1.2 Groups: definition and basic properties. Examples

Recall the set of symmetries of an equilateral triangle T. We noticed that

- symmetries can be composed giving rise to another symmetry
- there is one symmetry which acts trivially (we call it: identity)

Also note that for every symmetry we can find another one such that their composition brings T back to its original configuration (that is, one symmetry is the inverse of the other

Similar properties could be observed looking at the set of the integers $\mathbb{Z}$ together with the operation "+" [0 acts "neutrally"; the addition is a binary operation taking 2 integers to another integer; for every integer $x \in \mathbb{Z}$ $\exists$ $-x \in \mathbb{Z}$ such that $x+(-x)=0$]

The definition of a group is inspired by all these properties/observations.

Definition A group is a set G together with an operation $\star : G \times G \to G$ such that each of the following axioms is satisfied:

(A) Associativity: For all $a, b, c \in G$

$$(a \star b) \star c = a \star (b \star c)$$

Note: this tells us that first performing $(a \star b)$ and then taking $\star c$ is the same as first performing $(b \star c)$ and then taking $a \star$. Left and right do matter!

(Id) Existence of an identity element: There exists $e \in G$ such that

$$a \star e = e \star a = a \quad \text{for all } a \in G$$

(Inv) Existence of inverse elements: For each $a \in G$ there exists $b \in G$ such that

$$a \star b = e = b \star a.$$

Examples (1) The additive group of the integers $(\mathbb{Z}, +)$

(2) The symmetry of symmetries of the equilateral triangle equipped with composition: $(S(T), \circ)$

(3) $(\mathbb{C}^\times, \cdot)$ The nonzero complex numbers with multiplication. Let's check it.

(Complex) Multiplication of two nonzero complex numbers gives us another nonzero complex number. That is $\mathbb{C}^\times$ is closed under multiplication and the first requirement in the def. is satisfied.

Associativity (we take it for granted)

(Id) The complex number 1 satisfies $z \cdot 1 = 1 \cdot z = z$ for all $z \in \mathbb{C}^\times$

(Inv) Given $z \in \mathbb{C}^\times$ we can find an inverse (suppose $z = a+ib$ for $a, b \in \mathbb{R}$)

$$\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{a-ib}{(a+ib)(a-ib)} = \frac{a-ib}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{ib}{a^2+b^2}$$

Note that if we had included the 0 in our set, we would have lost this last property.

(4) $(\mathbb{Q}^+, \cdot)$ You can check it - taking associativity for granted.

(5) $(2\mathbb{Z}, +)$ The set of even integers with addition (again - no need to check (A)).

Non-examples Here are some examples of sets for which one axiom or another fail and that therefore are not groups.

- The set of positive integers with addition (Here both (Inv) and (Id) fail).
- The set of odd integers with addition. The sum of two odd numbers is even! The first requirement (that the set is closed under the operation) fails.

Facts • The identity element of a group G is unique.

•• The inverse of each element in a group is unique.

Let's verify the first:

Suppose e and f are elements of G satisfying (Id). By definition, for all x in G

$$x * e = e * x = x$$

and

$$x * f = f * x = x$$

In particular, this holds when substituting $f = x$ in the first identity and $e = x$ in the second, which become:

$$f * e = e * f = f$$

and

$$e * f = f * e = e$$

} therefore $e = f$.

A similar argument shows that the inverse of each element is unique. We shall write a^{-1} for the inverse of an element $a \in G$.

So far the sets underlying our groups were both finite (as in the case of SCT) or $\mathbb{R}(H)$) or infinite (as in the case of $(\mathbb{Z}, +)$, $(\mathbb{C}^\times, \cdot)$ and so on)

Terminology • We say that a group $(G, *)$ is finite (resp. infinite) if the underlying set is finite (resp. infinite).

• If $(G, *)$ is finite, we call $|G|$ the **order** of G.

Also, we have seen examples of groups which all elements commute and groups in which this is not the case

- We say that a group $(G, *)$ is commutative if $a * b = b * a$ for all $a, b \in G$

More examples

(6) $(GL(2,\mathbb{Q}), \cdot) = \left(\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Q} \text{ and } ad - bc \neq 0\right\}, \cdot\right)$

This is a non-commutative group:

→ closed under multiplication (if $A, B \in GL(2,\mathbb{Q})$ then the entries of AB are rational; why is the second condition also satisfied?)

→ Associativity ✓

→ (Id) the matrix $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ belongs to $GL(2,\mathbb{Q})$ and satisfies (Id)

→ (Inv) Does every element of $GL(2,\mathbb{Q})$ have an inverse in $GL(2,\mathbb{Q})$?

(7) Consider the following set of matrices:

$$S_3 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right\}$$

You can check that $(S_3, \cdot)$ is a group with matrix multiplication.

Is this group commutative?