$$g(\alpha\beta) = g(\alpha) \oplus g(\beta)$$

so that g is the required homomorphism.

Theorem 5. Let (S, $*$) and (T, Δ) be two semigroups and g be a semigroup homomorphism from (S, $*$) to (T, Δ). Corresponding to the homomorphism g, there exists a congruence relation R on (S, $*$) defined by

$$x \text{ R } y \quad \text{iff } g(x) = g(y) \quad \text{for } x, y \in S$$

Proof : It is easy to see that R is an equivalence relation on S. Let $x_1, x_2, x_1', x_2' \in S$ such that $x_1 \text{ R } x_1'$ and $x_2 \text{ R } x_2'$. From

$$g(x_1 * x_2) = g(x_1) \,\Delta\, g(x_2) = g(x_1') \,\Delta\, g(x_2') = g(x_1' * x_2')$$

it follows that R is a congruence relation on (S, $*$).

Theorem 6. Let (S, $*$) be a semigroup and R be a congruence relation on (S, $*$). The quotient set S/R is a semigroup (S/R, $\oplus$) where the operation $\oplus$ corersponds to the operation $*$ on S. Also, there exists a homorphism from (S, $*$) onto (S/R, $\oplus$) called the natural homomorphism.

Proof : For any $a \in S$, let $[a]$ denote the equivalence class corresponding to the congruence relation R. For $a, b \in S$ define an operation $\oplus$ on S/R given by

$$[a] \oplus [b] = [a * b]$$

The associativity of the operation $*$ guarantees the associativity of the operation $\oplus$ on S/R, so that (S/R, $\oplus$) is a semigroup. Next, define a mapping $g : S \rightarrow S/R$ given by

$$g(a) = [a] \text{ for any } a \in S$$

Property 1 : A semigroup homomosphism preserves the property of associativity.

Solution : Let $a, b, c \in S$

$$g[(a * b) * c] = g(a * b) \circ g(c)$$

$$= [(g(a) \circ g(b)) \circ g(c)] \quad \dots (1)$$

$$g[a * (b * c)] = g(a) \circ g(b * c)$$
$$= g(a) \circ [g(b) \circ g(c)] \quad \ldots (2)$$

But in S, $(a * b) * c = a * (b * c) \ \forall \ a, b, c \in S$

$$\therefore \quad g[(a * b) * c] = g[a * (b * c)]$$
$$\Rightarrow [g(a) \circ g(b)] \circ g(c) = g(a) \circ [g(b) \circ g(c)]$$

The property of associativity is preserved.

Property 2 : A semigroup homomorphism preserves idempotency.

Solution : Let $a \in S$ be an idempotent element.

$$\therefore \quad a * a = a$$
$$\therefore \quad g(a * a) = g(a)$$
$$g(a) \circ g(a) = g(a)$$

This shows that $g(a)$ is an idempotent element in T.

$\therefore$ The property of idempotency is preserved under semigroup homomorphism.

Property 3 : A semigroup homomosphism preserves commutativity.

Solution : Let $a, b \in S$.

Assume that $a * b = b * a$

$$g(a * b) = g(b * a)$$
$$g(a) \circ g(b) = g(b) \circ g(a)$$

This means that the operation $\circ$ is commutative in T.

$\therefore$ The semigroup homomorphism preserves commutativity.

Property 4 : Show that every finite semigroup has an idempotent element.

Solution : Consider the subsemigroup S generated by s (i.e.,) $S = \{s, s^2, s^3, \ldots s^n\}$, where ~~$n$ is~~ finite. S is a finite subset of a finite semigroup G. Therefore there exist r_1, r_2 such that $s^{r_1} = s^{r_2}$. Without loss of generality, we assume that $r_1 > r_2$.

$$g(\alpha\beta) = g(\alpha) \oplus g(\beta)$$

so that g is the required homomorphism.

Theorem 5. Let (S, *) and (T, Δ) be two semigroups and g be a semigroup homomorphism from (S, *) to (T, Δ). Corresponding to the homomorphism g, there exists a congruence relation R on (S, *) defined by

$$x \, R \, y \qquad \text{iff } g(x) = g(y) \qquad \text{for } x, y \in S$$

Proof : It is easy to see that R is an equivalence relation on S. Let $x_1, x_2, x_1', x_2' \in S$ such that $x_1 \, R \, x_1'$ and $x_2 \, R \, x_2'$. From

$$g(x_1 * x_2) = g(x_1) \,\Delta\, g(x_2) = g(x_1') \,\Delta\, g(x_2') = g(x_1' * x_2')$$

it follows that R is a congruence relation on (S, *).

Theorem 6. Let (S, *) be a semigroup and R be a congruence relation on (S, *). The quotient set S/R is a semigroup (S/R, $\oplus$) where the operation $\oplus$ corersponds to the operation * on S. Also, there exists a homorphism from (S, *) onto (S/R, $\oplus$) called the natural homomorphism.

Proof : For any $a \in S$, let $[a]$ denote the equivalence class corresponding to the congruence relation R. For $a, b \in S$ define an operation $\oplus$ on S/R given by

$$[a] \oplus [b] = [a * b]$$

The associativity of the operation * guarantees the associativity of the operation $\oplus$ on S/R, so that (S/R, $\oplus$) is a semigroup. Next, define a mapping $g : S \rightarrow S/R$ given by

$$g(a) = [a] \text{ for any } a \in S$$

Property 1 : A semigroup homomosphism preserves the property of associativity.

Solution : Let $a, b, c \in S$

$$g[(a * b) * c] = g(a * b) \circ g(c)$$
$$= [(g(a) \circ g(b)) \circ g(c)] \qquad \dots (1)$$

$$g[a * (b * c)] = g(a) \circ g(b * c)$$

$$= g(a) \circ [g(b) \circ g(c)] \quad \ldots (2)$$

But in S, $(a * b) * c = a * (b * c) \;\forall\; a, b, c \in S$

$$\therefore \quad g[(a * b) * c] = g[a * (b * c)]$$

$$\Rightarrow [g(a) \circ g(b)] \circ g(c) = g(a) \circ [g(b) \circ g(c)]$$

$\therefore$ The property of associativity is preserved.

Property 2 : A semigroup homomorphism preserves idempotency.

Solution : Let $a \in S$ be an idempotent element.

$$\therefore \quad a * a = a$$

$$\therefore \quad g(a * a) = g(a)$$

$$g(a) \circ g(a) = g(a)$$

This shows that $g(a)$ is an idempotent element in T.

$\therefore$ The property of idempotency is preserved under semigroup homomorphism.

Property 3 : A semigroup homomosphism preserves commutativity.

Solution : Let $a, b \in S$.

Assume that $a * b = b * a$

$$g(a * b) = g(b * a)$$

$$g(a) \circ g(b) = g(b) \circ g(a)$$

This means that the operation $\circ$ is commutative in T.

$\therefore$ The semigroup homomorphism preserves commutativity.

Property 4 : Show that every finite semigroup has an idempotent element.

Solution : Consider the subsemigroup S generated by s (i.e.,) $S = \{s, s^2, s^3, \ldots s^n\}$, where n is finite. S is a finite subset of a finite semigroup G. Therefore there exist r_1, r_2 such that $s^{r_1} = s^{r_2}$. Without loss of generality, we assume that $r_1 > r_2$.

Now we have two cases.

Case 1 : Suppose $r_1 - 2r_2 \geq 0$

Put $r = r_1 - 2r_2$

Now

$$s^{r_1} s^r = s^{r_2} s^r = s^{r_1 - r_2}$$

$$(\because r_2 + r = r_2 + r_1 - 2r_2 = r_1 - r_2)$$

$$s^{r_1 + r} = s^{2(r_1 - r_2)}$$

This implies that S has an idempotent.

Case 2 : Suppose $r_1 - 2r_2 < 0$

Put $r_1 - r_2 = r$

$$s^{r_1} s^r = s^{r_2 + r} = s^{r_1} = s^{r_2}$$

$$s^{r_1} s^r s^r = s^{r_2 + r} = s^{r_1} = s^{r_2}$$

Proceeding in this way, we can find an integer $r_1' \geq 2r_2$ such that

$$s^{r_1'} = s^{r_2}$$

which leads to case 1.

Thus we have proved that S has an idempotent which inturn implies that the semigroup G has an idempotent.

Problems under semi-group and monoid

Example 1. Give an example of a semi-group which is not a monoid. **[A.U. M/J 2009]**

Solution : Let $D = \{..., -4, -2, 0, 2, 4, ...\}$

$(D, \cdot)$ is a semi-group but not a monoid since multiplicative identity is 1, but $1 \notin D$

Example 2. Give an example of a monoid which is not a group.

Solution : $(Z^+, .)$ is a monoid which is not a group.

Since $\forall\ a \in G,\ \frac{1}{a} \notin G$

Example 3. What do you call a homomorphism of a semi-group into itself? [A.U. A/M 2003]

Solution : A homomorphism of a semi-group into itself is called a semi group endomorphism.

Example 4. If (Z, +) and (E, +) where Z is the set all integers and E is the set of all even integers, show that the two semi groups (Z, +) and (E, +) are isomorphic. [A.U. N/D 2010]

Solution :

Step 1 : We define the function

$G : Z \rightarrow E$ given by $g(a) = 2a$ where $a \in Z$

Step 2 : Suppose $g(a_1) = g(a_2)$ where $a_1, a_2 \in Z$

Then $2a_1 = 2a_2$ i.e., $a_1 = a_2$

Hence mapping by g is one-to-one.

Step 3 : Suppose b is an even integer

Let $a = b/2$. Then $a \in Z$ and

$g(a) = g(b/2) = 2 \cdot b/2 = b$

i.e., every element b in E has a preimage in Z.

So mapping by g is onto.

Step 4 : Let a and $b \in Z$

$$\begin{aligned} g(a+b) &= 2(a+b) \\ &= 2a + 2b \\ &= g(a) + g(b) \end{aligned}$$

Hence, $(Z, +)$ and $(E, +)$ are isomorphic semigroups.

Example 5. If * is a binary operation on the set R of real numbers defined by a * b = a + b + 2ab,

(1) Find < R, *> is a semigroup.

(2) **Find the identify element if it exists.**

(3) **Which elements has inverse and what are they?**

Solution :

[A.U A/M 2011]

(1) $(a * b) * c = (a + b + 2ab) + c + 2(a + b + 2ab)c$

$$= a + b + c + 2(ab + bc + ca) + 4abc$$

$$a * (b * c) = a + (b + c + 2bc) + 2a(b + c + 2bc)$$

$$= a + b + c + 2(ab + bc + ca) + 4abc$$

Hence, $(a * b) * c = a * (b * c)$

i.e., $*$ is associative.

(2) If the identity element exists, let it be e.

Then for any $a \in R$.

$$a * e = a$$

i.e., $a + e + 2ae = a$

i.e., $e(1 + 2a) = 0$

$\therefore$ $e = 0$, since $1 + 2a \neq 0$, for any $a \in R$

(3) Let a^{-1} be the inverse of an element $a \in R$. Then $a * a^{-1} = e$

i.e., $a + a^{-1} + 2a \cdot a^{-1} = 0$

i.e., $a^{-1} \cdot (1 + 2a) = -a$

$$\therefore a^{-1} = -\frac{a}{1 + 2a}$$

$\therefore$ If $a \neq \frac{1}{2}$, then $a^{-1} = \frac{-a}{1 + 2a}$

Example 6. Let $< M, *, e_M >$ be a monoid and $a \in M$. If a invertible, then show that its inverse is unique.

[A.U A/M 2011]

Solution : Let b and c be elements of M

such that $a * b = b * a = e$ and

$a * c = c * a = e$

since

$$\begin{aligned} b &= b * e \\ &= b * (a * c) \\ &= (b * a) * c \\ &= e * c \\ &= c \end{aligned}$$

Example 7. Show that a semi-group with more than one idempotents cannot be a group. Give an example of a semi-group which is not a group. [A.U N/D 2014]

Solution : Let $(S, *)$ be semi-group.

Let a, b are two idempotents

$\therefore \ a * a = a$ and $b * b = b$

Let us assume that $(S, *)$ is group then each element has the inverse.

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

L.H.S $= (a * a) * a^{-1} = a * a^{-1}$ $\quad [\because a * a = a]$

$= e$

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

also R.H.S $= a * (a * a^{-1}) = a * e = a \quad \ldots (2)$

From (1) & (2), we get $a = e$

Similarly we can prove that $b = e$

In a group we can not have two identities and hence $(S, *)$ cannot be group.

This contradiction is due to an assumption that $(S, *)$ has two idempotents.

Example : Let $S = \{a, b, c\}$ under the operation $*$

Now for $x, y \in A^*$,

$$g(x) = g(y) \Leftrightarrow x \text{ R } y$$

so that the congruence relation R is induced by the homomorphism g

Example 15. If $*$ is the operation defined on $S = Q \times Q$, the set of ordered pairs of rational numbers and given by $(a, b) * (x, y) = (ax, ay + b)$, show that $(S, *)$ is a semi group. Is it commutative? Also find the identity element of S. **[A.U N/D 2012]**

Solution : Given : $(a, b) * (x, y) = (ax, ay + b)$ ... (1)

To prove : $(S, *)$ is a semigroup.

i.e., $\boxed{\text{To prove : } * \text{ operation is associative.}}$

$\{(a, b) * (x, y)\} * (c, d)$

$= (ax + ay + b) * (c, d)$ by (1)

$= (acx, adx + ay + b)$ ... (2) by (1)

$(a, b) * \{(x, y) * (c, d)\}$

$= (a, b) * \{cx, dx + y\}$

$= (acx, adx + ay + b)$ ... (3)

From (2) & (3), $*$ is associative on S.

$\boxed{\text{To prove : } (S, *) \text{ is not commutative.}}$

$(x, y) * (a, b) = (ax, bx + y)$ ... (4)

$(a, b) * (x, y) = (ax, ay + b)$ ... (5)

(4) $\neq$ (5) $\therefore \{S, *\}$ is not commutative.

$\boxed{\text{To find the identity element of } (S, *)}$

Let (e_1, e_2) be the identity element of $(S, *)$, $\forall (a, b) \in S$

i.e., $(a, b) * (e_1, e_2) = (a, b)$

$(ae_1, ae_2 + b) = (a, b)$

$\Rightarrow$ $a e_1 = a, \ a e_2 + b = b$

$$\Rightarrow e_1 = 1, \qquad ae_2 = 0$$

$$e_2 = 0$$

$\therefore$ (1, 0) is the identity element of $\{S, *\}$

MONOID :

Example 1 : Let X be any given set and P (X) is its power set. Then find the zeros of the semigroups (P (X), ∩) and (P (X), ∪). Are these monoids ? If so, what are the identities ?

Solution : Let X be any given set. Then its power set p (X) contains 2^X subsets of X.

If $Z \in p(X)$ is zero with respect to the operation ∩ for p (X), then $Z \cap X_1 = X_1 \cap Z = Z$ implies that $Z = \phi$, empty set.

The zero Z of (p (X), ∪) is such that $Z \cup X_1 = X_1 \cup Z = Z$ for all $X_1 \in p(X)$, implies that Z = the whole set X.

The identity of (p (X), ∩) is given by the set S_e, such that $S \cap S_e = S_e \cap S = S$ for all $S \in p(X)$.

Therefore $S_e = X$, the whole set.

The identity of (p (X), ∪) is S_e, which satisfies the property that $S = S_e \cup S = S \cup S_e$. Therefore S_e is the empty set ϕ.

With this it is clear that $(p(X) \cap X)$ and $(p(X) \cup \phi)$ are monoids.

Example 2 : Let V = $\{a, b\}$ and A be set of all sequences on V including ∧ beginning with a. Show that (A, ∘ ∧) is a monoid.

Solution : Let V = $\{a, b\}$ and A be set of all sequence on V including ∧ beginning with a. Then $A = \{\wedge, a, ab, aa, ab, aba, abb, \ldots\}$. Let ∘ be a concatenation operation on the sequences in A. Clearly for any two elements α, $b \in A$.

$\alpha \circ \beta = \alpha\beta$ also belongs to A and hence (A, ∘) is closed. Also '∘' is associative. Because

$$(\alpha \circ \beta) \circ \gamma = \alpha \beta \gamma = a \circ (\beta \gamma)$$
$$= (\alpha \circ \beta \circ \gamma)$$

$\wedge$ is identity as $\wedge \circ \alpha = \alpha \circ \wedge = \alpha$ for all $\alpha \in A$.

Therefore $(A, \circ \wedge)$ is a monoid.

Example 3 : Show that the set N of natural numbers is a semigroup under the operation $x * y = \max \{x, y\}$. Is it a monoid ?

Solution : Let $N = \{0, 1, 2, ...\}$

Define the operation $x * y = \max \{x, y\}$ for $x, y \in N$.

Clearly $(N, *)$ is closed because $x * y = \max \{x, y\} \in N$ and $*$ is associative as

$$(x * y) * z = \max \{x * y, z\}$$
$$= \max \{\max \{x, y\}, z\}$$
$$= \max \{x, y, z\}$$
$$= \max \{x, \max \{y, z\}$$
$$= \max \{x, \max \{y * z\}$$
$$= x * (y * z)$$

Therefore, $(N, *)$ is semigroup.

The identity e of $(W, *)$ must satisfy the property that $x * e = e * x = e$. But as $x * e = e * x = \max \{x, e\}$, $e = x$, ∞ (the infinity). Therefore $(N, *, \infty)$ is monoid.

Example 4 : Every monoid (M, *, e) is isomorphic to $(M^M, \bullet, \Delta)$ where Δ is the identity mapping to M.

Solution : Define a mapping f from M to M^M by

$$f(a) = f_a \text{ where } f_a \in M^M$$

defined by $f_a(b) = a * b$ for any $b \in M$

Now

$$f(a * b) = f_{a * b}, \text{ where}$$

$$f_{a * b}(c) = (a * b) * c = a * (b * c)$$

$$= f_a(b * c) = f_a \cdot f_b(c)$$

Therefore, $f_{a * b} = f_a \circ f_b$, which implies that

$$f(a * b) = f_{a * b} = f_a \circ f_b = f(a) \circ f(b)$$

Therefore f is a homomorphism.

Clearly f is one-one and onto and hence f is an isomorphism from M onto M^M.

Example 5 : Prove that monoid homorphism preserves invertibility and monoid epimorphism preserves zero element (if it exists).

[A.U. N/D 2003]

Sol. Let $(M, *, e_M)$ and (T, Δ, e_T) be any two monoids and let $g: M \to T$ be a monoid homomorphism. If $a \in M$ is invertible, let a^{-1} be the inverse of a in M. We will now show that $g(a^{-1})$ will be an inverse of $g(a)$ in T.

$$a * a^{-1} = a^{-1} * a = e_M \qquad \text{(By definition of inverse)}$$

So $\quad g(a * a^{-1}) = g(a^{-1} * a) = g(e_M)$

Hence $g(a) \Delta g(a^{-1}) = g(a^{-1}) \Delta g(a) = g(e_M)$

(since g is a homomorphism)

But $\quad g(e_M) = e_T \qquad$ (since g is a monoid hmomorphism)

$$\therefore g(a) \Delta g(a^{-1}) = g(a^{-1}) \Delta g(a) = e_T$$

This means $g(a^{-1})$ is an inverse of $g(a)$ i.e., $g(a)$ is invertible. Thus the property of invertibility is preserved under monoid homomorphism.

Assume g is monoid epimorphism

$$t \,\Delta\, g(z) = g(b) \,\Delta\, g(z) = g(b * z) = g(z)$$

and $$g(z) \,\Delta\, t = g(z) \,\Delta\, g(b) = g(z * b) = g(z)$$

$\therefore$ $g(z)$ is zero element of T.

Example 6 : On the set Q of all rational numbers, the operation $*$ is defined by $a * b = a + b - ab$. Show that, under this operation, Q is a commutative monoid.

Solution : Since $a + b - ab$ is rational number for all rational numbers a, b the given operation $*$ is a binary operation on Q.

We note that, for all $a, b, c \in Q$.

$$\begin{aligned}(a * b) * c &= (a + b - ab) * c \\ &= (a + b - ab) + c - (a + b - ab)\, c \\ &= a + b - ab + c - ac - bc + abc \\ &= a + (b + c - bc) - a\,(b + c - bc) \\ &= a * (b + c - bc) \\ &= a * (b * c)\end{aligned}$$

Hence $*$ is associative.

We check that, for any $a \in Q$,

$$a * 0 = a + 0 - a \,.\, 0 = a$$

and $$0 * a = 0 + a - 0 \,.\, a = a$$

As such, 0 is the identity element in Q under the given $*$.

The definition of $*$ itself indicates that $*$ is commutative.

Thus, under the given $*$, Q is a commutative monoid with 0 as the identity.

Example 7: Let V = {a , b}. Show that (V*, •, ∧) is an infinite monoid.

Solution : While defining alphapet and set of strings V^*, we proved that (V^*, •, ∧) is a monoid where ∧ is a empty string. So, it is enough to show that V^* is an infinite set. As a is an element of V, a, aa, aaa, $aaaa$, ... b, bb, bbb, $bbbb$, ... ab, abb, $abbb$, ... are the elements of V^* and hence V^* contains infinitely many strings including empty set.

Example 8. Let $(M, *)$ be a monoid. Prove that there exists a subset $T \subseteq M^M$ such that $(M, *)$ is isomorphic to the monoid (T, O) ; here M^M denotes the set of all mappings from M to M and "O" denotes the composition of mappings. **[A.U M/J 2014]**

Proof : $\forall a \in M$, let $g(a) = f_a$ where $f_a \in M^M$ is defined by $f_a(b) = a * b$ for any $b \in M$.

Clearly, g is a function from M to M^M.

Now, $g(a * b) = f_{a*b}$, where $f_{a*b}(c) = (a * b) * c$

$$= a * (b * c) \quad [\because \text{Associative law}]$$

$$= f_a(b * c)$$

$$= (f_a \circ f_b)(c)$$

$$\therefore \quad f_{a*b} = f_a \circ f_b$$

Hence,
$$g(a * b) = f_{a*b}$$
$$= f_a \circ f_b$$
$$= g(a) \circ g(b)$$
$$\therefore g(a * b) = g(a) \circ g(b) \ \forall \ a, b \in M$$

$\therefore g : M \to M^M$ is a homomorphism.

Corresponding to an element $a \in M$, the function f_a is completely determined from the entries in the row corresponding to the element a in the composition table of $(M, *)$.

Since, $f_a = g(a)$, every row of such a table determines the image of 'a' under the homomorphism g.

Let $g(M)$ be the image of M under the homomorphism g such that $g(M) \subseteq M^M$.

Let $a, b \in M$, then $g(a) = f_a$ and $g(b) = f_b$ are elements in $g(M)$.

Also, $f_a \circ f_b = f(a * b) \in g(M)$ since, $a * b \in M$.

$\therefore$ $g(M)$ is closed under the operation, composition of functions.

The mapping $g : M \to g(M)$ is onto size $(M, *)$ is a monoid. No two rows of the composition table can be identical.

$\Rightarrow$ Two functions defined by these rows will be identical.

$\therefore$ The mapping $g : M \to g(M)$ is one-to-one and onto.

$\therefore$ $g : M \to g(M)$ is an isomorphism. If e is the identity element of M then we define $f_e(a) = a \ \forall \ a \in M$.

Clearly, this function $f_e \in T = g(M)$

Now, $\quad f_e = g(e)$

Also $\quad f_a \circ f_e = g(a) \circ g(e)$

$$= g(a * e) = g(a)$$

$$\therefore f_a \circ f_e = g(a) = f(a).$$

This shows that f_e is the identity element of $T = g(M)$, since $f_a, f_b \in T$, $f_a \circ f_b \in T$.

$\therefore$ T is closed under the operation composition of functions.

$\therefore$ $T = g(M)$ is a monoid.

Further, $g : M \to T$ is a isomorphism.

Hence, $(M, *)$ is isomorphic to the monoid (T, o).

4.2.(b) Groups

Theorem 1.

If a and b are any two elements of a group $(G, *)$, then show that G is an abelian group if and only if

$$(a * b)^2 = a^2 * b^2$$

[A.U A/M 2003, A/M 2011, N/D 2010, M/J 2013]

Proof : $\boxed{\text{If part}}$

Given : G is an abelian group

$\Rightarrow \forall\ a, b \in G$, then $a * b = b * a$ ... (1)

To prove : $(a * b)^2 = a^2 * b^2$

$$\begin{aligned}
(a * b)^2 &= (a * b) * (a * b) \\
&= a * (b * a) * b \\
&= a * (a * b) * b \quad \text{by (1)} \\
&= (a * a) * (b * b) \\
&= a^2 * b^2
\end{aligned}$$

$\boxed{\text{Only if part}}$

Given : $(a * b)^2 = a^2 * b^2$ ... (2)

To prove : $a * b = b * a$

$$\begin{aligned}
(2) \Rightarrow \quad (a * b)^2 &= a^2 * b^2 \\
\Rightarrow (a * b) * (a * b) &= (a * a) * (b * b) \\
\Rightarrow a * [b * (a * b)] &= a * [a * (b * b)] \\
\Rightarrow \quad b * (a * b) &= a * (b * b) \quad \text{[Left cancellation law]} \\
\Rightarrow \quad (b * a) * b &= (a * b) * b \quad \text{[Associative law]} \\
\Rightarrow \quad b * a &= a * b \quad \text{[Right cancellation law]}
\end{aligned}$$

$\Rightarrow G$ is an abelian.

Theorem 2.

If every element in a group is its own inverse, then the group must be abelian.

(OR)

For any group $(G, *)$ if $a^2 = e$ with $a \neq e$ then G is an abelian

Proof :

Given $a = a^{-1}$ for all $a \in G$.

Let $a, b \in G$. Then $a = a^{-1}$ and $b = b^{-1}$

Now $\quad (a * b) = (a * b)^{-1}$

i.e., $\quad a * b = b^{-1} * a^{-1}$

$$= b * a$$

$\Rightarrow G$ is abelian.

Theorem 3 :

The identity element of a group is unique. [A.U. M/J 2014]

Proof :

Let $(G, *)$ be a group.

Let e_1 and e_2 be two identity elements in G.

Then

$e_1 * e_2 = e_1 \quad$ [$\because$ e_2 is the identity]

$e_1 * e_2 = e_2 \quad$ [$\because$ e_1 is the identity]

Thus $e_1 = e_2$

Hence the identity is unique.

Theorem 4 :

For any element a in a group G, the inverse is unique.

Proof :

Let 'a' be any element of a group G.

If possible let a' and a'' be two inverses of a.

Then

$$a * a' = a' * a = e \quad \ldots \text{(i)}$$

$$a * a'' = a'' * a = e \quad \ldots \text{(ii)}$$

Now $a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$

Hence, the inverse is unique.

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

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

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

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

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

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

Theorem 5.

The identity element is the only idempotent element of a group.

Solution : Given $(G, *)$ is a group.

Since $e * e = e$, e is indempotent.

Let a be any idempotent element of G.

Then $a * a = a$.

$e * a = a$. [$\because$ e is the identity element]

It follows that $a * a = e * a$.

By right cancellation law, we have $a = e$ and so e is the only idempotent element.

Now let $q \in B_n$. Then $q_0 \circ q \in A_n$, and

$$f(q_0 \circ q) = q_0 \circ (q_0 \circ q) = (q_0 \circ q_0) = 1_A \circ q = q,$$

which means that f is an onto function. Since $f : A_n \to B_n$ is one to one and onto, we conclude that A_n and B_n have the same number of elements. Note that $A_n \cap B_n = \phi$ since no permutation can be both even and odd. Also, by Theorem $|A_n \cup B_n| = n!$.

$$n! = |A_n \cup B_n| = |A_n| + |B_n| - |A_n \cap B_n| = 2|A_n|.$$

We then have

$$|A_n| = |B_n| = \frac{n!}{2}$$

PROBLEMS BASED ON GROUP

Example 1. State any two properties of a group. **[A.U N/D 2010]**

Solution : (i) The identity element of a group is unique.

(ii) The inverse of each element is unique.

Example 2. In a group G prove that an element $a \in G$ such that $a^2 = e$, $a \neq e$ iff $a = a^{-1}$

Solution : Let us assume that $a = a^{-1}$

Then $a^2 = a * a = a * a^{-1} = e$

Conversely assume that $a^2 = e$ with $a \neq e$.

That is $\quad a * a = e$

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

i.e., $\quad e * a = a^{-1}$

i.e., $\quad a = a^{-1}$

Example 3. Determine whether the set

$*$	-1	1
-1	1	-1
1	-1	1

With the binary operation form a group. **[A.U June 2011]**

Solution : Yes. '1' is the identity element.

Inverse of each element is the element itself.

Example 4. Define the homomorphism of two groups.

[A.U June 2011]

Solution : Let $(G, *)$ and (H, Δ) be any two groups.

A mapping $f: G \to H$ is said to be a homomorphism if

$$f(a * b) = f(a) \,\Delta\, f(b), \text{ for any } a, b \in G$$

Example 5. If any group (G, *) and $a \in G$, then $(a^{-1})^{-1} = a$

Solution : Given : a^{-1} is the inverse of a.

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

$\Rightarrow$ a is the inverse of a^{-1}

i.e., $(a^{-1})^{-1} = a$

Example 6. If any group (G, *), show that $(a * b)^{-1} = b^{-1} * a^{-1}$

Solution : Given : $(G, *)$ is a group.

$\forall\ a \in G \Rightarrow a^{-1} \in G$ also $a * a^{-1} = a^{-1} * a = e$

$\forall\ b \in G \Rightarrow b^{-1} \in G$ also $b * b^{-1} = b^{-1} * b = e$

To prove : $(a * b)^{-1} = b^{-1} * a^{-1}$

i.e., To prove : $(a * b) * (b^{-1} * a^{-1}) = (b^{-1} * a^{-1}) * (a * b) = e$

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

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