2. Groups

2.1. Binary composition.

Let A be a non-empty set. A binary composition (or a binary operation) on A is a mapping $f : A \times A \to A$. Therefore a binary composition f assigns to each ordered pair of elements of A a definite element of A. This mapping f is generally denoted by the symbol $\circ$. For a pair of elements a, b in A, the image of (a, b) under the binary composition $\circ$ is denoted by $a \circ b$. The image of the element (b, a) is obviously $b \circ a$.

The symbols like $*, +, \cdot, \oplus, \odot$ are also used to denote a binary composition.

Examples.

1. On the set $\mathbb{Z}$ let $\circ$ stand for the binary composition 'addition'. Then $2 \circ 3 = 5, 4 \circ -4 = 0$.

2. On the set $\mathbb{Z}$ let $\circ$ stand for the binary composition 'multiplication'. Then $2 \circ 3 = 6, 3 \circ 0 = 0$.

3. On the set $\mathbb{Z}$ let $\circ$ stand for the binary composition 'subtraction'. Then $3 \circ 2 = 1, 1 \circ 3 = -2$.

4. On the set $\mathbb{Z}$ let a binary composition $\circ$ be defined by $a \circ b = a + 2b, a, b \in \mathbb{Z}$. Then $2 \circ 3 = 8, 3 \circ 0 = 3$.

5. On the set $\mathbb{Q}$ let a binary composition $*$ be defined by $a * b = \frac{1}{2}ab$. Then $2 * 5 = 5$, $3 * 8 = 12$.

A binary composition $\circ$ is said to be *defined* on a non-empty set A if $a \circ b \in A$ for all a, b in A. In this case the set A is said to be *closed* under (or closed with respect to) the binary composition $\circ$.

For example, the set $\mathbb{N}$ is closed under 'addition', since $a \in \mathbb{N}, b \in \mathbb{N} \Rightarrow a + b \in \mathbb{N}$. But the set $\mathbb{N}$ is not closed under 'subtraction', because $a - b$ does not belong to $\mathbb{N}$ for some a, b in $\mathbb{N}$.

Definition. Let $\circ$ be a binary composition on a set A.

$\circ$ is said to be *commutative* if $a \circ b = b \circ a$ for all $a, b \in A$.

$\circ$ is said to be *associative* if $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in A$.

Examples (continued).

6. Addition on the set $\mathbb{R}$ is both commutative and associative. Multiplication on the set $\mathbb{R}$ is both commutative and associative, but subtraction on the set $\mathbb{R}$ is neither commutative nor associative.

7. Let S be a non-empty set and $P(S)$ be the power set of S. Then $\cup$ (union), $\cap$ (intersection) and Δ (symmetric difference) are binary compositions on $P(S)$ and each of these is commutative and associative on $P(S)$.

8. Let $M_2(\mathbb{R})$ be the set of all 2×2 real matrices. Let $\circ$ stand for multiplication of matrices. Then $\circ$ is associative but not commutative.

9. Let n be a positive integer and let us consider the ρ-equivalence classes of the relation ρ on $\mathbb{Z}$ defined by "$a \rho b$ if and only if $a - b$ is divisible by n" for $a, b \in \mathbb{Z}$. There are n classes $cl(0), cl(1), cl(2), \ldots, cl(n-1)$. These are also called the *classes of residues* of integers modulo n. We use the notation $\bar{a}$ to denote the class $cl(a)$. Let $\mathbb{Z}_n$ be the set of residue classes $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$.

We define a binary composition $+$, called addition modulo n, on the set $\mathbb{Z}_n$ by $\bar{a} + \bar{b} = \overline{a+b}$.

In order that this definition may be valid we must check that it is well defined, i.e., it is independent of the choice of representatives of the equivalence classes. Therefore we have to show that if a, a', b, b' are integers such that $cl(a') = cl(a)$ and $cl(b') = cl(b)$ then $\overline{a+b} = \overline{a'+b'}$.

$\bar{a} = \bar{a}' \Rightarrow a - a' = kn$ for some integer k,

$\bar{b} = \bar{b}' \Rightarrow b - b' = pn$ for some integer p.

Therefore $(a+b) - (a'+b') = tn$, where $t(= k+p)$ is an integer.

Consequently, $\overline{a+b} = \overline{a'+b'}$.

This proves that 'addition modulo n' is a well defined binary composition on the set $\mathbb{Z}_n$.

In like manner, we define a binary composition, called multiplication modulo n, on the set $\mathbb{Z}_n$ by $\bar{a}.\bar{b} = \overline{ab}$ and we can prove similarly that it is a well defined composition on the set $\mathbb{Z}_n$, i.e., if $cl(a') = cl(a)$ and $cl(b') = cl(b)$ then $\overline{ab} = \overline{a'b'}$.

Both these compositions are commutative as well as associative, because

$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$ for all $\bar{a}, \bar{b} \in \mathbb{Z}_n$;

$\bar{a}.\bar{b} = \overline{ab} = \overline{ba} = \bar{b}.\bar{a}$ for all $\bar{a}, \bar{b} \in \mathbb{Z}_n$;

and $$\begin{aligned} \bar{a} + (\bar{b} + \bar{c}) &= \bar{a} + \overline{b+c} = \overline{a + (b+c)} = \overline{(a+b)+c} \\ &= \overline{a+b} + \bar{c} = (\bar{a} + \bar{b}) + \bar{c} \text{ for all } \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n; \end{aligned}$$

$$\bar{a}.(\bar{b}.\bar{c}) = \bar{a}.\overline{bc} = \overline{a(bc)} = \overline{(ab)c}$$
$$= \overline{ab}.\bar{c} = (\bar{a}.\bar{b}).\bar{c} \text{ for all } \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n.$$

2.2. Composition table.

When A is a non-empty finite set a binary composition $\circ$ on the set A can be defined by a table, called the *composition table*. If the number of elements in A be n, the table has n rows and n columns, one for each element of the set. The elements of the set are listed on the topmost row and the leftmost column in the same order.

If $A = \{a_1, a_2, \ldots, a_n\}$ then $a_i \circ a_j$ appears on the table in the ith row and jth column. The n^2 entries of the table are all elements of A, since A is closed under $\circ$.

If the table be symmetric about the principal diagonal (i.e., if $a_i \circ a_j = a_j \circ a_i$) then $\circ$ is commutative.

For example, the table for the binary composition of 'addition modulo 3' on the set $\mathbb{Z}_3$ is

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Here the composition is commutative.

Exercises 6

1. Examine whether the composition $\circ$ defined on the set is (i) commutative, (ii) associative.

(a) $\circ$ on $\mathbb{Z}$ defined by $a \circ b = a + b + 1, a, b \in \mathbb{Z}$;

(b) $\circ$ on $\mathbb{Q}$ defined by $a \circ b = ab + 1, a, b \in \mathbb{Q}$;

(c) $\circ$ on $\mathbb{R}$ defined by $a \circ b = a + 2b, a, b \in \mathbb{R}$;

(d) $\circ$ on $\mathbb{R}$ defined by $a \circ b = |ab|, a, b \in \mathbb{R}$;

(e) $\circ$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \circ (c, d) = (a - c, b - d), (a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$;

(f) $\circ$ on $M_2(\mathbb{R})$ defined by $A \circ B = \frac{1}{2}(AB - BA), A, B \in M_2(\mathbb{R})$.

2. Let $\circ$ be an associative binary composition on a set S. Let T be a subset of S defined by $T = \{a \in S : a \circ x = x \circ a \text{ for all } x \in S\}$. Prove that T is closed under $\circ$.

3. Let S be a set of two elements. How many different binary compositions can be defined on S? How many different commutative binary compositions can be defined on S?

2.3. Groupoid.

Let G be a non-empty set on which a binary composition $\circ$ is defined. Some algebraic strucure is imposed on G by the composition $\circ$ and $(G, \circ)$ becomes an algebraic system. The algebraic system $(G, \circ)$ is said to be a *groupoid*. The groupoid $(G, \circ)$ is comprised of two entities, the set G and the composition $\circ$ on G. The same set G may form different groupoids with respect to different binary compositions on it.

Examples.

1. $(\mathbb{Z}, +)$ and $(\mathbb{Z}, -)$ are both groupoids. They are different algebraic systems although the underlying set is $\mathbb{Z}$ in each case.
2. $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{Q}, .), (\mathbb{R}, .)$ are groupoids.
3. $(\mathbb{Z}_n, +), (\mathbb{Z}_n, .)$ are groupoids.
4. $(M_2(\mathbb{R}), +)$ is a groupoid, where $+$ is the matrix addition. $(M_2(\mathbb{R}), .)$ is a groupoid, where $.$ is the matrix multiplication.

Definitions.

A groupoid $(G, \circ)$ is said to be a *commutative groupoid* if the binary composition $\circ$ is commutative.

An element e in G is said to be an *identity element* in the groupoid $(G, \circ)$ if $a \circ e = e \circ a = a$ for all a in G.

Example 4. $(\mathbb{Z}, +)$ is a commutative groupoid but $(\mathbb{Z}, -)$ is not a commutative groupoid. 0 is an identity element in $(\mathbb{Z}, +)$. There is no identity element in $(\mathbb{Z}, -)$.

Definitions.

An element e in G is said to be a *right identity* in the groupoid $(G, \circ)$ if $a \circ e = a$ for all a in G.

An element e in G is said to be a *left identity* in the groupoid $(G, \circ)$ if $e \circ a = a$ for all a in G.

Examples (continued).

5. In the groupoid $(\mathbb{Z}, +)$, 0 is a left identity as well as a right identity. In the groupoid $(\mathbb{Z}, .)$, 1 is a left identity as well a right identity.
6. In the groupoid $(\mathbb{Z}, -)$, there is no left identity, but 0 is a right identity.

Theorem 2.3.1. If a groupoid $(G, \circ)$ contains an identity element, then that element is unique.

Proof. If possible, let there be two identity elements e and f in $(G, \circ)$. Then $e \circ a = a \circ e = a$ and $f \circ a = a \circ f = a$ for all a in G.

Now $e \circ f = e$, by the property of f
and $e \circ f = f$, by the property of e.
Therefore $e = f$.

Theorem 2.3.2. If a groupoid $(G, \circ)$ contains a left identity as well as a right identity then they are equal and the equal element is the identity element in the groupoid.

Proof. Let e be a left identity and f be a right identity in $(G, \circ)$.
Then $e \circ a = a$ for all a in G, $a \circ f = a$ for all a in G.
Now $e \circ f = f$ by the property of e
and $e \circ f = e$ by the property of f.
Therefore $e = f$.
This proves that e is an identity element in the groupoid and by the Theorem 2.3.1, e is the only identity element in the groupoid.

Definition.

Let $(G, \circ)$ be a groupoid containing the identity element e. An element a in G is said to be *invertible* if there exists an element a' in G such that $a' \circ a = a \circ a' = e$. a' is said to be *an inverse* of a in the groupoid.

An element a in G is said to be *left invertible* if there exists an element b in G such that $b \circ a = e$. b is said to be a *left inverse* of a in the groupoid.

An element a in G is said to be *right invertible* if there exists an element c in G such that $a \circ c = e$. c is said to be a *right inverse* of a in the groupoid.

Examples (continued).

7. 1 is the identity element in the groupoid $(\mathbb{Z}, .)$. -1 in $\mathbb{Z}$ is invertible because $x.(-1) = (-1).x = 1$ holds in $\mathbb{Z}$ for $x = -1$. 2 in $\mathbb{Z}$ has no left inverse in the groupoid because there is no element x in $\mathbb{Z}$ such that $x.2 = 1$. Also 2 has no right inverse in the groupoid because there is no element y in $\mathbb{Z}$ such that $2.y = 1$.

8. 1 is the identity element in the groupoid $(\mathbb{Q}, .)$. 2 in $\mathbb{Q}$ is invertible because there exists an element $\frac{1}{2}$ in $\mathbb{Q}$ such that $\frac{1}{2}.2 = 2.\frac{1}{2} = 1$. 0 in $\mathbb{Q}$ is not invertible.

Definition. If e be just a left identity in the groupoid $(G, \circ)$, then an element a in G is said to be *left e-invertible* if there exists an element b in G such that $b \circ a = e$ and a is said to be *right e-invertible* if there exists an element c in G such that $a \circ c = e$. b is said to be a *left e-inverse* of a and c is said be a *right e-inverse* of a.

When e is just a right identity, then a left e-inverse and a right e-inverse of an element can be defined in a similar manner.

Examples (continued).

9. In the groupoid $(\mathbb{Z}, -)$, 0 is a right identity. An element a in $\mathbb{Z}$ has a left 0-inverse as well as a right 0-inverse in the groupoid.

10. In the groupoid $(\mathbb{Z}, *)$ where $*$ is defined by $a * b = a + 2b, a, b \in \mathbb{Z}$, 0 is a right identity. 3 in $\mathbb{Z}$ is left 0-invertible but not right 0-invertible. 4 in $\mathbb{Z}$ is left 0-invertible as well as right 0-invertible.

2.4. Semigroup.

A groupoid $(G, \circ)$ is said to be a *semigroup* if $\circ$ is associative.

A semigroup $(G, \circ)$ is said to be a *commutative semigroup* if $\circ$ is commutative.

Examples.

1. $(\mathbb{Z}, +)$ is a semigroup. $(\mathbb{Q}, +), (\mathbb{R}, +)$ are semigroups.
2. $(\mathbb{Z}, .)$ is a semigroup. $(\mathbb{Q}, .), (\mathbb{R}, .)$ are semigroups.
3. $(\mathbb{Z}, -)$ is not a semigroup.
4. $(\mathbb{Z}_n, .)$ is a semigroup. It is a commutative semigroup.

Let $(G, \circ)$ be a semigroup and $a \in G$. Then $a \circ a \in G$.
$a \circ (a \circ a) = (a \circ a) \circ a$, since $\circ$ is associative.
Dropping the parantheses, each of them is written as $a \circ a \circ a$.
Thus $a \circ a \circ a \in G, a \circ a \circ a \circ a \in G, \ldots \quad \ldots$
Parantheses may, however, be inserted in any manner for the purpose of calculation.

The positive integral powers of $a \in G$ are defined as follows.
$a^1 = a, a^2 = a \circ a, a^3 = a \circ a \circ a, \ldots, a^{n+1} = a^n \circ a$ for all $n \in \mathbb{N}$.

Theorem 2.4.1. Let $(S, \circ)$ be a semigroup and $a \in S$. Then $a^{m+n} = a^m \circ a^n$ for all $m, n \in \mathbb{N}$.

Proof. $a^{m+n} = a \circ a \circ \cdots \circ a \quad (m + n \text{ times})$

$$a^m \circ a^n = \underbrace{(a \circ a \circ \cdots \circ a)}_{m \text{ times}} \circ \underbrace{(a \circ a \circ \cdots \circ a)}_{n \text{ times}}$$
$$= a \circ a \circ \cdots \circ a \quad (m + n \text{ times}), \text{ since } \circ \text{ is associative.}$$

Therefore $a^{m+n} = a^m \circ a^n$.

2.5. Monoid.

A semigroup $(G, \circ)$ containing the identity element is said to be a *monoid*. Therefore an algebraic system $(G, \circ)$ is said to be a monoid if
(i) $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$; and

(ii) there exists an element e in G such that $eoa = aoe = a$ for all a in G.

A monoid $(G, \circ)$ is said to be a *commutative monoid* if $\circ$ be commutative.

Examples.

1. $(\mathbb{Z}, +)$ is a monoid, 0 being the identity element.
2. $(\mathbb{Z}, .)$ is a monoid, 1 being the identity element.
3. Let E be the set of all even integers. Then $(E, .)$ is a semigroup but not a monoid.
4. $(\mathbb{Z}_n, .)$ is a monoid, $\bar{1}$ being the identity element.
5. $(M_2(\mathbb{R}), .)$ is a monoid, the identity matrix I_2 being the identity element. It is not a commutative monoid.

Theorem 2.5.1. In a monoid $(M, \circ)$ if an element a be invertible then it has a unique inverse.

Proof. Since a is invertible, there exists an element a' in M such that $a \circ a' = a' \circ a = e$, e being the identity element. a' is said to be an inverse of a.

If possible, let there be two inverses a', a'' of a in M.

Then $a \circ a' = a' \circ a = e$ and $a \circ a'' = a'' \circ a = e, e$ being the identity element.

Now $a' \circ (a \circ a'') = (a' \circ a) \circ a''$, since $\circ$ is associative.

But $a' \circ (a \circ a'') = a' \circ e = a'$ and $(a' \circ a) \circ a'' = e \circ a'' = a''$.

Therefore $a' = a''$. This proves the uniqueness of the inverse of a.

Theorem 2.5.2. In a monoid $(M, \circ)$ if an element a be left invertible as well as right invertible then a is invertible.

Proof. Let e be the identity element and b be a left inverse, c be a right inverse of a.

Then $b \circ a = e, a \circ c = e$.

Now $b \circ (a \circ c) = (b \circ a) \circ c$, since $\circ$ is associative.

But $b \circ (a \circ c) = b \circ e = b$ and $(b \circ a) \circ c = e \circ c = c$.

Therefore $b = c$ and $b \circ a = a \circ b = e$. This shows that a is invertible.

Definition. In a monoid an invertible element is said to be a *unit*.

2.6. Quasigroup.

A groupoid $(G, \circ)$ is said to be a *quasigroup* if for any two elements $a, b \in G$, each of the equations $a \circ x = b$ and $y \circ a = b$ has a unique solution in G.

Examples.

1. $(\mathbb{Z}, +)$ is a groupoid. Let $a, b \in \mathbb{Z}$. The equation $a + x = b$ has the solution $x = b - a$ in $\mathbb{Z}$ and the equation $y + a = b$ has the solution $y = b - a$ in $\mathbb{Z}$. Therefore $(\mathbb{Z}, +)$ is a quasigroup.

2. $(\mathbb{Z}, .)$ is a groupoid. $2 \in \mathbb{Z}, 3 \in \mathbb{Z}$. The equation $2.x = 3$ has no solution in $\mathbb{Z}$. Therefore $(\mathbb{Z}, .)$ is not a quasigroup.

3. $(\mathbb{Z}, -)$ is a quasigroup but not a semigroup.

4. $(M_2(\mathbb{R}), .)$ is a groupoid. The equation $A.X = B$ has no solution in M_2 if A be a singular matrix. Therefore $(M_2, .)$ is not a quasigroup.

Let G be a finite set and $a, b, c, d \in G$. The solvability of the equation $a \circ x = b$ can be read from the entries along the row of a in the composition table. If the row of a contains b in the column of the element c then $a \circ c = b$ and therefore c is a solution of the equation $a \circ x = b$. If b appears only once in the row of a, the solution of the equation $a \circ x = b$ is unique.

Similarly, the solvability of the equation $y \circ a = b$ can be read from the entries along the column of a in the composition table. If the column of a contains b in the row of the element d then $d \circ a = b$ and therefore d is a solution of the equation $y \circ a = b$. If b appears only once in thecolumn of a then the solution of the equation $y \circ a = b$ is unique.

For example, let us examine the $\circ$-composition table for the set $G = \{a, b, c\}$.

$\circ$	a	b	c
a	a	b	c
b	b	a	b
c	c	b	a

The row of b contains b twice. Therefore the equation $b \circ x = b$ has two solutions and they are $x = a, x = c$.

The row of b contains a. Therefore the equation $b \circ x = a$ has a solution in G. $x = b$ is a solution.

The row of b does not contain c. Therefore the eqution $b \circ x = c$ has no solution in G.

The column of b contains b twice. Therefore the equation $y \circ b = b$ has two solutions and they are $y = a, y = c$.

The column of b contains a. Therefore the equation $yob = a$ has a solution in G. $y = b$ is a solution.

The column of b does not contain c. Therefore the equation $y \circ b = c$ has no solution in G.

Worked Examples.

1. Define a binary composition $\circ$ on $\mathbb{Z}$ by $a \circ b = a + b - ab$ for $a, b \in \mathbb{Z}$. Show that $(\mathbb{Z}, \circ)$ is a monoid.

Let $a \in \mathbb{Z}, b \in \mathbb{Z}$. Then $a \circ b = a + b - ab \in \mathbb{Z}$. Therefore $\mathbb{Z}$ is closed under $\circ$.

Let $a, b, c \in \mathbb{Z}$.

$$\begin{aligned} a\circ(b\circ c) = a\circ(b + c - bc) &= a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - ab - bc - ca + abc. \\ (a\circ b)\circ c = (a + b - ab)\circ c &= (a + b - ab) + c - (a + b - ab)c \\ &= a + b + c - ab - bc - ca + abc. \end{aligned}$$

As $a\circ(b\circ c) = (a\circ b)\circ c$, $\circ$ is associative.

Let us examine if there exists an element e in $\mathbb{Z}$ such that $e\circ a = a\circ e = a$ for all a in $\mathbb{Z}$.

$$\begin{aligned} e\circ a = a &\Rightarrow e + a - ea = a \\ &\Rightarrow e(1 - a) = 0 \\ &\Rightarrow e = 0 \\ \text{and } a\circ e = a &\Rightarrow a + e - ae = a \\ &\Rightarrow e(1 - a) = 0 \\ &\Rightarrow e = 0. \end{aligned}$$

This shows that 0 is the identity element.

Therefore $(\mathbb{Z}, \circ)$ is a monoid.

2. Let $(S, \circ)$ be a finite semigroup and $a \in S$. Prove that there exist positive integers m, n such that $a^{m+n} = a^m$. Deduce that a^{mn} is an idempotent element in the semigroup.

[In a semigroup $(S, \circ)$, an element x is said to be an *idempotent element* if $x \circ x = x$.]

Since $(S, \circ)$ is a semigroup and $a \in S$, $a, a^2, a^3, \ldots$ all belong to S.

Since S is a finite set, there exist positive integers m and p (where $p > m$) such that $a^p = a^m$.

Let $p = m + n, n \geq 1$. Then $a^{m+n} = a^m$ for some positive integers m, n.

$a^m = a^{m+n} \Rightarrow a^m \circ a^n = a^{m+n} \circ a^n \Rightarrow a^{m+n} = a^{m+2n}$.

$a^{m+n} = a^{m+2n} \Rightarrow a^{m+n} \circ a^n = a^{m+2n} \circ a^n \Rightarrow a^{m+2n} = a^{m+3n}$.