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

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

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

we shall now prove the uniqueness.

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

$y_1 * a = b$ and $y_2 * a = b$.

$\Rightarrow y_1 * a = y_2 * a$

$\Rightarrow y_1 = y_2$ [by right cancellation law]

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

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

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

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

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

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

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

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

$\Rightarrow a = (a^{-1})^{-1}$ [by left-cancellation law

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

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

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

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

Now consider, $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b$

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

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

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

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

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

Worked Examples.

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

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

cayley table is

$\cdot$	1	−1
1	1	−1
−1	−1	1

Closure:

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

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

Identity: 1 is the identity element.

Inverse: Inverse of 1 is 1 and inverse of −1 is −1

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

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

Eg.(2) Let $G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$, show that G is a group under the operation of matrix multiplication.

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

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

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

I is the identity element.

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

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

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

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

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

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

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

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

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

$\therefore$ Cayley table is

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

Closure :

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

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

Identity: I is the identity element.

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

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

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

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

$AB = BA = C$; $BC = CB = A$ and $AC = CA = B$.

---

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

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

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

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

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

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

Hence G is closed under *.

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

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

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

$\therefore$ usual multiplication is associative.

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

So associative axiom is satisfied.

Identity:- Suppose $e \in G$ be the identity, then $a*e = a \; \forall \; a \in G$

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

so, identity is 2.

Inverse: Let a be any element of G. suppose a' is its inverse then,

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

so, for every element $a \in G$ inverse is $\frac{4}{a}$.

Thus inverse axiom is satisfied.

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

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

$= b*a$

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

---

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

Soln:

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