SELECTED PROBLEMS AND SOLUTIONS IN GROUP THEORY

We begin with some results which will not be proved, but will be used to solve the problems.

① If G is a group, then
(i) the identity element of G is unique.
(ii) every element of G has a unique inverse element in G.

② Cancellation Laws: If G is a group, then
(i) $ab = ac \Rightarrow b = c$ (left-cancellation law)
(ii) $ba = ca \Rightarrow b = c$ (right cancellation law)

③ If G is a group, then
(i) for every $a \in G$, $(a^{-1})^{-1} = a$
(ii) for every $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$

④ Let G be a group and $a, b \in G$. Then the equations $ax = b$ and $ya = b$ have unique solutions for x and y in G.

Problem 1: Prove that $(ab)^2 = a^2b^2$ for all $a, b \in G$, iff G is Abelian.

Soln: Let G be Abelian. Then for $a, b \in G$,
consider $(ab)^2 = (ab)(ab) = a(ba)b$
$= a(ab)b = (aa)(bb) = a^2b^2$.

Conversely, suppose for every $a, b \in G$, we have $(ab)^2 = a^2b^2$.
$\Rightarrow (ab)(ab) = (aa)(bb) \Rightarrow a(ba)b = a(ab)b$
Applying Cancellation laws, we get $ba = ab$.
$\therefore G$ is Abelian.

Problem 2: If every element of a group G is its own inverse, then show that G is Abelian.

Soln: Let $a, b \in G$. Then $a^{-1} = a$ $b^{-1} = b$

Clearly $ab \in G$ (closure property)

$\Rightarrow (ab)^{-1} \in G. \Rightarrow b^{-1}a^{-1} \in G$

But it is given that $(ab)^{-1} = ab.$

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

or $ba = ab.$

$\therefore$ G is Abelian.

Problem 3: If G is a group of even order, prove that it has a non-identity element a such that $a^2 = e$ (e is the identity element)

Soln: In a group G, every element has a unique inverse and obviously, e is its own inverse. Since G is has even order, there should be at least one more element $a \neq e$ in G, such that $a = a^{-1}$. Now $a^2 = aa = aa^{-1} = e.$ //

Problem 4: Show that every group of order 4 is Abelian.

Soln: Let $G = \{e, a, b, c\}$ be a group of order 4, with e being the identity element. Since 4 is even, from Problem 3, there must be at least one element, say $a \neq e$, such that

a is the inverse of itself. Now, there are two possibilities:

Case 1: $b^{-1} = b$, $c^{-1} = c$.

Thus in this case, every element of G is its own inverse. Hence from problem 2, G is Abelian. The composition table is as follows:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

[this group is also called Klein-4 group]

Case 2: $b^{-1} = c$, $c^{-1} = b$.

The composition table in such case is as follows:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Obviously, G is Abelian in this case as well.

Hence the result.

Subgroups

A non-empty subset H of a group G is called a subgroup of G if H is itself a group under the binary operation of G.

Lemma 1: A non-empty subset H of a group G is a subgroup of G iff

i) for every $a, b \in H$, $ab \in H$

ii) for every $a \in H$, $a^{-1} \in H$.

Lemma 2: A non-empty subset H of a group G is a subgroup of G iff for every $a, b \in H$, $ab^{-1} \in H$.

Problem 5: If H and K are subgroups of a group G, then show that $H \cap K$ is also a subgroup of G.

Soln: Obviously $H \cap K \neq \phi$. ($\because e \in H \cap K$)

Now, let $a, b \in H \cap K$

$\Rightarrow a, b \in H$ and $a, b \in K$

From Lemma 2,

$ab^{-1} \in H$ and $ab^{-1} \in K$

$\Rightarrow ab^{-1} \in H \cap K$.

Thus, $H \cap K$ is also a subgroup of G.

Problem 6: Show that a group G can not be a union of two proper subgroups of G.

Soln: Let H and K be two proper subgroups of G. Clearly, $H \cup K \subseteq G$.

If $H \subseteq K$, then $H \cup K = K \neq G$.

If $K \subseteq H$, then $H \cup K = H \neq G$.

So, suppose neither $H \subseteq K$ nor $K \subseteq H$.

$\Rightarrow \exists\ a \in H$ s.t. $a \notin K$ and $\exists\ b \in K$ s.t. $b \notin H$.

$\Rightarrow ab \notin H$ and $ab \notin K$. $\Rightarrow ab \notin H \cup K$.

But since $H \subseteq G$ & $K \subseteq G$, $\Rightarrow a, b \in G$

$\Rightarrow ab \in G$.

Thus, $\exists\ ab \in G$ which is not in $H \cup K$.

$\therefore H \cup K \neq G$. //

Cyclic Groups

If a group G contains an element 'a' such that every element of G is of the form a^k, for some integer k, we call, G a cyclic group and a, as its generator. We write $G = (a)$.

A cyclic group may have more than one generators.

If $G = (a)$, then $G = \{a^k / k = 0, \pm 1, \pm 2, \dots\}$.

This does not necessarily mean that a cyclic group need be of infinite order.

There are finite cyclic groups, too.

For ex. $\{1, -1\}$ under multiplication, generated by -1.

$\{1, -1, i, -i\}$ under multiplication, generated by i and also, $-i$.

$Z_5 = \{1, 2, 3, 4\}$ under multiplication modulo 5, generated by 2.

If G is any group and $a \in G$, then the least positive integer 'm' such that $a^m = e$, is called the <u>order of a</u> and is denoted by $o(a)$.

Theorem: If G is a group and $a \in G$, with $o(a) = n$, then the cyclic subgroup $H = (a)$ has order n. If $o(a)$ is infinite, then H also has infinite order.

Problem 7: Show that every cyclic group is Abelian.

Soln: Let $G = (a)$. Consider any two elements $x, y \in G$.
Clearly, $x = a^m$ and $y = a^n$ for some integers m & n.
Now, $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$.
$\therefore$ G is Abelian.

Problem 8: Show that every subgroup of a cyclic group is cyclic.

Soln: Let $G = (a)$, and H be a subgroup of G. If $H = \{e\}$, then obviously, H is cyclic & $H = (e)$.
If $H \neq \{e\}$, since $H \subseteq G$, any element of H is of the form a^k for some integer k.
Let m be the least positive integer such that $a^m \in H$.
Consider any $x \in H$. $\Rightarrow x = a^n$ for some integer n.

By the division algorithm, there exist integers q and r, such that $n = mq + r$, where $0 \le r < m$.

Now, $x = a^n = a^{mq+r} = (a^m)^q a^r$

$\Rightarrow a^r = (a^m)^{-q} a^n$

Since $a^m, a^n \in H$, $\Rightarrow a^r \in H$.

But $r < m$. So, $r = 0$.

$\Rightarrow n = mq \Rightarrow x = (a^m)^q$.

Thus, H is a cyclic group generated by a^m.

Problem 9: Prove that the order of an element a in a group G is the same as of a^{-1}.

Soln: Let $o(a) = m$ $\quad o(a^{-1}) = n$.

Then $a^m = e \rightarrow (1)$

$(a^{-1})^n = e \rightarrow (2)$

WLOG, let $m \le n$. $\longrightarrow (A)$

From (1), $a^m = e \Rightarrow (a^m)^{-1} = e^{-1} = e$

$\Rightarrow n \le m$. $\longrightarrow (B)$

From (A) & (B), we have $m = n$.

Now, if $o(a)$ is infinite, then $o(a^{-1})$ can not be finite, because otherwise $o((a^{-1})^{-1})$ would be finite $\Rightarrow o(a)$ would be finite. $\not\Rightarrow$.

Hence the result.

Problem 10: If G is a group, and $a, x \in G$, show that a and $x^{-1}ax$ have the same order.

Soln: Let $o(a) = m$ & $o(x^{-1}ax) = n$.

Also, let $m \leq n$ (WLOG). $\longrightarrow$ ①

$$(x^{-1}ax)^2 = (x^{-1}ax)(x^{-1}ax) = x^{-1}a(xx^{-1})ax$$
$$= x^{-1}aeax = x^{-1}a^2x.$$

Similarly, $(x^{-1}ax)^m = x^{-1}a^m x$

$$= x^{-1}ex \quad (\because a^m = e)$$
$$= e$$

$\Rightarrow n \leq m$ $\longrightarrow$ ②

From ① & ②, we have $m = n$.

If a is of infinite order, then $o(x^{-1}ax)$ can not be finite, because if $o(x^{-1}ax) = n$, it means $o(a) = n$. ※.

Hence the result.

Problem 11 Let G be a group. If $a \in G$ and $a^n = e$, then prove that $o(a)$ divides n.

Soln Let $o(a) = m$. $\Rightarrow m$ is the least positive integer such that $a^m = e$.

By division algorithm, there exist integers q and r such that $n = qm + r$, and $0 \leq r < m$.

Hence $a^n = a^{qm+r} = (a^m)^q a^r = e^q a^r = a^r$

Since $a^n = e$, $\Rightarrow a^r = e$. But $r < m$.

$\Rightarrow r = 0$. $\Rightarrow n = mq$.

That is, $o(a)$ divides n.

Cosets and Lagrange's Theorem

Let H be a subgroup of a group G.

Let $a \in G$. Then

$aH = \{ah \mid h \in H\}$ is called a left coset of H in G.

$Ha = \{ha \mid h \in H\}$ is called a right coset of H in G.

Since $e \in G$, $eH = He = H$. $\Rightarrow H$ is both a left and a right coset of itself in G.

Also, for any $a \in G$, $a = ae \in aH$ and $a = ea \in Ha$. $\Rightarrow$ every element of G is a member of a left coset of H in G and a member of a right coset of H in G.

If G is Abelian, then there is no distinction between the left and the right cosets of H in G.

Lemma A: Let H be a subgroup of a group G. Then any two left cosets of H in G are either identical or have no elements in common.

Lemma B: Let H be a subgroup of a group G. Then there exists a one-to-one correspondence between any two left cosets of H in G.

Lagrange's Theorem

If G is a finite group and H is a subgroup of G, then $o(H)$ divides $o(G)$.

Problem 12: Show that every group of prime order is cyclic.

Soln: Let $o(G) = p$, where p is a prime. Then G must have at least two elements. Let $a \in G$, where $a \neq e$. Clearly $o(a) \geq 2$. Let $o(a) = m$. Consider the cyclic subgroup $H = (a)$, generated by a. Then $o(H) = o(a) = m$. By Lagrange's Theorem, $o(H)$ divides $o(G)$.

$\Rightarrow$ m divides p. But p is a prime.

Hence $m = p$. $\Rightarrow$ G is cyclic.

[Note: Every non-identity element is a generator of the prime ordered group.]

Problem 13: Give an example of a group G in which every proper subgroup is cyclic; but G is not cyclic.

Soln: Let $G = \{e, a, b, c\}$ be the Klein-4 group (wherein every element is the inverse of itself).

G can not have a proper subgroup of order 3. (Lagrange's Theorem)

So, the only proper subgroups are $\{e\}, \{e, a\}$, $\{e, b\}$ and $\{e, c\}$, and all are cyclic.

But G is not cyclic.

Problem 14: Every group of order upto 5 is Abelian.

Soln: 1, 2, 3 and 5 are prime numbers.

So, every group of these orders are cyclic and hence Abelian. From problem 4, every group of order 4 is Abelian. Hence the result.

Normal Subgroups

A subgroup N of a group G is called a normal (or invariant) subgroup of G if $gng^{-1} \in N$ for every $g \in G$ and $n \in N$.

Lemma: A subgroup N of a group G is a normal subgroup of G iff $gNg^{-1} = N$ for every $g \in G$.

Theorem: A subgroup N of a group G is a normal subgroup of G iff every left coset of N in G is a right coset of N in G.

Theorem: A subgroup N of a group G is a normal subgroup of G iff the product of two left cosets of N in G is again a left-coset of N in G.

Quotient / Factor Groups

Let N be a normal subgroup of a group G. Let G/N denote the collection of all the distinct left cosets of N in G.

G/N forms a group under the product of subsets of G, and we call it the Quotient group or Factor group of G by N.

Further $o(G/N) = \dfrac{o(G)}{o(N)}$.

Problem 15: Show that every subgroup of an Abelian group is normal.

Soln: Let G be an Abelian group and H be a subgroup of G.

Let $g \in G$ and $h \in H$.

$ghg^{-1} = g(hg^{-1}) = g(g^{-1}h) = (gg^{-1})h = h \in H$

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

Problem 16: Show that the intersection of two normal subgroups is normal.

Soln: Let H and K be two normal subgroups of G. Clearly $H \cap K$ is a subgroup of G.

Let $g \in G$ and $x \in H \cap K$.

$\Rightarrow x \in H$ and $x \in K$

$\Rightarrow gxg^{-1} \in H$ and $gxg^{-1} \in K$ ($\because$ H & K are normal)

$\Rightarrow gxg^{-1} \in H \cap K$.

Thus $H \cap K$ is also a normal subgroup of G.

Problem 17: If H is a subgroup of G and N is a normal subgroup of G, then show that $H \cap N$ is a normal subgroup of H.

Soln: Since H and N are subgroups of G, $H \cap N$ is a subgroup of G. Since $H \cap N \subseteq H$, $H \cap N$ is a subgroup of H, too.

Let $h \in H$ and $x \in H \cap N$

$\Rightarrow x \in H$ and $x \in N$

So, $hxh^{-1} \in H$. Also, $hxh^{-1} \in N$ since N is normal in G.

$\therefore hxh^{-1} \in H \cap N$

Thus $H \cap N$ is a normal subgroup of H.

Def: If H is a subgroup of G, then any subset aHa^{-1}, where $a \in G$, is called a conjugate of H in G.

Since $e \in G$, $eHe^{-1} = H$ is a conjugate of itself.

Note: A normal subgroup is a subgroup for which all its conjugates coincide.

Permutation Groups

A one-to-one function from a set S into itself is called a permutation of the set S.

If S has n elements, then there are $n!$ permutations.

These permutations under the function composition forms a group, which we call a Permutation Group. Any subgroup of this permutation group is also called a permutation group.

Def: Let $(G, \circ)$ be a permutation groups of the set $S = \{a, b, c, \dots\}$ of n elements. A binary relation on the set S, called the binary relation induced by $(G, \circ)$, is defined to be such that an element a is related to an element b iff there is a permutation in G that maps a into b.

For ex. (*)

Let $G = \left\{ \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix} \right\}$

The binary relation induced on $S = \{a, b, c, d\}$ by $(G, \circ)$ is as follows:

	a	b	c	d
a	✓	✓		
b	✓	✓		
c			✓	✓
d			✓	✓

Note: The binary relation on S induced by $(G, \circ)$ is an equivalence relation. Therefore this binary relation partitions S into equivalence classes.

Given a small set S, the job is easy. But when S is large, Burnside's Theorem helps.

Burnside's Theorem

The no. of equivalence classes into which a set S is divided by the equivalence relation induced by a permutation group $(G, \circ)$ of S, is given by

$$\frac{1}{o(G)} \sum_{\pi \in G} \psi(\pi)$$

where $\psi(\pi)$ is the no. of elements that are invariant under the permutation π.

In the example (*) above, let

$\pi_1 = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$ $\pi_2 = \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}$ $\pi_3 = \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix}$

$\pi_4 = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$.

$\psi(\pi_1) = 4$ $\psi(\pi_2) = 2$ $\psi(\pi_3) = 2$ $\psi(\pi_4) = 0$.

$\therefore$ No. of equivalence classes $= \frac{1}{4}(4+2+2+0) = 2$

[This is evident in the table above].

Homomorphisms

A mapping f from a group $\langle G, * \rangle$ into a group $\langle G', \divideontimes \rangle$ is called a **homomorphism** if

$$f(a * b) = f(a) \divideontimes f(b) \quad \text{for every } a, b \in G$$

(*) A homomorphism of a group G into itself is sometimes called an **endomorphism**.

(*) A homomorphism of a group G onto a group G' is called an **epimorphism**.

Lemma: If f is a homomorphism of a group G into a group G', then

(1) $f(e) = e'$, identity elt. of G'.

(2) $f(a^{-1}) = [f(a)]^{-1}$ for every $a \in G$.

Theorem: Let f be a homomorphism of a group G into a group G'. If H is a subgroup of G, then $f(H)$ is a subgroup of G'. Further, if K is a subgroup of G', then $f^{-1}(K)$ is subgroup of G.

Remark: Since G is a subgroup of itself, from the above theorem, we can say that every homomorphic image of a group is a group.

Theorem: Let f be a homomorphism of a group G onto a group G'. (i.e., $f(G) = G'$) If N is a normal subgroup of G, then $f(N)$ is a normal subgroup of G'. Further, if M is a normal subgroup of G', then $f^{-1}(M)$ is a normal subgroup of G.

Def: If f is a homomorphism of a group G into a group G', then the **Kernel** of f is the set of all elements in G that are mapped into the identity element of G'.

$\text{Ker } f = \{ a \in G \mid f(a) = e' \}$, e' is the identity elt. of G'.

Lemma: If f is a homomorphism of a group G into a group G', then $\text{Ker } f$ is a normal subgroup of G.

Def: A homomorphism f of a group G into a group G' is called an **isomorphism** if f is one-one. Sometimes, it is also called **monomorphism**. We write $G \cong G'$.

Problem 18: Any infinite cyclic group G is isomorphic to the group $\mathbb{Z}$ of integers under addition.

Soln: Any infinite cyclic group is of the form $G = \langle a \rangle = \{a^n / n \in \mathbb{Z}\}$. Clearly, $a^m \neq a^n$ for $m \neq n$.

Define $f: G \to \mathbb{Z}$ by $f(a^n) = n$ for every $a^n \in G$.

f is clearly one-one and onto.

Also, f is a homomorphism, since for any $a^m, a^n \in G$,

$$f(a^m a^n) = f(a^{m+n}) = m+n = f(a^m) + f(a^n).$$

Hence $G \cong \mathbb{Z}$.

As an immediate consequence, we can say that "Any two infinite cyclic groups are isomorphic to each other".

Attention students:

1. All that is written in black color is notes (with no proofs).
2. All that is written in red color is usually a statement / problem, which has been solved / proved in blue color writing.
3. The exam questions in Group Theory will be similar to the problems that are solved here in this notes. But please don't assume that you will get only some of these problems that have been solved here!

All the best!