Groups
(For under graduate students)

**1.Binary operation:** Let $S$ be a non-empty and $*$ be an operation such that for any ordered pair $a,b \in S \Rightarrow a*b=c \in S$. Then the operation $*$ is called binary operation.

**Ex:** Ordinary addition and multiplications are binary operations in set of integers $Z$. But ordinary division is not binary operations in $Z$.

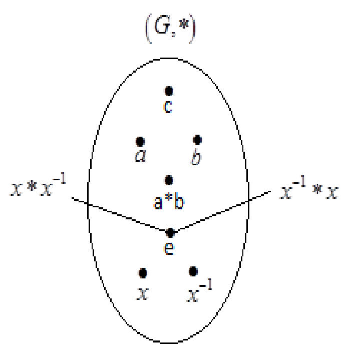
**2.Group:** Let $G$ be non-empty set and $*$ be a binary operations in $G$. The set $(G,*)$ is said to be a group if it satisfies.

i) **Closer axiom:** For $a,b \in G \Rightarrow a*b \in G$.

ii) **Associative axiom:** $a*(b*c)=(a*b)*c \; \forall a,b,c \in G$.

iii) **Identity axiom:** There exits $e \in G$ such that $a*e=e*a=a \; \forall a \in G$. The element $e$ is called identity element in $G$ with respect to $*$.

iv) **Inverse axiom:** For any $x \in G$, there exits $x^{-1} \in G$ such that $x*x^{-1}=x^{-1}*x=e$. The element $x^{-1}$ is called inverse of $x$ in $G$.




**Ex:** The set of $Z$ integers is a group under addition, the set of real numbers $R$ is a group under multiplication.

**Note:** The set $(G,*)$ is said to be a groupoid if it satisfies closer axiom only.

The set $(G,*)$ is said to be a semi group if it satisfies closer and associative axioms.

The set $(G,*)$ is said to be a monoid group if it satisfies closer, associative and identity axioms.

**3.Abelian group:** The group $(G,*)$ is said to be a abelian group if it satisfies

**Commutative axiom:** $a*b=b*a\ \forall\ a,b\in G$.

**Ex:** The set of $2\times 2$ matrices is a group under matrices multiplication but not abelian group. Because matrices multiplication is not commutative.

**4.Finite group:** If the number of elements in the group is finite, then it is called finite group.
**Ex:** The set of fourth roots of unity $\{1,-1,\ i,-i\}$ is a finite group under multiplication.

**5. Order of group:** The number of elements in the group is called order of group. The order of group $G$ is denoted by $o(G)$.

**Ex:** The order of group of fourth roots of unity $(G,.)=\{1,-1,\ i,-i\}$ is a 4.

**6. Order of an element of group:** Let $(G,.)$ be a group and $a\in G$. There exists a least positive integer $p$ such that $a^p=e$, then $p$ is called order of element $p$. It is denoted by $o(a)$.

**Ex:** The order of an elements $1,-1,\ i,-i$ in group $(G,.)=\{1,-1,\ i,-i\}$ are 1,2,4,4 respectively.

**Theorem. 7:** In a group $G$, identity element is unique.

**Proof:** If possible, let $e_1,e_2$ be two identity elements in the group $(G,*)$.

$\therefore\quad e_1*e_2=e_2*e_1=e_2$ ($\because$ $e_1$ is identity element in $G$)

and $e_1*e_2=e_2*e_1=e_1$($\because$ $e_2$ is identity element in $G$)

$\therefore\quad e_1=e_2$

Henceidentity element group is unique

**Theorem. 8:** In a group $G$, inverse of any element is unique.

**Proof:** Let $e$ be identity element in $(G,*)$ and $a\in G$.

If possible, let $b,c$ be two inverses of $a$ in $G$.

$\therefore\ a*b=b*a=e$ and $a*c=c*a=e$

$\therefore\quad c*(a*b)=c*e=c$ ……………,..(1)

and $c*(a*b)=(c*a)*b=e*b=b$ ……..(2)

$\therefore$ From $(1)$ and $(2)$, $b=c$

$\therefore$ Inverse of $a$ is unique in $G$.

Type.1: Special binary operation

**Example. 9:** prove that the set $G$ of rational numbers other than 1 with binary operation $*$ such that $a*b=a+b-ab$ for $a,b\in G$ is an abelian group.

**Solution:** Let $a,b,c$ be any three elements in $G$.

**Closure axiom:** $a*b=a+b-ab\in G$

**Associative axiom:**

$$a*(b*c)=a*(b+c-bc)=a+(b+c-bc)-a(b+c-bc)$$
$$=a+b+c-ab-bc-ca+abc=(a+b-ab)+c-(a+b-ab)c=(a*b)*c$$

**Identity axiom:** There exist $e\in G$ such that $a*e=a\Rightarrow a+e-ae=a\Rightarrow e=0\in G$

**Inverse axiom:** There exist $x\in G$ such that $a*x=e\Rightarrow a+x-ax=0\Rightarrow x=\frac{-a}{1-a}\in G$

**Commutative axiom:** For $a*b=a+b-ab=b+a-ba=b*a$

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

**Example.10:** prove that the set of integers $Z$ is an abelian group for the binary operation $*$ such that $a*b=a+b+1\,\forall\, a,b\in Z$.

Type.2: Finite sets

**Example.11:** prove that the set of $n^{th}$ roots of unity is a finite abelian group under multiplication.

**Solution:** Since $1=cas0+i\sin 0=cas2k\pi+i\sin 2k\pi$

$$\therefore 1^{\frac{1}{n}}=cas\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n} \text{ where } k=o,1,2,...,n-1$$
$$=e^{i\frac{2k\pi}{n}} \text{ where } k=o,1,2,...,n-1$$

Let $G=\left\{e^{i\frac{2k\pi}{n}} \mid k=o,1,2,...,n-1\right\}$ be set of $n^{th}$ roots of unity

and $x=e^{i\frac{2\alpha\pi}{n}}, y=e^{i\frac{2\beta\pi}{n}}, z=e^{i\frac{2\gamma\pi}{n}}\in G$

**Closure axiom:** $x.y=e^{i\frac{2\alpha\pi}{n}}.e^{i\frac{2\beta\pi}{n}}=e^{i\frac{2(\alpha+\beta)\pi}{n}}\in G$ if $\alpha+\beta\geq n,$ then $\alpha+\beta=\alpha+\beta-n$

**Associative axiom:**

$$x.(y.z)=e^{i\frac{2\alpha\pi}{n}}.\left(e^{i\frac{2\beta\pi}{n}}.e^{i\frac{2\beta\pi}{n}}\right)=e^{i\frac{2\alpha\pi}{n}}.e^{i\frac{2(\beta+\gamma)\pi}{n}}=e^{i\frac{2[\alpha+(\beta+\gamma)]\pi}{n}}$$
$$=e^{i\frac{2[(\alpha+\beta)+\gamma]\pi}{n}}=e^{i\frac{2(\alpha+\beta)\pi}{n}}.e^{i\frac{2\gamma\pi}{n}}=\left(e^{i\frac{2\alpha\pi}{n}}.e^{i\frac{2\beta\pi}{n}}\right).e^{i\frac{2\gamma\pi}{n}}=(x.y).z$$

**Identity axiom:** 1 is identity under multiplication. So $1 = e^{i\frac{2(0)\pi}{n}} \in G$.

**Inverse axiom:** The inverse of $x$ is $x^{-1}$.

Clearly $x^{-1} = e^{i\frac{2(n-\alpha)\pi}{n}} \in G$ such that $x.x^{-1} = x^{-1}.x = 1 \forall\, x \in G$.

**Commutative axiom:** $x.y = e^{i\frac{2\alpha\pi}{n}}.e^{i\frac{2\beta\pi}{n}} = e^{i\frac{2(\alpha+\beta)\pi}{n}} = e^{i\frac{2(\beta+\alpha)\pi}{n}} = e^{i\frac{2\beta\pi}{n}}.e^{i\frac{2\alpha\pi}{n}} = y.x$

Hence the set of $n^{th}$ roots of unity is a finite abelian group.

**Example.12:** prove that the set of fourth roots of unity $\{1, -1, i, -i\}$ is a finite abelian group under multiplication.

**Solution:** Let $G = \{1, -1, i, -i\}$

Binary operation table

| . | 1 | -1 | i | -i |
|---|---|---|---|---|
| 1 | 1 | -1 | i | -i |
| -1 | -1 | 1 | -i | i |
| i | i | -i | -1 | 1 |
| -i | -i | i | 1 | -i |

**Closure axiom:** Product of any two elements in $G$ is also in $G$.

**Associative and commutative axioms:** The elements in $G$ are complex numbers. These numbers obeys associative and commutative axioms.

**Identity axiom:** 1 is identity under multiplication which belongs to $G$.

**Inverse axiom:** The inverses of $1, -1, i, -i$ are $1, -1, -i, i$ respectively.

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

**Example.13:** prove that the set of cube roots of unity $\{1, \omega, \omega^2\}$ is a finite abelian group under multiplication.

**Example.15:** prove that the set $G = \{A, B, C, D\}$ is an abelian group under matrix multiplication.

Where $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $D \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

Type.3: Finite sets under additive (or multiplicative) modulo m.

**Example.16:** prove that the set $G=\{0,1,2,3,4\}$ is an abelian group with respect to $+_5$.

**Solution:**

Binary operation table

| $+_5$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

**Closure axiom:** Addition of any two elements in $G$ is also in $G$ under $+_5$.

**Associative and commutative axioms:** The elements in $G$ are integers. These numbers obeys associative and commutative axioms.

**Identity axiom:** 0 is identity under addition which belongs to $G$.

**Inverse axiom:** The inverses of 0,1,2,3,4 are 0,4,3,2,1 in $G$ respectively.

Hence $(G,+_5)$ is an abelian group.

**Example.17:** prove that the set $G=\{1,2,3,4\}$ is an abelian group with respect to $\times_5$.

Type.4: Special sets

**Example.14:** prove that the set $\left\{A_\alpha \mid A_\alpha=\begin{bmatrix} cos\,\alpha & -\sin\alpha \\ \sin\alpha & cas\,\alpha \end{bmatrix}, \alpha\in R\right\}$ is a group under matrix multiplication.

**Solution:** Let $G=\left\{A_\alpha \mid A_\alpha=\begin{bmatrix} cos\,\alpha & -\sin\alpha \\ \sin\alpha & cas\,\alpha \end{bmatrix}, \alpha\in R\right\}$ and $A_\alpha, A_\beta, A_\gamma \in G$.

**Closure axiom:**

$$A_\alpha A_\beta=\begin{bmatrix} cos\,\alpha & -\sin\alpha \\ \sin\alpha & cas\,\alpha \end{bmatrix}\begin{bmatrix} cos\,\beta & -\sin\beta \\ \sin\beta & cas\,\beta \end{bmatrix}$$

$$=\begin{bmatrix} cos\,\alpha\, cos\,\beta-\sin\alpha\sin\beta & -\sin\alpha\, cas\beta-cos\,\alpha\sin\beta \\ -\sin\alpha\, cas\beta-cos\,\alpha\sin\beta & cos\,\alpha\, cos\,\beta-\sin\alpha\sin\beta \end{bmatrix}$$

$$= \begin{bmatrix} cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & cas(\alpha+\beta) \end{bmatrix} \in G$$

**Associative axiom:**

$$A_\alpha\left(A_\beta A_\gamma\right) = \begin{bmatrix} cos\,\alpha & -\sin\alpha \\ \sin\alpha & cas\,\alpha \end{bmatrix} \left\{ \begin{bmatrix} cos\,\beta & -\sin\beta \\ \sin\beta & cas\,\beta \end{bmatrix} \begin{bmatrix} cos\,\gamma & -\sin\gamma \\ \sin\gamma & cas\,\gamma \end{bmatrix} \right\}$$

$$= \begin{bmatrix} cos\,\alpha & -\sin\alpha \\ \sin\alpha & cas\,\alpha \end{bmatrix} \begin{bmatrix} cos(\beta+\gamma) & -\sin(\beta+\gamma) \\ \sin(\beta+\gamma) & cas(\beta+\gamma) \end{bmatrix}$$

$$= \begin{bmatrix} cos\{\alpha+(\beta+\gamma)\} & -\sin\{\alpha+(\beta+\gamma)\} \\ \sin\{\alpha+(\beta+\gamma)\} & cas\{\alpha+(\beta+\gamma)\} \end{bmatrix}$$

$$= \begin{bmatrix} cos\{(\alpha+\beta)+\gamma\} & -\sin\{(\alpha+\beta)+\gamma\} \\ \sin\{(\alpha+\beta)+\gamma\} & cas\{(\alpha+\beta)+\gamma\} \end{bmatrix}$$

$$= \begin{bmatrix} cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & cas(\alpha+\beta) \end{bmatrix} \begin{bmatrix} cos\,\gamma & -\sin\gamma \\ \sin\gamma & cas\,\gamma \end{bmatrix} = \left(A_\alpha A_\beta\right) A_\gamma$$

**Identity axiom:** $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is identity under multiplication.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} cos\,0 & -\sin 0 \\ \sin 0 & cas\,0 \end{bmatrix} = A_0 \in G$$

**Inverse axiom:** The inverse of $A_\alpha$ is $A_\alpha^{-1}$.

$$A_\alpha^{-1} = \begin{bmatrix} cos\,\alpha & \sin\alpha \\ -\sin\alpha & cas\,\alpha \end{bmatrix} = \begin{bmatrix} cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & cas(-\alpha) \end{bmatrix} \in G \;\forall A_\alpha \in G.$$

Hence $(G, .)$ is a group.

Dr. K. Hanuma Reddy
Lecturer in Mathematics
Hindu College, Guntur

………………..