Sri SAI RAM ENGINEERING COLLEGE
INSTITUTE OF TECHNOLOGY
West Tambaram, Chennai - 44

SAIRAM DIGITAL RESOURCES

YEAR II SEM III

MA8351

DISCRETE MATHEMATICS

(COMMON TO CSE & IT)

UNIT-IV
ALGEBRAIC STRUCTURES

4.5 COSETS AND LAGRANGE'S THEOREM

SCIENCE & HUMANITIES

COSET AND LAGRANGE'S THEOREM

Let $(H,*)$ be a subgroup of $(G,*)$.

LEFT COSET : $a * H = \{a * h : h \in H\}$ for any $a \in G$ is called the left coset of H in G determined by a.

RIGHT COSET : $H * a = \{h * a : h \in H\}$ for any $a \in G$ is called the right coset of H in G determined by a.

EXAMPLE: Let $(Z_4, +_4)$ be a group and $H = \{0,2\}$ be a subgroup of Z_4.

Let $\boldsymbol{Z_n = \{0, 1, 2, 3, \ldots \ldots . n\}}$ and $Z_4 = \{0,1,2,3\}$

Left coset: $0 + H = \{0,2\} = H$

$1 + H = \{1,3\}$

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

$3 + H = \{3,1\} = 1 + H.$

Distinct Left cosets of Z_4 are H and $1 + H$

NOTE :

(i)If H is a subgroup of G then H itself is both left coset as well as right cosets of G.

(ii) If $a \in H * b$ the $H * a = H * b$.

(iii) If $a \in b * H$ the $a * H = b * H$.

(iv) Union of all Right and Left cosets of H is equal to G.

(v) Since $e \in H, a * e \in aH \Longrightarrow a \in aH$ and $e * a = a \in Ha$

Also $eH = \{e * h/h \in H\} = \{h/h \in H\} = H$

and $He = \{h * e/h \in H\} = \{h/h \in H\} = H$

So, H itself is a left coset as well as right coset.

(vi) In general, $Ha \neq aH$.

But if G is abelian, then $Ha = aH$.

That is every left coset is a right coset.

(vii) If the binary operation of G is denoted by + then the left coset will be written as $a + H = \{a + h/h \in H\}$

THEOREM

Any right or left cosets of H in G are either disjoint or identical.

PROOF:

Let H be a subgroup of a group G.

For any $a, b \in \mathrm{G}$, $\mathrm{a} * \mathrm{H}$ and $\mathrm{b} * \mathrm{H}$ are two left cosets of H.

Suppose $(\mathrm{a} * \mathrm{H}) \cap (\mathrm{b} * \mathrm{H}) \neq \emptyset$, then $x \in (\mathrm{a} * \mathrm{H}) \cap (\mathrm{b} * \mathrm{H})$.

$x \in (\mathrm{a} * \mathrm{H})$ and $x \in (\mathrm{b} * \mathrm{H}) \Longrightarrow x \in a * h_1 \text{ and } x \in b * h_2,$

for some $h_1, h_2 \in H$

$$a * h_1 = b * h_2 = (a * h_1) * h_1^{-1} = (b * h_2) * h_1^{-1}$$

$$\Longrightarrow a * \left(h_1 * h_1^{-1}\right) = b * \left(h_2 * h_1^{-1}\right)$$

$$a * e = b * \left(h_2 * h_1^{-1}\right) \Longrightarrow a = b * \left(h_2 * h_1^{-1}\right)$$

If x is an element in $\mathrm{a} * \mathrm{H}$, then

$$x = a * h = b * \left(h_2 * h_1^{-1}\right) * h = b * \left(h_2 * h_1^{-1} * h\right) \in b * H$$

Therefore, $x \in (\mathrm{a} * \mathrm{H}) \Longrightarrow x \in (\mathrm{b} * \mathrm{H})$

Hence $\mathrm{a} * \mathrm{H} \subseteq \mathrm{b} * \mathrm{H}$. Similarly, we can say that $\mathrm{b} * \mathrm{H} \subseteq \mathrm{a} * \mathrm{H}$

We get $\mathrm{a} * \mathrm{H} = \mathrm{b} * \mathrm{H}$

THEOREM

The set of all left or right cosets of H in G forms the partition of G.

PROOF:

Let us prove that every element of G appears in atleast one left coset.

Let $a * H = \{a * h : h \in H\}$ be a left coset of $H, a \in G$.

For $e \in H \Longrightarrow a * e \in a * H \Longrightarrow a \in a * H$. Therefore, every element of G appears in atleast one left coset. Also, we know that the left coset are either identical or disjoint. Hence each element of G appears in exactly one and only one left coset of H in G.

Since the union of all distinct left cosets of H in G equals G, the set of left cosets form a partition of G.

THEOREM

If $(H,*)$ is a subgroup of a group $(G,*)$ and $H * a$ is any right coset of H in G, then there exist a one-one correspondence between the elements of H and $H * a$.

PROOF:

Define a map $f: H \to H * a$ by $f(h) = h * a$, for any $a \in G$.

For any $h_1, h_2 \in H, f(h_1) = f(h_2) \Longrightarrow h_1 * a = h_2 * a \Longrightarrow h_1 = h_2 \Longrightarrow f$ is one-one. For every $h * a \in H * a$, there exist $h \in H$ such that $f(h) = h * a \Longrightarrow$ f is onto. Therefore there is one-one correspondence between $H \, and \, H * a$.

THEOREM: (LAGRANGE'S THEOREM)

Let G be a finite group of order n. Let H be a subgroup of G. Then order of H divides order of G.

PROOF: Let G be a finite group of order 'n'. Let $(H,*)$ be a subgroup of $(G,*)$ with 'm' distinct elements $H = \{h_1, h_2, \dots \dots . h_m\}$. Let $a \in G$ and $H * a$ is the right coset of H in G. $H * a = \{h_1 * a, h_2 * a, \dots \dots \dots, h_m * a\}$. Since there is one-one correspondence between the elements of H, there are 'm' distinct elements in $H * a$. W.k.t any right coset of H in G are either disjoint or identical. The number of distinct right cosets of H in G is finite(say k). The k distinct right cosets are

$H * a_1, H * a_2, \dots \dots . H * a_k$. The union of these k distinct right cosets of H in G is equal to G. $G = (H * a_1) \cup (H * a_2) \cup \cdots \dots \dots . . \cup (H * a_k)$

$$o(G) = O(H * a_1) + O(H * a_2) + \cdots \dots \dots . + O(H * a_k)$$

$$n = m + m + m + \dots \dots + m \quad (k \text{ times})$$

Since k is an integer, m is the divisor of n. Therefore m divides n . O(H) divides O(G).

THEOREM

If G is a finite group of order n, then $a^n = e$ for any $a \in G$.

PROOF:

Let G be a finite group of order n.

Let $a \in G$ be an element of order m.

Then the order of ‘a’ is same a the order of cyclic group.

By Langrage’s theorem, the order of the subgroup divides the order of G.

Hence m divides n. $n = km$. If ‘m’ is the order of ‘a’ then a^m=e.

Now $a^m = a^{km} = (a^m)^k = e^k = e \Longrightarrow a^n = e$.

THEOREM

The order of any element of a finite group is a divisor of order of the group.

Proof:

Let $a \in G$ and let $O(a) = m$. Then $a^m = e$. Let H be the cyclic subgroup generated by a. Then $H = \{a, a^2, a^3, \ldots\ldots, a^m = e\}. O(H) = m$.

Therefore, $O(a)$ is a divisor of $O(G)$.

THEOREM

Every group of prime order is cyclic.

Proof:

Let $a \neq e$ be any element of G.

$O(a)$ is a divisor of $O(G) = p$, a prime number.

Therefore, $O(a) = 1\ or\ p$.

If $O(a) = 1$, then $a = e$, which is not true.

Hence $O(a) = p \Longrightarrow a^p = e$.

Hence G can be generated by any element of G other than e and is of order p.

The cyclic group generated by $a \neq e$ is the entire G.

G is a cyclic group.