Subject: Abstract Algebra
Topic: Group Theory

Dr. Pankaj Kumar
Assistant Professor
Department of Mathematics,
Maharaja Agrasen University,
Kalujhanda, Solan (HP) - 173104

Binary Operations: Let A be a non empty set and let $*$ be any operation defined on A. Then, $*$ is said to be a binary operation if $x * y \in A, \forall\, x, y \in A$.

- **Examples :**
- Let R be the set of real numbers then operation of addition (+) is a binary operation on R, because, $x + y \in R, \forall\, x, y \in$ R.
- Let N be the set of natural numbers then operation of addition (+) is a binary operation on N, because, $x + y \in N, \forall\, x, y \in N$. However, operation of subtraction (-) is not a binary operation on N, because $x - y \notin N, \forall\, x, y \in$ N.

For example $2, 5 \in N\ but\ 2 - 5 = -3 \notin N$.

Algebraic Structure: Let G be a non empty set and $*$ be a binary operation defined on G. Then (G, $*$) is said to be an algebraic structure.

Examples:

- Addition (+) is a binary operation on the set of real numbers R. Therefore, (R, +) is an algebraic structure.
- Multiplication (×) is a binary operation on the set of integers Z. Therefore, (Z, ×) is an algebraic structure.
- Division (÷) is a binary operation on the set of non-zero real numbers R_0. Therefore, $(R_0, \div)$ is an algebraic structure. But Division (÷) is not a binary operation on the set of integers, therefore, (Z, ÷) is not an algebraic structure.

Group: Let G be a non empty set and $*$ be an operation defined on G then G is said to be a group with respect to $*$ or (G, $*$) be a group if the following properties are satisfied:

1. **Closure property:** Let $x, y \in G$ then $x * y \in G$.
2. **Associativity:** Let $x, y, z \in G$ then $(x * y) * z = x * (y * z)$
3. **Existence of Identity:** There exists an element e (say) in G such that $x * e = x \, and \, e * x = x$. Then, e is called the identity of the group.
4. **Existence of Inverse:** For each element $x \in G$ there exists an element $x^{-1} \in G$ such that $x * x^{-1} = e$. Then x^{-1} is said to be the inverse of x.

Example: The set of integers with respect to addition (Z, +) form a group.

Explanation:

1. **Closure property:** Let $x, y \in Z$, then $x + y \in Z$. Because sum of two integers again an integer.
2. **Associativity:** Let $x, y, z \in Z$ then $x + (y + z) = (x + y) + z$. Because ordering in addition of integers does not matters.
3. **Existence of Identity:** We know that $0 \in Z$. Let $x \in Z$ then $0 + x = x$, and $x + 0 = x$. So, 0 is identity element.
4. **Existence of Inverse:** Let $x \in Z$ then $-x \in Z$. Now, $x + (-x) = 0$, thus $-x$ is inverse of x. Thus inverse exists for each element of Z.

Some More Examples:

- (Q, +), (R, +), (C, +) are groups.
- $(Q_0, \times)$, $(R_0, \times)$, $(C_0, \times)$ are groups, where $Q_0 = Q - \{0\}$ and so on.
- M = $\{[a_{ij}]_{n\times n}: a_{ij} \in$ R} is a group with respect to addition of matrices.
- The set $Z_n = \{0,1,2, \dots \dots n-1\}$ is a group with respect to addition modulo n $(+_n)$ for all values of $n \in N$.

Abelian Group: Let (G, $*$) be a group, then it is called abelian if $\boldsymbol{x} * \boldsymbol{y} = \boldsymbol{y} * \boldsymbol{x}, \forall\, \boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{G}$.

Examples:

- (Q, +), (R, +), (C, +) are abelian groups.
- $(Z_n, +_n)$ is a abelian group.
- $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, where $i.j = k, j.k = i, k.i = j, j.i = -k, k.j = -i, i.k = -j, i^2 = -1, j^2 = -1, k^2 = -1$. Q_8 is a group with respect to multiplication but not an abelian group.

Order of Element: Let $(G,*)$ be a group and $a \in G$. A positive integer m is said to be the order of a if $a^m = e$ and $a^n \neq e$ for $n < m$. Then, we write $o(a) = m$.
Here, $a^m = a * a * a \ldots \ldots \ldots \ldots * a \ (m \ times)$.

If no such integer exists then the order of the element is said to be infinity.

Order of identity is always 1 and no other element of the group has order 1,
i.e., $o(e) = 1$.

Examples:

- In the group of non zero real numbers R_0 , 1 is the identity element. So, $o(1) = 1$. $-1 \in R_0$ and $-1 \times -1 = 1$, so $o(-1) = 2$.
- Now, let us check for $2 \in R_0$.

$2 \times 2 = 4$, $2 \times 2 \times 2 = 8$, $2 \times 2 \times 2 \times 2 = 16$ and so on. Thus, we are never going to get identity element 1. Thus in this case, there does not exists any positive integer m such that $2^m = 1$. So, order of 2 is infinite.

Cyclic group: A group $(\boldsymbol{G},*)$ is said to be cyclic if there exists an element $\boldsymbol{a}$ in G such that all the elements of G can be written in powers of $\boldsymbol{a}$.

It means, we can write the elements like $\boldsymbol{a}, \boldsymbol{a}^{2}, \boldsymbol{a}^{3}, \ldots \ldots \ldots$.

Then $\boldsymbol{a}$ is called generator of the group G.

If $\boldsymbol{a}$ is the generator of a group G then order of $\boldsymbol{a}$ is equal to the order of the group.

Examples:

- (Z, +) is a cyclic group and, 1 and -1 are the generators. It is an example of an infinite cyclic group.
- $(Z_n, +_n)$ is a cyclic group. The numbers relative prime to n are the generators. It is an example of a finite group.
- The order of the generator of cyclic group is always equal to the order of group.


Thank
you