Group Theory 7

08 October 2023 09:21

Lagrange's Theorem :-

If S is a subgroup of G and if $t \in G$, then a right coset of S in G is a subset of G,

$$St = \{st : s \in S\}$$

G be the $(\mathbb{R}, +)$.

$\hookrightarrow$ only subgroup of form $((a,b),+)$ in $\mathbb{R}$ for $a, b \in \mathbb{R}$ is $(\mathbb{R},+)$

G be $(\mathbb{R}^2, +)$.

$(x,y) \in G$, $(x',y') \in G$, $\Rightarrow$ $(x+x', y+y') \in G$

$(x, 0) \in S$, $(x,0) + (t_1, t_2) = (x+t_1, t_2) \in G$

$(t_1, t_2) \in G$

$S = \{(x,0) ; x \in \mathbb{R}\}$

$St = \{(x+t_1, t_2) ; x+t_1 \in \mathbb{R}, t_2 \in \mathbb{R}\}$

Left coset is like, $tS = \{ts \cdot s \in S\}$

Lemma :- If $S \leq G$, then $Sa = Sb$ if and only if $ab^{-1} \in S$ ($aS = bS$ if only if $b^{-1}a \in S$)

Proof :- $Sa = Sb$, $1 \in S$, $a \in Sa$, $b \in Sb$

$a = s_1 b \Rightarrow ab^{-1} = s_1$, $ab^{-1} \in S$

$ab^{-1} \in S$, $ab^{-1} = s_1 \Rightarrow a = s_1 b$

Theorem :- If $S \leq G$ then any two right cosets of G are either identical of disjoint.

Proof :- Sa, Sb be two right cosets.

$x \in Sa \cap Sb$

$s_1, s_2 \in S$

Proof :-

$x \in Sa \cap Sb$

$x = s_1 a = s_2 b$, $s_1, s_2 \in S$

$\Rightarrow s_1 a = s_2 b \Rightarrow s_1 a b^{-1} = s_2 \Rightarrow ab^{-1} = s_2 s_1^{-1} \in S$

$\Rightarrow Sa = Sb$

Theorem :- If $S \leq G$ then the no. of right cosets of G is equal to no. of left cosets of G.

Ans :- $f : L \to R$

$f(Sa) = a^{-1} S$

$Sa = Sb \Leftrightarrow a^{-1}S = b^{-1}S$

Onto & oneone so bijection.

Def :- If $S \leq G$ then index of S in G is denoted by $[G:S]$. which is the number of right cosets (or left cosets) of S in G

Def :- Order of group $|G|$ = number of elements in G

Theorem (Lagrange) :- If G is a finite group and $S \leq G$ then $|S|$ divides $|G|$ and $[G:S] = |G|/|S|$

Proof :- $G = St_1 \cup St_2 \cdots \cup St_n = St_1 \sqcup St_2 \sqcup \cdots \sqcup St_n$

and $|G| = \sum_{i=1}^{n} |St_n| = \sum_{i=1}^{n} |S| = n|S|$

$[G:S] = n|S| / |S| = n$ $\qquad |S| \mid |G|$

• If G is a finite group and $a \in G$, then the order of a divides $|G|$.

Definition:— A group G has exponents n if $x^n = 1 \; \forall x \in G$

•> If p is a prime and $|G| = p$ then G is a cyclic group

For reverse, $a^1, \ldots, a^{p-2}, a^{p-1}, a^p = 1$ $a^{kn} = 1$ when $k, n \in \mathbb{Z}$ & $kn = p$

$(a^k)^n = 1$ $a^k = 1$

•> (Fermat) If p is a prime and a is an integer, then $a^p \equiv a \mod p$

Q> G is a finite group and $K \leq H \leq G$, then,

$$[G:K] = [G:H][H:K]$$

Ans:— $|G|/|K| = \left(|G|/|H|\right)\left(|H|/|K|\right)$

Q> Let $a \in G$ have an order $n = mk$, where $m, k \geq 1$.
Prove that a^k has order m

Ans:— $\text{Ord}(a^k)$ to be s

$a^{ks} = 1 \Rightarrow n \mid ks$

$\frac{n}{\gcd(n,k)} \mid \frac{ks}{\gcd(n,k)} \Rightarrow m \mid s \Rightarrow s = mc$

$\text{Ord}(a^k)$ is m then.

Q> If $a \in G$ has order n and k is an integer with $a^k = 1$, then n divides k. Then $\{k \in \mathbb{Z} : a^k = 1\}$ consists of all multiples of n. Prove it

Ans:— $\text{Ord}(a) = n$ $a^k = 1$, $n \mid k$

Q> If $a \in G$ has finite order and $f: G \to H$ is a homomorphism then the order of $f(a)$ divides the order of a.

Ans:- Ord(a) be m

$a^m = 1 \qquad f(a^m) = f(1) = 1$

$f(a^m) = f(a)^m = f(a) \cdot \quad f(a) = 1$

$Ord(f(a)) \mid m \implies Ord(f(a)) \mid Ord(a)$

Cyclic Groups:-

Lemma:- If G is a cyclic group of order n then $\exists$ a unique subgroup of order d for every dividend of n.

Theorem:- If n is a positive integer, then,

$$n = \sum_{d \mid n} \varphi(d) \qquad \text{-- [}\varphi(\cdot)\text{ is the Euler's totient]}$$

where sum is over all divisors of n $1 \leq d \leq n$

Proof:- a^k is a generator of G if $\gcd(k, |G| = n) = 1$

$G = S_{d_1} \sqcup S_{d_2} \sqcup \cdots \sqcup S_{d_m} \rightarrow S_i$ are cyclic subgroups of G

$G = \{a_{d_{11}}, a_{d_{12}} \cdots\} \sqcup \{a_{d_{21}}, a_{d_{22}} \cdots\} \sqcup \cdots \sqcup \{a_{d_{m1}}, \cdots\}$

If $|S_1| = d \implies |\{a_{11}, a_{12} \cdots\}| = \varphi(d)$

$$n = |G| = \sum_{d \mid n} |\{a_{d1}, a_{d2}, \cdots\}| = \sum_{d \mid n} (\varphi(d))$$

Theorem:-

(i) If F is a field and if G is a finite subgroup of $F^\times$, the multiplicative group of non-zero elements of F, then G is cyclic.

(ii) If F is a finite field, then its multiplicative group $F^\times$ is cyclic.

(ii) If F is a finite field, then
$F^{\times}$ is cyclic.

<u>Theorem</u>:- Let p be a prime and a group G of order p^n is cyclic if and only if it is an abelian group having a unique subgroup of order p.