

Group

Adrien FRABETTI MATHIEU

Contents

Definition	1
First properties	1
Groups of automorphisms	1
Order of a group	1

Definition

First properties

Definition 1 (Group)

A *group* is a set X equipped with a binary operation $\cdot : X^2 \rightarrow X$, such that

Associativity $\cdot$ is associative.

Unitality There exists a neutral element $1 : X$ for $\cdot$.

Inversability For every $x : X$, there exists an inverse $x^{-1} : X$ such that

$$x \cdot x^{-1} = x^{-1} \cdot x = 1$$



Definition (..) => ..: Group

Lemma 2

Let G be a group. The neutral element, and the inverses, are unique.



Uniqueness of neutral Let e and e' be two neutral elements. We have

$$e = e \cdot e' = e'$$

Uniqueness of inverses Let $x : G$, and y and z be two inverses of x . We have

$$\begin{aligned} y &= y \cdot e \\ &= y \cdot x \cdot z \\ &= z \end{aligned}$$

Groups of automorphisms

Let $\mathcal{C}$ be a category, and $X : \mathcal{C}$ be an object. We can form its *group of automorphisms* $\text{Aut}(X)$ as follows: elements of $\text{Aut}(X)$ are isomorphisms $f : X \rightarrow X$ in $\mathcal{C}$, with inner operation the composition. Groups of automorphisms are extremely common.

Example 1 (Symmetry group)

Let X be a set. We note $\mathfrak{S}_X$ the group of its bijections, called *permutations*.

A sub-group of $\mathfrak{S}_X$ is called a *permutation group*.



Example (..) => ..: Symmetry group

We note

$$\mathfrak{S}_n := \mathfrak{S}_{[1,n]}$$

the canonical group of symmetries over a finite set of cardinal.

Example 2 (Linear group)

Let V be a linear space. We note $\text{GL}(V)$



Example (..) => ..: Linear group

Order of a group

The cardinal of a group is so important in characterizing groups that it has its own name:

Definition 1 (Group order)

Let G be a group. We note its cardinal $|G|$, and say it is its *order*.



Definition (..) => ...: Group order

Those two examples are instances of groups of automorphisms in a given category, respectively for **Set** and **Vect**.

Definition 2 (Group product)

Let $(G_i)_{i:I}$ be a family of groups. We can canonically equip $\prod_{i:I} G_i$ with a group law¹, which makes it the *product group of the G_i* .



Definition (..) => ...: Group product

This group is called the product of the G_i because it is a cartesian product in the category **Grp**.

Definition 3 (Abelian group)

We say that a group G is *abelian* if its multiplication is commutative



Definition (..) => ...: Abelian group

Example 4

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are abelian groups (for $+$). Similarly, $\{\pm 1\}$, $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{U}_n$, $\mathbb{U}_\infty$, $\mathbb{U} := \mathbb{S}^1$ are abelian (for $\times$).



Example 5

There exists a unique group law over $\mathbb{Z}/(n\mathbb{Z})$ such that $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/(n\mathbb{Z})$ is a group morphism.



Definition 6 (Sub-group)

A sub-group of a group G is a group $H \subseteq G$ such that the inclusion is a group morphism.



Definition (..) => ...: Sub-group

Example 7

- $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$
- $\text{GL}(V) \leq \mathfrak{S}_V$
- Let E be a Euclidian space. An isometry is a bijection of E that preserves the metric of E . We note the group of isometries $I_s(E)$. It holds that

$$I_s(E) \leq \text{frak}_E$$

- $O(E) \leq I_s(E)$, where $O(E)$ is the orthogonal group. As soon as an isometry fixes $O(E)$, it is linear.



¹Given by pointwise product.

Definition 8 (Generated sub-group)

Let G be a group, and $X \subseteq G$ a subset of G . The sub-group $\langle X \rangle \leq G$ generated by X is the smallest sub-group of G that contains X .



Definition (. .) $\Rightarrow$. . : Generated sub-group

One says that X *generates* G if $\langle X \rangle = G$.