Assignment-2

Soostik Bandi
CSE-A' Roll-175007

1) Prove that the order of a permutation on a finite set is the LCM of the lengths of its disjoint cycles.

Let p be a permutation on the finite set $S = \{1,2,3 \cdots n\}$. We further assume that p can be expressed as a product of m disjoint cycles $f_1, f_2 \cdots f_m$ of lengths $r_1, r_2 \cdots r_m$, so that

$$p = f_1 f_2 \cdots f_m$$

Since multiplication of disjoint cycles is commutative, we have for a positive integer n

$$p^n = f_1^n f_2^n \cdots f_m^n$$

Now we know that if I be the identity permutation then

$$f_1^{r_1} = f_2^{r_2} = \cdots = f_m^{r_m} = I.$$

Let s be the common multiple of $r_1, r_2 \cdots r_m$.

Then we have $p^s = f_1^s f_2^s \cdots f_m^s = I$.

Obviously the least positive integer r for which $p^r = I$ holds must be the least value of s

$\Rightarrow s$ is the lcm of $r_1, r_2 \cdots r_m$.

Hence order of p is the LCM of the lengths $r_1, r_2 \cdots r_m$

2) Prove that number of even permutations on a finite set (contains atleast 2 elements) is equal to the number of odd permutations on it.

Sol:- Let $S = \{a_1, a_2 \dots a_n\}$, $n \geq 2$. Let A be the set of all even permutations and B be the set of all odd permutations. Then both A and B are non empty, because the identity permutation i belongs to A and the transposition (a_1, a_2) belongs to B.

Let t be the transposition (a_1, a_2). Let us define a mapping $\phi : A \to B$ by $\phi(f) = tf$, $f \in A$. Since $f \in A$, f is even and therefore tf is odd and $tf \in B$.

Let $f_1, f_2 \in A$. $tf_1 = tf_2 \Rightarrow t^{-1}(tf_1) = t^{-1}(tf_2)$

$\Rightarrow f_1 = f_2$

$\therefore f_1 \neq f_2 \Rightarrow tf_1 \neq tf_2$

This proves that ϕ is injective.

Let g be an element in B. Then tg being even, belongs to A and $\phi(tg) = t(tg) = t^2 g = g$ $\because t^2 = i$.

This shows that tg is the pre image of g under mapping ϕ since ϕ is surjective.

Therefore ϕ is a bijection and since A & B are finite sets, they have equal number of elements. (proved).

8) Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 7 & 5 & 2 & 3 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 6 & 7 & 3 & 5 & 2 \end{pmatrix}$ be elements of S_7.

i) Write α as a product of disjoint cycles.

ii) Write β as a product of 2 cycles.

iii) Is β an even permutation?

iv) Is α^{-1} an even permutation?

i) Here $\alpha = (1\,6\,3\,7)(2\,4\,5)$

$\Rightarrow \alpha$ is a product of two disjoint cycles.

ii) $\beta = (2\,4\,7)(3\,6\,5) = (2\,7)(2\,4)(3\,5)(3\,6)$

iii) From (ii) we get β is an even permutation.

iv) From the given permutation α, we may calculate α^{-1} as follows:

α:	and α^{-1}:
$1 \to 6$	$1 \to 7$
$2 \to 4$	$2 \to 5$
$3 \to 7$	$3 \to 6$
$4 \to 5$	$4 \to 2$
$5 \to 2$	$5 \to 4$
$6 \to 3$	$6 \to 1$
$7 \to 1$	$7 \to 3$

Hence $\alpha^{-1} = (1\,7\,3\,6)(2\,5\,4)$

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

We see that α^{-1} is a product of odd number of two cycles. Hence α^{-1} is not an even permutation.

4) Let H, K be subgroups of a group G. Then HK is a subgroup of G if and only if $HK = KH$.

Let HK be a subgroup of G.

Let x be an element of HK. Since HK is a subgroup, $x^{-1} \in HK$. Let $x^{-1} = h_1 k_1$ then $x = k_1^{-1} h_1^{-1} \in KH$

Thus $x \in HK \Rightarrow x \in KH$. Therefore $HK \subset KH$ ... (i)

Let $k_2 h_2 \in KH$. Then $k_2 \in K$, $h_2 \in H$ and $h_2^{-1} k_2^{-1} \in HK$, since $h_2^{-1} \in H$, $k_2^{-1} \in K$.

Since HK is a subgroup $(h_2^{-1} k_2^{-1})^{-1} \in HK$ or $k_2 h_2 \in HK$.

Therefore $KH \subset HK$ ... (ii)

$\because$ HK is a subgroup, $(h_2^{-1}k_2^{-1})^{-1} \in HK$ or $k_2h_2 \in HK$

Therefore $KH \subset HK$ ... (ii)

From (i) & (ii), $HK = KH$.

Conversely, let $HK = KH$

Let $p \in HK$, $q \in HK$ & $p = h_3k_3$ $q = h_4k_4$ say,

Then $pq = (h_3k_3)(h_4k_4)$

$= h_3(k_3h_4)k_4 = h_3(h_4k_3)k_4$ (as $KH = HK$)

$= (h_3h_4)(k_3k_4) \in HK$

$\Rightarrow pq \in HK$ ... (iii)

Also $p^{-1} = (h_3k_3)^{-1} = k_3^{-1}h_3^{-1} \in KH = HK$.

Therefore $p \in HK \Rightarrow p^{-1} \in HK$. ... (iv)

From (iii) & (iv), HK is a subgroup.

5) Show that $Z(G) = \{x \in G : xg = gx \ \forall g \in G\}$ is a subgroup of G.

Let $x, y \in Z(G)$. Then $xg = gx$ and $yg = gy$

Now $yg = gy \Rightarrow y^{-1}(yg)y^{-1} = y^{-1}(gy)y^{-1}$

$\Rightarrow gy^{-1} = y^{-1}g$ ... (1)

Hence $y^{-1} \in Z(G)$.

Again $(xy^{-1})g = x(y^{-1}g) = x(gy^{-1})$ by (1),

$= (xg)y^{-1} = (gx)y^{-1} = g(xy^{-1})$

Hence $xy^{-1} \in Z(G)$, since $x, y \in Z(G)$

$\therefore$ $Z(G)$ is a subgroup of G.

Let G be a group and $a \in G$. Prove that $C(a) = \{x \in G : xa = ax\}$ is a subgroup of G.

Let $x, y \in C(a)$. Then $xa = ax$ and $ay = ya$.

Now $ya = ay \Rightarrow y^{-1}(ya)y^{-1} = y^{-1}(ay)y^{-1}$

$\Rightarrow ay^{-1} = y^{-1}a$.

Hence $y^{-1} \in C(a)$.

Again $(xy)a = x(y^{-1}a)$

$= x(ay^{-1})$ ~~$= (xy^{-1})a$~~.

$= (xa)y^{-1}$

$= (ax)y^{-1} = a(xy^{-1})$

Hence $xy^{-1} \in C(a)$, since $x, y \in C(a)$.

$\therefore$ $C(a)$ is a subgroup of G.

7. Prove that a cyclic group of finite order n has a subgroup of order d for every positive divisor d of n.

For $d=1$ and $d=n$, the theorem is obvious.

Let $1 < d < n$. Then $dk = n$ for some positive integer k.

Let $G = \langle a \rangle$. Then $o(a) = n$.

We have to show that cyclic subgroup $\langle a^k \rangle$ is a subgroup of order d.

Let $b = a^k$.

Then $b^d = a^{kd} = a^n = e$.

Let $o(b) = m$. Then m is a divisor of d ... (i)

Also $b^m = e \Rightarrow a^{km} = e$.

$\Rightarrow n$ is a divisor of km

$\Rightarrow kd$ is a divisor of km

$\Rightarrow d$ is a divisor of m. ... (ii)

From (i) & (ii) we get $d = m$.

Therefore order of the cyclic subgroup generated a^k is

let there be another subgroup $\langle a^r \rangle$ of order d.
Then $a^{rd} = e$. Since $o(a) = n$ and $a^{rd} = e$, n is a divisor of rd.

$\therefore rd = nk' = dkk'$ where k' is a positive integer.

We have $r = kk'$ & $a^r \in \langle a^k \rangle$

Since $o(a^r) = d$ & a^r is an element of the cyclic group $\langle a^k \rangle$ of order d, a^r is also a generator of $\langle a^k \rangle$.

$\Rightarrow \langle a^r \rangle = \langle a^k \rangle$

8. Prove that $(Q, +)$ is a non cyclic group.

let us consider that $(Q, +)$ is a cyclic group. let it be generated by a, a non zero element of Q.

Since a is a generator of additive cyclic group $(Q, +)$ thus every element can be expressed as ma where m is an integer.

But $\frac{1}{2}a$, $\frac{1}{3}a$.. belongs to Q and these cannot be expressed as ma for some m belongs to integer.

Therefore a is not a generator and $(Q, +)$ is not cyclic.

9. Prove that the intersection of any collection of subgroups of a group G is a subgroup of G.

Soln: $H \cap K$ is a non empty subset of G since e belongs to all of the subgroups of G, e being the identity element.

let $a, b \in H_1 \cap H_2 \cap \dots \cap H_n$. Then $a, b \in H_1$, $a, b \in H_2 \dots ab \in H_n$

$\because$ H_1 is a subgroup, $a, b \in H_1 \Rightarrow a \circ b^{-1} \in H_1$
H_2 is a subgroup, $a, b \in H_2 \Rightarrow a \circ b^{-1} \in H_2$
$\vdots$
H_n is a subgroup, $a, b \in H_n \Rightarrow a \circ b^{-1} \in H_n$

Therefore $a \in H_1 \cap H_2 \cap H_3 \cap \dots H_m$, $b \in H_1 \cap H_2 \cap H_3 \dots \cap H_m \Rightarrow$
$a * b^{-1} \in H \cap H_2 \dots \cap H_m$. Therefore it proves that $H_1 \cap H_2 \dots \cap H_m$ is a subgroup of $(G, *)$

10) Let $G = \langle a \rangle$ be cyclic group of order n. Prove that

i) If H is a subgroup of G then $|H|$ divides $|G|$.

ii) If m is a positive integer such that m divides n, then there exists an unique subgroup of order m.

Sol^n: i) Given group G is generated by generator a.

As H is a subgroup of G, so it can be generated by a^k where k is an integer.

Let the order of the subgroup be m.

$\therefore a^{km} = e$ ... (1)

Also for group G, $a^n = e$ [considering the order of G to be n]. ... (2)

From (1) and (2) we get that m is a divisor of n.

$\therefore$ If H is a subgroup of G then $|H|$ divides $|G|$.

ii) Let there be another subgroup $\langle a^r \rangle$ of order m. Then $a^{rm} = e$

Since $O(a) = n$ & $a^{rm} = e$, n is a divisor of rm.

$\therefore rm = nk' = kmk'$ where k' is a +ve integer.

$\therefore r = kk'$ & $a^r \in \langle a^k \rangle$

$\because O(a^r) = m$ by hypothesis & a^r is an element of the cyclic group $\langle a^k \rangle$ of order m, a^r is also a generator of $\langle a^k \rangle$.

In other words we can say $\langle a^r \rangle = \langle a^k \rangle$

$\Rightarrow$ There exists unique subgroup of order m.

12) Let G be a group and H be a subgroup of G. Let $a, b \in G$. Then $aH = bH$ if and only if $a^{-1}b \in H$.

Sol^{n}: Let $aH = bH$. Then $ah_1 = bh_2$ for some h_1, h_2 in H.

$\therefore ah_1 = bh_2 \Rightarrow h_1 = a^{-1}bh_2$

$\Rightarrow h_1h_2^{-1} = a^{-1}bh_2h_2^{-1}$

$\Rightarrow a^{-1}b = h_1h_2^{-1} \in H$ as H is a subgroup.

(proved)

Conversely,

let $a^{-1}b = h_3$ for some $h_3 \in H$.

$\therefore b = ah_3 \Rightarrow b \in aH$ but b belongs to bH.

$\therefore$ Two left cosets bH & aH have an element b in common.

We know that any two left (or right) cosets are either disjoint or identical.

$\because$ Then have atleast one element b in common already thus from the above proposition we get

$aH = bH$ (proved).

13) Prove that any two left cosets of GH in a group G have the same cardinality.

Sol^{n}: let aH and bH be two distinct left cosets of H in G.

Define $f: aH \to bH$ s.t $f(ah) = bh$, $\forall h \in H$.

let $h_1, h_2 \in H$ s.t.

$f(ah_1) = f(ah_2)$

i.e. $bh_1 = bh_2 \Rightarrow h_1 = h_2$ (LCL in G)

$\Rightarrow ah_1 = ah_2$ $\because ah_1 \neq ah_2 \Rightarrow f(ah_1) \neq f(ah_2)$

$\therefore f$ is injective

let $bh_3 \in bH$. Then as per the definition of f

$f(ah_3) = bh_3$

where $ah_3 \in aH$. Since f is surjective.

$\therefore f$ is ~~surj~~ ~~surjective~~ bijective from aH onto bH.

$\therefore |aH| = |bH|$.

Prove that the order of each element in a finite group G is a divisor of $o(G)$.

Sol^{n}: Let G be a finite group and $a \in G$.
Let there be a cyclic group generated by a.
Now this cyclic group is also a subgroup of G.
∴ By Lagrange's theorem we get that
$o(\langle a \rangle)$ is a divisor of $o(G)$.
But we know that $o(\langle a \rangle) = o(a)$.
$\Rightarrow o(a)$ is a divisor of $o(G)$ (proved)

15) Let G be a finite group and $a \in G$. Prove that $a^{o(G)} = e$. Hence prove Fermat's Little Theorem.

Sol^{n}: Let G be a finite group and $a \in G$.
From previous proof we get $o(a)$ is a divisor of $o(G)$.
Let $o(a) = m$
$\Rightarrow a^m = e$.
∵ m is a divisor of $o(G)$ thus
$mK = o(G)$ where K is a +ve integer.
$\Rightarrow m = \frac{o(G)}{K}$.

$\therefore a^{\frac{o(G)}{K}} = e$
$\Rightarrow \left(a^{\frac{o(G)}{K}}\right)^K = e^K = e$
$\Rightarrow a^{o(G)} = e$. (proved).

Let a be one of $1, 2 \ldots p-1$. Let us consider the group $(\mathbb{Z}_p - \{\bar{0}\}, \cdot)$. This being of order $p-1$ & $\bar{a}$ being an element of the group $o(\bar{a})$ is a divisor of $p-1$.
$(\bar{a})^{p-1} = \bar{1}$, $\bar{1}$ being the identity element.
$\Rightarrow a^{p-1} = 1 \pmod{p}$ (proved).

16) Prove that every group of order less than 6 is commutative.

Sol^{n}: A group of 1 contains the identity element only. Thus it is a cyclic group generated by e. Therefore its commutative.

A group of order 2 is cyclic, since 2 is prime.
∴ It is cyclic hence commutative.

Ily for group of order 3, 3 is is prime, thus cyclic
⇒ It is commutative.

Let us consider a group G of order 4. The order of every element of G is a divisor of O(G). The divisors of 4 are 1, 2 & 4.

Case-1

If there exists an element of order 4 in G, the group is cyclic hence commutative.

Case-2

If there exist no element of order 4, each non identity element would have order 2.

$$\therefore a \circ a = e \Rightarrow a = a^{-1}, \text{ \& } b = b^{-1}$$

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

$$\Rightarrow a \circ b = b^{-1} \circ a^{-1}$$

$$\Rightarrow a \circ b = b \circ a.$$

∴ It follows group of order 4 is commutative.

Also group of order 5 is cyclic hence commutative.

⇒ Every group of order less than 6 is commutative (proved)

Prove that $Z(G)$ is a normal subgroup of G.

We know $Z(G) = \{x \in G,\ xg = gx \text{ for all } g \in G\}$

Let $H = Z(G)$ & let $a \in G$.

We have to show $aH = Ha$.

Let $p \in aH$

Then $p = ah_1$ for some $h_1 \in H$.

$= h_1 a$ since $h_1 \in Z(G)$.

$\therefore p \in Ha \Rightarrow p \in aH$ & therefore $aH \subset Ha$ ...(1)

Let $q \in Ha$

Then $q = h_2 a$ for some $h_2 \in H$.

$= a h_2$ since $h_2 \in Z(G)$

$\therefore q \in aHa \Rightarrow q \in aH$ & therefore $Ha \subset aH$ ...(2)

From (1) and (2) we get

$aH = Ha$ & this holds for all values of $a \in G$. (proved)

19) Let H be a subgroup of a group G such that $[G:H] = 2$. Then prove that H is a normal subgroup of G.

Sol^n: Since $[G:H] = 2$ there are exactly two distinct left cosets which are H and $G - H$. Also there are exactly 2 distinct right cosets which are H & $G - H$.

Let $a \in H$. Then $aH = H$ & also $Ha = H$

$\Rightarrow aH = Ha$.

Let $a \in G - H$. Then $aH = G - H$ & also $Ha = G - H$

for left coset ↵ ↳ for right coset.

$\therefore aH = Ha$.

$\Rightarrow aH = Ha$ for all $a \in G$.

$\therefore H$ is a normal subgroup of G.

(8) Let H and K be finite subgroups of a group G. Then prove that $|HK| = \frac{|H||K|}{|H \cap K|}$

Soln:

We know

$HK = \{hk,\ h \in H, k \in K\}$

When no two products are equal then

$h_1k_1 \neq h_2k_2$

$\Rightarrow h_1^{-1}h_1k_1 \neq h_2h_1^{-1}h_2k_2$

$\Rightarrow k_1 \neq h_1^{-1}h_2k_2$

$\Rightarrow k_1k_2^{-1} \neq h_1^{-1}h_2$

Now $h_1^{-1}h_2 \in H$ as H is a subgroup.

also $k_1k_2^{-1} \in K$ as K is a subgroup.

$\therefore |HK| = |H||K|$ —(2)

Now if elements are common then,

$h_1k_1 = h_2k_2$

$\Rightarrow k_1k_2^{-1} = h_1^{-1}h_2$ ...(1)

Since H & K are subgroups

$h_1^{-1}h_2$ & $k_1k_2^{-1}$ belongs to H & K ~~simultaneously~~ respectively.

& from (1) we see that $k_1k_2^{-1} \in H \cap K$. —(3)

$\therefore$ Combining (2) & (3) we get,

$|HK| = \frac{|H||K|}{|H \cap K|}$ (proved)