

# Chapter 1

## GROUPS AND RINGS

### Binary Operation :-

Let  $S$  be a non-empty set. A Binary Operation  $*$  on  $S$  is a function  $*: S \times S \rightarrow S$ . The image of any ordered pair  $(a, b)$  of elements of  $S$  under  $*$  is denoted by  $a * b$ .

The Number sets are

$N$  = the set of positive integers.  $= \{1, 2, 3, \dots\}$

$Z$  = the set of integers  $= \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$

$Q$  = the set of rational numbers

$$= \left\{ \frac{p}{q} \mid p, q \in Z, q \neq 0 \right\}$$

$R$  = the set of real numbers.

$C$  = the set of complex numbers.

$$= \{a + ib \mid a, b \in R\}.$$

Thus  $(N, +)$ ,  $(Z, +)$ ,  $(Q, +)$ ,  $(R, +)$  and  $(C, +)$  are algebraic systems.

Let  $S = \{0, 1, 2\}$ . A Binary Operation  $*$  on  $S$  is defined by  $0 * 0 = 0$ ,  $0 * 1 = 1 * 0 = 1$ ,  $0 * 2 = 2 * 0 = 0$ .

$$1 * 1 = 2, 1 * 2 = 2 * 1 = 1, 2 * 2 = 1.$$

The result of the operation can be displayed as a two way table.

The table is

$*$	0	1	2
0	0	1	0
1	1	2	0
2	0	1	1

This table is called the multiplication table or operation table or cayley table.

(1) Associative property:

A Binary operation  $*$  on  $S$  is said to be associative if  $a*(b*c) = (a*b)*c \quad \forall a, b, c \in S$ .

(2) Commutative property:

A Binary operation  $*$  on  $S$  is said to be Commutative if  $a*b = b*a \quad \forall a, b \in S$

(3) Existence of Identity:

A Binary operation  $*$  on  $S$  is said to have an identity element  $e \in S$  if  $e*a = a*e = a \quad \forall a \in S$ .

(4) Existence of inverse:

Let  $*$  be a binary operation on  $S$  with an identity element  $e$  in  $S$ . An element  $a \in S$  is said to have an inverse  $a' \in S$  if  $a*a' = a'*a = e$ .

(5) Closure property:

Let  $*$  be a binary operation on  $S$  and  $A$  be a subset of  $S$ .  $A$  is said to be closed under  $*$  if  $a*b \in A \quad \forall a, b \in A$ .

(6) Group:

A non-empty set  $G$  with a binary operation  $*$  defined on it is called a group if the following axioms are satisfied. Let  $*$  be a binary operation on  $S$  and  $A$  be a subset of  $S$ .  $A$  is said to be closed under  $*$  if  $a*b \in A \quad \forall a, b \in A$ .

1. Associativity:

For all  $a, b, c \in G$ , we have  $a*(b*c) = (a*b)*c$ .

## 2. Identity:

There exists an element  $e \in G$  such that  
 $a * e = e * a = a \quad \forall a \in G$ .

## 3. Inverse:

For each  $a \in G$ , there exists an element  $a'$  such that  $a * a' = a' * a = e$ .

The group is denoted by  $(G, *)$  the set and the binary operation.

## Order of a Group:

Let  $G$  be a group under the operation  $*$ . The number of elements in  $G$  is called the order of Group  $G$  and is denoted by  $O(G)$ .

If  $G$  has  $n$  elements, then  $O(G) = n$ .

If the  $O(G)$  is finite, then  $G$  is called a finite group, otherwise it is an infinite group.

## Abelian group:

A group  $(G, *)$  is said to be abelian or commutative if  $a * b = b * a \quad \forall a, b \in G$ .

THEOREM 1: Let  $(G, *)$  be a group, then (i) identity element is unique (ii) For each  $a \in G$ , inverse is unique.

Proof: - Given  $(G, *)$  is a group.

(i) Let  $e$  and  $e'$  be two identity elements of  $G$ . Then by identity axiom (2) of a group we get.

$$e * e' = e \quad [\text{treating } e' \text{ as identity}]$$

$$\text{and } e * e' = e' \quad [\text{treating } e \text{ as "}]$$

$e = e'$   
 Hence identity element is unique.



(ii) Let  $e$  be the identity element of  $G$ . Let  $a \in G$  be any element. Suppose  $a'$  and  $a''$  are two inverses of  $a$ , then by inverse axiom,

$$a * a' = a' * a = e$$

$$\text{and } a * a'' = a'' * a = e$$

$$\text{Now, } a' = a' * e \quad [\because e \text{ is identity}]$$

$$= a' * (a * a'') \quad [\because a * a'' = e]$$

$$= (a' * a) * a'' \quad [\text{by associative axiom}]$$

$$= e * a'' \quad [\because a' * a = e]$$

$$= a''.$$

## THEOREM 2

In a group  $(G, *)$  the cancellation laws hold.

For all  $a, b, c \in G$ .

$$(i) a * b = a * c \Rightarrow b = c \quad [\text{Left cancellation law}]$$

$$(ii) b * a = c * a \Rightarrow b = c \quad [\text{Right cancellation law}].$$

Proof: Given  $(G, *)$  is a group. Let  $e$  be the identity element of  $G$ .

$$(i) \text{ Given } a * b = a * c$$

Let  $a^{-1}$  be the inverse of  $a$ .  
premultiplying by  $a^{-1}$ , we get.

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$

$$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c \quad [\text{by associative}]$$

$$\Rightarrow e * b = e * c \quad [\text{by inverse}]$$

$$\Rightarrow b = c \quad [\text{by identity}]$$

$$(ii) \text{ Given } b * a = c * a$$

$$\Rightarrow (b * a) * a^{-1} = (c * a) * a^{-1} \quad [\text{post multiplying by } a^{-1}].$$



$$\Rightarrow b * (a * a^{-1}) = c * (a * a^{-1}) \quad [\text{by associative}]$$

$$\Rightarrow b * e = c * e \quad [\text{by inverse}]$$

$$\Rightarrow b = c \quad [\text{by identity}]$$

**THEOREM 3** In a group  $(G, *)$  the equation  $a * x = b$  and  $y * a = b$  have unique solutions for the unknowns  $x$  and  $y$  as  $x = a^{-1} * b$ ,  $y = b * a^{-1}$ , where  $a, b \in G$ .

Proof: Given  $(G, *)$  is a group and let  $e$  be the identity element of  $G$  and  $a^{-1}$  be the inverse of  $a$ .

$$\text{Given } a * x = b$$

$$\Rightarrow a^{-1} * (a * x) = a^{-1} * b. \quad [\text{premultiplying by } a^{-1}]$$

$$\Rightarrow (a^{-1} * a) * x = a^{-1} * b \quad [\text{by associative}]$$

$$\Rightarrow e * x = a^{-1} * b \quad [\text{by inverse}]$$

$$\Rightarrow x = a^{-1} * b \quad [\text{by identity}]$$

Thus  $x = a^{-1} * b \in G$  is a solution.

We shall now prove the uniqueness.

Suppose,  $x_1, x_2 \in G$  be two solutions of  $a * x = b$  then

$$a * x_1 = b \quad \text{and} \quad a * x_2 = b$$

$$a * x_1 = a * x_2$$

$$\Rightarrow x_1 = x_2 \quad [\text{by left cancellation laws}]$$

Hence the solution is unique and the unique solution is  $x = a^{-1} * b$ .

Similarly we can prove that  $y * a = b$  has unique solution  $y = b * a^{-1}$ .

$$\text{Now } y * a = b$$

$$\Rightarrow (y * a) * a^{-1} = b * a^{-1} \quad [\text{post-multiplying by } a^{-1}]$$

$$\Rightarrow (y * (a * a^{-1})) = b * a^{-1} \quad [\text{by associative}]$$

$$y * e = b * a^{-1}$$

$$y = b * a^{-1}$$

$y = b * a^{-1} \in G$  is a solution.

We shall now prove the uniqueness.

Let  $y_1, y_2$  be two solutions of  $y * a = b$ .

$$y_1 * a = b \quad \text{and} \quad y_2 * a = b.$$

$$\Rightarrow y_1 * a = y_2 * a$$

$$\Rightarrow y_1 = y_2 \quad [\text{by right cancellation law}]$$

Hence the solution is unique and the unique solution is  $y = b * a^{-1}$ .

**THEOREM 4** Let  $(G, *)$  be a group, then

(i) for each  $a \in G, (a^{-1})^{-1} = a$ .

(ii) for all  $a, b \in G, (a * b)^{-1} = b^{-1} * a^{-1}$ .

Proof: (i) Let  $a \in G$ , then  $a^{-1}$  is the inverse of  $a$  and  $(a^{-1})^{-1}$  is the inverse of  $a^{-1}$ .

$$\therefore a * a^{-1} = a^{-1} * a = e \quad [\text{by inverse}]$$

$$\text{and } a^{-1} * (a^{-1})^{-1} = (a^{-1})^{-1} * (a^{-1}) = e \quad [\text{by inverse}]$$

$$\therefore a^{-1} * a = a^{-1} * (a^{-1})^{-1}$$

$$\Rightarrow a = (a^{-1})^{-1}$$

[by left-cancellation law]

(ii) we have to prove that the inverse of  $a * b = b^{-1} * a^{-1}$

consider  $(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$  [by associative law.

$$= a * e * a^{-1} \quad [\because b * b^{-1} = e]$$

$$= a * a^{-1} = e \quad [\because a * a^{-1} = e]$$

$$\begin{aligned}\text{Now consider, } (b^{-1} * a^{-1}) * (a * b) &= b^{-1} * (a^{-1} * a) * b \\ &= b^{-1} * e * b \\ &= b^{-1} * b = e\end{aligned}$$

$$\text{Thus } (a * b) * (b^{-1} * a^{-1}) = (b^{-1} * e^{-1}) * (a * b) = e$$

Hence  $b^{-1} * a^{-1}$  is the inverse of  $a * b$

$$\therefore (a * b)^{-1} = b^{-1} * a^{-1}.$$

### Worked Examples.

① Let  $G = \{1, -1\}$ . prove that  $G$  is a group under usual multiplication.

Soln: Given  $G = \{1, -1\}$  and the binary operation is usual multiplication. Since  $G$  is a finite set, we form cayley table and verify the axioms of the group.

cayley table is

$\cdot$	1	-1
1	1	-1
-1	-1	1

Closure:

The body of the table contains only elements of  $G$ . So  $G$  is closed under multiplication.

Associativity: Since multiplication is associative in any number set, it is true here also. Hence it is satisfied.

Identity: 1 is the identity element.

Inverse: Inverse of 1 is 1 and inverse of -1 is -1

so  $(G, \cdot)$  is a group.

Further it is abelian group, since  $\cdot$  is commutative.



Ex ② Let  $G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$ , Show

that  $G$  is a group under the operation of matrix multiplication.

Soln:- Let  $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ,  $A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$

$B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ ,  $C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

$\therefore G = \{I, A, B, C\}$ . Since it is finite set we shall form Cayley table and verify the axioms of a group.

$I$  is the identity element.

$A \cdot I = I \cdot A = A$ ,  $B \cdot I = I \cdot B = B$ ,  $C \cdot I = I \cdot C = C$

$\Rightarrow A^2 = A \cdot A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

$A \cdot B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = C$

$A \cdot C = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = B$

$\Rightarrow B^2 = B \cdot B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

$\Rightarrow C^2 = C \cdot C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

$B \cdot C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = A$

$CA = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = B$

Similarly  $BA = C$ ,  $CB = A$ .

∴ Cayley table is

$\cdot$	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

Closure:

The body of the table contains only all the elements of  $G$ . So  $G$  is closed under matrix multiplication.

Associative: since matrix multiplication is associative it is true for  $G$  also, so associative axiom is satisfied.

Identity:  $I$  is the identity element.

Inverse: Inverse of  $A$  is  $A$ ,  $B$  is  $B$ ,  $C$  is  $C$ .

So  $(G, \cdot)$  is a group under matrix multiplication.

Further elements equidistant from the main diagonal are same and hence the operation is commutative. Therefore  $(G, \cdot)$  is abelian.

Note: This is an example of a famous group called Klein's four group  $A^2 = B^2 = C^2 = I$ .

$$AB = BA = C; \quad BC = CB = A \quad \text{and} \quad AC = CA = B.$$

③ Show that the set of all non-zero real numbers is an abelian group under the operation  $*$  defined by  $a * b = \frac{ab}{2}$ .

soln:- Let  $G$  be the set of all non-zero real numbers.

∴  $G = \mathbb{R} - \{0\}$ , where  $\mathbb{R}$  is the set of real numbers.

The operation  $*$  on  $G$  is defined by  $a * b = \frac{ab}{2} \quad \forall a, b \in G$

closure:  $a * b = \frac{ab}{2}$ , where  $a$  and  $b$  are non-zero real numbers and so  $\frac{ab}{2}$  is non-zero.

$$\therefore \frac{ab}{2} \in G_1 \Rightarrow a * b \in G_1 \quad \forall a, b \in G_1$$

Hence  $G_1$  is closed under  $*$ .

Associativity: For any  $a, b, c \in G_1$

$$a * (b * c) = a * \frac{bc}{2} = \frac{a \left( \frac{bc}{2} \right)}{2} = \frac{a(bc)}{4}$$

$$\text{and } (a * b) * c = \left( \frac{ab}{2} \right) * c = \frac{\left( \frac{ab}{2} \right) c}{2} = \frac{a(bc)}{4}$$

$\therefore$  usual multiplication is associative.

$$\therefore a * (b * c) = (a * b) * c \quad \forall a, b, c \in G_1$$

So associative axiom is satisfied.

Identity: Suppose  $e \in G_1$  be the identity, then  $a * e = a \quad \forall a \in G_1$

$$\Rightarrow \frac{ae}{2} = a \Rightarrow \frac{e}{2} = 1 \Rightarrow e = 2 \quad [\because a \neq 0]$$

So, identity is 2.

Inverse: Let  $a$  be any element of  $G_1$ . Suppose  $a'$  is its inverse then,

$$a * a' = 2 \Rightarrow \frac{aa'}{2} = 2 \Rightarrow a' = \frac{4}{a} \quad [\because a \neq 0]$$

So, for every element  $a \in G_1$  inverse is  $\frac{4}{a}$ .

Thus inverse axiom is satisfied.

Commutative: Let  $a, b$  be any two elements of  $G_1$ , then

$$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a \quad [\text{usual multiplication is commutative}]$$

Hence  $(G_1, *)$  is an abelian group.

- ④ If  $S$  is the set of all ordered pairs  $(a, b)$  of real numbers with the binary operation  $\oplus$  defined by  $(a, b) \oplus (c, d) = (a+c, b+d)$ , where  $a, b, c, d$  are real numbers, prove that  $(S, \oplus)$  is a commutative group.

Soln:

$$\text{Given } S = \{(a, b) \mid a, b \in \mathbb{R}\}$$



closure: Let  $x, y \in S$ , then  $x = (a, b)$ ;  $y = (c, d)$

where  $a, b, c, d \in \mathbb{R}$

$$\text{Now } x \oplus y = (a, b) \oplus (c, d) = (a+c, b+d)$$

Since  $a, b, c, d$  are real numbers,  $a+c, b+d$  are real numbers.

Hence  $(a+c, b+d) \in S \Rightarrow x \oplus y \in S$

So,  $S$  is closed under  $\oplus$

Associativity: Let  $x, y, z$  be any three elements in  $S$ .

Then  $x = (a, b)$ ,  $y = (c, d)$ ,  $z = (p, q)$ .

where  $a, b, c, d, p, q$  are some real numbers.

$$\text{Now } x \oplus (y \oplus z) = (a, b) \oplus ((c, d) \oplus (p, q))$$

$$= (a, b) \oplus (c+p, d+q)$$

$$= (a + (c+p), b + (d+q))$$

$$= ((a+c) + p, (b+d) + q) \rightarrow \textcircled{1}$$

( $\because$  usual addition is associative)

$$\text{and } (x \oplus y) \oplus z = ((a, b) \oplus (c, d)) \oplus (p, q)$$

$$= (a+c, b+d) \oplus (p, q)$$

$$= ((a+c) + p, (b+d) + q) \rightarrow \textcircled{2}$$

From  $\textcircled{1}$  and  $\textcircled{2}$

$$x \oplus (y \oplus z) = (x \oplus y) \oplus z \quad \forall x, y, z \in S.$$

So associative axiom is satisfied.

Identity: Let  $x = (a, b)$  be any element in  $S$ .

Suppose  $e = (c, d)$  be the identity element in  $S$ ,

$$\text{then } x \oplus e = x$$

$$\Rightarrow (a, b) \oplus (c, d) = (a, b)$$

$$\Rightarrow (a+c, b+d) = (a, b)$$

$$\Rightarrow a+c = a, \quad b+d = b$$

$$\Rightarrow c=0, \quad d=0. \quad \therefore e = (0, 0) \text{ is identity element of } S.$$

Inverse: Let  $x = (a, b)$  be any element of  $S$ .

Suppose  $x' = (c, d)$  be the inverse,

then  $x \oplus x' = e$

$$\Rightarrow (a, b) \oplus (c, d) = (0, 0)$$

$$\Rightarrow (a+c, b+d) = (0, 0)$$

$$\Rightarrow a+c=0, b+d=0$$

$$\Rightarrow c=-a, d=-b$$

$\therefore x' = (-a, -b)$  is the inverse of  $x$ .

So, inverse axiom is satisfied.

Commutativity: Let  $x = (a, b)$  and  $y = (c, d)$  be any two elements on  $S$ .

$$\text{Now } x \oplus y = (a, b) \oplus (c, d)$$

$$= (a+c, b+d)$$

$$= (c+a, d+b) \quad \text{[Since addition is commutative]}$$

$$= (c, d) \oplus (a, b) \quad \text{[By definition of } \oplus \text{]}$$

$$= y \oplus x$$

$$\therefore x \oplus y = y \oplus x \quad \forall x, y \in S$$

Hence  $(S, \oplus)$  is a commutative group.

(i.e),  $(S, \oplus)$  is an abelian group.

## PERMUTATION

Let  $S$  be a non-empty set. A bijective function  $f: S \rightarrow S$  is called a permutation. If  $S$  has  $n$  elements, then the permutation is said to be of degree  $n$ .

Usually we take  $S = \{1, 2, 3, \dots, n\}$

The set of all permutations on a set of  $n$  symbols is denoted by  $S_n$ .

Q. If  $S = \{1, 2, 3\}$ , then prove that  $(S_3, \cdot)$  is a non-abelian group, where  $\cdot$  is composition of function.

Soln: Given  $S = \{1, 2, 3\}$ . The total number permutation on  $S$  is  $3! = 6$ . The permutations are

$$P_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \quad P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \quad P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

$$P_4 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \quad P_5 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \quad P_6 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

Then  $S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$  and the binary operations on  $S_3$  is the composition of functions.

The operation is performed on the left as below.

$$\text{For example (1) } (P_2 \cdot P_3) = (1) \cdot P_2 \cdot P_3 \quad \begin{matrix} P_2 & P_3 \\ \text{i.e. } 1 \rightarrow 1 \rightarrow 2 \end{matrix}$$

$$= (1) P_3 = 2 \quad (1) P_2 \cdot P_3 = 2$$

Similarly for other elements.

Since (1)  $P_1 = 1$ , (2)  $P_1 = 2$ , (3)  $P_1 = 3$ ,

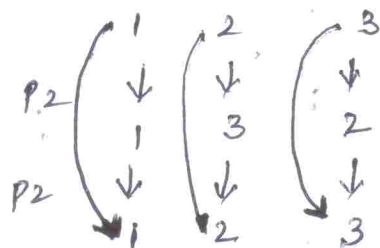
$P_1$  is the identity element on  $S$ .

$$P_1 \cdot P_1 = P_1; \quad P_1 \cdot P_2 = P_2 \cdot P_1 = P_2;$$

$$P_1 \cdot P_3 = P_3 \cdot P_1 = P_3; \quad P_1 \cdot P_4 = P_4 \cdot P_1 = P_4;$$

$$P_1 \cdot P_5 = P_5 \cdot P_1 = P_5; \quad P_1 \cdot P_6 = P_6 \cdot P_1 = P_6.$$

$$P_2 \cdot P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = P_1.$$

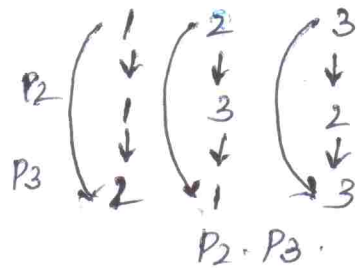


$P_2 \cdot P_2$



$$P_2 \cdot P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = P_1.$$

$$P_2 \cdot P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = P_4.$$



$$\therefore P_2 \cdot P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = P_4.$$

$$P_2 \cdot P_4 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = P_3.$$

$$P_2 \cdot P_5 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = P_6.$$

$$P_2 \cdot P_6 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = P_5.$$

$$P_3 \cdot P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = P_6.$$

$$P_3 \cdot P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = P_5.$$

$$P_3 \cdot P_4 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = P_2.$$

$$P_3 \cdot P_5 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = P_1.$$

$$P_3 \cdot P_6 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = P_4.$$

$$P_4 \cdot P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = P_5.$$



The cayley table is,

$\cdot$	$P_1$	$P_2$	$P_3$	$P_4$	$P_5$	$P_6$
$P_1$	$P_1$	$P_2$	$P_3$	$P_4$	$P_5$	$P_6$
$P_2$	$P_2$	$P_1$	$P_4$	$P_3$	$P_6$	$P_5$
$P_3$	$P_3$	$P_6$	$P_5$	$P_2$	$P_1$	$P_4$
$P_4$	$P_4$	$P_5$	$P_6$	$P_1$	$P_2$	$P_3$
$P_5$	$P_5$	$P_4$	$P_1$	$P_6$	$P_3$	$P_2$
$P_6$	$P_6$	$P_3$	$P_2$	$P_5$	$P_4$	$P_1$

Closure: Since the body of the table contains only the elements of  $S_3$ ,  $S_3$  is closed with respect to  $\cdot$ .

Associativity: We know composition of functions is associative and so it is true in  $S_3$  also. So associative axiom is verified.

Identity:  $P_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$  is the identity element of  $S_3$ .

Inverse: To find the inverse of an element  $P_i$ , find  $P_j$  in the row through  $P_i$ , the column head of  $P_j$  is the inverse of  $P_i$  i.e.  $P_i^{-1}$ .

from the table we see that

$$P_1^{-1} = P_1, \quad P_2^{-1} = P_2, \quad P_3^{-1} = P_5, \quad P_4^{-1} = P_4$$

$$P_5^{-1} = P_3, \quad P_6^{-1} = P_6.$$

Thus inverse exists for every element. Hence inverse axiom is verified. So  $(S_3, \cdot)$  is a group.



From the table we find that,

$$P_3 \cdot P_4 = P_2 \text{ and } P_4 \cdot P_3 = P_6.$$

$$\therefore P_3 \cdot P_4 \neq P_4 \cdot P_3.$$

Hence the group is not commutative.

## GROUP OF RESIDUE CLASSES Mod n

### Congruence mod n

Let  $n$  be a fixed positive integer. Let  $a$  and  $b$  be integers, we define  $a \equiv b \pmod{n}$ , if  $a-b$  is divisible by  $n$ .

For example,  $2 \equiv -1 \pmod{3}$ ,

since  $2 - (-1) = 3$  is divisible by 3.

$25 \equiv 5 \pmod{2}$ , since  $25 - 5 = 20$  is divisible by 2.

$-1 \equiv 3 \pmod{2}$ , since  $-1 - 3 = -4$  is divisible by 2.

The equivalence class of  $a$  is  $[a] = \{x \mid x \equiv a \pmod{n}\}$

For eg, the congruence classes mod 4 are

$$[0] = \{\dots, -8, -4, 0, 4, 8, \dots\}$$

$$[1] = \{\dots, -7, -3, 1, 5, 9, \dots\}$$

$$[2] = \{\dots, -6, -2, 2, 6, 10, \dots\}$$

$$[3] = \{\dots, -5, -1, 3, 7, 11, \dots\}$$

$$[4] = \{\dots, -8, -4, 0, 4, 8, \dots\} = [0]$$

similarly  $[5] = [1]$ ,  $[6] = [2]$  etc..

$\therefore$  The distinct congruence classes mod 4 are

$$[0], [1], [2], [3].$$

The set of congruence classes mod 4 is denoted by,

$Z_4 = \{[0], [1], [2], [3]\}$  and is called the set of residue classes mod 4 or residual classes mod 4.

more generally, the set of residue classes mod  $n$  is  $Z_n = \{[0], [1], [2], \dots, [n-1]\}$ .

- ⑨ Let  $Z_5^* = \{[1], [2], [3], [4]\}$  be the non-zero elements of  $Z_5$ .  
Prove that  $(Z_5^*, \cdot_5)$  is an abelian group.

Soln:  $Z_5^* : \{[1], [2], [3], [4]\}$

We form the Cayley table to verify axioms of a group.

$$[2] \cdot_5 [2] = [4].$$

$$[2] \cdot_5 [3] = [6] = [1] \quad [\because 6 \equiv 1 \pmod{5}]$$

ie the remainder when 6 is  $\div$  by 5 is 1

$$[2] \cdot_5 [4] = [8] = [3] \quad [\because 8 \equiv 3 \pmod{5}]$$

$$[3] \cdot_5 [2] = [6] = [1] \quad [\because 6 \equiv 1 \pmod{5}]$$

$$[3] \cdot_5 [3] = [9] = [4] \quad [\because 9 \equiv 4 \pmod{5}]$$

$$[3] \cdot_5 [4] = [12] = [2] \quad [\because 12 \equiv 2 \pmod{5}]$$

$$[4] \cdot_5 [1] = [4].$$

$$[4] \cdot_5 [2] = [8] = [3] \quad [\because 8 \equiv 3 \pmod{5}]$$

$$[4] \cdot_5 [3] = [12] = [2] \quad [\because 12 \equiv 2 \pmod{5}]$$

$$[4] \cdot_5 [4] = [16] = [1] \quad [\because 16 \equiv 1 \pmod{5}]$$

The Cayley table is

$\cdot_5$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[4]$	$[3]$	$[2]$	$[1]$

Closure: The body of table contains only elements of  $\mathbb{Z}_5$   
 $\therefore \mathbb{Z}_5^*$  is closed w.r to  $\cdot_5$

Associativity: Since usual multiplication is associative, it is true in  $\mathbb{Z}_5^*$  also.

Identity:  $[1]$  is the identity element, since  $[1] \cdot_5 [a] = [a] \quad \forall a \in \mathbb{Z}_5^*$

$$\text{ie } [1] \cdot_5 [1] = [1]; \quad [1] \cdot_5 [2] = 2,$$

$$[1] \cdot_5 [3] = [3]; \quad [1] \cdot_5 [4] = 4$$

Inverse: From the table we note that

inverse of  $[1]$  is  $[1]$ ; inverse of  $[2]$  is  $[3]$

inverse of  $[3]$  is  $[2]$ ; inverse of  $[4]$  is  $[4]$ .

Further, the elements equidistant from the main diagonal are same and so  $\cdot_5$  is commutative in  $\mathbb{Z}_5^*$ . So  $(\mathbb{Z}_5^*, \cdot_5)$  is an abelian group.

(10) Show that if every element in a group  $G$  is its own inverse, then the group  $G$  must be abelian.

(or)

In a group  $G$ , if  $a^2 = e \quad \forall a \in G$ , then  $G$  is abelian.

Soln:

Let  $a, b \in G$  be any two elements, then

$a^* b \in G$ . Given every element is its own inverse,

$$\begin{aligned} \therefore a^{-1} &= a, \quad b^{-1} = b \quad \text{and} \quad (a * b)^{-1} = a * b \\ &\Rightarrow b^{-1} * a^{-1} = a * b \\ &\Rightarrow b * a = a * b \quad \forall a, b \in G \\ \therefore G &\text{ is abelian.} \end{aligned}$$

note: 1. consider the second part.

$$\begin{aligned} \text{Given } a^2 &= e \quad \forall a \in G \\ \therefore a^{-1} * a^2 &= a^{-1} * e \\ &\Rightarrow (a^{-1} * a) * a = a^{-1} * e. \\ &\Rightarrow a = a^{-1} \quad \forall a \in G \quad [\because a^{-1} * a = e] \end{aligned}$$

ie, every element is its own inverse. How  $G$  is abelian by first part.

2. Is the converse true?

ie. If  $G$  is abelian, that every element is its own inverse

Ans: No. For example,  $(\mathbb{Z}, +)$  is an abelian group. But inverse of 2 is -2 and not 2.

3. Let  $(G, *)$  be a group. An element  $a \in G$  is called an independent element if  $a^2 = a$

Then  $a^{-1} = a^2 = a^{-1} * a \Rightarrow a = e$ . so, the only independent element in a group is the identity element.



- ⑭ Let  $f$  and  $g$  be the permutations of the elements of  $\{1, 2, 3, 4, 5\}$  given by  $f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix}$  and  $g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{bmatrix}$  find  $gf^2g^{-1}$  and  $g^{-1}fgf^{-1}$  [AU 2001]

Soln:

Given  $f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix}$ ,  $g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{bmatrix}$

then  $f^{-1} = \begin{bmatrix} 2 & 3 & 1 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix}$

[Reversing  $f$  we get  $f^{-1}$ ]

$g^{-1} = \begin{bmatrix} 5 & 4 & 3 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{bmatrix}$

$f^2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix}$

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

$\therefore gf^2g^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{bmatrix}$   
 $= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{bmatrix}$

$g^{-1}fgf^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix}$   
 $= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{bmatrix}$

- ⑮ If  $f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$  and  $g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{bmatrix}$  find  $f^{-1}gf$  and  $gfg^{-1}$ .

Soln:-

Given  $f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$  and  $g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{bmatrix}$

are permutations on four symbols

$$\therefore f^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$g^{-1} = \begin{pmatrix} 3 & 1 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

$$\therefore f^{-1}gf = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

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

and  $gf g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

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

⑩ If  $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$  and  $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$  are permutations, prove that  $(g \cdot f)^{-1} = f^{-1} \cdot g^{-1}$ . (AU 2006)

Soln

Given  $f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix}$  and  $g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$

$$g \cdot f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$$

$$(g \cdot f)^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \rightarrow \textcircled{1}$$

Now  $f^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix}$ ,  $g^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix}$

$$\therefore f^{-1} \cdot g^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$$

from ① and ② we get,

$$(g \cdot f)^{-1} = f^{-1} \cdot g^{-1}.$$

(17)

If  $f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{bmatrix}$  and  $h = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{bmatrix}$  are permutations on the set  $A = \{1, 2, 3, 4, 5\}$ , find a permutation  $g$  on  $A$  such that  $f \cdot g = h \cdot f$ .

Soln: Given  $f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{bmatrix}$ ,  $h = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{bmatrix}$  are permutations on five symbols  $A = \{1, 2, 3, 4, 5\}$ .

so, they are bijective function on  $A$  and  $f^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{bmatrix}$   
we have to find  $g$  such that  $f \cdot g = h \cdot f$ .

Now,  $f \cdot g = h \cdot f \Rightarrow f^{-1} \cdot (f \cdot g) = f^{-1} \cdot (h \cdot f)$ .

$\Rightarrow (f^{-1} \cdot f) \cdot g = f^{-1} \cdot (h \cdot f)$  [composition of functions is associative]

$$\Rightarrow I_A \cdot g = f^{-1} \cdot (h \cdot f)$$

$$\Rightarrow g = f^{-1} \cdot (h \cdot f)$$

$$\begin{aligned} g &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{bmatrix}. \end{aligned}$$

(18)

Prove that the set of all matrices  $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$  forms an abelian group with respect to matrix multiplication, where  $a$  and  $b$  are real numbers, not both 0.

Soln: Let  $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R}, a \neq 0 \text{ or } b \neq 0 \right\}$

we verify the group axioms.  $*$  is matrix multiplication.

1. Closure: Let  $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ ,  $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$  be any two elements of  $G$ . Not both  $a, b$  zero and not  $c, d$  zero (i.e)  $a^2 + b^2 \neq 0$  and  $c^2 + d^2 \neq 0$ .

$$A * B = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac - bd & ad + bc \\ -bc - ad & -bd + ac \end{bmatrix}$$

$$= \begin{bmatrix} x & y \\ -y & x \end{bmatrix}, \text{ where } \begin{matrix} x = ac - bd \\ y = ad + bc \end{matrix} \text{ are real numbers.}$$

$$\begin{aligned} \text{and } x^2 + y^2 &= (ac - bd)^2 + (ad + bc)^2 \\ &= a^2c^2 + b^2d^2 - 2abcd + a^2d^2 + b^2c^2 + 2abcd \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\ &= (a^2 + b^2)(c^2 + d^2) \neq 0 \end{aligned}$$

$$\therefore \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \in G \Rightarrow A * B \in G$$

$\therefore G$  is closed under  $*$ .

2. Associativity: We know matrix multiplication is associative. Hence it is true in  $G$  also.

3. Identity: Let  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  in  $G$  be the Identity element,  
Since  $A * I = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} * \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = A$ .

$$\text{and } I * A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} * \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = A.$$

4. Inverse: Let  $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$  be an element in  $G$ .

$$\text{where } a^2 + b^2 \neq 0. \text{ Suppose } A' = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}.$$

be the inverse  $A$  then  $A * A' = I$ .



$$\Rightarrow \begin{bmatrix} a & b \\ -b & a \end{bmatrix} * \begin{bmatrix} x & y \\ -y & x \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

$$\Rightarrow \begin{bmatrix} ax-by & ay+bx \\ -bx-ay & -by+ax \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\therefore ax-by=1 \rightarrow \textcircled{1} \text{ and } ay+bx=0 \rightarrow \textcircled{2}$$

$$(1) \quad x a \Rightarrow a^2 x - aby = a$$

$$(2) \quad x b \Rightarrow b^2 x + aby = 0.$$

$$\text{Adding, } (a^2+b^2)x = a \Rightarrow x = \frac{a}{a^2+b^2} \quad [\because a^2+b^2 \neq 0]$$

$$(2) \Rightarrow ay = -bx \Rightarrow y = \frac{-b}{a} \cdot \frac{a}{a^2+b^2} = \frac{-b}{a^2+b^2}.$$

$$\therefore A^{-1} = \begin{bmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{bmatrix}$$

$$\text{Now } x^2+y^2 = \frac{a^2}{(a^2+b^2)^2} + \frac{b^2}{(a^2+b^2)^2} = \frac{a^2+b^2}{(a^2+b^2)^2} = \frac{1}{a^2+b^2} \neq 0.$$

$$A^{-1} \in G.$$

Hence inverse exists.

Commutative: Let  $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ ,  $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$  be any elements in  $G$ , then  $A * B = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} * \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$

$$= \begin{bmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{bmatrix}.$$

$$\text{and } B * A = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} * \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{bmatrix}$$

$$\therefore A * B = B * A \quad \forall A, B \in G.$$

Hence  $(G, *)$  is an abelian group.

## MODULAR SYSTEM:-

In this set, we define the addition modulo  $n$  by  
 $a +_n b = r, 0 \leq r < n$ .

(i.e)  $r$  is the remainder when  $a+b$  is divided by  $n$ .

Multiplication mod  $n$  is  $a \cdot_n b = r, 0 \leq r < n$ ,

(i.e)  $r$  is the remainder when  $ab$  is divided by  $n$ .

For eg, if  $n=6$ , the set is  $\{0, 1, 2, 3, 4, 5\}$

$2 +_6 5 = 1$ , since when  $2+5=7$  is divided by 6, the remainder is 1 and  $3 \cdot_6 4 = 0$ , since when  $3 \times 4 = 12$  is divided by 6, the remainder is 0.

(19) Show that the set  $G = \{0, 1, 2, 3, 4, 5\}$  is group under addition modulo 6.

Soln: Given  $G = \{0, 1, 2, 3, 4, 5\}$  is the modulo set we have to prove that  $(G, +_6)$  is a group.

We form the cayley table and verify the group axioms

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Closure:- The body of the table contains only elements of  $G$  once in each row and column. So,  $G$  is closed under  $+_6$ .

Associativity: Since usual addition is associative,  $+_6$  is associative.

Inverse: Inverse of 0 is 0, Inverse of 1 is 5  
 " " 2 is 4, " " 3 is 3  
 " " 4 is 2, " " 5 is 1.

Further  $a +_6 b = b +_6 a \quad \forall a, b \in G$ , since the elements equidistant from the main diagonal are the same.

$\therefore (G, +_6)$  is an abelian group.

Why,  $G = \{0, 1, 2, 3, \dots, n-1\}$  is a group under  $+_n$ .

Note:

But  $G$  is not a group under  $\cdot_6$ .

The cayley table is given below.

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	3	0	4	3
5	0	5	4	3	2	1

In the body of the table, the elements are repeated in some of the rows and columns.

For a group, there should <sup>not</sup> be repetition in any row or column. So  $(G, \cdot_6)$  is not a group.

If  $n=p$  is a prime, then the non-zero modular set  $\{1, 2, 3, \dots, p-1\}$  is a group under multiplication mod  $p$ .

### SUBGROUP

Let  $(G, *)$  be a group. A non-empty subset  $H$  of  $G$  is said to be a subgroup of  $G$  if  $H$  itself is a group under the same operation  $*$  of  $G$ .

It is obvious  $\{e\}, (*)$  and  $\{G, (*)$  are subgroups of  $(G, *)$ . These two subgroups are called trivial subgroups of  $(G, *)$ . All other subgroups of  $(G, *)$  are called non-trivial subgroups.

The non-trivial subgroups are also known as proper subgroups.

**THEOREM 1** :- A non-empty subset  $H$  of a group  $(G, *)$  is a subgroup of  $G$  if and only if  $a * b^{-1} \in H \quad \forall a, b \in H$   
[Ar 2008, 2012]

Proof: Let  $H$  be a subgroup of  $G$ .

Then  $H$  itself is a group under  $*$ .

$$\therefore a, b \in H \Rightarrow a, b^{-1} \in H$$

Hence  $a * b^{-1} \in H$ , by closure.

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

We have to prove  $H$  is a subgroup of  $G$ . So, we have to verify the axioms.

Since  $H$  is non-empty, there exists an element  $a \in H$ .

Then by the given condition  $a * a^{-1} \in H \Rightarrow e \in H$ .

So, identity exists in  $H$ .

If  $x \in H$  is any element, then

$$\begin{aligned} x, e \in H &\Rightarrow e * x^{-1} \in H \\ &\Rightarrow x^{-1} \in H \end{aligned}$$

$\therefore$  inverse exists in  $H$  for every element in  $H$ .

Further,  $a, b \in H \Rightarrow a, b^{-1} \in H$   $\therefore$  inverse exists in  $H$ .



$$\Rightarrow a * (b^{-1})^{-1} \in H \Rightarrow a * b \in H$$

So,  $H$  is closed under  $*$  and hence closure axiom is satisfied.

Since  $H \subset G$ , associative axiom is inherited in  $H$  so associative axiom is satisfied.

$\therefore (H, *)$  is a group and hence a subgroup of  $(G, *)$ .

NOTE: If the Binary operation of a group  $G$  is denoted by  $+$ , then the inverse of  $a$  denoted by  $-a$  instead of  $a^{-1}$ . So the condition  $a * b^{-1} \in H$  is written as  $a - b \in H$ .

Next we shall prove that a finite subset is a subgroup if closure is satisfied.

(23) If  $H_1$  and  $H_2$  are subgroups of a group  $(G, *)$  prove that  $H_1 \cap H_2$  is a subgroup of  $(G, *)$ .

Soln: Given  $H_1, H_2$  are subgroups of  $(G, *)$

Let  $a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1$  and  $a, b \in H_2$ .

Since  $H_1$  and  $H_2$  are subgroups by criterion for subgroup (Theorem 7).

$$a, b \in H_1 \Rightarrow a * b^{-1} \in H_1$$

$$\text{and } a, b \in H_2 \Rightarrow a * b^{-1} \in H_2$$

$$\therefore a * b^{-1} \in H_1 \cap H_2$$

$$\text{Thus } a, b \in H_1 \cap H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2$$

Hence  $H_1 \cap H_2$  is a subgroup of  $G$ .

NOTE: It can be extended to more than two subgroups.

If  $H_1, H_2, \dots, H_n$  are subgroups of  $G$ , then

$H_1 \cap H_2 \cap \dots \cap H_n$  is a subgroup of  $G$ .

(24) Let  $S$  be a non-empty set and  $P(S)$  denote the power set of  $S$ . Verify whether  $(P(S), \cap)$  is a group. [AU 2008]

Soln: We know that the power set  $P(S)$  is the set of all subsets of  $S$ . The binary operation on  $P(S)$  is  $\cap$ .

Let  $G = P(S)$ . We shall verify the axioms of a group.

Closure: Let  $A, B$  be any two subsets of  $S$ .

$\therefore A \cap B$  is a subset of  $S$ .

Thus  $A, B \in P(S) \Rightarrow A \cap B \in P(S)$

So  $P(S)$  is closed under  $\cap$ .

Associativity: Since  $\cap$  is associative in any collection of sets, it is true in  $P(S)$ .

So associative axiom is satisfied.

Identity: Let  $A \in P(S)$  be any element. (i.e)  $A$  is any subset of  $S$ . Then  $A \cap S = S \cap A = A$ .

$\therefore S$  is the identity element in  $P(S)$  for  $\cap$ .

Inverse: Let  $A$  be any subset of  $S$ .

Since  $S$  is the identity, it is obvious there is no subset  $B$  of  $S$  such that  $A \cap B = S$ .

So inverse axiom is not satisfied.

Hence  $(P(S), \cap)$  is not a group.

NOTE:  $(P(S), \cap)$  is only a semi-group with identity or monoid.

(25) Find all the non-trivial subgroups of  $(\mathbb{Z}_6, +_6)$

Soln:  $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$  [AU 2006]

$H_1 = \{[0], [3]\}$ ,  $H_2 = \{[0], [2], [4]\}$  are all the non-trivial subgroups of  $(\mathbb{Z}_6, +_6)$ .

$+6$	$[0]$	$[3]$
$[0]$	$[0]$	$[3]$
$[3]$	$[3]$	$[0]$

$+6$	$[0]$	$[2]$	$[4]$
$[0]$	$[0]$	$[2]$	$[4]$
$[2]$	$[2]$	$[4]$	$[0]$
$[4]$	$[4]$	$[0]$	$[2]$

Since  $H_1, H_2$  are finite subsets of  $G$ ,  $H_1$  and  $H_2$  are closed under  $+6$ ,  $(H_1, +6)$ ,  $(H_2, +6)$  are subgroups of  $(Z_6, +6)$ .

- (21) Determine  $H = \{0, 5, 10\}$  and  $K = \{0, 4, 8, 12\}$  are subgroups of the group  $(Z_{15}, +_{15})$  [AU 2007]

Soln: The modular set  $Z_{15} = \{0, 1, 2, 3, \dots, 14\}$

Given  $H = \{0, 5, 10\}$ ,  $K = \{0, 4, 8, 12\}$  are finite subsets of  $Z_{15}$ . To verify they are subgroups, it is enough to verify the closure axiom.

$+_{15}$	0	5	10
0	0	5	10
5	5	10	0
10	10	0	5

H

$+5$	0	4	8	12
0	0	4	8	12
4	4	8	12	1
8	8	12	1	5
12	12	1	5	9

K

$H$  is closed under  $+_{15}$  and so  $H$  is a subgroup. But  $K$  is not closed under  $+_{15}$ , because the body of the composition table contains elements not in  $K$ . Hence  $K$  is not a subgroup of  $Z_{15}$ .



## CYCLIC SUBGROUP

Let  $(G, *)$  be a group and  $a \in G$ . Then  $H = \{a^n \mid n \in \mathbb{Z}\}$  is a subgroup of  $G$ .  $H$  is called the cyclic subgroup of  $G$  generated by  $a$  and it is denoted by  $\langle a \rangle$  or  $\langle a \rangle$ .

In the group  $(\mathbb{Z}_{12}, +_{12})$ ,  $\{[0], [3], [6], [9]\}$  is the cyclic subgroup generated by  $[3]$ , since  $2[3] = 6$ ,  $3[3] = 9$ ,  $4[3] = 12 = [0]$ .

## CYCLIC GROUP

A Group  $(G, *)$  is said to be a cyclic group if there exists an element  $a \in G$  such that every element  $x \in G$  is of the form  $a^n$  for some integer  $n$ . The element  $a$  is called a generator of  $G$  and is written as  $G = \langle a \rangle$  or  $\langle a \rangle$ . It is read as  $G$  is cyclic group generated by  $a$ .

For eg,

The multiplicative group  $G = \{1, -1, i, -i\}$  is cyclic group generated by  $i$ , since  $i^2 = -1$ ,  $i^3 = -i$ ,  $i^4 = 1$ .

It can be seen easily that  $-i$  is another generator



1. Theorem 9: Any cyclic group is abelian.

Proof: Let  $G$  be a cyclic group generated by  $a$ .

$$\text{Then } G = \{a^n \mid n \in \mathbb{Z}\}$$

Let  $x, y \in G$  be any 2 elements then  $x = a^m$   
 $y = a^n$  for some integers  $m$  and  $n$

$$\text{Now } x * y = a^m * a^n = a^{m+n}$$

$$y * x = a^n * a^m = a^{n+m}$$

$$x * y = y * x \quad \forall x, y \in G$$

Hence  $G$  is abelian.

Note: The converse is not true (i.e) abelian group is not cyclic. eg:  $(\mathbb{Q}, +)$  is abelian but not cyclic

2. Theorem 10: Every subgroup of cyclic group is cyclic

Proof: Let  $(G, *)$  be cyclic group generated by  $a$

$$\text{Then } G = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$$

Let  $H$  be a subgroup of  $G$

Since  $H$  is subset of  $G$ , every element of  $H$  is of the form  $a^n$  for some  $n \in \mathbb{Z}$

Since  $H$  is a group if  $a^n \in H$ , then its inverse  $(a^n)^{-1} = a^{-n} \in H$ . So either  $n$  or  $-n$  is +ve integer. Hence  $H$  contains positive integer powers of  $a$ .

Let  $m$  be a least +ve integer such that  $a^m \in H$ . We shall prove  $a^m$  is generator of  $H$ . Let  $x \in H$  be any element, then  $x = a^n$  for some  $n \in \mathbb{Z}$ .

For integers ' $n$ ', ' $m$ ' by Euclidean <sup>division</sup> algorithm, we can find integers ' $q$ ' and ' $r$ ' such that  $n = mq + r$ ,  $0 \leq r < m$ .

$$\text{Then, } x = a^n = a^{mq+r} = a^{mq} * a^r = (a^m)^q * a^r$$

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

$$= e * a^r$$

$$= a^r$$

$$\therefore a^r = (a^m)^{-q} * x = a^{-mq} * x$$

Now  $a^m \in H \Rightarrow (a^m)^q \in H$ , by closure

$$\Rightarrow a^{mq} \in H$$

$$\Rightarrow a^{-mq} \in H, \text{ since } H \text{ is group}$$

$$\therefore a^{-mn} \in H, \text{ by closure}$$

$$\Rightarrow a^r \in H, \text{ where } r < m$$

If  $a \neq 0$ , then  $a^r \in H$  is a contradiction to the fact that 'm' is the least positive integer such that  $a^m \in H$

Hence  $r = 0$

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

Thus any element of  $H$  is integral power of  $a^m$ .

So  $H$  is cyclic group generated by  $a^m$   
(i.e)  $H = \langle a^m \rangle$

Theorem 11 : If  $(G, *)$  is cyclic group generated by 'a', then prove  $a^{-1}$  is also generator.

Proof: ~~Given  $G = \langle a \rangle$~~  Given  $G = \langle a \rangle$

So any element  $x \in G$  is  $x = a^n$  for some integer  $n$ .

$$\text{Now } x = a^n = (a^{-1})^{-n}$$

Thus 'x' is integral power of  $a^{-1}$  and

So  $a^{-1}$  is also a generator.

## Order of element:

Definition: Let  $(G, *)$  be a group and let  $a \in G$ . The order of 'a' is least positive integer 'm' such that  $a^m = e$ .

The order of 'a' is denoted by  $O(a)$  and we write  $O(a) = m$

If no such integer exist, then we say that 'a' is of infinite order.

Example: In group  $G = \{1, -1, i, -i\}$  under usual multiplication,  $O(i) = 4$ ,  $O(-i) = 4$  and  $O(-1) = 2$

Ans: Since  $i^2 = -1$   
 $i^4 = (-1)^2 = 1$  and  $(-1)^2 = 1$

Theorem 12: Let  $(G, *)$  be finite cyclic group generated by an element  $a \in G$ .

If  $O(a) = n$ , then  $a^n = e$  and so

$G = \{a, a^2, a^3, \dots, a^{n-1}, a^n = e\}$ . Further  $O(a) = n$  that is 'n' is least positive integer such that  $a^n = e$



Proof: Given  $(G, *)$  is finite cyclic group generated by 'a'.

First we shall prove that  $a^m = e$  is not possible for  $m < n$ .

Assume it is possible (i.e)  $a^m = e$ ,  $m < n$

Since  $G$  is cyclic group generated by 'a' any element  $x \in G$  is integral power of 'a'. (i.e)  $x = a^k$  for some integers  $k$ .

Now for integers  $m, k$  by Euclidean division, we can find integers  $q$  &  $r$  such that  $k = mq + r$ ,  $0 \leq r < m$ .

$$\therefore x = a^k = a^{mq+r} = a^{mq} * a^r = e * a^r = a^r$$

Thus any element of  $G$  is  $a^r$  for  $r < m$ . This means the no. of elements of  $G$  is at most 'm'.

(i.e)  $O(G) = m < n$ , which contradicts the hypothesis  $O(G) = n$ .

Hence  $a^m = e$  is not possible for  $m < n$

$$\therefore a^n = e$$

Next we shall prove that elements  $a, a^2, a^3, \dots, a^n$  are all distinct.

Suppose it is not true, then there are repetitions.

$$\text{let } a^s = a^r, 0 < r < s \leq n$$

$$\Rightarrow a^s * a^{-r} = a^r * a^{-r}$$

$$\Rightarrow a^{s-r} = a^0 = e, 0 < s-r < n$$

This is again a contradiction by 1st part,

$\therefore$  all elements are distinct

$\therefore a, a^2, \dots, a^n = e$  are all distinct

Since  $O(a) = n$ , it follows  $G = \{a, a^2, \dots, a^n = e\}$  and  $a^n = e$ . So  $O(a) = n$ .

## Cycles and Transpositions

Def: Let  $S = \{a_1, a_2, \dots, a_n\}$  and  $\sigma$  be permutation on  $S$ .  $\sigma$  is called cycle of length  $n$  if there exist  $n$  elements  $a_1, a_2, \dots, a_n$  such that  $\sigma(a_1) = a_2$ ,  $\sigma(a_2) = a_3, \dots, \sigma(a_{n-1}) = a_n$  and  $\sigma(a_n) = a_1$ .

This cycle is represented by symbol  $(a_1, a_2, \dots, a_n)$  or  $(a_1 a_2 \dots a_n)$

Def: Two cycles are said to be disjoint if they have no elements in common

eg:  $(1\ 2\ 3), (4\ 5)$  disjoint cycles.

Def: A cycle of length 2 is transposition

Def: If a permutation  $\sigma$  is a product of even number of transposition, then  $\sigma$  is even transposition.

If a permutation  $\sigma$  is pdt. of odd no. of transposition, then  $\sigma$  is odd transposition.

Example sum

1. Compute pdt.  $(1\ 2)(2\ 4)(3\ 6)$  as permutation on  $\{1, 2, 3, 4, 5, 6\}$ . Find (i) even/odd (ii) order

ANSWER:

$$\text{Let } \sigma = (1\ 2)(2\ 4)(3\ 6)$$

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

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

We shall write  $\sigma$  as pdt. of disjoint cycles

$$\sigma = (1\ 4\ 2)(3\ 6) \quad \begin{array}{l} 1 \rightarrow 4 \rightarrow 2 \rightarrow 1 \text{ cycles} \\ 3 \rightarrow 6 \rightarrow 3 \end{array}$$

Order of cycle (1 4 2) is 3 and the order of cycle (3 6) is 2

$$\therefore \text{Order of } \sigma = \text{lcm}\{3, 2\} = 6$$

Now to decide  $\sigma$  is odd or even, we shall write  $\sigma$  as product of transposition

$$\sigma = (1\ 4)\ (1\ 2)\ (3\ 6)$$

$\sigma$  is pdt of 3 transposition.

$\therefore \sigma$  is odd permutation

Examples 2:

Express  $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$  in  $S_9$

as a pdt. of disjoint cycles. Decide its order and test it is odd or even.

ANSWER:

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$$

We see  $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 1$

So one cycle is (1 2 3 4 5)

6 and 7 are left fixed.

$8 \rightarrow 9 \rightarrow 8$ , so another cycle (8 9)

$$\theta = (1\ 2\ 3\ 4\ 5)(8\ 9)$$



Order of  $(1\ 2\ 3\ 4\ 5)$  is 5 and order of  $(8\ 9)$  is 2.

$\therefore$  order of  $\theta = \text{lcm}(5, 2) = 10$ .

Further  $\theta = (1\ 2)(1\ 3)(1\ 4)(1\ 5)(8\ 9)$  is a pdt 5 transposition.

$\therefore \theta$  is odd permutation.

Cosets & Lagrange's theorem

Cosets: Let  $(H, *)$  be a subgroup of  $(G, *)$ .

Let  $a \in G$  be any element. Then set

$aH = \{a * h \mid h \in H\}$  is called left coset of  $H$  in  $G$  determined by 'a'.

Sometimes  $aH$  is written as  $a * H$

The set  $Ha = \{h * a \mid h \in H\}$  is called right coset of  $H$  in  $G$  determined by 'a'.

Theorem 13: Let  $(H, *)$  be a subgroup of  $(G, *)$ . Then the set of all left cosets of  $H$  in  $G$  form partition of  $G$ . That is every element of  $G$  belongs to only one left coset of  $H$  in  $G$ .

Proof: Let  $aH$  and  $bH$  be any 2 left coset.  
we shall prove either  $aH = bH$  or  $aH \cap bH = \emptyset$

Suppose  $aH \cap bH \neq \emptyset$  then there exist an element  $x \in aH \cap bH$

$$\Rightarrow x \in aH \text{ and } x \in bH$$

$$\Rightarrow x = a * h_1 \text{ and } x = b * h_2, \text{ for some } h_1, h_2 \in H$$

$$\therefore a * h_1 = b * h_2$$

$$\Rightarrow (a * h_1) * h_1^{-1} = (b * h_2) * h_1^{-1}$$

$$\Rightarrow a * (h_1 * h_1^{-1}) = b * (h_2 * h_1^{-1})$$

$$\Rightarrow a * e = b * (h_2 * h_1^{-1})$$

$$\Rightarrow a = b * (h_2 * h_1^{-1})$$

If 'x' is any element in  $aH$ , then

$$x = a * h$$

$$x = b * (h_2 * h_1^{-1}) * h$$

$$= b * (h_2 * h_1^{-1} * h) \in bH$$

$$x \in aH \Rightarrow x \in bH$$

$$\therefore aH \subseteq bH \rightarrow \textcircled{2}$$

Similarly we can prove  $bH \subseteq aH \rightarrow \textcircled{3}$

From (2) & (3),  $\boxed{aH = bH}$

Thus any 2 cosets are either equal or disjoint

Further  $\bigcup_{a \in G_1} aH \subseteq G_1$ . since union of subset is

Subset.

If 'x' is any element in  $G_1$ , then

$$xe = x * e \in xH$$

$\therefore x$  is in left coset and hence  $x \in \bigcup_{a \in G_1} aH$

Hence

$$x \in G_1 \Rightarrow x \in \bigcup_{a \in G_1} aH$$

$$\Rightarrow G_1 \subseteq \bigcup_{a \in G_1} aH$$

$$\therefore G_1 = \bigcup_{a \in G_1} aH$$

This is all left coset partition  $G_1$ .

Theorem 14: There is one to one correspondence between any 2 left cosets of  $H$  in  $G_1$

Proof: let  $(H, *)$  be subgroup of  $(G_1, *)$

let  $aH$  be any left coset of  $H$  in  $G_1$ . we know  $H$  itself is left coset. so its enough to prove that there is 1 to 1 correspondence between  $H$  and  $aH$

let  $f: H \rightarrow aH$  be defined by  $f(h) = a * h$   
 $\forall h \in H$

The mapping is 1 to 1.

For any  $h_1, h_2 \in H$  if  $f(h_1) = f(h_2)$

$$\text{then } a * h_1 = a * h_2$$

$$\Rightarrow h_1 = h_2 \text{ (left cancellation law)}$$

Now we prove  $f$  is onto

Let  $x \in aH$  be any element, then  
 $x = a * h$  for some  $h \in H$ . For this  
 $h$  we have  $f(h) = a * h = x$ .

So,  $f$  is onto.

Hence ' $f$ ' is bijective function of  $H$  onto  $aH$

$\therefore f$  set up a 1 to 1 correspondence between  
 $H$  and  $aH$

Note: (1) If  $H$  is finite,  $H$  and  $aH$  have  
Same no: of elements

$$\therefore o(H) = o(aH)$$

(2) 13 and 14 theorem are true for  
every coset also.

Theorem 15: Lagrange Theorem. 

The order of a subgroup  $H$  of finite group  $G$   
divides the order of group. That is of  
Order  $H$  divides order of  $G$ .



Proof: let  $(G, *)$  be a group of order  $n$  and  $(H, *)$  be a subgroup of order  $m$ .

Since  $G$  is finite group, the no. of left coset of  $H$  in  $G$  is finite

let ' $\alpha$ ' be no. of cosets of  $H$  in  $G$

let ' $\alpha$ ' cosets be  $a_1H, a_2H, \dots, a_\alpha H$

we know that left coset of  $G$  form partition of  $G$ . [by theorem-13]

$$G = a_1H \cup a_2H \cup \dots \cup a_\alpha H$$

$$\begin{aligned} \therefore O(G) &= O(a_1H \cup a_2H \cup \dots \cup a_\alpha H) \\ &= O(a_1H) + O(a_2H) + \dots + O(a_\alpha H) \end{aligned}$$

$$\text{But } O(a_iH) = O(H) \text{ (theorem-14)}$$

$$\therefore O(G) = O(H) + O(H) + \dots + O(H), \alpha \text{ times}$$

$$\Rightarrow O(G) = \alpha O(H)$$

$$\Rightarrow \frac{O(G)}{O(H)} = \alpha$$

Thus  $O(H)$  divides  $O(G)$ .

Index of  $H$  in  $G$

Def: let  $(H, *)$  be subgroup of  $(G, *)$ .

Then the no. of different left (right)

cosets of  $H$  in  $G$  is called index of  
 $H$  in  $G$  and is denoted by  $[G:H]$  or  $i_G H$

Note: \* In case of finite group  $i_G(H) = \frac{O(G)}{O(H)}$

\* It is quite possible in an infinite group there is a subgroup of finite index.

Corollary 1: The order of any element of finite group  $G$  divides  $O(G)$

Proof: Let  $G$  be finite group of order  $n$ .  
 Let  $a \in G$  be element &  $O(a) = m$ .

Then cyclic group  $\langle a \rangle$  is of order  $m$ .

By Lagrange theorem,

$$[O(\langle a \rangle) \mid O(G) \Rightarrow m \mid n]$$

$\therefore$  order of element divides  $O(G)$

Corollary 2: any group of prime order is cyclic

Proof: Let  $G$  be a group of order  $P$ ,  
 where  $P$  is a prime number

Let  $a \in G$ ,  $a \neq e$ . Let  $H = \langle a \rangle$

Since  $a \neq e$ ,  $O(H) \neq 1 \therefore O(H) \geq 2$

By Lagrange theorem,  $O(H) \mid O(G)$

$\Rightarrow O(H) \mid P \Rightarrow O(H) = P$  (since  $P$  is prime  $\geq 2$ )  
 $= O(G)$

Hence  $G = H = \langle a \rangle$ .  $G$  is cyclic.

$\therefore$  Any group of prime order is cyclic.

Note: \* If  $O(G) = P$ , then every element other than identity  $e$  is generator of group.

\* If  $G$  is cyclic group of order  $P$ , a prime then  $G$  has no proper subgroup

## Normal Subgroups & Quotient groups.

Normal Subgroups: In general,  $Ha \neq aH$ . The subgroup  $H$  of  $G$  for which  $Ha = aH \forall a \in G$  is a special class of subgroups called normal subgroups.

Def: A subgroup  $(H, *)$  of  $(G, *)$  is called normal subgroup of  $G$  if  $aH = Ha \forall a \in G$



Examples 1: Every group of an abelian group is normal

Sol: Let  $(G, *)$  be an abelian group and  $(H, *)$  be a subgroup of  $G$ .

Let  $a \in G$  be any element

$$\text{Then } aH = \{a * h \mid h \in H\}$$

$$= \{h * a \mid h \in H\} \quad [\because G \text{ is abelian}]$$

$$= Ha$$

Since 'a' is arbitrary,  $aH = Ha \quad \forall a \in G$

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

Note: Since  $H_n = n\mathbb{Z}$  is subset of  $\mathbb{Z}$  and  $(\mathbb{Z}, +)$  is an abelian group, subgroup  $(H_n, +)$  is a normal subgroup of  $\mathbb{Z}$

Examples: Prove that intersection of two normal subgroup of  $(G, *)$  is a normal subgroup of  $(G, *)$

Sol: Let  $(N_1, *)$  and  $(N_2, *)$  be 2 normal subgroup of  $(G, *)$ .

~~Since~~ TO prove  $(N_1 \cap N_2, *)$  is normal subgroup of  $(G, *)$

Since  $N_1, N_2$  are normal subgroup of  $G$ , they are basically subgroups. We know  $N_1 \cap N_2$  is subgroup of  $G$ . Now we shall prove



it is a normal subgroup of  $G$ .

let  $n \in N_1 \cap N_2$  be any element and  $a \in G$  be any element.

then  $n \in N_1$  and  $n \in N_2$ .

Since  $N_1, N_2$  are normal,  $an a^{-1} \in N_1$  and  $a n a^{-1} \in N_2$ .

$\therefore a n a^{-1} \in N_1 \cap N_2$ .

Hence  $N_1 \cap N_2$  is normal, from above example.

Quotient group or factor group:

If  $(N, *)$  is a normal subgroup of  $(G, *)$  then the group  $(G/N, \oplus)$  is called quotient group or factor group of  $G$  by  $N$  or quotient group modulo  $N$ .

Direct product of 2 groups:

Theorem 17: let  $(G, *)$  and  $(H, \Delta)$  be two groups.

let  $G \times H$  be cartesian product of  $G$  and  $H$ .

If  $\bullet$  is the binary operation  $G \times H$  giv. by  $(g_1, h_1) \bullet (g_2, h_2) = (g_1 * g_2, h_1 \Delta h_2)$  for any  $(g_1, h_1), (g_2, h_2) \in G \times H$  then  $(G \times H, \bullet)$  is group.

Proof: Given  $(G, *)$ ,  $(H, \Delta)$  are groups, let  $e_1, e_2$  be identities of  $G$  and  $H$ .

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$

$\circ$  is binary operation componentwise multiplication.

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 * g_2, h_1 \Delta h_2) \quad \forall (g_1, h_1), (g_2, h_2) \in G \times H$$

$$g_1 * g_2 \in G \text{ and } h_1 \Delta h_2 \in H$$

$$(g_1 * g_2, h_1 \Delta h_2) \in G \times H$$

$$\Rightarrow (g_1, h_1) \circ (g_2, h_2) \in G \times H$$

So closure is satisfied.

Associativity: let  $x, y, z$  be any 3 elements of  $G \times H$ .

$$\therefore x = (g_1, h_1), y = (g_2, h_2), z = (g_3, h_3)$$

for some  $g_1, g_2, g_3 \in G$  and  $h_1, h_2, h_3 \in H$ .

$$\text{Now } x \circ (y \circ z) = (g_1, h_1) \circ ((g_2, h_2) \circ (g_3, h_3))$$

$$= (g_1, h_1) \circ (g_2 * g_3, h_2 \Delta h_3)$$

$$= (g_1 * (g_2 * g_3), h_1 \Delta (h_2 \Delta h_3))$$

$$= ((g_1 * g_2) * g_3, (h_1 \Delta h_2) \Delta h_3)$$

[ $\because * \text{ and } \Delta \text{ are associative}$ ]

$$= ((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3)$$

$$= (x \cdot y) \cdot z$$

$\therefore$  associative axiom is satisfied

Identity:  $(e_1, e_2)$  is identity element of  $G \times H$ , where  $e_1$  is the identity of  $G$  and  $e_2$  is identity of  $H$ .

For if  $(g, h) \in G \times H$  be any element then

$$(g, h) \cdot (e_1, e_2) = (g * e_1, h \Delta e_2) = (g, h)$$

$$\text{and } (e_1, e_2) \cdot (g, h) = (e_1 * g, e_2 \Delta h) = (g, h)$$

$\therefore (e_1, e_2)$  is identity of  $G \times H$

Inverse: let  $(g, h)$  be any element of  $G \times H$ .

Since  $g \in G$ ,  $h \in H$  and so  $(g^{-1}, h^{-1}) \in G \times H$

$$\text{Now } (g, h) \cdot (g^{-1}, h^{-1}) = (g * g^{-1}, h \Delta h^{-1}) = (e_1, e_2)$$

$$(g^{-1}, h^{-1}) \cdot (g, h) = (g^{-1} * g, h^{-1} \Delta h) = (e_1, e_2)$$

$\therefore (g^{-1}, h^{-1})$  is inverse of  $(g, h)$

$\therefore$  Inverse axiom is satisfied.

Hence  $(G \times H, \cdot)$  is group.

This group is called direct product of  $G$  and  $H$

## Group Homomorphism:

Let  $(G, *)$  and  $(G', \cdot)$  be 2 groups. A mapping  $f: G \rightarrow G'$  is called group homomorphism if for all  $a, b \in G$ .

$$f(a * b) = f(a) \cdot f(b)$$

## Elementary properties of homomorphism:

Theorem 18: If  $f$  is a homomorphism from group  $(G, *)$  into  $(G', \cdot)$  then prove that

(i)  $f(e) = e'$ , where  $e, e'$  are identities of  $G$  and  $G'$  respectively.

(ii)  $f(a^{-1}) = [f(a)]^{-1}$  for all  $a \in G$

Proof of (i): Let  $a \in G$  be any element.

$$\text{Then } a * e = a$$

$$\Rightarrow f(a * e) = f(a)$$

$$\Rightarrow f(a) \cdot f(e) = f(a) \quad [\because f \text{ is homomorphism}]$$

$$\Rightarrow f(a) \cdot f(e) = f(a) \cdot e'$$

By left cancellation law in  $G'$ , we get  $f(e) = e'$



ii) let  $a \in G$  be any element.

$$\text{Then } a * a^{-1} = a^{-1} * a = e$$

$$\therefore f(a * a^{-1}) = f(e) = f(a) \cdot f(a^{-1}) = e' \quad (\text{by (i)})$$

$$\text{and } f(a^{-1} * a) = f(e) \Rightarrow f(a^{-1}) \cdot f(a) = e'$$

$\therefore f(a^{-1})$  is inverse of  $f(a)$  in  $G'$ .

$$\Rightarrow [f(a)]^{-1} = f(a^{-1})$$

This theorem says that under homomorphism identities correspond and inverse correspond.

### Types of homomorphism:

Def: let  $f: G \rightarrow G'$  be homomorphism of groups

- i) If  $f$  is one-one, then  $f$  is monomorphism
- ii) If  $f$  is onto, then  $f$  is epimorphism
- iii) In case  $G'$  is called homomorphic image of  $G$
- iv) If  $f$  is one-one and onto, then  $f$  is isomorphism.

In case the two groups are said to be isomorphic and we write  $G \cong G'$ .

Def: Let  $(G, *)$  be a group. A homomorphism  $f: G \rightarrow G$  is called endomorphism.

If  $f$  is one-one and onto, then  $f$  is automorphism of  $G$ . (i.e) an isomorphism of  $G$  onto  $G$  is called automorphism.

Def: Kernel of group homomorphism

Let  $(G, *)$  and  $(G', \circ)$  be groups with  $e'$  as identity of  $G'$ . Let  $f: G \rightarrow G'$  be homomorphism.

The kernel of  $f$  is set of all elements of  $G$  which are mapped onto  $e'$  and denoted by  $\ker f$ .

$$\text{Thus } \ker f = \{a \in G \mid f(a) = e'\}$$

Theorem 19: Show that kernel of a group homomorphism is a normal subgroup of the group.

Proof: Let  $(G, *)$  and  $(G', \circ)$  be the group

and  $f: G \rightarrow G'$  is a group homomorphism then we know  $f(e) = e'$ , where  $e, e'$  are identities of  $G$  and  $G'$

$\therefore e \in \ker f$  and hence  $\ker f$  is non-empty subset of  $G$ .

First we shall prove  $\ker f$  is a subgroup of  $G$ .

Let  $x, y \in \ker f$ , then  $f(x) = e'$  &  $f(y) = e'$

$$\begin{aligned} \text{Now } f(xy^{-1})^{-1} &= f(x) \cdot f(y^{-1}) \quad [ \because f \text{ is homomorphism} ] \\ &= f(x) \cdot [f(y)]^{-1} \\ &= e' \cdot (e')^{-1} = e' \end{aligned}$$

$$\therefore xy^{-1} \in \ker f.$$

Hence  $\ker f$  is subgroup of  $G$

Next we shall prove that  $\ker f$  is normal subgroup.

Let  $n \in \ker f$  be any element and  $a \in G$  be any element.

$$\therefore f(n) = e', \quad f(a) \in G'$$

$$\begin{aligned} \text{Now } f(a * n * a^{-1}) &= f(a) \cdot f(n) \cdot f(a^{-1}) \\ &= f(a) \cdot e' \cdot (f(a))^{-1} \\ &= f(a) \cdot (f(a))^{-1} = e' \end{aligned}$$

$$\therefore a * n * a^{-1} \in \ker f$$

∴ Hence  $\ker f$  is normal subgroup of  $G$

Theorem 21: Fundamental theorem of group homomorphism.

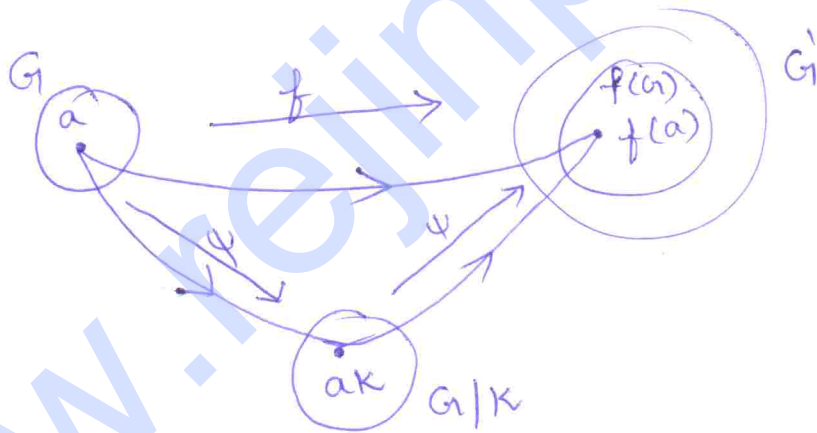
Let  $(G, *)$  and  $(G', \circ)$  be two groups.

Let  $f: G \rightarrow G'$  be a homomorphism of groups with kernel  $K$ . Then  $G/K$  is isomorphic to  $f(G) \subseteq G'$ .

Proof: we have to prove  $G/K \cong f(G)$

Define the map  $\psi: G/K \rightarrow f(G)$

by  $\psi(aK) = f(a) \forall aK \in G/K$  and  $a \in G$



First we shall prove  $\psi$  is well defined.

If  $aK = bK$ , then  $a * x_1 = b * x_2$  for some  $x_1, x_2 \in K$

$$\Rightarrow a = b * x_2 * x_1^{-1} = b * x, \text{ where } x = x_2 * x_1^{-1} \in K$$

$$\therefore f(a) = f(b * x) = f(b) \cdot f(x)$$

[ $\because f$  is homomorphism]



$$= f(b) \cdot e' = f(b) \quad [\because x \in K \Rightarrow f(x) = e']$$

$$\Rightarrow \psi(a_K) = \psi(b_K)$$

$\therefore \psi$  is well defined.

Now we shall prove  $\psi$  is homomorphism.

Let  $a_K, b_K \in G/K$  be any 2 elements.

$$\begin{aligned} \text{Then } \psi(a_K \oplus b_K) &= \psi((a * b)_K) = f(a * b) \\ &= f(a) \cdot f(b) \\ &= \psi(a_K) \cdot \psi(b_K) \end{aligned}$$

$\therefore \psi$  is homomorphism of  $G/K$  into  $f(G)$ .

Next we shall prove  $\psi$  is one-one and onto.

$$\text{Suppose } \psi(a_K) = \psi(b_K)$$

$$\text{then } f(a) = f(b)$$

$$\Rightarrow [f(a)]^{-1} \cdot f(b) = e' \Rightarrow f(a^{-1} * b) = e'$$

$$\Rightarrow a^{-1} * b \in K \Rightarrow b = a_K$$

$$\Rightarrow b_K = a_K \quad [\because KK = K]$$

$\therefore \psi$  is one-one

Finally, suppose  $x \in f(G)$  then there exist an  $a \in G$  such that

$$x = f(a) = \psi(a_K)$$

$\therefore \psi$  is onto

Thus  $\psi$  is isomorphism of  $G/K$  onto  $f(G)$

$$\therefore G/K \cong f(G)$$

Note Suppose  $f: G \rightarrow G'$  is onto,  $G' = f(G)$   
 $\therefore$  the result will be  $G/K \cong G'$

Theorem 24: Cayley's theorem.

Every finite group of order  $n$  is isomorphic to permutation group of degree  $n$ .

Proof: Let  $a \in G$  be any element. Corresponds to 'a' we define a map

$$f_a: G \rightarrow G \text{ by } f_a(x) = a * x \quad \forall x \in G$$

Then  $f$  is one-one, for  $f_a(x) = f_a(y)$ .

$$\Rightarrow a * x = a * y.$$

$$\Rightarrow x = y \text{ (by left cancellation)}$$

Now  $y \in G$  (codomain), then  $a^{-1} * y \in G$  such

$$\text{that } f_a(a^{-1} * y) = a * (a^{-1} * y) = (a * a^{-1}) * y \\ = e * y = y$$

$\therefore f_a$  is onto

Thus  $f_a$  is one-one and onto function

from  $G_1 \rightarrow G_1$  and so it is permutation on  $G_1$ . Since  $G_1$  has 'n' elements  $f_a$  is a permutation on 'n' symbols or permutation of degree 'n'.

Let  $G'_1 = \{f_a \mid a \in G_1\}$ . we shall prove  $G'_1$  is group.

we verify axioms of the group.

Let  $f_a, f_b \in G'_1$  be any 2 elements, (i.e)  $f_a, f_b$  are functions from  $G_1 \rightarrow G_1$ .

$$\begin{aligned} \text{Then } (f_a \cdot f_b)(x) &= f_a(f_b(x)) = f_a(b * x) \\ &= a * (b * x) \\ &= (a * b) * x \\ &= f_{a+b}(x) \quad \forall x \in G_1 \end{aligned}$$

$$\Rightarrow f_a \cdot f_b = f_{a+b} \quad \text{--- (1)}$$

Since  $a, b \in G_1 \Rightarrow a * b \in G_1$  and so  $f_{a * b} \in G'_1$

$\Rightarrow f_a \cdot f_b \in G'_1$ . Hence  $G'_1$  is closed under composition of func. operation.

$f_e \in G'_1$  is identity element.  $f_{a^{-1}}$  is inverse of  $f_a \in G'_1$ .

So,  $G'_1$  is group.

Finally, we prove  $G_1 \cong G'_1$

Let  $\phi: G_1 \rightarrow G_1$  be defined by  $\phi(a) = f_a \forall a \in G_1$

$$\begin{aligned} \text{Now for any } a, b \in G_1, \phi(a * b) &= f_{a * b} \\ &= f_a \cdot f_b \\ &= \phi(a) \cdot \phi(b) \end{aligned}$$

$\therefore \phi$  is homomorphism.

Suppose  $\phi(a) = \phi(b)$ , then  $f_a = f_b$

$$\Rightarrow f_a(x) = f_b(x) \forall x \in G_1$$

$$\Rightarrow a * x = b * x$$

$$\Rightarrow a = b$$

$\therefore \phi$  is one-one

Now let  $f_a \in G_1'$  be any element, with  $a \in G_1$

Then  $\phi(a) = f_a$  and so  $\phi$  is onto

Thus  $\phi$  is isomorphism of  $G_1$  onto  $G_1'$

$$\therefore G_1 \cong G_1'$$

Example sums:

38. Determine all cosets of subgroup  $H = \{1, a^2\}$  of group  $G = \{1, a, a^2, a^3\}$  under multiplication where  $a^4 = 1$



ANSWER:

Given  $G = \{1, a, a^2, a^3\}$ ,  $a^4 = 1$  is group under

$H = \{1, a^2\}$  we shall find all left cosets of  $H$

$$\text{Now } H = \{1 \cdot h \mid h \in H\} = \{1, a^2\} = H$$

$$aH = \{a \cdot h \mid h \in H\} = \{a \cdot 1, a \cdot a^2\} = \{a, a^3\}$$

$$a^2H = \{a^2 \cdot h \mid h \in H\} = \{a^2 \cdot 1, a^2 \cdot a^2\} = \{a^2, a^4\}$$

$$a^3H = \{a^3 \cdot h \mid h \in H\} = \{a^3 \cdot 1, a^3 \cdot a^2\} = \{a^3, a^5\}$$

$$[\because a^4 = 1]$$

$$\rightarrow a^2H = \{a^2, 1\} = H$$

Thus there are 2 distinct left cosets of  $H$  in  $G$  namely

$$H = \{1, a^2\} \text{ and } \{a, a^3\}$$

Example sum

39.) If  $H$  is a subgroup of  $G$  such that  $x^2 \in H \forall x \in G$ , prove  $H$  is normal subgroup of  $G$

ANSWER:

Let  $G$  be a multiplicative group.

$G$  is a group,  $H$  is subgroup of  $G$  such that  $x^2 \in H \forall x \in G$

$$x^2 \in H \quad \forall x \in G \longrightarrow \textcircled{1}$$

we have to prove  $H$  is normal subgroup.  
 Let  $h \in H$  be any element and  $a \in G$   
 be any element.

Then  $ah \in G \therefore (ah)^2 \in H$  (from ①)

Since  $a^{-1} \in G$ ,  $(a^{-1})^2 \in H \Rightarrow a^{-2} \in H$  (from ①)

Since  $h \in H$  and  $H$  is subgroup, we have  $h^{-1} \in H$

$$\therefore h^{-1} a^{-2} \in H$$

Hence  $(ah)^2 h^{-1} a^{-2} \in H$  [closure] by

$$\Rightarrow ah (ah) h^{-1} a^{-2} \in H$$

$$\Rightarrow aha(hh^{-1})a^{-2} \in H \quad [\text{associative}]$$

$$\Rightarrow ahae a^{-2} \in H \quad [e \rightarrow \text{identity}]$$

$$ahaa^{-2} \in H$$

$$aha^{-1} \in H$$

Hence  $H$  is normal subgroup of  $G$

Example sum:

40) Let  $G$  be group and  $a \in G$ . Show that  
 the map  $f: G \rightarrow G$  defined by  $f(x) = axa^{-1}$   
 $\forall x \in G$  is an isomorphism

ANSWER

Let  $G$  be multiplicative group

Given  $f: G \rightarrow G$  and  $f(x) = axa^{-1} \forall x \in G$   
and  $a \in G$  is fixed element.

First we shall prove it is homo-  
-morphism

$$\begin{aligned} \text{For any } x, y \in G, \quad f(xy) &= a(xy)a^{-1} \quad [\text{by definition}] \\ &= axey a^{-1} \quad [e \text{ identity of } G] \\ &= ax(a^{-1}a)ya^{-1} \\ &= (axa^{-1})(aya^{-1}) \\ &= f(x)f(y) \end{aligned}$$

$\therefore f$  is homomorphism

Now we shall prove  $f$  is one-one & onto.

Suppose  $f(x) = f(y)$  then  $axa^{-1} = aya^{-1}$   
 $\Rightarrow x = y$

$\therefore f$  is one-one.

If  $y \in G$  (co-domain) be any element

then  $a^{-1}ya \in G$

let  $x = a^{-1}ya$

$$\begin{aligned} \text{Now } f(x) &= axa^{-1} = a(a^{-1}ya)a^{-1} \\ &= \cancel{ae} e y e \\ &= y \end{aligned}$$

Thus for any  $y \in G$  we are able to find  
 $x \in G$  whose image is  $y$ . Hence  $f$  is onto.

Hence  $f$  is isomorphism

## Semi group & Monoids

Semigroups: Let  $S$  be non-empty set with binary operation  $*$  defined on it. The algebraic system  $(S, *)$  is called semi group if  $*$  is associative.

$$(i.e) \quad a * (b * c) = (a * b) * c \quad \forall a, b, c \in S$$

Monoids: A semi group  $(M, *)$  with identity element  $e$  is called monoid

### Example Sum

48.) For any commutative monoid  $(M, *)$  prove that set of all idempotent element of  $M$  forms a submonoid

ANSWER: Given  $(M, *)$  be commutative monoid.

Let  $e$  be its identity element.

Let  $S$  be set of all idempotent elements of  $M$ . (i.e)  $S = \{x \in M \mid x * x = x\}$

Since  $e * e = e$ ,  $e$  is an idempotent element of  $M$ .



$\therefore e \in S$  and hence  $S$  is non-empty.

Let  $a, b \in S$  be any 2 elements. They are idempotent elements.

$$\therefore a * a = a \quad \text{and} \quad b * b = b$$

We have to prove  $a * b$  is idempotent

$$\text{Now } (a * b) * (a * b) = a * (b * a) * b \quad [\because * \text{ associative}]$$

$$= a * (a * b) * b \quad [\because * \text{ commutative}]$$

$$= (a * a) * (b * b) \quad [\because * \text{ associativity}]$$

$$= a * b$$

Hence  $a * b$  is idempotent and so  $S$  is closed under  $*$  and  $e \in S$ . So  $(S, *)$  is submonoid of  $(M, *)$

Q. If  $Z_6$  is the set of equivalence classes generated by the equivalence relation "congruence modulo 6", prove that  $(Z_6, \times_6)$  is a monoid where the operation  $\times_6$  on  $Z_6$  is defined as  $[j] \times_6 [k] = [(j \times k) \bmod 6]$  for any  $[j], [k] \in Z_6$ .

A. We know  $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$

We shall form the composition table

$\times_6$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$	$[3]$
$[4]$	$[0]$	$[4]$	$[2]$	$[0]$	$[4]$	$[2]$
$[5]$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

The body of the table contains only all the elements of  $Z_6$ .

So  $Z_6$  is closed under  $\times_6$

Since the  $[a] \times_6 ([b] \times_6 [c])$

$$= [a] \times_6 [bc] = [a(bc) \bmod 6]$$

$\times_6$  depends on associativity of usual multiplication

$\therefore \times_6$  is associative

From the table we find  $[1] \times_6 [a] = [a]$  for all  $[a] \in Z_6$

$\therefore [1]$  is the identity element

Hence  $(Z_6, \times_6)$  is a monoid

Q. Let  $S = \mathbb{N} \times \mathbb{N}$ , the set of ordered pairs of positive integers with the operation  $*$  defined by  $(a, b) * (c, d) = (ad + bc, bd)$  and if  $f : (S, *) \rightarrow (\mathbb{Q}, +)$  is defined by  $f(a, b) = \frac{a}{b}$ , then show that  $f$  is a semi-group homomorphism.

A. We have the semigroups  $(S, *)$  and  $(\mathbb{Q}, +)$ .  
Given  $f : (S, *) \rightarrow (\mathbb{Q}, +)$  is defined by  $f(a, b) = \frac{a}{b}$ .  
Let  $x, y \in S$  be any two elements, then  $x = (a, b)$ ,  $y = (c, d)$  for integers  $a, b, c, d$ .

$$\text{Now } x * y = (a, b) * (c, d) = (ad + bc, bd)$$

$$\begin{aligned} \therefore f(x * y) &= f(ad + bc, bd) = \frac{ad + bc}{bd} \\ &= \frac{a}{b} + \frac{c}{d} = f(a, b) + f(c, d) \end{aligned}$$

$$\therefore f(x * y) = f(x) + f(y)$$

Q. If  $*$  is the operation defined on  $S = \mathbb{Q} \times \mathbb{Q}$ , the set of ordered pairs of rational numbers and given by  $(a, b) * (x, y) = (ax, ay + b)$ . Show that  $(S, *)$  is a semi group. Is it commutative? Also find the identity element of  $S$ .

A. Given  $S = \mathbb{Q} \times \mathbb{Q}$ , where  $\mathbb{Q}$  is the set of all rational numbers

$$\therefore S = \{ (x, y) \mid x, y \in \mathbb{Q} \}$$

A binary operation  $*$  on  $S$  is [www.rejinpaul.com](http://www.rejinpaul.com)  $(x, y) =$  37

$$(ax, ay + b)$$

To prove  $(S, *)$  is a semigroup, we have to prove  $*$  is associative

let  $A = (a, b)$ ,  $B = (c, d)$ ,  $C = (x, y)$  be any three elements in

$$\text{Then } A * (B * C) = (a, b) * ((c, d) * (x, y))$$

$$= (a, b) * (cx, cy + d)$$

$$= (a(cx), a(cy + d) + b)$$

$$= (acx, acy + ad + b)$$

$$\text{and } (A * B) * C = ((a, b) * (c, d)) * (x, y)$$

$$= (ac, ad + b) * (x, y)$$

$$= ((ac)x, (ac)y + ad + b)$$

$$= (acx, acy + ad + b)$$

From (1) and (2) we find  $A * (B * C) = (A * B) * C$  for all  $A, B, C \in S$ .

So  $*$  is associative. Hence  $(S, *)$  is a semigroup

Now we shall test  $*$  is commutative

$$A * B = (a, b) * (c, d)$$

$$= (ac, ad + b)$$

$$B * A = (c, d) * (a, b)$$

$$= (ca, cb + d)$$

$$= (cac, bc + d)$$

$$\therefore A * B \neq B * A$$

Hence  $*$  is not commutative and so  $(S, *)$  is not commutative

We shall now find identity element of  $S$ .



Suppose identity element  $I = (x, y)$  exists in  $S$  [www.rejinpaul.com](http://www.rejinpaul.com)

then  $I * A = A * I = A$  for any  $A = (a, b) \in S$

$$\text{Now } A * I = A \Rightarrow (a, b) * (x, y) = (a, b)$$

$$\Rightarrow (ax, ay + b) = (a, b)$$

$$\Rightarrow ax = a \text{ and } ay + b = b$$

$$\Rightarrow x = 1 \text{ and } ay = 0 \Rightarrow y = 0$$

$\therefore I = (1, 0)$  exists in  $S$ , since  $0, 1 \in \mathbb{Q}$

### Definition 1 : Ring

A non empty set  $R$  with two binary operations denoted by  $+$  and  $\cdot$ , called addition and multiplication is called a ring if the following axioms are satisfied

(i)  $(R, +)$  is an abelian group, with  $0$  as identity

(ii)  $(R, \cdot)$  is a semigroup

(iii) The operation  $\cdot$  is distributive over  $+$

$$\text{i.e. } a \cdot (b + c) = a \cdot b + a \cdot c$$

$$\text{and } (b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in R$$

The additive identity  $0$  is called the zero element of the ring

Definition 2 : A ring  $(R, +, \cdot)$  is said to be commutative if

$$a \cdot b = b \cdot a \quad \forall a, b \in R.$$

Note : (1) The multiplicative identity  $1$  is called the unit element or identity of  $R$ .

Definition : Integral domain

A commutative ring  $(R, +, \cdot)$  with identity and without zero is called an integral domain.

Definition : Field

A commutative ring  $(R, +, \cdot)$  with identity in which every non-zero element has multiplicative inverse is called as field.

Theorem 3 :

Every field is an integral domain

Proof :

Let  $(F, +, \cdot)$  be a field. Then it is a commutative ring with identity.

To prove  $F$  is an integral domain, it is enough to prove that it has no zero divisors.

Suppose  $a, b \in F$  with  $a \cdot b = 0$ ,  $a \neq 0$

Since  $a$  is non-zero element, its multiplicative inverse  $a^{-1}$  exists.

$$\therefore a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0$$

$$\Rightarrow (a^{-1} \cdot a) \cdot b = 0$$

$$1 \cdot b = 0 \rightarrow b = 0$$

Thus  $ab = 0, a \neq 0 \Rightarrow b = 0$

$\therefore F$  has no zero divisors

Hence  $(F, +, \cdot)$  is an integral domain

Theorem 4: Prove that any finite integral domain is a field

Proof: Let  $(R, +, \cdot)$  be a finite integral domain.

$\therefore R$  is a commutative ring with identity and without zero divisors. Hence to prove  $R$  is a field.

it is enough to prove that every non-zero element in  $R$  has multiplicative inverse

$$\text{Let } R = \{0, 1, a_1, a_2, \dots, a_n\}$$

where  $0$  is zero of the ring

$1$  is identity of ring

Let  $a \in R$  and  $a \neq 0$

Multiplying the non-zero elements of  $R$  by  $a$ , we get the set  $\{a \cdot 1, a \cdot a_1, \dots, a \cdot a_n\}$

Since  $R$  is without zero divisors, these elements are all non-zero and they are distinct.

Suppose  $aa_r = aa_s$ ,  $r \neq s$ ,

then  $a(a_r - a_s) = 0$

$\Rightarrow a_r - a_s = 0$ , since  $a \neq 0$

$\Rightarrow a_r = a_s$  which is a contradiction to the fact that  $a_r$  and  $a_s$  are distinct elements in  $R$

$\therefore aa_r \neq aa_s$

And all the  $aa_i$  are distinct from 'a' also

Since  $R$  is finite, these  $(n+1)$  elements are as same as  $(n+1)$  non-zero element of  $R$  in some order by pigeon hole principle.

$\therefore 1 = aa_i$  for some  $a_i \in R$

Since  $R$  is commutative  $aa_i = a_i a$

$\therefore aa_i = a_i a = 1 \Rightarrow a_i = a^{-1}$

$\therefore$  every non-zero element in  $R$  has multiplicative inverse

Hence any finite integral domain is a field



## CHAPTER 2

### Groups and group actions

#### 1. Groups

Let  $tt$  be set and  $*$  a *binary operation* which combines each pair of elements  $x, y \in tt$  to give another element  $x * y \in tt$ . Then  $(tt, *)$  is a *group* if the following conditions are satisfied.

Gp1: for all elements  $x, y, z \in tt$ ,  $(x * y) * z = x * (y * z)$ ;

Gp2: there is an element  $\iota \in tt$  such that for every  $x \in tt$ ,  $\iota * x = x = x * \iota$ ;

Gp3: for every  $x \in tt$ , there is a unique element  $y \in tt$  such that  $x * y = \iota = y * x$ .

Gp1 is usually called the associativity law.  $\iota$  is usually called the identity element of  $(tt, *)$ . In Gp3, the unique element  $y$  associated to  $x$  is called the inverse of  $x$  and is denoted  $x^{-1}$ .

EXAMPLE 2.1. The following are examples of groups.

(1)  $tt = \mathbb{Z}$ ,  $*$  = +,  $\iota = 0$  and  $x^{-1} = -x$ .

(2)  $tt = \mathbb{Q}$ ,  $*$  = +,  $\iota = 0$  and  $x^{-1} = -x$ .

(3)  $tt = \mathbb{R}$ ,  $*$  = +,  $\iota = 0$  and  $x^{-1} = -x$ .

EXAMPLE 2.2. Let  $n > 0$  be a natural number. Then  $(\mathbb{Z}/n, +)$  is a group with

$$\iota = 0_n$$

$$x^{-1} = -x_n = (-x)_n.$$

EXAMPLE 2.3. Let  $R = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ . Then each of these choices gives a group  $(GL_2(R), *)$  with

$$GL_2(R) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R, ad - bc \neq 0,$$

$*$  = multiplication of matrices,

$$\iota = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

EXAMPLE 2.4. Let  $X$  be a finite set and let  $\text{Perm}(X)$  be the set of all bijections  $f: X \rightarrow X$ . Then  $(\text{Perm}(X), \circ)$  is a group where

$\circ$  = composition of functions,

$\iota = \text{Id}_X$  = the identity function on  $X$ ,

$f^{-1}$  = the inverse function of  $f$ .

$(\text{Perm}(X), \circ)$  is called the *permutation group* of  $X$ . We will study these and other examples in more detail.

If a group  $(\mathcal{G}, *)$  has a finite underlying set  $\mathcal{G}$ , then the number of elements in the  $\mathcal{G}$  is called the *order* of  $\mathcal{G}$ , written  $|\mathcal{G}|$ .

## 2. Permutation groups

We will follow the ideas of Example 2.4 and consider the *standard set with  $n$  elements*

$$\mathbf{n} = \{1, 2, \dots, n\}.$$

The  $S_n = \text{Perm}(\mathbf{n})$  is called the *symmetric group on  $n$  objects* or the *symmetric group of degree  $n$*  or the *permutation group on  $n$  objects*.

THEOREM 2.5.  $S_n$  has order  $|S_n| = n!$ .

Proof. Defining an element  $\sigma \in S_n$  is equivalent to specifying the list

$$\sigma(1), \sigma(2), \dots, \sigma(n)$$

consisting of the  $n$  numbers  $1, 2, \dots, n$  taken in some order with no repetitions. To do this we have

- $n$  choices for  $\sigma(1)$ ,
- $n - 1$  choices for  $\sigma(2)$  (taken from the remaining  $n - 1$  elements),
- and so on.

In all, this gives  $n \times (n - 1) \times \dots \times 2 \times 1 = n!$  choices for  $\sigma$ , so  $|S_n| = n!$  as claimed. We will often describe  $\sigma$  using the notation

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Q

EXAMPLE 2.6. The elements of  $S_3$  are the following,

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

We can calculate the composition  $\tau \circ \sigma$  of two permutations  $\tau, \sigma \in S_n$ , where  $\tau\sigma(k) = \tau(\sigma(k))$ . Notice that we apply  $\sigma$  to  $k$  first then apply  $\tau$  to the result  $\sigma(k)$ . For example,

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I.$$

In particular,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

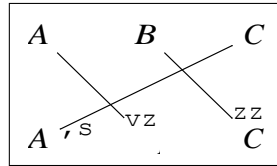
Let  $X$  be a set with exactly  $n$  elements which we list in some order,  $x_1, x_2, \dots, x_n$ . Then there is an *action* of  $S_n$  on  $X$  given by

$$\sigma \cdot x_k = x_{\sigma(k)} \quad (\sigma \in S_n, k = 1, 2, \dots, n).$$

For example, if  $X = \{A, B, C\}$  we can take  $x_1 = A$ ,  $x_2 = B$ ,  $x_3 = C$  and so

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot A = B, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot B = C, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot C = A.$$

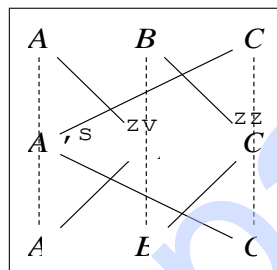
Often it is useful to display the effect of a permutation  $\sigma: X \rightarrow X$  by indicating where each element is sent by  $\sigma$  with the aid of arrows. To do this we display the elements of  $X$  in two similar rows with an arrow joining  $x_i$  in the first row to  $\sigma(x_i)$  in the second. For example, the permutation  $\sigma = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$  acting on  $X = \{A, B, C\}$  can be displayed as



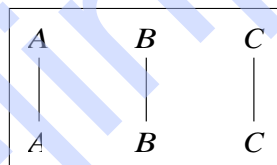
We can compose permutations by composing the arrows. Thus

$$\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

can be determined from the diagram



which gives the identity function whose diagram is



### 3. The sign of a permutation

Let  $\sigma \in S_n$  and consider the arrow diagram of  $\sigma$  as above. Let  $c_\sigma$  be the number of crossings of arrows. The **sign** of  $\sigma$  is the number

$$\text{sgn } \sigma = (-1)^{c_\sigma} = \begin{cases} +1 & \text{if } c_\sigma \text{ is even,} \\ -1 & \text{if } c_\sigma \text{ is odd.} \end{cases}$$

Then  $\text{sgn}: S_n \rightarrow \{+1, -1\}$ . Notice that  $\{+1, -1\}$  is actually a group under multiplication.

**PROPOSITION 2.7.** *The function  $\text{sgn}: S_n \rightarrow \{+1, -1\}$  satisfies*

$$\text{sgn}(\tau\sigma) = \text{sgn}(\tau) \text{sgn}(\sigma) \quad (\tau, \sigma \in S_n).$$

**Proof.** By considering the arrow diagram for  $\tau\sigma$  obtained by joining the diagrams for  $\sigma$  and  $\tau$ , we see that the total number of crossings is  $c_\sigma + c_\tau$ . If we straighten out the paths starting at each number in the top row, so that we change the total number of crossings by 2 each time. So  $(-1)^{c_\sigma + c_\tau} = (-1)^{c_\tau}$ . Q

A permutation  $\sigma$  is called *even* if  $\text{sgn } \sigma = 1$ , otherwise it is *odd*. The set of all even permutations in  $S_n$  is denoted by  $A_n$ . Notice that  $\iota \in A_n$  and in fact the following result is true.

PROPOSITION 2.8. *The set  $A_n$  forms a group under composition.*

Proof. By Proposition 2.7, if  $\sigma, \tau \in A_n$ , then

$$\text{sgn}(\tau\sigma) = \text{sgn}(\tau) \text{sgn}(\sigma) = 1.$$

Note also that  $\iota \in A_n$ .

The arrow diagram for  $\sigma^{-1}$  is obtained from that for  $\sigma$  by interchanging the rows and reversing all the arrows, so  $\text{sgn } \sigma^{-1} = \text{sgn } \sigma$ . Thus if  $\sigma \in A_n$ , then  $\text{sgn } \sigma^{-1} = 1$ .

Hence,  $A_n$  is a group under composition. Q

$A_n$  is called the *n-th alternating group*.

EXAMPLE 2.9. The elements of  $A_3$  are

$$\iota = \begin{matrix} & \Sigma & \\ \begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix} & , & \begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix} & , & \begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix} \end{matrix}.$$

We will see later that  $|A_n| = |S_n|/2 = n!/2$ .

#### 4. The cycle type of a permutation

Suppose  $\sigma \in S_n$ . Now carry out the following steps.

- Form the sequence

$$1 \rightarrow \sigma(1) \rightarrow \sigma^2(1) \rightarrow \cdots \rightarrow \sigma^{r_1-1}(1) \rightarrow \sigma^{r_1}(1) = 1$$

where  $\sigma^k(j) = \sigma(\sigma^{k-1}(j))$  and  $r_1$  is the smallest positive power for which this is true.

- Take the smallest number  $k_2 = 1, 2, \dots, n$  for which  $k_2 \neq \sigma^t(1)$  for every  $t$ . Form the sequence

$$k_2 \rightarrow \sigma(k_2) \rightarrow \sigma^2(k_2) \rightarrow \cdots \rightarrow \sigma^{r_2-1}(k_2) \rightarrow \sigma^{r_2}(k_2) = k_2$$

where  $r_2$  is the smallest positive power for which this is true.

- Repeat this with  $k_3 = 1, 2, \dots, n$  being the smallest number for which  $k_3 \neq \sigma^t(k_2)$  for every  $t$ .
- . . .

Writing  $k_1 = 1$ , we end up with a collection of *disjoint cycles*

$$k_1 \rightarrow \sigma(k_1) \rightarrow \sigma^2(k_1) \rightarrow \cdots \rightarrow \sigma^{r_1-1}(k_1) \rightarrow \sigma^{r_1}(k_1) = k_1$$

$$\rightarrow \sigma(k_2) \rightarrow \sigma^2(k_2) \rightarrow \cdots \rightarrow \sigma^{r_2-1}(k_2) \rightarrow \sigma^{r_2}(k_2) = k_2$$

.

$$k_d \rightarrow \sigma(k_d) \rightarrow \sigma^2(k_d) \rightarrow \cdots \rightarrow \sigma^{r_d-1}(k_d) \rightarrow \sigma^{r_d}(k_d) = k_d$$

in which every number  $k = 1, 2, \dots, n$  occurs in exactly one row.



The  $s$ -th one of these cycles can be viewed as corresponding to the permutation of  $\mathbf{n}$  which behaves according to the action of  $\sigma$  on the elements that appear as  $\sigma^t(k_s)$  and fix every other element. We indicate this permutation using the *cycle notation*

$$(k_s \sigma(k_s) \cdots \sigma^{s-1}(k_s)).$$

Then we have

$$\sigma = (k_1 \sigma(k_1) \cdots \sigma^{r_1-1}(k_1)) \cdots (k_d \sigma(k_d) \cdots \sigma^{r_d-1}(k_d)),$$

which is the *disjoint cycle decomposition* of  $\sigma$ . It is unique apart from the order of the factors and the order in which the numbers within each cycle occur.

For example, in  $S_4$ ,

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

$$(1 \ 2 \ 3)(1) = (3 \ 1 \ 2)(1) = (2 \ 3 \ 1)(1) = (1)(1 \ 2 \ 3) = (1)(3 \ 1 \ 2) = (1)(2 \ 3 \ 1).$$

We usually leave out cycles of length 1, so for example  $(1 \ 2 \ 3)(1) = (1 \ 2 \ 3)$ .

Recall that when performing elementary row operations (ERO's) on  $n \times n$  matrices, one of the types involves interchanging a pair of rows, say rows  $r$  and  $s$ , this operation is denoted by  $R_r \leftrightarrow R_s$ . The corresponding elementary matrix  $E(R_r \leftrightarrow R_s)$  is obtained from the identity matrix  $I_n$  by performing this operation. In fact, we can do a sequence of such operations to obtain any *permutation matrix*  $P_\sigma = [p_{ij}]$ , whose rows are obtained by applying the permutation  $\sigma \in S_n$  to those of  $I_n$  so that

$$p_{ij} = \delta_{\sigma(i)j} = \begin{cases} 1 & \text{if } j = \sigma(i), \\ 0 & \text{if } j \neq \sigma(i). \end{cases}$$

For example, if  $n = 3$  and  $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ , then

$$P_\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

PROPOSITION 2.10. For  $\sigma \in S_n$ ,  $\det P_\sigma = \text{sgn } \sigma$ .

A permutation  $\tau \in S_n$  which interchanges two elements of  $\mathbf{n}$  and leaves the rest fixed is called a *transposition*.

PROPOSITION 2.11. Let  $\sigma \in S_n$ . Then there are transpositions  $\tau_1, \dots, \tau_k$  such that  $\sigma = \tau_1 \cdots \tau_k$ .

One way to decompose a permutation  $\sigma$  into transpositions is to first decompose it into disjoint cycles then use the easily checked formula

$$(2.1) \quad (i_1 \ i_2 \ \dots \ i_r) = (i_1 \ i_r) \cdots (i_1 \ i_3)(i_1 \ i_2).$$

EXAMPLE 2.12. Decompose

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} \in S_5$$

into a product of transpositions.

SOLUTION. We have

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

Some alternative decompositions are

$$\sigma = (2\ 1)(2\ 4)(2\ 5) = (5\ 2)(5\ 1)(5\ 4).$$

Q

## 5. Symmetry groups

Let  $S$  be a set of points in  $\mathbb{R}^n$ , where  $n = 1, 2, 3, \dots$ . A *symmetry* of  $S$  is a surjection  $\phi : S \rightarrow S$  which preserves distances, i.e.,

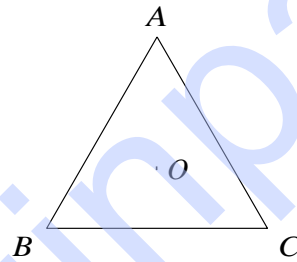
$$|\phi(\mathbf{u}) - \phi(\mathbf{v})| = |\mathbf{u} - \mathbf{v}| \quad (\mathbf{u}, \mathbf{v} \in S).$$

THEOREM 2.13. Let  $\phi$  be a symmetry of  $S \subseteq \mathbb{R}^n$ . Then

- (a)  $\phi$  is a bijection and  $\phi^{-1}$  is also a symmetry of  $S$ ;
- (b)  $\phi$  preserves distances between points and angles between lines joining points.

COROLLARY 2.14. Let  $S \subseteq \mathbb{R}^n$ . Then the set  $\text{Sym}(S)$  of all symmetries of  $S$  is a group under composition.

EXAMPLE 2.15. Let  $T \subseteq \mathbb{R}^2$  be an equilateral triangle  $O$  with vertices  $A, B, C$ .



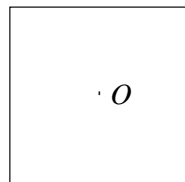
Then a symmetry is defined once we know where the vertices go, hence there are as many symmetries as permutations of the set  $\{A, B, C\}$ . Each symmetry can be described using permutation notation and we obtain the 6 symmetries

$$\iota = \begin{matrix} \Sigma & \Sigma & \Sigma & \Sigma & \Sigma & \Sigma \\ \begin{smallmatrix} A & B & C \\ A & B & C \end{smallmatrix} & \begin{smallmatrix} A & B & C \\ B & C & A \end{smallmatrix} & \begin{smallmatrix} A & B & C \\ C & A & B \end{smallmatrix} & \begin{smallmatrix} A & B & C \\ A & C & B \end{smallmatrix} & \begin{smallmatrix} A & B & C \\ C & B & A \end{smallmatrix} & \begin{smallmatrix} A & B & C \\ B & A & C \end{smallmatrix} \end{matrix}.$$

Therefore we have  $|\text{Sym}(O)| = 6$ .

EXAMPLE 2.16. Let  $S \subseteq \mathbb{R}^2$  be the square  $Q$  centred at the origin  $O$  with vertices at  $A(1, 1)$ ,  $B(-1, 1)$ ,  $C(-1, -1)$ ,  $D(1, -1)$ .

B A  
C D

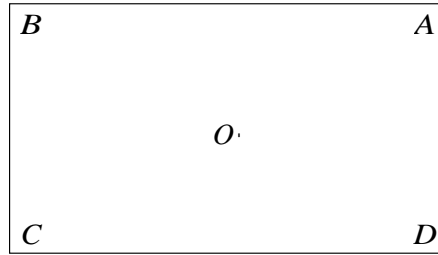


Then a symmetry is defined by sending  $A$  to any one of the 4 vertices then choosing how to send  $B$  to one of the 2 adjacent vertices. This gives a total of  $4 \times 2 = 8$  such symmetries, thus  $|\text{Sym}(Q)| = 8$ .

Again we can describe symmetries in terms of their effect on the vertices. Here are the 8 elements of  $\text{Sym}(\mathbf{Q})$  described in permutation notation.

$$\iota = \begin{array}{c} \begin{array}{c} \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} A & D & C & B \end{array} \end{array} \quad \begin{array}{c} \begin{array}{c} \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} B & C & D & A \end{array} \\ \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} D & C & B & A \end{array} \end{array} \quad \begin{array}{c} \begin{array}{c} \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} C & D & A & B \end{array} \\ \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} C & B & A & D \end{array} \end{array} \quad \begin{array}{c} \begin{array}{c} \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} D & A & B & C \end{array} \\ \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} B & A & D & C \end{array} \end{array} \end{array}$$

EXAMPLE 2.17. Let  $R \subseteq \mathbf{R}^2$  be the rectangle centred at the origin  $O$  with vertices at  $A(2, 1)$ ,  $B(-2, 1)$ ,  $C(-2, -1)$ ,  $D(2, -1)$ .



A symmetry can send  $A$  to any of the vertices, and then the long edge  $AB$  must go to the longer of the adjacent edges. This gives a total of 4 such symmetries, thus  $|\text{Sym}(R)| = 4$ .

Again we can describe symmetries in terms of their effect on the vertices. Here are the 4 elements of  $\text{Sym}(R)$  described in permutation notation.

$$\iota = \begin{array}{c} \begin{array}{c} \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} A & B & C & D \end{array} \end{array} \quad \begin{array}{c} \begin{array}{c} \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} B & A & D & C \end{array} \\ \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} B & A & D & C \end{array} \end{array} \quad \begin{array}{c} \begin{array}{c} \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} C & D & A & B \end{array} \\ \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} C & D & A & B \end{array} \end{array} \quad \begin{array}{c} \begin{array}{c} \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} D & C & B & A \end{array} \\ \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{array}{cccc} D & C & B & A \end{array} \end{array} \end{array}$$

Given a regular  $n$ -gon (i.e., a regular polygon with  $n$  sides all of the same length and  $n$  vertices  $V_1, V_2, \dots, V_n$ ) the symmetry group is the *dihedral group of order  $2n$*   $D_{2n}$ , with elements

$$\iota, \alpha, \alpha^2, \dots, \alpha^{n-1}, \tau, \alpha\tau, \alpha^2\tau, \dots, \alpha^{n-1}\tau$$

where  $\alpha^k$  is an anticlockwise rotation through  $2\pi k/n$  about the centre and  $\tau$  is a reflection in the line through  $V_1$  and the centre. Moreover we have

$$|\alpha| = n, |\tau| = 2, \tau\alpha\tau = \alpha^{n-1} = \alpha^{-1}.$$

In permutation notation this becomes

$$\alpha = (V_1 V_2 \cdots V_n),$$

but  $\tau$  is more complicated to describe.

For example, if  $n = 6$  we have

$$\alpha = (V_1 V_2 V_3 V_4 V_5 V_6), \quad \tau = (V_2 V_6)(V_3 V_5),$$

while if  $n = 7$

$$\alpha = (V_1 V_2 V_3 V_4 V_5 V_6 V_7), \quad \tau = (V_2 V_7)(V_3 V_6)(V_4 V_5).$$

We have seen that when  $n = 3$ ,  $\text{Sym}(\mathbf{O})$  is the permutation group of the vertices and so  $D_6$  is essentially the same group as  $S_6$ .

## 6. Subgroups and Lagrange's Theorem

Let  $(tt, *)$  be a group and  $H \subseteq tt$ . Then  $H$  is a *subgroup* of  $tt$  if  $(H, *)$  is a group. In detail this means that

- for  $x, y \in H$ ,  $x * y \in H$ ;
- $\iota \in H$ ;
- if  $z \in H$  then  $z^{-1} \in H$ .

We write  $H \triangleleft tt$  whenever  $H$  is a subgroup of  $tt$  and  $H < tt$  if  $H \neq tt$ , i.e.,  $H$  is a *proper subgroup* of  $tt$ .

EXAMPLE 2.18. For  $n \in \mathbb{Z}^+$ ,  $A_n$  is a subgroup of  $S_n$ , i.e.,  $A_n \triangleleft S_n$ .

By Example 2.3, for each choice of  $R = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ , there is a group  $(GL_2(R), *)$  with

$$GL_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R, ad - bc \neq 0 \right\}.$$

EXAMPLE 2.19. Let

$$SL_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R, ad - bc = 1 \right\} \subseteq GL_2(R).$$

Then  $SL_2(R)$  is a subgroup of  $GL_2(R)$ , i.e.,  $SL_2(R) \triangleleft GL_2(R)$ .

SOLUTION. This follows easily with aid of the three identities

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc; \quad \det(AB) = \det A \det B; \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in Q.$$

Let  $(tt, *)$  be a group. From now on, if  $x, y \in tt$  we will write  $xy$  for  $x * y$ . Also, for  $n \in \mathbb{Z}$  we write

$$x^n = \begin{cases} x(x^{n-1}) & \text{if } n > 0, \\ \iota & \text{if } n = 0, \\ (x^{-1})^{-n} & \text{if } n < 0. \end{cases}$$

If  $g \in tt$ ,

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\} \subseteq tt$$

is a subgroup of  $tt$  called the *subgroup generated by*  $g$ . This follows from the three equations

$$g^m g^n = g^{m+n}; \quad \iota = g^0; \quad (g^n)^{-1} = g^{-n}.$$

If  $\langle g \rangle$  is finite and contains exactly  $n$  elements then  $g$  is said to have *finite order*  $|g| = n$ . If  $\langle g \rangle$  is infinite then  $g$  is said to have *infinite order*  $|g| = \infty$ .

PROPOSITION 2.20. If  $g \in tt$  has finite order  $|g|$  then

$$|g| = \min\{m \in \mathbb{Z}^+ : m > 0, g^m = \iota\}.$$

EXAMPLE 2.21. In the group  $S_n$  the cyclic permutation  $(i_1 i_2 \cdots i_r)$  of length  $r$  has order

$$|(i_1 i_2 \cdots i_r)| = r.$$



SOLUTION. Setting  $\sigma = (i_1 i_2 \cdots i_r)$ , we have

$$\sigma^k(1) = \begin{cases} i_{k+1} & \text{if } k < r, \\ i_1 & \text{if } k = r, \end{cases}$$

hence  $|\sigma| \nmid r$ . As  $i_k \neq 1$  for  $1 < k \leq r$ ,  $r$  is the smallest such power which is 1, hence  $|\sigma| = r$ . Q

So for example,  $|(1\ 2)| = 2$ ,  $|(1\ 2\ 3)| = 3$  and  $|(1\ 2\ 3\ 4)| = 4$ . But notice that the product  $(1\ 2)(3\ 4\ 5)$  satisfies

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

hence  $|(1\ 2)(3\ 4\ 5)| = 6$ . On the other hand, the product  $(1\ 2)(2\ 3\ 4)$  satisfies

$$((1\ 2)(2\ 3\ 4))^2 = (1\ 2)(2\ 3\ 4)(1\ 2)(2\ 3\ 4) = (1\ 3)(2\ 4)$$

so  $|(1\ 2)(3\ 4\ 5)| = |(1\ 3)(2\ 4)| = 2$ .

A group  $(G, *)$  is called **cyclic** if there is an element  $c \in G$  such that  $G = \langle c \rangle$ ; such a  $c$  is called a **generator** of  $G$ . Notice that for such a group,  $|G| = |c|$ .

EXAMPLE 2.22. The group  $(\mathbb{Z}, +)$  is cyclic of infinite order with generators  $\pm 1$ .

EXAMPLE 2.23. If  $0 < n \in \mathbb{N}_0$ , then the group  $(\mathbb{Z}/n, +)$  is cyclic of finite order  $n$ . Two generators are  $\pm 1_n \in \mathbb{Z}/n$ . More generally,  $t_n$  is a generator if and only if  $\gcd(t, n) = 1$ .

SOLUTION. We have that for each  $k \in \mathbb{Z}$ ,  $k = \pm(1+1+\cdots+1)$  (with  $\pm k$  summands). From this we see that  $\pm 1_n$  are obvious generators and so  $\mathbb{Z}/n = \langle \pm 1_n \rangle$ .

If  $\gcd(t, n) = 1$ , then by Theorem 1.9, there is an integer  $u$  such that  $ut \equiv 1 \pmod{n}$ . Hence  $1_n \in \langle t_n \rangle$  and so  $\mathbb{Z}/n = \langle t_n \rangle$ .

Conversely, if  $\mathbb{Z}/n = \langle t_n \rangle$  then for some  $k \in \mathbb{N}_0$  we have  $1 \equiv 1 + \cdots + 1 \pmod{n}$  (with  $k$  summands) and so  $kt \equiv 1 \pmod{n}$ , hence  $kt + An = 1$  for some  $A \in \mathbb{Z}$ . But this implies  $\gcd(t, n) \mid 1$ , hence  $\gcd(t, n) = 1$ . Q

The **Euler  $\phi$ -function**  $\phi : \mathbb{Z}^+ \rightarrow \mathbb{N}_0$  is defined by

$$\begin{aligned} \phi(n) &= \text{number of generators of } \mathbb{Z}/n \\ &= \text{number of elements } t_n \in \mathbb{Z}/n \text{ with } \gcd(t, n) = 1. \end{aligned}$$

In order to state some properties of  $\phi$ , we need to introduce some notation. For a positive natural number  $n$  and a function  $f$  defined on the positive natural numbers, the symbol  $\sum_{d|n} f(d)$  denotes the sum of all the numbers  $f(d)$  where  $d$  ranges over all the positive integer divisors of  $n$ , including 1 and  $n$ . For example,

$$\sum_{d|6} f(d) = f(1) + f(2) + f(3) + f(6).$$

THEOREM 2.24. The Euler function  $\phi$  enjoys the following properties:

- (a)  $\phi(1) = 1$ ;
- (b) if  $\gcd(m, n) = 1$  then  $\phi(mn) = \phi(m)\phi(n)$ ;
- (c) if  $p$  is a prime and  $r \geq 1$  then  $\phi(p^r) = (p-1)p^{r-1}$ .
- (d) for a non-zero natural number  $n$ ,  $\sum_{d|n} \phi(d) = n$ .

For example,

$$\phi(120) = \phi(8 \cdot 3 \cdot 5) = \phi(8)\phi(3)\phi(5) = \phi(2^3)\phi(3)\phi(5) = 2^2 \cdot 2 \cdot 4 = 2^5 = 32.$$

The next result is actually a consequence of *Lagrange's Theorem* which follows immediately after it and is of great importance in the study of finite groups.

**PROPOSITION 2.25.** *Let  $\mathfrak{G}$  be a finite group and let  $g \in \mathfrak{G}$ . Then  $g$  has finite order and  $|g|$  divides  $|\mathfrak{G}|$ .*

**THEOREM 2.26 (Lagrange's Theorem).** *Let  $(\mathfrak{G}, *)$  be a finite group and  $H \trianglelefteq \mathfrak{G}$ . Then  $|H|$  divides  $|\mathfrak{G}|$ .*

**Proof.** The idea is to divide up  $\mathfrak{G}$  into disjoint subsets of size  $|H|$ . We do this by defining for each  $x \in \mathfrak{G}$  the *left coset of  $x$  with respect to  $H$* ,

$$xH = \{g \in \mathfrak{G} : x^{-1}g \in H\} = \{g \in \mathfrak{G} : g = xh \text{ for some } h \in H\}.$$

We need the following facts.

i) For  $x, y \in \mathfrak{G}$ ,  $xH \cap yH \neq \emptyset \iff xH = yH$ .

This is seen as follows. If  $xH = yH$  then  $xH \cap yH \neq \emptyset$ . Conversely, suppose that  $xH \cap yH \neq \emptyset$ . If  $yh \in xH$  for some  $h \in H$ , then  $x^{-1}yh \in H$ . For  $k \in H$ ,

$$x^{-1}yk = (x^{-1}yh)(h^{-1}k),$$

which is in  $H$  since  $x^{-1}yh, h^{-1}k \in H$  and  $H$  is a subgroup of  $\mathfrak{G}$ . Hence  $yH \subseteq xH$ . Repeating this argument with  $x$  and  $y$  interchanged we also see that  $xH \subseteq yH$ . Combining these inclusions we obtain  $xH = yH$ .

ii) For each  $g \in \mathfrak{G}$ ,  $|gH| = |H|$ .

If  $gh = gk$  for  $h, k \in H$  then  $g^{-1}(gh) = g^{-1}(gk)$  and so  $h = k$ . Thus there is a bijection

$$\theta : H \longrightarrow gH; \quad \theta(h) = gh,$$

which implies that the sets  $H$  and  $gH$  have the same number of elements.

Thus every element  $g \in \mathfrak{G}$  lies in exactly one such coset  $gH$ . Thus  $\mathfrak{G}$  is the union of these disjoint cosets which all have size  $|H|$ . Denoting the number of these cosets by  $[\mathfrak{G} : H]$  we have  $|\mathfrak{G}| = |H|[\mathfrak{G} : H]$ . Q

The number  $[\mathfrak{G} : H]$  of cosets of  $H$  in  $\mathfrak{G}$  is called the *index of  $H$  in  $\mathfrak{G}$* . The set of all cosets of  $H$  in  $\mathfrak{G}$  is denoted  $\mathfrak{G}/H$ , i.e.,

$$\mathfrak{G}/H = \{gH : g \in \mathfrak{G}\}.$$

**COROLLARY 2.27.** *If  $\mathfrak{G}$  is a finite group and  $H \trianglelefteq \mathfrak{G}$ , then  $|\mathfrak{G}| = |H| |\mathfrak{G}/H| = |H|[\mathfrak{G} : H]$ .*

Proposition 2.25 now follows easily by taking  $H = \langle g \rangle$  and using the fact that  $|g| = |H|$ .

This allows us to give a promised proof of a number theoretic result, the Primitive Element Theorem 1.27. Indeed the following generalisation is true.

**THEOREM 2.28.** *Let  $\mathfrak{G}$  be a group of finite order  $n = |\mathfrak{G}|$  and suppose that for each divisor  $d$  of  $n$  there are at most  $d$  elements of  $\mathfrak{G}$  satisfying  $x^d = 1$ . Then  $\mathfrak{G}$  is cyclic and so abelian.*

Proof. Let  $\theta(d)$  denote the number of elements in  $tt$  of order  $d$ . By Proposition 2.25,  $\theta(d) = 0$  unless  $d$  divides  $|tt|$ . Since

$$tt = \bigsqcup_{d \mid |tt|} \{g \in tt : |g| = d\},$$

we have

$$|tt| = \sum_{d \mid |tt|} \theta(d).$$

By Theorem 2.24(d), we also have

$$|tt| = \sum_{d \mid |tt|} \phi(d).$$

Combining these we obtain

$$(2.2) \quad \sum_{d \mid |tt|} \phi(d) = \sum_{d \mid |tt|} \theta(d).$$

We will show that for each divisor  $d$  of  $|tt|$ ,  $\theta(d) = \phi(d)$ . For each such  $d$  of  $|tt|$ , we have  $\theta(d) \geq 0$ . If  $\theta(d) = 0$  then  $\theta(d) < \phi(d)$ , since the latter is positive. So suppose that  $\theta(d) > 0$ , hence there is an element  $a \in tt$  of order  $d$ . In fact, the distinct powers  $\iota = a^0, a, a^2, \dots, a^{d-1}$  are all solutions of the equation  $x^d = \iota$  and indeed, by assumption on  $tt$ , they must be the only such solutions since there are  $d$  of them. But now an element  $a^k \in \langle a \rangle$  with  $k = 0, 1, 2, \dots, d-1$  has order  $d$  precisely if  $\gcd(d, k) = 1$  since this requires  $a^k = \iota$  and so for some  $u \in \mathbb{Z}$ ,  $uk \equiv 1 \pmod{d}$  which happens precisely when  $\gcd(d, k) = 1$  as we know from Theorem 1.9. By the definition of  $\phi$ , there are  $\phi(d)$  of such elements in  $\langle a \rangle$ , hence  $\theta(d) = \phi(d)$ . Thus we have shown that in all cases  $\theta(d) = \phi(d)$ .

Notice that if  $\theta(d) < \phi(d)$  for some  $d$  dividing  $|tt|$ , this would give a *strict* inequality in place of Equation (2.2). Hence we must always have  $\theta(d) = \phi(d)$ . In particular, there are  $\phi(n)$  elements of order  $n$ , hence there must be an element of order  $n$ , so  $tt$  is cyclic.  $\square$

Taking  $tt = U_p$ , the group of invertible elements of  $\mathbb{Z}/p$  under multiplication, we obtain Theorem 1.27.

## 7. Group actions

If  $X$  is a set and  $(tt, *)$  then a (*group*) *action* of  $(tt, *)$  on  $X$  is a rule which assigns to each  $g \in tt$  and  $x \in X$  an element  $gx \in X$  so that the following conditions are satisfied.

**GpAc1** For all  $g_1, g_2 \in tt$  and  $x \in X$ ,  $(g_1 * g_2)x = g_1(g_2x)$ .

**GpAc2** For  $x \in X$ ,  $1x = x$ .

Thus each  $g \in tt$  can be viewed as acting as a permutation of  $X$ .

**EXAMPLE 2.29.** Let  $tt = S_n$  and let  $X = \mathbf{n}$ . For  $\sigma \in tt$  and  $k \in \mathbf{n}$  let  $\sigma k = \sigma(k)$ . This defines an action of  $(tt, \circ)$  on  $\mathbf{n}$ .

**EXAMPLE 2.30.** Let  $X \subseteq \mathbb{R}^n$  and let  $tt = \text{Sym}(X)$  be a subgroup of the symmetry group of  $X$ . For  $\phi \in tt$  and  $x \in X$ , let  $\phi x = \phi(x)$ . This defines an action of  $(tt, \circ)$  on  $X$ .

Suppose we have an action of a group  $(tt, *)$  on a set  $X$ . For  $x \in X$ , the *stabilizer* of  $x$  is

$$\text{Stab}_{tt}(x) = \{g \in tt : gx = x\} \subseteq tt,$$

and the *orbit* of  $x$  is

$$\text{Orb}_{tt}(x) = \{gx : g \in tt\} \subseteq X.$$

Notice that  $x = \iota x$ , so  $x \in \text{Orb}_{tt}(x)$  and  $\iota \in \text{Stab}_{tt}(x)$ . Thus  $\text{Stab}_{tt}(x) \neq \emptyset$  and  $\text{Orb}_{tt}(x) \neq \emptyset$ .

THEOREM 2.31. For each  $x, y \in X$ ,

- (a)  $\text{Stab}_{tt}(x) \cong tt$ ;
- (b)  $y \in \text{Orb}_{tt}(x)$  if and only if  $x \in \text{Orb}_{tt}(y)$ ;
- (c)  $y \in \text{Orb}_{tt}(x)$  if and only if  $\text{Orb}_{tt}(y) = \text{Orb}_{tt}(x)$ .

Proof.

a) If  $g_1, g_2 \in \text{Stab}_{tt}(x)$  then by GpAct1,

$$(g_1 * g_2)x = g_1(g_2x) = g_1x = x.$$

By GpAct2,  $\iota x = x$ , hence  $\iota \in \text{Stab}_{tt}(x)$ . Finally, if  $g \in \text{Stab}_{tt}(x)$  then by GpAct1 and GpAct2,

$$g^{-1}x = g^{-1}(gx) = (g^{-1} * g)x = \iota x = x,$$

hence  $g^{-1} \in \text{Stab}_{tt}(x)$ . So  $\text{Stab}_{tt}(x) \cong tt$ .

b) If  $y \in \text{Orb}_{tt}(x)$ , then  $y = gx$  for some  $g \in tt$ . Hence  $x = (g^{-1} * g)x = g^{-1}(gx) = g^{-1}y$  and so  $x \in \text{Orb}_{tt}(y)$ . The converse is similar.

c) If  $y \in \text{Orb}_{tt}(x)$  then by (b),  $x \in \text{Orb}_{tt}(y)$  and so  $x = ky$  for some  $k \in tt$ . Hence if  $g \in tt$ ,  $gx = g(ky) = (g * k)y \in \text{Orb}_{tt}(y)$  and so  $\text{Orb}_{tt}(x) \subseteq \text{Orb}_{tt}(y)$ . By (b),  $x \in \text{Orb}_{tt}(y)$  and so we also have  $\text{Orb}_{tt}(y) \subseteq \text{Orb}_{tt}(x)$ . This gives  $\text{Orb}_{tt}(y) = \text{Orb}_{tt}(x)$ .

Conversely, if  $\text{Orb}_{tt}(y) = \text{Orb}_{tt}(x)$  then  $y \in \text{Orb}_{tt}(y) = \text{Orb}_{tt}(x)$ . Q

EXAMPLE 2.32. Let  $X = Q$  be the square with vertices  $A, B, C, D$  and let  $tt = \text{Sym}(Q)$ . Determine  $\text{Stab}_{tt}(x)$  and  $\text{Orb}_{tt}(x)$  where

- (a)  $x$  is the vertex  $A$ ;
- (b)  $x$  is the midpoint  $M$  of  $AB$ ;
- (c)  $x$  is the point  $P$  on  $AB$  where  $AP : PB = 1 : 3$ .

SOLUTION. Recall Example 2.16. We will write permutations of the vertices in cycle notation.

a) We have

$$\text{Stab}_{tt}(A) = \{\iota, (B D)\}.$$

Also, every vertex can be obtained from  $A$  by applying a suitable symmetry, hence

$$\text{Orb}_{tt}(x) = \{A, B, C, D\}.$$

b) A symmetry  $\phi$  fixes the midpoint of  $AB$  if and only if it maps this edge to itself. The symmetries doing this have one of the effects  $\phi(A) = A, \phi(B) = B$  or  $\phi(A) = B, \phi(B) = A$ . Thus

$$\text{Stab}_{tt}(M) = \{\iota, (A B)(C D)\}.$$

Also, we can arrange to send  $A$  to any other vertex and  $B$  to either of the adjacent vertices of the image of  $A$ , hence the orbit of  $M$  consists of the set of 4 midpoints of edges.

c) A symmetry  $\phi$  can only fix  $P$  if it sends  $A$  to a vertex  $A^j$  say, and  $B$  to a vertex  $B^j$  with  $A^jP : PB^j = 1 : 3$  and this is only possible if  $A^j = A$  and  $B^j = B$ , hence  $\phi$  must also fix  $A, B$ . So  $\text{Stab}_{tt}(P) = \{\iota\}$ . On the other hand, since we can select a symmetry to send  $A$  to any



other vertex and  $B$  to either of the adjacent vertices to the image,  $P$  can be sent to any of the points  $Q$  which cut an edge in the ratio 1 : 3. So the orbit of  $P$  is the set consisting of these 8 points. Q

**THEOREM 2.33 (Orbit-Stabilizer Theorem).** *Let  $(\mathfrak{tt}, *)$  act on  $X$ . Then for  $x \in X$  there is a bijection  $F: \mathfrak{tt}/\text{Stab}_{\mathfrak{tt}}(x) \rightarrow \text{Orb}_{\mathfrak{tt}}(x)$  between the set of cosets of  $\text{Stab}_{\mathfrak{tt}}(x)$  in  $\mathfrak{tt}$  and the orbit of  $x$ , defined by  $F(g \text{Stab}_{\mathfrak{tt}}(x)) = gx$ . Moreover we have*

$$F((t * g) \text{Stab}_{\mathfrak{tt}}(x)) = tF(g \text{Stab}_{\mathfrak{tt}}(x)) \quad (t \in \mathfrak{tt}).$$

*Proof.* We begin by checking that  $F$  is well defined. If  $g_1 \text{Stab}_{\mathfrak{tt}}(x) = g_2 \text{Stab}_{\mathfrak{tt}}(x)$ , then  $g_1^{-1}g_2 \in \text{Stab}_{\mathfrak{tt}}(x)$  and

$$g_1 x = g_1((g_1^{-1}g_2)x) = (g_1 g_1^{-1}g_2)x = g_2 x.$$

Hence  $F$  is well defined.

Notice that  $gx = kx$  if and only if  $(g^{-1}k)x = x$ , i.e.,  $g^{-1}k \in \text{Stab}_{\mathfrak{tt}}(x)$  which means that

$$g \text{Stab}_{\mathfrak{tt}}(x) = k \text{Stab}_{\mathfrak{tt}}(x).$$

So  $F$  is an injection. Also, every  $y \in \text{Orb}_{\mathfrak{tt}}(x)$  has the form  $tx = F(t \text{Stab}_{\mathfrak{tt}}(x))$  for some  $t \in \mathfrak{tt}$ , which shows that  $F$  is surjective. Q

The final equation property is a consequence of the definition of  $F$ .

**COROLLARY 2.34.** *If  $\mathfrak{tt}$  is finite then for each  $x \in X$ ,*

$$|\text{Orb}_{\mathfrak{tt}}(x)| = \frac{|\mathfrak{tt}|}{|\text{Stab}_{\mathfrak{tt}}(x)|}.$$

*Proof.* This follows from Corollary 2.27. Q

The sizes of the orbits in Example 2.32 can be found using this result.

**THEOREM 2.35.** *The orbits of an action of  $(\mathfrak{tt}, *)$  on  $X$  decompose  $X$  into a union of disjoint subsets,*

$$X = \bigsqcup_{U \text{ an orbit}} U.$$

**COROLLARY 2.36.** *If  $X$  is finite then*

$$|X| = \sum_{U \text{ an orbit}} |U|.$$

In these results, each orbit  $U$  has the form  $\text{Orb}_{\mathfrak{tt}}(x_U)$  for some element  $x_U \in X$ . Moreover, if  $\mathfrak{tt}$  is finite, then

$$|U| = [\mathfrak{tt} : \text{Stab}_{\mathfrak{tt}}(x_U)] = \frac{|\mathfrak{tt}|}{|\text{Stab}_{\mathfrak{tt}}(x_U)|}.$$

The formula in Corollary 2.36 becomes the **orbit-stabilizer equation**:

$$(2.3) \quad |X| = \sum_{U \text{ an orbit}} \frac{|\mathfrak{tt}|}{|\text{Stab}_{\mathfrak{tt}}(x_U)|}.$$

If there is only one orbit, then the action is said to be **transitive**, and in this case, for any  $x \in X$  we have  $X = \text{Orb}_{\mathfrak{tt}}(x)$  and  $|X| = |\mathfrak{tt}|/|\text{Stab}_{\mathfrak{tt}}(x)|$ .

Given an action of  $(\mathfrak{tt}, *)$  on  $X$ , another useful idea is that of the **fixed point set** or **fixed set** of an element  $g \in \mathfrak{tt}$ ,

$$\text{Fix}_{\mathfrak{tt}}(g) = \{x \in X : gx = x\}.$$

$\text{Fix}_{\pi}(g)$  is also often denoted  $X^g$ .

THEOREM 2.37 (Burnside Formula). *If  $(\pi, *)$  acts on  $X$  with  $\pi$  and  $X$  finite, then*

$$\text{number of orbits} = \frac{1}{|\pi|} \sum_{g \in \pi} |\text{Fix}_{\pi}(g)|.$$

Proof. The right hand side of the formula is

$$\begin{aligned} \frac{1}{|\pi|} \sum_{g \in \pi} |\text{Fix}_{\pi}(g)| &= \frac{1}{|\pi|} \sum_{g \in \pi} \sum_{x \in \text{Fix}_{\pi}(g)} 1 \\ &= \frac{1}{|\pi|} \sum_{x \in X} \sum_{g \in \text{Stab}_{\pi}(x)} 1 \\ &= \frac{1}{|\pi|} \sum_{x \in X} |\text{Stab}_{\pi}(x)| \\ &= \frac{1}{|\pi|} \sum_{U = \text{Orb}_{\pi}(x) \text{ an orbit}} |U| \cdot |\text{Stab}_{\pi}(x)| \quad (\text{by Corollary 2.34}) \\ &= \frac{1}{|\pi|} \sum_{U \text{ an orbit}} |\pi| \\ &= \sum_{U \text{ an orbit}} 1 \\ &= \text{number of orbits.} \end{aligned}$$

Q

EXAMPLE 2.38. Let  $X = \{1, 2, 3, 4\}$  and let  $\pi \cong S_4$  be the subgroup

$$\pi = \{i, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

acting on  $X$  in the obvious way. How many orbits does this action have?

SOLUTION. Here  $|\pi| = 4 = |X|$ . Furthermore we have

$$\text{Fix}_{\pi}(i) = X, \quad \text{Fix}_{\pi}((1\ 2)) = \{3, 4\}, \quad \text{Fix}_{\pi}((3\ 4)) = \{1, 2\}, \quad \text{Fix}_{\pi}((1\ 2)(3\ 4)) = \emptyset.$$

The Burnside Formula gives

$$\text{number of orbits} = \frac{1}{4} (4 + 2 + 2 + 0) = \frac{8}{4} = 2.$$

So there are 2 orbits, namely  $\{1, 2\}$  and  $\{3, 4\}$ .

Q

EXAMPLE 2.39. Let  $X = \{1, 2, 3, 4, 5, 6\}$  and let  $\pi = ((1\ 2\ 3)(4\ 5)) \cong S_6$  be the cyclic subgroup acting on  $X$  in the obvious way. How many orbits does this action have?

SOLUTION. Here  $|\pi| = 6$  and  $|X| = 6$ . The elements of  $\pi$  are

$$i, (1\ 2\ 3)(4\ 5), (1\ 3\ 2), (4\ 5), (1\ 2\ 3), (1\ 3\ 2)(4\ 5).$$

The fixed sets of these are

$$\begin{aligned} \text{Fix}_{\pi}(i) &= X, & \text{Fix}_{\pi}((1\ 2\ 3)(4\ 5)) &= \text{Fix}_{\pi}((1\ 3\ 2)(4\ 5)) = \{6\}, \\ \text{Fix}_{\pi}((4\ 5)) &= \{1, 2, 3, 6\}, & \text{Fix}_{\pi}((1\ 2\ 3)) &= \text{Fix}_{\pi}((1\ 3\ 2)) = \{4, 5, 6\}. \end{aligned}$$

By the Burnside Formula,

$$\text{number of orbits} = \frac{1}{6} (6 + 1 + 3 + 4 + 3 + 1) = \frac{18}{6} = 3.$$

So there are 3 orbits, namely  $\{1, 2, 3\}$ ,  $\{4, 5\}$  and  $\{6\}$ . Q

EXAMPLE 2.40. A dinner party of seven people is to sit around a circular table with seven seats. How many distinguishable ways are there to do this if there is to be no 'head of table'?

SOLUTION. View the seven places as numbered 1 to 7. There are  $7!$  ways to arrange the diners in these places. Take  $X$  to be the set of all possible such arrangements, so  $|X| = 7!$ . Regard two such arrangements as indistinguishable if one is obtained from the other by a rotation of the diners around the places. Clearly there are 7 such rotations, each involving everyone moving  $k$  seats to the right for some  $k = 0, 1, \dots, 6$ . Let  $\alpha$  denote the rotation corresponding to everyone moving one seat to the right. Then to get everyone to move  $k$  seats we repeatedly apply  $\alpha$   $k$  times in all, i.e.,  $\alpha^k$ . This suggests we should consider the group

$$tt = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$$

consisting of all of these operations, with composition as the binary operation. This provides an action of  $tt$  on  $X$ .

The number of indistinguishable seating plans is the number of orbits under this action, i.e.,

$$\frac{1}{|tt|} \sum_{g \in tt} |\text{Fix}_{tt}(g)|.$$

Notice that apart from the identity element, no rotation can fix any arrangement, so when  $g \neq 1$ ,  $\text{Fix}_{tt}(g) = \emptyset$ , while  $\text{Fix}_{tt}(1) = X$ . Hence the number of indistinguishable seating plans is  $7!/7 = 6! = 720$ . Q

EXAMPLE 2.41. Find the number of distinguishable ways there are to colour the edges of an equilateral triangle using four different colours, where each colour can be used on more than one edge.

SOLUTION. Let  $X$  be the set of all possible such colourings of the equilateral triangle  $ABC$  whose symmetry group is  $tt = S_3$ , which we view as the permutation group of  $\{A, B, C\}$ ; hence  $|tt| = 6$ . Also  $|X| = 4^3 = 64$  since each edge can be coloured in 4 ways.  $tt$  acts on  $X$  in the obvious way. A pair of colourings is indistinguishable precisely if they are in the same orbit.

By the Burnside formula, the number of distinguishable colourings is given by

$$\text{number of orbits} = \frac{1}{6} \sum_{\sigma \in tt} |\text{Fix}_{tt}(\sigma)|.$$

The fixed sets of elements of the various cycle types in  $tt$  are as follows.

Identity element  $1$ :  $\text{Fix}_{tt}(1) = X$ ,  $|\text{Fix}_{tt}(1)| = 64$ .

3-cycles (i.e.,  $\sigma = (ABC), (ACB)$ ): these give rotations and can only fix a colouring that has all sides the same colour, hence  $|\text{Fix}_{tt}(\sigma)| = 4$ .

2-cycles (i.e.,  $\sigma = (AB), (AC), (BC)$ ): each of these gives a reflection in a line through a vertex and the midpoint of the opposite edge. For example,  $(AB)$  fixes  $C$  and interchanges the edges  $AC, BC$ , it will therefore fix any colouring that has these edges the same colour. There are  $4 \times 4 = 16$  of these, so  $|\text{Fix}_{tt}((AB))| = 16$ . Similarly for the other 2-cycles.

By the Burnside formula,

$$\text{number of distinguishable colourings} = \frac{1}{6} (64 + 2 \times 4 + 3 \times 16) = \frac{120}{6} = 20. \quad \text{Q}$$

[www.rejinpaul.com](http://www.rejinpaul.com)



## Problem Set 2

2-1. Which of the following pairs  $(\mathcal{G}, *)$  forms a group?

- (a)  $\mathcal{G} = \{x \in \mathbb{Z} : x \neq 0\}$ ,  $*$  =  $\times$ ;
- (b)  $\mathcal{G} = \{x \in \mathbb{Q} : x \neq 0\}$ ,  $*$  =  $\times$ ;
- (c)  $\mathcal{G} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}, a^2 + b^2 = 1$ ,  $*$  = multiplication of matrices;
- (d)  $\mathcal{G} = \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} : z, w \in \mathbb{C}, |z|^2 + |w|^2 = 1$ ,  $*$  = multiplication of matrices;
- (e)  $\mathcal{G} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc \neq 0$ ,  $*$  = multiplication of matrices;
- (f)  $\mathcal{G} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1$ ,  $*$  = multiplication of matrices;
- (g)  $\mathcal{G} = \{\phi \in S_n : \phi(n) = n\}$ ,  $*$  = composition of functions.

2-2. For each of the following permutations in  $S_6$ , determine its sign and decompose it into disjoint cycles:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 5 & 6 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix}.$$

2-3. Find the orders of the symmetry groups of the following geometric objects, and in each case try to describe the symmetry groups as groups of permutations:

- a regular pentagon;
- a regular hexagon;
- a regular hexagon with vertices alternately coloured red and green;
- a regular hexagon with edges alternately coloured red and green;
- a cube;
- a cube with the pairs of opposite faces coloured red, green and blue respectively.

2-4. [**Challenge question.**] Suppose Tet is a regular tetrahedron with vertices  $A, B, C, D$ .

- Show that the symmetry group  $\text{Sym}(\text{Tet})$  of Tet can be identified with the symmetric group  $S_4$  which acts by permuting the vertices.
- For each pair of distinct vertices  $P, Q$ , how many symmetries map the edge  $PQ$  into itself? Show that these symmetries form a group.
- Find a geometric interpretation of the alternating group  $A_4$  acting as symmetries of Tet.

2-5. In each of the following groups  $(\mathcal{G}, *)$  decide whether the subset  $H$  is a subgroup of  $\mathcal{G}$  and when it is, decide whether it is cyclic.

- $\mathcal{G} = \{x \in \mathbb{Q} : x \neq 0\}$ ,  $H = \{x \in \mathcal{G} : x > 0\}$ ,  $*$  =  $\times$ ;
- $\mathcal{G} = \{x \in \mathbb{Q} : x \neq 0\}$ ,  $H = \{x \in \mathcal{G} : x < 0\}$ ,  $*$  =  $\times$ ;
- $\mathcal{G} = \{x \in \mathbb{Q} : x \neq 0\}$ ,  $H = \{x \in \mathcal{G} : x^2 = 1\}$ ,  $*$  =  $\times$ ;
- $\mathcal{G} = \{x \in \mathbb{C} : x \neq 0\}$ ,  $H = \{x \in \mathcal{G} : x^d = 1\}$ ,  $*$  =  $\times$ ;
- $\mathcal{G} = \{z \in \mathbb{C} : z \neq 0\}$ ,  $H = \{z \in \mathcal{G} : |z| < \infty\}$ ,  $*$  =  $\times$ ;

f)  $\mathcal{H} = \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} : z, w \in \mathbb{C}, |z|^2 + |w|^2 = 1 \right\}, H = \{A \in \mathcal{H} : |A| < \infty\},$   
 $*$  = matrix multiplication;  
g)  $\mathcal{H} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}, H = \left\{ A \in \mathcal{H} : A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right\},$

$*$  = matrix multiplication;

h)  $\mathcal{H} = \text{Sym}(\mathbb{Q})$ ,  $H$  = the subset of rotations in  $\mathcal{H}$ ,  $*$  = composition of functions.

2-6. Using Lagrange's Theorem, find all possible orders of elements of each of the following groups and decide whether there are indeed elements of those orders:

$$\mathbb{Z}/6, S_3, A_3, S_4, A_4, D_8, D_{10}.$$

2-7. [Challenge question] Let  $\mathcal{H}$  be a group. Show that each of the following subsets of  $\mathcal{H}$  is a subgroup:

- (a)  $C_{\mathcal{H}}(x) = \{c \in \mathcal{H} : cx = xc\}$ , where  $x \in \mathcal{H}$  is any element;
- (b)  $Z(\mathcal{H}) = \{c \in \mathcal{H} : cg = gc \text{ for all } g \in \mathcal{H}\}$ ;
- (c)  $N_{\mathcal{H}}(H) = \{n \in \mathcal{H} : \text{for every } h \in H, nhn^{-1} \in H, \text{ and } n^{-1}hn \in H\}$ , where  $H \trianglelefteq \mathcal{H}$  is any subgroup.

2-8. Using Lagrange's Theorem, find all subgroups of each of the groups

$$\mathbb{Z}/6, S_3, A_3, S_4, A_4, D_8, D_{10}.$$

2-9. Let  $\mathcal{H} = S_4$  and let  $X$  denote the set consisting of all subsets of  $\mathbf{4} = \{1, 2, 3, 4\}$ . For  $\sigma \in S_4$  and  $U \in X$ , let

$$\sigma U = \{\sigma(u) \in X : u \in U\}.$$

- a) Show that this defines an action of  $\mathcal{H}$  on  $X$ .
- b) For each of the following elements  $U$  of  $X$ , find  $\text{Orb}_{\mathcal{H}}(U)$  and  $\text{Stab}_{\mathcal{H}}(U)$ :

$$\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}, \{1, 2, 3, 4\}.$$

- c) For each of the following elements of  $\mathcal{H}$  find  $\text{Fix}_{\mathcal{H}}(g)$ :

$$1, (1\ 2), (1\ 2\ 3), (1\ 2\ 3\ 4), (1\ 2)(3\ 4).$$

2-10. Let  $\mathcal{H} = \text{GL}_2(\mathbb{R})$  be the group of  $2 \times 2$  invertible real matrices under matrix multiplication and let  $X = \mathbb{R}^2$  be the set of all real column vectors of length 2. For  $A \in \mathcal{H}$  and  $\mathbf{x} \in X$  let  $A\mathbf{x}$  be the usual product.

- a) Show that this defines an action of  $\mathcal{H}$  on  $X$ .
- b) Find the orbit and stabilizer of each the following vectors:

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

- c) For each of the following matrices  $A$  find  $\text{Fix}_{\mathcal{H}}(A)$ :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & -3 \end{pmatrix}, \begin{pmatrix} \sin \theta & \cos \theta \\ \cos \theta & -\sin \theta \end{pmatrix}, \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix},$$

where  $\theta, u \in \mathbb{R}$  with  $u \neq 0$ .

2-11. [*Challenge question*] Using the same group  $\mathfrak{tt} = \text{GL}_2(\mathbf{R})$  and notation as in the previous question, let  $Y$  denote the set of all lines through the origin in  $\mathbf{R}^2$ . For  $A \in \mathfrak{tt}$  and  $L \in Y$ , let

$$AL = \{A\mathbf{x} \in \mathbf{R}^2 : \mathbf{x} \in L\}.$$

- Show that  $AL$  is always a line and that this defines an action of  $\mathfrak{tt}$  on  $Y$ .
- For each of the following vectors  $\mathbf{v}$  find the line  $L_{\mathbf{v}}$  through the origin containing it and find the orbit and stabilizer of  $L_{\mathbf{v}}$ :  

$$\begin{matrix} \Sigma & \Sigma & \Sigma & \Sigma & \Sigma & \Sigma \\ 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}$$
- For each of the matrices  $A$  in (c) of the previous question, find  $\text{Fix}_{\mathfrak{tt}}(A)$  for this action.

$$\begin{matrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{matrix}$$

2-12. Let  $\mathfrak{tt} = \text{Sym}(\text{Tet})$  be the symmetry group of the regular tetrahedron Tet with vertices  $A, B, C, D$ . Let  $X$  denote the set of edges of Tet. For  $\phi \in \mathfrak{tt}$  and  $E \in X$  let

$$\phi E = \{\phi(P) \in \text{Tet} : P \in E\}.$$

- Show that  $\phi E$  is an edge and that this defines an action of  $\mathfrak{tt}$  on  $X$ .
- Find  $\text{Orb}_{\mathfrak{tt}}(E)$  and  $\text{Stab}_{\mathfrak{tt}}(E)$  for the edge  $AB$ .
- For each of the following elements of  $\mathfrak{tt}$  find  $\text{Fix}_{\mathfrak{tt}}(g)$ :

$$1, (AB), (AB\ C), (AB\ C\ D), (AB)(C\ D).$$

2-13. Let  $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$  and  $\mathfrak{tt} = ((1\ 2\ 3\ 4\ 5\ 6)(7\ 8))$  be the cyclic subgroup of  $S_7$  acting on  $X$  in the obvious way. How many orbits does this action of  $\mathfrak{tt}$  have?

2-14. How many distinguishable 5-bead circular necklaces can be made where each bead has to be a different colour chosen from 5 colours? Here two such necklaces are deemed to be indistinguishable if one can be obtained from the other by a combination of rotations and flips. What if the number of colours used is 6? 7? 8?

What if we only allow rotations between indistinguishable necklaces?

2-15. How many distinguishable regular tetrahedral dice can be made where each face has one of the numbers 1,2,3,4 on it? Here two such dice are deemed to be indistinguishable if one can be obtained from the other by a rotation.

What about if we allow arbitrary symmetries between indistinguishable such dice?

## CHAPTER 3

### Arithmetic functions

#### 1. Definition and examples of arithmetic functions

Let  $\mathbf{Z}^+ = \mathbf{N}_0 - \{0\}$  be the set of positive integers. A function  $\psi : \mathbf{Z}^+ \rightarrow \mathbf{R}$  (or  $\psi : \mathbf{Z}^+ \rightarrow \mathbf{C}$ ) is called a real (or complex) *arithmetic function* if  $\psi(1) = 1$ . There are many important and interesting examples.

EXAMPLE 3.1. The following are all real arithmetic functions:

(a) The 'identity' function

$$\text{id} : \mathbf{Z}^+ \rightarrow \mathbf{R}; \quad \text{id}(n) = n.$$

(b) The Euler function  $\phi : \mathbf{Z}^+ \rightarrow \mathbf{R}$  of Theorem 2.24.

(c) For each positive natural number  $r$ ,

$$\sigma_r : \mathbf{Z}^+ \rightarrow \mathbf{R}; \quad \sigma_r(n) = \sum_{d|n} d^r.$$

$\sigma_1$  is often denoted  $\sigma$ ;  $\sigma(n)$  is equal to the sum of the (positive) divisors of  $n$ .

(d) The function given by

$$\delta : \mathbf{Z}^+ \rightarrow \mathbf{R}; \quad \delta(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

(e) The function given by

$$\eta : \mathbf{Z}^+ \rightarrow \mathbf{R}; \quad \eta(n) = 1.$$

The set of all real (or complex) arithmetic functions will be denoted by  $\text{AFR}$  (or  $\text{AFC}$ ).

An arithmetic function  $\psi$  is called (*strictly*) *multiplicative* if

$$\psi(mn) = \psi(m)\psi(n) \quad \text{whenever } \gcd(m, n) = 1.$$

By Theorem 2.24(b), the Euler function is strictly multiplicative. In fact, each of the functions in Example 3.1 is strictly multiplicative.

An important example is the *Möbius function*  $\mu : \mathbf{Z}^+ \rightarrow \mathbf{R}$  defined as follows. If  $n \in \mathbf{Z}^+$  then by the Fundamental Theorem of Arithmetic and Corollary 1.19, we have the prime power factorization  $n = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ , where for each  $j$ ,  $p_j$  is a prime,  $1 \leq r_j$  and  $2 \leq p_1 < p_2 < \cdots < p_t$ .

We set

$$\mu(n) = \mu(p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}) = \begin{cases} 0 & \text{if any } r_j > 1, \\ (-1)^t & \text{if all } r_j = 1. \end{cases}$$

So for example, if  $n = p$  is a prime,  $\mu(p) = -1$ , while  $\mu(p^2) = 0$ . Also,  $\mu(60) = \mu(2^2 \times 3 \times 5) = 0$ .

PROPOSITION 3.2. *The Möbius function  $\mu$  is multiplicative.*



Proof. This follows from the definition and the fact that the prime power factorizations of two coprime natural numbers  $m, n$  have no common prime factors. Q

So for example,

$$\mu(105) = \mu(3)\mu(5)\mu(7) = (-1)^3 = -1.$$

PROPOSITION 3.3. *The Möbius function  $\mu$  satisfies*

$$\sum_{d|n} \mu(d) = 1, \quad \text{if } n = 1, \\ \sum_{d|n} \mu(d) = 0 \quad \text{if } n \neq 1.$$

Proof. By Induction on  $r$ , the number of prime factors in the prime power factorization of  $n = p_1^{r_1} \cdots p_r^{r_r}$ , so  $r = r_1 + \cdots + r_t$ .

If  $r = 1$ , then  $n = p$  is prime and  $\mu(p) = -1$ , hence

$$\sum_{d|p} \mu(d) = 1 - 1 = 0.$$

Assume that whenever  $r < k$ . Then if  $r = k$ , let  $n = mp_t^{r_t}$  where  $p_t$  is a prime factor of  $n$ . Then  $\mu(n) = \mu(m)\mu(p_t^{r_t})$  and so

$$\sum_{d|n} \mu(d) = \sum_{d|m} (\mu(d) + \mu(dp_t)) = \sum_{d|m} (\mu(d) + \mu(d)\mu(p_t)) = \sum_{d|m} \mu(d)(1 - 1) = 0.$$

This gives the Inductive Step. Q

## 2. Convolution and Möbius Inversion

Let  $\theta, \psi : \mathbb{Z}^+ \rightarrow \mathbb{R}$  (or  $\mathbb{C}$ ) be arithmetic functions. The *convolution* of  $\theta$  and  $\psi$  is the function  $\theta * \psi$  for which

$$\theta * \psi(n) = \sum_{d|n} \theta(d)\psi(n/d).$$

PROPOSITION 3.4. *The convolution of two arithmetic functions is an arithmetic function. Moreover,  $*$  satisfies*

(a) *for arithmetic functions  $\alpha, \beta, \gamma$ ,*

$$(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma);$$

(b) *for an arithmetic function  $\theta$ ,*

$$\delta * \theta = \theta = \theta * \delta;$$

(c) *for an arithmetic function  $\theta$ , there is a unique arithmetic function  $\tilde{\theta}$  for which*

$$\theta * \tilde{\theta} = \delta = \tilde{\theta} * \theta;$$

(d) *For two arithmetic functions  $\theta, \psi$ ,*

$$\theta * \psi = \psi * \theta.$$

Hence  $(\text{AF}_{\mathbb{R}}, *)$  and  $(\text{AF}_{\mathbb{C}}, *)$  are commutative groups.

Proof.

(a) For  $n \in \mathbb{Z}^+$ ,

$$\begin{aligned} (\alpha * \beta) * \gamma(n) &= \sum_{d|n} \alpha * \beta(d) \gamma(n/d) \\ &= \sum_{d|n} \sum_{k|d} \alpha(k) \beta(d/k) \gamma(n/d) \\ &= \sum_{k|d, d|n} \alpha(k) \beta(d/k) \gamma(n/d), \end{aligned}$$

and similarly

$$, \alpha * (\beta * \gamma)(n) = \sum_{k|d, d|n} \alpha(k) \beta(d/k) \gamma(n/d).$$

Hence  $(\alpha * \beta) * \gamma(n) = \alpha * (\beta * \gamma)(n)$  for all  $n$ , so  $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$ .

(b) We have

$$\delta * \theta(n) = \sum_{d|n} \delta(d) \theta(n/d) = \theta(n),$$

and similarly  $\theta * \delta(n) = \theta(n)$ .

(c) Take  $t_1 = 1$ . We will show by Induction that there are numbers  $t_n$  for which

$$\sum_{d|n} t_d \theta(n/d) = \delta(n).$$

Suppose that for some  $k > 1$  we have such numbers  $t_n$  for  $n < k$ . Consider the equation

$$\sum_{d|k} t_d \theta(k/d) = \delta(k) = 0.$$

Rewriting this as

$$t_k = - \sum_{\substack{d|k \\ d \neq k}} t_d \theta(k/d),$$

we see that  $t_k$  is uniquely determined from this equation. Now define  $\tilde{\theta}$  by  $\tilde{\theta}(n) = t_n$ . By construction,

$$\theta * \tilde{\theta}(n) = \sum_{d|n} \theta(n/d) \tilde{\theta}(d) = \delta(n).$$

By (d) we also have  $\tilde{\theta} * \theta = \theta * \tilde{\theta}$ .

(d) We have

$$\theta * \psi(n) = \sum_{d|n} \theta(d) \psi(n/d) = \sum_{d|n} \psi(n/d) \theta(d) = \sum_{k|n} \psi(k) \theta(n/k) = \psi * \theta(n). \quad \text{Q}$$

In each of the groups  $(\text{AFR}, *)$  and  $(\text{AFC}, *)$ , the inverse of an arithmetic function  $\theta$  is  $\tilde{\theta}$ . Here is an important example.

**PROPOSITION 3.5.** *The inverse of  $\eta$  is  $\tilde{\eta} = \mu$ , the Möbius function.*

Proof. Recall that  $\eta(n) = 1$  for all  $n$ . By Proposition 3.3 we have

$$\sum_{d|n} \mu(d)\eta(n/d) = \sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1, \\ 0 & n > 1. \end{cases}$$

Hence  $\mu = \tilde{\eta}$  is the inverse of  $\eta$  by the proof of Proposition 3.4(c). Q

THEOREM 3.6 (Möbius Inversion). *Let  $f, g: \mathbb{Z}^+ \rightarrow \mathbb{R}$  (or  $f, g: \mathbb{Z}^+ \rightarrow \mathbb{C}$ ) be arithmetic functions satisfying*

$$f(n) = \sum_{d|n} g(d) \quad (n \in \mathbb{Z}^+).$$

Then

$$g(n) = \sum_{d|n} f(d)\mu(n/d) \quad (n \in \mathbb{Z}^+).$$

Proof. Notice that  $f = g * \eta$  from which we have

$$g = g * \delta = g * (\eta * \mu) = (g * \eta) * \mu = f * \mu.$$

Hence for  $n \in \mathbb{Z}^+$ ,

$$g(n) = \sum_{d|n} f(d)\mu(n/d). \quad \text{Q}$$

EXAMPLE 3.7. Use Möbius Inversion to find a formula for  $\phi(n)$ , where  $\phi$  is the Euler function.

SOLUTION. By Theorem 2.24(d),

$$\sum_{d|n} \phi(d) = n.$$

This can be rewritten as the equation  $\phi * \eta = \text{id}$  where  $\text{id}(n) = n$ . Applying Möbius Inversion gives  $\phi = \text{id} * \mu$ , i.e.,

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = \sum_{d|n} \mu(n/d) d. \quad \text{Q}$$

So for example, if  $n = p^r$  where  $p$  is a prime and  $r \geq 1$ ,

$$\phi(p^r) = \sum_{d|p^r} \mu(d) \frac{p^r}{d} = \sum_{0 \leq s \leq r} \mu(p^s) p^{r-s} = \mu(1)p^r + \mu(p)p^{r-1} = p^r - p^{r-1} = (p-1)p^{r-1}.$$

EXAMPLE 3.8. Show that the function  $\sigma = \sigma_1$  satisfies

$$\sum_{d|n} \mu(d)\sigma(n/d) = n \quad (n \in \mathbb{Z}^+).$$

SOLUTION. By definition,

$$\sigma(n) = \sum_{d|n} d,$$

hence  $\sigma = \text{id} * \eta$ . By Möbius Inversion,

$$\text{id} = \text{id} * \delta = \text{id} * (\eta * \mu) = (\text{id} * \eta) * \mu = \sigma * \mu = \mu * \sigma,$$

so for  $n \in \mathbb{Z}^+$ ,

$$n = \sum_{d|n} \mu(d)\sigma(n/d) = \sum_{d|n} \sigma(d)\mu(n/d). \quad \text{Q}$$

PROPOSITION 3.9. *If  $\theta, \psi$  are multiplicative arithmetic functions, then  $\theta * \psi$  is multiplicative.*

Proof. If  $m, n$  be coprime positive integers,

$$\begin{aligned}
 \theta * \psi(mn) &= \sum_{d|mn} \theta(d) \psi(mn/d) \\
 &= \sum_{\substack{d|mn \\ r|m \\ s|n}} \theta(rs) \psi(mn/rs) \\
 &= \sum_{\substack{r|m \\ s|n}} \theta(r) \theta(s) \psi((m/r)(n/s)) \\
 &= \sum_{\substack{r|m \\ s|n}} \theta(r) \theta(s) \psi(m/r) \psi(n/s) \\
 &= \sum_{r|m} \theta(r) \psi(m/r) \sum_{s|n} \theta(s) \psi(n/s) \\
 &= \theta * \psi(m) \theta * \psi(n).
 \end{aligned}$$

Hence  $\theta * \psi$  is multiplicative. Q

COROLLARY 3.10. *Suppose that  $\theta$  is a multiplicative arithmetic function, and  $\psi$  is the arithmetic function satisfying*

$$\theta(n) = \sum_{d|n} \psi(d) \quad (n \in \mathbb{Z}^+).$$

*Then  $\psi$  is multiplicative.*

Proof.  $\theta = \psi * \eta$ , so by Möbius Inversion,  $\psi = \theta * \mu$ , implying that  $\psi$  is multiplicative. Q



### Problem Set 3

3-1. Let  $\tau : \mathbb{Z}^+ \rightarrow \mathbb{R}$  be the function for which  $\tau(n)$  is the number of positive divisors of  $n$ .

a) Show that  $\tau$  is an arithmetic function.

b) Suppose that  $n = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$  is the prime power factorization of  $n$ , where  $2 \leq p_1 < p_2 < \cdots < p_t$  and  $r_j > 0$ . Show that

$$\tau(p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}) = (r_1 + 1)(r_2 + 1) \cdots (r_t + 1).$$

c) Is  $\tau$  multiplicative?

d) Show that  $\eta * \eta = \tau$ .

3-2. Show that each of the functions  $\sigma_r (r \in \mathbb{Z})$  of Example 3.1 are multiplicative.

3. For each  $r \in \mathbb{N}_0$  define the arithmetic function  $[r] : \mathbb{Z}^+ \rightarrow \mathbb{R}$  by

$$[r](n) = n^r.$$

In particular,  $[0] = \eta$  and  $[1] = \text{id}$ .

a) Show that  $[r]$  is multiplicative.

b) If  $r > 0$ , show that  $\sigma_r = [r] * \eta$ . Deduce that  $\sigma_r$  is multiplicative.

c) Show that  $[r] * [r]$  satisfies  $[r] * [r](n) = n^r \tau(n)$ .

d) Find a general formula for  $[r] * [s](n)$  when  $s < r$ .

3-4. For  $n \in \mathbb{Z}^+$ , prove the following formulæ, where the functions are defined in the text or in earlier questions.

$$(a) \sum_{d|n} \mu(d) \sigma(n/d) = n; \quad (b) \sum_{d|n} \mu(d) \tau(n/d) = 1; \quad (c) \sum_{d|n} \sigma_r(d) \mu(n/d) = n^r.$$

## CHAPTER 4

### Finite and infinite sets, cardinality and countability

The natural numbers originally arose from counting elements in sets. There are two very different possible ‘sizes’ for sets, namely *finite* and *infinite*, and in this section we discuss these concepts in detail.

#### 1. Finite sets and cardinality

For a positive natural number  $n \neq 1$ , set

$$\mathbf{n} = \{1, 2, 3, \dots, n\}.$$

If  $n = 0$ , let  $\mathbf{0} = \emptyset$ . Then the set  $\mathbf{n}$  has  $n$  elements and we can think of it as the standard set of that size.

DEFINITION 4.1. Let  $f: X \rightarrow Y$  be a function.

- $f$  is an *injection* or *one-one* (1-1) if for  $x_1, x_2 \in X$ ,

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

- $f$  is a *surjection* or *onto* if for each  $y \in Y$ , there is an  $x \in X$  such that  $y = f(x)$ .
- $f$  is a *bijection* or *1-1 correspondence* if  $f$  is both injective and surjective. Equivalently,  $f$  is a bijection if and only if it has an inverse  $f^{-1}: Y \rightarrow X$ .

DEFINITION 4.2. A set  $X$  is *finite* if for some  $n \in \mathbb{N}_0$  there is a bijection  $\mathbf{n} \rightarrow X$ .  $X$  is *infinite* if it is not finite.

The next result is a formal version of what is usually called the *Pigeonhole Principle*.

THEOREM 4.3 (Pigeonhole Principle: first version).

- (a) If there is an injection  $\mathbf{m} \rightarrow \mathbf{n}$  then  $m \leq n$ .
- (b) If there is a surjection  $\mathbf{m} \rightarrow \mathbf{n}$  then  $m \geq n$ .
- (c) If there is a bijection  $\mathbf{m} \rightarrow \mathbf{n}$  then  $m = n$ .

Proof.

- (a) We will prove this by Induction on  $n$ . Consider the statement

$$P(n): \text{For } m \in \mathbb{N}_0, \text{ if there is an injection } \mathbf{m} \rightarrow \mathbf{n} \text{ then } m \leq n.$$

When  $n = 0$ , there is exactly one function  $\emptyset \rightarrow \emptyset$  (the identity function) and this is a bijection; if  $m > 0$  then there are no functions  $\mathbf{m} \rightarrow \emptyset$ . So  $P(0)$  is true.

Suppose that  $P(k)$  is true for some  $k \in \mathbb{N}_0$  and let  $f: \mathbf{m} \rightarrow \mathbf{k} + 1$  be an injection. We have two cases to consider: (i)  $k + 1 \in \text{im } f$ , (ii)  $k + 1 \notin \text{im } f$ .

(i) For some  $r \in \mathbf{m}$  we have  $f(r) = k + 1$ . Consider the function  $g : \mathbf{m} - \mathbf{1} \rightarrow \mathbf{k}$  given by

$$g(j) = \begin{cases} f(j) & \text{if } 0 \leq j < r, \\ f(j+1) & \text{if } r \leq j < m. \end{cases}$$

Then  $g$  is an injection, so by the assumption that  $m - 1 \leq k$ , hence  $m \leq k + 1$ .

(ii) Consider the function  $h : \mathbf{m} \rightarrow \mathbf{k}$  given by  $h(j) = f(j)$ . Then  $h$  is an injection, and by the assumption that  $P(k)$  is true,  $m \leq k$  and so  $m \leq k + 1$ .

In either case we have established that  $P(k) \rightarrow P(k + 1)$ .

By PMI,  $P(n)$  is true for all  $n \in \mathbf{N}_0$ .

(b) This time we proceed by Induction on  $m$ . Consider the statement

$Q(m)$ : For  $n \in \mathbf{N}_0$ , if there is a surjection  $\mathbf{m} \rightarrow \mathbf{n}$  then  $m \leq n$ .

When  $m = 0$ , there is exactly one function  $\emptyset \rightarrow \emptyset$  (the identity function) and this is a bijection; if  $n > 0$  there are no surjections  $\emptyset \rightarrow \mathbf{n}$ . So  $Q(0)$  is true.

Suppose that  $Q(k)$  is true for some  $k \in \mathbf{N}_0$  and let  $f : \mathbf{k} + \mathbf{1} \rightarrow \mathbf{n}$  be a surjection. Let  $f^j : \mathbf{k} \rightarrow \mathbf{n}$  be the restriction of  $f$  to  $\mathbf{k}$ , i.e.,  $f^j(j) = f(j)$  for  $j \in \mathbf{k}$ . There are two cases to deal with: (i)  $f^j$  is a surjection, (ii)  $f^j$  is not a surjection.

(i) By the assumption that  $Q(k)$  is true,  $k \leq n$  which implies that  $k + 1 \leq n$ .

(ii) There must be exactly one  $s \in \mathbf{n}$  not in  $\text{im } f^j$ . Define  $g : \mathbf{k} \rightarrow \mathbf{n} - \mathbf{1}$  by

$$g(j) = \begin{cases} f^j(j) & \text{if } 0 \leq f^j(j) < s, \\ f^j(j) - 1 & \text{if } s \leq f^j(j) < k. \end{cases}$$

Then  $g$  is a surjection, so by the assumption that  $Q(k)$  is true,  $k \leq n - 1$ , hence  $k + 1 \leq n$ .

In either case, we have established that  $Q(k) \rightarrow Q(k + 1)$ .

By PMI,  $Q(n)$  is true for all  $n \in \mathbf{N}_0$ .

(c) This follows from (a) and (b) since a bijection is both injective and surjective. Q

**COROLLARY 4.4.** Suppose that  $X$  is a finite set and suppose that there are bijections  $\mathbf{m} \rightarrow X$  and  $\mathbf{n} \rightarrow X$ . Then  $m = n$ .

**Proof.** Let  $f : \mathbf{m} \rightarrow X$  and  $g : \mathbf{n} \rightarrow X$  be bijections. Using the inverse  $g^{-1} : X \rightarrow \mathbf{n}$  which is also a bijection, we can form a bijection  $h = g^{-1} \circ f : \mathbf{m} \rightarrow \mathbf{n}$ . By part (c),  $m = n$ . Q

For a finite set  $X$ , the unique  $n \in \mathbf{N}_0$  for which there is a bijection  $\mathbf{n} \rightarrow X$  is called the **cardinality** of  $X$ , denoted  $|X|$ . If  $X$  is infinite then we sometimes write  $|X| = \infty$ , while if  $X$  is finite we write  $|X| < \infty$ .

We reformulate Theorem 4.3 without proof to give some important facts about cardinalities of finite sets.

**THEOREM 4.5 (Pigeonhole Principle).** Let  $X, Y$  be two finite sets.

- (a) If there is an injection  $X \rightarrow Y$  then  $|X| \leq |Y|$ .
- (b) If there is a surjection  $X \rightarrow Y$  then  $|X| \geq |Y|$ .
- (c) If there is a bijection  $X \rightarrow Y$  then  $|X| = |Y|$ .

The name Pigeonhole Principle comes from the use of this when distributing  $m$  letters into  $n$  pigeonholes. If each pigeonhole is to receive at most one letter,  $m \leq n$ ; if each pigeonhole is to receive at least one letter,  $m \geq n$ .

Let  $X$  be a set and  $P \subseteq X$ . Then  $P$  is a **proper subset** of  $X$  if  $P \neq X$ , i.e., there is an element  $x \in X$  with  $x \notin P$ .

Notice that if  $X$  is a finite set and  $S$  a subset, then the inclusion function  $\text{inc}: S \rightarrow X$  given by  $\text{inc}(j) = j$  is an injection. So we must have  $|S| \leq |X|$ . If  $P$  is a proper subset then we have  $|P| < |X|$  and this implies that there can be no injection  $X \rightarrow P$  nor a surjection  $P \rightarrow X$ . These conditions actually characterise finite sets. In the next section we investigate how to recognise infinite sets.

## 2.

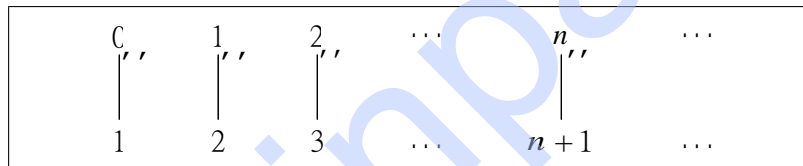
### Infinite sets

THEOREM 4.6. Let  $X$  be a set.

- (a)  $X$  is infinite if and only if there is an injection  $X \rightarrow P$  where  $P \subseteq X$  is a proper subset.
- (b)  $X$  is infinite if and only if there is a surjection  $Q \rightarrow X$  where  $Q \subseteq X$  is a proper subset.
- (c)  $X$  is infinite if and only if there is an injection  $\mathbb{N}_0 \rightarrow X$ .
- (d)  $X$  is infinite if and only if there is a subset  $T \subseteq X$  and an injection  $\mathbb{N}_0 \rightarrow T$ .

EXAMPLE 4.7. The set of all natural numbers  $\mathbb{N}_0 = \{0, 1, 2, \dots\}$  is infinite.

SOLUTION. Let us take the subset  $P = \{1, 2, 3, \dots\}$  and define a function  $f: \mathbb{N}_0 \rightarrow P$  by  $f(n) = n + 1$ .



If  $f(m) = f(n)$  then  $m + 1 = n + 1$  so  $m = n$ , hence  $f$  is injective. If  $k \in P$  then  $k \geq 1$  and so  $(k - 1) \geq 0$ , implying  $(k - 1) \in \mathbb{N}_0$  whence  $f(k - 1) = k$ . Thus  $f$  is also surjective, hence bijective. Q

EXAMPLE 4.8. Show that there are bijections between the set of all natural numbers  $\mathbb{N}_0$  and each of the sets

$$S_1 = \{2n : n \in \mathbb{N}_0\}, \quad S_2 = \{2n + 1 : n \in \mathbb{N}_0\}, \quad S_3 = \{3n : n \in \mathbb{N}_0\}.$$

In each case find a bijection and its inverse.

SOLUTION. For  $S_1$ , let  $f_1: \mathbb{N}_0 \rightarrow S_1$  be given by  $f_1(n) = 2n$ . Then  $f_1$  is a bijection: it is injective since  $2n_1 = 2n_2$  implies  $n_1 = n_2$ , and surjective since given  $2m \in S_1$ ,  $f_1(m) = 2m$ . The inverse function is given by  $f_1^{-1}(k) = k/2$ .

For  $S_2$ , let  $f_2: \mathbb{N}_0 \rightarrow S_2$  be given by  $f_2(n) = 2n + 1$ . Then  $f_2$  is a bijection: it is injective ( $2n_1 + 1 = 2n_2 + 1$  implies  $n_1 = n_2$ ) and surjective since given  $2m + 1 \in S_2$ ,  $f_2(m) = 2m + 1$ . The inverse function is given by  $f_2^{-1}(k) = (k - 1)/2$ .

For  $S_3$ , let  $f_3: \mathbb{N}_0 \rightarrow S_3$  be given by  $f_3(n) = 3n$ . Then  $f_3$  is a bijection: it is injective since  $3n_1 = 3n_2$  implies  $n_1 = n_2$ , and surjective since given  $3m \in S_3$ ,  $f_3(m) = 3m$ . The inverse function is given by  $f_3^{-1}(k) = k/3$ . Q

Notice that each of the sets  $S_1, S_2, S_3$  is a proper subset of  $\mathbb{N}_0$ , yet each is in 1-1 correspondence with  $\mathbb{N}_0$  itself.



### 3. Countable sets

DEFINITION 4.9. A set  $X$  is *countable* if there is a bijection  $S \rightarrow X$  where either  $S = \mathbf{n}$  for some  $n \in \mathbf{N}_0$  or  $S = \mathbf{N}_0$ . A countable infinite set is said to be *countably infinite* or *of cardinality*  $\aleph_0$ . An infinite set which is not countable is said to be *uncountable*.

EXAMPLE 4.10. The following sets are countably infinite.

- (a) Any infinite subset  $S \subseteq \mathbf{N}_0$ .
- (b)  $X \cup Y$  where  $X, Y$  are countably infinite.
- (c)  $X \cup Y$  where  $X$  is countably infinite and  $Y$  is finite.
- (d) The set of all ordered pairs of natural numbers

$$\mathbf{N}_0 \times \mathbf{N}_0 = \{(m, n) : m, n \in \mathbf{N}_0\}.$$

- (e) The set of all positive rational numbers

$$\mathbf{Q}^+ = \left\{ \frac{a}{b} : a, b \in \mathbf{N}_0, a, b > 0 \right\}.$$

SOLUTION.

(a) Since  $S$  is infinite it cannot be empty. Let  $S_0 = S$ . By WOP,  $S_0$  has a least element  $s_0$  say. Now consider the set  $S_1 = S - \{s_0\}$ ; this is not empty since otherwise  $S$  would be finite. Again WOP ensures that there is a least element  $s_1 \in S_1$ . Continuing, we can construct a sequence  $s_0, s_1, \dots, s_n, \dots$  of elements in  $S$  with  $s_n$  the least element of  $S_n = S - \{s_0, s_1, \dots, s_{n-1}\}$  which is never empty. Notice in particular that

$$s_0 < s_1 < \dots < s_n < \dots,$$

from which it easily follows that  $s_n \ll n$ . If  $s \in S$ , then for some  $m \in \mathbf{N}_0$  must satisfy  $m \ll s$ , so by construction of the  $s_n$  we must have  $s = s_{m_0}$  for some  $m_0$ . Hence

$$S = \{s_n : n \in \mathbf{N}_0\}.$$

Now define a function  $f: \mathbf{N}_0 \rightarrow S$  by  $f(n) = s_n$ ; this is easily seen to be a bijection.

(b) The simplest case is where  $X \cap Y = \emptyset$ . Then given bijections  $f: \mathbf{N}_0 \rightarrow X$  and  $g: \mathbf{N}_0 \rightarrow Y$  we construct a function  $h: \mathbf{N}_0 \rightarrow X \cup Y$  by

$$h(n) = \begin{cases} f\left(\frac{n}{2}\right) & \text{if } n \text{ is even,} \\ g\left(\frac{n-1}{2}\right) & \text{if } n \text{ is odd.} \end{cases}$$

Then  $h$  is a bijection.

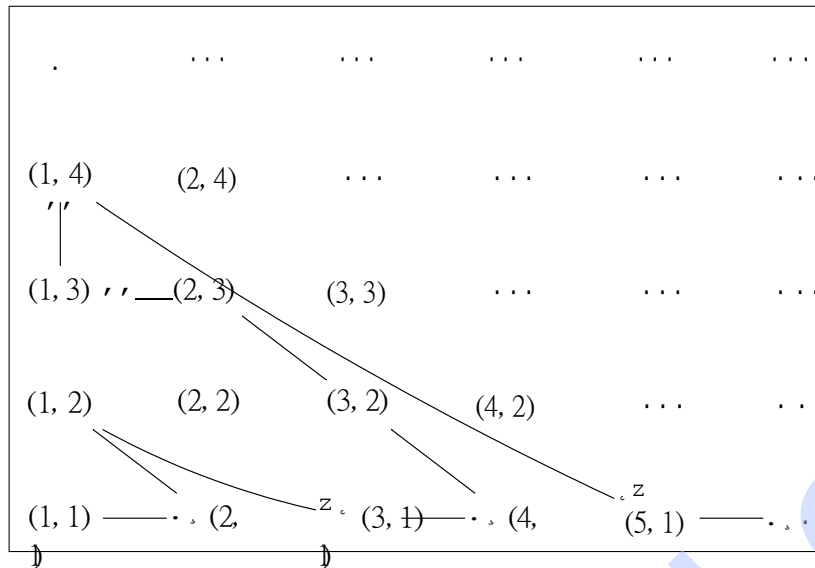
If  $Z = X \cap Y$  and  $X - Z$  and  $Y - Z$  are both countably infinite, let  $f: \mathbf{N}_0 \rightarrow X - Z$  and  $g: \mathbf{N}_0 \rightarrow Y - Z$  be bijections. Then we define  $h: \mathbf{N}_0 \rightarrow X \cup Y$  by

$$h(n) = \begin{cases} f\left(\frac{n}{2}\right) & \text{if } n \text{ is even,} \\ g\left(\frac{n-1}{2}\right) & \text{if } n \text{ is odd.} \end{cases}$$

This is again a bijection.

The case where one of  $X - X \cap Y$  and  $Y - X \cap Y$  is finite is easy to deal with by the method used for (c).

61



This gives us a sequence  $\{r_n\}_{n \in \mathbb{N}}$  of elements of  $\mathbb{Q}^+$  which contains every element exactly once. The function

$$f: \mathbb{N}_0 \rightarrow \mathbb{Q}^+; \quad f(n) = r_n,$$

is a bijection.

Q

#### 4. Power sets and their cardinality

For two sets  $X$  and  $Y$ , let

$$Y^X = \{f: X \rightarrow Y \mid f \text{ is a function}\}.$$

EXAMPLE 4.11. Let  $X$  and  $Y$  be finite sets. Then  $Y^X$  is finite and has cardinality

$$|Y^X| = |Y|^{|X|}.$$

SOLUTION. Suppose that the distinct elements of  $X$  are  $x_1, \dots, x_m$  where  $m = |X|$  and those of  $Y$  are  $y_1, \dots, y_n$  where  $n = |Y|$ . A function  $f: X \rightarrow Y$  is determined by specifying the values of the  $m$  elements  $f(x_1), \dots, f(x_m)$  of  $Y$ . Each  $f(x_k)$  can be chosen in  $n$  ways so the total number of choices is  $n^m$ . Hence  $|Y^X| = n^m$ .

Q

A particular case of this occurs when  $Y$  has two elements, e.g.,  $Y = \{0, 1\}$ . The set  $\{0, 1\}^X$  is called the **power set** of  $X$ , and has  $2^{|X|}$  elements and indeed it is often denoted  $2^{|X|}$ . It has another important interpretation.

For any set  $X$ , we can consider the set of all its subsets

$$\mathcal{P}(X) = \{U : U \subseteq X \text{ is a subset}\}.$$

Before stating and proving our next result we introduce the **characteristic** or **indicator function** of a subset  $U \subseteq X$ ,

$$\chi_U: X \rightarrow \{0, 1\}; \quad \chi_U(x) = \begin{cases} 1 & \text{if } x \in U, \\ 0 & \text{if } x \notin U. \end{cases}$$

THEOREM 4.12. For a set  $X$ , the function

$$\Theta: \mathcal{P}(X) \rightarrow \{0, 1\}^X; \quad \Theta(U) = \chi_U,$$

is a bijection.

**Proof.** The indicator function of a subset  $U \subseteq X$  is clearly determined by  $U$ , so  $\Theta$  is well defined. Also, a function  $f \in \{0, 1\}^X$  determines a corresponding subset of  $X$

$$U_f = \{x \in X : f(x) = 1\}$$

with  $\chi_{U_f} = f$ . This shows that  $\Theta$  is a bijection whose inverse function satisfies

$$\Theta^{-1}(f) = U_f.$$

**EXAMPLE 4.13.** If  $X$  is finite then  $\mathbf{P}(X)$  is finite with cardinality  $|\mathbf{P}(X)| = 2^{|X|}$ . Q

**Proof.** This follows from Example 4.11. Q

Using the standard finite sets  $\mathbf{n} = \{1, \dots, n\}$  ( $n \in \mathbf{N}_0$ ) we have

$$|\mathbf{P}(\mathbf{0})| = 2^0 = 1, |\mathbf{P}(\mathbf{1})| = 2^1 = 2, |\mathbf{P}(\mathbf{2})| = 2^2 = 4, |\mathbf{P}(\mathbf{3})| = 2^3 = 8, \dots$$

where

$$\mathbf{P}(\mathbf{0}) = \{\emptyset\},$$

$$\mathbf{P}(\mathbf{1}) = \{\emptyset, \{1\}\},$$

$$\mathbf{P}(\mathbf{2}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\},$$

$$\mathbf{P}(\mathbf{3}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

We will now see that for any set  $X$  the power set  $\mathbf{P}(X)$  is always ‘bigger’ than  $X$ .

**THEOREM 4.14** (Russell’s Paradox). *For a set  $X$ , there is no surjection  $X \rightarrow \mathbf{P}(X)$ .*

**Proof.** Suppose that  $g: X \rightarrow \mathbf{P}(X)$  is a surjection.

Consider the subset

$$W = \{x \in X : x \notin g(x)\} \subseteq X.$$

Then by surjectivity of  $g$  there is a  $w \in X$  such that  $g(w) = W$ . If  $w \in W$ , then by definition of  $W$  we must have  $w \notin g(w) = W$ , which is impossible. On the other hand, if  $w \notin W$ , then  $w \in g(w) = W$  and again this is impossible. But then  $w$  cannot be in  $W$  or the complement  $X - W$ , contradicting the fact that every element of  $X$  has to be in one or other of these subsets since  $X = W \cup (X - W)$ . Thus no such surjection can exist. Q

Russell’s Paradox is often stated in terms of ‘the set of all sets’, and the key ideas of this proof can also be used to show that no such ‘set’ can exist (can you think of a suitable argument?). It shows that naive notions of sets can lead to problems when sets are allowed to be too large. Modern set theory sets out to axiomatise the idea of a set theory to avoid such problems.

When  $X$  is finite, this result is not surprising since  $2^n > n$  for  $n \in \mathbf{N}_0$ . For  $X$  an infinite set, it leads to the idea that there are different ‘sizes’ of infinity. Before showing how this result allows us to determine some concrete examples, we give a generalization.

**COROLLARY 4.15.** *Let  $X$  and  $Y$  be sets and suppose that  $Y$  has a subset  $Z \subseteq Y$  which admits a surjection  $g: Z \rightarrow \mathbf{P}(X)$ . Then there is no surjection  $X \rightarrow Y$ .*

Proof. Suppose that  $f: X \rightarrow Y$  is a surjection. Choose any element  $P \in \mathbf{P}(X)$  and define the function

$$h: X \rightarrow \mathbf{P}(X); \quad h(x) = \begin{cases} g(f(x)) & \text{if } f(x) \in Z, \\ P & \text{if } f(x) \notin Z. \end{cases}$$

We easily see that  $h$  is a surjection, contradicting Russell's Paradox. Thus no such surjection can exist. Q

## 5. The real numbers are uncountable

THEOREM 4.16 (Cantor). *The set of real numbers  $\mathbf{R}$  is uncountable, i.e., there is no bijection  $\mathbf{N}_0 \rightarrow \mathbf{R}$ .*

Proof. Suppose that  $\mathbf{R}$  is countable and therefore the obviously infinite subset  $(0, 1] \subseteq \mathbf{R}$  is countable. Then we can list the elements of  $(0, 1]$ :

$$q_0, q_1, \dots, q_n, \dots$$

For each  $n$  we can uniquely express  $q_n$  as a non-terminating expansion infinite decimal

$$q_n = 0.q_{n,1}q_{n,2} \dots q_{n,k} \dots,$$

where for each  $k$ ,  $q_{n,k} = 0, 1, \dots, 9$  and for every  $k_0$  there is always a  $k > k_0$  for which  $q_{n,k} \neq 0$ .

Now define a real number  $p \in (0, 1]$  by requiring its decimal expansion

$$p = 0.p_1p_2 \dots p_k \dots$$

to have the property that for each  $k \geq 1$ ,

$$p_k = \begin{cases} 1 & \text{if } q_{k-1,k} \neq 1, \\ 2 & \text{if } q_{k-1,k} = 1. \end{cases}$$

Notice that this is also non-terminating. Then  $p \neq q_1$  since  $p_1 \neq q_{0,1}$ ,  $p \neq q_2$  since  $p_2 \neq q_{1,2}$ , etc. So  $p$  cannot be in the list of  $q_n$ 's, contradicting the assumption that  $(0, 1]$  is countable. Q

The method of proof used here is often referred to as *Cantor's diagonalization argument*. In particular this shows that  $\mathbf{R}$  is much bigger than the familiar subset  $\mathbf{Q} \subseteq \mathbf{R}$ , however it can be hard to identify particular elements of the complement  $\mathbf{R} - \mathbf{Q}$ . In fact the subset of all *real algebraic numbers* is countable, where such a real number is a root of a monic polynomial of positive degree,

$$X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbf{Q}[X].$$



**Problem Set 4**

4-1. Show that each of the following sets is countable:

- (a)  $\mathbb{Z}$ , the set of all integers;
- (b)  $\{n^2 : n \in \mathbb{Z}\}$ , the set of all integers which are squares of integers;
- (c)  $\{n \in \mathbb{Z} : n \neq 0\}$ , the set of all non-zero integers;
- (d)  $\mathbb{Q}$ , the set of all rational numbers;
- (e)  $\{x \in \mathbb{R} : x^2 \in \mathbb{Q}\}$ , the set of all real numbers which are square roots of rational numbers.

4-2. Show that a subset of a countable set is countable.

4-3. Let  $X$  be a countable set. If  $Y$  is a finite set, show that the cartesian product

$$X \times Y = \{(x, y) : x \in X, y \in Y\}$$

is countable.

Use Example 4.10(d) or a modification of its proof to show that this is still true if  $Y$  is countably infinite.