Group Theory

Paolo Bettelini

Contents

1 Groups

1.1 Binary operations

Let G be a set. A *binary operation* $\circ$ on G is a map

$$G \times G \to G, \qquad\qquad (x, y) \to x \circ y$$

1.2 Cayley tables

A binary operation $\circ$ on a finite set G can be visualized using a *Cayley table*.

Example: $G = \{0, 1\}$ and $\circ \equiv$ multiplication.

$\circ$	0	1
0	0	0
1	0	1

1.3 Definition

A *group* $(G, \circ)$ is a tuple containing a set G and a binary operation $\circ$ where $\circ$ satisfies. The operation $\circ$ between a and b may be written as $a \circ b$ or just ab.

1. **Associativity**: $\forall a, b, c \in G a \circ (b \circ c) = (a \circ b) \circ c$
2. **Identity**: $\exists e \,|\, \forall a \in G, ea = ae = a$
3. **Inverse**: $\forall a \in G \exists a^{-1} | a^{-1} a = aa^{-1} = e$

The element e is unique whereas a^{-1} depends on a.

1.4 Proof of uniqueness of the identity element

Suppose there is more than one identity element, e_1 and e_2.

$$\begin{aligned} e_1 &= e_1 \circ e_2 && \text{since } e_2 \text{ is an identity} \\ &= e_2 && \text{since } e_1 \text{ is an identity} \end{aligned}$$

Thus, e_1 and e_2 must be the same. This reasoning can be extended to when we may suppose to have n identity elements.

1.5 Proof of uniqueness of the inverse element

Suppose we have $a \in G$ with inverses c and c.

$$\begin{aligned} b &= b \circ e = b \circ (a \circ c) \\ (b \circ a)c &= e \circ c \\ &= c \end{aligned}$$

Thus, b and c must be the same. This reasoning can be extended to when we may suppose to have n inverses of a.

1.6 Inverse of Product

This theorem says that $(a \circ b)^{-1} = a^{-1} \circ b^{-1}$.

We start by noticing that by association we have

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

This implies that $(a \circ b)$ is the inverse of $(b^{-1} \circ a^{-1})$. Since $(a \circ b) \circ (a \circ b)^{-1} = e$ we have

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = e = (a \circ b) \circ (a \circ b)^{-1}$$

We can clearly see that $(b^{-1} \circ a^{-1}) = (a \circ b)^{-1}$.

2 Subgroups

Given a group $(G, \circ)$, a subset $H \subseteq G$ is called a *subgroup* of G $(H \leq G)$ if $(H, \circ)$ is also a group with closure under $\circ$.

2.1 One-Step Subgroup Test