Abstract Algebra

[Handwritten Study Material with solved examples]

[For NET, GATE, SET, JAM, NBHM, PSC, MSc, ...etc.]

Group Theory

P. Kalika & K. Munesh
(NET(JRF), GATE, SET)
Email: maths.whisperer@gmail.com

No. of Pages: 250

Ver.: 2021.1-1

Your Remarks/Notes

Content:

Set Theory

Set: A well defined collection of objects.

Eg. (a). Collection of natural no. ≥ 5

$$= \{5, 6, 7, 8, \dots\}$$

Sets are generally denoted by A, B, P, Q.... If 'a' is a member of A then it is denoted by $a \in A$.

Subset: A set B is said to be the subset of A if $b \in B$, then $b \in A$. It is denoted by $B \subseteq A$.
i.e $\forall b \in B \Rightarrow b \in A$

Equal Sets: We say set A and B are equal if $A \subseteq B$ and $B \subseteq A$.

Proper Subset: If $A \subseteq B$, then we say A is proper subset of B if $A \neq B$ (Also denoted as $A \subsetneq B$)

Power Set: If A is any set, then power set of A is denoted by $\mathcal{P}(A)$ and defined by

$$\mathcal{P}(A) = \{B : B \subseteq A\}$$

i.e 'Power set of A' is a collection of all subjects of A.

Cardinality of set: No. of elements in a set A is called 'Cardinality of set A'. It is denoted by $\#A$ or $|A|$ or $Card(A)$.

Theorem (1): $\boxed{\text{If } \#A = n \text{ then } \#\mathcal{P}(A) = 2^n.}$ (UVI)

Proof: Let $A = \{a_1, a_2, \ldots, a_n\}$ & $B = \{b_1, b_2, \ldots b_m\}$

and $B \subseteq A$

Now, for each elt, $a_i \in B$ or $a_i \notin B$

So, we have two independent choice for a_i

so total possibility $= 2 \times 2 \times \cdots \times 2 = 2^n$

So $\#\mathcal{P}(A) = 2 \times 2 \times \cdots \times 2 = 2^n$

Method :- II

If $B \subseteq A$, $\#B \leq \#A = n$

Here, $\#B = 0 \xrightarrow{\text{Possibility}} {}^nC_0$

$\#B = 1 \xrightarrow{\text{Possibility}} {}^nC_1$

$\#B = 2 \xrightarrow{\text{Possibility}} {}^nC_2$

$\vdots$

$\#B = n \xrightarrow{\text{Possibility}} {}^nC_n$

So, total no. of subsets $= {}^nC_0 + {}^nC_1 + \cdots + {}^nC_{n-1} + {}^nC_n = 2^n$

(**Recall:** $(a+b)^n = \sum_{r=0}^{n} {}^nC_r a^r b^{n-r}$, Now put $a = 1 = b$, then

$$(1+1)^n = 2^n = \sum_{r=0}^{n} {}^nC_r$$)

So $\#\mathcal{P}(A) = 2^n$.

Thus, total no. of Proper subset $= 2^n - 1$

* **Difference of sets:** The difference of two set A & B is defined to be the set

$$A - B = \{x \mid x \in A \text{ but } x \notin B\}$$

* ~~let~~ we will use following standard Notation throughout these Notes.

$\mathbb{N}$ or $\mathbb{N}$: set of natural no. $= \{1, 2, 3, 4, \ldots\}$

$\mathbb{W}$ = set of whole no.s $= \{0, 1, 2, 3, \ldots\}$

$\mathbb{Z}$ = set of integers $= \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbb{Q}$ = set of rational no.s $= \{ p/q : p, q \in \mathbb{Z} \text{ \& } q \neq 0 \}$

$\mathbb{R}$ = set of real numbers.

$\mathbb{C}$ = set of complex no.s.

Let $a, b \in \mathbb{R}$ and $x = a + ib$ then $x \in \mathbb{C}$.

- $\mathbb{C}$ $(a+ib,\ a, b \in \mathbb{R})$
  - If $a = 0$ (Imaginary)
  - If $b = 0$ then $\mathbb{R}$
    - $\mathbb{R}$
      - Irrationals Numbers ($\mathbb{Q}^c$)
      - Rational Number ($\mathbb{Q}$)
        - Integer ($\mathbb{Z}$)
          - Positive Integer ($\mathbb{N}$) or ($\mathbb{Z}^+$)
          - $\{0\}$
          - Negative Integer ($\mathbb{Z}^-$)
        - fraction (p/q) ($p \neq kq$ & $q \neq 0$)

$\underbrace{\text{Positive Integer } (\mathbb{N}) \text{ and } \{0\}}$

$\mathbb{N} \cup \{0\} = \mathbb{W} \rightarrow$ whole Number.

Summary

$\mathbb{N} \subseteq \mathbb{W} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Theorem: (2) If A, B, C are sets, then following results hold:

(a). $A \cap A = A$ & $A \cup A = A$

(b). $A \cap \phi = \phi$ & $A \cup \phi = A$

(c). $A \cap B = B \cap A$, $A \cup B = B \cup A$ & $A \cap B \subseteq A \subseteq A \cup B$

(d). $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$

(e). $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(f). $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Theorem: (DeMorgan's Law). Consider set X, Y in S.

ⓐ. $S - (X \cup Y) = (S - X) \cap (S - Y)$

or $(X \cup Y)' = X' \cap Y'$

ⓑ. $S - (X \cap Y) = (S - X) \cup (S - Y)$ or $(X \cap Y)' = X' \cup Y'$

(Note: Interested reader may look proof in any 12^{th}-class book)

Que: If total # proper subsets is 63, then no. of elements in a set is ?

Soln: If $\# A = n$ then $\# \mathcal{P}(A) = 2^n$

& # proper subsets $= 2^n - 1$

$\therefore 2^n - 1 = 63 \Rightarrow 2^n = 64$

$\Rightarrow 2^6 = 64 = 2^n \Rightarrow n = 6$.

Que. Which of the following (w.o.t.f) is/are possible ?

1. $\exists$ a set s.t # proper subsets $= 2k$, $k \in \mathbb{N}$ ✗
2. $\exists$ a set s.t # proper subsets $= 263$ ✗
3. ✓ $\exists$ a set s.t # proper subsets $= 1023$
4. ✓ $\exists$ a set s.t # proper subsets $= 7$
5. ✓ $\exists$ a set s.t # proper subsets is prime.

Sol^n: Recall # proper subsets $= 2^n - 1 = \text{odd}$

(1) $2^n - 1 = 2k \Rightarrow 2^n = 2k+1 = \text{odd} \rightarrow \leftarrow$

as $2^n = 2k$ for some $k \in \mathbb{N}$.

(2). No, Because $2^n - 1 = 263 \Rightarrow 2^n = 264 \rightarrow\leftarrow$

(3). Yes, $2^n - 1 = 1023 \Rightarrow 2^n = 1024 \Rightarrow n = 10$ ✓

(4). Yes, $2^n - 1 = 7 \Rightarrow 2^n = 8 \Rightarrow n = 3$ ✓

(5). Yes, $2^n - 1 = \text{prime} \Rightarrow 2^n = \text{prime} + 1 = \text{even}$, eg $2^n - 1 = 31$

Que. Which of the following (w.o.t.f). is/are possible ?

(a). $\exists$ A s.t $\mathcal{P}(A) = \phi$ ✗

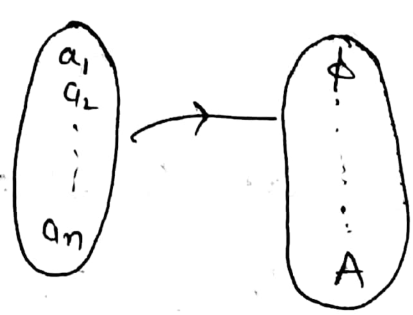
✓ (b). $\exists$ A s.t $\mathcal{P}(A) = \{\phi\}$

✓ (c). $\exists$ A s.t $\mathcal{P}(A) =$ finite

✓ (d). $\exists$ A s.t $\mathcal{P}(A)$ is countable.

✓ (e). $\exists$ A s.t $\mathcal{P}(A)$ is uncountable

$\#A = n$ $\quad$ $\#\mathcal{P}(A) = 2^n$

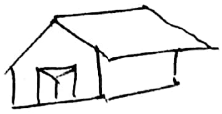


Sol^n:- (a). $\because \forall A$, $\phi \subseteq A$

$\Rightarrow \phi \in \mathcal{P}(A)$ so $\mathcal{P}(A) \neq \phi$

(b). Let $A = \phi$ then $\mathcal{P}(A) = \{\phi\}$

(c). $A = \{1\} \Rightarrow \mathcal{P}(A) = \{\phi, \{1\}\} = \text{finite}$



Group

Group: Let G be a non-empty set and '$*$' is a binary operation on G, then G is said to be a GROUP w.r.t '$*$' if —

(i). '$*$' is associative i.e $a*(b*c) = (a*b)*c$

(ii). $\exists$ an identity element i.e $\exists\ e \in G$ s.t $a*e = e*a = a$

(iii). $\exists$ an invertible element ie $\exists\ b \in G$ s.t $ab = ba = e$ $\forall\ a \in G$

Such a group is denoted by $(G, *)$ or simply G.

Note:

'$*$' is a binary operation it means $\forall\ a, b \in G$ $a*b$ is unique in G. This property is called closure property.

In other way

Group: A non-empty set G with binary composition $*$ is called group, if following condⁿ are satisfied:

(G1). Closure law ($a*b \in G$ $\forall\ a, b \in G$)

(G2). Associative law ($a*(b*c) = (a*b)*c$ $\forall\ a, b, c \in G$)

(G3). Existence of Identity ($\exists$s $e \in G$ s.t $a*e = e*a = a$ $\forall a \in G$)

(G4). Existence of Inverse (For each $a \in G$, $\exists$s an elt. $b \in G$ s.t $a*b = b*a = e$)

- 'e' is called identity in G & 'b' is inverse of 'a' in G.

Remarks:

(1). A group G is called finite or infinite according to it contains a finite or Infinite no. of elements.

(2). If a grp G contains n-elt, we say

$$\boxed{\text{'order of } G \text{ is } n\text{'} \ \& \ O(G) = n}$$

(3). let $a \in G$, then we define $a^0 = e$ and for $n \in N$,

$$a^n = \underbrace{a * a * \dots * a}_{n\text{-times}}$$

Also $a^{-n} = (a^{-1})^n$

Abelian Group: A gp. G is said to be abelian (or commutative) if —

$$a * b = b * a \quad \forall\ a, b \in G$$

Examples

(1) The set $A(S)$ of all one-to-one mappings of a n.e set S onto itself is a group w.r.t the product mappings.

(2). $(I, +)$ is a gp. (or $(\mathbb{Z}, +)$)
(where $0 \in I$ is identity & inverse of a is $-a \in I$)

(3). $(N, +)$ is NOT a gp.
(axioms G3 & G4 are NOT satisfied in N)

(4). $(I, \times)$ is Not a gp. (or $(\mathbb{Z}, \times)$)
(Axiom G4 is NOT satisfied Here).

Sylow Theorem

Sylow's Theorem and it's Application

Def^n: Let G be a group & let p be a prime. A group of order p^α for some $\alpha \geq 1$ is called a p-Group.

A subgroup of G is called p-subgroup.

*. If G is a group of order $p^\alpha m$, where $p \nmid m$ then a subgroup of order p^α is called a sylow p-subgroup of G.

*. $Syl_p(G)$ = set of sylow p-subgroups of G

$n_p(G)$ = No. of sylow p-subgroups of G.

SYLOW'S THEOREMS

(i).. **Sylow Theorem - 1:**

Let G be a group of order $p^\alpha m$, where p is prime not dividing m i.e $p \nmid m$. Then $\exists$ a sylow p-subgroup of G of order p^α i.e

$$Syl_p(G) \neq \phi$$

OR, If $p^k \mid o(G)$, then $\exists$ $H \trianglelefteq G$ s.t $o(H) = p^k$.

(ii). **Sylow Theorem-2 :**

Let P is a sylow p-subgrp. of G and Q is any p-subgrp. of G, then $\exists$s $g \in G$ s.t $Q \subseteq gPg^{-1}$ i.e Q is contained in some conjugate of P.

NB: In particular, any two sylow p-subgroups are conjugate in G.

(iii) **Sylow Theorem-3 :**

The no. of distinct sylow p-subgroups divides $|G|$ is of the form $kp+1$

i.e $n_p = k_p + 1$

or $n_p = 1 \mod p$

i.e $n_p = |G : N_G(P)|$

P-SSG (P-sylow subgroup of G)

If $p^k \mid o(G)$, $p^{k+1} \nmid o(G)$, then G has a subgroup of order p^k, called P-SSG.

Result : P is normal in G $\Leftrightarrow$ All subgroups generated by elt.s of P-power order are p-groups. i.e if X is any subset of G s.t $|x| =$ power of P $\forall x \in X$, then $\langle x \rangle$ is a p-group.

JAM- 2020 (ABSTRACT ALGEBRA)

Ques 2M Let G be a group with identity e. Let H be an abelian non-trivial proper subgroup of G with the property that $H \cap gHg^{-1} = \{e\}$ for all $g \notin H$.

If $K = \{g \in G ; gh = hg \text{ for all } h \in H\}$, then

(A) K is a proper subgroup of H.

(B) H is a proper subgroup of K.

(C) $K = H$.

(D) There exists no abelian subgroup $L \subseteq G$ s.t. K is a proper subgroup of L.

Ans: (C), (D)

Soln

Here, $K = \{g \in G ; gh = hg \text{ for all } h \in H\}$

$\Rightarrow K$ is centralizer of H.

$\because H$ is abelian $\Rightarrow \forall h \in H \Rightarrow h \in K \Rightarrow H \subseteq K$. — (1)

Also, $K \subseteq H$ (If not, then $\exists$ a $k \in K$ s.t. $k \notin H$.

$\Rightarrow kh = hk \ \forall h \in H \Rightarrow kH = Hk \Rightarrow kHk^{-1} = H$

$\Rightarrow kHk^{-1} \cap H = H \neq \{e\}$ ($\because H$ is non-trivial subgroup)

So, $K \subseteq H$) — (2)

$\therefore$ (1) + (2) $\Rightarrow K = H$ – opt (A) + opt (B) – False

opt (C) – True

(D) Suppose, $\exists$ an abelian subgroup $L \subseteq G$ s.t. $K \subset L$.

Then, choose $a \in L \setminus K$, $k \cap kHk^{-1} = e$ ($\because K = H$)

$\Rightarrow \exists$ atleast one element $b \in H$ s.t. $ba \neq ab$

$\Rightarrow L$ is not abelian, which is not true.

$\therefore$ opt (D) – True.

GATE-2020 (ABSTRACT ALGEBRA)

Ques Let G be a non-cyclic group of order 57. Then the number of elements of order 3 in G is 38.

Sol^n **Recall:** ① If G be a non-abelian group of order pq with $p<q$, then the no. of elements of order q are, $\phi(q)=q-1$ and no. of elements of order p are, $\phi(p)\cdot q=(p-1)\cdot q$.

Here, $|G|=3\times19$, $3<19$ and G is non-cyclic

$\Rightarrow G$ is non-abelian

($\because$ If $|G|=pq$ with $p<q$ & G is non-cyclic then G is non-abelian)

So, No. of elements of order 3 $=(3-1)\times19$
$=2\times19$
$=\underline{38}$

Method-2

No. of 3-sylow subgroup in $G=1+3k$ s.t $1+3k \mid 19$
$=1$ or 19

and no. of 19-sylow subgroup $=1+19k$ s.t. $1+19k \mid 3$

$=1$

Let H_1 s.t. $|H_1|=19$ $\because \exists$ unique 19 sylow subgroup.

$\Rightarrow$ No. of elements in H_1 of order $19=18$

and In each 3-sylow subgroup no. of elements of order $3=2$ ($\because$ one element is identity)

and Total no. of 3-sylow subgroups $=19$

So, No. of elements of order $3=2\times19=\underline{\underline{38}}$