COSET : Definition

Let H be a sub-group of group G and $a \in G$, then then the set $aH = \{a * h \mid h \in H\}$ is called the left coset of H in G and $Ha = \{h * a \mid h \in H\}$ is called the right coset of H in G. By this definition it is very clear the corresponding to every element of G, we have, left coset and right coset of H in G. It is obvious that,

$$aH \subset G, \quad Ha \subset G \quad \forall a \in G$$

Further, $e * H = H = H * e$

i.e the left & right cosets of H corresponding to identity e coincide with H.

(If not abelian, $ah \neq ha$.
if abelian, $ah = ha$)

Hence H itself is a left as well as right coset of H in G.

Scanned with CamScanner

Q1) Let $G = (\mathbb{Z}, +)$ and $H = 2\mathbb{Z} = \{0, \pm 2, \pm 4 \cdots\}$ then the right cosets of H in G are:

$H+0 = \{0, \pm 2, \pm 4 \cdots\} = H$

$H+1 = \{0+1, \pm 2+1, \pm 4+1\} = \{\pm 1, \pm 3, \pm 5 \cdots\}$

$H+2 = \{0+2, 2+2, +4+2 \cdots\} = \{0, \pm 2, \pm 4 \cdots\} = H$

It can be easily observed that right coset and its corresponding left coset are equal i.e. $H+1 = 1+H$, $H+2 = 2+H$ etc

Again,

$H+3 = \{\cdots -6, -3, 0, 3, 6 \cdots\} = H$

$H+4 = \{\cdots -5, -2, 1, 4, 7, 10, 13 \cdots\} = H+1$

Similarly, $H+5 = H$, $H+6 = H$

$\therefore$ H has only two distinct cosets $H, H+1$ in $\mathbb{Z}$

Clearly $G = H \cup (H+1)$

of $H = n\mathbb{Z}$, no. of cosets $= n$

Q2) Find all cosets of $3\mathbb{Z}$ in the group $(\mathbb{Z}, +)$

Let $H = 3\mathbb{Z} = \{\cdots -6, -3, 0, 3, 6, \cdots\}$

The following distinct cosets of H in G are obtained:

$0+H = H+0 = \{\cdots -6, -3, 0, 3, 6 \cdots\} = H$

$1+H = H+1 = \{\cdots -5, -2, 1, 4, 7 \cdots\}$

$2+H = H+2 = \{\cdots -4, -1, 2, 5, 8 \cdots\}$

$3+H = H+3 = \{\cdots -6, -3, 0, 3 \cdots\} = H$

$4+H = H+4 = \{\cdots -2, 1, 4, 7, 10 \cdots\} = H+1$

$5+H = H+5 = \{\cdots -1, 2, 5, 8, 11 \cdots\} = H+2$

Scanned with CamScanner

$6+H = H+6 = \{\cdots 0, 3, 6, 9 \cdots\} = H+0$

On observing the above cosets, its clear that

$H+0 = H+3 = H+6 = H+9 \cdots = H+(-3) = H+(-6) \cdots$

$H+1 = H+4 = H+7 = H+10 \cdots = H+(-2) = H+(-5) \cdots$

$H+2 = H+5 = H+8 = H+11 \cdots = H+(-1) = H+(-4) \cdots$

Therefore three cosets of H in G are following:

$H, H+1, H+2$:

$G = H \cup (H+1) \cup (H+2)$

(Q3) Find all cosets of $H = [0, 4]$ in the group $G = (Z_8, +_8)$

Here $G = \{0, 1, 2, 3, 4, 5, 6, 7\}$ & $H = \{0, 4\}$

The following distinct cosets of H in G are obtained:

$0 +_8 H = H +_8 0 = \{0+_8 0, 4+_8 0\} = \{0, 4\} = H$

$1 +_8 H = H +_8 1 = \{0+_8 1, 4+_8 1\} = \{1, 5\}$

$2 +_8 H = H +_8 2 = \{0+2, 4+2\} = \{2, 6\}$

$3 + H = H + 3 = \{0+3, 4+3\} = \{3, 7\}$

$4 + H = H + 4 = \{0+4, 4+4\} = \{4, 0\} = H$

$5 + H = H + 5 = \{0+5, 4+5\} = \{5, 1\} = H+1$

$6 + H = H + 6 = \{0+6, 4+6\} = \{6, 2\} = H+2$

$7 + H = H + 7 = \{0+7, 4+7\} = \{7, 3\} = H+3$

~~$8 + H = H + 8 = \{0+8, 4+8\} = \{0, 4\}$~~

On observing the above cosets, it is clear that four cosets of H in G are:—

$H, H+1, H+2, H+3$

(Q4) If H is a subgroup of a group G and $g \in G$, then prove that

Scanned with CamScanner

a) $ghg^{-1} = \{ghg^{-1} \mid h \in H\}$ is a subgroup of G

b) If H is finite, then $O(H) = O(gHg^{-1})$

a) (We do it by the theorem, $a \in H, b \in H \Rightarrow ab^{-1} \in H$)

~~If H is a subgroup of group G.~~

Let $x = gh_1g^{-1}$, $y = gh_2g^{-1}$

Now, $xy^{-1} = (gh_1g^{-1})(gh_2g^{-1})^{-1}$

$= (gh_1g^{-1})[(g^{-1})^{-1}(h_2)^{-1}(g)^{-1}]$

$= (gh_1g^{-1})(gh_2^{-1}g^{-1})$

$= gh_1(g^{-1}g)h_2^{-1}g^{-1}$ (By associativity)

$= gh_1eh_2^{-1}g^{-1}$

$= g(h_1h_2^{-1})g^{-1} \in gHg^{-1}$ $[\because h_1h_2^{-1} \in H]$

Similarly $x \in gHg^{-1}$, $y \in gHg^{-1}$

$\Rightarrow xy^{-1} \in gHg^{-1}$

$\therefore gHg^{-1}$ is a sub-group of G

b) Define a map f from H to gHg^{-1} as follows:

$f: H \to gHg^{-1}$, $f(h) = ghg^{-1}$ $\forall h \in H$

$\therefore f(h_1) = f(h_2)$

$gh_1g^{-1} = gh_2g^{-1}$

$h_1 = h_2$ [$\because$ By cancellation law]

$\therefore f$ is one-one

Again for every $ghg^{-1} \in gHg^{-1}$, there is $h \in H$ s.t. $f(h) = ghg^{-1}$

Scanned with CamScanner

$\therefore f$ is onto

Hence, f is a bijection which proves that

$$O(H) = O(gHg^{-1})$$

THEOREMS

1) If H is a sub-group of a group G and $a \in G$ then, $a \in aH$ and $a \in Ha$

Proof: Let e be the identity element of G so also of H.

So for every $a \in G$, $e \in H \Rightarrow ae = a \in aH$

$e \in H \Rightarrow ea = a \in Ha$

Remark:

From the above theorem, it is clear that

$aH \neq 0$, $Ha \neq 0$, $a \in G$

2) Any two left (right) cosets of a subgroup are either identical or disjoint.

Let H be a subgroup of a group G have two left cosets aH and bH are are not disjoint.

$\therefore$ To prove: $aH = bH$

$\because aH \cap bH \neq \emptyset \Rightarrow$ There exists atleast one common element in bH and aH

Let $x \in aH$ and $x \in bH$ where $x = ah_1$, $x = bh_2$, $h_1, h_2 \in H$

Now $x = ah_1 = bh_2 \Rightarrow$

$a = bh_2h_1^{-1}$ and $b = ah_2h_1^{-1}$

Therefore, for any $h \in H$

$ah \in aH \Rightarrow ah = (bh_2h_1^{-1})h$

$= b(h_2h_1^{-1}h) \in bH \quad [\because h_2h_1^{-1}h \in H]$

$aH \subset bH$

Scanned with CamScanner

Again $bh \in bH \Rightarrow bh = (ah_1h_2^{-1})h$

$= a(h_1h_2^{-1}h) \in aH$

$= bH \subset aH$ $[\because (h_1h_2^{-1}h) \in H]$

(2) & (3) $\Rightarrow$ $aH = bH$

$\because aH \cap bH \neq \phi \Rightarrow aH = bH$

i.e any two left cosets are identical if they are not disjoint.

(Similarly prove for right cosets)

3) LAGRANGES THEOREM:

The order of every sub-group of a finite group is a divisor of the order of the group.

Let H be a subgroup of a finite supgroup G such that,

$O(G) = n$ & $O(H) = m$

We know that $G = \bigcup_{g=G} gH$ (Union of all distinct cosets gives back G)

Since all left cosets of H are not different, so let H have k distinct cosets viz,

$g_1H, g_2H \cdots g_kH$

Thus, $G = g_1H \cup g_2H \cup g_3H \cdots \cup g_kH$

Since all these left cosets are pairwise disjoint, so

$O(G) = O(g_1H) + O(g_2H) \cdots O(g_kH)$

Again, $O(H) = O(gH)$ $\forall g \in G$

$\therefore O(G) = O(H) + O(H) \cdots + O(H)$

$n = m + m \cdots m$ (k times)

$n = mk$

$\Rightarrow \boxed{k = n/m}$

Scanned with CamScanner

$O(H)$ is a divisor of $O(G)$

Important!
The converse of Lagrange's theorem is not always true i.e if m is a divisor of $n = O(G)$, then its not necessary that G has a subgroup of order m.

Cor 1: The order of every element of a finite group is a divisor of the order of the group.
Let a be an element of a finite group G. If H is a cyclic sub-group generated by a i.e, $H = [a]$, then
$O(a) = O(H)$. ($a^n = e$)
Since H is a sub-group of a finite group G,
$O(H) \mid O(G)$ ($O(G)$ divided by $O(H)$)
(∵ By Lagrange's theorem)
$O(a) \mid O(G)$ [∵ $O(a) = O(H)$]

Cor 2: If G is a finite group of order n and $a \in G$, then $a^n = e$
Let $O(a) = m$
Since G is a finite group, therefore by Cor 1, the order of $a \in G$ is a divisor of the order of G.
∴ $n = mk$, where k is any integer
$a^n = a^{mk}$
$= (a^m)^k = e^k = e$ [∵ $O(a) = m \Rightarrow a^m = e$]

Cor 3: Every group of prime order is cyclic
Let G be a group of order p, where p is prime
Now $O(G) = p$ (prime) $\rightarrow p > 1$

Scanned with CamScanner

⇒ G has atleast one element other than identity

∴ Let $a \in G$, $a \neq e$

If $H = [a]$, then

$O(H) \mid O(G)$ [by Lagrange's theorem]

$O(H) \mid p$

(If $O(H)$ divides p it will be either 1 or p as p is prime)

$O(H) = p$ or $O(H) = 1$

$\therefore O(H) = p = O(G)$ (as $O(H) \neq 1$)

Sim, $H \subset G$ and $O(H) \mid O(G)$

$\Rightarrow G = H = [a]$

($a^0 = e$, $\Rightarrow a^r = e$)

∴ G is a cyclic group with its every element as a generator except the identity

NORMAL SUB-GROUP

If a group is abelian, then for its subgroup H, the left and right cosets are equal.

$$aH = Ha$$

But if a group is not abelian, but still there can be a possibility that left coset & right coset is equal.

Such a subgroup is known as normal subgroup. So in case of an abelian group, all sub-groups are normal subgroups

Scanned with CamScanner

A sub-group H of group G is said to be normal subgroup of G if $x \in G$ and $h \in H \Rightarrow$

$$xh = hx$$
$$h = xhx^{-1}$$
$$\Rightarrow xhx^{-1} \in H$$

If H is a normal subgroup of G, then we symbolically write it as:

$$\boxed{H \triangleleft G}$$

From this definition we may observe that:

$$H \triangleleft G \Leftrightarrow xHx^{-1} \subseteq H, \forall x \in G$$

(another definition)

Eg: $(H = \{1, -1\}, \times)$ is a normal subgroup of $(G = \{1, -1, i, -i\}, \times)$ because for every $x \in G$ and $h \in H$

$$xhx^{-1} \Rightarrow xx^{-1}h \quad (\because G \text{ is commutative})$$
$$= eh = h \in H.$$

Proper and Improper Normal Sub-groups:

It can be observed that every group G has atleast following two normal sub-groups.

i) G itself
ii) $\{e\}$, the group consisting of the identity alone.

These two sub-groups are called IMPROPER NORMAL SUBGROUPS of G and a sub-group other than these is called a PROPER NORMAL SUBGROUP.

Scanned with CamScanner

SIMPLE GROUPS : Definition

A group which has no proper normal sub-groups is called as simple group.

eg: Every group of prime order is simple because such a group has no proper sub-group.

HAMILTONIAN GROUP : Definition

If all the subgroups of a non-abelian group are normal, then its called Hamiltonian group.

#NOTE: The normal sub-group is also called a special sub-group or invariant sub-group or self conjugate sub-group.

THEOREMS :

1) Every sub-group of an abelian group is a normal subgroup.

Let H be a sub-group of an abelian group G.

If $x \in G$ and $h \in H$ then,

$$x * h * x^{-1} \Rightarrow h * x * x^{-1} \quad [\because G \text{ is commutative}]$$
$$\Rightarrow h * (x * x^{-1})$$
$$\Rightarrow h * e = h \in H$$

Thus, $x \in G, h \in H \Rightarrow x * h * x^{-1} \in H$

$\therefore$ H is a normal sub-group of G.

Every sub-group of a cyclic group is a normal sub-group.

Scanned with CamScanner

POPU

2) A sub-group H of group G is a normal sub-group iff $a^{-1} * h * a \in H$ for every $a \in G$ and $h \in H$.

Let $H \triangleleft G$,

$a \in G$, $h \in H$ and $H \triangleleft G$,

$aH = Ha$

$h * a = a * h$

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

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

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

$\therefore a^{-1} * h * a \in H$

Now premultiply by a,

$a * a^{-1} * h * a \in a * H$

$e * h * a \in a * h$

$h * a \in a * h$

$H * a \in a * H$

$Ha \subseteq aH$ —— (1)

Now, $a \in G$, $a^{-1} \in G$

$\Rightarrow b = a^{-1} \in G$

so, $b^{-1} * h * b \in H$

$(a^{-1})^{-1} * h * a^{-1} \in H$

$a * h * a^{-1} \in H$

$a * h * a^{-1} * a \in H * a$

$a * h * e \in H * a$

$a * H \subset H * a$

$aH \subseteq Ha$ —— (2)

From (1) and (2)

$aH = Ha$

Scanned with CamScanner

3) A sub-group H of a group G is a normal sub-group iff each left coset H is right coset of H (and vice-versa)

$H \lhd G \Leftrightarrow xH = Hx \quad \forall x \in G$

Proof: Let $H \lhd G$ then,

~~xHx^{-1}~~

$x * h * x^{-1} \in H, \quad h \in H$

$x * h * x^{-1} * x \in H * x$

$x * h * e \in H * x$

$x * h \in H * x$

$xH \subset Hx$

$xHx^{-1} = H \quad \forall x \in G$

$(xHx^{-1})x = Hx$

$(xH)(x^{-1}x) = Hx$

$xH = Hx \quad \forall x \in G$

Conversely, if $xH = Hx \quad \forall x \in G$,

$xH = Hx$

$xHx^{-1} = Hxx^{-1}$

$xHx^{-1} = He = H$

$H \lhd G$

$\therefore H \lhd G \Leftrightarrow xH = Hx, \forall x \in G$

4) Show that intersection of two normal sub-groups of a group G is also a normal sub-group of a.

$a \in G$ and $h \in H_1 \cap H_2$

$\therefore a \in G$ and $h \in H_1, \; h \in H_2$

$\therefore a^{-1} * h * a \in H_1, \; a^{-1} * h * a \in H_2$

Scanned with CamScanner

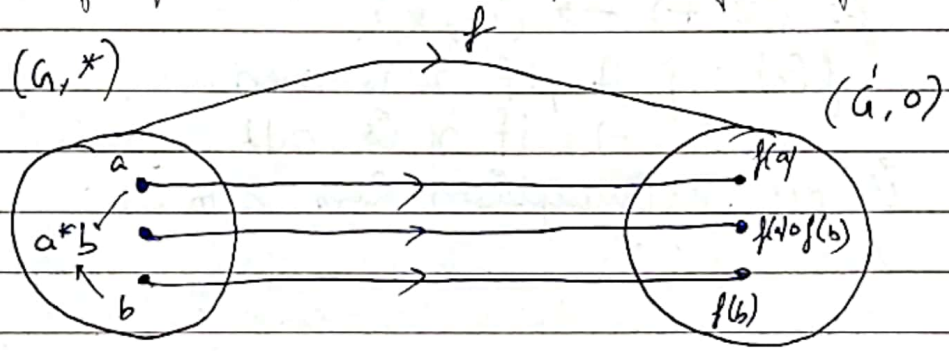
$\therefore a^{-1} * h * a \in H_1 \cap H_2$

HOMOMORPHISM: Definition

A mapping f from groups $(G, *)$ to a group (G', o) is called a group homo-morphism (or group morphism) from G to G' if:

$$\boxed{f(a * b) = f(a) \circ f(b)} \quad \forall\ a, b \in G$$

Thus if f is a morphism from G to G', then it preserves the composition in both groups G & G' i.e image of composite = composite of images



Eg: Let $(R, +)$ be the additive group of real numbers & $(R_0, \times)$ be the multiplicative group of non-zero real numbers. The mapping $f: (R, +) \to (R_0, \times) : f(x) = 2^x$ $\forall\ x \in R$ is homomorphism of R into R_0, because for any $x_1, x_2 \in R$

$$f(x_1 + x_2) = 2^{x_1 + 2x_2}$$
$$= 2^{x_1} 2^{x_2} = f(x_1) f(x_2)$$

$\therefore$ Homomorphism is defined b/w ~~R & R_0~~ $(R, +) \to (R_0, \times)$

Scanned with CamScanner

Various Morphisms:

A ~~map~~ morphism f of a group G into G' is called

i) Monomorphism, if f is injection (one one)

ii) Epimorphism, if f is surjection (onto)

Here G' is called the homomorphic image of group G.

Q1) Let $G = \{1, -1\}$ we a multiplicative group. Then the map →

$f: (Z, +) \to (G, \times)$

$$f(x) = \begin{cases} 1, & \text{if } x \text{ is even} \\ -1, & \text{if } x \text{ is odd} \end{cases}$$

is an epimorphism from Z to G.

Let $x_1, x_2 \in Z$

i) When x_1, x_2 both are even:

$f(x_1 + x_2) = 1 = 1 \cdot 1 = f(x_1) \cdot f(x_2)$

ii) When x_1, x_2 both are odd:

$f(x_1 + x_2) = 1 = (-1)(-1) = f(x_1) \cdot f(x_2)$

iii) When x_1 is odd, x_2 is even:

$f(x_1 + x_2) = -1 = (-1) \cdot 1 = f(x_1) \cdot f(x_2)$

iv) When x_1 is even, x_2 is odd:

$f(x_1 + x_2) = -1 = (1) \cdot (-1) = f(x_1) \cdot f(x_2)$

Thus $f(x_1 + x_2) = f(x_1) \cdot f(x_2) \ \forall \ x_1, x_2 \in Z$

$\therefore f(Z) = G \Rightarrow f$ is onto

Hence f is an epimorphism from Z to G.

Scanned with CamScanner

Theorem 5

1) If f is a homo-morphism from a group G to G' and if e and e' be their respective identities, then:

a) $f(e) = e'$

b) $f(a^{-1}) = [f(a)]^{-1}$

a) Let $a \in G$, then $a * e = a = e * a$

$f(a * e) = f(a) = f(e * a)$

$f(a) \Delta f(e) = f(a) = f(e) \Delta f(a)$ [$\because f$ is homomorphism]

From this we can say,

$f(e)$ is identity in $G' \Rightarrow f(e) = e'$

Therefore, the image of the identity of G under the group morphism f is the identity of G'

b) Let a^{-1} be inverse of $a \in G$, then,

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

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

$f(a) \Delta f(a^{-1}) = e' = f(a^{-1}) \Delta f(a)$ [$\because f(e) = e'$]

$f(a) \Delta f(a^{-1}) \Delta [f(a^{-1})]^{-1} = e' \Delta [f(a^{-1})]^{-1}$

$f(a) \Delta e' = [f(a^{-1})]^{-1}$

$$f(a) = [f(a^{-1})]^{-1}$$

$\therefore$ The f-image of the inverse of any element of G under f is the inverse of f-image of a in G'.

Scanned with CamScanner

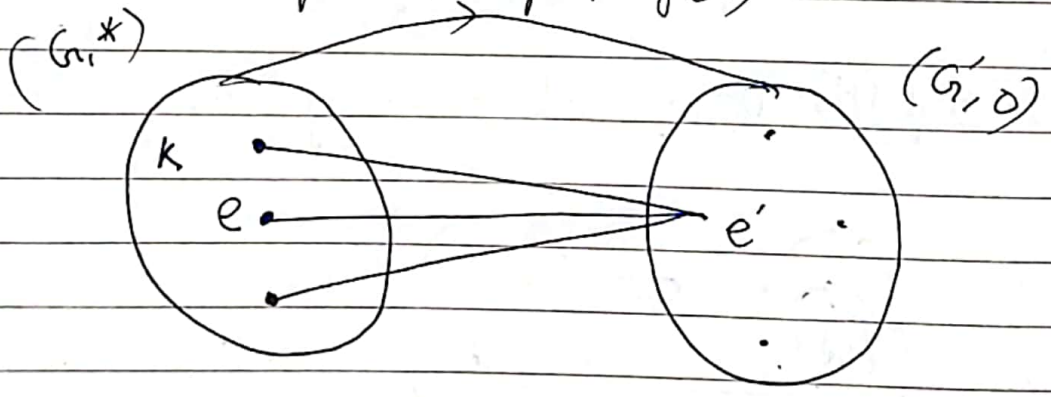
KERNEL OF HOMOMORPHISM

Let f be a homomorphism of group G into G', then the set K of all those elements of G which are mapped to the identity e' of G' is called the kernel of the homomorphism f.

It is denoted by $\ker f$ or $\ker(f)$

$$\ker f = \{ x \in G \mid f(x) = e' \}$$

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



Ex 1: The mapping $f : (C_0, \times) \to (R_0, \times)$, $f(z) = |z| \ \forall z \in C_0$ is a homomorphism of C_0 to R_0 because for,

$z_1, z_2 \in C_0$

$$f(z_1 z_2) = |z_1 z_2|$$
$$= |z_1| \, |z_2|$$
$$= f(z_1) \cdot f(z_2)$$

Again $\ker(f) = \{ z \in C_0 \mid f(z) = 1 \}$

Scanned with CamScanner

$= \{ z \in C_0 \mid |z| = 1 \}$

Ex 2: $f: R_0 \to R_0$, $f(x) = x^4$, $x \in R_0$ is a homomorphism on R_0 because for any $x_1, x_2 \in R_0$

$$f(x_1, x_2) = (x_1 x_2)^4$$
$$= x_1^4 \cdot x_2^4$$
$$= f(x_1) \cdot f(x_2)$$

$$\ker(f) = \{ x \in R_0 \mid f(x) = 1 \}$$
$$x^4 = 1$$
$$x^4 - 1 = 0$$
$$(x^2 - 1)(x^2 + 1) = 0$$
$$x = 1, -1, \cancel{x^2 = -1}$$
$$x = \pm 1$$
$$\ker(f) = \{ x \in R_0 \mid x^4 = 1 \}$$
$$= \{ 1, -1 \}$$

Ex 3: The mapping $f: (R, +) \to (C_0, \cdot)$, $f(x) = e^{ix} \forall x \in R$ is a homomorphism from R to C_0 because for $x_1, x_2 \in R$

$$f(x_1 + x_2) = e^{i(x_1 + x_2)}$$
$$= e^{ix_1} \cdot e^{ix_2}$$
$$= f(x_1) \cdot f(x_2)$$

Again, $\ker(f) = \{ x \in R : f(x) = 1 \}$
$$= \{ x \in R : e^{ix} = 1 \}$$
$$= \{ x \in R : \cos x + i \sin x = 1 \}$$
$$= \{ 2m\pi : m \in Z \}$$
$$= \{ 0, \pm 2\pi, \pm 4\pi \ldots \}$$

Scanned with CamScanner

Ex 4: If $f: (C, +) \to (R, +)$, $f(x+iy) = x$, then f is a homomorphism from C to R because for any $(x_1 + iy_1), (x_2 + iy_2) \in C$

$$f[(x_1+iy_1) + (x_2+iy_2)] = f[(x_1+x_2) + i(y_1+y_2)]$$

$$\Rightarrow x_1 + x_2$$
$$= f(x_1+iy_1) + f(x_2+iy_2)$$

Again $\text{Ker}(f) = \{(x+iy) \in C \mid f(x+iy) = 0\}$
$= \{(x+iy) \in C \mid x = 0\}$
= The set of imaginary numbers

Theorem :-

The kernel of homomorphism f from group $(G, *) \to (G', \Delta)$ is a subgroup of $(G, *)$

Assuming that $a, b \in \text{Ker}(f)$
and $f(a) = e'$
$f(b) = e'$
By definition of homomorphism,
$f(a * b^{-1}) = f(a) \Delta f(b^{-1})$
$= f(a) \Delta [f(b)]^{-1}$
$= e' \Delta (e')^{-1}$
$= e'$
$f(a * b^{-1}) = e'$
$\therefore a * b^{-1} \in \text{Ker}(f)$

Ker(f) is a sub-group of $\{G, *\}$

Scanned with CamScanner

ISOMORPHISM :→

A morphism f of a group $(G, *)$ to a group $(G', \circ)$ is an isomorphism if,

i) f is one-one
i.e $f(a) = f(b) \Rightarrow a = b \quad \forall\ a, b \in G$

ii) f is onto i.e. $f(G) = G'$

iii) f is morphism i.e $f(a*b) = f(a) \circ f(b)$
$\forall\ a, b \in G$

From the above definition it is clear that a group morphism is an isomorphism if f is bijection.

Isomorphic groups : Definition →
A group is said to be isomorphic to a group G', if there exists an isomorphism of G onto G'.

Symbolically we write it as $G \cong G'$

Eg A: For every group G, the identity mapping I_o defined by $I_o : G \to G'$, $I_o(x) = x \quad \forall\ x \in G$ is an isomorphism of G onto itself because I_o is clearly one-one & onto & $a, b \in G$.

$$I_o(a*b) = ab = I_o(a) \circ I_o(b)$$

Eg B: The map $f : (Z, +) \to (2Z, +)$, $f(x) = 2x \quad \forall\ x \in Z$ is an isomorphism from Z to $2Z$, because for any

Scanned with CamScanner

$x_1, x_2 \in \mathbb{Z}$

i) $f(x_1+x_2) = 2(x_1+x_2)$
$= 2x_1 + 2x_2$
$= f(x_1) + f(x_2)$

$\therefore f$ is homomorphism

ii) $f(x_1) = f(x_2)$
$2x_1 = 2x_2$
$x_1 = x_2$
$\therefore f$ is one-one

iii) $f(\mathbb{Z}) = 2\mathbb{Z}$
Every image has its unique preimage
$\therefore f$ is onto.
Hence, $\mathbb{Z} \cong 2\mathbb{Z}$

Eg: The map $f: (R', \times) \to (R, +)$, $f(x) = \log x \ \forall x \in R'$ to R is an homomorphism for $x_1, x_2 \in R'$

i) $f(x_1 x_2) = \log(x_1 x_2)$
$= \log x_1 + \log x_2$
$= f(x_1) + f(x_2)$

ii) $f(x_1) = f(x_2)$
$\log x_1 = \log x_2$
$x_1 = x_2$

iii) $f(R') = R$
Hence $R' \cong R$

Scanned with CamScanner

Q1) If m is a fixed integer then show that the following mapping f is an isomorphism from $\mathbb{Z}$ to $m\mathbb{Z}$

$f: (\mathbb{Z}, +) \to (m\mathbb{Z}, +)$, $f(x) = mx \quad \forall x \in \mathbb{Z}$

For any $x_1, x_2 \in \mathbb{Z}$,

$f(x_1) = f(x_2)$

$mx_1 = mx_2$

$x_1 = x_2$

$\therefore f$ is one-one

and for any $mx \in m\mathbb{Z}$ there exists $x \in \mathbb{Z}$ such that,

$f(x) = mx$

$\therefore f$ is onto

Again, $f(x_1 + x_2) = m(x_1 + x_2)$

$= mx_1 + mx_2$

$= f(x_1) + f(x_2)$

$\therefore f$ is homomorphism

Thus we see that f is homomorphism from group $\mathbb{Z}$ onto $m\mathbb{Z}$ which is bijective

Consequently, $\mathbb{Z} \cong m\mathbb{Z}$

Q2) Show that the additive group $(R, +)$ of real numbers is isomorphic to the multiplication group $(R', \times)$ of the real numbers.

$(R, +) \cong (R', \times)$

Consider the mapping f from the group $(R, +)$ to group $(R', \times)$ defined as,

$f: R \to R'$, $f(x) = e^x$, $x \in R$

i) We know that for any $x_1, x_2 \in R$

Scanned with CamScanner

$x_1 \neq x_2 \Rightarrow e^{x_1} \neq e^{x_2} \Rightarrow f(x_1) \neq f(x_2)$
f is one-one.

and for every $x \in R'$, there exist $\log x \in R$, such that,

$$f(\log x) = e^{\log x} = x$$

$\therefore f$ is onto.

Again, $f(x_1 + x_2) = e^{x_1 + x_2}$
$= e^{x_1} \cdot e^{x_2}$
$= f(x_1) \cdot f(x_2)$

$\therefore f$ is homomorphism from the group $(R, +)$ to the group $(R', \times)$ which is bijection
Hence, f is isomorphism

Q3) Prove that the following groups are iso-morphic groups:

a) $(\{1, -1\}, \times)$ and $(\{0, 1\}, +_2)$
b) $(\{0, 1, 2, 3\}, +_4)$ and $(\{1, 2, 3, 4\}, \times_5)$

a) Let $G = \{1, -1\}$ and $G' = \{0, 1\}$
(The identity element of G will be mapped to identity element of G')

Define a map f from G to G' as,
$f(1) = 0$, $f(-1) = 1$
Clearly f is bijection
The composition table of both the groups G and G' are as follows

Scanned with CamScanner

G

X	1	-1
1	1	-1
-1	-1	1

G'

$+_2$	0	1
0	0	1
1	1	0

- In table II if we replace 0 by 1 and 1 by -1, then the two tables become identical. This shows that f preserves composition and is a bijection. Therefore f is isomorphism.
Hence $G \cong G'$.

b) Let $G = \{0, 1, 2, 3\}$ and $G' = \{1, 2, 3, 4\}$
Define a map from G to G' as,
$f(0) = 1$, $f(1) = 2$, $f(2) = 3$, $f(3) = 4$
Clearly f is bijection. The composition of both the groups are

G

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

G'

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	3	1
3	4	3	1	2
4	3	1	2	4

Replacing 1, 2, 3, 4 by 0, 1, 2, 3 resp. the two tables becomes identical.
This shows that f preserves composition and is a bijection. Therefore f is isomorphism.
Hence $G \cong G'$.

Scanned with CamScanner

Q9) Find the permutation group isomorphic to the group $(\{1,-1,i,-i\}, \times)$.

Let $G = \{1, -1, i, -i\}$. Define a map for $a \in G$ as $f_a : G \to G$, $f_a(x) = ax \ \forall \ x \in G$

Then we shall have,

$$f_1 = \begin{pmatrix} 1 & -1 & i & -i \\ 1\cdot 1 & -1\cdot 1 & i\cdot 1 & -i\cdot 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{pmatrix}$$

$$f_{-1} = \begin{pmatrix} 1 & -1 & i & -i \\ 1\cdot(-1) & (-1)(-1) & i(-1) & -i(-1) \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{pmatrix}$$

$$f_i = \begin{pmatrix} 1 & -1 & i & -i \\ 1\cdot i & -1\cdot i & i\cdot i & -i\cdot i \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ i & -i & -1 & 1 \end{pmatrix}$$

$$f_{-i} = \begin{pmatrix} 1 & -1 & i & -i \\ -i\cdot 1 & -i\cdot(-1) & i\cdot(-i) & -i\cdot -i \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{pmatrix}$$

Hence by Cayley's theorem the permutation group isophomic to G is

$$G' = \{f_1, f_{(-1)}, f_i, f_{-i}\}$$

It can be easily seen that the corresponding isophomism ϕ is defined as,

$$\phi(x) = f_x, \ \forall \ x \in G.$$

Scanned with CamScanner

POPU

SOME RESULTS OF ORDER OF AN ELENT:

1) If $O(a) = n$, then $a^{mn} = e$ where $m \in Z$

2) If $O(a) = n$ then $O(a^{-1}) = n$

In: $(\{1, -1, i, -i\} \times) = G$

$O(i) = 4$, $O(-i) = 4$

3) If $a \in G$ then $O(a) \mid O(G)$

In G, $O(G) = 4$

$O(i) = 4$

$\checkmark$ $4 \mid 4$

4) If $a^m = e$, $m \in Z$, then $O(a) \mid m$

Suppose $i^8 = 1$. But $O(i) = 4$ (smallest integer)

$4 \mid 8$. $\checkmark$

5) If $a^m = e$, $m \in Z$, then $O(a) \leq m$

and $O(a) \mid m$

If, $i^{16} = 1$ $m = 16$

$O(i) = 4$

So, $4 < 16$, and 4 divides 16

6) If $O(a) = n$, $k(m, n) = 1$ (GCD) then $O(a^m) = n$

Eg: $i^4 = 1$, $O(i) = 4$

GCD of 4, 3 $= 1$

So order of i^3 is also 4.

Eg: $(Z_6, +6) = \{0, 1, 2, 3, 4, 5\}$

Identity $= 0$

$O(0) = 1$ $O(1) = 6$ $O(2) = 3$

$O(3) = 2$ $O(4) = 3$ $O(5) = 6$.

All posible orders for a group & no of elements that have it :—

Scanned with CamScanner

~~positive~~

Possible order of elements	Number of elements having that order.
1	$\phi(1) = 1$
2	$\phi(2) = 1$
3	$\phi(3) = 2$
6	$\phi(6) = 2$

Theorems Isomorphism:

1) A homomorphism f defined from a group G onto G' is an isomorphism iff $\text{Ker}(f) = \{e\}$

o Suppose f is an isomorphism of G onto G' & K is the kernel of f. If $a \in G$, then

$a \in K \Rightarrow f(a) = e'$ where e' is the identity of G'

$\Rightarrow f(a) = f(e)$ $[\because f(e) = e']$

$\Rightarrow a = e$ $[\because f$ is one-one$]$

This shows that K contains only the identity e i.e., $\therefore K = \{e\}$

~~Let $a, b \in G$ then,~~

~~$f(a) = f(b) \Rightarrow$~~

Conversely: Suppose that $K = \{e\}$

Let $a, b \in G$, then

$f(a) = f(b) \Rightarrow f(a)[f(b)]^{-1} \Rightarrow f(b)[f(b)]^{-1}$

$\Rightarrow f(a)f(b^{-1}) = e' = f(ab^{-1}) = e'$

Scanned with CamScanner

$\Rightarrow ab^{-1} \in K$

$\Rightarrow ab^{-1} = e$

$\Rightarrow a = b$

$\therefore f$ is bijective homomorphism

Hence it is an isomorphism

2) The relation of isomorphism '$\cong$' in the set of all groups is an equivalence relation.

i) Reflexive: For any group G, the identity mapping I_G (onto itself) defined by $I_G(x) = x$ is an isomorphism because I_G is a bijection, and for any $a, b \in G$, $I_G(ab) = ab = I_G(a) I_G(b)$

$G \cong G$

$\Rightarrow$ relation is reflexive

ii) Symmetric: Let G and G' be two groups such that $G \cong G'$ and let f be corresponding isomorphism. Since by definition f is a bijection so its inverse $f^{-1}: G' \to G$ exists and it is also bijection. Further if $a, b \in G$ and $a', b' \in G'$ such that

$f(a) = a'$ and $f(b) = b'$ then

$a = f^{-1}(a')$ and $b = f^{-1}(b')$ ——— (1)

$f^{-1}(a'b') = f^{-1}[f(a) f(b)]$ by (1)

$= f^{-1}[f(ab)]$ [$\because f$ is isomorphism]

$= ab$

$= f^{-1}(a') f^{-1}(b')$

Therefore f^{-1} is isomorphism from G' onto G

Hence $G' \cong G$

Scanned with CamScanner

$G \cong G' \Rightarrow G' \cong G$

Therefore relation $\cong$ is Symmetric

iii) Transitive : Let G, G' and G'' be three groups such that $G \cong G'$ and $G' \cong G''$.
Also let f and g be their respective isomorphism.
Since by definition f and g are bijections, so $gof : G \to G''$ also bijection.
gof is a homomorphism of G to G''.

Hence gof is an isomorphism from G to G''
$G \cong G''$

Therefore the relation $\cong$ is transitive.
From the above discussion, the relation of isomorphism $\cong$ is an equivalence relation.

CAYLEY'S THEOREM :

Every group is isomorphic to some permutation group $G \cong P_A$.
Let G be a group. Corresponding to every a in G we define a map f_a as follows :-

$f_a(x) = ax, \quad x \in G$

$a \in G, x \in G \Rightarrow ax \in G$

$f_a : G \to G$

Further for any $x, y \in G$

$f_a(x) = f_a(y) \Rightarrow ax = ay$

$x = y$ [$\because$ by cancellation law in G]

$\therefore f$ is one-one

and for every $x \in G$, there exists $a^{-1}x \in G$ such that $f_a(a^{-1}x) = a(a^{-1}x) \Rightarrow (aa^{-1})x = x$

Scanned with CamScanner

$\therefore f_a$ is onto

As such f_a is a one-one mapping of G onto G itself.

Hence f_a is a permutation of G.

Let $G' = \{f_a \mid a \in G\}$

Clearly $G' \subset S_G$ ($S_G \rightarrow$ of all permutations of G)

Let us now consider the mapping the mapping f from G to S_G, defined by,

$$\phi : G \to S_G, \quad \phi(x) = f_x \quad \forall x \in G$$

Now for any $x, y \in G$

$$\phi(x*y) = f_{xy} = f_x f_y = f(x) f(y)$$

$\therefore \phi$ is a ~~consequently~~ homomorphism from a group G onto S_G.

Consequently $f(G) = G'$ is a subgroup of the permutation group S_G and ϕ is an epimorphism from G onto G'.

Also for any $a, b \in G$

$$\phi(a) = \phi(b) \Rightarrow f_a = f_b$$
$$\Rightarrow f_a(x) = f_b(x), \quad x \in G$$
$$ax = bx \Rightarrow a = b$$

$\therefore \phi$ is one-one

Hence ϕ is an isomorphism from a group G onto permutation group G'.

Consequently $G \cong G'$.

4) ★ Every infinite cyclic group is isomorphic to the additive group of integers $(Z, +)$

Scanned with CamScanner

Let $G = [a]$ be a infinite cyclic group generated by a.

First we show that no two distinct integral powers of a can be equal.

For if possible, let $a^i = a^j$, where $i, j \in Z$, $i \neq j$

then $a^i = a^j \Rightarrow$

$$a^{i-j} = a^0 = e$$

$i - j \neq 0$

$i \neq j$

$O(a)$ is finite.

$\Rightarrow$ G is finite which is a contradiction

$G = \{\ldots a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3 \ldots\}$ has a distinct elements.

Consider the mapping f from the group G to the group Z defined as,

$f : G \to Z$, $f(a^n) = n \ \forall\ a^n \in G$

We see that for any $a^m, a^n \in G$

$$a^m = a^n$$

$$m = n$$

$$f(a^m) = f(a^n)$$

f is one-one.

and for any $n \in Z$, there exists a such that

$f(a^n) = n$

f is onto

Again, $f(a^m a^n) = f(a^{m+n}) = m + n = f(a^m) + f(a^n)$

$\therefore$ f is homomorphism from group G to Z

Hence f is an isomorphism of G onto Z which proves that $G \cong Z$

Scanned with CamScanner

Remark: Since the relation of isomorphism is an equivalence relation, so we conclude any to infinite cyclic group are isomorphic to each other. Hence we can say that there exists one & only one infinite cyclic group.

PERMUTATION GROUP

A permutation of a finite set S is a bijection from S to itself.

$$f : S \xrightarrow{1\text{-}1 \text{ onto}} S$$

$\Rightarrow$ if $a \in S$ then $f(a) \in S$

Notation: Let S be a finite set on n elements $S = \{a_1, a_2, a_3, \cdots a_n\}$

The permutation f

$$f = \begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ f(a_1) & f(a_2) & f(a_3) & \cdots & f(a_n) \end{bmatrix}$$

Let $S = \{1, 2, 3, 4\}$ and $f : S \to S$

$f(1) = 2$, $f(2) = 3$, $f(3) = 4$, $f(4) = 1$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Scanned with CamScanner

Equality of two permutation:

Let f and g be two permutations then they are called iff

$f(a) = g(a) \quad \forall\ a \in S$

i.e image of every element of S under both f and g are equal.

Eg: $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$

They are equal

Eg: $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ & $g = \begin{pmatrix} 4 & 2 & 3 & 1 \\ 1 & 4 & 2 & 3 \end{pmatrix}$

Here, $f(1) = 3 = g(1)$

$f(2) = 4 = g(2)$

$f(3) = 2 = g(3)$

$f(4) = 1 = g(4)$

$f(a) = g(a) \quad \forall\ a \in S = \{1, 2, 3, 4\}$

Identity Permutation:

Let set S be finite set of n elements then a permutation f is called identity permutation iff,

$f(a) = a \quad \forall\ a \in S$

Eg:

Let $S = \{a_1, a_2 \cdots a_n\}$

$f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix}$

Scanned with CamScanner

$$I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Product of Composition of Permutation:
Let f and g be permutation of A then product of two permutation is also composition of permutation

$$(f \cdot g)(x) = fog(x) = f[g(x)]$$

Eg:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \& \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

Find $f \cdot g$ and $g \cdot f$

Sol:

i) $(f \cdot g)(x) \; (fog)(x) = f[g(x)]$

$(fog)(1) = f[g(1)] = f(3) = 4 \quad [\because g(1) = 3]$

$(fog)(2) = f[g(2)] = f(4) = 1$

$$f \cdot g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

$$g \cdot f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

$$f \cdot g \neq g \cdot f$$

Scanned with CamScanner

Cyclic Permutation or Cycles:

A permutation σ of a set S is a cycle permutation or a cycle if $\exists$ a finite subset $(a_1, a_2, a_3 \cdots a_n)$ of S such that:

$\sigma(a_1) = a_2$, $\sigma(a_2) = a_3 \cdots \sigma(a_n) = a$

If $\sigma(x) = x$ and $x \in S$

Then $x \notin (a_1, a_2, a_3 \cdots a_n)$

Then we can write cycle permutation σ

$\sigma = (a_1, a_2, a_3 \cdots a_n)$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & & \downarrow & \downarrow \\ 3 & 2 & 4 & 1 \end{pmatrix} \Rightarrow \underset{\text{(cycle)}}{(1\ 3\ 4)}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow\nearrow & \downarrow\nearrow & \downarrow\nearrow & \downarrow \\ 2 & 3 & 4 & 1 \end{pmatrix} \Rightarrow \underset{\text{(cycle)}}{(1\ 2\ 3\ 4)}$$

Eg: $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$ is a permutation

We can write the cycle →

$f(1) = 4$

$f(2) = 1$

$f(3) = 3$

$f(4) = 2$

Then $\sigma = (1\ 4\ 2)$

$3 \neq \sigma = (1\ 4\ 2)$ $[\because f(3) = 3]$

Eg: Let $\sigma = (2\ 4\ 5\ 6) \in S$ be a cycle here then,

$\sigma(2) = 4$, $\sigma(4) = 5$, $\sigma(5) = 6$, $\sigma(6) = 2$

Then,

Scanned with CamScanner

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 5 & 6 & 2 \end{bmatrix}$$

Length of cycle:
No. of elements in a cycle is called length of a cycle

Eg: $\sigma = (1\ 2\ 3\ 4)$ then length of s is 4
If length of cycle is s, then its called s-cycle
Above example is 4-cycle

Eg: $(2\ 4\ 5)$ is 3-cycle
Note: length of identity permutations is 1

like: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

Order of Cycle:→
Let $\sigma(2) = 4$
$\sigma(4) = 5$
$\sigma[\sigma(2)] = 5$
$\Rightarrow \sigma^2(2) = 5$
$\sigma^3(2) = 6 \Rightarrow \sigma(\sigma(\sigma(2))) = 6$
and, $\sigma^4(2) = 2$
i.e $\sigma^4(4) = 4$, $\sigma^4(5) = 5$, $\sigma^4(6) = 6$
$\sigma^4(1) = 1$, $\sigma^4(3) = 3$

$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = I$$

Scanned with CamScanner

$\sigma^4 = I$

$O(\sigma) = 4$

⇒ ∧ length of cycle is order of cycle

Eg: $\sigma = (3\ 4\ 6)$ then $O(\sigma) = 3$

⇒ Inverse of Cycle:

Let $\sigma = (2\ 4\ 3\ 5)$

Then $\sigma^{-1} = (5\ 3\ 4\ 2)$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix}$$

inverse ⇒ $\begin{pmatrix} 1 & 4 & 5 & 3 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{pmatrix}$

⇒ Disjoint Cycle:

Two cycles are said to be disjoint if they have no common elements.

$\sigma_1 = (1\ 2\ 4) \in S_5$

$\sigma_2 = (3\ 5) \in S_5$

They have no elements in common

⇒ σ_1 and σ_2 are disjoint cycle.

⇒ Product of Disjoint cycle:

Let σ_1, σ_2 be disjoint cycle then they have no common elements.

$\sigma_1(x) \neq x \Rightarrow \sigma_2(x) = x$

$\sigma_1\sigma_2(x) = \sigma_1(x)$

and, $\sigma_2(x) = x$ and then $\sigma_1(x) \neq x$

$\sigma_1\sigma_1(x) = \sigma_1(x)$

Scanned with CamScanner

$\Rightarrow \sigma_1\sigma_2(x) = \sigma_2\sigma_1(x)$

$\Rightarrow \sigma_1\sigma_2 = \sigma_2\sigma_1$

∴ Product of two disjoint cycle is commutative.

Eg: $\sigma = (3\ 4\ 6)$ & $\rho = (1\ 2\ 5)$, $\rho \in S_6$

Then $\rho\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 4 & 1 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 6 & 5 & 3 \end{pmatrix}$

$\rho\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 6 & 1 & 3 \end{pmatrix}$

$\sigma\rho = \rho\sigma$

(It is commutative)

NOTE: Every permutation can be expressed as the product of disjoint cycle

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 6 & 3 \end{pmatrix}$

$= (1\ 2)(3\ 4\ 5\ 6)$

Order of permutation:

We know that every permutation can be written as product of disjoint cycle.

Let f be the permutation

Then $O(f)$ = LCM of length of disjoint cycle

Example

$O(\sigma) = LCM(2, 4) = 4$

Scanned with CamScanner

Transposition:

Any cycle of length 2 is called transposition

Eg: $\sigma = (1,2), (a\ b)$ both are transposition

Notes:

i) Order of every transposition is 2.
⇒ Every transposition is self inverse

ii) Every permutation is a product transposition
Let a cycle $(a_1, a_2, a_3 \cdots a_{n-1}, a_n)$
$= (a_1, a_2)(a_1, a_3) \cdots (a_1, a_{n-1})(a_1, a_n)$

Eg:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 2 & 5 & 1 & 3 & 8 & 7 \end{pmatrix}$$

$\sigma = (1\ 4\ 5)(2\ 6\ 3)(7\ 8)$

⇒ Order ⇒ LCM(3,3,2) = 6

$\sigma = (1\ 4)(1\ 5)(2\ 6)(2\ 3)(7\ 8)$

4 (Transposition)

Inversion:

Let σ be a permutation then the pair (i,j), $0 < i < j \leq n$ is an inversion for σ if $\sigma(i) > \sigma(j)$

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$

Here, $1 < 3$ but $f(1) > f(3) \Rightarrow 2 > 1$
$2 < 4$ but $f(2) > f(4) \Rightarrow 4 > 3$

Scanned with CamScanner

$2 < 3$ but $f(2) > f(3) \Rightarrow 4 > 1$

$5 < 6$ but $f(5) > f(6) \Rightarrow 6 > 5$

Then the pair $(1,3), (2,4), (2,3), (5,6)$ are called inversion.

Signature:

The total number of such inversion (pairs) for the permutation σ is called signature & it is denoted by $sig\ \sigma$

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$

$Sig\ \sigma = 5$

EVEN & ODD PERMUTATION

A permutation is called an even (odd) if the total number of transposition are even (odd)

Ex:

Let $\sigma = (1\ 2\ 3\ 4\ 5)$

$\sigma = (1\ 2)(1\ 3)(1\ 4)(1\ 5)$

{4 transposition}

Even transposition $\Rightarrow$ Even permutation

Note:

i) A cycle of length n is called even (odd) if n is odd (even)

Scanned with CamScanner

POPU

Examples:

i) $\sigma = (1\ 2\ 3\ 4\ 5)$

$\sigma = (1\ 2)(1\ 3)(1\ 4)(1\ 5)$

Even number of transposition

ii) 4-cycle is odd permutation

$\sigma = (1\ 2\ 3\ 4)$

$\sigma = (1\ 2)(1\ 3)(1\ 4)$

Odd number of transposition

⇒ Identity permutation is an even permutation

⇒ Every transposition is and odd permutation

PRODUCT OF EVEN (ODD) PERMUTATION)

(a) Product of two even permutation is an even permutation

Ex: $\sigma = (1\ 2\ 3)$ & $\rho = (3\ 4\ 5)$

then $\sigma\rho = (1\ 2\ 3\ 4\ 5)$ is even permutation

(b) Product of two odd permution is an even permutation

Eg: $(1\ 2)(3\ 4) =$

(c) Product of even and odd permutations is odd permutation

$\sigma = (1\ 2\ 3)$ $\rho = (1\ 2\ 3\ 4)$

σ is even & ρ is odd

$\sigma\rho = (1\ 2\ 3)(1\ 2\ 3\ 4) = (1\ 3\ 4\ 2)$

⇒ $\sigma\rho$ is odd permutation

Scanned with CamScanner