1.1.6. Some General Properties of Groups

1) **Uniqueness of Inverse Element:** The inverse of a group element g is unique. Let h and k are both inverses of g, i.e., (g•h) = (h•g) = e and (g•k) = (k•g) = e (where 'e' is the identity element)

Theorem: Inverse of a group is unique.

Proof: Suppose <G, *> be a group and $b \in G$
Suppose inverse of b are a and e
a*b = b*a = e [if a is inverse]
e*b = b*e = e [if e is inverse]

From Associative Law, we have
$a = ae = a(b*e) \Rightarrow (a*b)e$ (By Associative Law)
$= ee = e$
i.e., a = e

Therefore, the inverse of a group is unique.

2) **Uniqueness of Identity Element**

Theorem (Uniqueness of Identity): The identity of a group is unique.

Proof: Suppose <G, *> is a group and e_1 and e_2 are two identity elements.
$\forall a \in G,\ a \times e_1 = e_1 \times a = a$
$\forall a \in G,\ a \times e_2 = e_2 \times a = a$
$(e_1 \times e_2) = e_1 =$ if e_2 is identity
$(e_1 \times e_2) = e_2 =$ if e_1 is identity
So, $e_1 = e_2$
Hence, group has unique identity.

3) **Associativity:** The consequence of the composition of any number of elements is independent of the way in which the product is bracketed, then
a•((b•c)•d) = (a•b)•(c•d).

4) **Cancellation Laws**
Theorem: In a group G, if a•g = b•g, then a = b. Similarly, if g•a = g•b, then a = b.

Proof: Let $a \bullet g = b \bullet g$ and $h = g^{-1}$ i.e.,
$a = a \bullet e = a \bullet (g \bullet h) = (a \bullet g) \bullet h = (b \bullet g) \bullet h = b \bullet (g \bullet h)$
$= b \bullet e \quad = b.$

For example, Suppose Z is the set of integers then

i) $<Z, +>$ hold cancellation law as $(a + b) = (a + c)$ $\Rightarrow (b = c)$

ii) $<Z, ->$ hold cancellation law as $(a - b) = (a - c)$ $\Rightarrow (b = c)$

iii) $<Z, \times>$ does not hold cancellation law as $a \times b \neq a \times c \Rightarrow b \neq c$

Theorem 6: In a group (G, ∗) show that $(a^{-1})^{-1} = a \; \forall a \in G$

Proof: Hence G is a group
Thus, $\forall a \in G \Rightarrow a^{-1} \in G \Rightarrow (a^{-1})^{-1} \in G$

From definition, we have
$a * a^{-1} = e = a^{-1} * a$ .....(1)
$a^{-1} * (a^{-1})^{-1} = e = (a^{-1})^{-1} * a^{-1}$ .....(2)

Here, e is an identity element in G.

Suppose, $a * a^{-1} = e$

Post operating $(a^{-1})^{-1}$ on both sides we obtain,
$a * a^{-1} * (a^{-1})^{-1} = e * (a^{-1})^{-1} = (a^{-1})^{-1}$
$a * (a^{-1} * (a^{-1})^{-1}) = (a^{-1})^{-1}$
(∵ '∗' is associative and 'e' is an identity element)
$a * e = (a^{-1})^{-1}$
$a = (a^{-1})^{-1}$. Hence proved

Theorem 7: The left inverse of an element is also its right inverse.

Or

Theorem: The left inverse of an element is also its right inverse, i.e., if a^{-1} is the left inverse of a, then also $aa^{-1} = e$.

Proof: Suppose e is the identity element and $a \in G$. Suppose a^{-1} is the left inverse of a, i.e., $a^{-1} a = e$.
Verify that $aa^{-1} = e$.

By associativity, we know that
$a^{-1}(aa^{-1}) = (a^{-1} a) a^{-1} = ea^{-1}$ [∵ $a^{-1} a = e$]
$= a^{-1}$ [∵ e is left identity]

When e is a left identity then,
$= a^{-1} = a^{-1} e.$ [∵ e is also right identity]

When e is also right identity then
Now $a^{-1}(aa^{-1}) = a^{-1} e$
$\Rightarrow \quad aa^{-1} = e$ [by left cancellation law]

According to left cancellation law, we have
$\Rightarrow \quad aa^{-1} = e$

Hence, a^{-1} is also the right inverse of a. Therefore, a^{-1} is the inverse of a, i.e., $a^{-1} a = e = aa^{-1}$.

Note 1: To verify that a non-empty set G which is equipped with a binary operation is a group, it is adequate to verify that the operation is associative, that there exists a left identity and a left inverse of every element of G.