ARULMIGU PALANIANDAVAR ARTS COLLEGE FOR WOMEN, PALANI

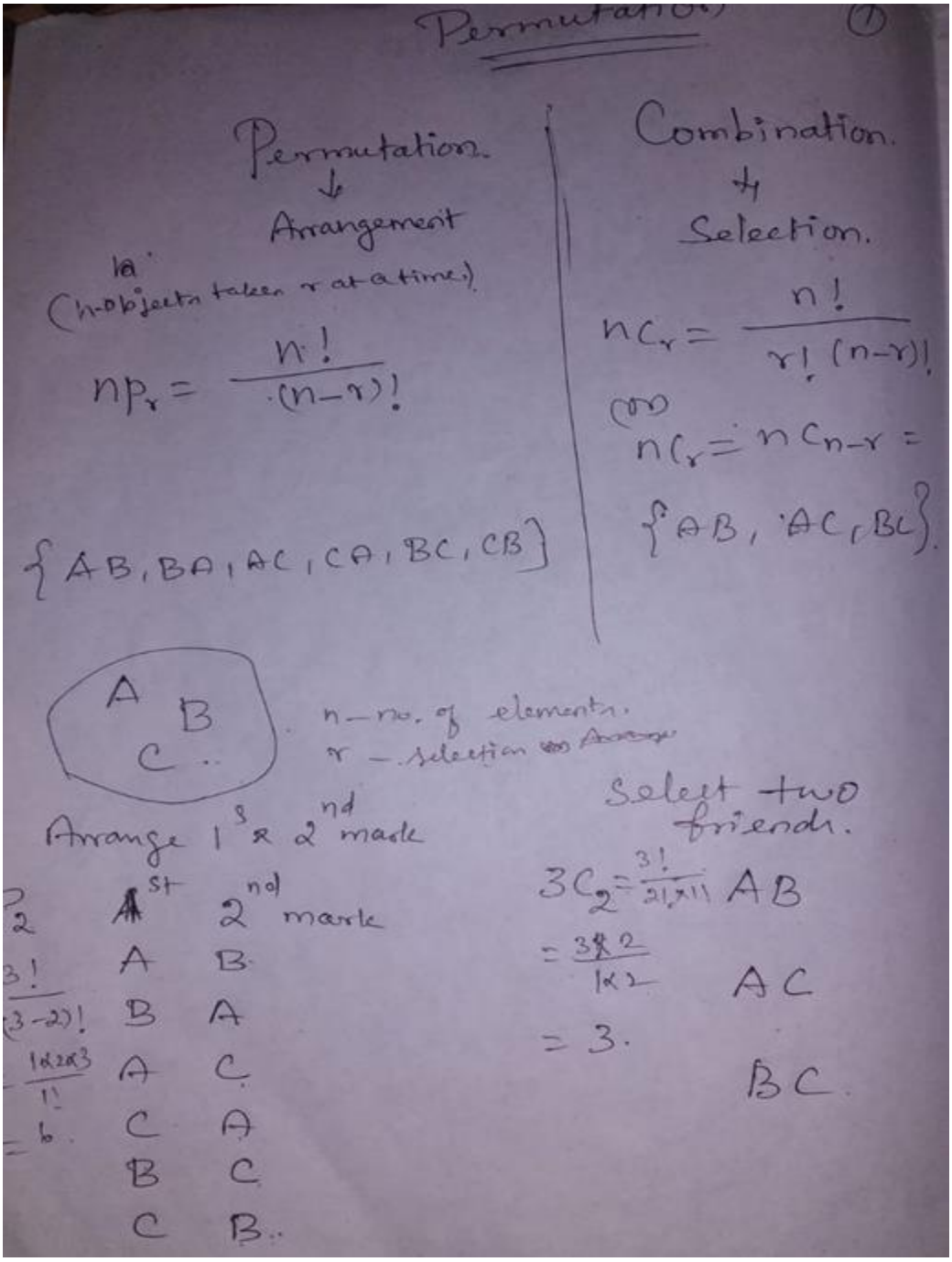
Department of Mathematics

Learning Resources

Title of the paper: Modern Algebra

Prepared By

Dr.K.Meena, Associate Professor and Head

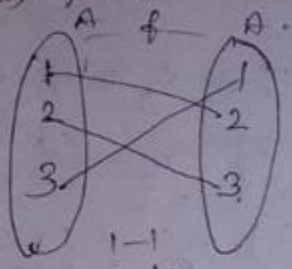


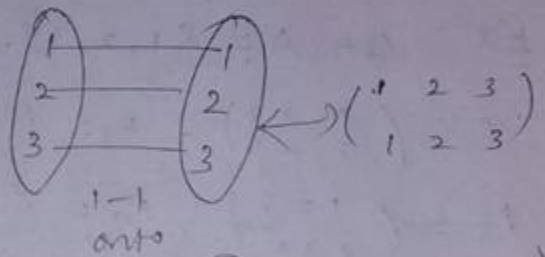
Permutation Group.

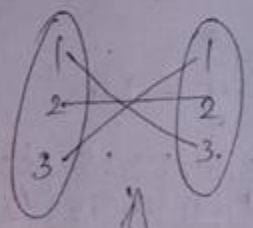
Defn:- Let A be a finite set. A bijection from A to itself is called a permutation of A.

Ex: If $A = \{1, 2, 3\}$ $f: A \to A$ defined by $f(1)=2$, $f(2)=3$, $f(3)=1$ is a permutation of A.

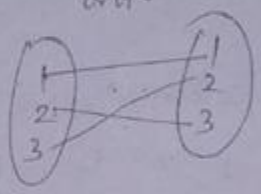
(ie) permutation of $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

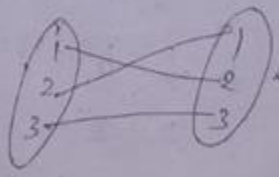


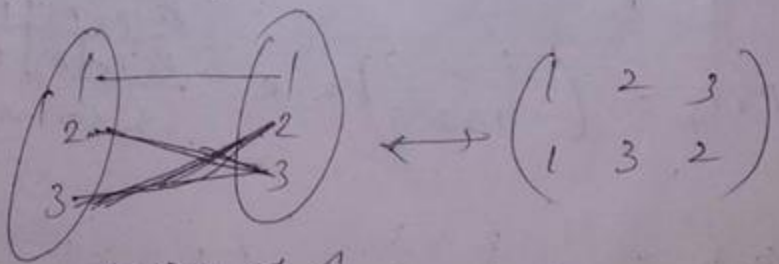




$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$







No. of Permutation of A
$= 3!$ Permutations of A.

I

Cycle Let p be a permutation on $A = \{1, 2, \cdots n\}$. p is called a cycle of length r if r distinct symbols $a_1, a_2, \cdots a_r$ such that $p(a_1) = a_2$, $p(a_2) = a_3, \cdots p(a_{r-1}) = a_r$ and $p(a_r) = a_1$ and $p(b) = b$ for all $b \in A - \{a_1, a_2, \cdots a_r\}$.

It is denoted by $(a_1 a_2 \cdots a_r)$.

(6)

Ex Let $A = \{1, 2, 3, 4, 5\}$.

Consider the cycle of length 4 given by (2451).

$2 \to 4 \to 5 \to 1$

Then $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 1 \end{pmatrix}$

Remaining $p(b) = b$ $\forall b \in A - \{2, 4, 5, 1\}$

Take (4 5 1 2). Then $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$

$\therefore (2\,4\,5\,1) = (4\,5\,1\,2) = (5\,1\,2\,4) = (1\,2\,4\,5)$.

Note The product of cycles need not be a cycle.

Ex Let $P_1 = (2\ 3\ 4)$ and $P_2 = (1, 5)$ Then

$$P_1 P_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$$

$$= \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 3 & 4 & 2 & 1 \end{matrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$$ This is not a cycle

$P_2 P_1 = (1\,5)(2\,3\,4)$

II

Defn:- Two cycles are said to be disjoint if they have no symbols in common.

for Eg (2 1 5) and (3 6) are disjoint cycles

(2 3 4) and (1 5) ''

$$P_1 P_2 = (2\ 3\ 4)(1\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$$

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

$$\boxed{P_1 P_2 = P_2 P_1}$$

Hence multiplication of disjoint cycles is commutative.

Eg Consider the permutation.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 5 & 6 & 7 & 4 \end{pmatrix} = (1\ 2)(4\ 5\ 6\ 7)$$

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

III

Ex 1

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 7 & 5 & 4 & 1 & 6 \end{pmatrix} = (1\ 2\ 3\ 7\ 6)(4\ 5).$$

Ex 2

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 2 & 5 \end{pmatrix} = (1\ 4\ 3)\cdot(2\ 6\ 5).$$

Homework: Express the following permutation as a product of disjoint cycles.

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$ b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$

c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 6 & 1 \end{pmatrix}$ d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 3 & 7 & 2 & 1 & 6 \end{pmatrix}$.

Ex 1 $(1\ 2\ 3\ 4)(3\ 4\ 5)$. (P_1, P_2)

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

$$= \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 & 5 \end{matrix} \quad P_1$$

$$\begin{matrix} \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 5 & 1 & 3 \end{matrix} \quad P_2$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

$$= (1\ 2\ 4)\cdot(3\ 5).$$

Ex $(1,3)(3\,4)(4\,5)$ (Take $= P_1 P_2 P_3$)

$$P_1P_2P_3 = \begin{pmatrix}1&2&3&4&5\\3&2&1&4&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\1&2&4&3&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix}$$

$$= \begin{matrix}1&2&3&4&5\\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\3&2&1&4&5\end{matrix} \; P_1$$

$$\begin{matrix}1&2&3&4&5\\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\1&2&4&3&5\end{matrix} \; P_2$$

$$\begin{matrix}1&2&3&4&5\\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\1&2&4&3&5\end{matrix} \; P_3$$

$$= \begin{pmatrix}1&2&3&4&5\\5&2&1&3&4\end{pmatrix} = (1\,5\,4\,3)$$

Home work $(1\,2\,3)$ $(1\,6\,5\,4\,3)$

P_1 P_2.

V.

Thm Any Permutation can be expressed as a product of disjoint cycles.

Proof Let p be a given permutation of the set $S = \{1, 2, 3, \cdots n\}$.

Let us start with any symbol $a_1 \in S$.

Let $p(a_1) = a_2$, $p(a_2) = a_3$ ---- since S is finite, these symbols cannot all be distinct one hence there exists a least positive integer r such that $1 \le r \le n$ and $p(a_r) = a_1$

Let $c = (a_1 a_2 \cdots a_r)$. If $r = n$ then $p = c$. So that p is a cycle.

If $r < n$, let b_1 be a symbol in S such that $b \notin (a_1, a_2, \cdots a_r)$. Starting with b_1 we can construct the cycle $d = (b_1, b_2, \cdots b_s)$ as before.

Clearly the cycles c and d are disjoint.

If $r + s = n$. then $p = cd$.

If $r + s < n$. We repeat the above process to obtain more cycles until all the symbols appear in one of the cycles.

Thus We get any permutation can be expressed as a product of disjoint cycles.

(or)

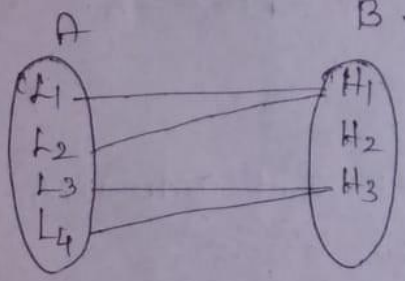
We get a decomposition of permutation p into disjoint cycles.

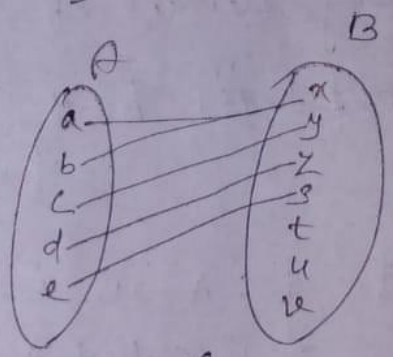
Function.

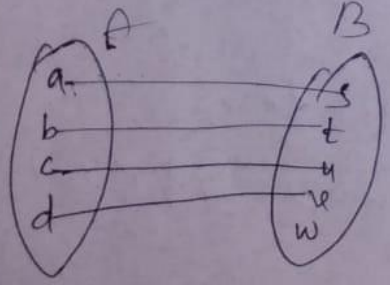
Let A and B be a non-empty sets. A function or a mapping f from A into B is $f: A \to B$ which assigns to each element $a \in A$ a unique element $b \in B$. $f(a) = b$. [b is called the image of a.]

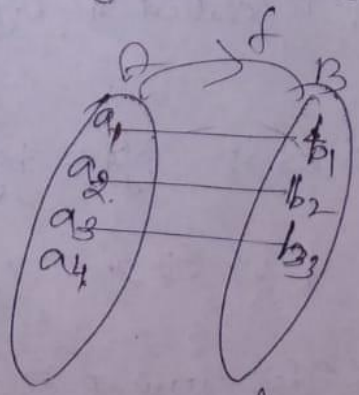
A - is domain.

$\{ f(a) \mid a \in A \}$ - range of f.









f is not a function.

(2)

* A function $f: A \to B$ is one-one (injective) if distinct elements in A have distinct images in B under f.

(i) f is 1-1 if $x, y \in A$ and $x \neq y \Rightarrow f(x) \neq f(y)$.

(or) $f(x) = f(y) \Rightarrow x = y$.

* The mapping f is called onto (Surjective) if the range of f is equal to B. Thus if f is onto, every element of B has a pre-image in A.

(i) ~~$f: A \to B$~~ Let $b \in B$ $\exists$ $a \in A$ $\ni$ $f(a) = b$.

f is onto.

If $f: A \to B$ is both 1-1 and onto then f is called a bijection.

Ex $f: \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = 2x$.

$f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y$ $\therefore$ f is 1-1.

$3 \in \mathbb{Z}$, The element $3 \in \mathbb{Z}$ does not have any pre-image. Hence f is not onto.

Ex $f: R \to R$ given $f(x) = 2x$.

f is 1-1 & onto.

Group.

A non-empty set G is group if

i) Closure law holds in G

(i) for $a, b \in G$, $a * b \in G$

ii) Associative law holds in G

(i) for $a, b, c \in G$, $a*(b*c) = (a*b)*c$

iii) Identity law holds in G

(i) for $a \in G$, $a * e = e * a = a$

where e is identity element.

iv) Inverse law holds in G

(i) for $a \in G$, $\exists\ a' \in G$ s.t.

$a * a' = a' * a = e$. a' is inverse of a.

If commutative law holds in G then G is called abelian group.

Ex. $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$ are Example of group and $(Z_n, \oplus)$ is a group.

$(N, +)$ is not a group.

Z_n = integer modulo n.

$\{0, 1, 2, 3, \ldots, (n-1)\}$.

Defn The group A_n of all even ... is called the alternating group on n symbols.

Subgroups Let G be a set with a binary operation $*$ defined on it. Let $S \subseteq G$. If for each $a, b \in S$, $a * b \in S$ we say that S is closed with respect to the binary operation '$*$'

Defn. A subset H of a group G is called a subgroup of G if H forms a group with respect to the binary operation in G.

Ex 1. Let G be any group.
Then $\{e\}$ and G are subgroups of G.
They are called improper subgroups of G.

Ex2: $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.

Ex3: $(\mathbb{R}, +)$ is a subgroup of $(\mathbb{C}, +)$

Ex4: In $(\mathbb{Z}_8, \oplus)$ is a group. Let $H_1 = \{0, 4\}$ and $H_2 = \{0, 2, 4, 6\}$

Cayley table H_1

$\oplus$	0	4
0	0	4
4	4	0

$H_1 \Rightarrow$ 0 is the inverse of 0, 4 is the inverse of 4.

From the Cayley tables.
H_1 and H_2 are closed under $\oplus$. identity, inverse

Cayley table for H_2

$\oplus_8$	0	2	4	6
0	0	2	4	6
2	2	4	6	0
4	4	6	0	2
6	6	0	2	4

H_2: 0 is the inverse of 0, 2 is the inverse of 6, 6 is the inverse of 2, 4 is the inverse of 4.

$(H_1, \oplus)$ and $(H_2, \oplus)$ are subgroups.
$\therefore H_1$ and H_2 are subgroups of $(\mathbb{Z}_8, \oplus)$

$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

a: $\{1, -1\}$ is a subgroup of $(\mathbb{R}^*, \cdot)$

b: $\{1, i, -1, -i\}$ is a subgroup of $(\mathbb{C}^*, \cdot)$

where $\mathbb{R}^*$ = The set of all non-zero real numbers.
$\mathbb{C}^*$ = " " complex numbers

Note . The above thm is not true ...

Proof If H is infinite . Take $H = N$ is an infinite subset of $(\mathbb{Z}, +)$.
and N is closed under addition
N is not a subgroup of $(\mathbb{Z}, +)$.

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

Proof . Clearly $e \in H \cap K$. and hence $H \cap K$ is non-empty
Now let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$.
Since H and K are subgroups of G.
$ab^{-1} \in H$ and $ab^{-1} \in K$.
$\therefore ab^{-1} \in H \cap K$.

$\therefore$ $H \cap K$ is a subgroup of G.

Note ① The Intersection of any number of subgroups of G is a subgroup of G.

② The union of two subgroups of a group need not be a subgroup

For ex : . $2\mathbb{Z}$ and $3\mathbb{Z}$ are subgroups of $(\mathbb{Z}, +)$

But $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subgroup of $\mathbb{Z}$

Since $3, 2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$.

but $3 + 2 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

$\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \pm 8, \cdots\}$
$\{\pm 6, \pm 9, \cdots\}$

$2\mathbb{Z} \cup 3\mathbb{Z} = \{0, \pm 2, \pm 4, \cdots$
$\pm 3, \pm 6, \pm 9, \cdots$

Thm 3: A non-empty subset H of a group G is a subgroup of G iff $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof Let H be a subgroup of G.

Then $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow ab^{-1} \in H$.

Conversely let H be a non-empty subset of G such that $a, b \in H \Rightarrow ab^{-1} \in H$.

Since $H \neq \phi$ there exists an element $a \in H$.

Hence $a a^{-1} \in H$. Thus $e \in H$.

Also since $e, a \in H$, $ea^{-1} \in H$ Hence $a^{-1} \in H$.

Now let $a, b \in H$, Then $a, b^{-1} \in H$.

Hence $a(b^{-1})^{-1} = ab \in H$

Thus H is closed under the binary operation in G.

$\therefore$ H is a subgroup of G. by thm 2.

Note If the operation is $+$ then H is a subgroup of G iff $a, b \in H \Rightarrow a - b \in H$.

Thm 4:- Let H be a non-empty finite subset of G If H is closed under the operation in G then H is a subgroup of G.

If :- Let $a \in H$

Since H is closed $a, a^2, a^3, \ldots a^n, \ldots$ are all elements of H.

But since H is finite the elements $a, a^2, a^3, \ldots$ cannot all be distinct.

Hence let $a^r = a^s$, $r < s$ Then $a^{s-r} = e \in H$.

Now let $a \in H$. we have proved that $a^n = e$ for some n.

Hence $a^{-1} = a^{n-1} \in H$.

Hence $a a^{n-1} = e$. Hence $a^{-1} = a^{n-1} \in H$.

Thm H is a subgroup of G.

Thm 6: The Union of two subgroups of a group G is a subgroup iff one is contained in the other.

Proof Let H and K be two subgroups of G such that one contained in the other. Hence either $H \subseteq K$ or $K \subseteq H$.

$\therefore HUK = K$ or $HUK = H$

Hence HUK is a subgroup of G.

Conversely. Suppose HUK is a subgroup of G.

We claim that $H \subseteq K$ or $K \subseteq H$.

Suppose that H is not contained in k and k is not contained in H.

Then there exists elements a, b such that

$a \in H$ and $a \notin K$ — (1)

$b \in K$ and $b \notin H$ — (2).

Clearly $a, b \in HUK$. Since HUK is a subgroup of G.

$ab \in HUK$. Hence $ab \in H$ or $ab \in K$.

Case(i) let $ab \in H$. Since $a \in H$, $\bar{a}^1 \in H$.

Hence $\bar{a}^1(ab) = b \Rightarrow \in$ to (2).

Case(ii) Let $ab \in K$ since $b \in K$, $\bar{b}^1 \in K$

Hence $(ab)\bar{b}^{-1} = a \in K$ which is a contradiction to (1)

Hence our assumption that H is not contained in k.

and K is not contained in H is false.

$\therefore H \subseteq K$ or $K \subseteq H$.

Ex Suppose $n=4$. p is the cycle $(1,3,4,2)$.

$$\Delta = (x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4).$$

Then $P(\Delta) = (x_3-x_1)(x_3-x_4)(x_3-x_2)(x_1-x_4)(x_1-x_2)(x_4-x_2)$.

$$= -\Delta.$$

Just like Δ, the product $P(\Delta)$ will have nC_2 factors. For any pair of variables x_i and x_j either $x_i - x_j$ or $x_j - x_i$ will be a factor of $P(\Delta)$.

either $P(\Delta)$ is Δ or it is $-\Delta$.

n variables $x_1, x_2, \ldots x_n$.

Take product $\prod_{i<j} (x_i - x_j)$.

Call this product Δ. when $n = 4$.

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

$\left[\frac{n(n-1)}{2} = {}^nC_2 \text{ factors in this product}\right]$

For any pair of variables x_i and x_j either $x_i - x_j$ or $x_j - x_i$ is a factor of Δ. but not both.

We can view a permutation as a rearrangement of the variables.

We can view a permutation p as changing the product Δ.

$$p(\Delta) = \prod_{i<j} (x_{p(i)} - x_{p(j)})$$

Cyclic group

Defn Let G be a group let $a \in G$. Then $H = \{a^n / n \in \mathbb{Z}\}$ is a subgroup of G. H is called the cyclic subgroup of G generated by a and is denoted by $\langle a \rangle$.

Ex In $(\mathbb{Z}, +)$

$\langle 2 \rangle = \{ -2, \underset{=-4}{-2-2}, \underset{=-6}{-2-4}, \underset{=-8}{-2-6}, \underset{=-10}{-2-8}, \ldots$

$2 \quad \underset{=4}{2+2} \quad \underset{=6}{2+4} \quad \underset{=8}{2+6} \quad \underset{=10}{2+8}, \ldots \}$

$= \{ 0, \pm 2, \pm 4, \pm 6, \pm 8, \pm 10, \ldots \}$

$= 2\mathbb{Z}$

Ex In the group $G = (\mathbb{Z}_{12}, \oplus)$, $\mathbb{Z}_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$

$\langle 3 \rangle = \{ 3, 3+3=6, 3+6=9, \underset{=0}{3+9=12} \}$ → next $3+0=3$, $3+3=6$ Repeats

$= \{3, 6, 9, 0\}$.

$\langle 3 \rangle = \{0, 3, 6, 9\}$

$\langle 5 \rangle = \{ 5, 5+5=10, \underset{=3}{5+10=15}, 5+3=8, \underset{=1}{5+8=13}, 5+1=6,$

$5+6=11, \underset{=4}{5+11=16}, 5+4=9, \underset{=2}{5+9=14}, 5+2=7$

$\underset{=0}{5+7=12}, \}$ next $5+0=5$ Repeat $5+5=0$

Stop

$= \{ 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0 \}$

$= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Ex3 In the group $G_1 = \{1, i, -1, -i\}$.

$\langle i \rangle = \{i, i.i = i^2, i.i^2 = i^3, i.i^3 = i^4, \ldots\}$

$= \{i, -1, -i, 1\}$.

$\langle i \rangle = G_1$.

$\langle -1 \rangle = \{-1, -1 \times -1 = 1, -1 \times 1, \ldots\}$

$= \{-1, 1\}$.

$\langle -i \rangle = \{-i, (-i)(-i) = i^2 = -1, -i \times i^2 = -i^3 = i, -i \times i = -i^2 = 1.\}$

$= \{-i, -1, i, 1\} = G_1$.

Defn Let G_1 be a group and let $a \in G_1$, a is called a generator of G if $\langle a \rangle = G_1$.

Ex $(\mathbb{Z}, +)$ is a cyclic group.

$\langle 1 \rangle = \{1, 1+1 = 2, 1+2 = 3, 1+3 = 4, \ldots$

$-1, -1-1 = -2, -1-2 = -3, -1-3 = -4, \ldots\}$

$= \{0, \pm 1, \pm 2, \ldots\} = \mathbb{Z}$.

Also $\langle -1 \rangle = \mathbb{Z}$.

Then 1 and -1 are generators of $(\mathbb{Z}, +)$

Then a cyclic group can have more than one generator.

Ex2 $(n\mathbb{Z}, +)$ is a cyclic group, n and $-n$ are generators of this group.

Ex 3 $(Z_8, \oplus)$ is a cyclic group. $Z_8 = \{0,1,2,3,4,5,6,7\}$

1, 3, 5, 7 are all generators of this group.

$\langle 1 \rangle = \{1, 1+1=2, 1+2=3, 1+3=4, 1+4=5, 1+5=6, 1+6=7, 1+7=8=0\}$

$= \{1,2,3,4,5,6,7,0\} = Z_8$.

$\langle 2 \rangle = \{2, 2+2=4, 2+4=6, 2+6=8=0, 2+0=2 \text{ Repeat}\}$.

$= \{2,4,6,0\} = \{0,2,4,6\}$

$\langle 3 \rangle = \{3, 3+3=6, 3+6=9=1, 3+1=4, 3+4=7, 3+7=10=2, 3+2=5, 3+5=8=0, 3+0 \text{ Repeat}\}$

$= \{3,6,1,4,7,2,5,0\}$

$= \{0,1,2,3,4,5,6,7\} = Z_8$

$\langle 5 \rangle = \{5, 5+5=10=2, 5+2=7, 5+7=12=4, 5+4=9=1, 5+1=6, 5+6=11=3, 5+3=8=0\}$

$= \{5,2,7,4,1,6,3,0\} = Z_8$

$\langle 7 \rangle = \{7, 7+7=14=6, 7+6=13=5, 7+5=12=4, 7+4=11=3, 7+3=10=2, 7+2=9=1, 7+1=8=0\}$

$= \{7,6,5,4,3,2,1,0\} = Z_8$

Ex4 $(Z_n, \oplus)$ is a cyclic group for all $n \in N$.

1 is a generator of this group.

In fact if $m \in Z_n$ and $(m,n) = 1$.

then m is a generator of this group.

Ex5: $G = \{1, w, w^2\}$ $\quad w^3 = 1$.

$1 + w + w^2 = 0$.

$\langle w \rangle = \{ w, w \cdot w = w^2, w \cdot w^2 = w^3 = 1 \}$ $\quad w \neq 1$.

$= \{1, w, w^2\}$

$\langle w^2 \rangle = \{ w^2, w^0 \cdot w^2 = w^4 = w, w^2 \cdot w = w^3 = 1 \}$.

$= \{1, w, w^2\}$.

Ex7 $G = (Z_7 - \{0\}, \odot)$. $\quad Z_7 - \{0\} = \{1, 2, 3, 4, 5, 6\}$.

$\langle 3 \rangle = \{ 3, 3 \cdot 3 = 9 = 2, 3 \times 2 = 6, 3 \times 6 = 18 = 4, 3 \times 4 = 12 = 5, 3 \times 5 = 15 = 1, 3 \times 1 = 3 \text{ Repeat} \}$

~~3 x 66~~ 3.

$= \{3, 2, 6, 4, 5, 1\} = Z_7 - \{0\}$.

(ii) Home work

$\langle 5 \rangle = Z_7 - \{0\}$

$\langle 2 \rangle = \{ 2, 2 \times 2 = 4, 2 \times 4 = 8 = 1, 2 \times 1 = 2 \text{ Repeat} \}$

$= \{2, 4, 1\} \neq G$. $\therefore$ 2 is not a generator of G.

Ex Let A be a set containing more than one element.
Then $(P(A), \Delta)$ is not cyclic.

Sol Let $B \in P(A)$ be any element.
Then $B \Delta B = \phi$.
So that $\langle B \rangle = \{B, \phi\} \neq P(A)$.

[power set of A. = P(A).]

Theorem : Any cyclic group is abelian.

Proof Let $G = \langle a \rangle$ be a cyclic group.
Let $x, y \in G$. Then $x = a^r$ and $y = a^s$ for some $r, s \in \mathbb{Z}$.
Hence $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$.
$\therefore$ G is abelian.

Thm :- A subgroup of cyclic group is cyclic.

Proof Let G be a cyclic group generated by a and Let H be a subgroup of G.
We claim H is cyclic.
Clearly every element of H is of the form a^n for some integer n.
Let m be the smallest positive integer such that $a^m \in H$.
We claim that a^m is a generator of H.
Let $b \in H$. Then $b = a^n$ for some $n \in \mathbb{Z}$.
Let $n = mq + r$ where $0 \leq r < m$.
Then $b = a^n = a^{mq+r} = a^{mq} a^r = (a^m)^q a^r$.

$\therefore a^r = (a^m)^{-q} b$. —①

Now $a^m \in H$. Since H is a subgroup, $(a^m)^{-q} \in H$.
Also $b \in H$.

By (1), $a^r \in H$, $0 \le r < m$.

But m is the least positive integer such that $a^n \in H$

$\therefore r = 0$ Hence $b = a^n = a^{qm} = (a^m)^q$

$\therefore$ Every element of H is a powers of a^m

$\therefore H = \langle a^m \rangle$ and H is cyclic.

A subgroup of cyclic group is cyclic.

Proof

Let G be a cyclic group

Then G has a generator, i.e. $G = \langle a \rangle = \{ a^n / n \in \mathbb{Z} \}$.

Let H be a subgroup of G.

If $H = \{e\}$ Then H is cyclic.

If $H \neq \{e\}$

Let H be a subgroup $G_1 = \{ a^n / n \in \mathbb{Z} \}$.

Then $a^n \in H$ for some $n \in \mathbb{Z}^+$

* Let m be the smallest +ve integer such that $a^m \in H$.

Claim $H = \langle a^m \rangle$. $m \in \mathbb{Z}^+$

(ie) T.P.T If $b \in H$ Then $b = (a^m)^q$ for $q \in \mathbb{Z}^+$

Using Division algorithm.

"If m is a positive integer, and n is any integer. Then there exists unique integers q and r such that $n = mq + r$ and $0 \leq r < m$."

Ex:- Given $m = 4$

If $n = 35$

Then $35 = 4 \times 8 + 3$ $\quad 0 \leq r < 4$.

$\downarrow \quad \downarrow \; \downarrow \; \downarrow$

$\quad n \; m \; q \; r$.

Since $b \in H < G = \{a^n / n \in \mathbb{Z}\}$

So $b = a^n$ for some $n \in \mathbb{Z}$.

· by Division algorithm $n = mq + r$, $0 \le r < m$.

So $b = a^n = a^{mq+r}$ $\quad 0 \le r < m$

$b = (a^m)^q \cdot a^r$ $\quad 0 \le r < m$.

So $\left[(a^m)^q\right]^{-1} b = a^r$ $\quad 0 \le r < m$.

$a^r = \left((a^m)^q\right)^{-1} b$

$\uparrow$ H $\quad \uparrow$ H

Since H is a subgroup of G. H is closed.

$\therefore a^r \in H$.

If $r \neq 0$. This a contradiction;

since m is the smallest +ve integer such that $a^m \in H$. and now $a^r \in H$ with $r < m$.

$\therefore r = 0$,

$\therefore b = a^n = (a^m)^q \cdot a^r$

$b = (a^m)^q$

(ie) If $b \in H$ then $b = (a^m)^q$, $q \in \mathbb{Z}$

So $H = \langle a^m \rangle$.

$\therefore$ H is cyclic.

Cosets and Lagrange's

Defn Let H be a subgroup of a group G. Let $a \in G$. Then the set $aH = \{ah / h \in H\}$ is called the left Coset of H defined by a in G.

by

$Ha = \{ha / h \in H\}$ is called the right coset of H defined by a.

Ex $G = (\mathbb{Z}, +)$ is a group

$H = (5\mathbb{Z}, +)$ is subgroup of $G = (\mathbb{Z}, +)$.

The left cosets $(5\mathbb{Z}, +)$ are.

$0 + 5\mathbb{Z} = 5\mathbb{Z}$

$1 + 5\mathbb{Z} = \{1 + 5n / n \in \mathbb{Z}\}$.

$2 + 5\mathbb{Z} = \{2 + 5n / n \in \mathbb{Z}\}$

...

$G = (Z_{12}, \oplus) = G$ and $H = \{0, 4, 8\}$. is a subgroup of G.

The left cosets of H are

$0 + H = \{0, 4, 8\} = H$

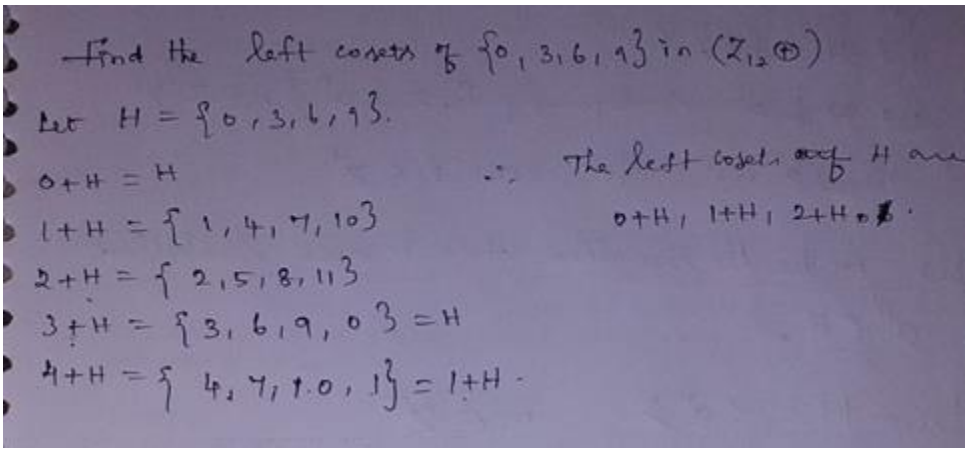
$1 + H = \{1, 5, 9\} =$

$2 + H = \{2, 6, 10\}$

$3 + H = \{3, 7, 11\}$.

$4 + H = \{4, 8, 0\} = H$.

$5 + H = \{5, 9, 1\} = 1 + H$ etc.



Staff in charge