Groups and Subgroups

Sanjyot Shenoy

2021

Table of Contents:

1 Introduction **1**
1.1 Group 1

1 Introduction

Definition 1.1 (Binary Operation)**:**
A binary operation $*$ on a set G is a function $* : G \times G \to G$. We shall write $*(a, b)$ as $a * b$.

Definition 1.2 (Associative Binary Operation)**:**
A binary operation $*$ on a set G is said to be associative if $\forall a, b, c \in G$ we have that $a*(b*c) = (a*b)*c$.

Definition 1.3 (Commutative Binary Operation)**:**
A binary operation $*$ on a set G is said to be commuative if $\forall a, b \in G$ we have $a * b = b * a$.

Example 1.1:

1. $+$ (usual addition) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ respectively).
2. $\times$ (usual multiplication) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ respectively).
3. $-$ (usual subtraction) is a non-commutative binary operation on $\mathbb{Z}$, where $-(a, b) = a - b$. The map $a \mapsto -a$ is not a binary operation.
4. Taking the vector cross-product of two vectors in 3-space $\mathbb{R}^3$ is a binary operation which is not associative and not commutative.

Remark(s):

1. Suppose that $*$ is a binary operation on a set G and $H \subset G$. If the restriction of $*$ to H is a binary operation on H, i.e, $\forall a, b \in H$, $a * b \in H$, then H is said to be **closed** under $*$.
2. Observe that is $*$ is associative (respectively, commutative) binary operation on G and $*$ restricted to some subset H of G is a binary operation on H, then $*$ is automatically associative (respectively, commutative) on H as well.

1.1 Group

Definition 1.4 (Group)**:**
A **Group** is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying the following axioms:

1. (Associative) $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$, i.e.,$*$ is associative.
2. (Existence of Identity) There exists an element e, called an identity of G, such that $\forall a \in G$, we have $a * e = e * a = a$.

3. (Existence of Inverses) $\forall a \in G$, $\exists a^{-1} \in G$, called an inverse of a, such that $a * a^{-1} = a^{-1} * a = e$.

Definition 1.5 (Abelian Group)**:**
A Group $(G, *)$ is said to be an Abelian group if the binary operation $*$ on G is commutative for all elements of G.

Remark(s):

1. We shall immediately become less formal and say G is a group under * if $(G, *)$ is a group (or just G is a group when the operation $*$ is clear from the context).

2. (Finite Group) - If the set G is a finite set, then the group G is called a finite group.

3. (Non-emptiness of set): By axiom on existence of identity, the set G is non-empty.

Direct Product of Groups

If $(A, *)$ and $(B, \diamond)$ are groups, we can form a new group $A \times B$ called their **direct product**, whose elements are those in the Cartesian product.

$$A \times B = \{(a, b) | a \in A,\, b \in B\}.$$

and whose operation is defined componentwise:

$$(a_1, b_1)(a_2, b_2) = (a_1 * a_2, b_1 \diamond b_2).$$

It is easy to check that this is a group.