2^3 = 2^2 2 = 2,\ 2^4 = 2^3 2 = 2 \cdot 2 = 1,$$
$$2^5 = 2^4 2 = 2, 2^6 = 2^5 2 = 4 = 1, \cdots$$

  *So we see that $2^k = 1$ whenever $k$ is a multiple of* 2. *So $2^{34} = 1$ in $\mathbb{Z}/3\mathbb{Z}$, i.e. $56^{34}$ is a multiple of* 3 *plus* 1. *In other words, $56^{34} - 1$ is a multiple of* 3.

  *This approach to computations has many practical applications.*

**Remark 1.7. (Important)** *In the second example, we replaced* 56 *by* 2 *(since* $56 = 2 \bmod 3$*) but we did NOT replace* 34 *by* 1 *(despite the fact that* $34 = 1 \bmod 3$*). It is because Proposition 1.4 tells us that we can replace numbers in a product, but not in an exponent.*

*And replacing numbers in an exponent is usually wrong. Here, replacing* 34 *by* 1 *would give us a wrong result:* $56^1 = 56 = 2$ *in* $\mathbb{Z}/3\mathbb{Z}$*, not the right result...*

*Be careful with this!*

# Chapter 2

# Groups, part 1

## 2.0 Some idea of the motivations

Let us first consider an example (from a long time ago):

Looking at different triangles with side lengths $a$, $b$, $c$, you notice that in many cases, you get $a^2 + b^2 = c^2$. Then you may not be satisfied anymore with checking it for every new triangle, and you want to understand better when it does happen. Thinking further, you could come up with the notion of right-angled triangle and show in general that this relation is true for every such triangle. In this way you don't have to check it again, you only need to check if you have a right angle.

Something similar happened in algebra sometime in the early 19th century. People where working with sets that had one operation, and probably ended up doing again and again very similar reasonings, to get very similar results.[1] (I did not check the history in detail.) When this happens, it is natural to wonder if there is a common setup that would explain all these similar results, and allow to prove them once and for all.

Eventually, a common setup that would cover all these different cases was indeed devised: It is the notion of group. We say that we have a group if we have a set together with an operation on this set that has some "nice enough" properties (see Definition 2.2). These properties make it possible to prove a lot of results once and for all (we will only need to check that what we have is a group, and the results proved for groups wil be automatically true. So it will apply to a lot of different situations).

## 2.1 Introduction to groups

**Definition 2.1.** *Let $S$ be a set. An **operation** on $S$ is a map from $S \times S$ to $S$, i.e. a map that takes as input two elements of $S$ and returns an element of $S$.*

*Such a map is usually not written as a function, in the form $f(a, b)$, but rather in the form $a \star b$ (similar to how we usually write sum or product). Of course, we may use other symbols than $\star$.*

[1] This was all linked to the study of solutions of equations $P(x) = 0$ where $P$ is a polynomial, and the proof there is no general formula if the degree of $P$ is at least 5.

You already know plenty of examples: The sum or the product in $\mathbb{Z}$, in $\mathbb{Z}/n\mathbb{Z}$, in $\mathbb{R}$, $M_n(\mathbb{C})$, the composition of maps, etc. Anything that takes two elements from a set and returns an element from the same set is an operation. (Strictly speaking it should be called a binary operation, because it takes 2 entries, but we will only look at these, so we drop the "binary".)

**Definition 2.2.** *A group is a set $G$ together with an operation $\star$ on $G$ that has the following "nice" properties:*

*(G1) For every $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$.*

*(We say that the operation $\star$ is associative.)*

*(G2) There is an element $e \in G$ such that $e \star a = a$ and $a \star e = a$ for every $a \in G$.*

*(We say that $e$ is an identity element for the operation $\star$.)*

*(G3) For every $a \in G$ there is $b \in G$ such that $a \star b = e$ and $b \star a = e$.*

*(Every element has an inverse for $\star$; $b$ is called an inverse of $a$.)*

*Additionally, the group is called* ***commutative*** *(or* ***abelian****) if the following property also holds:*

*(G4) For every $a, b \in G$, $a \star b = b \star a$.*

*We will denote such a group by $(G, \star)$ (since it is given by both the set $G$ and the operation $\star$).*

**Definition 2.3.** *The order of a group $(G, \star)$ is the number of elements in $G$. It is an integer or $\infty$. We denote it by $|G|$ or $o(G)$.*

When $|G|$ is finite, we say that $G$ is finite, and otherwise that $G$ is infinite.

**Examples 2.4.** *1. $(\mathbb{Z}, +)$ is a group.*

*$0$ is an identify element of this group. Why is that?*

*We check property (G2) in Definition 2.2: For this we take $G = \mathbb{Z}$, $\star = +$ and $e = 0$ and see if the property holds, i.e., do we have*

$$0 + a = a \text{ and } a + 0 = a \text{ for every } a \in \mathbb{Z}?$$

*Obviously yes, so $0$ is an identity element for the operation $+$ on $\mathbb{Z}$.*

*Similarly, it is easy to check property (G1), and also property (G3) (with $e = 0$ since we found that $e$ is an identity).*

*The group $(\mathbb{Z}, +)$ is abelian and infinite.*

*2. Similarly $(\mathbb{R}, +)$ is also a group. The element $0$ is an identity element. The group $(\mathbb{R}, +)$ is abelian and infinite.*

*3. $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group: Properties G1, G2, G3 are true if you replace $G$ by $\mathbb{Z}/n\mathbb{Z}$ and $\star$ by $+$. The element $0$ is an identity element. This group has order $n$.*

*4. $(\mathbb{R} \setminus \{0\}, \cdot)$ is a group: Properties G1, G2, G3 are true if you replace $G$ by $\mathbb{R} \setminus \{0\}$ and $\star$ by $\cdot$. The element $1$ is an identity element. This group is infinite and abelian.*

5. *$(\mathbb{R}, \cdot)$ is not a group. How do we see it? It means that at least one of properties (G1), (G2) or (G3) is false. Properties (G1) and (G2) are true (same as in the previous case), and $1$ is an identity element (it is also the only identity element, because it is the only element $e$ that will work in property (G2)). We look now at property (G3): The problem is when we take $a = 0$. Then you want $a \cdot b = 1$ for a well-chosen $b$, which is not possible since $a \cdot b = 0 \cdot b = 0$. So property (G3) does not hold.*

6. *We denote by $\mathrm{GL}_n(\mathbb{R})$ the set of all invertible $n \times n$ matrices with coefficients in $\mathbb{R}$. Then $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ is a group with identity element the identity matrix $I_n$ of size $n$ (again: properties G1, G2, G3 are true if you replace $G$ by $\mathrm{GL}_n(\mathbb{R})$ and $\star$ by $\cdot$). It is infinite, but not abelian (if $n \geq 2$): in general $AB \neq BA$ for matrices.*

We will see more examples of groups later.

**Remark 2.5.** 1. *So, a group is simply a set together with an operation that has a few nice properties. We do not know in general what set it is or what the operation is, except that it has the properties listed in the definition. So every time we will want to prove a result about groups, we will only be able to use what the definition of groups gives us, and nothing more.*

2. *Why do this?*

   *The properties that appear in the definition of group are rather common in mathematics (we saw a few examples, and will see more) and even in sciences in general[2], and have many interesting consequences. Investigating what we can obtain using only the definition of group (and not what $G$ precisely is or what the operation is) will allow us to prove results that will be true every time we have a group, so that we will not have to prove them again and again for each different example.*

3. *Why this particular list of properties in the definition of group? Could we have taken other properties?*

   *These properties were chosen so that: They occur often, and there are enough of them to be able to prove interesting results. But people who defined groups could very well have chosen a different set of "nice" properties for their definition (it would have given a different concept). In practice we often add to this list of properties to look at more precise cases, for instance we saw property (G4) that asks a little bit more.*

   *That being said, this definition was well chosen, and it is possible to prove quite a lot of results with this particular list of properties, so people stick to it.*

We will now spend a few minutes looking at some very basic properties of groups, then will look at a few more examples (one of them for quite some time), then will come back to groups in general.

[2]Some book titles from the UCD library: Group theory and quantum mechanics, Molecular symmetry and group theory, Group theory and physics, Chemical applications of group theory, Group theory for atoms, molecules and solids, Group theory in physics, Topics in group theory and computation, Group theory for the physical properties of crystals, Group theory and chemistry, Applied group theory for chemists, physicists and engineers, Readable group theory for chemists.

**Notation 2.6.** *We will write $a^{-1}$ for the inverse of $a$ (the element called $b$ in definition 2.2). The terminology "the" inverse suggests that $a$ has only one inverse. We will actually check this in Lemma 2.7.*

*It is also usual to write $\cdot$ instead of $\star$ and call the operation "multiplication", or "product". We then write $a \cdot b$ instead of $a \star b$ for $a, b \in G$. We can even go further and replace $\cdot$ by the "empty notation". We then write $ab$ instead of $a \cdot b$ and simply $G$ instead of $(G, \cdot)$.*

**Lemma 2.7.** *Let $G$ be a group. The following properties hold:*

1. *The identity element is unique;*
2. *The inverse of any element $a \in G$ is unique (i.e., $a$ has only one inverse, i.e., if $a$ has 2 inverses then they are equal);*
3. *For every $a \in G$, $(a^{-1})^{-1} = a$;*
4. *For every $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.*
5. *For every $a_1, \ldots, a_n \in G$, $(a_1 a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$.*

*Proof.* 1. By Definition 2.2, an element $e$ is called an identity element if

$$ae = ea = a \text{ for every } a \in G. \tag{2.1}$$

If we have another identity element $f$, then

$$af = fa = a \text{ for every } a \in G. \tag{2.2}$$

The trick is to look at $ef$ and compute it in two ways: Once using that $e$ is an identity element, once using that $f$ is an identity element.

If we use that $e$ is an identity element, we get $ef = f$ (take $a = f$ in line (2.1) above). If we use that $f$ is an identity element we get $ef = e$ (take $a = e$ in line (2.2) above).

Therefore $e = f$.

2. By Definition 2.2, an element $b$ is the inverse of $a$ if $ab = ba = e$. If $c$ is another inverse of $a$, then $ac = ca = a$. Computing $bac$ we obtain: $bac = ec = c$ (using that $ba = e$ and $e$ is the identity), and $bac = be = b$ (using that $ac = e$ and $e$ is the identity). So $c = b$.

3. We want to show that the inverse of $a^{-1}$ is equal to $a$. By Definition 2.2, an element $b$ is the inverse of $a^{-1}$ if $ba^{-1} = e$ and $a^{-1}b = e$. So we just have to check that the element $a$ has these two properties:

$$aa^{-1} = 1 \text{ (it is because } a^{-1} \text{ is the inverse of } a),$$

$$a^{-1}a = 1 \text{ (again, it is because } a^{-1} \text{ is the inverse of } a).$$

4. We want to show that the inverse of $ab$ is $b^{-1}a^{-1}$. Going back to the definition of the inverse (Definition 2.2), we have to show that $(ab)(b^{-1}a^{-1}) = e$

and $(b^{-1}a^{-1})(ab) = e$:

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} \text{ by associativity} \\ &= aea^{-1} \text{ since } b^{-1} \text{ is the inverse of } b \\ &= aa^{-1} \text{ since } ae = a \\ &= e \text{ since } a^{-1} \text{ is the inverse of } a.\end{aligned}$$

The verification of $(b^{-1}a^{-1})(ab) = e$ is similar and is left as a very worthwhile exercise. Do it!

5. This one is left as an exercise. You can either apply result 4. above $n-1$ times, or prove it directly using the same method as in 4.

□

**Notation 2.8.** *Let $G$ be a group and let $a \in G$. For $k \in \mathbb{N}$ we write $a^k$ for the product $a \cdot a \cdots a$ ($k$ times), and $a^{-k}$ for $a^{-1} \cdot a^{-1} \cdots a^{-1}$ ($k$ times). It is an easy exercise to check that $(a^k)^{-1} = a^{-k}$ (just compute to products $a^k a^{-k}$ and $a^{-k}a^k$ and check that both are equal to $e$, see the proof of Lemma 2.7).*

*We also define $a^0 = e$.*

*It is easy, but rather tedious (there are several cases to consider) to check that for every $r, s \in \mathbb{Z}$ and $a \in G$ we have*

$$a^r a^s = a^{r+s}.$$

*Note that it is obvious (by definition of $a^k$) if $r, s > 0$.*

**Notation 2.9.** *It is sometimes natural to use the symbol $+$ for the group operation (for instance in the case of $(\mathbb{Z}, +)$ or $(\mathbb{Z}/n\mathbb{Z}, +)$). In this case, the usual notation is to denote $e$ by $0$, and the element $a^{-1}$ by $-a$. Also, if $k \in \mathbb{N}$, the element $a+a+\cdots+a$ ($k$ times) is denoted by $ka$ and the element $(-a)+\cdots+(-a)$ ($k$ times) is denoted by $(-k)a$ (and is equal to $k(-a)$).*

**Lemma 2.10.** *Let $G$ be a group and let $a, u, w \in G$. The following properties hold:*

1. *$au = aw$ implies $u = w$ (left cancellation),*
2. *$ua = wa$ implies $u = w$ (right cancellation).*

*Proof.* We prove the first first statement and leave the second as an exercise. The elements $au$ and $aw$ are equal, so they stay equal if we multiply both on the left by $a^{-1}$: $a^{-1}au = a^{-1}aw$. But $a^{-1}a = e$, so $eu = ew$ and thus $u = w$. □

**Remark 2.11.** *In general there is no "mixed" cancellation law:*

$$au = wa \not\Rightarrow u = w,$$

*because there is no reason why we should have $au = ua$ (this would allow us to prove this statement, using lemma 2.10), since in general our group $G$ may not be abelian. In case $G$ is abelian, we do have such a cancellation law.*

## 2.2 The order of an element

**Definition 2.12.** *Let $G$ be a group and let $a \in G$. The **order** of $a$, denoted $o(a)$ (or $|a|$), is the least positive integer $k$ such that $a^k = e$. If no such integer exists, then the order of $a$ is defined to be infinite.*

**Lemma 2.13.** *Let $G$ be a finite group, and let $a \in G$. Then $o(a)$ is finite.*

*Proof.* Consider the powers of $a$: $a, a^2, a^3, \ldots$. They cannot be all different since they all belong to $G$ and $G$ is finite. So there are $i, j \in \mathbb{N}$ such that $a^i = a^{i+j}$, in other words: $a^i = a^i a^j$. Therefore $(a^i)^{-1}a^i = (a^i)^{-1}a^i a^j$, so $e = ea^j$ and thus $e = a^j$. □

We will prove a much more precise result later: $o(a)$ is always a divisor of $|G|$.

**Remark 2.14.** *You may find the document "Groups 1" on the following page (from the maths support centre) useful to help you understand the notion of group:*

*http://www.ucd.ie/msc/mathematicsresources/advancedalgebraandproofs/*

# Chapter 3

# Permutations

**Definition 3.1.** *Let $X$ be a set. A* **permutation of $X$** *is a bijection from $X$ to $X$. We denote by $S(X)$ the set of all permutations of $X$.*

Permutations have some very interesting properties, and are also regularly used as a tool to describe more complicated objects in mathematics.

We will only consider the case where $X$ is finite and has $n$ elements, say $X = \{x_1, \ldots, x_n\}$. Furthermore:

> To simplify notation, we will only consider the case $X = \{1, \ldots, n\}$.
>
> (for the more general case, simply replace 1 by $x_1$, 2 by $x_2$, and so on... in what follows)

If $f \in S(X)$, then $f(1) = i_1$ (for some $i_1 \in \{1, \ldots, n\}$), $f(2) = i_2$ (for some $i_2$), $\ldots$, $f(n) = i_n$ (for some $i_n$). So we could denote $f$ by

$$f : X \to X,\ 1 \mapsto i_1,\ 2 \mapsto i_2, \ldots,\ n \mapsto i_n.$$

This notation is a bit cumbersome, so we will use a more compact notation:

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

where the first row lists all the elements of $X$, and we indicate under each one of them its image under $f$.

**Example 3.2.** *The map*

$$g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

*is the permutation of $\{1, 2, 3\}$ that sends 1 to 2, 2 to 1 and 3 to 3 (so: $g(1) = 2$, $g(2) = 1$, $g(3) = 3$).*

**Definition 3.3.** *We denote by $S_n$ the set of all permutations of $\{1, \ldots, n\}$.*

Let us go back to our notation for elements of $S_n$:

$$\begin{pmatrix} 1 & 2 & \dots, & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

denotes the map that sends 1 to $i_1$, 2 to $i_2$, ..., $n$ to $i_n$. Observe that since this map is bijective, we have:

1. $i_1$, $i_2$, ..., $i_n$ are all different (because it is injective);
2. the list $i_1$, $i_2$, ..., $i_n$ contains all the elements $1, 2, \dots, n$, just possibly in a different order (because the map is surjective).

**Proposition 3.4.** *The set $S_n$ has $n!$ elements.*

*Proof.* To construct an element of $S_n$ we have to give the sequence $i_1, i_2, \dots, i_n$. We have $n$ choices for $i_1$, $n-1$ choices for $i_2$ (since it has to be different from $i_1$, $n-2$ choices for $i_3$, ..., 2 choices for $i_{n-1}$, and finally only one choice for $i_n$ (the only remaining element). The total number of possibilities in building an element of $S_n$ is therefore

$$n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!. \qquad \square$$

**Remark 3.5.** *The value of $n!$ grows quite quickly as $n$ increases. For instance* $3! = 6$, $4! = 24$, $5! = 120$, ..., $10! = 3628800$, ...,

$$50! = 30414093201713378043612608166064768844377641568960512000000000000.$$

*So we will only see examples with small values of $n$.*

If $\sigma$ and $\gamma$ are in $S_n$, i.e., are bijective maps from $\{1, \dots, n\}$ to $\{1, \dots, n\}$, we know that $\sigma \circ \gamma$ and $\gamma \circ \sigma$ are also bijective maps from $\{1, \dots, n\}$ to $\{1, \dots, n\}$. i.e. belong to $S_n$ (see Proposition 0.15).

**Notation 3.6.** *We will constantly use the composition of elements of $S_n$, so to make the notation a bit easier, we will almost always drop the symbol $\circ$, i.e. we will simply write $\sigma\gamma$ for the composition of maps $\sigma \circ \gamma$. We will also simply call $\circ$ the product on $S_n$.*

**Remark 3.7.** *Remember that the composition of maps is computed from right to left, i.e. $\sigma \circ \gamma(x) = \sigma(\gamma(x))$. So if $\gamma(1) = 6$ and $\sigma(6) = 3$, then $\sigma\gamma(1) = 3$.*

**Examples 3.8.** *1. Compute $\sigma\gamma$ and $\gamma\sigma$ where*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \ \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

*Solution:*

$$\sigma\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

*How did we obtain this?*
*$\gamma$ sends 1 to 3 and $\sigma$ sends 3 to 2, so $\sigma\gamma(1) = 2$. Similarly:*

$\gamma(2) = 1$ *and* $\sigma(1) = 3$, *so* $\sigma\gamma(2) = 3$;
$\gamma(3) = 4$ *and* $\sigma(4) = 4$, *so* $\sigma\gamma(4) = 4$;
$\gamma(4) = 2$ *and* $\sigma(2) = 1$, *so* $\sigma\gamma(4) = 1$.

*We also obtain (exercise, do it and check that you get the right result)*

$$\gamma\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

*Observe that* $\sigma\gamma \neq \gamma\sigma$. *It means that the order in which we write the elements can change the result! (So be careful about the order.)*

2. *Compute* $\sigma^2$ $(= \sigma\sigma)$ *and* $\sigma^3$ $(=\sigma\sigma\sigma)$ *with the same* $\sigma$ *as above.*
*Solution:*

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix},$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

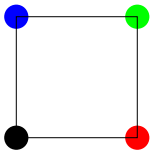
*Observe that we obtain* $\sigma^3 = \mathrm{Id}$. *We will come back to this later (in Proposition 3.15).*

3. *Compute*

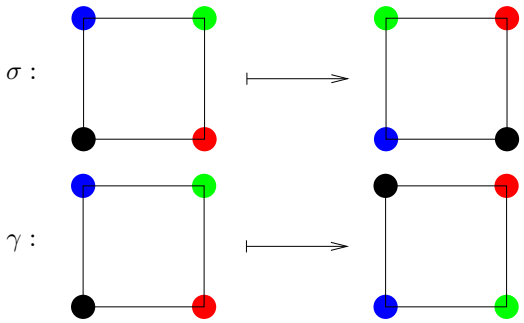
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix}.$$

**Remark 3.9.** *In the above example we obtained that* $\sigma\gamma \neq \gamma\sigma$, *so the composition of elements of* $S_n$ *(the product on* $S_n$*) is not commutative: The order in which we compute the product does matter!*

*This is something that does occur in the "real world". A simple example can be provided by a square (in space) with a different colour at each vertex, for instance:*

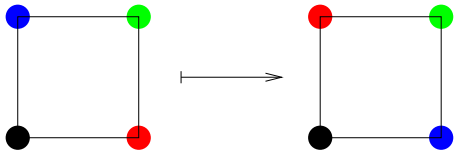


*Let* $\sigma$ *be the operation "rotate the square counterclockwise by 90 degrees", and let* $\gamma$ *be the operation "flip the square around the horizontal axis":*



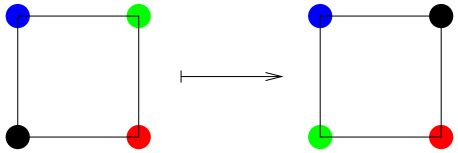
*Imagining the movements of the square in space (or cut a square piece of paper and colour its corners), we obtain:*

$\sigma\gamma$ :



*(remember, we apply $\gamma$ first)*

$\gamma\sigma$ :



*(this time we appled $\sigma$ first).*

The first two statements in the following proposition are general properties of the composition of functions, and the third one is a direct consequence of the fact that the elements of $S_n$ are bijective maps.

**Proposition 3.10.** *Let $\sigma, \gamma, \tau \in S_n$. Then*

1. *$(\sigma\gamma)\tau = \sigma(\gamma\tau)$ (the product in $S_n$ is associative);*
2. *$\mathrm{Id}\,\sigma = \sigma\,\mathrm{Id} = \sigma$ (Id is an identity element for the product in $S_n$);*
3. *For every $\sigma$ in $S_n$ there is a map $\gamma$ in $S_n$ such that $\sigma\gamma = \gamma\sigma = \mathrm{Id}$ (take $\gamma = \sigma^{-1}$). In other words, every element in $S_n$ has an inverse.*

**Corollary 3.11.** *The set $S_n$, with operation the composition of maps, is a group.*

In particular every property that we have already proved for groups is true in $S_n$.

**Remark 3.12.** *How do we compute something like $(\sigma\gamma)^2$?*
*By definition it is the product of $\sigma\gamma$ by $\sigma\gamma$, so:*

$$(\sigma\gamma)^2 = (\sigma\gamma)(\sigma\gamma) = \sigma\gamma\sigma\gamma.$$

*WARNING:*
*As observed above, this product is not commutative, so we cannot change the order of the elements in it. In particular we cannot regroup the $\sigma$ and the $\gamma$ together and expect to get the same result: In general $(\sigma\gamma)^2 \neq \sigma^2\gamma^2$. You can use the following simple example to convince you of this:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

*We have*

$$\sigma\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad (\sigma\gamma)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

*but*

$$\sigma^2 = \gamma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{Id}, \text{ so } \sigma^2\gamma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{Id}\,.$$

Since $S_n$ is a group, we can use what we already proved about groups:

**Proposition 3.13.** *1. Let $\sigma, \sigma_1, \ldots, \sigma_k \in S_n$. Then*

$$(\sigma_1\sigma_2\cdots\sigma_k)^{-1} = \sigma_k^{-1}\sigma_{k-1}^{-1}\cdots\sigma_2^{-1}\sigma_1^{-1}.$$

*2. Let $\sigma, \gamma, \tau \in S_n$. Then*

$$\sigma\gamma = \sigma\tau \text{ implies } \gamma = \tau,$$

*and*

$$\gamma\sigma = \tau\sigma \text{ implies } \gamma = \tau.$$

*In other words, it is possible to cancel on the left and on the right.*

*Proof.* The first part is Lemma 2.7, and the second is Lemma 2.10. To get a bit of extra practice, we redo the proof of some of it: Since $\sigma\gamma = \sigma\tau$, we still have an equality if we compose on the left by $\sigma^{-1}$:

$$\sigma^{-1}\sigma\gamma = \sigma^{-1}\sigma\tau,$$

so (using Proposition 3.10):

$$(\sigma^{-1}\sigma)\gamma = (\sigma^{-1}\sigma)\tau,$$

which gives, since $\sigma^{-1}\sigma = \mathrm{Id}$: $\mathrm{Id}\,\gamma = \mathrm{Id}\,\tau$, so $\gamma = \tau$. □

**Example 3.14.** *1.*

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

*How did we obtain this? If $\sigma(x) = y$, then, applying the function $\sigma^{-1}$ (let's not forget that the elements of $S_n$ are functions) to both sides, we obtain $\sigma^{-1}(\sigma(x)) = \sigma^{-1}(y)$, i.e. $\sigma^{-1}(y) = x$. In other words, $\sigma^{-1}$ is just $\sigma$ in "reverse" order.*

*2. Check that $(\sigma^k)^{-1} = (\sigma^{-1})^k$. We denote this element by $\sigma^{-k}$.*

*3. We will not spend the time to check it carefully, but the following is easy to check (there are many cases to consider, and it is not very interesting): For every $\sigma \in S_n$ and every $r, s \in \mathbb{Z}$, we have*

$$\sigma^r\sigma^s = \sigma^{r+s},$$

*with the convention that $\sigma^0 = \mathrm{Id}$.*

**Proposition 3.15.** *Let $\sigma \in S_n$. Then there is $k \in \mathbb{N}$ (which may depend on $\sigma$) such that $\sigma^k = \mathrm{Id}$. Recall that the smallest such $k$ is called the **order** of $\sigma$.*

*Proof.* We already proved this result (and saw this definition) for groups. □

**Example 3.16.** *Determine the order of* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$.

*(How to do this? Compute the successive powers of this element of* $S_n$ *and stop when you get the identity map:*

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

*We will see later a more efficient way to compute the order of an element of* $S_n$*.)*

## 3.1 Cycles

**Definition 3.17.** *A permutation* $\sigma \in S_n$ *is called a* **cycle of length** $k$ *if there are elements* $a_1, \ldots, a_k \in \{1, \ldots, n\}$*, all different, such that*

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3, \ldots,\ \sigma(a_{k-1}) = a_k,\ \sigma(a_k) = a_1,$$

*and* $\sigma(x) = x$ *for all the other elements of* $\{1, \ldots, n\}$ *(*$\sigma$ *does not move the other elements).*

*We write* $(a_1\ a_2 \cdots a_k)$ *to denote the cycle* $\sigma$*.*

**Remark 3.18.**

1. *Observe that* $(a_1\ a_2 \cdots a_k) = (a_i\ a_{i+1} \cdots a_k\ a_1\ a_2 \cdots a_{i-1})$ *for every* $i$ *in* $\{1, \ldots, k\}$ *(so we can start writing the cycle where we want, as long as we "cycle").*
2. *A cycle of length one:* $(a)$*, is the identity map, because it sends* $a$ *to* $a$*, and it does not move the other elements.*

**Example 3.19.**

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (1\ 6\ 2\ 3\ 5\ 4) = (2\ 3\ 5\ 4\ 1\ 6)$$

*is a cycle of length* 6*. Observe again that if an element* $x$ *does not appear in the cycle notation, we have* $\sigma(x) = x$*. For instance here* $\sigma(7) = 7$*.*

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix} = (2\ 4\ 3)$$

*is a cycle of length* 3*.*

*Not every permutation is a cycle:*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1\ 2\ 4\ 3)(5\ 6)$$

*is a product of a cycle of length 4 and a cycle of length 2, and is not a cycle.*

**Proposition 3.20.** *The order of a cycle of length $k$ is $k$.*

**Definition 3.21.** *Two cycles in $S_n$, $(a_1\ a_2\ \cdots a_k)$ and $(b_1\ b_2\ \cdots b_\ell)$, are called* **disjoint** *if $a_i \neq b_j$ for all $i$ and $j$.*

**Example 3.22.** *The cycles (in $S_6$) $(1\ 2\ 6)$ and $(3\ 5)$ are disjoint, the cycles $(1\ 3\ 5)$ and $(3\ 6)$ are not. Computing their products, we observe:*

$$(1\ 2\ 6)(3\ 5) = (3\ 5)(1\ 2\ 6),$$

*but*

$$(1\ 3\ 5)(3\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 4 & 1 & 5 \end{pmatrix} = (1\ 3\ 6\ 5) \neq$$

$$(3\ 6)(1\ 3\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 5 & 4 & 1 & 3 \end{pmatrix} = (1\ 6\ 3\ 5).$$

**Proposition 3.23.** *Let $\sigma$ and $\gamma$ be two disjoint cycles in $S_n$. Then $\sigma\gamma = \gamma\sigma$.*

**How can we prove this?**

How can we prove an equality $\sigma = \tau$ when $\sigma$ and $\tau$ are in $S_n$?
We can sometimes do it with a clever computation if we have some information about $\sigma$ and $\tau$, but there is another way that is sometimes useful.
Remember that both $\sigma$ and $\tau$ are functions from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$. And two functions are equal if they always return the same value. So $\sigma = \tau$ if for every $x \in \{1, \ldots, n\}$ we have $\sigma(x) = \tau(x)$.

*Proof.* Write $\sigma = (a_1\ a_2 \cdots a_k)$ and $\gamma = (b_1\ b_2 \cdots b_\ell)$. We have to show that $\sigma\gamma(x) = \gamma\sigma(x)$ for every $x \in \{1, \ldots, n\}$.

If $x \notin \{a_1, \ldots, a_k, b_1, \ldots, b_\ell\}$ then $\sigma(x) = x$ and $\gamma(x) = x$, so $\sigma\gamma(x) = x = \gamma\sigma(x)$.

If $x = a_i \in \{a_1, \ldots a_k\}$. By definition of $\sigma$, $\sigma(a_i) = a_j$ where $j = i + 1$ if $i \in \{1, \ldots, k\}$ and $j = 1$ if $i = k$. Observe also that $\gamma(a_i) = a_i$ and $\gamma(a_j) = a_j$ since the cycles are disjoint and thus $a_i, a_j \notin \{b_1, \ldots, b_\ell\}$. Therefore

$$\sigma\gamma(a_i)) = \sigma(\gamma(a_i)) = \sigma(a_i) = a_j,$$

and

$$\gamma\sigma(a_i) = \gamma(a_j) = a_j.$$

If $x = b_i \in \{b_1, \ldots, b_\ell\}$. The argument is similar to the previous one and is left as an exercise. □

**Theorem 3.24.** *Every element of $S_n$ can be written as a product of disjoint cycles.*

First observe that in this product we do not need to write the cycles of length one because they are all equal to the identity (and $\mathrm{Id}\,\sigma = \sigma\,\mathrm{Id} = \sigma$, so it is not necessary to indicate it in a product).

**Idea of the proof:** Before we start with the proof, let us consider an example. Let

$$\sigma = (a_1\ a_2\ a_3\ a_4)(b_1\ b_2\ b_3),$$

be a product of two disjoint cycles.

If we only have $\sigma$ in the usual form of a table with two rows, how can we find the two cycles $(a_1\ a_2\ a_3\ a_4)$ and $(b_1\ b_2\ b_3)$?

Assume for a few seconds that we have the element $a_1$. Then, using the fact that

$$\sigma = (a_1\ a_2\ a_3\ a_4)(b_1\ b_2\ b_3),$$

we get $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\sigma(a_3) = a_4$, and finally $\sigma(a_4) = a_1$. So: Starting with $a_1$ we found all the other elements of the first cycle by successively applying $\sigma$ (and we stop when we are back at $a_1$).

What if we do not have $a_1$ to start with? If we have, for instance, $a_3$, we do the same:

$$a_4 = \sigma(a_3),\ a_1 = \sigma(a_4),\ a_2 = \sigma(a_1),\ a_3 = \sigma(a_2),\ a_4 = \sigma(a_3).$$

But what if we don't have one of the $a_i$? If we have one of the $b_i$, it will work in the same way. And if we start with an element $x$ that is not an $a_i$ or $b_i$, we get $\sigma(x) = x$, so our cycle construction stops at once and we get the cycle $(x)$ which is the identity map.

The proof of the Theorem is a formalization of this idea: We start with an element and keep applying $\sigma$ to it: It will give us the first cycle. Then take a new element an keep applying $\sigma$ to it, it will give us the second cycle, etc.

*Proof of Theorem 3.24.* Let $\sigma \in S_n$. We first define $X_1 = \{1, \sigma(1), \sigma^2(1), \ldots\}$. The set $X_1$ is finite, since it is included in $\{1, \ldots, n\}$.

Fact 1: $X_1 = \{1, \sigma(1), \sigma^2(1), \ldots, \sigma^k(1)\}$ for some $k \in \mathbb{N}$, with $\sigma^{k+1}(1) = 1$. Proof of Fact 1: Since $X_1$ in included in $\{1, \ldots, n\}$ which is finite, the sequence $1, \sigma(1), \sigma^2(1), \ldots$ must repeat itself at some point. Let $k$ be the smallest integer such that $\sigma^{k+1}(1) \in \{1, \sigma(1), \ldots, \sigma^k(1)\}$. Then $X_1 = \{1, \sigma(1), \ldots, \sigma^k(1)\}$ and we only have to check that $\sigma^{k+1}(1) = 1$. Assume that $\sigma^{k+1}(1) = \sigma^i(1)$ for some $i \in \{1, \ldots, k\}$. Then, applying $\sigma^{-i}$ to both sides of the equality, we get $\sigma^{k-i+1}(1) = 1$. Since $k - i + 1 < k + 1$, we find that $k - i$ has the same property as $k$ but is smaller, which is impossible by choice of $k$. End of the proof of Fact 1.

If $X_1 = \{1, \ldots, n\}$ we stop here, otherwise let $i$ be the first element of $\{1, \ldots, n\}$ not in $X_1$, and define $X_2 = \{i, \sigma(i), \sigma^2(i), \ldots\}$. As above $X_2 = \{i, \sigma(i), \sigma^2(i), \ldots, \sigma^\ell(i)\}$ where $\sigma^{\ell+1}(i) = i$.

Observe that $X_1$ and $X_2$ are disjoint: If it were not the case, we would have $\sigma^s(1) = \sigma^t(i)$ for some integers $s, t$. Assume for instance that $t \leq s$ (the case $t > s$ is similar). Then, applying $\sigma^{-t}$ to both sides, we get $\sigma^{s-t}(1) = i$, which is impossible since $i \notin X_1$ by choice.

If $X_1 \cup X_2 = \{1, \ldots, n\}$, we stop here, otherwise let $j$ be the first element of $\{1, \ldots, n\}$ not in $X_1 \cup X_2$, and we define $X_3$ in the same way as $X_1$ and $X_2$.

Continuing in this way, we obtain disjoint sets $X_1, \ldots, X_r$ such that $\{1, \ldots, n\} = X_1 \cup X_2 \cup \cdots \cup X_r$, and if we define $\sigma_i$ to be the cycle

$$\sigma_i(x) = \begin{cases} \sigma(x) & \text{if } x \in X_i \\ x & \text{otherwise} \end{cases}$$

then $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$, and these cycles are disjoint since the sets $X_i$ are disjoint. □

**Example 3.25.** *As observed before it, the proof of the previous theorem is actually an algorithm to write $\sigma$ as a product of disjoint cycles. We apply it to*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 4 & 5 \end{pmatrix}.$$

*Take an element of $\{1, \ldots, n\}$, for instance 1, and keep applying $\sigma$. It will give us the first cycle:* $(1\ 3)$. *Then take another element, for instance 2, and keep applying $\sigma$. It gives us the second cycle:* $(2)$. *Then take another element, for instance 4, and keep applying $\sigma$. It gives us the third cycle:* $(4\ 6\ 5)$. *There is no element left, so we stop:*

$$\sigma = (1\ 3)(2)(4\ 6\ 5).$$

*Finally, we can observe that a cycle of length one is equal to the identity, so we do not need to write it, and we obtain:*

$$\sigma = (1\ 3)(4\ 6\ 5).$$

*(In the terminology of the proof: $X_1 = \{1, 3\}$, $X_2 = \{2\}$, $X_3 = \{4, 6, 5\}$, and*

$$\sigma_1 = (1\ 3),\ \sigma_2 = (2),\ \sigma_3 = (4\ 6\ 5).$$

*You can notice that the cycles $\sigma_i$ are simply given by the sets $X_i$ (if we list their elements as they are obtained in the proof by successive applications of $\sigma$).)*

As exercise, you should consider some of the permutations we already saw and write them as products of disjoint cycles.

**Exercise 3.26.** *Write as a product of disjoint cycles the following permutations (the answer is indicated for the first two, so that you can check what you do):*

1. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (1\ 3\ 2)(4) = (1\ 3\ 2).$
2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 5 & 4 & 2 \end{pmatrix} = (1\ 3)(2\ 6)(4\ 5).$
3. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$

4. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$.

Writing a permutation as a product of disjoint cycles provides an easy way to compute its order:

**Proposition 3.27.** *Let $\sigma = \sigma_1 \cdots \sigma_k$ where $\sigma_1, \ldots, \sigma_k$ are disjoint cycles. Then*

$$|\sigma| = \operatorname{lcm}(|\sigma_1|, \ldots, |\sigma_k|).$$

*Recall that* $\operatorname{lcm}(n_1, \ldots, n_k)$ *denotes the least common multiple of* $n_1, \ldots, n_k$.

The proof is in the exercise sheets.

## 3.2 Transpositions

**Definition 3.28.** *A transposition is a cycle of length* 2*, i.e. is a permutation of the form* $(a\ b)$ *with* $a \neq b$*, which sends* $a$ *to* $b$*,* $b$ *to* $a$*, and does not move the other elements.*

Observe that

1. A transposition is never the identity map.
2. $(a\ b)^{-1} = (a\ b)$. The reason is that $(a\ b)(a\ b) = \mathrm{Id}$.
3. $$(a_1\ a_2 \cdots a_k) = (a_1\ a_k)(a_1 a_{k-1}) \cdots (a_1\ a_3)(a_1\ a_2),$$
   so that every cycle can be written as a product of transpositions. Combining this with Theorem 3.24 we obtain

**Theorem 3.29.** *Every permutation can be written as a product of transpositions.*

**Example 3.30.** *A simple computation shows that*

$$(1\ 6)(2\ 5\ 3) = (1\ 6)(2\ 3)(2\ 5) = (1\ 6)(4\ 5)(2\ 3)(4\ 5)(2\ 5).$$

*From this we conclude that there can be several different ways to write a permutation as a product of transpositions.*

*But we will see below that the parity of the number of transpositions used to express a given permutation is fixed: No permutation can be written as a product of an odd number of transpositions and also of an even number of transpositions. This fact has important consequences (but we will not see them, sorry).*

**Lemma 3.31.** *If the identity permutation can be written as a product of* $r$ *transpositions, then* $r$ *is even.*

(The proof of this lemma is possibly the trickiest of this section, feel free to skip it on first reading.)

*Proof.* We proceed by induction on $r$. A transposition cannot be the identity, so $r > 1$. If $r = 2$, we are done. Suppose that $r > 2$, and that

$$\mathrm{Id} = \tau_1 \tau_2 \cdots \tau_r.$$

We consider the product $\tau_{r-1}\tau_r$. It has to be one of the following cases, for some $a, b, c, d$ all different (we also indicate how they can be re-written):

$$\begin{aligned}
(a\ b)(a\ b) &= \mathrm{Id},\\
(b\ c)(a\ b) &= (a\ c)(b\ c),\\
(c\ d)(a\ b) &= (a\ b)(c\ d),\\
(a\ c)(a\ b) &= (a\ b)(b\ c).
\end{aligned}$$

In the first case, we have $\mathrm{Id} = \tau_1 \tau_2 \cdots \tau_{r-2}$. By induction $r - 2$ is even, so $r$ is even.

In all the other cases, we rewrite the product $\tau_{r-1}\tau_r$ as indicated. The main point is that now the element $a$ appears in $\tau_{r-1}$ and not in $\tau_r$. We repeat this process with the product $\tau_{r-2}\tau_{r-1}$ and we obtain either that it is equal to Id, in which case we conclude by induction, or we rewrite $\tau_{r-2}\tau_{r-1}$ as above in such a way that $a$ only appears in $\tau_{r-2}$.

If we keep doing that, either we will at some point that Id is a product of $r - 2$ transposition (if we obtain a product of two successive transpositions that is the identity) and conclude by induction, or we will have rewritten this product so that $a$ only appears in $\tau_1$, so $\tau_1$ is of the form $(a\ b)$ for some $b \neq a$. But in this case $(\tau_1 \cdots \tau_r)(a) = b$, so $\tau_1 \cdots \tau_r \neq \mathrm{Id}$, contradiction (so this case cannot actually occur). □

**Theorem 3.32.** *Let $\sigma \in S_n$ and assume that*

$$\sigma = \gamma_1 \cdots \gamma_r,$$

$$\sigma = \tau_1 \cdots \tau_s,$$

*where $\gamma_1, \ldots, \gamma_r, \tau_1, \ldots, \tau_s$ are transpositions. Then $r$ and $s$ have the same parity.*

*Proof.* We have $\gamma_1 \cdots \gamma_r = \tau_1 \cdots \tau_s$. Therefore

$$(\tau_1 \cdots \tau_s)^{-1} \gamma_1 \cdots \gamma_r = \mathrm{Id},$$

$$\tau_s^{-1} \cdots \tau_1^{-1} \gamma_1 \cdots \gamma_r = \mathrm{Id},$$

i.e., using that $\tau_i^{-1} = \tau_i$:

$$\tau_s \cdots \tau_1 \gamma_1 \cdots \gamma_r = \mathrm{Id},$$

so $r + s$ is even by lemma 3.31. It follows that $r$ and $s$ are both even or both odd. □

**Definition 3.33.** *Let $\sigma$ be a permutation in $S_n$. We say that $\sigma$ is odd if it can be written as a product of an odd number of transpositions, and that $\sigma$ is even if it can be written as a product of an even number of transpositions. This is referred to as the parity of the permutation $\sigma$.*

Observe that, by Theorem 3.32, this notion is well-defined: $\sigma$ is either even or odd (and cannot be both).

# Chapter 4

# Equivalence relations

**Definition 4.1.** *Let $S$ be a set. A* **binary relation** *$R$ on $S$ is a property involving two elements of $S$. For $x, y \in S$ we write $xRy$ if the property is true for $x$ and $y$, and $x \not R y$ if not.*

**Example 4.2.** *Some examples of binary relations are:*

1. *$=$ (the equality between elements). It is defined between elements of any set.*
2. *$\leq$. It is defined for instance between elements of $\mathbb{R}$.*
3. *$|$ (the divisibility relation: $x|y$ means "$x$ divides $y$"), defined between elements of $\mathbb{Z}$.*
4. *It can also be something arbitrary, for instance we can define, for $x, y \in \mathbb{N}$: $xRy$ if and only if $x - y = \sqrt{x}$.*

Some binary relations have nice properties and are often useful in mathematics:

**Definition 4.3.** *Let $S$ be a set. A binary relation $\sim$ on $S$ is called an equivalence relation if it possesses the following properties, for every $x, y, z \in S$:*

1. *$x \sim x$ (we say that $\sim$ is reflexive);*
2. *$x \sim y$ implies $y \sim x$ (we say that $\sim$ is symmetric);*
3. *$x \sim y$ and $y \sim z$ imply $x \sim z$ (we say that $\sim$ is transitive).*

Of the relations in Example 4.2, only the equality is an equivalence relation. The relation $\leq$ is not symmetric: $2 \leq 3$ but $3 \not\leq 2$. The division relation is also not symmetric: $2|6$ but $6 \not| 2$, and the fourth relation in the example is not even reflexive: $2 \not R 2$.

**Example 4.4.** *Here are some other examples.*

1. *If $S$ is the set of all pens, the relations "pen 1 has the same colour as pen 2" is an equivalence relation.*

2. *Let $S$ the the set of $2 \times 2$ matrices. The relation defined on $S$ by $A \sim B$ if there is an invertible matrix $P$ such that $P^{-1}AP = B$, is an equivalence relation (exercise; and it is a useful relation in linear algebra).*

3. *Let $S$ be the set of all real differentiable functions. The relation defined by $f \sim g$ if $f' = g'$ is an equivalence relation (exercise).*

Equivalence relations are very useful in practice to regroup elements that share some common property. This is possible because, given an equivalence relation, we can associate a set to every element:

**Definition 4.5.** *Let $\sim$ be an equivalence relation on a set $S$ and let $a \in S$. The set*

$$[a] = \{y \in S \mid a \sim y\}$$

*of all elements of $S$ that are in relation with $a$, is called the **equivalence class** of $a$.*

**Example 4.6.** *If we go back to Example 4.4(1): Let $a$ be a red pen. The equivalence class of $a$ is the set of all red pens:*

$$\begin{aligned}[a] &= \{b \in S \mid a \text{ is in relation with } b\} \\ &= \{\text{pens } b \mid a \text{ has the same colour as } b\} \\ &= \{\text{all red pens}\}.\end{aligned}$$

**Lemma 4.7.** *Let $\sim$ be an equivalence relation on a set $S$ and let $a, b \in S$ be such that $b \in [a]$. Then $[b] = [a]$.*

*Proof.* The hypothesis $b \in [a]$ means (by definition) $a \sim b$, and so we have $b \sim a$ by symmetry.

The statement $[b] = [a]$ is an equality between sets, so to prove it we need to show that the sets $[b]$ and $[a]$ contain exactly the same elements:

Let $x \in [b]$, i.e. $b \sim x$. Then we have $a \sim b$ and $b \sim x$. Using transitivity we obtain $a \sim x$, i.e. $x \in [a]$.
Let $x \in [a]$, i.e. $a \sim x$. But we know that $a \sim b$, i.e. $b \sim a$. So we have $b \sim a$ and $a \sim x$. Using transitvity we obtain $b \sim x$, i.e. $x \in [b]$. □

**Corollary 4.8.** *Let $\sim$ be an equivalence relation on a set $S$ and let $a, b \in S$. Then $a \sim b$ if and only if $[a] = [b]$.*

*Proof.* Assume first that $a \sim b$. Then $b \in [a]$ and the conclusion follows by Lemma 4.7.

Assume now that $[a] = [b]$. Since $b \in [b]$ (because $b \sim b$), we have $b \in [a]$, i.e. $a \sim b$. □

**Proposition 4.9.** *Let $\sim$ be an equivalence relation on a set $S$ and let $a, b \in S$. Then either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.*

*In other words: two equivalence classes are either equal or have no common element.*

*Proof.* We want to show that $[a] = [b]$ and $[a] \cap [b] = \emptyset$ are the only two possibilities. So we assume that one of them does not hold for our choice of $a$ and $b$, and check, using this knowledge, that the other then necessarilly holds.

So we assume (for instance) that $[a] \cap [b] \neq \emptyset$, so there is $c \in [a] \cap [b]$. By Lemma 4.7 we deduce $[c] = [a]$ and $[c] = [b]$, so $[a] = [b]$. □

**Example 4.10.** *This is an example of a more "graphical" equivalence relation. We define it between points of the plane* $\mathbb{R}^2$.

*For* $\theta \in \mathbb{R}$ *we denote by* $r_\theta$ *the rotation of centre* $O = (0,0)$ *and angle* $\theta$.

*For* $x, y \in \mathbb{R}^2$, *we define*

$$x \sim y$$

$$\Leftrightarrow$$

*there is* $\theta \in \mathbb{R}$ *such that* $y = r_\theta(x)$

*(i.e.,* $y$ *can be obtained from* $x$ *by a rotation of centre* $O$*).*

*This relation is an equivalence relation:*

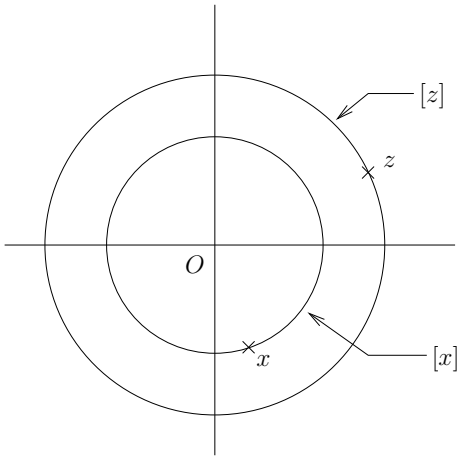
*(1)* $x \sim x$*: Becauce* $x = r_0(x)$.

*(2)* $x \sim y \Rightarrow y \sim x$*: Because, if* $y = r_\theta(x)$, *then* $x = r_{-\theta}(y)$ *(so* $y \sim x$*).*

*(3)* $(x \sim y$ *and* $y \sim z) \Rightarrow\ x \sim z$*: Because* $x \sim y$ *and* $y \sim z$ *mean* $y = r_\theta(x)$ *and* $z = r_\alpha(y)$ *for some angles* $\theta$ *and* $\alpha$. *Then* $z = r_\alpha(r_\theta(x)) = r_{\alpha+\theta}(x)$, *so* $x \sim z$.

*What is the equivalence class of* $x$*?*

$$[x] = \{y \in \mathbb{R}^2 \mid y \text{ can be obtained from } x \text{ by a rotation of centre } O\}$$
$$= \text{the circle of centre } O \text{ containing } x.$$




*Observe that we can see that the result of Proposition 4.9 is correct: The equivalence classes are the circles of centre* $O$, *and clearly two such circles are either equal or have no common element.*

# Chapter 5

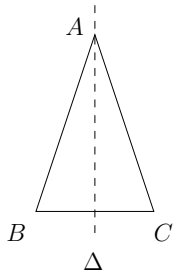
# Groups, part 2

We saw in the previous chapter that $S_n$ is a group. We first see some more examples of groups.

## 5.1 Symmetry groups

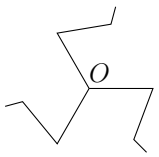
Imagine an objcet $T$ in space. A symmetry of $T$ is a movement of $T$ such that at the end of it the object $T$ occupies the exact same place in space. This is a somewhat informal definition (what is a movement?) but it will be enough for us.[1]

**Examples 5.1.** *1. If $T$ is a triangle $ABC$ where $|AB| = |AC|$ and is longer that $|BC|$:*




*Then the only symmetries of $T$ are the identity ($T$ does not move) and the reflexion across the line $\Delta$ ($T$ is "flipped").*

*2. Let $T$ be a kind of triskelion (see the coat of arms of the isle on Man or of Sicily), and let $O$ be the "middle" of $T$:*




[1] If you really want to know: A movement should be defined as a bijection $f : \mathbb{R}^3 \to \mathbb{R}^3$ that does not modify the distances, i.e. for every points $A, B$, the distance between $f(A)$ and $f(B)$ is the same as the distance between $A$ and $B$.

*Then the only symmetries of $T$ are the identity and the rotations of centre $O$ and angles $120°$, $240°$.*

**Lemma 5.2.** *The symmetries of $T$, with operation the composition of maps, is a group. Its identity element is the identity map.*

*Proof.* If we composote two symmetries of $T$, we still get a symmetry of $T$ ($T$ still ends up at the same place). The composition of isometries is associative since it is simply a composition of maps (which is always associative). The identity map is the identity element. The inverse of a symmetry is simply the "reverse movement" (in terms of maps: the inverse map). □

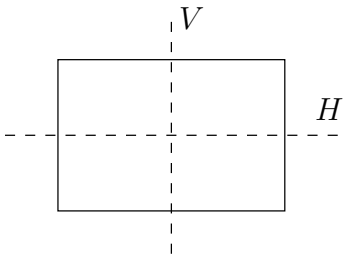
In the examples above the symmetry groups were all finite. It is not necessarilly the case. For instance a circle with centre $O$ has an infinite number of symmetries (all the rotations of centre $O$ are symmetries; there are others).

Symmetry groups are a convenient way to investigate the symmetries of objects or of repeating patterns, and have found applications in crystallography (description of crystal patterns), chemistry (symmetries of molecules, etc), computer graphics (repeating patterns to fill some space), arts (Escher drawings)...

## 5.2 The Klein 4-group

The **Klein 4-group** $V_4$ is the symmetry group of a rectangle that is not a square. The symmetries of a rectangle are:

- The identity map Id (the identity element of the group),
- $h$, the reflection across the horizontal axis $H$,
- $v$, the reflection across the vertical axis $V$, and
- $r$, the rotation of $\pi$ radians around the center.



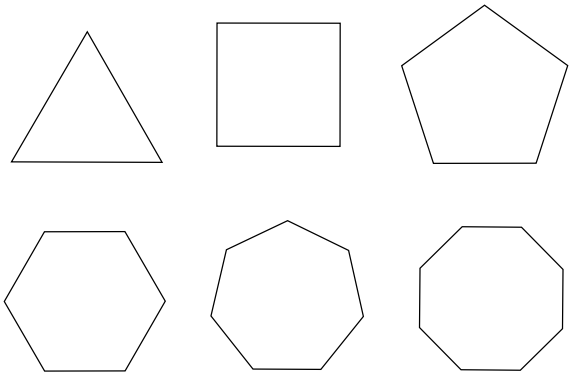

Obviously (consider how the rectangle moves; use a rectangle of paper if you want) we have:

$$h^2 = v^2 = \mathrm{Id}, hv = vh = r.$$

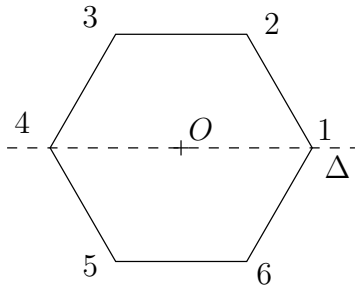
## 5.3 The dihedral group of order $2n$

**Definition 5.3.** *Let $n \geq 3$. The **dihedral group of order** $2n$ is the symmetry group of a regular $n$-sided polygon. This group is denoted by $D_{2n}$.*

Here are the first 6 regular $n$-sided polygons:



Let us fix a regular $n$-sided polygon, let $O$ be the centre of this polygon and let $\Delta$ be a fixed line going through a vertex of the polygon and the point $O$ (it is a line of mirror symmetry of the polygon). For convenience, we also number the vertices of the polygon from 1 to $n$. For $n = 6$ it would look like:




We denote by $s$ the mirror symmetry across $\Delta$ and by $r$ the rotation of centre $O$ and angle $2\pi/n$. Both are clearly elements of $D_{2n}$.

There are exactly $2n$ elements in $D_{2n}$ (see exercise sheets), and they can all be expressed as follows

$$\mathrm{Id}, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}. \tag{5.1}$$

Observe that the following properties also hold:

$$r^n = \mathrm{Id},$$

$$s^2 = \mathrm{Id},$$

$$sr = r^{n-1}s.$$

(For this last one you can cut a polygon in a piece of paper and try it "for real".)

**Exercise 5.4.** *When $n = 6$, take a few isometries of the regular hexagon (for instance: The reflection across the line (3 6), the rotation of angle $240°$, the rotation of angle $120°$ followed by the reflection across the line $\Delta$) and express then in the form (5.1).*

**Remark 5.5.** *Some people write $D_n$ when we write $D_{2n}$ (they indicate the number of sides of the polygon, while we indicate the number of elements of the group), so be careful, if you look at something in a book or online, to check what terminology is used.*

## 5.4 Cayley tables

**Definition 5.6.** *The* **Cayley table** *of a group is simply the table of the group operation (see examples below). There is no particular order in which you should list the elements of the group in the starting row and column.*

**Examples 5.7.** *1. Consider the Klein 4-group $V_4$. We completely described it, and its Cayley table is*

| $\cdot$ | Id | $h$ | $v$ | $r$ |
|---|---|---|---|---|
| Id | Id | $h$ | $v$ | $r$ |
| $h$ | $h$ | Id | $r$ | $v$ |
| $v$ | $v$ | $r$ | Id | $h$ |
| $r$ | $r$ | $v$ | $h$ | Id |

*2. Consider the group $S_3$. Its elements are:*

$$\mathrm{Id}, \tau_1 = (2\ 3), \tau_2 = (1\ 3), \tau_3 = (1\ 2),$$
$$\omega_1 = (1\ 2\ 3), \omega_2 = (1\ 3\ 2).$$

*We know there are no other elements because $|S_3| = 6$ and the above elements are all different.*

*The Cayley table of $S_3$ is (check a few of them to be sure you get the idea).*

| $\cdot$ | Id | $\omega_1$ | $\omega_2$ | $\tau_1$ | $\tau_2$ | $\tau_3$ |
|---|---|---|---|---|---|---|
| Id | Id | $\omega_1$ | $\omega_2$ | $\tau_1$ | $\tau_2$ | $\tau_3$ |
| $\omega_1$ | $\omega_1$ | $\omega_2$ | Id | $\tau_3$ | $\tau_1$ | $\tau_2$ |
| $\omega_2$ | $\omega_2$ | Id | $\omega_1$ | $\tau_2$ | $\tau_3$ | $\tau_1$ |
| $\tau_1$ | $\tau_1$ | $\tau_2$ | $\tau_3$ | Id | $\omega_1$ | $\omega_2$ |
| $\tau_2$ | $\tau_2$ | $\tau_3$ | $\tau_1$ | $\omega_2$ | Id | $\omega_1$ |
| $\tau_3$ | $\tau_3$ | $\tau_1$ | $\tau_2$ | $\omega_1$ | $\omega_2$ | Id |

## 5.5 Subgroups

It is possible for a group to be inside another group (for instance $\mathbb{Z} \subseteq \mathbb{R}$, both with the operation $+$). This is the object of the next definition.

**Definition 5.8.** *Let $G$ be a group. If $H$ is a non-empty subset of $G$ such that $H$, equipped with the operation from $G$, it itself a group, then $H$ is called a subgroup of $G$.*

So to check if a subset $H$ of $G$ is a subgroup, you have several things to check

1. That $h_1 h_2 \in H$ for every $h_1, h_2 \in H$. Why? Because in a group, the product of two elements is always an element of the group.

2. That all the properties of group hold for $(H, \star)$ (if we call $\star$ the operation of $G$).

**Lemma 5.9.** *If $H$ is a subgroup of $G$, the identity of the group $H$ is the same as the identity of $G$, and if $a \in H$, then the inverse of $a$ computed in the group $H$ is the same as the inverse of $a$ computed in the group $G$.*

*Proof.* Let $e_H$ be the identity of $H$. We have $ae_H = a$ for every element of $H$ and therefore

$$e_H e_H = e_H.$$

Now multiplying both sides of this equality on the left by $e_H^{-1}$ (in $G$) gives us $e_H = e$.

Let $a \in H$ and let us denote by $\tilde{a}$ the inverse of $a$ computed in the group $H$. We have $a\tilde{a} = e$ (since $e_H = e$) and $aa^{-1} = e$. Therefore $a\tilde{a} = aa^{-1}$ and multiplying both sides on the left by $a^{-1}$ gives $\tilde{a} = a^{-1}$. □

**Easier way to check when we have a subgroup**

Suppose we have a subset $H$ of a group $G$, and want to check if it is a subgroup. Since $G$ is already a group, we do not need to check if $H$ satisfies all the properties in the definition of group, some of them will be automatically true, and we only have to check much less:

**Proposition 5.10.** *Let $G$ be a group and let $H$ be a subset of $G$. The following are equivalent:*

1. *$H$ is a subgroup of $G$.*
2. *The following three properties hold:*
   (a) *$H \neq \emptyset$,*
   (b) *For every $a, b \in H$, $ab \in H$,*
   (c) *For every $a \in H$, $a^{-1} \in H$.*

*Proof.* If $H$ is a subgroup of $G$, it is in particular a group, so it is non-empty since it contains an identity element. We also know that the product of two elements and the inverse of one element of a group are still in the group.

Assume now that all three properties hold. We want to check that $H$ is a group. The first thing to check is that the product of elements of $H$ gives an element of $H$. This is true by the second property. The first point in the definition of group (associativity of the product) is true because $G$ is a group and we know that the product is associative. The second point in the definition of group is the existence of an identity element in the group: We know that $H$ is non-empty, so let us take $a \in H$. Then $a^{-1} \in H$ and so $e = aa^{-1} \in H$. Finally we know that if $a \in H$ then the inverse of $a$ is in $H$, which provides the last property in the definition of group. □

**Example 5.11.** *1. Let $n \in \mathbb{Z}$. Then $n\mathbb{Z}(= \{nx \mid x \in \mathbb{Z}\})$, the set of all multiples of $n$, is a subgroup of the group $(\mathbb{Z}, +)$ (actually every subgroup of $(\mathbb{Z}, +)$ is of the form $n\mathbb{Z}$ for some well-chosen $n$, we will see this in an exercise sheet). We simply check the 3 conditions of proposition 5.10:*

(a) *Clearly $n\mathbb{Z}$ is non-empty.*

(b) *If $a, b \in n\mathbb{Z}$ (i.e., $a, b$ are multiples of $n$), then $a+b$ is also a multiple of $n$ i.e., $a + b \in n\mathbb{Z}$ (observe that the group operation is $+$, so it is what we use between $a$ and $b$).*

(c) *If $a \in n\mathbb{Z}$ then $-a \in n\mathbb{Z}$. (Here: The identity element of $(\mathbb{Z}, +)$ is $0$, and thus the inverse of $a$ is $-a$, because $a + (-a) = 0$).*

2. *$\mathbb{Q}\setminus\{0\}$ is a subgroup of the group $(\mathbb{R}\setminus\{0\}, \cdot)$. It is left an exercise. Again, use proposition 5.10.*

**Definition 5.12.** *Let $G$ be a group. The **centre** of $G$, denoted $Z(G)$, is the set of elements of $G$ that commute with all elements of $G$:*

$$Z(G) = \{a \in G \mid ax = xa \text{ for every } x \in G\}.$$

**Proposition 5.13.** *$Z(G)$ is a subgroup of $G$.*

*Proof.* Exercise. □

**Definition 5.14.** *Let $G$ be a group and let $A$ be a non-empty subset of $G$. We denote by $\langle A\rangle$ the set of all possible products of elements of $A$ and of their inverses. By Proposition 5.10, $\langle A\rangle$ is a subgroup of $G$ (more on this in a few lines), called the subgroup **generated by** $A$.*

*We say that $G$ is **generated** by $A$ if $G = \langle A\rangle$ (we also say that $A$ is a set of generators of $G$).*

If $A = \{a_1, \ldots, a_k\}$ we often simply write $\langle a_1, \ldots, a_n\rangle$ instead of $\langle\{a_1, \ldots, a_n\}\rangle$.

**Remark 5.15.** *Why is $\langle A\rangle$ a subgroup? By definition:*

$$\langle A\rangle = \{x_1 x_2 \cdots x_n \mid n \in \mathbb{N},\ x_i = a_i \text{ or } x_i = a_i^{-1} \text{ with } a_i \in A\}.$$

*(Again: $\langle A\rangle$ is the set of all possible products of elements of $A$ and their inverses.)*

*We now use proposition 5.10:*

1. *Clearly $\langle A\rangle$ is non-empty (since $A$ is non-empty).*
2. *If $a, b \in \langle A\rangle$, then $ab \in \langle A\rangle$ (it is just a longer product of elements of $A$ and their inverses).*
3. *If $a \in \langle A\rangle$ then $a^{-1} \in \langle A\rangle$ (the inverse of a product of elements of $A$ and their inverses is still of this form).*

**Definition 5.16.** *A group generated by only one element is called a **cyclic group**.*

**Remark 5.17.** *In other words, $G$ is a cyclic group if there is $a \in G$ such that*

$$G = \langle a\rangle = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, a^3, \ldots\}.$$

*Observe that $G$ can be finite:*
*If $o(a) = n < \infty$, then $a^n = e$. Therefore:*

$$a^{n+1} = a,\ a^{n+2} = a^2, \ldots$$

$$a^{-1} = a^{n-1},\ a^{-2} = a^{n-2}, \ldots$$

*so that*

$$\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}.$$

The last line of this remark gives us the following result:

**Proposition 5.18.** *Let $G$ be a group and let $a \in G$ be such that $o(a)$ is finite. Then*

$$o(a) = |\langle a \rangle|.$$

*(The order of $a$ is equal to the number of elements in the subgroup generated by $a$.)*

**Examples 5.19.**

1. *The Klein 4-group is generated by $h$ and $v$. But also by $h$ and $r$, or by $v$ and $r$. (In particular you can see that a group can have different sets of generators.)*
2. *The dihedral group $D_{2n}$ is generated by $r$ and $s$.*
3. *The symmetric group $S_n$ is generated by the transpositions (see Proposition 3.29). It is also generated by the cycles.*

# Chapter 6

# Cosets and Lagrange's theorem

We begin by revisiting what we saw when looking at $\mathbb{Z}/n\mathbb{Z}$.

Recall that two numbers that differ by a multiple of $n$ are equal in $\mathbb{Z}/n\mathbb{Z}$, so we use this as the definition of a relation:

$$x \sim y \Leftrightarrow x - y \in n\mathbb{Z}. \tag{6.1}$$

It is easy to check that this relation is an equivalence relation. And for $x \in \mathbb{Z}$, the equivalence class of $x$ is: relation is:

$$\begin{aligned}
[x] &= \{y \in \mathbb{Z} \mid x \sim y\} \\
&= \{y \in \mathbb{Z} \mid x - y \in n\mathbb{Z}\} \\
&= \{x + k \mid k \in n\mathbb{Z}\} \\
&= x + n\mathbb{Z} \\
&(= \{\ldots, x - 2n, x - n, x, x + n, x + 2n, x + 3n, \ldots\}).
\end{aligned}$$

So the equivalence class of $x$ is the set of all integers that are equal to $x$ on the $n$-hours clock.

We want to extend this equivalence relation to arbitrary groups, so we replace $\mathbb{Z}$ by an arbitrary group $G$, and the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ by a subgroup $H$ of $G$. It will turn out to be quite useful:

**Definition 6.1.** *Let $G$ be a group and let $H$ be a subgroup of $G$. We define an equivalence relation $\sim_H$ between elements of $G$ by*

$$x \sim_H y \Leftrightarrow y^{-1}x \in H.$$

*We write $x = y \bmod H$ if $x \sim_H y$ and say that $x$ is equal to $y$ modulo $H$.*

Observe that the definition of $\sim_H$ follows exactly the pattern of (6.1), we are just using $H$ instead of $n\mathbb{Z}$ and a multiplicative notation for the group operation: For a Abelian group $(G, +)$ where the operation is denoted by the symbol $+$ (so for instance $(\mathbb{Z}, +)$) we would write

$$x \sim_H y \Leftrightarrow -y + x \in H \Leftrightarrow x - y \in H.$$

**Lemma 6.2.** *The relation $\sim_H$ is an equivalence relation.*

*Proof.* We check the three properties of equivalence relations:
We have $x \sim_H x$ because $x^{-1}x = e \in H$.
Assume $x \sim_H y$, i.e. $y^{-1}x \in H$. Since $H$ is a subgroup, we have $(y^{-1}x)^{-1} \in H$, i.e. $x^{-1}y \in H$, in other words $y \sim_H x$.
Finally assume $x \sim_H y$ and $y \sim_H z$, i.e. $y^{-1}x \in H$ and $z^{-1}y \in H$. Since $H$ is a subgroup we have $(z^{-1}y)(y^{-1}x) \in H$, i.e. $z^{-1}x \in H$, which gives $x \sim_H z$. □

**Proposition 6.3.** *The equivalence class of $a \in G$ for the relation $\sim_H$, denoted $\bar{a}$ in this case, is:*

$$\overline{a} = aH,$$

*where $aH$ is defined as follows*

$$aH := \{ax \mid x \in H\}.$$

*Proof.* We want to show an equality between two sets. One way to do this is to show that they contain exactly the same elements, i.e. that each set is contained in the other.

We start with $b \in \overline{a}$ and show that $b \in aH$. By definition of $\overline{a}$ we have $a \sim b$ i.e, $b^{-1}a \in H$, so there is $x \in H$ such that $b^{-1}a = x$. We solve for $b$: Multiplying both sides on the left by $b$ give $a = bx$, and on the right by $x^{-1}$ gives $b = ax^{-1}$, which belongs to $aH$ since $x^{-1} \in H$.

Take now $b \in aH$, i.e. $b = ax$ for some $x \in H$. Then $b^{-1}a = x^{-1}a^{-1}a = x^{-1} \in H$, so $a \sim_H b$, i.e. $b \in \overline{a}$. □

**Definition 6.4.** *Let $H$ be a subgroup of $G$. A set of the form $aH$, for somce $a \in G$, is called a* **left coset** *of $H$. A* **right coset** *of $H$ is a set of the form $Ha$.*

**Remark 6.5.**
1. *In general we do not have $aH = Ha$. See exercise sheets for an easy counter-example.*
2. *We could define another equivalence relation on $G$ by $x \sim'_H y$ if and only if $xy^{-1} \in H$. The equivalence class of an element $a$ would then be $Ha = \{xa \mid x \in H\}$. This whole chapter can actually be written using this equivalence relation and right cosets instead of left cosets.*

The next result is the key to Lagrange's theorem, and we have already proved most of it.

**Proposition 6.6.**
1. *Assume $H$ is finite and let $a \in G$. Then $|aH| = |H|$ $(= |Ha|)$.*
2. *Every element of $G$ belongs to a left coset of $H$.*
3. *Any two left cosets of $H$ are equal or have no element in common.*

*Proof.* 1. To show that $H$ and $aH$ have the same number of elements we define a bijection between them:

$$f : H \to aH,\ x \mapsto ax.$$

$f$ is injective: Assume that $ax = ay$. Then, multiplying on the left by $a^{-1}$ we obtain $x = y$.
$f$ is surjective: Every element of $aH$ is in the image of $f$ by definition of $f$.

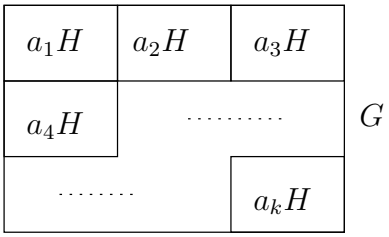
2. We know that $x \sim_H x$ since $\sim_H$ is an equivalence relation, which means $x \in \overline{x} = xH$.

3. This is a consequence of Proposition 4.9 since the left cosets of $H$ are equivalence classes.

□

**Theorem 6.7** (Lagrange's Theorem)**.** *Let $G$ be a finite group and let $H$ be a subgroup of $G$. Then $|H|$ divides $|G|$.*

*Proof.* By Proposition 6.6, the group $G$ is "paved" by the left cosets of $H$: Every element belongs to one, and they do not overlap. In particular there are only finitely many different left cosets of $H$: $a_1H$, ..., $a_kH$, and a picture would look like this:




Counting the elements of $G$, we obtain

$$\begin{aligned} |G| &= |a_1H| + |a_2H| + \cdots + |a_kH| \\ &= |H| + |H| + \cdots + |H| \qquad \text{by Proposition 6.6} \\ &= k|H|. \end{aligned}$$

□

**Remark 6.8.** *1. One of the remarkable aspects of this result is that the definitions of group and subgroup are algebraic conditions that do not appear to require anything about the number of elements. But they actually do.*

*2. Lagrange's theorem was not proved by Lagrange. The notion of group did not even exist at the time. But he was the first (or one of the first) to come up with similar ideas in the domain that would later give rise to the notion of group (the study of solutions of polynomial equations).*

**Definition 6.9.** *Let $G$ be a group and let $H$ be s subgroup of $G$. The **index of $H$ in $G$**, denoted $[G : H]$, is the number of distinct left cosets of $H$ in $G$.*

**Remark 6.10.** *So by Lagrange's theorem (or more precisely its proof):*

$$[G : H] = |G|/|H|.$$

The set of all left cosets of $H$ in $G$ is often denoted by $G/H$ i.e.,:

$$G/H = \{aH \mid a \in G\},$$

so $[G : H] = |G/H| = |G|/|H|$.

**Corollary 6.11.** *Let $G$ be a finite group and let $a \in G$. Then $o(a)$ divides $|G|$.*

*Proof.* We saw in Proposition 5.18 that $o(a)$ is equal to the number of elements in $\langle a \rangle$, the subgroup generated by $a$. The result follows by Lagrange's theorem. □

**Corollary 6.12.** *Let $G$ be a finite group and let $a \in G$. Then $a^{|G|} = e$.*

*Proof.* By the Corollary 6.11 $|G| = k \cdot o(a)$ for some $k \in \mathbb{N}$. Therefore

$$a^{|G|} = a^{ko(a)} = (a^{o(a)})^k = e^k = e.$$ □

**Theorem 6.13.** *Let $G$ be a group such that $|G|$ is a prime number. Then $G$ is a cyclic group.*

*Proof.* Let $p = |G|$. Let $a \in G$ such that $a \neq e$ (it exists since $|G| = p \geq 2$). Consider $\langle a \rangle$, the subgroup generated by $a$. It contains at least 2 dictinct elements: $e$ and $a$, so $|\langle a \rangle| \geq 2$. But $|\langle a \rangle|$ divides $p$, so, since $p$ is prime, we must have $|\langle a \rangle| = p = |G|$, which gives $\langle a \rangle = G$. □

Observe that what we proved is slightly stronger than the conclusion of the theorem: $G$ is generated by any one of its elements that is not $e$.

# Chapter 7

# Isomorphisms

We begin with an example.

We consider the group $(\mathbb{Z}/2\mathbb{Z}, +)$. Its Cayley table is

| $+$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $1$ |
| $1$ | $1$ | $0$ |

We now define a group $(G, \cdot)$ of order 2 by $G = \{a, b\}$ and by giving the table for the operation $\cdot$ (it is easy, but tedious, to check that $(G, \cdot)$ is a group):

| $\cdot$ | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $b$ |
| $b$ | $b$ | $a$ |

It should be clear that the groups $(\mathbb{Z}/2\mathbb{Z}, +)$ and $(G, \cdot)$ are the same, but with $+$ written $\cdot$, $0$ written $a$ and $1$ writen $b$.

We want to give a more precise definition for what it means to be "the same". We want a correspondence between the elements of both groups (i.e. a bijection), and we also want that performing the group operation in one group of the other and comparing the results using this correspondence gives us the same element.

**Definition 7.1.** *Let $(G, \cdot)$ and $(H, \star)$ be two groups. A map $f : G \to H$ is called an isomorphism (of groups) if the following holds*

1. *$f$ is bijective.*
2. *For every $a, b \in G$, $f(a \cdot b) = f(a) \star f(b)$ (i.e. computing the product $a \cdot b$ in $G$ and then moving the result to $H$ is the same as first moving $a$ and $b$ to $H$ and then computing the product in $H$).*

*We say that the groups $(G, \cdot)$ and $(H, \star)$ are isomorphic if there is an isomorphism $f : G \to H$, and we write $G \cong H$.*

We can see that, in the above example, the map

$$f : \mathbb{Z}/2\mathbb{Z} \to G,\ f(0) = a,\ f(1) = b$$

is an isomorphism.

Intuitively, two groups are isomorphic when they are "the same group", the only differences being that the elements and the operation are called differently (but their behaviour is the same, as stated in the second property in the definition of isomorphism).

**Lemma 7.2.** *Let $f : G \to H$ be an isomorphism, with notation as in Definition 7.1. Then*

1. *$f(e_G) = e_H$ (where $e_G$ denotes the identity of $G$ and $e_H$ the identity of $H$).*
2. *For every $a \in G$, $f(a^{-1}) = f(a)^{-1}$.*

*Proof.* 1. We have $f(e_G) = f(e_G \cdot e_G) = f(e_G) \star f(e_G)$. Multiplying on both sides by the inverse of $f(e_G)$ we obtain $e_H = f(e_G)$.

2. To check that $f(a^{-1}) = f(A)^{-1}$ we have to show that $f(a^{-1}) \star f(a) = e_H$ and $f(a) \star f(a^{-1}) = e_H$. We do the first one:
$f(a^{-1}) \star f(a) = f(a^{-1} \cdot a) = f(e_G) = e_H$.

□

**Proposition 7.3.** *Let $f : G \to H$ be an isomorphism, with notation as in Definition 7.1. Then $f^{-1} : H \to G$ is an isomorphim.*

*Proof.* We have to show that $f^{-1}$ is bijective (this is clearly true) and that, for every $x, y \in H$, $f^{-1}(x \star y) = f^{-1}(x) \cdot f^{-1}(y)$. We have

$$\begin{aligned} f^{-1}(x \star y) = f^{-1}(x) \cdot f^{-1}(y) &\Leftrightarrow f(f^{-1}(x \star y)) = f(f^{-1}(x) \cdot f^{-1}(y))) \\ &\qquad \text{(since } f \text{ is bijective)} \\ &\Leftrightarrow x \star y = f(f^{-1}(x) \cdot f^{-1}(y))) \\ &\Leftrightarrow x \star y = f(f^{-1}(x)) \star f(f^{-1}(y))) \\ &\qquad \text{(since } f \text{ is an isomorphism)} \\ &\Leftrightarrow x \star y = x \star y, \end{aligned}$$

which is true. □

# Chapter 8

# Rings and fields

We introduced the notion of group as a convenient way to study common properties of structures that have a well-behaved binary operation.

But there are of course structures with two binary operations, for instance $Z$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $M_n(\mathbb{R})$. In all these example the operations are a sum and a product. And many more such structures appear in mathematics. For the same reasons that groups where introduced, it makes sense to try to single out some key properties of such structures, and see what general results can be deduced.

**Definition 8.1.** *A **ring** is a triple $(R, +, \cdot)$, where $R$ is a non-empty set and $+$ and $\cdot$ are two binary operations on $R$, such that the following properties hold:*

1. *$(R, +)$ is an abelian group. Its identity is denoted $0$, and the additive inverse of an element $a$ is denoted by $-a$;*
2. *The product is associative (i.e. $a(bc) = (ab)c$ for every $a, b, c \in R$);*
3. *There is an element in $R$, denoted by $1$, such that $a \cdot 1 = 1 \cdot a = a$ for every $a \in R$ ($1$ is the identity for $\cdot$).*
4. *The operation $\cdot$ is distributive over $+$, i.e. for every $a, b, c \in R$:*

$$a(b + c) = ab + ac, \text{ and}$$

$$(a + b)c = ac + bc.$$

**Example 8.2.**
1. *$Z$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $M_n(\mathbb{R})$, $M_n(\mathbb{Z})$, $\mathbb{Z}/n\mathbb{Z}$ are all examples of rings, when equipped with their usual sum and product.*
2. *$\mathbb{N}$ is not a ring, since $(\mathbb{N}, +)$ is not a group (there is no identity for $+$). $\mathbb{N} \cup \{0\}$ is also not a ring (there is no additive inverse).*
3. *Observe that the product need not be commutative, it is the case for instance of $M_n(\mathbb{R})$ when $n \geq 2$.*

Some people do not require the existence of the element 1 in the definition of ring.

**Lemma 8.3.** *Let $(R, +, \cdot)$ be a ring. Then $a \cdot 0 = 0 \cdot a = 0$ for every $a \in R$.*

*Proof.* We only show $a \cdot 0 = 0$, the other is similar. We have

$$\begin{aligned} a \cdot 0 &= a \cdot (0 + 0) \\ &= a \cdot 0 + a \cdot 0. \end{aligned}$$

Adding $-(a \cdot 0)$ to both sides, we get $0 = a \cdot 0$. □

Some rings, for instance $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, have the following extra properties:

1. The product is commutative;
2. Every non-zero element has a multiplicative inverse.

These rings are common enough and important enough in mathematics that they deserve a separate definition:

**Definition 8.4.** *A **field** is a triple $(F, +, \cdot)$, where $F$ is a non-empty set and $+$ and $\cdot$ are two binary operations on $F$, such that the following properties hold:*

1. *$(F, +, \cdot)$ is a ring with $0 \neq 1$.*
2. *The operation $\cdot$ is commutative (i.e. $ab = ba$ for every $a, b \in F$).*
3. *For every $a \in F \setminus \{0\}$, there is an element $a^{-1}$ such that $a \cdot a^{-1} = 1$ ($a^{-1}$ is called the inverse of $a$).*

**Remark 8.5.** *The condition $0 \neq 1$ allows us to avoid an uninteresting case: Assume that $0 = 1$ in some ring $R$. Then, for every $a \in R$ we have $a = a \cdot 1 = a \cdot 0 = 0$, so $R = \{0\}$. In other words, asking that $0 \neq 1$ in $R$ is the same as asking $R \neq \{0\}$.*

**Lemma 8.6.** *Let $F$ be a field. Then $(F \setminus \{0\}, \cdot)$ is a group with identity element 1.*

*Proof.* We know that the product is associative and that 1 is an identity for $\cdot$ (since $F$ is a ring). Finally, every element in $F \setminus \{0\}$ has a multiplicative inverse by definition of field. □

**Example 8.7.** *$\mathbb{Z}/nZ$ is a field if and only if $n$ is a prime number.*
*We alredy know that $\mathbb{Z}/n\mathbb{Z}$ is a ring, that the product is commutative, and that $0 \neq 1$ (since $n \geq 2$). The fact that any non-zero element has an inverse is statement 4. in proposition 1.5 (since $n$ is prime).*

We can use what we have seen to get a very short proof of Fermat's little theorem:

**Theorem 8.8** (Fermat's little theorem)**.** *Let $p$ be a prime number and let $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$. Then*

$$a^{p-1} = 1 \bmod p.$$

*Proof.* We know that $\mathbb{Z}/p\mathbb{Z}$ is a field, so $(\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}, \cdot)$ is a group. It has $p - 1$ elements. Moreover $\overline{a} \neq \overline{0}$ since $p$ does not divide $a$, so $\overline{a}$ belongs to this group. By Corollary 6.12, we know that $\overline{a}^{p-1} = \overline{1}$, in other words:

$$a^{p-1} = 1 \bmod p.$$

□

# Index