Group Theory

Jonathan Gribbins

Contents

1 Introduction to Groups

1.1 Basic Axioms

A group is one of the fundamental algebraic objects studied in abstract algebra. Groups are sets coupled with a binary operation in the ordered pair $(G, \star)$, where $\star$ is a **binary operation**—

(1) A *binary operation* is a function on a set G mapping $G \times G$ to G: $\star : G \times G \to G$. This operation upon an ordered pair in G is denoted $\star(a, b)$ for $a, b \in G$.

(2) A binary operation is *associative* if for all $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$.

(3) Two elements $a, b \in G$ *commute* if $a \star b = b \star a$. A binary operation is *commutative* if $\forall a, b \in G, a \star b = b \star a$.

A **group** is an ordered pair of a set and a binary operation upon this set $(G, \star)$ such that three axioms are fulfilled:

(1) G is **associative**, so for all $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$.

(2) There is some element $e \in G$ such that for all elements $a \in G$, $a \star e = a$.

(3) For all $a \in G$, there is some element $a^{-1} \in G$ such that $a \star a^{-1} = e$.

A group G is called **abelian** or **commutative** if for all $a, b \in G$, $a \star b = b \star a$.

It can be shown that for any group G under binary operation $\star$,

(1) The identity (e) of G is unique.

(2) For each $a \in G$, a^{-1} is unique.

(3) $(a^{-1})^{-1} = a$ for all $a \in G$.

(4) $(a \star b)^{-1} = (b)^{-1} \star (a)^{-1}$.

(5) For any $a_1, a_2, a_3, ...a_n \in G$, the value of $a_1 \star a_2 \star a_3 \star ... \star a_n$ does not vary based on parentheses or brackets.

Because of **(5)**, for any element $a \in G$, the product of $n \in Z^+$ as $(a \star a \star a...(ntimes))$ can be denoted a^n. Additionally, if we let a be the inverse x^{-1} of an element $x \in G$, we would denote the nth product of x^{-1} as x^{-n}. The identity of a group G can be denoted a^0 for all $a \in G$.

Order of an element $x \in G$: The order of an element $x \in G$ is the *smallest positive integer* n such that $x^n = 1$ (where is the identity of G). This integer is also denoted $|x|$. If there is no integer n such that $x^n = 1$, x is said to be of infinite order.

Cayley table of group G The *Cayley, multiplication, or group table* of a finite group $G = \{g_1, g_2, g_3, ...g_n\}$ is an $n \times n$ table where the entry at location (i, j) in the table is equal to $g_i g_j$.