مدونة المناهج السعودية

https://eduschool40.blog

الموقع التعليمي لجميع المراحل الدراسية

في المملكة العربية السعودية

Groups

Definition: (Binary operation)

Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element i.e

$$*: G \times G \longrightarrow G$$

The set G is said to be closed under the operation $*$.

For example: $\{ R$

$$+: R \times R \to R \qquad\qquad \cdot: R \times R \to R$$
$$(a,b) \longrightarrow a+b \qquad\qquad (a,b) \longrightarrow a \cdot b$$

Example 1:

- $(+)$ and $(\cdot)$ are binary operations on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.
- $(-)$ is binary operation on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ but not on $\mathbb{N}$ since $3-5=-2 \notin \mathbb{N}$ $\quad 2/3 \quad \frac{a}{0}$
- $(\div)$ is not binary operation on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$. but it is binary operation on $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ and $\mathbb{R}^* = \mathbb{R} - \{0\}$

Definition: A binary operation is said to be associative if

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

Example 2:

1. The operations "+" and $(\cdot)$ on $\mathbb{R}$ are associative.
2. The operation $(-)$ on $\mathbb{Z}$ is not associative since
$$(3-5)-1 \neq 3-(5-1)$$

Definition: A binary operation is said to be commutative if

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

Example 3:

- The binary operation $(+)$ is always assumed to be commutative.

- Multiplication are commutative for numbers, so $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ and $(\mathbb{C}, \cdot)$ are all commutative. However, matrix multiplication is usually not commutative.

- subtraction $(-)$ on $\mathbb{R}$ is not commutative since $5-7 \neq 7-5$

Definition: (Cayley table)

A binary operation $*$ on a finite set G displayed in the form of an array, called the Cayley table.

For example:

Let $G = \{0, 2\}$ and $*$ is just multiplication of numbers. Then the cayley table is given by:

$*$	0	1
0	0	0
1	0	1

Remark: A binary operation on a finit set is commutative $\Leftrightarrow$ the table is symmetric about the diagonal runing from upper left to lower right

Definition (Group):

A group is a set G together with a binary operation $* : G \times G \to G$ satisfing:

Associativity holds:

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

Idintity:

There exsist an element $e \in G$ such that

$e * a = a * e = a$ for all $a \in G$.

Inverse:

For every $a \in G$, there is an element $a^{-1} \in G$ s.t

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

Notations:-

1. We will often write $(G, *)$ to distinguish the operation on G.

2. For most of the groups, the operation $*$ is denoted by addition $+$ or multiplication lik $\cdot$ or $\times$. Note we can write

   $5 - 3$ as $5 + (-3)$

   $3 \div 5$ as $3 \times \frac{1}{5}$

3. If we use multiplication notation then

   $e = 1$ and $a^{-1} = \frac{1}{a}$

   If we use additive notation then

   $e = 0$ and $a^{-1} = -a$

Example 1:

$\mathbb{Z}$: The set of integers

$(\mathbb{Z}, +)$ is a group. However, $(\mathbb{Z}, \cdot)$ is not a group since the inverses do not always exsist. For example,

$$5 \in \mathbb{Z} \text{ but } \frac{1}{5} \notin \mathbb{Z}.$$

what about $(\{1, -1\}, \cdot)$. Is it a group?

Example 2:

$\mathbb{Q}$: The set of rational numbers

$(\mathbb{Q}, +)$ is a group. However, $(\mathbb{Q}, \cdot)$ is not a group since the ratio $\frac{a}{b}$ is undefined whenever $b=0$.

$(\mathbb{Q}^*, \cdot)$ where $\mathbb{Q}^* = \mathbb{Q} - \{0\}$

What about $\mathbb{Q}^* = \mathbb{Q} - \{0\}$. Is it a group? Yes ضرب

- This ~~Yes~~. defines a binary operation
- Multiplication is associative.
- The identity is 1 and 1
- The inverse of $\frac{a}{b}$ is just $\frac{b}{a}$

$$\frac{a}{b} \cdot \frac{b}{a} = 1.$$

Similarly, we could define $\mathbb{R}^*$, $\mathbb{C}^*$ and these would be groups under multiplication.

Example 3:

$\mathbb{Z}_n$: The set of integers mod n.

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$$

$(\mathbb{Z}_n, +)$ is a group. However, $(\mathbb{Z}_n, \cdot)$ is not a group since inverses fail. For example:

$(\mathbb{Z}_4, +)$

+	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 $\mathbb{Z}_4$ is closed under +
- The operation is associative.
- 0 is the identity element
- Inverse

a	0	1	2	3
a^{-1}	0	3	2	1

$(\mathbb{Z}_4, \cdot)$

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- $\mathbb{Z}_4$ is closed under ·
- The operation · is associative.
- 1 is the identity element
- Inverse.

a	0	1	2	3
a^{-1}	X	1	X	3

* What about $(\mathbb{Z}_n^*, \cdot)$. Is it a group.

Consider $(\mathbb{Z}_4^*, \cdot)$ and $(\mathbb{Z}_5^*, \cdot)$

$(\mathbb{Z}_4^*, \cdot)$ → composite.

·	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

The operation . is not binary on $\mathbb{Z}_4$ because $2 . 2 = 0 \notin \mathbb{Z}_4^*$

Remark: $(\mathbb{Z}_n^*, \cdot)$ is a group iff n is prime.

$(\mathbb{Z}_5^*, \cdot)$ → prime

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

- The operation is binary on $\mathbb{Z}_5^*$
- The operation (·) is associative
- 1 is the identity element.
- Inverse:

a	1	2	3	4
a^{-1}	1	3	2	4

Example 4:

$M_n(\mathbb{R})$: The set of all $n\times n$ matrices with real number entries. $(M_n(\mathbb{R}), +)$ is a group. However $(M_n(\mathbb{R}), \circ)$ is not a group because inverses fail. For example:

let $A = \begin{pmatrix} 2 & 1 \\ 6 & 3 \end{pmatrix} \in M_2(\mathbb{R})$. Since $\det(A) = 6-6 = 0$, A^{-1} will not exsist.

Remember the fact: Given a $\overset{2\times 2}{\text{squar}}$ matrix A:

1. if $\det(A) \neq 0$ then A^{-1} will exsist.
2. If $\det(A) = 0$ then A^{-1} will no exsist.

Example 5:

General linear group ← $GL_n(\mathbb{R})$: The set of all invertable $n\times n$ matrices with
or
$GL(n, \mathbb{R})$ real number entries

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$$

$(GL_n(\mathbb{R}), +)$ is not a group since if we take

$$A = \begin{pmatrix} 3 & 2 \\ 2 & 2 \end{pmatrix} \in GL_2(\mathbb{R}) \quad \text{so} \quad -A = \begin{pmatrix} -3 & -2 \\ -2 & -2 \end{pmatrix} \in GL_2(\mathbb{R})$$

and $\begin{pmatrix} 3 & 2 \\ 2 & 2 \end{pmatrix} + \begin{pmatrix} -3 & -2 \\ -2 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin GL_2(\mathbb{R})$

So $+$ is not binary operation on $GL_2(\mathbb{R})$.

However, $(GL_n(\mathbb{R}), \cdot)$ is a group. (Prove)!

closure ← 1- $GL_n(\mathbb{R})$ is closed under matrix multiplication because if $\det(A) \neq 0$ and $\det(B) \neq 0$ then

$$\det(AB) = \det(A) \cdot \det(B) \neq 0$$

Asso ← 2- For all matrices the associativity holds and so for $GL_n(\mathbb{R}) \subseteq M_n(\mathbb{R})$ it automatically holds

3- The identity matrix $I \in GL_n(R)$ since

$\det(I) = 1 \neq 0$.

4- The inverses exsist becaus of the fact that :

A^{-1} exsists $\Leftrightarrow \det(A) \neq 0$

Remark: For simplicity, we will restrict our matrix example to 2×2 case.

Example 6:

Special linear group $\leftarrow$ $SL_n(R)$ or $SL(n,R)$: The set of all $n\times n$ matrices with real number entries and determinant 1.

$SL_n(R) = \{A \in M_n(R) \mid \det(A) = 1\}$

H.W: prove that $SL_2(R)$ forms a group under matrix multiplicati

Remarks:

1- In $GL_2(R)$, the inverse of

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ is } \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

2- In $SL_2(R)$, the inverse of

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ is } \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$ since $\det(A) = ad-bc = 1$

3- What about the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in $GL_2(\mathbb{Z}_p)$, $SL_2(\mathbb{Z}_p)$.

. Find the inverse of the element $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ in $GL(2, \mathbb{Z}_{11})$.

$$\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}^{-1} = \frac{1}{2\cdot 5 - 6\cdot 3}\begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix} = \frac{1}{-8}\begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix}$$

In $\mathbb{Z}_{11}$, $-8 = 3$, $-6 = 5$, and $-3 = 8$.

$$\frac{1}{-8}\begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix} = \frac{1}{3}\begin{bmatrix} 5 & 5 \\ 8 & 2 \end{bmatrix} = 3^{-1}\begin{bmatrix} 5 & 5 \\ 8 & 2 \end{bmatrix}$$

Finally, $3 \cdot 4 \bmod 11 = 1$ so $3^{-1} = 4$ in $\mathbb{Z}_{11}^*$. Therefore

Example 7:

$U(n)$: The set of all positive integers (number > 0) in $\mathbb{Z}_n$ that is less than n and relatively prime to n.

$$U(n) = \{ a \in \mathbb{Z}_n \mid \gcd(a, n) = 1 \}$$

$(U(n), \cdot)$ is a group. For example:

For $n = 10$ we have $U(10) = \{1, 3, 7, 9\}$

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

From the table we see that:

- $\cdot$ is binary operation on $U(10)$
- $\cdot$ is associative.
- The identity element is 1
- Eeach element in $U(10)$ has an inverse.

So $(U(10), \cdot)$ is a group.

Definition:

Let $(G, *)$ be a group. Then G is abelian if $*$ is commutative i.e $a * b = b * a$.

Remarks:

$\boxed{1}$ $+$ is alway commutative.

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(M_n(\mathbb{R}), +)$, $(\mathbb{Z}_n, +)$ are all abelian groups.

$\boxed{2}$ $\cdot$ might or might not be abelian.

- commutative for numbers

$(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\mathbb{Z}_n^*, \cdot)$ and $(U(n), \cdot)$ are all abelian groups.

- non-commutative for matrix multiplication.

$(M_n(\mathbb{R}), \cdot)$, $(GL_n(\mathbb{R}), \cdot)$ and $(SL_n(\mathbb{R}), \cdot)$ are not abelian group for $n \geq 2$.

Example 8:

Let $G = \mathbb{Q}^+$ and define a binary operation on G by

$$a * b = \frac{ab}{3}$$

Prove that $(G, *)$ is an abelian group.

- Closure Law: Let $a, b \in \mathbb{Q}^+$. product ab of two rational numbers is again a rational number~~s~~ and $\frac{ab}{3}$ is also a rational number. Thus $\forall a, b \in \mathbb{Q}^+$, $a * b = \frac{ab}{3} \in \mathbb{Q}^+$

So $*$ is binary operation

- Associative Law: Let $a, b, c \in \mathbb{Q}^+$

$$(a * b) * c = \frac{ab}{3} * c = \frac{abc}{3}$$

$$=$$

$$a * (b * c) = a * \frac{bc}{3} = \frac{abc}{3}$$

So $*$ is associative.

- Identity Law: Let $a, e \in \mathbb{Q}^+$ s.t

$$a * e = a$$

$$\frac{ae}{3} = a$$

$\Rightarrow e = 3$ is the identity element.

- Inverse Law: Let $a, a^{-1} \in \mathbb{Q}^+$ s.t

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

$$\frac{aa^{-1}}{3} = 3$$

$$\Rightarrow a^{-1} = \frac{9}{a}$$

- Commutative Law: Let $a, b \in \mathbb{Q}^+$ then

$$a * b = \frac{ab}{3} = \frac{ba}{3} = b * a$$

So $*$ is Commutative

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

Eelmentary Properties of Groups

Theorem: Let G be a group. Then

1- There is only one identity element.

proof:

Let e_1, e_2 be two identity elements. Then

$e_1 * e_2 = e_2$ as e_1 is the identity

$e_1 * e_2 = e_1$ as e_2 is the identity

Thus e_1 and e_2 are both equal to $e_1 * e_2$ and so are equal to eachother

2- The right and left cancellation laws hold; That is

$ba = ca \Rightarrow b = c$ and $ab = ac \Rightarrow b = c$

proof:

suppose that $ab = ac$. Let a^{-1} be an inverse of a. Then

$$
\begin{aligned}
& a^{-1}(ab) = a^{-1}(ac) \\
\Rightarrow\ & (a^{-1}a)b = (a^{-1}a)c \\
\Rightarrow\ & eb = ec \\
\Rightarrow\ & b = c
\end{aligned}
$$

Similarly, one can prove that $ba = ca \Rightarrow b = c$ by multiplying a^{-1} on the right. See for example: (Contemporary Abstract Algebra. p(24)).

3- The inverse of any element is unique.

let b_1, b_2 be two inverses of a. Then

$b_1 a = e$ and $b_2 a = e$ so that

$b_1 a = b_2 a$. Canceling the a on both sides gives

$b_1 = b_2$

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

Since $(ab)(ab)^{-1} = e$ and

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

$$= aea^{-1} = aa^{-1} = e$$

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

5. The equation $ax = b$ has a unique solution and the equation $xa = b$ has a unique Solution.

Examples: Solve the following equations:

1- $3x = 5$ in $(\mathbb{Q}^*, \times)$

$x = 3^{-1} . 5 = \frac{1}{3} . 5 = 5/3$.

2- $3 . x = 5$ in $(\mathbb{Z}_7^*, \cdot)$

$x = 3^{-1} . 5$

$\Rightarrow x = 5 . 5 = 25 = 4 \pmod 7$.

$\cdot$	1	2	3	4	5	6
3	2	6	2	5	1	4

3- $3 + x + 4 = 1$ in $(\mathbb{Z}_8, +)$

$x = 3^{-1} + 4^{-1} + 1$. Since the inverse of a in $(\mathbb{Z}_n, +)$ is given by:

$a^{-1} = n - a$. we have

$3^{-1} = 8 - 3 = 5$ and $4^{-1} = 8 - 4 = 4$

Thus: $x = 5 + 4 + 1 = 10 = 2 \pmod 8$.

4. If we define $*$ on $\mathbb{Q}^+$ by $a * b = \frac{ab}{3}$, then solve the equation $4 * x = 7$

Sol:

$$4 * x = 7 \Rightarrow \frac{4x}{3} = 7$$

$$\Rightarrow x = \frac{7 . 3}{4} = \frac{21}{4}$$

Terminology and notation:

- Exponential Notation:

Given a group G, $a \in G$ then:

* For operation $\cdot$ we have:

1- $a^n = a \cdot a \cdot a \cdot \dots \cdot a$

2- $a^0 = 1$

3- $a^{-n} = (a^{-1})^n = a^{-1} \cdot a^{-1} \cdot a^{-1} \cdots \cdot a^{-1}$

* For operation $+$ we have:

1 $a^n = a^n + a^n + a^n + \dots + a^n = n \cdot a$

$a^n \cdot a^m = a^{n+m}$

$(a^n)^m = a^{nm}$

$(a \cdot b)^n = abab$

Note that: If G is abelian then $(a \cdot b)^n = a^n b^n$.

- Definitions (order of a group)

The order of a group G, denoted by $|G|$ is the number of element in G. If G is infinite, we say that G has infinite order.

Examples:

1- $|\mathbb{Z}_n| = n$

2- $|\mathbb{Z}_p^*| = p-1$

3- $|\mathbb{Z}| = \infty$

4- $|\{1, -1, i, -i\}| = 4$

5- $|GL_2(\mathbb{R})| = \infty$

Definition (order of an element)

The order of an element g in G is the smallest positive integer n such that

- In multiplication notation: $g^n = 1$
- In additive notation: $n \cdot g = 0$

Example 1:

Consider the group $U(15) \to$ this is a group with $\cdot$

a)- Find the order of $U(15)$.

b)- Find the order of the element 7.

a)- $U(15) = \{ \underset{a>0}{a} \in \mathbb{Z}_{15} \mid \gcd(a, 15) = 1 \}$

$= \{1, 2, 4, 7, 8, 11, 13, 14\}$

So $|U(15)| = 8$

b)- To compute the order of the ement 7, we have to compute the sequence:

$7^1 = 7$

$7^2 = 49 \equiv 4$

$7^3 = 7^2 \cdot 7 = 4 \cdot 7 = 28 \equiv 13$

stop $7^{\boxed{4}} = 7^3 \cdot 7 = 13 \cdot 7 = 91 \equiv \boxed{1}$

So $|7| = 4$

Example 2:

Compute the order of element 2 in $\mathbb{Z}_{10}$ $\to$ this is a group with $+$

$2 \cdot 1 = 2$, $2 \cdot 4 = 8$

$2 \cdot 2 = 4$, $2 \cdot \boxed{5} = 10 \equiv \boxed{0}$ stop

$2 \cdot 3 = 6$

Thus $|2| = 5$

Example 3: Find the order of each element in a group $(\mathbb{Z}_7^*, \cdot)$

1 is the identity element $\Rightarrow |1| = 1$

2

$2^1 = 2$

$2^2 = 4$

stop ← $2^{\boxed{3}} = 2^2 \cdot 2 = 4 \cdot 2 = 8 \equiv \boxed{1}$

$\Rightarrow |2| = \boxed{3}$

4

$4^1 = 4$

$4^2 = 16 \equiv 2$

stop ← $4^{\boxed{3}} = 2^2 \cdot 4 = 8 \equiv \boxed{1}$

$\Rightarrow |4| = \boxed{3}$

3

$3^1 = 3$

$3^2 = 9 \equiv 2$

$3^3 = 3^2 \cdot 3 = 2 \cdot 3 = 6$

$3^4 = 3^3 \cdot 3 = 6 \cdot 3 \equiv 4$

$3^5 = 3^4 \cdot 3 = 4 \cdot 3 \equiv 5$

$3^6 = 3^5 \cdot 3 = 5 \cdot 3 \equiv 1$

$\Rightarrow |3| = \boxed{6}$

5

$5^1 = 5$

$5^2 = 25 \equiv 4$

$5^3 = 5^2 \cdot 5 = 4 \cdot 5 \equiv 6$

$5^4 = 5^3 \cdot 5 = 6 \cdot 5 \equiv 2$

$5^5 = 5^4 \cdot 5 = 2 \cdot 5 \equiv 3$

$5^6 = 5^5 \cdot 5 = 3 \cdot 5 = 1$

$\Rightarrow |5| = 6$

6

$6^1 = 6$

$6^{\boxed{2}} = 36 \equiv \boxed{1}$ — stop

$\Rightarrow |6| = 1$

What relation do yo see between the orders of the elements of a group and the order of the group.

we see that $|3| = |5| = 6$ and $|2| = |4| = 3$. معكوس

This is becaus 5 is the inverse of 3 i.e

$3x \equiv 1 \mod 7 \Rightarrow x = 5$

Also,

$|\mathbb{Z}_7^*| = 6$ and the order of all ements divide 6.

Corollary: Let G be a finite group then:

1. $|e| = 1$
2. $|a| = |a^{-1}|$ رتبة العنصر = رتبة معكوسه
3. $|a| \mid |G|$ رتبة العنصر تقسم رتبة القروب
4. every element has an order.

Example 4: Find the order of each element in a group $(\mathbb{Z}_5^*, \cdot)$

$|1| = 1$

2

$2^1 = 2$

$2^2 = 4$

$2^3 = 8 \equiv 3$

$2^4 = 2^3 \cdot 2 = 3 \cdot 2 \equiv 1$

$\Rightarrow |2| = 4 = |3|$

معكوس

4

$4^1 = 4$

$4^2 = 16 \equiv 1$

$\Rightarrow |4| = 2$

More Exercises

Let $G = \mathbb{R} - \{-1\}$ and define the binary operation on G by

$$a * b = a + b + ab$$

Prove that $(G, *)$ is an abelian group.

Solution:

1- Closure Law: To show that G is closed under $*$ i.e

if $a, b \in G \Rightarrow a * b \in G$, we need to show that

If $a \neq -1$ and $b \neq -1$ then $a * b \neq -1$

Assume that $a * b = -1$

$$a + b + ab = -1$$

$$a(1+b) = -(1+b) \quad [\text{since } b \neq -1 \text{, we divide both side by } (1+b)]$$

$$\Rightarrow a = -1 \quad \text{whic is a contradiction}$$

Therefore, $a * b \neq -1$ and $a * b \in G$. Thus $*$ is binary operation on G.

2- Associative Law: Let $a, b, c \in G$ s.t

$$\begin{aligned}(a*b)*c &= (a+b+ab)*c \\ &= a+b+ab+c+(a+b+ab)c \\ &= a+b+ab+c+ac+bc+abc\end{aligned}$$

$$\begin{aligned}a*(b*c) &= a*(b+c+bc) \\ &= a+b+c+bc+a(b+c+bc) \\ &= a+b+c+bc+ab+ac+abc\end{aligned}$$

So $*$ is associative.

3- Identity Law: Let $a, e \in G$ s.t

$$a * e = a$$

$$\Rightarrow a + e + ae = a$$

$$\Rightarrow e(1+a) = 0 \quad (1+a=0 \Rightarrow a=-1 \times)$$

$$\Rightarrow e = 0$$

4- Inverse Law: Let $a, a^{-1} \in G$ s.t

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

$a + a^{-1} + aa^{-1} = 0$

$a^{-1}(1+a) = -a$

$a^{-1} = \frac{-a}{1+a}$ is the inverse of a.

5- Commutative Law: Let $a, b \in G$ then

$a * b = a + b + ab = b + a + ba = b * a$

so $*$ is a commutative

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

Let $G = R - \{1\}$ and define a binary operation on G by

$$a * b = a + b - ab$$

prove that $(G, *)$ is an abelian group.

Hint:

1- Associative Law: $a * (b * c) = (a * b) * c$.

2- Identity element $e = 0$

3- Inverse Law: $a^{-1} = \frac{-a}{1+a}$

Let $G = Q^+$ and define a binary operation on G by

$$a * b = \frac{ab}{2}$$

prove that $(G, *)$ is an abelian group.

Hint:

1- Associative Law: $(a * b) * c = a * (b * c) = \frac{abc}{4}$

2- Identity element $e = 2$

3- Inverse Law: $a^{-1} = \frac{4}{a}$.

Let $G = \mathbb{Z}$ and define the binary operation by

$$a * b = a + b - 5$$

a).- prove that $(G, *)$ is an abelian group.

b).- Solve $x * 3^{-1} = 2$.

Solution:

a).- - closure: Let $a, b \in \mathbb{Z}$. Clearly, $a+b-5$ is again an element of $\mathbb{Z}$. Thus $a, b \in \mathbb{Z} \Rightarrow a * b = a+b-5 \in \mathbb{Z}$.

- Associative Law: Let $a, b, c \in \mathbb{Z}$ s.t

$$\begin{aligned}(a*b)*c &= (a+b-5)*c \\ &= a+b-5+c-5 \\ &= a+b+c-10\end{aligned}$$

$$\begin{aligned}a*(b*c) &= a*(b+c-5) \\ &= a+b+c-5-5 \\ &= a+b+c-10\end{aligned}$$

So $*$ is associative.

- Identity Law: Let $a, e \in \mathbb{Z}$ s.t

$a * e = a$

$\Rightarrow a + e - 5 = a$

$\Rightarrow e = 5$ is the identity element.

- Inverse Law: Let $a, a^{-1} \in \mathbb{Z}$ s.t

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

$\Rightarrow a + a^{-1} - 5 = 5$

$\Rightarrow a^{-1} = 10 - a$ is the inverse of a.

- Commutative Law: $\forall a, b \in \mathbb{Z}$ we have

$a * b = a+b-5 = b+a-5 = b * a$

so $*$ is commutative.

Thus $(\mathbb{Z}, *)$ is an abelian group.

b).- $x * 3^{-1} = 2$

First we compute 3^{-1}. From (a) we have:

$a^{-1} = 10 - a$. Thus

$3^{-1} = 10 - 3 = 7$

So:

$$x * 3^{-1} = 2 = x * 7 = 2$$
$$= x + 7 - 5 = 2$$
$$\Rightarrow x = 0$$

Let $G = \mathbb{Z}$ and define the binary operation by

$$a * b = a + b - 7$$

Find the identity and the inverse of 14.

Solution:

Identity: Let $a, e \in \mathbb{Z}$ s.t

$$a * e = a$$
$$\Rightarrow a + e - 7 = a$$
$$\Rightarrow e = 7 \text{ is the identity}$$

Inverse: Let $a, a^{-1} \in \mathbb{Z}$ s.t

$$a * a^{-1} = e$$
$$\Rightarrow a + a^{-1} - 7 = 7$$
$$\Rightarrow a^{-1} = 14 - a$$

So: $14^{-1} = 14 - 14 = 0$

Prove that if $a = a^{-1}$ for all a in a group G, then G is abelian.

Suppose that $a^{-1} = a$ for all $a \in G$

let $a, b \in G \Rightarrow ab \in G$

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

By the law $(ab)^{-1} = b^{-1}a^{-1}$

$$\Rightarrow b^{-1}a^{-1} = ab$$

since we assume $a^{-1} = a$, $b^{-1} = b$

$$\Rightarrow ba = ab$$

$\Rightarrow$ G is abelian.

Let G be a group. prove that $(ab)^2 = a^2b^2$ for all $a, b \in G$ iff G is abelian.

($\Rightarrow$) If G is abelian then

$$(ab)^2 = abab$$
$$= aabb$$
$$= a^2 b^2$$

($\Leftarrow$) If $(ab)^2 = a^2b^2$ then

$$\cancel{a}ba\cancel{b} = \cancel{a}ab\cancel{b}$$
$$ba = ab$$

$\Rightarrow$ G is abelian

pr

prove that a group G is abelian $\Leftrightarrow$ $(ab)^{-1} = a^{-1}b^{-1}$.

($\Rightarrow$) Let G be abelian that is for any $a, b \in G$,

$ab = ba$. Then

G abelian $(ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1}$

($\Leftarrow$) suppose that $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$. Then

$$(ab)(ab)^{-1} = e$$

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

$$\Rightarrow (ab)\cancel{(ab)^{-1}} = (ba)\cancel{(ab)^{-1}}$$

$$\Rightarrow ab = ba$$

$\Rightarrow$ G is abelian

Subgroups

Definition: A subset H of a group G is a subgroup of G if H itself a group underf the operation of G.

By otherwords:

A subset H of a group G is a subgroup of G if:

$x, y \in H \Rightarrow x * y \in H$

$x \in H \Rightarrow x^{-1} \in H$

$e \in H$

Remark:

we do not need to check the associativity in H because it comes automatically from G.

Notation:

If H is a subgroup of G, we write $H \leqslant G$.

Example 1:

1- $(\mathbb{Z}, +) \leqslant (\mathbb{Q}, +) \leqslant (\mathbb{R}, +) \leqslant (\mathbb{C}, +)$

2- $(\{1, -1\}, \cdot) \leqslant (\mathbb{Q}^*, \cdot) \leqslant (\mathbb{R}^*, \cdot) \leqslant (\mathbb{C}^*, \cdot)$.

3- The singleton $\{e\}$ is a subgroup of G which is called the trivial subgroup.

4- $(\mathbb{N}, +)$ is not a subgroup of $(\mathbb{Z}, +)$ since $1 \in \mathbb{N}$ but $-1 \notin \mathbb{N}$.

Remark:-

1- Every group G has at least two subgroups:

G itself and $\{e\}$

G itself → Imporper subgroup

$\{e\}$ → trivial subgroup.

All other subgroups of G are said to be proper subgroups or non-trivial subgroups.

2- It is important to know that to sets must have the same operation. For example,

$(\mathbb{Q}^*, .)$ is not a subgroup of $(\mathbb{R}, +)$

Although $\mathbb{Q}^* \subseteq \mathbb{R}$ but the operation on these two sets are different

Another example:

$(\underset{+ \bmod n}{\mathbb{Z}_n, +})$ is not a subgroup of $(\underset{\text{ordinary } +}{\mathbb{Z}, +})$.

(the operation is not the same)

Example 2: Show that $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.

1. Closure:

For any $A, B \in SL_2(\mathbb{R})$, we have $AB \in SL_2(\mathbb{R})$ because $\det(AB) = \det(A) . \det(B)$

$$= 1 . 1 = 1$$

and so $AB \in SL_2(\mathbb{Z})$.

2. Identity:

The multiplicative identity is $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\det(I) = 1$

so $I \in SL_2(\mathbb{R})$.

3. Inverse:

For $A \in SL_2(\mathbb{R})$, we have $A^{-1} \in SL_2(\mathbb{R})$ because

$$\det(A^{-1}) = \frac{1}{\underset{\in SL_2(\mathbb{Z})}{\det(A)}} = \frac{1}{1} = 1$$

or:

$$\boxed{1} = \det I = \det(A A^{-1}) = \det(A) . \det(A^{-1}) = \boxed{\det(A^{-1})}$$

so $A^{-1} \in SL_2(\mathbb{R})$.

Example 3: Show that $\{0, 3, 6\}$ is a subgroup of $\mathbb{Z}_4$.

+	0	3	6
0	0	3	6
3	3	6	0
6	6	6	3

- + is binary operation on $\mathbb{Z}_4$
- The identity element is 0
- Eeach element has an inverse.

a	0	3	6
a^{-1}	0	6	3

So $\{0, 3, 6\} \leq \mathbb{Z}_4$.

Definition: Let n be a positive integer. The number of divisors of n is denoted by $d(n)$.

For example:

The number of divisors of $n = 8$ is $d(8) = 4$ عدد قواسمه

Theorem: The number of all subgroups of $(\mathbb{Z}_n, +)$ is equal to $d(n)$.

For example

All subgroups of $\mathbb{Z}_8$ are equal to $d(8) = 4$.

They are:

$H_1 = \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8$ (Improper subgroup)

$H_2 = \{0, 2, 4, 6\}$ } proper subgroups or

$H_3 = \{0, 4\}$ } non trivial subgroups

$H_4 = \{0\}$ (trivial subgroup)

Theorem: The number of proper subgroups of $(\mathbb{Z}_n, +)$ is equal to $d(n) - 2$

For example:

The number of proper subgroups of $(\mathbb{Z}_8, +)$ is

$$d(8) - 2 = 4 - 2 = 2$$

قواسم ٨ هي

٨ ٤ ٢ ١

impro pr

They are:

$H_1 = \{0, 2, 4, 6\}$ and $H_2 = \{0, 4\}$

Remark:

If $n=p$ (prime) then $(\mathbb{Z}_p, +)$ has no proper subgroups since the divisors of p are just 1 and p thus $d(p)=2$ and the number of proper subgroups $= d(p)-2 = 2-2=0$.

Subgroup Test:

one step subgroup test:

Let G be a group and $\phi \neq H \subseteq G$

In multiplication notation

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

In additive notation

If $a,b \in H \Rightarrow a-b \in H$.

Example

1- Let $G=(\mathbb{Q}^*, \cdot)$ and $H=\{3^n : n\in \mathbb{Z}\}$. Then

If $3^n, 3^m \in H$ then we have

$$(3^n)(3^m)^{-1} = 3^n \cdot \underset{(\frac{1}{3^m})}{3^{-m}} = 3^{n-m} \in H$$

Thus $H \leq \mathbb{Q}^*$

2- Let $G=\mathbb{Z}$ and $H=7\mathbb{Z}=\{7r : r\in \mathbb{Z}\}$.

If $7r_1, 7r_2 \in H$ then we have

$$(7r_1)(7r_2)^{-1} = 7r_1 - 7r_2 = 7(r_1-r_2) \in 7\mathbb{Z}.$$

Thus $H \leq \mathbb{Q}^*$.

Theorem:

H.W prove!! The intersection of two subgroups of a group G is also a group.

Remark:

The union of two subgroups need not to be a sub group.

"Cyclic Groups"

Definition:

A group G is cyclic if G can be generated by a single element.

In the other words:

There exsist $a \in G$ s.t

If G is a group under $\cdot$

$G = \{a^n : n \in \mathbb{Z}\} = \langle a \rangle$

If G is a group under $+$

$G = \{n \cdot a \mid n \in \mathbb{Z}\} = \langle a \rangle$

we call a the generator.

Example 1: Show that $(\mathbb{Z}_7^*, \cdot)$ is cyclic group.

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

alway gives 1

$2^0 = 1$

$2^1 = 2$

$2^2 = 4$

$2^3 = 2^2 \cdot 2 = 4 \cdot 2 = 8 \equiv 1$ stop

$\Rightarrow \langle 2 \rangle = \{1, 2, 4\}$

$3^0 = 1$

$3^1 = 3$

$3^2 = 9 \equiv 2$

$3^3 = 3^2 \cdot 3 = 2 \cdot 3 = 6$

$3^4 = 3^3 \cdot 3 = 6 \cdot 3 \equiv 4$

$3^5 = 3^4 \cdot 3 = 4 \cdot 3 \equiv 5$

$3^6 = 3^5 \cdot 3 = 5 \cdot 3 \equiv 1$

$\langle 3 \rangle = \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\}$

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

So $\mathbb{Z}_7^*$ is cyclic group generated by 3.

ملاحظات

① لكي نثبت بأن زمرة ما مولدة، نكتفي فقط بإيجاد مولد واحد للزمرة.

② المولد غير وحيد فمثلاً الزمرة $\mathbb{Z}_7^*$ لها مولد آخر وهو 5

③ العلاقة بين المولد 3 و 5 هي أن 5 معكوس للعدد 3 أي $3x = 1 \bmod \mathbb{Z}_7^*$ يكون الناتج $x = 5$

Example 2: Show that $(\mathbb{Z}_4, +)$ is cyclic group.

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$1 \cdot 0 = 0$	$2 \cdot 0 = 0$	$3 \cdot 0 = 0$
$1 \cdot 1 = 1$	$2 \cdot 1 = 2$	$3 \cdot 1 = 3$
$1 \cdot 2 = 2$	$2 \cdot 2 = 4 \equiv 0$ stop	$3 \cdot 2 = 2$
$1 \cdot 3 = 3$	$\langle 2 \rangle = \{0, 2\}$	$3 \cdot 3 = 9 \equiv 1$
$\langle 1 \rangle = \{0, 1, 2, 3\} = \mathbb{Z}_4$	$\neq \mathbb{Z}_4$	$\langle 3 \rangle = \{0, 1, 2, 3\} = \mathbb{Z}_4$

ملاحظات:

① في هذا المثال لإثبات أن $\mathbb{Z}_4$ زمرة مولدة قد نكتفي بالواحد فقط.

② العلاقة بين المولد ١ و ٣ هو أن ٣ معكوس للعدد واحد لأن في $(\mathbb{Z}_n, +)$ معكوس $a^{-1} = n - a$ وبالتالي $3^{-1} = 4 - 3 = 1$

Remarks :

1- The generator is not unique

2- If $G = \langle a \rangle$ is cyclic then $G = \langle a^{-1} \rangle$

3- $(\mathbb{Z}_n, +)$ is cyclic group generated by 1 and $n-1$ $\Rightarrow$

1 و n-1 ليست
فقط هي المولدات ،
المعنى هنا أن نأكد
بأن هـ

Theorem :- If G is a cyclic group generated by a then

1- If G is infinite then a, a^{-1} are only the generator.

2- If G is finite and $|G| = n$ then all generator take the form:

elements of G — order of G

generator of G $\leftarrow a^t$ where $\gcd(t, n) = 1$

Example: Find all generator of $(\mathbb{Z}_7^*, \cdot)$

we have proved that $\mathbb{Z}_7^*$ is cyclic group generated by 3.

So all generator of $\mathbb{Z}_7^*$ take the form:

$$3^t \text{ where } \gcd(t, 6) = 1$$

So $t = 1, 5$ and there are two generator of $\mathbb{Z}_7^*$

$3^1 = 3$ and $3^5 = 3^4 \cdot 3 = 5$.

Example: Find all generator of $(\mathbb{Z}_{30}, +)$

$\mathbb{Z}_{30} = \{0, 1, 2, \ldots 29\}$ is cyclic group generated by 1, $|\mathbb{Z}_{30}| = 30$

So all generator of $\mathbb{Z}_{30}$ take the form

means

$1 \cdot t = (1)^t$ where $\gcd(t, 30) = 1$

لأن العملية +

So $t = 1, 7, 11, 13, 17, 19, 23$ and 29. They are the generator of $\mathbb{Z}_{30}$

Example: Show that $(\mathbb{Z}_{13}^*, \cdot)$ is cyclic and find all of its generator.

Solution:

$\mathbb{Z}_{13}^* = \{1, 2, 3, \dots 12\}$ and $|\mathbb{Z}_{13}^*| = 12$

$2^0 = 1$ $\quad$ $2^5 = 2^4 \cdot 2 = 3 \cdot 2 = 6$ $\quad$ $2^9 = 2^8 \cdot 2 = 9 \cdot 2 \equiv 5$

$2^1 = 2$ $\quad$ $2^6 = 2^5 \cdot 2 = 6 \cdot 2 = 12$ $\quad$ $2^{10} = 2^9 \cdot 2 = 5 \cdot 2 = 10$

$2^3 = 8$ $\quad$ $2^7 = 2^6 \cdot 2 = 12 \cdot 2 = 11$ $\quad$ $2^{11} = 2^{10} \cdot 2 = 10 \cdot 2 \equiv 7$

$2^4 = 16 \equiv 3$ $\quad$ $2^8 = 2^7 \cdot 2 = 11 \cdot 2 \equiv 9$

So $\mathbb{Z}_{13}^*$ is cyclic group generated by 2.

- All generator of $\mathbb{Z}_{13}^*$ take the form

2^t where $\gcd(t, 12) = 1$

So $t = 1, 5, 7, 11$ and there are four generator of $\mathbb{Z}_{13}^*$

$2^1, 2^5, 2^7, 2^{11}$

$= 2, 6, 11, 7$.

Example: Show that $U(10)$ is cyclic and find all of its generator:

Solution: $\quad > 0$

$U(10) = \{a \in \mathbb{Z}_{10} \mid \gcd(a, 10) = 1\}$

$= \{1, 3, 7, 9\}$ $\quad$ and $\quad$ $|U(10)| = 4$.

$3^0 = 1$, $3^1 = 3$, $3^2 = 9$, $3^3 = 7$, $3^4 = 3^3 \cdot 3 = 7 \cdot 3 \equiv 1$

So $\langle 3 \rangle = \{1, 3, 7, 9\} = U(10)$

Thus $U(10)$ is cyclic group generated by 3.

All generator of $U(10)$ take the form:

3^t where $\gcd(t, 4) = 1$.

So $t = 1$ and 3, and there are 2 generator of $U(10)$

$3^1 = 3$ and $3^3 = 7$

Example: Is $U(8) = \{1, 3, 5, 8\}$ cyclic group.

$3^0 = 1$	$5^0 = 1$	$7^0 = 1$	
$3^1 = 3$	$5^1 = 5$	$7^1 = 7$	
$3^2 = 1$	$5^2 = 25 \equiv 1$	$7^2 = 49 \equiv 1$	stop
$\Rightarrow \langle 3 \rangle = \{1, 3\}$	$\langle 5 \rangle = \{1, 5\}$	$\langle 7 \rangle = \{1, 7\}$	

So $U(8)$ is not cyclic group because

$U(8) \neq \langle a \rangle$ for any $a \in U(8)$

Theorem:

Every cyclic group is abelian. But the converse is not true. For example: العكس غير صحيح

$(\mathbb{Q}, +)$ is abelian but not cyclic.

Assume

Assume that $(\mathbb{Q}, +)$ is cyclic group generated by $\frac{a}{b}$

In $+$:
$\langle a \rangle = \{na : n \in \mathbb{Z}\}$

$\Rightarrow \mathbb{Q} = \langle \frac{a}{b} \rangle = \{n(\frac{a}{b}) : n \in \mathbb{Z}\}$

Since $\frac{a}{2b} \in \mathbb{Q} \Rightarrow \frac{a}{2b} = n(\frac{a}{b})$

$$\Rightarrow n = \frac{1}{2} \notin \mathbb{Z}$$

which is a contradiction.

Permutation Groups

Definitions: (permutation of A)
A permutation of a set A is a function from A to A that is both 1-1 and onto.

Note: We will focus on the case where A is finite. We usually take $A = \{1, 2, \dots, n\}$ for $n \in \mathbb{N}$. **For example:** we define a permutation α of the set $\{1, 2, 3, 4\}$ by specifing
$\alpha(1) = 2$, $\alpha(2) = 3$, $\alpha(3) = 1$, $\alpha(4) = 4$

- We can express α in arry form as

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

Definitions (Symmetric Group S_n)
Let $A = \{1, 2, \dots n\}$. The set of all permutations of A is called the symmetric group of degree n and is denoted by S_n.

- **Elements of S_n have the form:**

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & & \alpha(n) \end{pmatrix}$$

- **Example:** Find all permutations on $A = \{1, 2, 3\}$.
There are six permutations. We will represent these permutations using the array forms as follows:

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I \quad , \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad , \quad P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad , \quad P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Thus $S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$

Theorem: The order of S_n is $n!$

For example: The order of $S_3 = 3! = 6$ permutations

The order of $S_4 = 4! = 24$. permutations.

* **Definition:** A group of permutations, with composition as operation is called a permutation group on A. For example S_n is a permutation group.

* **Composition of permutations:-**

composition of permutations expressed in arry notation is carried out from right to left by going from top to the bottom, then again from top to the bottom. For example,

let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$

then $\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$

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

and

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

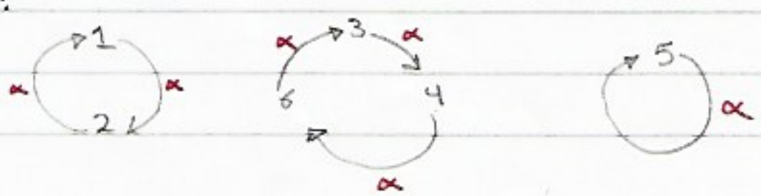
$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$

$\alpha \circ \beta \neq \beta \circ \alpha$

* **cycle Notation:**

Ex (1):-

Consider $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$, α follows the circle pattern:



In cycle notation we can write $\alpha = (1\,2)(3\,4\,6)(5)$.

Ex: Express the permutation $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$ using cycle notation.

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

Remarks:

1- We can omit cycles that have only one entry. In this case it is understood that any missing element is mapped to itself. (fixed element). For example:

Fixed elements.

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

one entry

2- The identity permutation consists only of cycles with one entry, so we can not omit all of these!. In this case one usually writes just one cycle. For example

$$I = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (1) \text{ or } (3) \text{ or any cycle}$$

Ex: How many permutations in S_5 fix 1.

Fixing 1 means that the permutation becomes a permutation on the set $\{2, 3, 4, 5\}$ and there are $4! = 24$ such a permutations.

How many permutations in S_5 fix both 1 and 3.

* Product of permutation in cyclic form:-

A multiplication of cycles is performed by applying the right permutation first. For examples:

Let:

1- $\alpha = (12)(45)$, $\beta = (153)(24)$. Then $\alpha\underset{\uparrow}{\beta} = (24)(253)$ Right permutation

2- $\alpha = (13524)$, $\beta = (32456)$. Then $\alpha\beta = (2134)(56)$

3- $\alpha = (243)$, $\beta = (1235)$, $\gamma = (245631)$. Then

$\alpha\beta\underset{\uparrow}{\gamma} = \;?$ Right

since $\beta\gamma = (2413)(56)$, we have

$$\alpha\beta\gamma = (243)(2413)(56)$$
$$= (2341)(56)$$

4- $\alpha = (134)$, $\beta = (2658)$. Then $\alpha\beta = (134)(2658)$

Did you notic some thing about α and β .?!

Definition:

If α and β are two cycle, they are called disjoint if their cycle presentation contain diferent elements of the set $A = \{1, 2, 3, \ldots n\}$.

Ex: The cycle (124) and (356) are disjoint but the cycle (124) and (346) are not disjoint. Since they have number 4 in common.

Th: If α and β are disjoint cycles then $\alpha\beta = \beta\alpha$

For example:

$\alpha = (13)$, $\beta = (256)$. Then

$\alpha\beta = (13)(256) = (256)(13)$ and

$\beta\alpha = (256)(13) = (13)(256)$.

Give an example of $\alpha, \beta, \gamma \in S_5$, non of which is the identity. with $\alpha\beta = \beta\alpha$ and $\alpha\gamma = \gamma\alpha$ but with $\beta\gamma \neq \gamma\beta$.

Sol:

we choose α, β, and γ to be cycles s.t

α and β are disjoint,

α and γ are disjoint, and

β and γ are not disjoint.

For example:

Take $\alpha = (1\,2)$, $\beta = (3\,4)$, $\gamma = (4,5)$. Then

$\beta\gamma = (3\,4\,5)$ while $\gamma\beta = (3\,5\,4)$

Th: Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Theorem: The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the length of the cycle.

Ex: What is the order of each of the following permutation:

$(1\,2\,4)(3\,5\,7)$

$(1\,2\,4)$ and $(3\,5\,7)$ are of length 3. Thus $L.c.m(3,3) = 3$ and hence $(1\,2\,4)(3\,5\,7)$ has order 3.

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

$(1\,2\,4)$ of length 3 and $(3\,5)$ of length 2. Thus $L.c.m(3,2) = 6$. Hence $(1\,2\,4)(3\,5)$ has order 6.

Parity of permutations: (Even or odd permutation)

The parity of an n-cycle is even if n is odd and vice versa. والعكس

For example:

(1 3 4 5) is an 4-cycle and so it is an odd permutation.

(1 4 6 8 2 5 3) is an 7 cycle and so it is an even permutation.

Remark:-

even + even = even

odd + odd = even

odd + even = odd.

For example:

(1 3 4) (2 5 6 3) is an odd permutation since (1 3 4) is an 3-cycle and (2 5 6 3) is an 4-cycle.

(1 2) (1 3 4) (1 5 2) is an odd permutation since (1 2) is an 2-cycle, (1 3 4) and (1 5 2) are cycles of length 3.

Ex: Find all even and odd permutation of S_3.

Sol:

$S_3 = \{ I, (12), (13), (23), (123), (132) \}$

- All even permutations of S_3 are

$E_3 = \{ I, (123), (132) \}$

- All odd permutations of S_3 are

$O_3 = \{ (12), (13), (23) \}$

Th:

$$|E_n| = |O_n| = \frac{1}{2} |S_n| = \frac{n!}{2}$$

Definition: The length of permutations

An expression of the form $(a_1, a_2, \dots a_n)$ is called a cycle of length n or n-cycle

For example:

$(1\ 3\ 4\ 5)$ is a cycle of length 4 or an 4-cycle

$(2\ 8)$ is a cycle of length 2 or an 2-cycle

$(6\ 7\ 3)$ is a cycle of length 3 or an 3-cycle.

Ex: Write the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 3 & 7 & 5 & 4 & 2 \end{pmatrix}$ as an 4-cycle.

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

Remark:

Note that one can write the same cycle in many ways using this type of notation. We have:

$$\begin{aligned} \alpha &= (2\,6\,4\,7) \\ &= (6\,4\,7\,2) \\ &= (4\,7\,2\,6) \\ &= (7\,2\,6\,4) \end{aligned}$$

but be carfule:

$$\alpha = (2\,6\,4\,7) \neq (6\,7\,2\,4)$$

Th: A k-cycle can be written in k-different ways, since

$$(a_1, a_2, \dots a_k) = (a_2, a_3, \dots a_k, a_1) = \dots\dots = (a_k, a_1, \dots a_{k-1}).$$

* The inverse of permutation:

If $\alpha = (a_0\ a_1 \dots a_n)$ then the inverse of α is

$$\alpha^{-1} = (a_n \dots a_2\ a_1\ a_0)$$

For example:

$$(1\,3\,4\,2\,5)^{-1} = (5\,2\,4\,3\,1)$$
$$= (1\,5\,2\,4\,3)$$

$$(1\,4\,6\,3)^{-1} = (3\,6\,4\,1)$$
$$= (1\,3\,6\,4)$$
$$= (6\,4\,1\,3)$$

Note:

$$(\alpha \circ \beta)^{-1} = \beta^{-1} \circ \alpha^{-1}$$

* Show that $(S_3, \circ)$ is non commutative group.

$S_3 = \{ I, (12), (13), (23), (123), (132) \} \neq \phi$.

·	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	id	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	id	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	id	(1 2 3)

From the table:

1)- The operation is binary on S_3.

2)- " " is associative on S_3.

3)- I is the identity element

4)-

a	I	(12)	(13)	(23)	(123)	(132)
a^{-1}	I	(12)	(13)	(23)	(132)	(123)

Hence $(S_3, \circ)$ is a group. Since

$(12) \circ (13) = (1\,3\,2)$ and $(13) \circ (12) = (123)$

Thus $(12) \circ (13) \neq (13) \circ (12)$. The operation is not commutative.

Hence $(S_3, \circ)$ is non-commutative group.

Theorem: The set of even permutation in S_n forms a subgroup of S_n.

Ex: IS E_3 a subgroup of S_3.

$E_3 = \{ I, (1\,2\,3), (1\,3\,2) \}$

$\circ$	I	(123)	(132)
I	I	(123)	(132)
(123)	(123)	(132)	I
(132)	(132)	I	(123)

From the table:

- The operation is binary and associative on E_3.
- I is the identity element.
-

Hence $(E_3, \circ)$ is a subgroup of S_3.

Remark:

Every subgroup of abelian group is abelian.

Ex: Give two reasons why the set of odd permutation in S_n is not a subgroup.

1. The identity is even permutation
2. The set is not closed since the (odd per) $\circ$ (odd per) = (even per).

For example: The set of odd permutation in S_3 is

$O_3 = \{ (12), (13), (23) \} \neq \phi$

1) O_3 has no identity element (I).

2) $(12) \circ (13) = (1\,3\,2) \notin O_3$. The operation is not binary on O_3.

$\therefore$ O_3 is not a subgroup of S_3.

Ex: Find the order of each element in a group S_3. IS S_3 a cyclic ?

Sol:

I is the identity element in a group $S_3 \Rightarrow o(I) = 1$

$(12)^2 = (12)(12) = I \Rightarrow o(12) = 2 = o(13) = o(23).$

$(123)^2 = (123)(123) = (132)$

$(123)^3 = (123)^2 . (123) = (132)(123) = I$

$\Rightarrow o((123)) = 3 = o((132)).$

a	I	(12)	(13)	(23)	(123)	(132)
$o(a)$	1	2	2	2	3	3

No, S_3 is not a cyclic group since there is no $a \in S_3$ s.t $o(a) = |S_3| = 6$.

* Ex: Is E_3 a cyclic ?!

Yes, E_3 is a cyclic group generated by (123) or (132) as $o((123)) = 3 = |E_3|$

Remarks:

1. Every subgroup of cyclic group is cyclic.

2. (S_n, o) is a group $\nearrow$ non-commutative if $n > 2$; $\searrow$ commutative if $n = 1, 2$

$S_1 = \{I\}$, $S_2 = \{I, (12)\}$

1. Express each of the following permutations as a product of disjoint cycles:

   (a) The permutation $\sigma \in S_8$ given by

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

   (b) $(135)(357)(579) \in S_9$

   (c) $(13)(234)(4578) \in S_8$

   (d) $(12)(23)(43)(57)(24)(61) \in S_7$

   Solution:

   (a) $\sigma = (15862374)$.

   (b) $(13)(79)$

   (c) (1345782)

   (d) $(162)(34)(57)$

2. For each of the permutations of question 1 say, giving a reason, whether it is even or odd.

   Solution:

   (a) This is an 8-cycle. It is odd, since 8 is even.

   (b) This is even; it is a product of two transpositions.

   (c) This is a 7-cycle and hence is even.

   (d) This is even; it is a product of six transpositions.

3. For each of the permutations of question 1 say, giving a reason, what its order is.

   Solution:

   (a) This is an 8-cycle and has order 8.

   (b) This is a product of 2 disjoint transpositions and has order 2.

   (c) This is a 7-cycle and has order 7.

   (d) From its representation as a product of disjoint cycles, the order of this permutation is $\text{lcm}(3, 2, 2) = 6$.

4. Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix} \text{ and } \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}.$$

Compute each of the following.

(a) α^{-1}

$$\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix}$$

(b) $\beta\alpha$

$$\beta\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 2 & 3 & 4 & 5 \end{bmatrix}$$

(c) $\alpha\beta$

$$\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 5 & 3 & 4 \end{bmatrix}$$

5 Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{bmatrix} \text{ and } \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}.$$

Write α, β, and $\alpha\beta$ as

(a) products of disjoint cycles;

$$\alpha = (12345)(678),\ \beta = (23847)(56),\ \alpha\beta = (12485736)$$

(b) products of 2-cycles.

$$\alpha = (15)(14)(13)(12)(68)(67),\ \beta = (27)(24)(28)(23)(56),$$

$$\alpha\beta = (16)(13)(17)(15)(18)(14)(12)$$

6 Write each of the following permutations as a product of disjoint cycles.

(a) (1235)(413)

(15)(234)

(b) (13256)(23)(46512)

(124)(35) or (124)(35)(6)

7. For each of the following permutations, do four things: (i) Write it as a product of disjoint cycles (disjoint cycle notation), (ii) Find its order, (iii) Write it as a product of transpositions (not necessarily disjoint), and (iv) Find its parity (even or odd).

(a) (1 2 3 5 7)(2 4 7 6)

Solution: (i) (1 2 4)(3 5 7 6) (ii) order = 12, (iii) (1 4)(1 2)(3 6)(3 7)(3 5) (iv) odd

(b) (1 2)(1 3)(1 4)

Solution: (i) (1 4 3 2) (ii) 4 (iii) already done (iv) odd

(c) (1 2 3 4 5)(1 2 3 4 6)(1 2 3 4 7)

Solution: (i) (1 4 7 3 6 2 5) (ii) 7 (iii) (1 5)(1 2)(1 6)(1 3)(1 7)(1 4) (iv) even

(d) (1 2 3)(1 3 2)

Solution: (i) ε (ii) 1 (iii) (1 2)(1 2) (iv) even

(e) $(1\ 2\ 3)(3\ 5\ 7)(1\ 2\ 3)^{-1}$

Solution: (i) (1 5 7) (ii) 3 (iii) (1 7)(1 5) (iv) even

(f) $(1\ 2\ 3\ 4\ 5)^3$

Solution: (i) (1 4 2 5 3) (ii) 5 (iii) (1 3)(1 5)(1 2)(1 4) (iv) even

Cosets of a subgroup.

Definition:

Let G be a group, $H \leq G$. A right H-coset in G is a set of the form:

$$Ha = \{ha \mid h \in H\}, \text{ for some } a \in G.$$

Similarly,

a left H-coset in G is the set of the form

$$aH = \{ah \mid h \in H\}, \text{ for some } a \in G.$$

Definition (Index)

The number of distincit right (left) cosets of G is called the index of H in G and is denoted by $[G : H]$.

Remarks:

1). If G and H are both finite group, then $[G:H] = \frac{|G|}{|H|}$
If G and H are both infinite; then $[G:H]$ can be finite.

Example :

Let $G = S_3$ and $H = \{(1), (13)\}$. Then;
All left cosets of H in G are

$(1)H = H$

$(12)H = \{(12), (12)(13)\} = \{(12), \underline{(132)}\}$

$(13)H = \{(13), (13)(13)\} = \{(13), (1)\} = H$

$(23)H = \{(23), (23)(13)\} = \{(23), \underline{(123)}\} = (123)H.$

$\underline{(123)}H = \{(123), (13)(123)\} = \{(123), (23)\}$

$\underline{(132)}H = \{(132), (13)(132)\} = \{(132), (12)\} = (12)H$

All distinct left cosets of H in G are

$$H, (12)H, (23)H.$$

All right cosets of H in G are:

$H(1) = H$

$H(12) = \{(12), (13)(12)\} = \{(12), \underline{(123)}\} = (123)H$

$H(13) = H$ as $(13) \in H$.

$H(23) = \{(23), (13)(23)\} = \{(23), \underline{(132)}\} = (132)H$

All distinct right cosets of H in G are

H, $H(12)$, $H(23)$.

Since $|S_3| = 3! = 6$ and $|H| = 2$, the index of H in G is given by

$$[G:H] = \frac{|G|}{|H|} = \frac{6}{2} = 3.$$

Note that: $(12)H \neq H(12)$

H.W: Find all distinct left and right cosets of $H = \{(1), (12)\}$ in S_3.

Remark:

I G is abelian group, $H \leq G$, $a \in G$. Then

$$aH = Ha.$$

Ex: Let $G = \mathbb{Z}$ and $H = 5\mathbb{Z} = \{0, \pm 5, \pm 10, \dots\}$. Then All left (= right) cosets of $5\mathbb{Z}$ in $\mathbb{Z}$ are

$0 + 5\mathbb{Z} = \{\dots -10, -5, 0, 5, 10, \dots\}$

$1 + 5\mathbb{Z} = \{\dots, -9, -4, 1, \boxed{6}, 11, \dots\}$

$2 + 5\mathbb{Z} = \{\dots, -8, -3, 2, \boxed{7}, 12, \dots\}$

$3 + 5\mathbb{Z} = \{\dots, -7, -2, 3, 8, 13, \dots\}$

$4 + 5\mathbb{Z} = \{\dots, -6, -1, 4, 9, 14, \dots\}$

$5 + 5\mathbb{Z} = \{\dots, -5, 0, 5, 10, 15, \dots\}$

$6 + 5\mathbb{Z} = 1 + 5\mathbb{Z}$

$7 + 5\mathbb{Z} = 2 + 5\mathbb{Z}$

7 mod 5

All distinct left (right) cosets of $5\mathbb{Z}$ in $\mathbb{Z}$ are

$5\mathbb{Z}$, $1+5\mathbb{Z}$, $2+5\mathbb{Z}$, $3+5\mathbb{Z}$, $4+5\mathbb{Z}$.

In general:

All left (right) cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are

$n\mathbb{Z}$, $1+n\mathbb{Z}$, $2+n\mathbb{Z}$, ..., $(n-1)+n\mathbb{Z}$.

Note that : $[\underset{\text{infinite}}{\mathbb{Z}}, \underset{\text{infinite}}{5\mathbb{Z}}] = \underset{\text{finite}}{5}$

In general: $[\mathbb{Z}, n\mathbb{Z}] = n$

Ex 3: Find all distinct left and right cosets of $H=\{1,-1\}$ of $G=\{1,-1,i,-i\}$.

Since G is abelian group, $H \leq G$, then all left (= right) cosets of H in G are

$(1)H = H = (-1)H$ as $-1, 1 \in H$.

$(i)H = \{i, -i\}$

$(-i)H = \{-i, i\}$

Thus all distinct cosets are: H, iH.

Properties of cosets:

Let H be a subgroup of G, and let a and b belong to G. Then,

1. $a \in aH$,
2. $aH = H$ *if and only if* $a \in H$,
3. $aH = bH$ *if and only if* $a \in bH$
4. $aH = bH$ *or* $aH \cap bH = \varnothing$,
5. $aH = bH$ *if and only if* $a^{-1}b \in H$,
6. $|aH| = |bH|$,
7. $aH = Ha$ *if and only if* $H = aHa^{-1}$,
8. aH *is a subgroup of G if and only if* $a \in H$.

Lagrange's theorem:

If G is a finite group, $H \leq G$, then

$$|H| \mid |G|$$

Proof:

Since G is a finite group, then $\exists$ a finite distinct left (right) cosets of H in G, say

$a_1H, a_2H, \ldots a_nH$

$\Rightarrow G = a_1H \cup a_2H \cup a_3H \ldots \cup a_nH.$

where

$a_iH \cap a_jH = \Phi \quad \forall i \neq j$

$\Rightarrow |G| = |a_1H| + |a_2H| + \cdots + |a_nH|$

$= |H| + |H| + \cdots + |H|$

$= n|H|$

$\Rightarrow |H| \mid |G|.$

Example:

If $|G| = 12$ then the only possible orders for a subgroups are 1, 2, 3 4, 6 and 12.

* Remark:

1. Lagrange's Theorem greatly simplifies the problem of determing all the subgroups of a finite group.

2. The converse of lagrang's Theorem is not true ingeneral. That is, if n is a divisor of $G \not\Rightarrow G$ has a subgroup of order n.

For example: -

The set of all even permutations E_4 in S_4 is given by

$E_4 = \{(1), (12)(34), (13)(24), (14)(23), (123), (132),$
$(124), (142), (134), (143), (234), (243)\}$

$|E_4| = 12$, then the only possible orders for a subgroups are:

$\{(1)\}$ of order 1

$\{(12)(34), (13)(24), (14)(23)\}$ of order 2

$\{(123), (132), (124), (142), (134), (143), (234), (243)\}$
of order 3

$\{A_4\}$ of order 12.

We see that E_4 has no subgroup of order 6.

In general:-

For $n \geq 3$, A_n doesn't contain a subgroup of order
$\frac{n!}{4}$.

Theorem:- Every subgroup of cyclic group is cyclic.

Proof: See p. 77-78 (Contemporary Abstract Algebra).

Corollary: Subgroups of $\mathbb{Z}_n$:

For each positive divisor k of n the set $\langle n/k\rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k. Moreover, these are the only subgroups of $\mathbb{Z}_n$.

Ex: Find all subgroups of $\mathbb{Z}_{12}$

$\mathbb{Z}_{12}$ is finite cyclic group. All subgroups of $\mathbb{Z}_{12}$

$\langle 12/\overset{k}{12}\rangle = \langle 1\rangle = \{0, 1, 2, \ldots, 12\}$ of order 12

$\langle 12/6\rangle = \langle 2\rangle = \{0, 2, 4, 6, 8, 10\}$ of order 6

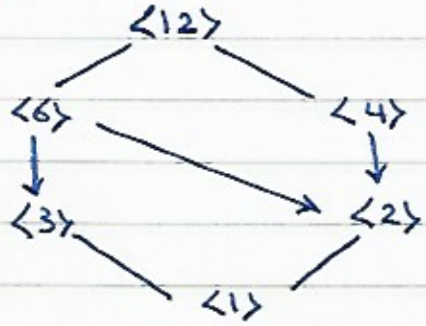
$\langle 12/4\rangle = \langle 3\rangle = \{0, 3, 6, 9\}$ of order 4

$\langle 12/3\rangle = \langle 4\rangle = \{0, 4, 8\}$ of order 3

$\langle 12/2\rangle = \langle 6\rangle = \{0, 6\}$ of order 2

$\langle 12/1\rangle = \langle 12\rangle = \{0\}$ of order 1.

Subgroup lattic of Z_{12}:



Ex: Find all subgroups of Z_{24}.

Z_{24} is finite cyclic group of order 24. All subgroups of Z_{24} are:

$\langle 24/24 \rangle = \langle 1 \rangle = \{0, 1, 2, \dots 24\}$

$\langle 24/12 \rangle = \langle 2 \rangle = \{0, 2, 4, 8, 10, \dots 22\}$

$\langle 24/8 \rangle = \langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21\}$

$\langle 24/6 \rangle = \langle 4 \rangle = \{0, 4, 8, 12, 16, 20\}$

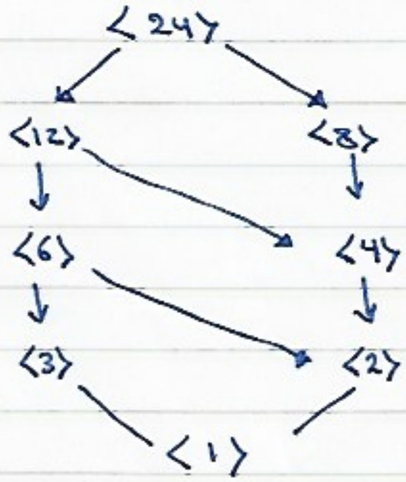
$\langle 24/4 \rangle = \langle 6 \rangle = \{0, 6, 18, 18\}$

$\langle 24/3 \rangle = \langle 8 \rangle = \{0, 8, 16\}$

$\langle 24/2 \rangle = \langle 12 \rangle = \{0, 12\}$

$\langle 24/1 \rangle = \langle 24 \rangle = \{0\}$

Subgroup lattic of Z_{24}:—



Nice Corollaries of Lagrang:

Corollary 1:

Every group of order prime is cyclic. (abelian)

Proof:

Let G be a group, $|G| = p$

Let H be cyclic subgroup of G generated by a where $a \neq e$. By Lagrange's theorem we have

$$|H| \mid |G|$$

but $|G| = p \Rightarrow |H| = 1$ or $|H| = p$

If $|H| = 1 \Rightarrow H = \{e\} = \langle e \rangle$ which is a contradiction with $a \neq e$

Hence $|H| = p = |G| \Rightarrow G = H$ is cyclic

(G is abelian group).

Corollary 2:

If G is a finite group, $a \in G$, then

- $o(a) \mid |G|$
- $a^{|G|} = e$

Remark:

Every group of order prime has only two subgroups, namely $\{e\}$ and the group itself.

For example: The subgroups of $\mathbb{Z}_5$ are: 1 and $\mathbb{Z}_5$ since $|\mathbb{Z}_5| = 5$ (prime).

Normal subgroup.

Definition:

If G is a group, $H \leq G$, then H is called normal if

$$aH = Ha \quad \forall a \in G.$$

we write $H \trianglelefteq G$.

Remark:

If G is abelian group, $H \leq G$, then $aH = Ha \quad \forall a \in G$ and H is normal subgroup. i.e:

" Every subgroup of abelian group is normal."

For example:

1. $5\mathbb{Z}$ is normal subgroup of $\mathbb{Z}$ since $\mathbb{Z}$ is abelian group and $5\mathbb{Z} \leq \mathbb{Z}$. We write $5\mathbb{Z} \trianglelefteq \mathbb{Z}$.

2. $H = \{(1), (13)\}$ is not normal subgroup of S_3 since

$$(12)\,H \neq H\,(12)$$

Ex: Show that a subgroup E_3 is normal of S_3.

Solution:

$$E_3 = \{I, (123), (132)\} \leq S_3.$$

① $IE_3 = E_3 = E_3 I$. as $I \in E_3$

② $(12)E_3 = \{(12)I, (12)(123), (12)(132)\} = \{(12), (23), (13)\}$
$= (13)E_3 = (23)E_3$

③ $\left.\begin{array}{l} (123)E_3 = E_3 = E_3(123) \\ (132)E_3 = E_3 = E_3(132) \end{array}\right\}$ as (123) and $(132) \in H$.

we just need to check that: $E_3(12) = (12)E_3$

$E_3(12) = \{I(12), (123)(12), (132)(12)\}$
$= \{(12), (13), (23)\}$
$= (12)E_3$.

Thus E_3 is normal subgroup of S_3.

Theorem:

If G is a group, $H \leq G$ then $H \trianglelefteq G$ iff $aHa^{-1} \subseteq H$ $\forall a \in G$.

Proof:

($\Rightarrow$) H is normal of G (given)

$\Rightarrow aH = Ha \quad \forall a \in G$.

$aHa^{-1} = Haa^{-1} = He = H$.

$\therefore aHa^{-1} \subseteq H$

($\Leftarrow$) $aHa^{-1} \subseteq H \quad \forall a \in G$ (given)

we need to show that

$aH = Ha \quad \forall a \in G$.

let $ah \in aH \Rightarrow aha^{-1} \in aHa^{-1}$

Since $aHa^{-1} \subseteq H \Rightarrow aha^{-1} \in aHa^{-1} \subseteq H$

$\Rightarrow aha^{-1} \in H \Rightarrow aha^{-1}a \in Ha$

$\Rightarrow aH \subseteq Ha \rightarrow (1)$

Also, $Ha \subseteq aH \rightarrow (2)$

Thus: $aH = Ha \quad \forall a \in G$

Therefore, H is normal subgroup of G.

Theorem:

If G is a group, $H \leq G$ s.t $[G : H] = 2$ then $H \trianglelefteq G$.

Proof:

Since $[G:H]=2$, then there exists only two distinct left (Right) cosets of H in G. Say

H , aH $\quad$ (H, Ha)

$\Rightarrow G = H \cup aH \quad , \quad H \cap aH = \phi$

and

$G = H \cup Ha \quad , \quad H \cap Ha = \phi$

since

$$aH \subseteq G = H \cup Ha$$

$$\Rightarrow aH \subseteq Ha$$

Also, $\quad Ha \subseteq aH$

$$\Rightarrow aH = Ha \quad \forall a \in G$$

Thus:

H is normal of G.

For example:

we have seen that E_3 is normal subgroup. By this theorem: we can say:

$E_3 \leq P_3$ and $[P_3 : E_3] = \dfrac{|P_3|}{|E_3|} = \dfrac{3!}{3} = \dfrac{6}{3} = 2$

Then E_3 is normal subgroup of S_3.

Remark:

The converse of theorem is not true. For example:

$3\mathbb{Z}$ is normal subgroup of $\mathbb{Z}$ as $\mathbb{Z}$ is abelian group.

But

$$[\mathbb{Z} : 3\mathbb{Z}] = 3 \neq 2.$$

Quotient Group.

Definition:

Let H be a normal subgroup of G. The factor group or (quotient group) G/H is the set of all left cosets of H in G. i.e

$G/H = \{aH : a \in G\}$. where the multiplication is defined by

$$aH * bH = abH \quad \text{or } a+bH$$

- Theorem: $(G/H, *)$ is a group.
- order of G/H:

  The order of G/H is given by

$$|G/H| = [G:H] = |G|/|H|.$$

Example:

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

a. Compute the cosets of $\mathbb{Z}_8/H$.

b. Does it form a group.

Solution

a. All cosets of H:

$$|G/H| = \frac{|G|}{|H|} = \frac{8}{2} = 4$$

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

$1 + \{0,4\} = \{1,5\}$

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

$3 + \{0,4\} = \{3,7\}$

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

b.

+	{0,4}	{1,5}	{2,6}	{3,7}
{0,4}	{0,4}	{1,5}	{2,6}	{3,7}
{1,5}	{1,5}	{2,6}	{3,7}	{0,4}
{2,6}	{2,6}	{3,7}	{0,4}	{1,5}
{3,7}	{3,7}	{0,4}	{1,5}	{2,6}

How the computation is done.

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

or:- نختار أي عدد من كل وحدة مثلاً نختار 2 من {2,6} و 1 من {1,5} ونجمعهم 2+1=3 ونشوف حاصل الجمع في أي coset. نجد أن 3 موجودة في {3,7}.

1- $\mathbb{Z}_8/H$ is closed under +.

2- it has an identity element $H = \{0,4\}$

3- Every element has an inverse

4- Associativity

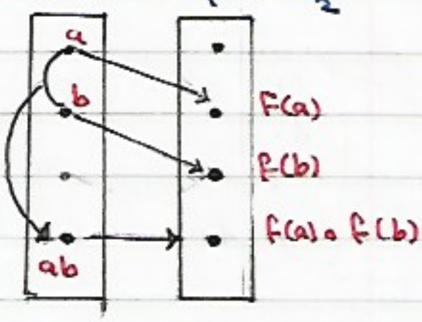
$\Rightarrow$ G/H forms a group.

Homomorphism.

Definition:

Let $(G_1, *)$ and $(G_2, \circ)$ be groups. A function $f: G_1 \to G_2$ is called **homomorphism** if $\forall a, b \in G$

$$\underbrace{f(a * b)}_{\text{operation in } G_1} = \underbrace{f(a) \circ f(b)}_{\text{operation in } G_2}$$



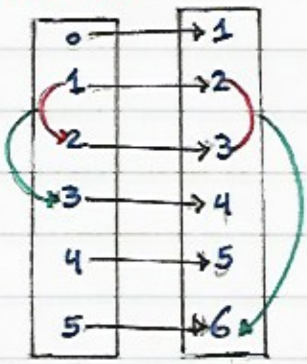
Furthermore:

If f is one-to-one function, we may call it a monomorphism
" " " onto " " " epimorphism
" " " bijective " " " " isomorphism

If $G_1 = G_2$ we may call a
a homomorphisim $f: G \to G$ endomorphisim of G.
an Isomorphisim $f: G \to G$ automorphisime "

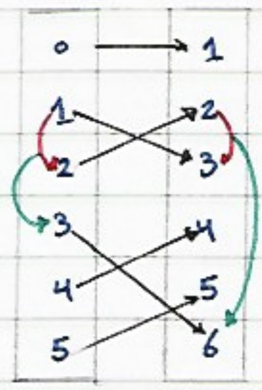
Examples:

1. Let $f: \mathbb{Z}_6 \to U_7$ given by $f(n) = n+1$ then
f is not a homomorphisim since
$f(1+2) = f(3) = 4$
and
$f(1) \cdot f(2) = 2 \times 3 = 6$
Thus
$f(1+2) \neq f(1) f(2)$.



$(\mathbb{Z}_6, +)$ $(U_7, \times)$

2. Let $f: \mathbb{Z}_6 \to U_7$ given by $f(n) = 3^n$
f is a homomorphism since
$f(n+m) = 3^{n+m}$
$= 3^n \cdot 3^m$
$= f(n) \cdot f(m)$
Moreover, f is an isomorphism since it is 1-1 and onto.



$f(0) = 3^0 = 1$
$f(1) = 3$
$f(2) = 9 \equiv 2$
$f(3) = 27 \equiv 6$
$f(4) = 81 \equiv 4$
$f(5) = 243 \equiv 5$

$(\mathbb{Z}_6, +)$ $(U_7, \times)$
works!

The Kernal of homomorphism

Definition:

If $f: G_1 \to G_2$ is homomorphisim, then the kernal of f is defined by

$$\text{Ker} f = \{a \in G_1 : f(a) = \overset{\in G_2}{e_2}\}$$

For example:

1. The kernal of the map $f: Z_6 \to U_7$ defined by $f(n) = n+1$ is given by:

$$\text{Ker} f = \{a \in Z_6 : f(a) = 1\} \quad \text{Idintity in } G_2 = U_7$$

$$= \{a \in Z_6 : a+1 = 1\}$$

$$= \{0\}.$$

2. The kernal of $f: Z_6 \to U_7$ defined by $f(n) = 3^n$ is

$$\text{Ker} f = \{a \in Z_6 : f(a) = 1\}$$

$$= \{a \in Z_6 : 3^a = 1\}$$

$$= \{0\}.$$

3. The kernal of $f: (R^+, \times) \to (R, +)$ defined by $f(x) = \ln(x)$ is given by

$$\text{Ker} f = \{a \in R^+ : f(a) = 0\} \quad \text{Identity in} (R,+)$$

$$= \{a \in R^+ : \ln(a) = 0\}$$

$$= \{1\}$$

Example: If $f : (R^+, \times) \longrightarrow (R, +)$ is a function defined by
$f(x) = \ln x \quad \forall x \in R^+$, show that f is isomorphisim.

1- let $a, b \in R^+$ then $f(ab) = \ln(ab) = \ln(a) + \ln(b)$
$= f(a) + f(b)$

Thus f is homomorphisim.

2- let $a, b \in R^+$ such that $f(a) = f(b)$
$\Rightarrow \ln(a) = \ln(b)$
$\Rightarrow a = b$

Thus f is 1-1

3- let $b \in R$, $a \in R^+$ such that $f(a) = b$
$\Rightarrow \ln a = b$
$\Rightarrow a = e^b$

Thus $\forall b \in R \ \exists \ a = e^b \in R^+$ s.t $f(a) = b$ i.e
f is onto

Hence from (1), (2), (3), f is isomorphisim.

Theorem: If $f : G_1 \rightarrow G_2$ is homomorphism then
1)- $\ker f$ is normal subgroup of G_1.
2)- $\ker f = \{e\}$ iff f is one-to-one.