Products and Quotients of semigroups

Theorem 1

- If $(S, *)$ and $(T, *')$ are semigroups, then $(S \times T, *'')$ is also a semigroup, where $*''$ is defined as

$$(s_1, t_1) *'' (s_2, t_2) = (s_1 * s_2, t_1 *' t_2)$$

→ It clearly follows that if S and T a monoids with identities e_S and e_T, then $(S \times T, *'')$ is also a monoid with identity (e_S, e_T)

- Now we shall examine equivalence relations on a semigroup $(S, *)$. Since a semi-group is not merely a set, we shall find that certain equivalence relations on a semigroup gives additional information about the structure of the semigroup.

An equivalence relation R on a semigroup $(S, *)$ is called a **congruence relation** if $a R a'$ and $b R b'$ implies that $(a * b) R (a' * b')$

eg→1 consider the semigroup $(Z, +)$ and the equivalence relation R on Z defined by aRb if and only if $\underbrace{a \equiv b \pmod 2}$

⇒ $(a-b)$ is divisible by 2

show that R is a congruence relation.

Soln:

If $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$

Then $2 \mid (a-b)$ and $2 \mid (c-d)$

i.e let $a-b = 2n$ and $c-d = 2m$ where $m, n \in Z$

$$\therefore (a-b)+(c-d) = 2(m+n)$$

$$\Rightarrow (a+c) - [b+d] = 2(m+n)$$

$$\Rightarrow (a+c) \equiv [b+d] \pmod 2$$

Thus aRb and cRd implies $(a+c)R(b+d)$

Hence, R is a congruence relation by definition.

Eg 2 Let $A = \{0, 1\}$ and consider a free semigroup $(A^*, \circ)$ generated on A. Define a relation R on the set A, $\alpha R \beta$ if and only if α and β have the same Number of 1s, where $\alpha, \beta \in A^*$.
Show that R is a congruence relation on $(A^*, \circ)$.

Solution:

I - 1st show R is an equivalence relation.
II - Then show R is a congruence relation.

I (a) $\alpha R \alpha$ for $\alpha \in A^*$ $\therefore$ R is reflexive.
(b) If $\alpha R \beta$ then α and β have the same No. of 1s $\therefore$ $\beta R \alpha$ $\therefore$ R is symmetric
(c) If $\alpha R \beta$ and $\beta R \gamma$ then α, β, γ have the same No of 1s $\therefore$ $\alpha R \gamma$
$\therefore$ R is transitive

II Let $\alpha R \alpha'$ and $\beta R \beta'$ (α and α' have same No of 1s so does β & β')

Since the No of 1s in $\alpha \circ \beta$ is same as $\alpha' \circ \beta'$ it can concluded that $(\alpha \circ \beta) R (\alpha' \circ \beta')$

Thus R is a congruence relation.

eg 3 Consider a semigroup $(\mathbb{Z},+)$. Let $f(x)=x^2-x-2$ define a relation R on $\mathbb{Z}$ as

aRb if and only if $f(a)=f(b)$

Find if R is a congruence Relation.

Solution: examining $\in \mathbb{Z}$

$0 R 1$ since $f(0)=f(1)=-2$

$-1 R 2$ since $f(-1)=f(2)=0$

$-2 R 3$ since $f(-2)=f(3)=4$

$-3 R 4$ since $f(-3)=f(4)=10$

$\vdots$

$k R (-k+1)$

Steps

I: Establish if R is an equivalence relation on $(\mathbb{Z},+)$

II: Establish if R is a congruence relation on $(\mathbb{Z},+)$

- R is reflexive ($\because aRa \ \forall a \in \mathbb{Z}$)
- whenever (aRb) then bRa) $\therefore R$ is symmetric
- There does not exist $a,b,c \in \mathbb{Z}$ such that aRb, bRc and $a \not R c$ $\therefore R$ is reflexive

Hence R is an equivalence relation on $(\mathbb{Z},+)$

Now check if R is a congruence relation, i.e. if (aRa' and $bR'b$) implies $(a*b) R (a'*b')$

But $[(-1)+(-2)] \not R [(2)+(3)]$

$\therefore f(-3)=10$

and $f(5)=18$

counter example

$[(0)+(-1)] \not R [(1)+(2)]$

$\because f(-1)=0$ and $f(3)=4$

counter example

$\therefore$ R is NOT a congruence relation even though it is an equivalence relation on the semigroup $(Z, +)$

- An equivalence relation R on a semigroup $(S, *)$ determines the partition of S. Let $[a] = R(a)$ be the equivalence class containing a and S/R denote the set of all equivalence classes determined by R. The notation $[a]$ is more traditional and causes less confusion. We shall be using $[a]$ to referer to the equivalence class containing a rather than the notation of $R(a)$, the R relative set of a during the study of semigroups and groups.

Theorem 2

- If R is an congruence relation on a semigroup $(S, *)$, consider the relation $\circledast$ from $S/R \times S/R$ to S/R in which the ordered pairs $([a], [b])$ is related to $([a*b])$, $\{a, b \in S\}$ then

(a) $\circledast$ is a function from $S/R \times S/R \rightarrow S/R$ and as usual we denote $\circledast([a], [b])$ as $[a] \circledast [b]$. Thus $[a] \circledast [b] = [a*b]$

(b) $(S/R, \circledast)$ is a semigroup.

Corrolary

Let R be a congruence relation on the monoid $(S, *)$. If we define the operation $\circledast$ in S/R as $[a] \circledast [b] = [a * b]$, then $(S/R, \circledast)$ is a monoid

- S/R is called the quotient semigroup or factor semigroup
- Also observe that $\circledast$ is a type of "quotient binary relation" on S/R that is constructed from the original binary relation $*$ on S by the congruence relation R.

- eg>4. Let $A = \{0,1\}$ and consider the free semi-group $(A^*, \circ)$ generated by A. Let R be a congruence relation on A defined by $\alpha R \beta$ if and only if α and β have the same number of 1s. ; $\alpha, \beta \in A^*$

Since R is a congruence relation on the monoid $(A^*, \circ)$, we can conclude that $(S/R, \odot)$ is a monoid, where $[\alpha] \odot [\beta] = [\alpha \circ \beta]$

The identity of A^* is the empty string, Λ

(a) Establish R is an equivalence relation (b) Establish R is a congruence relation
- symmetric, reflexive, transitive

eg 5. Define a relation R on the semigroup $(Z,+)$ as aRb if and only if $a \equiv b \pmod{n}$, where $n \geq 1$
(It can be shown that $a \equiv b \pmod{n}$ is a congruence relation - do this as self study)

- Let $n=4$. Let us evaluate equivalence classes determined by the congruence relation $\equiv \pmod{4}$ on Z

$[0] = \{\cdots, -8, -4, 0, 4, 8, \cdots\} = [4] = [8] = [12] = \cdots$
$[1] = \{\cdots, -7, -3, 1, 5, 9, \cdots\} = [5] = [9] = [13] = \cdots$
$[2] = \{\cdots, -6, -2, 2, 6, 10, \cdots\} = [6] = [10] = [14] = \cdots$
$[3] = \{\cdots, -5, -1, 3, 7, 11, \cdots\} = [7] = [11] = [15] = \cdots$

These are all distinct equivalence classes that form the quotient set $Z/\equiv \pmod{4}$. It is customary to denote the quotient set $Z/\equiv \pmod{n}$ by Z_n. Z_n is a monoid with the operation $\oplus$ and identity $[0]$.

The addition table for the semigroup Z_4 with operation $\oplus$ can be obtained by using $[a] \oplus [b] = [a+b] = [r]$ where r is the remainder when $a+b$ is divided by n (4 in the case of Z_4)

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

It can be seen that in general Z_n has an equivalence class $[0], [1], [2], \cdots, [n-1]$ and that $[a] + [b] = [r]$ where r is the remainder when $(a+b)$ is divided by n.

Thus if $n=6$, $[2] \oplus [3] = [5]$, $[4] \oplus [5] = [3]$, $[3] \oplus [5] = [2]$
$[3] \oplus [3] = [0]$, $\cdots$

Let us now examine the connection between the structure of the semigroup $(S, *)$ and the Quotient semigroup $(S/R, \circledast)$, where R is an equivalence relation on $(S, *)$

- **Theorem 3**: Let R be a congruence relation on a semigroup $(S, *)$ and let $(S/R, \circledast)$ be the corresponding quotient semigroup. Then, the function $f_R : S \to S/R$ defined by $f_R(a) = [a]$ is an onto homomorphism called the natural homomorphism.

- **Fundamental Homomorphism Theorem (Theorem 4)**

Let $f : S \to T$ be a homomorphism from the semigroup $(S, *)$ onto the semigroup $(T, *')$.
Let R be the relation on S defined by $a R b$ if and only if $f(a) = f(b)$ for $a, b \in S$. Then :-
(a) R is a congruence relation.
(b) $(T, *')$ and the quotient subgroup $(S/R, \circledast)$ are isomorphic.

- **eg 6**. Let $A = \{0, 1\}$ and consider the free semigroup A^* generated by A under the operation of catination. (Note that A^* is a monoid with the empty string as its identity)
Let $\mathbb{N}$ be the set non-negative integers (i.e natural numbers). Then $\mathbb{N}$ is a semigroup under the operation of addition i.e $(\mathbb{N}, +)$.
The function $f : A^* \to \mathbb{N}$ defined by $f(\alpha) =$ No. of 1s in α is a homomorphism.
Let R be the following relation on A^*
$\alpha R \beta$ if and only if $f(\alpha) = f(\beta)$ } i.e α and β have the same number of 1s.

$\therefore A^*/R \cong \mathbb{N}$ under the isomorphism $\bar{f} : A^*/R \to \mathbb{N}$ defined by $\bar{f}([\alpha]) = f(\alpha) =$ No. of 1s in α.

Theorem 4(b) can be described by the diagram shown opposite. Here f_A is the natural Homomorphism. It follows from the definition of f_A and $\tilde{f}$ that

$$
\begin{tikzcd}
S \arrow[rr, "f"] \arrow[dr, "f_R"'] & & T \\
& S/T \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}
$$

$$\tilde{f} \circ f_R = f$$

since $(\tilde{f} \circ f_R)(a) = \tilde{f}(f_R(a)) = \tilde{f}([a]) = f(a)$

Groups :

(A special type of a monoid that has application in every area where symmetry occurs egs maths, physics, chemistry, sociology, particle physics, solution of Rubics cube; binary codes etc)

Definition: A group $(G,*)$ is a monoid, with identity e, that has the additional property that for every element $a \in G$ there exists an element $a' \in G$, such that $a*a' = a'*a = e$.

Thus a group is a set together with a binary operator $*$ on G such that:-

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

(b) The exists an unique element $e \in G$ such that $a*e = e*a = a \; \forall a \in G$

(c) For all $a \in G$, there exists an element $a' \in G$, called the inverse of a, such that $a*a' = a'*a = e$.

- Observe that if $(G,*)$ is a group, then $*$ is a binary operation, so G is closed under $*$, i.e $a*b \in G \; \forall a,b \in G$

- To simplify the notation, when only one group $(G,*)$ is under consideration and there is no possibility of confusion, the product $a*b$ of $a,b \in (G,*)$ is simply written as ab, and $(G,*)$ is also referred to as G

- A group G is said to be **Abelian** if $ab = ba \; \forall a,b \in G$ i.e a commutative group $(G,*)$ is said to be Abelian

---

- eg 1. $(Z,+)$ is an Abelian group. If $a \in Z$ then the inverse of a is $-a$.
- eg 2. $(Z^+, \times)$ is NOT a group. eg $4 \in Z^+$ has no inverse in Z^+. However $(Z^+, \times)$ is a monoid with $e = 1$
- eg 3. (Set of Non-Zero Real Numbers, $\times$) is a group; an inverse of $a \neq 0$ is $1/a$

• eg24. Let $G = \{$set of non-zero real numbers$\}$ and let $a*b = \frac{a \cdot b}{2}$

Is $(G,*)$ an Abelian Group?

Approach: verify (i) is $*$ a Binary operation
(ii) is $*$ associative.
(iii) Find the identity of $*$
(iv) Find inverse of $a \in A$
(v) verify if $*$ is commutative

(i) + (ii) $\Rightarrow$ $(G,*)$ is a semi-group.

(i) + (ii) + (iii) $\Rightarrow$ $(G,*)$ is a monoid.

(i) + (ii) + (iii) + (iv) $\Rightarrow$ $(G,*)$ is a group.

(i) + (ii) + (iii) + (iv) + (v) $\Rightarrow$ $(G,*)$ is an Abelian Group.

Solution: (a) If $a, b \in G$, then $\frac{ab}{2} \in G$ $\therefore$ $*$ is a binary operation by definition!

(b) $(a*b)*c = \frac{ab}{2} * c = \frac{abc}{4}$ and

$a*(b*c) = a * \frac{bc}{2} = \frac{abc}{4}$ $\therefore$ $*$ is an associative operation.

(c) 2 is the identity of $*$ for all $a \in G$

$a*2 = \frac{a \cdot 2}{2} = a = 2 \cdot \frac{a}{2} = 2*a$ (ie $a*e = e*a = a$)

(d) If $a \in G$ then $a' = 4/a$ is an inverse of a

since $a*a' = a*\frac{4}{a} = \frac{a(4/a)}{2} = 2 = e$

and $a'*a = \frac{4}{a}*a = \frac{(4/a) \cdot a}{2} = 2 = e$

(e) Since $a*b = b*a$ $\forall a, b \in G$ $\therefore$ $(G,*)$ is commutative

Hence $(G,*)$ is an Abelian Group.

Properties of Groups :

1. If G is a group, each element $a \in G$ has exactly one inverse in G.

2. If G is a group and $a, b, c \in G$, then
   (a) $a*b = a*c$ (or $ab = ac$) implies $b = c$ (left cancellation property)
   (b) $b*a = c*a$ (or $ba = ca$) implies $b = c$ (right cancellation property)

3. Let G be a group and let $a \in G$. Define a function $M_a : G \to G$ by the formula $M_a(g) = ag$, then M_a is one-to-one.

4. If G is a group and $a, b \in G$, then
   (a) $(a^{-1})^{-1} = a$
   (b) $(ab)^{-1} = b^{-1}a^{-1}$

5. (c) The equation $ax = b$ has a unique solution in G
   (d) The equation $ya = b$ has a unique solution in G

Proof for 1 : Let a' and a'' be the two inverses of a

$a'(aa'') = a' \cdot e = a'$ and $(a'a)a'' = ea'' = a''$

As G is a group $*$ is associative, i.e. $a'(aa'') = (a'a)a''$

i.e $a' = a''$. i.e the inverse of a is unique.

Note : The inverse of a is usually denoted as a^{-1}. Thus in a group $aa^{-1} = a^{-1}a = e$

Proof for 2 : suppose $ab = ac$ (multiplying by a^{-1} on left side)

$a^{-1}(ab) = a^{-1}(ac)$

or $(a^{-1}a)b = (a^{-1}a)c$ (by associativity)

or $eb = ec$ (by definition of inverse)

or $b = c$ (by definition of identity)

Similarly $ba = ca$ implies $b = c$.

Proof for 4(a)

show that a acts as inverse of a^{-1}

by definition of inverse $a^{-1}a = aa^{-1} = e$. Since inverse of a is unique, it can be concluded that $(a^{-1})^{-1} = a$

4(b) $(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1})$
$= a(ea^{-1}) = aa^{-1} = e$

similarly $(b^{-1}a^{-1})(ab) = e$

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

Proof for 5(c) : The element $x = a^{-1}b$ is a solution of the equation $ax = b$, since $a(a^{-1}b) = (aa^{-1})b = eb = b$

suppose x_1 and x_2 are two solutions of the equation $ax = b$, then $ax_1 = b$ and $ax_2 = b$
i.e. $ax_1 = ax_2$. using left cancellation rule $x_1 = x_2$

similarly it can be shown that $ya = b$ has a unique solution in G.

• Multiplication Table

If group G has finite number of elements, then its operations can be given by a table, which is generally called a multiplication table. The multiplication of $G = \{a_1, a_2, \dots, a_n\}$ must satisfy the following:-

1. The row labelled by e must be $a_1, a_2, \dots, a_n$ and the column labelled by e must be $\begin{matrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{matrix}$

2. It follows from properties 4(a) and 4(b) that each element b of the group must appear exactly once in each row / column of the table.
   - Thus each row / column is a permutation of the elements $a_1, a_2, \dots, a_n$ of G and each row/column determines a different permutation.

• If G is a group that has finite number of elements, G is called a finite group and the order of G is $|G|$

Multiplication Tables of non-isomorphic groups of order n

(We shall examine multiplication tables of groups of order 1 to 4)

*	e
e	e

• If G is a group of order 1, then $G = \{e\}$ and we have $ee = e$

• Let $G = \{e, a\}$ be a group of order 2. Then the multiplication table will be as shown

*	e	a
e	e	a
a	a	e

→ After filling in row/column corresponding to e, the blank can be filled in by a or e

→ ensure associativity and other properties are preserved

(Working sheet next page)

- Let $G = \{e, a, b\}$ be a group of order 3. Then the multiplication table will be as shown below

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

ensure that associativity and othe properties relating to permutation preserved for each row / column.

- Let $G = \{e, a, b, c\}$ be a group of order 4. Then the multiplication tables will be as shown in Tables 1 to 4. Each of these tables satisfy the associative and other properties of the group.

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

Table : 1

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

Table : 2

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

Table : 3

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

Table : 4

- There are 4 possible multiplication tables for a group of order 4
- A group of order 4 is Abelian
- There are only two different non-isomorphic groups of order 4 (more latter)

(Worksheet)

$G = \{e, a, b\}$

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

$G = \{e, a, b, c\}$

Case I : each element is an inverse of itself
$a*a^{-1} = e$, $b*b^{-1} = e$, $cc^{-1} = e$,

Case II : $a*a^{-1} = e = a^{-1}*a$ (ie a is the inverse of itself)
$c^{-1} = b$ and $b^{-1} = c$

Case III : b is the inverse of itself ie $b*b^{-1} = e$
$a = c^{-1}$ and $c = a^{-1}$

Case IV : $c*c^{-1} = e = c^{-1}*c$
$a = b^{-1}$ and $b = a^{-1}$ i.e $a*b = e = b*a$

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

Case I :

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

Case II

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

Case III

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

Case IV

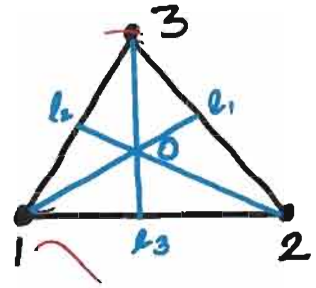
• eg 5. Let $B = \{0, 1\}$ and let $*$ be the operation defined on B as shown in the table. Is B a group?

$*$	0	1
0	0	1
1	1	0

– It can be observed from the table that $*$ is associative and B is a group with 0 as the identity element and every element being it's own inverse.

Symmetry of Geometric Figures

• eg 6. Consider the equilateral triangle shown in the figure below with vertices 1, 2, 3. A symmetry of the triangle (or any other geometric figure) is a one-to-one correspondence from the set of points forming the triangle (or the geometric figure) to itself that preserves the distance between any adjacent points.



• Let l_1, l_2, l_3 be the angular bisectors of the corresponding angles, as shown in figure, and let O be their point of intersection.

On examining the symmetries of this triangle, it is evident that there are two types of symmetries, one relating to reflection and other relating to rotation.

I (a). There is counter-clockwise rotation, f_2, of the triangle about O through $120°$. Then f_2 can be written as the permutation

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

I(b). Similarly, a counter-clockwise rotation, f_3, about O through $240°$, is $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

I(c). Finally, a counter-clockwise rotation, f_1, about O through $360°$, is $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, which is the identity permutation.

II. Three additional symmetries of the triangle g_1, g_2 and g_3 can be obtained by reflection about the lines l_1, l_2 and l_3 respectively, denoted by permutations

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

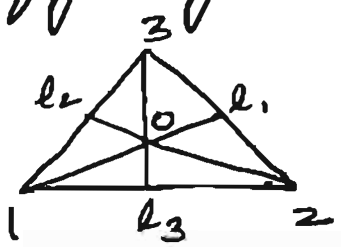
Note that the set of all symmetries of the triangle are described by the permutation on set $\{1, 2, 3\}$ and can be denoted by S_3. Thus $S_3 = \{f_1, f_2, f_3, g_1, g_2, g_3\}$

Let $*$ be the operation "followed by" on the set S_3 for which the multiplication table as given below:

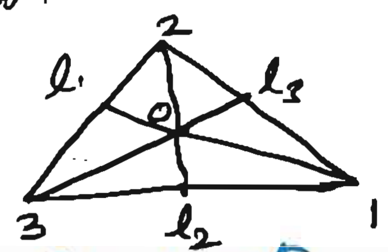
$*$	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_3	g_2	f_1	f_2	f_3
g_2	g_2	g_1	g_3	f_2	f_1	f_2
g_3	g_3	g_2	g_1	f_2	f_3	f_1

- The entries in the table can be obtained in two ways → algebrically. → geometrically.

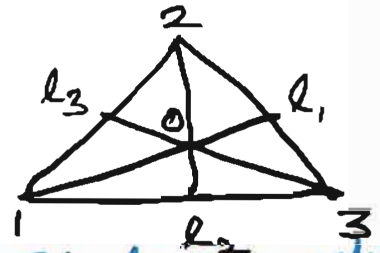
- eg: $f_2 * g_2$ can be computed geometrically and proceed as in figure given below:



Given Triangle



Triangle after applying f_2



Triangle after applying g_2 on triangle on left.

$= g_1$

NOTE : "followed by" refers to the geometric order

To compute $f_2 * g_2$ algebrically, compute $f_2 \circ g_2$, where $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

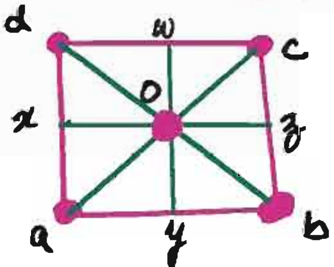
$$f_2 \circ g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = g_1$$

- Since composition of functions is always associative, we see that $*$ is an associative operator on S_3.
- Also f_1 is the identity of $*$ in S_3
- every element of S_3 has an unique inverse in S_3
  - egs $f_2^{-1} = f_3$, $g_1^{-1} = g_1$ etc
- Hence S_3 is a group called the group of symmetries of the triangle
- Note that S_3 is NOT an Abelian group.

- eg 7. The set of all permutations of n elements is called a group of order $n!$ under the operation of composition. This group is called the symmetric group of n letters and is denoted by S_n

* We have seen that S_3 also represents the group of symmetries of equilateral triangles.

* It is also feasible to consider the group of symmetries of a square.



- 4 rotations
- 4 reflections.

However, it turns out that this group is of order 8. So it does NOT agree with the group S_n, whose order is $4! = 24$.

• eg 8. The monoid Z_n can be shown to be a group.

soln (Recall that the quotient set $Z/\equiv \bmod (n)$, denoted by Z_n is a monoid with operation $\oplus$ and identity $[0]$ where $[a] \oplus [b] = [a+b] = [r]$)

R is defined on subgroup $(Z,+)$ as aRb if and only if $a \equiv b \pmod n$, $n \in Z^+$

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

Let $[a] \in Z_n$, then it is assured that $0 \leq a < n$ and also $[n-a] \in Z_n$

Since $[a] \oplus [n-a] = [a+n-a] = [n] = [0]$, it can be concluded that $[n-a]$ is the inverse of $[a]$.

Thus by definition, Z_n is a group

Note that Z_n is an Abelian group.

Subsets of a Group

• Let H be a subset of a group G, such that :-

(a) The identity of $G \in H$.

(b) If $a, b \in H$, then $ab \in H$.

(c) If $a \in H$, then $a^{-1} \in H$.

Then H is called a subgroup of G.

(a) and (b) says that H is a submonoid of G. Thus subgroups can be viewed as a submonoid having properties (b) and (c)

Note: If G is a group and H is a subgroup of G, then H is also a group w.r.t the operation in G, since associativity in G also holds in H.

- **eg> 9.** Let G be a group, then G and $H = \{e\}$ are subgroups of G called the trivial subgroups of G.

- **eg> 10.** Consider S_3, the group of symmetries of equilateral triangles. It is easy to verify that $H = \{f_1, f_2, f_3\}$ is a subgroup of G.

- **eg> 11.** Let A_n be the set of even permutations in the group S_n. It can be shown from the definition of even permutation that A_n is a sub-group of S_n called the alternating group of n letters.

- Let $(G, *)$ and $(G', *')$ be two groups. Since groups are also semigroups, isomorphism and homomorphism can be considered from $(G, *)$ to $(G', *')$

- Since an isomorphism must be one-to-one and onto function (in addition to being everywhere defined), it follows that the two groups whose orders are unequal cannot be isomorphic.

- **eg> 13.** Let G be a group of real numbers under the operation of addition; and let G' be a group of positive real numbers under the operation of multiplication. Let $f : G \to G'$ be defined by $f(x) = e^x$. Prove or disprove that f is an isomorphism.

<u>Solution</u> (Approach: establish f is one-to-one, onto and everywhere defined; image of products = product of images)

- If $f(a) = f(b)$ then $e^a = e^b \Rightarrow a = b$. Thus f is one-to-one
- If $c \in G'$, then $\ln(c) \in G$ and $f(\ln(c)) = e^{\ln(c)} = c$ so f is onto as well as everywhere defined.

- $f(a+b) = e^{a+b} = e^{a} \cdot e^{b} = f(a) \times f(b)$

Hence f is an isomorphism.

{i.e. set of all permutations of n letters}

- eg 14. Let G be a symmetric group of n letters, and let G' be the group Z_n (the quotient set $Z/\equiv(\text{mod } n)$) under addition.

Let $f: G \to G'$ be defined as follows for $p \in G$,

$$f(p) = \begin{cases} 0 & \text{if } p \in A_n \text{ (the subgroup of all even permutations of } G) \\ 1 & \text{if } p \notin A_n \end{cases}$$

It can be easily established that f is a homomorphism.

- eg 15. Let G be a group of integers under addition $(Z,+)$, and let G' be the group Z_n (the quotient set $Z/\equiv \text{mod}(n)$ under addition) $(Z_n,+)$ $n \in Z^+$

Let $f: G \to G'$ be defined as follows:

If $m \in G$, then $f(m) = [x]$, where x is the remainder when m is divided by n.

Prove or disprove that f is an homomorphism from G to G'

Solution:

- Let $[x] \in Z_n$, then it can be assumed that $0 \le x < n$ so $x = 0 \cdot n + x$, which means that the remainder when x is divided by n is x. Hence $f(x) = [x]$, and thus f is an everywhere defined function (or into function)

• Let $a, b \in G$ be expressed as

$$a = q_1 n + r_1 \;, \quad 0 \le r_1 < n \;;\; r_1 ; q_1 \in \mathbb{Z} \quad \text{——— (1)}$$

$$b = q_2 n + r_2 \;, \quad 0 \le r_2 < n \;;\; r_2 , q_2 \in \mathbb{Z} \quad \text{——— (2)}$$

so that $f(a) = [r_1]$ and $f(b) = [r_2]$

Then $f(a) + f(b) = [r_1] + [r_2] = [r_1 + r_2]$

To find $[r_1 + r_2]$ remember that $r_1 + r_2$ is divided by n

i.e write $r_1 + r_2 = q_3 n + r_3 \;, 0 \le r_3 < n \;;\; r_3 , q_3 \in \mathbb{Z}$

Thus $f(a) + f(b) = [r_3]$

Hence $a + b = q_1 n + q_2 n + r_1 + r_2 = (q_1 + q_2) n + r_3$

so $f(a+b) = [r_1 + r_2] = [r_3]$

Thus $f(a+b) = f(a) + f(b)$, which implies that f is a homomorphism.

• **Theorem**: Let $(G, *)$ and $(G', *')$ be two groups, and let $f : G \to G'$ be a homomorphism from G to G'.

(a) If e is the identity element of G and e' is the identity element of G', then $f(e) = e'$

(b) If $a \in G$, then $f(a^{-1}) = (f(a))^{-1}$

(c) If H is a subgroup of G, then $f(H) = \{f(h) \mid h \in H\}$ is a subgroup of G'

eg→16. The groups S_3 and Z_6 are both groups of order 6. However, S_3 is not Abelian and Z_6 is Abelian. Hence, they are not isomorphic (Remember that isomorphism preserves all properties defined in terms of group operations)

---

eg→17. Let $G = \{e, a, b, c\}$ be a group of order 4 with multiplication tables as given in Tables 1, 2, 3 and 4.

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

Table : 1

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

Table : 2

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

Table : 3

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

Table : 4

It can be shown that groups with multiplication tables 2, 3 and 4 are isomorphic

Let $G = \{e, a, b, c\}$; $G' = \{e', a', b', c'\}$, $G'' = \{e'', a'', b'', c''\}$

- Let $(G, *)$ be the group with Multiplication Table 2 and let $(G', *')$ be the group with Multiplication Table 3

Let $f: G \to G'$ be defined by

$f(e) = e'$, $f(a) = a'$, $f(b) = b'$, $f(c) = c'$

- It can be verified under renaming of elements of the two tables that the corresponding groups are isomorphic.

- similarly let $g: G \to G''$ be defined as

$g(e) = e''$, $g(a) = a''$, $g(b) = b''$, $g(c) = c''$; it can be verified that G and G'' are isomorphic groups

i.e groups given by Tables 2, 3 and 4 are isomorphic.

W.r.t Table 1, note that $\forall x \in$ Table 1, $x * x = e$ i.e every element is its own inverse.
If the group determined by Table 1 was isomorphic with the group determined by other tables (i.e Table 2 or Table 3 or Table 4), this property would be preserved across the tables.

- Hence it can be concluded that these groups are NOT isomorphic and there are only two different non-isomorphic groups of order 4.

(The group with multiplication Table 1 is called Klien 4 group and the group with multiplication Tables 2/3/4 is denoted by Z_4, since the relabeling of the elements of Z_4 results in these multiplication tables)

[recall Z_4 is a monoid with operation $\oplus$ and identity $[0]$]

with multiplication table as given below

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

The entries are obtained from

$$[a] \oplus_4 [b] = [a+b] = [r]$$

where r is the remainder when $(a+b)$ is divided by 4.