PROBLEMS ON GROUP THEORY – I.

①. Prove that if G is an abelian group, then $(a \circ b)^n = a^n \circ b^n$; $\forall\, a, b \in G$ and $\forall\, n \in \mathbb{Z}$.

We first prove the result that holds for +ve integers by the mathematical induction.

For $n=1$, we have $(a \circ b)^1 = a^1 \circ b^1$. So it is valid for $n=1$.

Let us suppose that the result holds for $n = K-1$, i.e. $(a \circ b)^{K-1} = a^{K-1} \circ b^{K-1}$.

Now
$$\begin{aligned}(a \circ b)^K &= (a \circ b)^{K-1} \circ (a \circ b) = (a^{K-1} \circ b^{K-1}) \circ (b \circ a).\\ &= a^{K-1} \circ (b^{K-1} \circ b) \circ a = (a^{K-1} \circ b^K) \circ a\\ &= a \circ (a^{K-1} \circ b^K), \text{ as } G \text{ is abelian}\\ &= (a \circ a^{K-1}) \circ b^K = a^K \circ b^K\end{aligned}$$

So the result holds for $n=K$ also.

$\therefore$ the result holds $\forall\, n \in \mathbb{N}$.

Next, we prove the result holds for $n=0$.

For $n=0$, $(a \circ b)^0 = e = e \circ e = a^0 \circ b^0$. So it is valid for $n=0$.

Next, let us suppose that n is a negative integer.

So $n = -m$, m being some +ve integer.

We have
$$\begin{aligned}(a \circ b)^n &= (a \circ b)^{-m} = ((a \circ b)^{-1})^m = (b^{-1} \circ a^{-1})^m\\ &= (a^{-1} \circ b^{-1})^m = (a^{-1})^m \circ (b^{-1})^m, \left[\text{since } m \in \mathbb{Z}^+\right]\\ &= a^{-m} \circ b^{-m}\\ &= a^n \circ b^n\end{aligned}$$

So the result holds for negative integers too.

Hence the result that $(a \circ b)^n = a^n \circ b^n$ holds in an abelian group $\forall\, n \in \mathbb{Z}$.

②. If G is a group such that $(a \circ b)^2 = a^2 \circ b^2$; $\forall\, a, b \in G$, show that G must be abelian.

We have $(a \circ b)^2 = a^2 \circ b^2 \Rightarrow (a \circ b) \circ (a \circ b) = (a \circ a) \circ (b \circ b)$

$\Rightarrow a \circ ((b \circ a) \circ b) = a \circ ((a \circ b) \circ b) \Rightarrow (b \circ a) \circ b = (a \circ b) \circ b$

$\Rightarrow b \circ a = a \circ b$; since $a^{-1}, b^{-1} \in G$. Also by Cancellation laws.

③. If G is a group in which $(a \circ b)^i = a^i \circ b^i$ for three consecutive integers i for all $a, b \in G$, show that G is abelian.

Let $n, n+1, n+2$ be some three consecutive integers. Therefore we have

$$(a \circ b)^n = a^n \circ b^n \longrightarrow ①$$

$$(a \circ b)^{n+1} = a^{n+1} \circ b^{n+1} \longrightarrow ②$$

$$(a \circ b)^{n+2} = a^{n+2} \circ b^{n+2} \longrightarrow ③$$

Using ② we have

$$(a \circ b)^{n+1} = a^{n+1} \circ b^{n+1}$$

$$\Rightarrow (a \circ b)^n \circ (a \circ b) = a^{n+1} \circ (b^n \circ b)$$

$$\Rightarrow ((a^n \circ b^n) \circ a) \circ b = (a^{n+1} \circ b^n) \circ b \quad [\text{using ①}]$$

$$\Rightarrow (a^n \circ b^n) \circ a = a^{n+1} \circ b^n \quad [\text{by cancellation law}].$$

$$\Rightarrow a^n \circ (b^n \circ a) = a^n \circ (a \circ b^n)$$

$$\Rightarrow b^n \circ a = a \circ b^n \quad [\text{by cancellation law}].$$

$\longrightarrow ④$

Again using ③, analogously we have

$$b^{n+1} \circ a = a \circ b^{n+1} \quad [\text{using ②}]$$

$$\Rightarrow b \circ (b^n \circ a) = a \circ b^{n+1}$$

$$\Rightarrow b \circ (a \circ b^n) = (a \circ b) \circ b^n \quad [\text{using ④}]$$

$$\Rightarrow (b \circ a) \circ b^n = (a \circ b) \circ b^n$$

$$\Rightarrow b \circ a = a \circ b \quad [\text{by cancellation law}]$$

So we have $a \circ b = b \circ a \ \forall a, b \in G$.

Hence G is abelian.

④. If G is a finite group, show that there exists a +ve integer N such that $a^N = e$, $\forall\, a \in G$.

Since G is finite, we assume $G = \{g_1, g_2, \cdots, g_m\}$ for some +ve integer m.

For some $g_K \in G$, let us consider the sequence $g_K, g_K^2, g_K^3, \cdots$. Since G is finite and closed under binary operation, there must exist some +ve integers i and j with $i > j$ such that

$$g_K^i = g_K^j \Rightarrow g_K^{i-j} = e \Rightarrow g_K^{n_K} = e, \text{ where } i-j = n_K.$$

Thus, we have n_K corresponding to every g_K s.t.

$$g_K^{n_K} = e.$$

Let $N = n_1 \times n_2 \times \cdots \times n_m$. Then $g_K^N = g_K^{(n_1 \times n_2 \times \cdots \times n_K \times \cdots \times n_m)}$

$$\Rightarrow g_K^N = \left(g_K^{n_K}\right)^{(n_1 \times n_2 \times \cdots \times n_{K-1} \times n_{K+1} \times \cdots \times n_m)}$$

$$= e^{(n_1 \times n_2 \times \cdots \times n_{K-1} \times n_{K+1} \times \cdots \times n_m)} = e$$

i.e., $g_K^N = e$ $\forall\, K$, showing the existence of required +ve integer N.

⑤. Show that the group G must be abelian, if

ⓐ G has 3 elements

ⓑ G has 4 "

ⓒ G has 5 " .

ⓐ Let $O(G) = 3$ and $a, b \in G$ with $a \neq b$.

Case 1. If $a = e$, then $aob = eob = b$, and $boa = boe = b$ $\Rightarrow aob = boa$.

If $b = e$, then $aob = aoe = a$ and $boa = eoa = a$ $\Rightarrow aob = boa$.

So, either $a = e$, or $b = e$, we have $aob = boa$.

Case 2. If $a \neq e$ and $b \neq e$, then considering aob, we have $aob \neq a$, otherwise $\Rightarrow b = e$, not true.

Similarly $a \circ b \neq b$, otherwise $\Rightarrow a = e$, not true.
Since $O(G) = 3$ and $a \neq b \neq e$, then $a \circ b = e$.
A similar argument will show that $b \circ a = e$.
Thus $a \circ b = b \circ a \Rightarrow G$ is abelian for $O(G) = 3$.

(b) Let $O(G) = 4$ and $a, b \in G$.

Case 1. Either $a = e$, or $b = e$. For this case, clearly $a \circ b = b \circ a$ [As shown previously in (a)].

Case 2. If $a \neq e$ and $b \neq e$, then considering $a \circ b$, we have, as before, $a \circ b \neq a$, $a \circ b \neq b$.
Since $O(G) = 4$, let $c \neq e$ be the 4th element.
So either $a \circ b = e$, or $a \circ b = c$.

(i) When $a \circ b = e$, then $a = b^{-1}$
$\Rightarrow b \circ a = b \circ b^{-1} = e$; i.e. $a \circ b = e = b \circ a$.

(ii) When $a \circ b = c$, then clearly, $b \circ a \neq a$, $b \circ a \neq b$.
So either $b \circ a = e$, or $b \circ a = c$.
If $b \circ a = e \Rightarrow b = a^{-1} \Rightarrow a \circ b = a \circ a^{-1} = e$, not true.
Hence $b \circ a = c = a \circ b$

Thus, we have $a \circ b = b \circ a \ \forall a, b \in G$.
Hence G is abelian for $O(G) = 4$.

(c) Let $O(G) = 5$.
Since the order of G is prime, therefore it is cyclic.
And we know that a cyclic group is abelian,
So G must be abelian for $O(G) = 5$.

⑥ If G is a group of even order, prove it has an element $a \neq e$ satisfying $a^2 = e$. [i.e., $O(a) = 2$].

We prove the result by contradiction.
Here G is a finite group.
Let us assume that there is no element x in G satisfying $x^2 = e$ except for $x = e$.
$\therefore$ if some $g (\neq e) \in G$, then $g^2 \neq e \Rightarrow g \neq g^{-1}$.
This means every non-identity element g has another element g^{-1} associated with it.
So the non-identity elements can be paired as $\{g, g^{-1}\}$ into mutually disjoint subsets of order 2; and let n be the number of these subsets.
Then the number of elements of G would be $2n+1$. [1 is added for e].
So G would become a group of odd order, which is a contradiction, as $O(G)$ is even.
Hence there must exist an element $a \neq e$ s.t. $a^2 = e$ for G is a group of even order.

S.K.Mapa Ex-9 (11) ⑦ Let $(G, \circ)$ be a finite abelian group with elements $a_1, a_2, \cdots, a_n$ and $x = a_1 \circ a_2 \circ \cdots \circ a_n$. Show that $x \circ x = e$ [identity element].

Since $a_i \in G$, $a_i^{-1} \in G$ for all $i = 1, 2, \cdots, n$.
Each $a_i^{-1} \in G$ is some $a_i \in G$, which are all n distinct elements of G.
$x \circ x = (a_1 \circ a_2 \circ \cdots \circ a_n) \circ (a_1 \circ a_2 \circ \cdots \circ a_n)$ can form a pair (a_i, a_j) such that $a_i^{-1} = a_j$ or $a_i = a_j^{-1}$.
[Since G is abelian].
$\therefore x \circ x = e \circ e \circ \cdots \circ e = e$. (proved)

Ex-10. (S.K. Mapa)

(3) In a group (G,o), $(aob)^3 = a^3ob^3$, $(aob)^5 = a^5ob^5$; $\forall a,b \in G$. Prove that the group is abelian.

$(aob)^3 = a^3ob^3 \longrightarrow (i)$; $(aob)^5 = a^5ob^5 \longrightarrow (ii)$.

$\Rightarrow (aob)o(aob)o(aob) = ao(a^2ob^2)ob$

$\Rightarrow ao(boa)^2ob = ao(a^2ob^2)ob$ [by associative law]

$\Rightarrow (boa)^2 = a^2ob^2 \longrightarrow (iii)$ [by cancellation laws].

From (ii), we write $(aob)o(aob)^3o(aob) = ao(a^4ob^4)ob$

$\Rightarrow ao[bo(aob)^3oa]ob = ao(a^4ob^4)ob$ [by associative law]

$\Rightarrow bo(a^3ob^3)oa = a^4ob^4$ [by cancellation laws and using (i)]

$\Rightarrow (boa)o(a^2ob^2)o(boa) = a^4ob^4$

$\Rightarrow (boa)o(boa)^2o(boa) = a^4ob^4$ [using (iii)]

$\Rightarrow (boa)^2o(boa)^2 = a^4ob^4$

$\Rightarrow (a^2ob^2)o(a^2ob^2) = a^2o(a^2ob^2)ob^2$ [using (iii)]

$\Rightarrow b^2oa^2 = a^2ob^2$ [by cancellation laws]

$\therefore b^2oa^2 = (boa)^2 \longrightarrow (iv)$ [by (iii)]

$\Rightarrow bo(boa)oa = bo(aob)oa$

$\Rightarrow boa = aob$ [by cancellation laws]

$\therefore$ (G,o) is abelian. (proved)

(5) In a group G, $a^2b^2 = b^2a^2$ and $a^3b^3 = b^3a^3$; $\forall a,b \in G$. Prove that the group is abelian.

$a^2b^2 = b^2a^2 \Rightarrow a^2 = b^2a^2b^{-2} \longrightarrow (1)$, $\forall a,b \in G$

$a^2b^2 = b^2a^2 \Rightarrow b^2 = a^{-2}b^2a^2 \longrightarrow (2)$, $\forall a,b \in G$.

From $a^3b^3 = b^3a^3$, we have

$a^2(ab)b^2 = b^2(ba)a^2$

$\Rightarrow (ab)b^2 = a^{-2}[b^2(ba)]a^2 = b^2(ba)$ [using (2)]

$\Rightarrow ab = b^2(ba)b^{-2} = ba$ [using (1)]

$\therefore$ $ab = ba$

$\Rightarrow$ G is abelian. (proved).

Ex – 10 / S. K. Mapa.

⑥ In a group G, a and b are distinct elements of order 2.
(i) If a and b commute, prove that $O(ab)=2$
(ii) If a and b do not commute, prove that $O(aba^{-1})=2$.
Deduce that a group G cannot contain exactly two elements of order 2.

Solution: (i) $ab=ba$, $O(a)=2 \Rightarrow a^2=e \Rightarrow a=a^{-1}$

$O(b)=2 \Rightarrow b^2=e \Rightarrow b=b^{-1}$

$\therefore ab=ba \Rightarrow ab=b^{-1}a^{-1}=(ab)^{-1}$

$\Rightarrow (ab)^2=e \Rightarrow O(ab)=2$,

Since $ab\neq e$. If $ab=e \Rightarrow a=b^{-1}=b$

not possible, as a & b are distinct.

(ii) $O(a)=2 \Rightarrow a=a^{-1}$; $O(b)=2 \Rightarrow b=b^{-1}$.

$aba^{-1}=ab^{-1}a^{-1}=a(ab)^{-1}=(aba^{-1})^{-1}$

$\Rightarrow (aba^{-1})^2=e \Rightarrow O(aba^{-1})=2$, since

$aba^{-1}\neq e$. If $aba^{-1}=e$, then $ab=a \Rightarrow b=e$

$\Rightarrow O(b)=1$, not possible.

Therefore, G contains the elements ab and aba^{-1} whose orders are 2 except the elements a & b whose orders are 2.

$\Rightarrow G$ cannot contain exactly two elements of order 2.

⑨ Find the number of elements of order 5 in the group $(\mathbb{Z}_{20}, \oplus)$.

Let $O(\bar{m})=5$ where $0<m<20$, in the group $(\mathbb{Z}_{20},\oplus)$

$O(\bar{0})=1$, $O(\bar{1})=20$.

Now $O(\bar{m})=O(m.\bar{1})=\dfrac{O(\bar{1})}{\gcd(m, O(\bar{1}))}=\dfrac{20}{\gcd(m,20)}$.

$\Rightarrow 5=\dfrac{20}{\gcd(m,20)} \Rightarrow \gcd(m,20)=\dfrac{20}{5}=4$

$\Rightarrow \gcd\left(\frac{m}{4},\frac{20}{4}\right)=1 \Rightarrow \gcd\left(\frac{m}{4},5\right)=1$

$\therefore \dfrac{m}{4}=1,2,3,4$.

$\Rightarrow \bar{m}=\bar{4},\bar{8},\overline{12},\overline{16}$.

$\therefore$ The No. of elements of order 5 is 4. (Ans)

(10) Find all elements of order 10 in the group $(Z_{30}, \oplus)$.

Let $o(\bar{m}) = 10$, $0 < m < 30$, in the group $(Z_{30}, \oplus)$.

$o(\bar{0}) = 1$, $o(\bar{1}) = 30$.

$$o(\bar{m}) = o(m.\bar{1}) = \frac{o(\bar{1})}{\gcd(m, o(\bar{1}))} = \frac{30}{\gcd(m,30)}.$$

$$\Rightarrow 10 = \frac{30}{\gcd(m,30)} \Rightarrow \gcd(m,30) = \frac{30}{10} = 3.$$

$$\Rightarrow \gcd\left(\frac{m}{3}, \frac{30}{3}\right) = 1 \Rightarrow \gcd\left(\frac{m}{3}, 10\right) = 1$$

$\Rightarrow \frac{m}{3} = 1, 3, 7, 9 \Rightarrow m = \bar{3}, \bar{9}, \overline{21}, \overline{27}$ are all the elements of order 10 in the group $(Z_{30}, \oplus)$.

(11) If b be an element of a group and $o(b) = 20$, find the order of the element (i) b^6, (ii) b^8, (iii) b^{15}.

(i) $o(b^6) = \frac{o(b)}{\gcd(6, o(b))} = \frac{20}{\gcd(6,20)} = \frac{20}{2} = 10.$

(ii) $o(b^8) = \frac{o(b)}{\gcd(8, o(b))} = \frac{20}{\gcd(8,20)} = \frac{20}{4} = 5.$

(iii) $o(b^{15}) = \frac{o(b)}{\gcd(15, o(b))} = \frac{20}{\gcd(15,20)} = \frac{20}{5} = 4.$

(12) Let (G, o) be a group and $a, b \in G$. If $o(a) = 3$ and $a o b o a^{-1} = b^2$, find $o(b)$ if $b \neq e$.

$a o b o a^{-1} = b^2 \Rightarrow a^2 o b o a^{-2} = a o b^2 o a^{-1} = (a o b o a^{-1}) o (a o b o a^{-1})$
$= b^2 o b^2 = b^4 \longrightarrow$ (i)

$\Rightarrow a^3 o b o a^{-3} = a o b^4 o a^{-1} = (a o b^2 o a^{-1}) o (a o b^2 o a^{-1})$
$= b^4 o b^4 = b^8$ [by (i)]

$\Rightarrow e o b o e^{-1} = b^8$ [$\because o(a) = 3 \Rightarrow a^3 = e, a^{-3} = e^{-1}$]

$\Rightarrow b = b^8 \Rightarrow b o b^{-1} = b^8 o b^{-1}$

$\Rightarrow e = b^7$

$\Rightarrow o(b) \mid 7 \Rightarrow o(b) = 1$ or 7; but $o(b) \neq 1$, as $b \neq e$

$\therefore$ $o(b) = 7$. (Ans)

Ex: Show that a group of order 27 must have a proper subgroup of order 3.

Solution: Let G be a group s.t. $O(G) = 27$.
Let $g (\neq e) \in G$. Then possible orders of g are 3, 9, 27.

If $O(g) = 3$, then $\exists$ a cyclic subgroup
$\langle g \rangle = \{g, g^2, g^3 (=e)\}$ of order 3.

If $O(g) = 9$, then $O(g^3) = \dfrac{O(g)}{\gcd(3,9)} = \dfrac{9}{3} = 3$.
$\therefore$ $\exists$ an element $g^3 \in G$ of order 3 s.t. we get a cyclic subgroup $\langle g^3 \rangle = \{g^3, g^6, g^9 (=e)\}$ of order 3.

If $O(g) = 27$, then $O(g^9) = \dfrac{O(g)}{\gcd(9,27)} = \dfrac{27}{9} = 3$.
$\therefore$ $\exists$ an element $g^9 \in G$ of order 3 s.t. we get a cyclic subgroup $\langle g^9 \rangle = \{g^9, g^{18}, g^{27} (=e)\}$ of order 3.

Hence for a group of order 27 must have a proper subgroup of order 3. (proved)

Ex: Show that a group of order 27 must have a proper subgroup of order 3.

Solution: Let G be a group s.t. $O(G) = 27$.

Let $g (\neq e) \in G$. Then possible orders of g are 3, 9, 27.

If $O(g) = 3$, then $\exists$ a cyclic subgroup $\langle g \rangle = \{g, g^2, g^3 (=e)\}$ of order 3.

If $O(g) = 9$, then $O(g^3) = \dfrac{O(g)}{\gcd(3,9)} = \dfrac{9}{3} = 3$.

$\therefore \exists$ an element $g^3 \in G$ of order 3 s.t. we get a cyclic subgroup $\langle g^3 \rangle = \{g^3, g^6, g^9 (=e)\}$ of order 3.

If $O(g) = 27$, then $O(g^9) = \dfrac{O(g)}{\gcd(9,27)} = \dfrac{27}{9} = 3$.

$\therefore \exists$ an element $g^9 \in G$ of order 3 s.t. we get a cyclic subgroup $\langle g^9 \rangle = \{g^9, g^{18}, g^{27} (=e)\}$ of order 3.

Hence for a group of order 27 must have a proper subgroup of order 3. (proved)