Group Theory

Definition

- An abstract group G is a set of elements $a, b, c, \ldots$ for which a "product" ab is defined such that

1. if $ab = c$, then c is in the set
2. multiplication is associative i.e. $a(bc) = (ab)c$.
3. an identity element e is in the set such that $ae = ea = a$ for all a
4. For every a, there exists an element b such that $ab = ba = e$. Then $b = a^{-1}$.

Examples

1. the set of rational fractions under multiplication. ($e = 1$)
2. the set of integers under addition ($e = 0$)
   $n_1 + n_2 = n_3$, $n_1^{-1} = -n_1$.
3. the transformations of an equilateral triangle which bring it into coincidence with itself.
4. permutations of n objects.

Group Structure

- Defined by the multiplication table. The above are particular realizations of the abstract group structure.

Abelian Group

- any commutative group. Examples 1-3 are abelian while 4 is not.

$$123 \xrightarrow{1 \rightleftarrows 2} 213 \xrightarrow{2 \rightleftarrows 3} 312$$
$$\xrightarrow{2 \rightleftarrows 3} 132 \xrightarrow{1 \rightleftarrows 2} 231$$

Order of a Group

- The number of elements in the group.

Order of an Element a

- Consider the sequence $a, a^2, a^3, \ldots$
If $a^n = e$, then a is of order n.

- The set of elements $a, a^2, \ldots a^n = e$ forms the cyclic group of order n.

Examples of Group Structure

Order 1 - e, $e^2 = e$.

Order 2 $e, a, a^2 = e$

	e	a
e	e	a
a	a	e

e.g. co-ord. inversions $(x, y, z) \to (-x, -y, -z)$

Permutations of 2 symbols.

$$e = \begin{cases} 1 \to 1 \\ 2 \to 2 \end{cases} \qquad a = \begin{cases} 1 \to 2 \\ 2 \to 1 \end{cases}$$

Isomorphism

Groups G and G' are isomorphic ($G \simeq G'$) ~~are isomorphic~~ if the elements can be put into a one-to-one correspondence which is preserved under combination.

ie if $a \to a'$
$b \to b'$
$c \to c'$
then $ab = c \implies a'b' = c'$.

All isomorphic groups have the same multiplication table.

All groups of order 2 are isomorphic.

Order 3

- Elements a, b, e.

$ab \neq a$ or b since this would imply that $b = e$ or $a = e$.

$\therefore ab = e$.

Similarly $a^2 \neq e$ since $a^2 b = ae = a$

$\Rightarrow b = a$ if $a^2 = e$.

$\therefore a^2 = b$ and $b^2 = a$

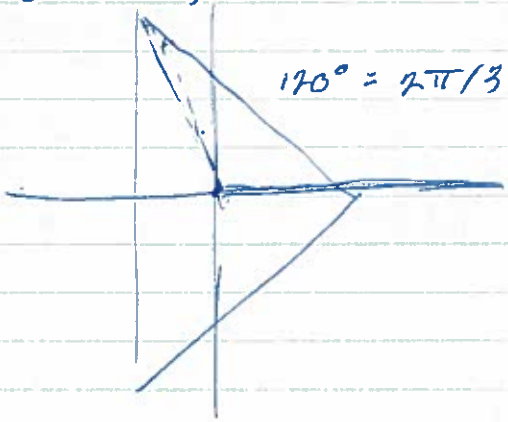
Thus the cyclic group $a, a^2, a^3 = e$ is the only group of order 3.

Examples

1.- Rotations in a plane of an equilateral triangle

2.- The cube roots of unity with ordinary mult.

$1, e^{i2\pi/3}, e^{i4\pi/3}$



	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

- The n'th. roots of unity always form an n-dimensional cyclic group.

$e^{2\pi m i/n}$, $m = 0, 1, \cdots, n-1$.

$\therefore$ there is at least one group for any finite order n.

Order 4

- There are two distinct structures.

e	a	b	c
a	b	c	e
b	c	e	a
c	e	a	b

ie $b = a^2$

$c = ab = a^3$

This is the cyclic group $a, a^2, a^3, a^4 = e$.

e	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

ie $a^2 = b^2 = c^2 = e$

$ab = c$, $bc = a$, $ca = b$.

called the "four group".

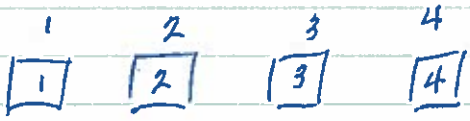
- Realizations - rotations through 180° about x, y, z axes.

$$a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad b = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Permutations

- Label a set of boxes from 1 to n. Each box contains an object.
- a permutation consists of rearranging the objects so that once more each box contains one object.



$$a = \left\{ \begin{array}{l} 1 \to 4 \\ 2 \to 3 \\ 4 \to 2 \\ 3 \to 1 \end{array} \right\}$$

a	3	4	2	1	
a^2	2	1	4	3	
a^3	4	3	1	2	
a^4	1	2	3	4	$= e$

Notation

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} \text{boxes} \\ \text{images} \end{pmatrix}$$

Any rearrangement of columns denotes the same permutation

$$\text{eg. } \begin{pmatrix} 1 & 3 & 2 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = a.$$

- This is a permutation of degree 4. If there are n symbols, then there are in all n! permutations.

An arbitrary permutation is denoted

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix}$$

if p_1 is the image of box 1 etc.

Linear Transformations

$$x_i' = \sum_{j=1}^{n} a_{ij} x_j \qquad \text{general linear transformation.}$$

A permutation can be regarded as a special case of a linear transformation. Replace $1, 2, 3, \cdots$ by the co-ordinates of a point $(x_1, x_2, x_3, \cdots)$.

The permutation transforms this point to a new point $(x_1', x_2', x_3', \cdots)$ such that $x_{p_1}' = x_1$, $x_{p_2}' = x_2$, $\cdots$.

· As the previous example,

$$x_1' = x_3$$
$$x_2' = x_4$$
$$x_3' = x_2$$
$$x_4' = x_1$$

$$\therefore \underset{\sim}{a} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

objects (~~boxes~~) →

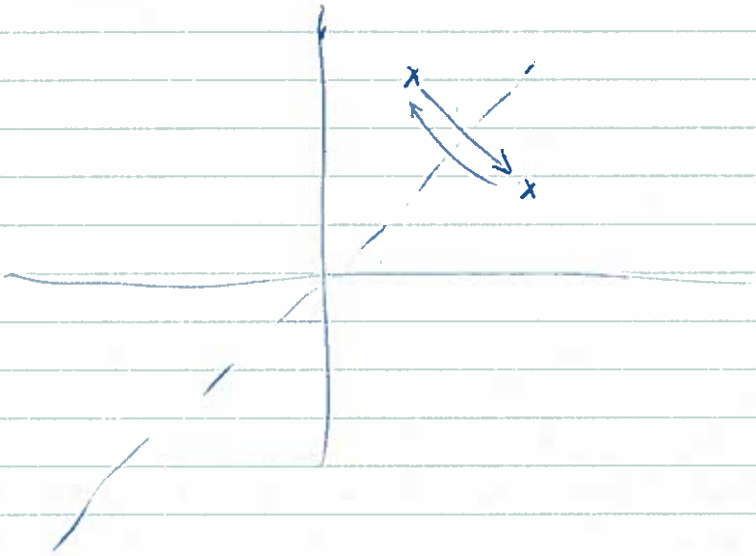
images ↓

$a_{32} = 1 \Rightarrow$ ~~the image of box 2 is~~ ~~object~~ ~~in box~~ box 3 ~~is the image of box 2.~~ ~~object~~

object in box 3 moves to box 2.

For 2 boxes, $a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$\begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$$



The Symmetric Group (S_n)

- all permutations of degree n form a group of order $n!$ called the symmetric group.

$$\pi_a = \begin{pmatrix} 1 & 2 & \cdots & n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix},$$

$$\pi_b = \begin{pmatrix} 1 & 2 & \cdots & n \\ q_1 & q_2 & \cdots & q_n \end{pmatrix} = \begin{pmatrix} p_1 & p_2 & \cdots & p_n \\ q_{p_1} & q_{p_2} & \cdots & q_{p_n} \end{pmatrix}$$

Then $\pi_c = \pi_b \pi_a = \begin{pmatrix} p_1 & p_2 & \cdots & p_n \\ q_{p_1} & q_{p_2} & & q_{p_n} \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ p_1 & p_2 & & p_n \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & \cdots & n \\ q_{p_1} & q_{p_2} & \cdots & q_{p_n} \end{pmatrix}$$

i.e. perform the permutation Π_b on the bottom row of Π_a to obtain Π_c.

$$\Pi_a^{-1} = \begin{pmatrix} P_1 & P_2 & \cdots & P_n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

In general, $\Pi_b \Pi_a \neq \Pi_a \Pi_b$ so the group is non-abelian.

Cycle Structure

consider $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 4 & 7 & 6 & 8 \end{pmatrix}$

$= (1\,2\,3)(4\,5)(6\,7)(8)$

i.e. write the image after each symbol. The total permutation decomposes into 1-3 cycle, 2-2 cycles and 1-1 cycle. Cycles have no elements in common.

also $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 1 & 4 & 7 & 6 & 8 \end{pmatrix}$

$= (1\,2\,3\,5\,4)(6\,7)(8)$

$= (3\,5\,4\,1\,2)(6\,7)(8)$

- a two-cycle is a transposition. Any cycle can be written as a product of transpositions with elements in common.

in general $(1\,2 \cdots n) = (1\,n) \cdots (1\,3)(1\,2)$

i.e. an n-cycle is equivalent to n-1 transpositions.

A permutation with an even no. of transpositions is called even and conversely if the no. is odd.

e.g. $(123)(45)(67) = (13)(12)(45)(67)$ is even.

Decrement = no. of symbols - no. of cycles
= $7 - 3 = 4$.

The decrement determines whether the permutation is even or odd.

- The even and odd permutations combine under multiplication like +1 and -1.

∴ the even permutations alone form a group A_n called the alternating group of order $n!/2$.

Cayley's Theorem
- Every group G of order n is isomorphic with a subgroup of S_n.

ie. S_n exhausts the possible structures of finite groups. The no. of possible structures is finite.

Subgroup
- If the elements in a subset H of G form a group, then H is a subgroup of G.
$H \subset G$.

e.g. $A_n \subset S_n$.

Every group has two trivial subgroups -
$H = G$
$H = e$
} improper

The problem is to find proper subgroups.

Example - S_3 consists of
$e, (1\,2\,3), (1\,3\,2)$; $(1\,2), (1\,3), (2\,3)$
$\underbrace{\qquad\qquad}_{A_3}$

Other subgroups are $H_1 = \{e, (2\,3)\}$
$H_2 = \{e, (1\,3)\}$
$H_3 = \{e, (1\,2)\}$

- Clearly $H_1 \simeq H_2 \simeq H_3$.

In general, S_n contains, among others, the n subgroups $H_1, H_2, \cdots, H_n$

H_i leaves element i unchanged.

All are isomorphic to S_{n-1}.

Proof of Theorem

- Take any element b of $C_{T_x} = \{a_1, a_2, \cdots, a_n\}$

and form the products $ba_1, ba_2, \cdots ba_n$. All the products are distinct since $ba_1 = ba_2 \Rightarrow a_1 = a_2$.

$\therefore$ multiplying the list by b corresponds to writing the original list in a different order.

Replace b by $\pi_b = \begin{pmatrix} a_1 & \cdots & a_n \\ ba_1 & \cdots & ba_n \end{pmatrix}$

" c " $\pi_c = \begin{pmatrix} a_1 & \cdots & a_n \\ ca_1 & \cdots & ca_n \end{pmatrix}$

$$\pi_c \pi_b = \begin{pmatrix} a_1 & \cdots & a_n \\ ca_1 & \cdots & ca_n \end{pmatrix}\begin{pmatrix} ca_1 & \cdots & ca_n \\ cba_1 & \cdots & cba_n \end{pmatrix} = \begin{pmatrix} a_1 & \cdots & a_n \\ cba_1 & \cdots & cba_n \end{pmatrix}$$

$$\begin{pmatrix} ba_1 & \cdots & ba_n \\ cba_1 & \cdots & cba_n \end{pmatrix}\begin{pmatrix} a_1 & \cdots & a_n \\ ba_1 & \cdots & ba_n \end{pmatrix} = \pi_{cb} \longrightarrow cb$$

- $\pi_b \neq \pi_c$ if $b \neq c$ so the mapping is one-to-one and is preserved under combination.
∴ mapping is an isomorphism.

Example - the four group

#	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

e - 1
a - 2
b - 3
c - 4

$$\pi_c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\pi_a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\,2)(3\,4)$$

$$\pi_b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\,3)(2\,4)$$

$$\pi_c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1\,4)(2\,3)$$

The cyclic group of order 4.

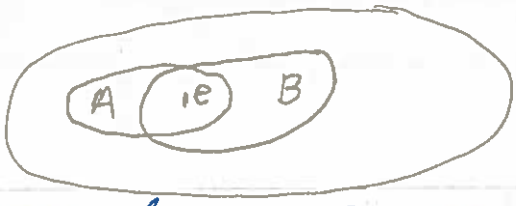
	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$$\pi_e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\pi_a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\,2\,3\,4)$$

$$\pi_b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\,3)(2\,4)$$

$$\pi_c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1\,4\,3\,2)$$



Notice that the common elements π_e, π_b themselves form a group. In general, elements in common to two subgroups themselves form a subgroup.

General Properties.

1. They are subgroups of order n of S_n.
2. Each permutation leaves no symbol unchanged. (except for π_e). eg. π_b takes a_i into ba_i, which equals a_i only if $\pi_b = \pi_e$.
   Permutations of this type are called regular permutations and the subgroups are called regular subgroups.

Consequences.

1. No two permutations, π_a, π_b can take a given element c into the same element d, since $\pi_a \pi_b^{-1}$ would leave c and d unchanged.

2. all cycles must have the same length for a given element. eg. $\{(12)(345)\}^2 = (1)(2)(354)$
   member of group, but leaves 1 unchanged

Application
- consider a group of prime order n'. The only possible cycle structure is

$$\pi_a = (1\,2 \cdots n')$$

$$\pi_a^2, \pi_a^3, \cdots \pi_a^{n'} = e.$$

ie. the cyclic group of order n'.

Exercise - Using Cayley's Theorem, find the possible groups of order 6.

Lagrange's Theorem

Example - notice that the four group has the subgroups
(e, a), (e, b), (e, c) each of order 2.
2 is an integral division of 4.

Theorem - for any finite group, the order of a subgroup is a division of the order of the group.

Proof
- Consider a group G of order g and a subgroup H of order h.
Case I - If H = G i.e. h = g.

Case II - H is a proper subgroup contained in G.
i.e. h < g.

H has elements $H_1, H_2, \cdots, H_h$.

Let a be an element of G not in H. Form the products
$\{aH_1, aH_2, \cdots, aH_h\} = aH$. Left coset
(all different)

No element of aH is in H, for if, say
$aH_1 = H_2$, then $a = H_2 H_1^{-1}$ is in H.

Case I' - $H + aH = G$ i.e. $h = g/2$

Case II' - $H + aH \subset G$ i.e. $h < g/2$.

- Pick another element b not in H or aH and form bH.

No element of bH can be in H or aH

e.g. if $aH_1 = bH_2$, then $b = aH_1H_2^{-1}$ is in aH.

Continuing in this way, the group G_T must eventually be exhausted, and

$$G_T = H + aH + bH + \cdots + kH.$$

ie $g = \cancel{nH}\ mh.$

m is called the index of subgroup H under group G_T.

∴ We could similarly have made the resolution into right cosets

$$G_T = H + Ha' + Hb' + \cdots + Hk'$$

Are the cosets subgroups? Are the left and right cosets necessarily equal?

Consequences

1. - any element and its powers form a subgroup $a, a^2, \cdots a^h = e$ $h =$ ~~period~~ order of a.
∴ h is a divisor of g.

2. - Groups of prime order must be cyclic.