

# Group Theory

Paolo Bettelini

## Contents

<b>1</b>	<b>Groups</b>	<b>2</b>
1.1	Cayley tables . . . . .	2
1.2	Definition . . . . .	2
1.3	Proof of uniqueness of the identity element . . . . .	2
1.4	Proof of uniqueness of the inverse element . . . . .	2
1.5	Cancellation laws . . . . .	3
1.6	Inverse of Product . . . . .	3
<b>2</b>	<b>Subgroups</b>	<b>3</b>
2.1	Definition . . . . .	3
2.2	One-Step Subgroup Test . . . . .	3
2.3	The centralizer subgroup . . . . .	4
2.4	The conjugate subgroup . . . . .	4
<b>3</b>	<b>Center of a group</b>	<b>5</b>

# 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

### Definition Group

A *group*  $(G, \circ)$  is a tuple containing a set  $G$  and a binary operation  $\circ$  on  $G \times G$ .

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:**  $\exists e \mid \forall a \in G, ea = ae = a$
3. **Inverse:**  $\forall a \in G, \exists a^{-1} \in G \mid a^{-1}a = aa^{-1} = e$
4. **Closure:**  $\forall a, b \in G, a \circ b \in G$

The operation  $\circ$  between  $a$  and  $b$  may be written as  $a \circ b$  or just  $ab$ .

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

### Theorem Uniqueness of the inverse element

If  $e$  is an identity element of a group, then it is unique.

### Proof 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

### Theorem Uniqueness of the inverse element

If  $a^{-1}$  is an inverse of  $a$  in a group, then it is unique.

### Proof 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

### Theorem Right cancellation law

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

### Theorem Left cancellation law

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

## 1.6 Inverse of Product

### Theorem Inverse of Product

Consider a group  $(G, \circ)$ . For any two elements  $a, b \in G$

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

### Proof Inverse of Product

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

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

## 2 Subgroups

### 2.1 Definition

#### Definition Subgroups

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

### 2.2 One-Step Subgroup Test

#### Theorem One-Step Subgroup Test

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 One-Step Subgroup Test

( $\implies$ ): 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  $a, b \in H$ .

## 2.3 The centralizer subgroup

### Definition The centralizer subgroup

Let  $H \leq G$  be groups and define

$$C_G(H) = \{g \in G \mid \forall h \in H, gh = hg\}$$

as the centralizer of  $H$ .

This is the set of all elements of  $G$  such that they commute with every element of  $H$ .

### Theorem

Let  $H \leq G$ , then  $C_G(H) \leq G$ .

### Proof

Suppose  $a, b \in C_G(H)$ . We want to show  $ab^{-1} \in C_G(H)$ .

Note that the condition  $gh = hg \iff hg^{-1} = g^{-1}h$ .

Consider the expression  $(ab^{-1})h = a(b^{-1}h) = ahb^{-1} = h(ab^{-1})$ . This means that  $ab^{-1} \in C_G(H)$  and thus in  $H$ .

## 2.4 The conjugate subgroup

### Definition The conjugate subgroup

Let  $H \leq G$  be groups and define

$$g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$$

as the conjugate subgroup.

### Theorem

Let  $H \leq G$ , then  $g^{-1}Hg \leq G$ .

### Proof

Suppose  $a, b \in g^{-1}Hg$ . We want to show  $ab^{-1} \in g^{-1}Hg$ .

Note that  $a = g^{-1}h_1g$  and  $b = g^{-1}h_2g$  for some  $h_1, h_2 \in H$ .

This means that  $ab^{-1} = (g^{-1}h_1g)(g^{-1}h_2g)^{-1} = a(g^{-1}h_2^{-1}g) = g^{-1}h_1gg^{-1}h_2^{-1}g = g^{-1}(h_1h_2^{-1})g \in g^{-1}Hg$  because  $h_1h_2^{-1} \in H$ .

### 3 Center of a group

**Definition** Center of a group

Let  $G$  be a group. The center of the group  $G$  is defined as

$$Z(G) = \{g \in G \mid \forall x \in G, gx = xg\}$$

This is the set of all elements that commute with every other element. The condition  $gx = xg$  is also sometimes expressed as  $gxg^{-1} = x$ .

**Theorem**

Let  $G$  be a group, then  $Z(G) \leq G$ .

**Proof**

Assume  $a, b \in Z(G)$  meaning  $a = gag^{-1}$  and  $b = gbg^{-1}$  for any  $g \in G$ .

We want to show  $ab^{-1} \in Z(G)$ .  $ab^{-1} = (gag^{-1})(gbg^{-1})^{-1} = gag^{-1}gb^{-1}g^{-1} = gab^{-1}g^{-1}$  which is precisely the requirement to be in  $Z(G)$ .