GROUPS

Definition:

An operation on a set G is a function $* : G \times G \to G$.

Definition:

A group is a set G which is equipped with an operation $*$ and a special element $e \in G$, called the identity, such that

(i) the associative law holds: for every $x, y, z \in G$,

$$x * (y * z) = (x * y) * z;$$

(ii) $e * x = x = x * e$ for all $x \in G$;

(iii) for every $x \in G$, there is $x' \in G$ (so-called, inverse) with $x * x' = e = x' * x$.

Example:

Set	Operation "+"	Operation "$*$"	Additional Condition
$\mathbb{N}$	no	no	—
$\mathbb{Z}$	yes	no	—
$\mathbb{Q}$	yes	no	"$*$" for $\mathbb{Q} \setminus \{0\}$
$\mathbb{R}$	yes	no	"$*$" for $\mathbb{R} \setminus \{0\}$
$\mathbb{R} \setminus \mathbb{Q}$	no	no	—

Example:

Set	Operation "+"	Operation "$*$"
$Z_{>0}$	no	no
$Z_{\geq 0}$	no	no
$Q_{>0}$	no	yes
$Q_{\geq 0}$	no	no
$R_{>0}$	no	yes
$R_{\geq 0}$	no	no

Example:

Set	Operation "+"	Operation "$*$"
$\{2n : n \in \mathbb{Z}\}$	yes	no
$\{2n+1 : n \in \mathbb{Z}\}$	no	no
$\{3n : n \in \mathbb{Z}\}$	yes	no
$\{kn : n \in \mathbb{Z}\}$, where $k \in \mathbb{N}$ is some fixed number	yes	no
$\{a^n : n \in \mathbb{Z}\}$, where $a \in \mathbb{R}, a \neq 0, \pm 1$, is some fixed number	no	yes
$\left\{\frac{p}{2^n} : p \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}\right\}$	yes	no

Example:

Set	Operation: $a * b = a^2 b^2$	Operation: $a * b = a^b$
$\mathbb{R}_{>0}$	no	no

Definition:
A group is called abelian if $x * y = y * x$ for any $x, y \in G$.

Example:
The parity group $\mathcal{P}$ has two elements, the words "even" and "odd," with operation

$$\text{even} \boxplus \text{even} = \text{even} = \text{odd} \boxplus \text{odd}$$

and

$$\text{even} \boxplus \text{odd} = \text{odd} = \text{odd} \boxplus \text{even}.$$

It is clear that:

1. "even" is the identity element;
2. The inverse of "even" is "even" and the inverse of "odd" is "odd".

Example:

The group $\mathbb{Z}_2$ has two elements: [0] is the set of all even numbers and [1] is the set of all odd numbers. Operation:

$$[0] \boxplus [0] = [1] \boxplus [1] = [0]$$

and

$$[0] \boxplus [1] = [1] \boxplus [0] = [1].$$

It is clear that:

1. [0] is the identity element;
2. The inverse of [0] is [0] and the inverse of [1] is [1].

Example:

The group $\mathbb{Z}_3$ has three elements:

[0] is the set of numbers which are congruent to 0 mod 3;

[1] is the set of numbers which are congruent to 1 mod 3;

[2] is the set of numbers which are congruent to 2 mod 3.

Operation:

$$[0] \boxplus [0] = [1] \boxplus [2] = [2] \boxplus [1] = [0],$$
$$[0] \boxplus [1] = [1] \boxplus [0] = [2] \boxplus [2] = [1],$$

and

$$[0] \boxplus [2] = [2] \boxplus [0] = [1] \boxplus [1] = [2].$$

It is clear that:

1. [0] is the identity element;
2. The inverse of [0] is [0], the inverse of [1] is [2], and the inverse of [2] is [1].

Example:

The group $\mathbb{Z}_3^\times$ has two elements:

[1] is the set of numbers which are congruent to 1 mod 3;

[2] is the set of numbers which are congruent to 2 mod 3.

Operation:

$$[1] \boxtimes [1] = [2] \boxtimes [2] = [1]$$

and

$$[1] \boxtimes [2] = [2] \boxtimes [1] = [2].$$

It is clear that:

1. [1] is the identity element;
2. The inverse of [1] is [1] and the inverse of [2] is [2].

Notation:

We denote by S_n the set of all the permutations of the set $X = \{1, 2, \ldots, n\}$.

Theorem:

S_n is a nonabelian group (so-called, symmetric group) under operation of composition.

Proof (Sketch): It is obvious that S_n is closed under operation of composition. One can show that this operation is associative. The identity element is (1). Finally, by the theorems above *every permutation α is either a cycle or a product of disjoint (with no common elements) cycles* and *the inverse of the cycle $\alpha = (i_1 i_2 \ldots i_r)$ is the cycle $\alpha^{-1} = (i_r i_{r-1} \ldots i_1)$*. Therefore, every element of S_n is invertible. To show that S_n is nonabelian, we note that, for example, $(123)(13) \neq (13)(123)$. ■

Notation:

We denote by $GL(2, \mathbb{R})$ the set of all 2×2 nonsingular (determinant is nonzero) matrices with real entries and with operation matrix multiplication.

Theorem:

$GL(2, \mathbb{R})$ is a nonabelian group (so-called, general linear group).

Proof (Sketch): It is obvious that $GL(2, \mathbb{R})$ is closed under operation of multiplication. One can show that this operation is associative. The identity element is

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Finally, for every element

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

there exists the inverse

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

To show that $GL(2, \mathbb{R})$ is nonabelian, we note that, for example,

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}. \blacksquare$$

Theorem:

Let G be a group.

(i) If $x * a = x * b$ or $a * x = b * x$, then $a = b$.

(ii) The identity element e is unique.

(iii) For all $x \in G$, the inverse element x^{-1} is unique.

(iv) For all $x \in G$ we have $(x^{-1})^{-1} = x$.

(v) For all $a, b \in G$ we have $(a * b)^{-1} = b^{-1} * a^{-1}$.

Proof:

(i) Let $x * a = x * b$, then

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

therefore by the associative law we get

$$\left(x^{-1} * x\right) * a = \left(x^{-1} * x\right) * b,$$

so

$$e * a = e * b,$$

and the result follows. In the same way one can deduce $a = b$ from $a * x = b * x$.

(ii) Assume to the contrary that there are two identity elements e_1 and e_2. Then

$$e_1 = e_1 * e_2 = e_2,$$

which is a contradiction.

(iii) Assume to the contrary that for some $x \in G$ there are two inverse elements x_1^{-1} and x_2^{-1}. Then

$$x_2^{-1} = \left(x_1^{-1} * x\right) * x_2^{-1} = x_1^{-1} * \left(x * x_2^{-1}\right) = x_1^{-1},$$

which is a contradiction.

(iv) We have

$$\left(x^{-1}\right)^{-1} * x^{-1} = e.$$

Multiplying both sides by x, we get

$$\left(x^{-1}\right)^{-1} * \left(x^{-1} * x\right) = e * x,$$

hence

$$\left(x^{-1}\right)^{-1} * e = x,$$

and the result follows.

(v) We have

$$(a * b) * \left(b^{-1} * a^{-1}\right) = \left[a * \left(b * b^{-1}\right)\right] * a^{-1} = (a * e) * a^{-1} = a * a^{-1} = e,$$

and the result follows. ■

SUBGROUPS

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

(i) $e \in H$;

(ii) if $x, y \in H$, then $x * y \in H$;

(iii) if $x \in H$, then $x^{-1} \in H$.

Notation:
If H is a subgroup of G, we write $H \leq G$.

Example:
It is obvious that $\{e\}$ and G are always subgroups of a group G.

Definition:
We call a subgroup H proper, and we write $H < G$, if $H \neq G$. We call a subgroup H of G nontrivial if $H \neq \{e\}$.

Example:

The parity group $\mathcal{P}$ has two elements, the words "even" and "odd," with operation

$$\text{even} \boxplus \text{even} = \text{even} = \text{odd} \boxplus \text{odd}$$

and

$$\text{even} \boxplus \text{odd} = \text{odd} = \text{odd} \boxplus \text{even}.$$

It is clear that:

1. **"even" is the identity element;**
2. **The inverse of "even" is "even" and the inverse of "odd" is "odd".**

Example:

The group Z_2 has two elements: $[0]$ is the set of all even numbers and $[1]$ is the set of all odd numbers. Operation:

$$[0] \boxplus [0] = [1] \boxplus [1] = [0]$$

and

$$[0] \boxplus [1] = [1] \boxplus [0] = [1].$$

It is clear that:

1. **$[0]$ is the identity element;**
2. **The inverse of $[0]$ is $[0]$ and the inverse of $[1]$ is $[1]$.**

Example:

The group Z_3 has three elements:

[0] is the set of numbers which are congruent to 0 mod 3;

[1] is the set of numbers which are congruent to 1 mod 3;

[2] is the set of numbers which are congruent to 2 mod 3.

Operation:

$$[0] \boxplus [0] = [1] \boxplus [2] = [2] \boxplus [1] = [0],$$

$$[0] \boxplus [1] = [1] \boxplus [0] = [2] \boxplus [2] = [1],$$

and

$$[0] \boxplus [2] = [2] \boxplus [0] = [1] \boxplus [1] = [2].$$

It is clear that:

1. [0] is the identity element;

2. The inverse of [0] is [0], the inverse of [1] is [2], and the inverse of [2] is [1].

Example:

The group $Z_3^\times$ has two elements:

[1] is the set of numbers which are congruent to 1 mod 3;

[2] is the set of numbers which are congruent to 2 mod 3.

Operation:

$$[1] \boxtimes [1] = [2] \boxtimes [2] = [1]$$

and

$$[1] \boxtimes [2] = [2] \boxtimes [1] = [2].$$

It is clear that:

1. [1] is the identity element;

2. The inverse of [1] is [1] and the inverse of [2] is [2].

Notation:
We denote by S_n the set of all the permutations of the set $X = \{1, 2, \ldots, n\}$.

Theorem:
S_n is a nonabelian group (so-called, symmetric group) under operation of composition.

Proof (Sketch):

It is obvious that S_n is closed under operation of composition. One can show that this operation is associative. The identity element is (1). Finally, by the theorems above *every permutation* α *is either a cycle or a product of disjoint (with no common elements) cycles* **and** *the inverse of the cycle* $\alpha = (i_1 i_2 \dots i_r)$ *is the cycle* $\alpha^{-1} = (i_r i_{r-1} \dots i_1)$**. Therefore, every element of S_n is invertible. To show that S_n is nonabelian, we note that, for example, $(123)(13) \neq (13)(123)$.** ■

Notation:

We denote by $GL(2, R)$ the set of all 2×2 nonsingular (determinant is nonzero) matrices with operation matrix multiplication.

Theorem:

$GL(2, R)$ is a nonabelian group (so-called, general linear group).

Proof (Sketch): It is obvious that $GL(2, R)$ is closed under operation of multiplication. One can show that this operation is associative. The identity element is

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Finally, for every element

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

there exists the inverse

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

To show that $GL(2, R)$ is nonabelian, we note that, for example,

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}. \blacksquare$$

Theorem:

Let G be a group.

(i) If $x * a = x * b$ or $a * x = b * x$, then $a = b$.

(ii) The identity element e is unique.

(iii) For all $x \in G$, the inverse element x^{-1} is unique.

(iv) For all $x \in G$ we have

$$\left(x^{-1}\right)^{-1} = x.$$

(v) For all $a, b \in G$ we have

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

(i) Let $x * a = x * b$, then

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

therefore by the associative law we get

$$\left(x^{-1} * x\right) * a = \left(x^{-1} * x\right) * b,$$

so

$$e * a = e * b,$$

and the result follows. In the same way one can deduce $a = b$ from $a * x = b * x$.

(ii) Assume to the contrary that there are two identity elements e_1 and e_2. Then

$$e_1 = e_1 * e_2 = e_2,$$

which is a contradiction.

(iii) Assume to the contrary that for some $x \in G$ there are two inverse elements x_1^{-1} and x_2^{-1}. Then

$$x_2^{-1} = \left(x_1^{-1} * x\right) * x_2^{-1} = x_1^{-1} * \left(x * x_2^{-1}\right) = x_1^{-1},$$

which is a contradiction.

(iv) We have

$$\left(x^{-1}\right)^{-1} * x^{-1} = e.$$

Multiplying both sides by x, we get

$$\left(x^{-1}\right)^{-1} * \left(x^{-1} * x\right) = e * x,$$

hence

$$\left(x^{-1}\right)^{-1} * e = x,$$

and the result follows.

(v) We have

$$\begin{aligned}
&(a * b) * \left(b^{-1} * a^{-1}\right) \\
&= \left[a * \left(b * b^{-1}\right)\right] * a^{-1} \\
&= (a * e) * a^{-1} \\
&= a * a^{-1} \\
&= e,
\end{aligned}$$

and the result follows.

Definition:

A subset H of a group G is a subgroup if

(i) $e \in H$;

(ii) if $x, y \in H$, then $x * y \in H$;

(iii) if $x \in H$, then $x^{-1} \in H$.

Notation:

If H is a subgroup of G, we write

$$H \leq G.$$

Example:
It is obvious that $\{e\}$ and G are always subgroups of a group G.

Definition:
We call a subgroup H proper, and we write $H < G$, if $H \neq G$. We call a subgroup H of G nontrivial if $H \neq \{e\}$.