Theorem

Suppose $(S, *)$ has an identity element e for $*$. If $\phi : S \to S'$ is an isomorphism of $(S, *)$ with $(S', *')$, then $\phi(e)$ is the identity element for the binary operation $*'$ on S'

proof

To show that $\phi(e)$ is an identity element for the binary operation $*'$ on S'. we have to prove that

$$x *' \phi(e) = x = \phi(e) *' x \quad \forall x \in S'$$

We have $\phi : S \to S'$ is an isomorphism.
and 'e' is an identity element for $(S, *)$

ie, $a * e = a = e * a$.

$\therefore \quad a * e = a = e * a$.

$\Longrightarrow \phi(a * e) = \phi(a) = \phi(e * a)$

$\Longrightarrow \phi(a) *' \phi(e) = \phi(a) = \phi(e) *' \phi(a)$ —— (1)

[$\because \phi$ is an Homomorphism]

Since $\phi : S \to S'$ is onto. [Isomorphism]
Choose any $x \in S'$ $\exists$ a unique $a \in S$ s.t. $\phi(a) = x$. —— (2)

(2) in (1) we get

$$x *' \phi(e) = x = \phi(e) *' x \quad \forall x \in S'$$

Hence $\phi(e)$ is the identity element for the binary operation $*'$ on S'.

§ 4. GROUPS

Definition. A ***group*** *$(G, *)$ is a set G, closed under a binar[y] operation $*$, such that the following axioms* (known as ***group axioms***) *are satisfied:*

G_1: *For all $a, b, c \in G$ we have*

$$(a*b)*c = a*(b*c) \qquad \textbf{(associativity of } *)$$

G_2: *There is an element e, called an identity of $*$, in G such that for all $a \in G$,*

$$e*a = a*e = a \qquad \textbf{(existence of identity)}$$

G_3: *Corresponding to each $a \in G$, there is an element b in G such that*

$$a*b = e = b*a \qquad \textbf{(existence of inverse)}$$

The element b is then called the ***inverse of*** a and is denoted by a^{-1} or a', so that $a*a^{-1} = e = a^{-1}*a$ or $a*a' = e = a'*a$

Abelian Group. *A group $(G, *)$ is said to be* ***abelian*** or ***commutative group****, if in addition to the axioms* $\mathbf{G_1}$, $\mathbf{G_2}$ *and* $\mathbf{G_3}$ *the following axiom also hold:*

$\mathbf{G_4}$: *For any* $a, b \in G$, $a * b = b * a.$ **(*commutativity of* $*$)**

Remark. For your information, we remark that binary algebraic structures with weaker axioms than those for a group have also been studied quite extensively. Of these weaker structures, two important binary structures are ***semigroup*** and ***monoid***. *A* ***semigroup*** *is a set with an associative binary operation. A* ***monoid*** *is a semigroup that has an identity element for the binary operation.* Note that every group is both a semigroup and a monoid.

It is possible to give axioms for a group $(G, *)$ that seem at first glance

Problem 1. *Show that the set $\mathbb{Z}$ of all integers*

$$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

is an abelian group with respect to the operation of addition of integers.

Solution. In order to show that $\mathbb{Z}$ is a group, we should verify all the group axioms. Since the sum of any two integers is an integer, addition is a binary operation defined on $\mathbb{Z}$. The closure property is therefore satisfied.

G_1: For any $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + b + c = a + (b + c)$.

Therefore addition of integers is associative.

G_2: The element 0 is in $\mathbb{Z}$ and

$$0 + a = a = a + 0, \quad \text{for all } a \in \mathbb{Z}.$$

Therefore 0 is the identity element.

G_3: If a is in $\mathbb{Z}$, then $-a$ is also in $\mathbb{Z}$ and

$$a + (-a) = 0 = (-a) + a.$$

Thus every integer possesses additive inverse.

Hence $(\mathbb{Z}, +)$ is a group. Also, we know that addition of numbers is commutative. Hence

G_4: For any $a, b \in \mathbb{Z}$, $\quad a + b = b + a$.

Hence $(\mathbb{Z}, +)$ is an abelian group.

Problem 2. *Show that the set $\mathbb{Z}^+$, of natural numbers is not a group with respect to addition.*

Solution. Since sum of two natural numbers is a natural number, addition is a binary operation on $\mathbb{Z}^+$, i. e., $\mathbb{Z}^+$ is closed with respect to addition. Also addition of natural numbers is an associative operation. But there exists no natural number e, such that $e + a = a = a + e$, for all $a \in \mathbb{Z}^+$. For the addition of numbers 0 is the identity element and $0 \notin \mathbb{Z}^+$. Therefore $(\mathbb{Z}^+, +)$ is not a group.