Binary composition:

Let A be a non empty set. A function $*: A \times A \to A$ is called a binary composition or binary operation on A.

Ex: $+, \times$ are binary operation from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$, $\mathbb{N}$ is a set of Natural numbers. But $-$ is not a binary operation on $\mathbb{N}$ since,

$-(2, 3) = 2 - 3 = -1 \notin \mathbb{N}$

Similarly, $\div$ is not a binary operation on $\mathbb{N}$.

Ex: $+, \times, -$ are binary operation on $\mathbb{Z}$, $\mathbb{Z}$ is the set of integers.

Group: A non empty set G, together with a binary composition $*$ is said to form a group if it satisfies the following postulates:

(1) Associativity: $a*(b*c) = (a*b)*c$, $\forall a,b,c \in G$

(2) Existence of identity: $\exists$ an element $e \in G$ such that, $a*e = a = e*a$, $\forall a \in G$

(3) Existence of inverse: For every $a \in G$, $\exists$ any element $b \in G$ such that $a*b = e = b*a$, e is the identity and b is called the inverse of a.

If G is a group with the binary operation $*$, then we denote it by $\langle G, * \rangle$

Ex: $\langle \mathbb{Z}, + \rangle$ is a group, i.e. the set of integers with the operation '$+$' is a group.

Let $a, b, c \in \mathbb{Z}$ be any three elements

(i) $a+(b+c) = (a+b)+c$, therefore associativity hold

(ii) $\exists\ 0 \in \mathbb{Z}$ such that $a+0 = a = 0+a$, $\forall a \in \mathbb{Z}$

$\therefore$ 0 is the identity in $\mathbb{Z}$ with respect to the operation $+$ (it is called additive identity)

(iii) Since, $a+(-a) = 0 = (-a)+a$, $\forall a \in \mathbb{Z}$.

$\therefore -a$ is the inverse of a,

Note: $\mathbb{N}$, the set of natural numbers is not a group with respect to addition. In $\mathbb{N}$, associativity holds, but it does not possess identity element and inverse of any element.

Ex: The set of real numbers, the set of Rational numbers are groups under ordinary addition. In each case 0 is the identity and inverse of a is $-a$.

Ex: The set of integers $\mathbb{Z}$ under ordinary multiplication is not a group. Here, associativity law is trivially held, and 1 is the identity. But $a\ (\neq 1)$ of $\mathbb{Z}$ does not have inverse, $\forall a \in \mathbb{Z}$, e.g. 5 has no inverse element under $\times$ in $\mathbb{Z}$ because there does not exist an integer b such that $5b = 1$.

Ex: The set $G = \{1, -1, i, -i\}$ is a group under complex multiplication.

Ex: The set $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$ is a group under matrix addition.

Semigroup: Let G is a non empty set. Then G is called a semigroup under a binary operation $*$ if $a*(b*c) = (a*b)*c$, $\forall a, b, c \in G$. i.e if G satisfy only associativity law, then G is called a semigroup.

Ex: We know that $\langle \mathbb{N}, + \rangle$ is not a group, but it is a semigroup.

Ex: $\langle \mathbb{Z}, \cdot \rangle$ is a semigroup with ordinary multiplication.

Abelian group: Let $\langle G, * \rangle$ is a group. Then G is said to be abelian if $a*b = b*a$, $\forall a, b \in G$. i.e if the operation $*$ is commutative in G then G is called an abelian group.

Ex: $\langle \mathbb{Z}, + \rangle$ is an abelian group. Since '+' is commutative.

Ex: $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} ; a, b, c, d \in \mathbb{R} \right\}$ is an abelian group with respect to matrix addition.