Basic definitions

Sets and functions

Definition 1

1. *A* **set** *is a well-defined collection of objects called* **elements**. *We write $s \in S$ to mean the element s is in the set S.*
2. *Given any collection of sets $S_1, \dots, S_n$ we can form a* **direct product**

$$S_1 \times \cdots \times S_n = \{(s_1, \dots, s_n) \mid s_i \in S_i \text{ for each} i = 1, \dots, n\},$$

also a set. The elements $(s_1, \dots, s_n)$ are called **n-tuples**.

In part 1. of Definition 1, *well-defined* is meant in the sense that one cannot give the same name to two different elements. There is a more typical use of the term which we will make explicit shortly.

Example 1

The following are examples of sets.

1. $\mathbb{N} = \{1, 2, 3, \dots\}$ = the **natural numbers**. Also denoted $\mathbb{Z}^+$ or $\mathbb{Z}_{>0}$.
2. $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ = the **integers**.
3. $\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z} \text{ and } n \neq 0\}$ = the **rational numbers**.
4. $\mathbb{R}$ = the **real numbers**.
5. $\mathbb{C}$ = the **complex numbers**.
6. $\mathrm{Mat}_R(n, n)$ = the set of $n \times n$ matrices with entries in $R = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, etc.
7. $R^\times := R \setminus \{0\}$ = the **multiplicative group of** R, where $R = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Definition 2

1. *A* **function** *(or* **map***)* φ *is a rule*
$$\varphi : S \to T$$
which assigns each element s *in the set* S *to an element* $\varphi(s)$*, called its* **image***, in the set* T*.*
2. *Given a function* $\varphi : S \to T$*,* S *is called the* **domain** *(or* **source***) of* φ *and* T *is called the* **codomain** *(or* **target***) of* φ*.*
3. *The* **image** *of a function* $\varphi : S \to T$ *is the set of elements* $t \in T$ *such that there exists* $s \in S$ *satisfying* $\varphi(s) = t$*. We use the notation* $\varphi(S)$ *or* $\mathrm{image}(\varphi)$*.*
4. *The set of functions from one set* S *to another* T *is called a* **function space***, denoted* T^S*.*

In order to be **well-defined** as a function, $\varphi : S \to T$ cannot map the same element $s \in S$ to more than one distinct element in T.

However, we may have $\varphi(s_1) = \varphi(s_2)$ with $s_1 \neq s_2$.

We also do not require every element $t \in T$ to have a **preimage** in S, meaning, there need not exist any $s \in S$ such that $t = \varphi(s)$.

Example 2

Define $\varphi : \mathbb{Q} \to \mathbb{Z}$ by $\varphi(\frac{m}{n}) = n$. Why isn't φ well-defined?

As one might expect, we have terms to describe such situations where no two elements in S have the same image and/or every element in T has a preimage.

Definition 3

Suppose $\varphi : S \to T$ is a map between sets.

(a) *φ is* **one-to-one** *(or* **injective***) means for all $s_1, s_2 \in S$, if $\varphi(s_1) = \varphi(s_2)$ then $s_1 = s_2$.*

(b) *φ is* **onto** *(or* **surjective***) means for all $t \in T$, there exists $s \in S$ such that $t = \varphi(s)$.*

(c) *φ is* **bijective** *means it is both injective and surjective.*

The phrasing of Definition 3 suggests an approach to proving injectivity and surjectivity.

Example 3

The exponential function $f(x) = e^x$, or,

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto e^x, \end{aligned}$$

is injective. To prove, suppose $f(x) = f(y)$ for $x, y \in \mathbb{R}$. Then

$$\begin{aligned} e^x = e^y &\text{ implies} \\ \ln(e^x) = \ln(e^y) &\text{ implies} \\ x = y&. \end{aligned}$$

Thus x and y had to be the same element.

On the other hand, the map f in Example 3 is not surjective.

Question

How would you prove f in Example 3 is not surjective? How would you change the codomain to make f surjective?

Example 4

The **projection map**

$$\pi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$(a, b) \mapsto a$$

is surjective; to see why, choose any element $x \in \mathbb{Z}$. Then x has a preimage since, for example, $\pi(x, x) = x$.

Question

Is the projection map π in Example 4 injective? Answer with proof.

Exercise 1 (cf. Problem 38)

Which of the following are functions? Of those, which are injective and which are surjective?

(a) $\varphi_1 : \mathbb{Z} \to \mathbb{Z}$, where $\varphi_1(n) = n^2$;

(b) $\varphi_2 : \mathbb{Z} \to \mathbb{Q}$, where $\varphi_2(n) = \frac{2}{5n+1}$;

(c) $\varphi_3 : \mathbb{Z} \times \mathbb{N} \to \mathbb{Z}$, where $\varphi_3(n, m) = n^m$;

(d) $\varphi_4 : \mathbb{Z} \to \{-1, 1\}$, where $\varphi_4(n) = \sin(\frac{\pi}{2} n)$.

Binary operations

Definition 4

A map of the form $\star : S \times S \to S$ is called a **binary operation***.*

Authors often write $s_1 \star s_2 = \star(s_1, s_2)$ or, as a further shorthand when the context is clear, $s_1 s_2 = \star(s_1, s_2)$. The latter is called **mutliplicative notation**.

In defining the operation $\star$ on S, authors may use the "maps to" symbol

$$\star : (s_1, s_2) \mapsto \star(s_1, s_2)$$

or the "definition" symbol

$$s_1 \star s_2 := \star(s_1, s_2).$$

Example 5

(a) Multiplication is a binary operation on $\mathbb{R}$:

$$\begin{aligned} \star : &\mathbb{R} \times \mathbb{R} \to \mathbb{R} \\ &(r_1, r_2) \mapsto r_1 r_2 \end{aligned}$$

Why? Because multiplying two elements in $\mathbb{R}$ results in another element in $\mathbb{R}$.

(b) Similarly, adding two elements in $\mathbb{R}$ results in another element in $\mathbb{R}$:

$$\begin{aligned} \bullet : &\mathbb{R} \times \mathbb{R} \to \mathbb{R} \\ &(r_1, r_2) \mapsto r_1 + r_2 \end{aligned}$$

(Here we use the symbol $\bullet$ to distinguish the operation from the $\star$ in part (a).)

Binary operations are ubiquitous!

Example 6

Addition and multiplication are each binary on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathrm{Mat}_{\mathbb{R}}(n, n)$, and more.

Example 7

Division is binary on each of $\mathbb{Q}^\times$, $\mathbb{R}^\times$, and $\mathbb{C}^\times$.

Question

Why isn't division binary on $\mathbb{Z}^\times$?

Exercise 2 (cf. Problem 39)

Which of the following are binary operations?

(a) On $\mathbb{N}$, $n \star m := n$;

(b) On $\mathbb{N}$, $n \ominus m := n - m$;

(c) On $\mathbb{Z}$, $n \ominus m := n - m$;

(d) On $\mathbb{Z}$, $n \odot m := 2^{n+m}$;

(e) On $\mathbb{Q}$, $n \diamond m := n^m$;

(f) On S^S, composition – i.e., the operation $f \circ g$ where $f, g \in S^S$;

(g) On S^T, composition.

Definition of a group

Definition 5

A **group** $(G, \star)$ *is a set* G *with a binary operation* $\star$*, satisfying the following properties:*

- $\star$ *is* **associative***, meaning for any elements* $g_1, g_2, g_3 \in G$*,* $(g_1 \star g_2) \star g_3 = g_1 \star (g_2 \star g_3)$*.*
- G *contains an element* e *called the* **identity** *of* G*, satisfying* $g \star e = g$ *and* $e \star g = g$ *for all* $g \in G$*.*
- *every element* $g \in G$ *has an* **inverse** $h \in G$*, satisfying* $g \star h = e$ *and* $h \star g = e$*. Depending on the context we denote the inverse of* g *by either* g^{-1} *or* $-g$*.*

The three items listed in Definition 5, along with the existence of $\star$, are called the **group axioms**.

In this example, the objects we work with are very abstract, but it does not stop us from using the definitions to deduce things!

Example 8

Suppose $(G_1, \star_1), \ldots, (G_n, \star_n)$ are groups. Then their direct product $G := G_1 \times \cdots \times G_n$ is a group under the operation

$$\star : G \times G \to G$$
$$((g_1, \ldots, g_n), (h_1, \ldots, h_n)) \mapsto (g_1 \star_1 h_1, \cdots, g_n \star_n h_n).$$

We say $\star$ is defined **component-wise**.

To prove G is a group we verify the group axioms:

- Existence of a binary operation?
  Yes. The operation $\star$ is defined component-wise and each of the respective components' operations is binary.

- Associativity?
  Yes. Again, it follows from associativity on each of the components; take $f = (f_1, \ldots, f_n)$, $g = (g_1, \ldots, g_n)$, and $h = (h_1, \ldots, h_n)$ in G:
$$\begin{aligned}(f \star g) \star h &= (f_1 \star_1 g_1, \ldots, f_n \star_n g_n) \star h \\ &= ((f_1 \star_1 g_1) \star_1 h_1, \ldots, (f_n \star_n g_n) \star_n h_n) \\ &= (f_1 \star_1 (g_1 \star_1 h_1), \ldots, f_n \star_n (g_n \star_n h_n)) \\ &= f \star (g_1 \star_1 h_1, \ldots, g_n \star_n h_n) \\ &= f \star (g \star h)\end{aligned}$$
- Existence of an identity element?
  Yes. Let $e = (e_1, \ldots, e_n)$, where e_i is the identity element in G_i, for $i = 1, \ldots, n$. For $g = (g_1, \ldots, g_n) \in G$,
$$\begin{aligned}g \star e &= (g_1 \star_1 e_1, \ldots, g_n \star_n e_n) = (g_1, \ldots, g_n) = g \\ &= (e_1 \star_1 g_1, \ldots, e_n \star_n g_n) = (g_1, \ldots, g_n) = g \\ &= e \star g.\end{aligned}$$

- Existence of inverse elements?
  Yes. Suppose $g = (g_1, \dots, g_n) \in G$. Then we must have $g^{-1} = (g_1^{-1}, \dots, g_n^{-1})$:

$$\begin{aligned} g \star g^{-1} &= (g_1 \star_1 g_1^{-1}, \dots, g_n \star_n g_n^{-1}) \\ &= (e_1, \dots, e_n) = e \\ &= (g_1^{-1} \star_1 g_1, \dots, g_n^{-1} \star_n g_n) \end{aligned}$$

$\square$

If $G_1 = \cdots = G_n$ are the same group H, then we may write

$$H^n := \underbrace{H \times \cdots \times H}_{n \text{ times}}.$$

A group operation doesn't have to be commutative! If it is though, we say G is **abelian**.

Exercise 3 (cf. Problem 41)

Which of the following pairs are groups? Which, among the groups, are abelian?

(a) $(\mathbb{Q}^+, \cdot)$, where $\mathbb{Q}^+$ denotes the set of all positive rational numbers

(b) $(\mathbb{Z}, -)$

(c) $(\mathbb{R}^+, \div)$, where $\mathbb{R}^+$ denotes the set of all positive real numbers

(d) $(\mathbb{Z}_{12}, \oplus_{12})$, where $\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 11\}$ and $\oplus_{12}$ refers to **modular arithmetic**:

$$n \oplus_{12} m = \text{the remainder of } n + m \text{ when divided by } 12$$

(e) $(\mathrm{GL}(2, \mathbb{R}), \cdot)$, the set of invertible 2×2 matrices with entries in $\mathbb{R}$, under matrix multiplication

Exercise 4 (cf. Problem 42)

Let Γ denote the graph in Figure 1.1.

(a) Show the set $\mathcal{S}(\Gamma)$ of **recurrent sandpiles** under **stable addition** form a group.

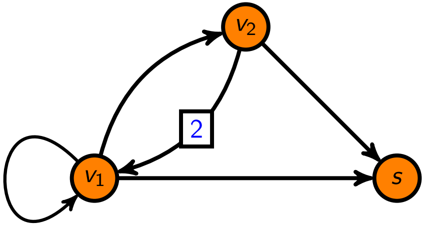

Figure 1.1: Directed graph with a self-loop.

(b) Show the set $\mathcal{M}(\Gamma)$ of **stable sandpiles** is not a group.

Dihedral groups

One special class of groups are the **dihedral groups**. Denoted D_n, their elements correspond to symmetries of a regular n-gon.

Example 9

$D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$, the dihedral group of order 4, is the set of symmetries on a square:

$$
\begin{aligned}
e &= \text{identity; do nothing} \\
r &= \text{rotate 90 degrees clockwise} \\
r^2 &= \text{rotate 180 degrees} \\
r^3 &= \text{rotate 90 degree counter-clockwise} \\
s &= \text{reflect across the vertical axis} \\
rs &= \text{reflect across the diagonal with negative slope} \\
r^2s &= \text{reflect across the horizontal axis} \\
r^3s &= \text{reflect across the diagonal with positive slope}
\end{aligned}
$$

We illustrate the (right) action of each element in D_4 on a portrait of Niels Henrik Abel†:

e

r

r^2

r^3

s

rs

$r^2 s$

$r^3 s$

Question

Why is the action of D_4 qualified as a *right* action?

† Image by Johan Gørbitz - Originally uploaded to English wikipedia by en:User:Pladask, `http://goo.gl/DkGu1P`, Public Domain, `https://goo.gl/ugIjzo`.

Exercise 5 (cf. Problem 40)

(a) Complete the **multiplication table** for D_4.

D_4	e	r	r^2	r^3	s	rs	r^2s	r^3s
e	e							
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
r^2								
r^3								
s								
rs								
r^2s								
r^3s								

(b) For each element in D_4, write down its inverse.

(c) Prove D_4 is not abelian.

Permutation groups

Another special class of groups are the **permutation groups**.

Definition 6

A **permutation** *of a set S is a bijection $\sigma : S \to S$.*

Exercise 6

(Prove:) Given a fixed set S with finitely many elements, the set of permutations on S forms a group under composition.

Definition 7

The group of permutations of the set $\{1, 2, \ldots, n\}$ *is called the* **symmetric group of order** n*, and is denoted* S_n*.*

Exercise 7

For which values of n is the permutation group S_n abelian?

Example 10

One way to denote elements in S_n is using matrices. For example, the matrix

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix} \in S_5$$

represents the permutation

$$\begin{aligned} \sigma : \{1, 2, 3, 4, 5\} &\to \{1, 2, 3, 4, 5\} \\ 1 &\mapsto 3 \\ 2 &\mapsto 1 \\ 3 &\mapsto 5 \\ 4 &\mapsto 4 \\ 5 &\mapsto 2. \end{aligned}$$

Monoids

In Exercise 3 some of the set/operation pairs listed were not groups, but satisfied most of the required axioms. In fact, there is a more general notion of such a pair.

Definition 8

A **monoid** $M = (M, \star)$ *is a set* M*, for which the following properties hold:*

- $\star$ *is a binary operation on* M
- $\star$ *is associative*
- M *contains an identity element with respect to* $\star$

A monoid is **commutative** *means* $a \star b = b \star a$ *for all* $g, h \in M$.

Some authors refer to monoids as **semigroups**, and the difference is the presence of the identity element – there is no convention on which term refers to which situation, so most authors specify or else use the terms *monoid* and *semigroup* interchangeably.

Question

All groups are monoids. What is the missing axiom that makes a monoid, in general, not a group?

Example 11

Given a directed graph Γ with a global sink, the set $\mathcal{M}(\Gamma)$ of all stable sandpiles forms a monoid, known as the **sandpile monoid of Γ**. (See Exercise 4.)

Example 12

$\mathbb{Q}$ is a group under addition, but not multiplication – the element 0 has no inverse. However, $\mathbb{Q}$ is a monoid under multiplication. For this reason, when we refer to $\mathbb{Q}$ as a group, its implied operation is always addition.

On the other hand, $\mathbb{Q}^\times$ is a group under multiplication (hence, the name).

Question

Is $\mathbb{Q}^\times$ a group under addition?

Exercise 8

Prove the statements in Example 12:

(a) $\mathbb{Q}$ is a group under addition, but not multiplication.

(b) $\mathbb{Q}$ is monoid under multiplication.

(c) $\mathbb{Q}^\times$ is a group (implied operation is multiplication).