Algebraic Structures

Thm: The identity elements of a binary operation $*$ in a set A, if it exist and is unique.

Proof: If possible, Let e' and e'' be two identity elements in A with respect to the binary operation $*$.

e' is an identity element in A

$\Rightarrow e' * e'' = e'' * e' = e''$

and e'' is an identity element in A

$\Rightarrow e'' * e' = e' * e'' = e'$

which together show that $e' = e''$

Thm: If $*$ is an associative binary operation in A, then the inverse of every invertible element is unique.

Proof: Let $a \in A$, be an invertible element w.r.t. $*$.

If possible let b and c be two distinct inverse of the element a in A.

Let e be the identity elements in A w.r.t. $*$.

Then we have

$b * a = a * b = e$

and $c * a = a * c = e$

now $(b * a) * c = b * (a * c)$ ($\because *$ is associative in A)

$\Rightarrow e * c = b * e$

$\Rightarrow c = b$

This completes the proof of the theorem.

Thm: If $*$ is an associative binary operation in a set A, such every element is invertible, then $*$ satisfies the left as well as the right cancellation laws i.e.

$$a * b = a * c \Rightarrow b = c$$
$$b * a = c * a \Rightarrow b = c \;; \quad \forall a, b, c \in A.$$

Proof: Let e be the identity element of A w.r.t. $*$.

Every element in A is invertible

$\Rightarrow a \in A$ is invertible.

Let a' denote the inverse of a in A then

$a * b = a * c$

$\Rightarrow a' * (a * b) = a' * (a * c)$

$\Rightarrow (a' * a) * b = (a' * a) * c$ ($\because$ $*$ is associative in A)

$\Rightarrow e * b = e * c$ ($\because$ a' is the inverse of a)

$\Rightarrow b = c$

similarly we can prove that

$$b * a = c * a \Rightarrow b = c \;; \quad \forall a, b, c \in A.$$

Thm: Let $(S, *)$, $(T, \cdot)$ and (V, Δ) be semigroups, $f: S \to T$ and $g: T \to V$ be semigroup homomorphism. Then $gof: S \to V$ is a semigroups homomorphism from $(S, *)$ to (V, Δ).

Proof: Let $a, b \in S$ then

$$
\begin{aligned}
(gof)(a * b) &= g[f(a * b)] \\
&= g[f(a) \cdot f(b)] \\
&= g(f(a)) \,\Delta\, g(f(b)) \\
&= (gof)(a) \,\Delta\, (gof)(b)
\end{aligned}
$$

$\Rightarrow gof: S \to V$ is a semigroup homomorphism.

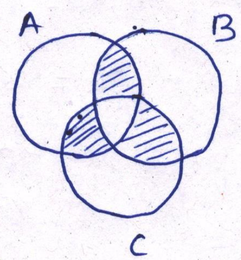
Ex: Let S be non-empty set and $P(S)$ be the collection of all subsets of S. Let the binary operation Δ called the symmetric difference of sets be defined as $A \Delta B = (A-B) \cup (B-A)$: $\forall\, A, B \in P(S)$.
then show that $(P(S), \Delta)$ is an abelian group.

Sol^n: If A and B are any two subsets of S, then $A \Delta B$ is also a subset of S,

Therefore $(P(S), \Delta)$ is closed w.r.t. Δ.

Associativity: $\forall\, A, B, C \in P(S)$

$(A \Delta B) \Delta C = A \Delta (B \Delta C)$ can easily be verified by ven diagram.



Existence of identity:

$\phi \in P(S)$ such that $A \Delta \phi = A = \phi \Delta A$

$\Rightarrow \phi$ is the identity in $(P(S), \Delta)$.

Existance of inverse:

$\forall\, A \in P(S)$,

$A \Delta A = \phi \Rightarrow A$ is the inverse of A.

Commutative law: $\forall\, A, B \in P(S)$

$$A \Delta B = (A-B) \cup (B-A)$$
$$= (B-A) \cup (A-B)$$
$$= B \Delta A$$

Hence $(P(S), \Delta)$ is an abelian group.

Ex: Prove that the set $\mathbb{Z}$ of all integers with binary operation $*$ defined by $a*b = a+b+1$ $\forall\, a, b \in \mathbb{Z}$ is

Thm: If $(G, *)$ is a group, then the identity element in G is unique.

Proof: Let e_1 and e_2 be identity elements in G.

e_1 is the identity element and $e_2 \in G$.

$\Rightarrow e_1 * e_2 = e_2 = e_2 * e_1$ —— ①

Imp

e_2 is the identity element and $e_1 \in G$.

$\Rightarrow e_2 * e_1 = e_1 = e_1 * e_2$ —— ②

From ① and ②, we get

$$e_1 = e_2$$

Thm: The inverse of each element in a group $(G, *)$ is unique.

Proof: Let $a \in G$ and e be the identity element in G.

Let $b \in G$ be an inverse of a in G also let $c \in G$ be an inverse of a in G.

Since b is the inverse of a, we have

$$a * b = b * a = e$$

Also c is an inverse of a in G

Imp

$$\Rightarrow a * c = c * a = e$$

Now
$$\begin{aligned} b &= b * e \\ &= b * (a * c) \quad (\because e \text{ is the identity.}) \\ &= (b * a) * c \quad (\text{by associative law}) \\ &= e * c \\ &= c \end{aligned}$$

Note: The identity element is its own inverse.

Thm: In a group $(G, *)$, $(a^{-1})^{-1} = a$, $\forall a \in G$

Imp i.e. a^{-1} is the inverse of a in G.

Proof G is a group.

$\therefore$ $a \in G \Rightarrow a^{-1} \in G$ such that

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

Now $a^{-1} \in G \Rightarrow (a^{-1})^{-1} \in G$ such that

$$(a^{-1}) * (a^{-1})^{-1} = e = (a^{-1})^{-1} * (a^{-1})$$

Consider $a^{-1} * a = e$

$\Rightarrow (a^{-1})^{-1} * (a^{-1} * a) = (a^{-1})^{-1} * e$ (multiplying both sides on the left by $(a^{-1})^{-1}$)

$\Rightarrow \{(a^{-1})^{-1} * a^{-1}\} * a = (a^{-1})^{-1}$

$\Rightarrow e * a = (a^{-1})^{-1}$

$\Rightarrow a = (a^{-1})^{-1}$

$\therefore (a^{-1})^{-1} = a$, $\forall a \in G$.

thm: If $(G, *)$ is a group then $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$. (Reversal law).

Imp

Proof: Let $a, b \in G$ and e be the identity element in G.

$a \in G \Rightarrow a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$

and $b \in G \Rightarrow b^{-1} \in G$ such that $b * b^{-1} = b^{-1} * b = e$

Now, $a, b \in G \Rightarrow a * b \in G$ and $(a * b)^{-1} \in G$

Consider $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b$ (by associative law)

$= b^{-1} * e * b$ $(\because a^{-1} * a = e)$

$= b^{-1} * b$ $(\because e$ is the identity$)$

$= e \quad (\because b^{-1} * b = e)$

and $(a*b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$

(by associative law)

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

$= a * a^{-1}$

$= e$

$\therefore (b^{-1} * a^{-1}) * (a*b) = (a*b) * (b^{-1} * a^{-1}) = e$

$\Rightarrow (a*b)^{-1} = b^{-1} * a^{-1}, \quad \forall a, b \in G$ (by defn. of inverse)

Thm: Cancellation laws holds good in G

i.e. for all $a, b, c, \in G$

$a * b = a * c \Rightarrow b = c$ (left cancellation law)

$b * a = c * a \Rightarrow b = c$ (Right ")

Proof: $a \in G \Rightarrow a^{-1} \in G$ s.t.

$a * a^{-1} = a^{-1} * a = e$, where e is the identity element in G.

Consider,

$a * b = a * c$

$\Rightarrow a^{-1} * (a * b) = a^{-1} * (a * c)$

$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$ (by associative law)

$\Rightarrow e * b = e * c$ ($\because a^{-1}$ is the inverse of a)

$\Rightarrow b = c$ ($\because$ e is the identity element in G)

Now

$b * a = c * a$

$\Rightarrow (b * a) * a^{-1} = (c * a) * a^{-1}$

$\Rightarrow b * (a * a^{-1}) = c * (a * a^{-1})$ (by associative law)

$\Rightarrow b * e = c * e$ ($\because a * a^{-1} = e$)

$\Rightarrow b = c$ ($\because$ e is the identity element in G)