State and prove Lagrange's theorem

Statement:

As per the statement, the order of the subgroup H divides the order of the group G. This can be represented as: $|G| = |H|$

1) If G is a group with subgroup H, then there is a one to one correspondence between H and any coset of H

2) If G is a group with subgroup H, then the left coset relation, $g_1 \sim g_2$ if and only if $g_1 * H = g_2 * H$ is an equivalence relation

3) Let S be a set and ~ be an equivalence relation on S. If A and B are two equivalence classes with $A \cap B = \emptyset$, then $A = B$.

Proof:
Let H be any subgroup of the order n of a finite group G of order m. Let us consider the cost breakdown of G related to H

Now let us consider each coset of aH comprises n different elements.

let $H = \{h_1, h_2 \ldots h_n\}$ then ah_1, ah_2 ah_n are the n distinct members of aH

suppose $ah_i = ah_j \Rightarrow h_i = h_j$ be the cancellation law of G.

Since G is a finite group, the number of discrete left coset will also be finite. says P. So, the total number of elements of all cosets is np which is equal to the total number of elements of G

Hence, $m = np$

$p = m/n$

This shows that n, the order of H, is a divisor of m, the order of the finite group G.

we also see that the index p is also a divisor of the order of group

Hence, proved $|G| = |H|$.

let $a = \{1, 2, 3, 5, 6, 15, 30\}$. show that divides is a partial ordering A and draws the hasse diagram

$A = \{1, 2, 3, 5, 6, 15, 30\}$

$[A, 1]$ is POSET

$A = \{ (1,1)\ (1,2)\ (1,3)\ (1,5)\ (1,6)\ (1,15)\ (1,30)$

$(2,2)\ (2,6)\ (2,30)$

$(3,3)\ (3,6)\ (3,5)\ (3,30)$

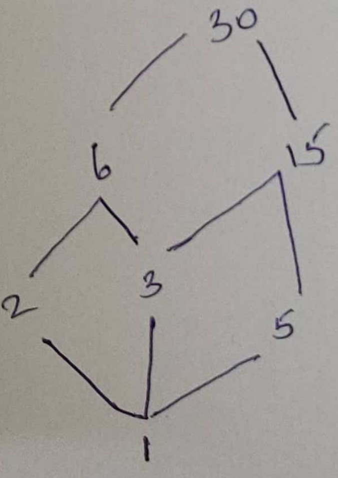
$(5,5)\ (5,3)\ (5,30)$

$(6,6)\ (6,30)$

$(15,15)\ (15,30)$

$(30,30) \}$

Hasse diagram.



∴ The Hasse diagram of a finet poset S is different graph whose vertices are the elements of S & there is a edge from a to b ∴ $a << b$ in S.

3) i) obtain PDNF of

$P \vee (\sim P \wedge \sim Q \wedge R)$

P	Q	R	$\sim P$	$\sim Q$	$\sim P \wedge \sim Q$	$\sim P \wedge \sim Q \wedge R$	$P \vee (\sim P \wedge \sim Q \wedge R)$
T	T	T	F	F	F	F	T
T	T	F	F	F	F	F	T
T	F	T	F	T	F	F	T
T	F	F	F	T	F	F	T
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	T	T	T	T
F	F	F	T	T	T	F	F

PDNF = sum of minterms.

$= (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \sim R) \vee (P \wedge \sim Q \wedge R) \vee (P \wedge \sim Q \wedge \sim R) \vee (\sim P \wedge \sim Q \wedge R)$ //

---

3) ii) obtain PCNF of $(\sim P \to R) \wedge (Q \to P)$

By conditional law

$(\sim(\sim P) \vee R) \wedge (\sim Q \vee P)$

$(P \vee R) \wedge (\sim Q \vee P)$

By identity law

$((P \vee R) \vee F) \wedge ((\sim Q \vee P) \vee F)$

$((P \vee R) \vee (Q \wedge \sim Q)) \wedge ((\sim Q \vee P) \vee (R \wedge \sim R))$

$(P \vee Q \vee R) \wedge (P \vee \sim Q \vee R) \wedge (P \vee \sim Q \vee R) \wedge (P \vee \sim Q \vee \sim R)$

$= (P \vee Q \vee R) \wedge (P \vee \sim Q \vee R) \wedge (P \vee \sim Q \vee \sim R)$ is required PCNF //

4) prove that subgroup of a cyclic group is cyclic

To prove:

Every subgroup of a cyclic group is cyclic

Cyclic group:

It is a group generated by a single element, and the element is called a generator of that cyclic group.

or a cyclic group G is one which every element is a power of a particular element g, in the group That is every element of G can be written as g^n for some integer n for a multiplicative group or ng for some integer n for an additive group. So g is a generator of group G.

Proof:

let us suppose that G is cyclic group generated by

$G = \{a\}$

If another group H is equal to G or $H = \{a\}$, then obviously H is cyclic.

So let H be a proper subgroup of G.

Therefore, the elements of H will be the integral powers of a.

If $a^s \in H$, then the inverse of a^s i.e

$a^{-s} \in H$

Therefore, H contains elements that are positive as well as negative integral powers of a.

Now, let m be the least positive integer such that

$a^m \in H$

Then we shall prove that:

$H = \{a^m\}$

H is cyclic and is generated by a^m. Let a^t be any arbitrary element of H. By division algorithm, there exists integers q and r, such that:

$t = mq + r, \quad 0 \leq r \leq m$

Now,

$a^m \in H$

$\Rightarrow (a^m)^q \in H$

$= a^{mq} \in H$

$= (a^{mq})^{-1} \in H$

$= a^{-mq} \in H$

Also,

$a^t \in H$

$a^{-mq} \in H$

$= a^t a^{-mq} \in H$

$= a^{t-mq} \in H$

$= a^r \in H$ (since, $r = t - mq$)

Now m is least positive integer, such that

$a^m \in H$, $0 \le r < m$.

$\therefore$ r must be equal to 0.

$t = mq$

$\therefore a^t = a^{mq} = (a^m)^q$

Hence, every element $a^t \in H$ is of the form $(a^m)^q$.

$\therefore$ H is cyclic and a^m is generate of H.

Hence, it is proved that every subgroup (in this case H) of a cyclic group (G) is cyclic.