Group Theory

Paolo Bettelini

Contents

1 Groups

1.1 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

1.2 Definition

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

The relation must satisfy the following properties

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**: $\forall a \in G, \exists a^{-1} \in G \,|\, a^{-1}a = aa^{-1} = e$
4. **Closure**: $\forall a, b \in G, a \circ b \in G$

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

1.3 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.

1.4 Proof of uniqueness of the inverse element

Suppose we have $a \in G$ with inverses b 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.

1.5 Cancellation laws

Rigth cancellation law

$$ba = ca \implies b = c$$

Left cancellation law

$$ab = ac \implies b = c$$

1.6 Inverse of Product

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

We start by noticing that by associativity 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 $(b^{-1} \circ a^{-1}) = (a \circ b)^{-1}$.

In general, we have

$$(a_1 \circ a_2 \circ \dots a_n)^{-1} = a_n^{-1} \circ \dots \circ a_2^{-1} \circ a_1^{-1}$$

2 Subgroups

2.1 Definition

Given an algebraic structure $g = (G, \circ)$ and a group $h = (H, \circ)$, h is a subgroup of g ($g \leq h$) if $H \subseteq G$.

2.2 One-Step Subgroup Test

Theorem. *Let $(G, \circ)$ be a group and let $H \subseteq G$ where $\emptyset \neq H$.*
Then $(H, \circ)$ is a subgroup of $(G, \circ)$ $\iff \forall a, b \in H, a \circ b^{-1} \in H$.

Proof. ($\implies$): Assume $(H, \circ) \leq (G, \circ)$. The properties of a group directly infer $\forall a, b \in H, a \circ b^{-1} \in H$
($\impliedby$): Assume $\forall a, b \in H, a \circ b^{-1} \in H$

- **Identity**: let $a = b$, then $a \circ a^{-1} H \implies e \in H$.
- **Inverse**: Let $k \in H$, $a = e$ and $b = k$. $a \circ b^{-1} = e \circ k^{-1} \implies k^{-1} \in H$.
- **Closure**: Let $m, n \in H \implies n^{-1} \in H$ and let $a = m$ and $b = n^{-1}$. $a \circ b^{-1} = a \circ (b^{-1})^{-1} = a \circ b$. This implies $a, b \in H$.

□