Algebra: Chapter - 1

Binary composition: A binary composition is a mapping from $S \times S \to S$

For $a, b, c \in S,\ (a, b) \overset{*}{\to} c$, where $*$ is a given binary composition.

Example: Let $S = \mathbb{Z}, 2,3 \in \mathbb{Z},\ (2,3) \overset{+}{\to} 5$

Example: Let $S = \mathbb{Z}, 2,3 \in \mathbb{Z},\ (2,3) \overset{\times}{\to} 6$

Example: Let $S = \mathbb{Z}, 2,3 \in \mathbb{Z},\ (2,3) \overset{\div}{\to} 2/3$; thus, division is not a binary composition on $\mathbb{Z}$.

A binary composition $*$ defined on a set $S \equiv$ The set S is closed under the binary composition $*$

A binary composition $*$ is ***commutative*** on S if $a * b = b * a,\ \forall a, b \in S$

Example: $+$ is commutative on $\mathbb{Z}$ since $\forall a, b \in \mathbb{Z},\ a + b = b + a$

A binary composition $*$ is ***associative*** on S if $(a * b) * c = a * (b * c),\ \forall a, b, c \in S$

Example: $+$ is associative on $\mathbb{Z}$ since $\forall a, b, c \in \mathbb{Z},\ (a + b) + c = a + (b + c)$

A binary composition $*$ defined on a set S.
If $\exists e \in S,\ s.t.\ a * e = e * a = a,\ \forall a \in S$, e is the ***Identity Element***.

Example: 0 is the identity element w.r.t. $+$ in $\mathbb{Z}$, $s.t.\ \ a + 0 = 0 + a = a\ \forall a \in \mathbb{Z}$.

A binary composition $*$ defined on a set S and let e be the identity element.
If for each $a \in S,\ \exists b \in S$, such that $a * b = b * a = e$.
Then b is called the ***Inverse*** of a with respect to the binary composition $*$.

Example: Given $a \in \mathbb{Z},\ \exists -a \in \mathbb{Z},$ such that, $a + (-a) = (-a) + a = 0$. Then $-a$ is the inverse of a with respect to addition.

Algebraic system: A set along with a binary composition, define an "Algebraic System".

Groupoid: Most basic algebraic system. $(S,*)$ is a groupoid if the binary composition $*$ is defined on S.

Semigroup: A groupoid $(S,*)$ is a semigroup if $*$ is associative.

Monoid: A semigroup $(S,*)$ is a monoid if $\exists$ identity in S with respect to binary composition $*$.

Group: A monoid $(S,*)$ is a group if each element of S has an inverse in S with respect to $*$.

Example: $(\mathbb{Z}, +)$ is a groupoid as $\mathbb{Z}$ is closed under $+$.

$(\mathbb{Z}, +)$ is a semigroup as $+$ is associative.

$(\mathbb{Z}, +)$ is a monoid as 0 is the identity of $\mathbb{Z}$ w.r.t. $+$.

$(\mathbb{Z}, +)$ is a group as for each $a \in \mathbb{Z} - a \in \mathbb{Z}$.

Properties of a Group:

1. Closure; 2. Associativity; 3. Existence of Identity; 4. Existence of Inverse.

Abelian Group: Let $(G,*)$ be a group. If $*$ is commutative then $(G,*)$ is called a commutative/ abelian group.

Basic Properties:

A group has unique identity

Let $(G,*)$ has two identities $e, f \in G \Rightarrow a * e = e * a = a,\ \forall a \in G$ and $a * f = f * a = a, \forall a \in G$

Then $e * f = f \ \ \& \ \ e * f = e \ \Rightarrow e = f$.

Each element has unique inverse in a group

Let $a \in G$ has two inverses $a' \& a''$; then $a * a' = a' * a = e$ (identity of G) and $a * a'' = a'' * a = e$

Hence, $(a' * a) * a'' = a' * (a * a'') \Rightarrow a'' = a'$.

In $(G,*)$, $a * b = a * c \Rightarrow b = c$, $\forall a, b, c \in G$ [*Left Cancellation Law*]
$b * a = c * a \Rightarrow b = c$, $\forall a, b, c \in G$ [*Right Cancellation Law*]

Since $a \in G \Rightarrow a^{-1} \in G \ \& \ (a^{-1} * a) * b = (a^{-1} * a) * c \Rightarrow b = c$ [**Left Cancellation Law**]

Similarly, $b * (a * a^{-1}) = c * (a * a^{-1}) \Rightarrow b = c$ [**Right Cancellation Law**]

In $(G,*)$, $\forall a, b \in G$, each of the equations $a * x = b$ & $y * a = b$ has unique solutions

Since $a \in G \Rightarrow a^{-1} \in G \Rightarrow a^{-1} * b \in G$ and, $a * (a^{-1} * b) = b \Rightarrow a^{-1} * b$ is a solution of $a * x = b$
Assuming the solution is not unique, let x_1 & x_2 be two solutions;
then $a * x_1 = b = a * x_2 \Rightarrow x_1 = x_2$ (i.e. the solution is unique)

In $(G,*)$, $\forall a, b \in G$ $(a * b)^{-1} = b^{-1} * a^{-1}$

$\forall a, b \in G, (a * b) * (b^{-1} * a^{-1}) = (b^{-1} * a^{-1}) * (a * b) = e$;
This shows that $b^{-1} * a^{-1}$ is the inverse of $a * b$.

Finite Group:

A group $(G,*)$ is ***finite*** if G contains a finite number of elements. Otherwise it is called an ***infinite group***.

Example:

$(S,.)$, where $S = \{z \in \mathbb{C} : z^n = 1\}$ is a finite group;
$(\mathbb{Z},+)$ is an infinite group.

The ***order of a finite group*** is the number of elements present in it and is denoted by ***o(G)***.

Composition Table: Tabular form to denote all compositions in a finite group.

Example: Composition table for the abelian group $(S,.)$ where $S = \{z \in \mathbb{C} / \ z^3 = 1\}$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Example: Composition table for the abelian group $(\mathbb{Z}_5, \oplus_5)$,

$\mathbb{Z}_5$ →residue classes of integers $modulo\ 5$, $\oplus_5$→ addition $modulo\ 5$

$\oplus_5$	$\overline{\mathbf{0}}$	$\overline{\mathbf{1}}$	$\overline{\mathbf{2}}$	$\overline{\mathbf{3}}$	$\overline{\mathbf{4}}$
$\overline{\mathbf{0}}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{\mathbf{1}}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{\mathbf{2}}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{\mathbf{3}}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{\mathbf{4}}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Example: Composition table for Klein's 4 group $\{e, a, b, c\}$, where e is the identity, each element is its own inverse and $a * b = c = b * a,\ a * c = b = c * a,\ b * c = a = c * b$

$*$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$
$\boldsymbol{e}$	e	a	b	c
$\boldsymbol{a}$	a	e	c	b
$\boldsymbol{b}$	b	c	e	a
$\boldsymbol{c}$	c	b	a	e

Integral powers of an element of a group:

$(G,*)$ → group, and $a \in G$ be any element;

Define: (i) $a^n = a * a * a * \ldots * a\ (n\ factors)$; (ii) $a^0 = e$; (iii) $a^{-n} = a^{-1} * a^{-1} * a^{-1} * \ldots \ldots * a^{-1}\ \ (n\ \ factors)$

Laws of indices:

(i) $a^m * a^n = a^{m+n}, m, n \in \mathbb{Z}$;
(ii) $(a^m)^n = a^{mn}, m, n \in \mathbb{Z}$;
(iii) $(a^n)^{-1} = a^{-n} = (a^{-1})^n, n \in \mathbb{Z}$

Clearly, $a^m * a^n = \underbrace{(a * a * \ldots * a)}_{m\ terms} * \underbrace{(a * a * \ldots * a)}_{n\ terms} = \underbrace{(a * a * \ldots * a)}_{m+n\ terms} = a^{m+n}$

Similarly, one can show, $(a^m)^n = a^{mn}, m, n \in \mathbb{Z}$;
Again, as $a^n * a^{-n} = a^{n-n} = a^0 = e \Rightarrow a^{-n}$ is the inverse of a^n.
Thus, $(a^n)^{-1} = a^{-n} = a^{(-1).n} = (a^{-1})^n$

Order of an element of a group:

$(G,*)$ → group, and $a \in G$ be any element; a is said to be of finite order if $\exists n \in \mathbb{Z}$, such that $a^n = e$ (Identity of G).

Order of a is the least positive integer n such that $a^n = e$, denoted by $o(a) = n$.

If no such n exists then n is said to have infinite order.

Result: $o(a^{-1}) = o(a)$

Let $o(a) = m \Rightarrow a^m = e$, and if $a^p = e \Rightarrow m < p$; also, $(a^{-1})^m = e$;

Let if possible, $o(a^{-1}) = n(n < m) \Rightarrow a^{-n} = e \Rightarrow a^{m-n} = e$, $m - n < m$ (contradiction); hence the result.

Result: If $o(a) = n$ and $a^m = e \Rightarrow n|m$ $(i.e.\ n$ divides $m)$

As $o(a) = n, n$ is the least positive integer such that $a^n = e \Rightarrow m > n$;

let $m = nq + r,\ 0 \leq r < n$

$a^r = a^{m-nq} = a^m * (a^n)^{-q} = e$ (contradiction); hence, $r = 0 \Rightarrow m = nq$. i.e. $n|m$

Result: Each element of a finite group is of finite order.

$(G,*)$ be a finite group and $a \in G \Rightarrow a, a^2, a^3, \ldots$ are all elements of G ;

since G is finite all these cannot be distinct;

let m, n be such integers such that $a^m = a^n, m > n \Rightarrow a^{m-n} = e \Rightarrow o(a)$ is finite.

Example: Let G be a finite group with identity e. Then there exists a positive integer m such that $a^m = e, \forall a \in G$.

Let, $G = \{a_1, a_2, \ldots, a_n\}$ and also let $o(a_i) = m_i,\ \forall i = 1,2,..,n$

Let, $m = lcm\{m_1, m_2, \ldots, m_n\} \Rightarrow a^m = e, \forall a \in G$.

Result: If $o(a) = n$, then $o(a^m) = \frac{n}{\gcd(m,n)}$

Let, $\gcd(m,n) = h \Rightarrow m = hp\ \&\ n = hq$, $[\gcd(p,q) = 1]$;

Let, $o(a^m) = k \Rightarrow a^{mk} = e \Rightarrow n|mk \Rightarrow hq|hpk \Rightarrow q|pk \Rightarrow q|k \ldots.(1)[\because q \nmid p]$

Also, $(a^m)^q = a^{hpq} = (a^n)^p = e \Rightarrow k|q \ldots(2)$;

from (1)& (2), $o(a^m) = k = q = \frac{n}{h} = \frac{n}{\gcd(m,n)}$

Example: If b be an element of a group such that $o(b) = 20$;

then, $o(b^6) = \frac{20}{\gcd(20,6)} = 10$ & $o(b^8) = \frac{20}{\gcd(20,8)} = 5$.

Result: for any two elements $a, b \in G$, $o(ab) = o(ba)$

Let $o(ab) = n\ \&\ o(ba) = m \Rightarrow (ab)^n = e$ & $(ba)^m = e$

Again, $(ab)^n = \underbrace{ab.ab\ldots.ab}_{n\ factors} = a.\{\underbrace{ba.ba\ldots.ba}_{n-1\ factors}\}.b = a.(ba)^{n-1}.b = e \Rightarrow (ba)^{n-1} = a^{-1}b^{-1} = (ba)^{-1}$

Then, $(ba)^n = (ba)^{n-1}.ba = (ba)^{-1}.ba = e \Rightarrow m|n$…(1)

By, similar arguments, we can show that $n|m$…(2); Combining them we get $n = m$ i.e. $o(ab) = o(ba)$

Problems on Chapter 1:

1. A binary composition $*$ defined on $\mathbb{Z}$ as $a * b = a + b - ab,\ a, b \in \mathbb{Z}$.
   Examine the properties of commutativity, associativity, existence of identity and existence of inverse.
2. Examine if $(S, .)$, where $S = \{z \in \mathbb{C} / z^n = 1\}$, is an abelian group or not.
3. Examine if $(\mathbb{Z}, *)$ is a group, where $a * b = a + b + 1,\ a, b \in \mathbb{Z}$.
4. Examine if $(M_2(\mathbb{R}), \times)$, the set of all 2×2 matrices with matrix multiplication as binary composition form a group, or not.
5. Let S be a non-empty set. Examine if $(P(S), \cup)$ is a group or not.
6. Show that a group $(G, *)$ is abelian if each element of G is its own inverse.
7. If in $(G, *)$, $(a * b)^2 = a^2 * b^2$, then show that the group is abelian.
8. In a group $(G, *)$, $a * b * c = e$, where e is the identity; show that $b * c * a = e$.
9. Let $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} / a, b \in \mathbb{R},\ ab \neq 0 \right\}$; examine if S is a group under matrix multiplication.
10. Find all elements of order 5 in $(\mathbb{Z}_{20}, +)$.

Hints & Solutions:

1. Commutativity: $a * b = a + b - ab = b + a - ba = b * a$
   Associativity: $(a * b) * c = (a + b - ab) * c = a + b - ab + c - (a + b - ab)c$
   $= a + b + c - ab - bc - ca + abc = a * (b * c)$
   Existence of Identity: $a * e = a \Rightarrow a + e - ae = a \Rightarrow e = 0$
   Existence of inverse: $a * b = e \Rightarrow a + b - ab = 0 \Rightarrow b = \frac{a}{a-1} \notin \mathbb{Z}$; hence inverse does not exist.
2. Clearly $S \neq \phi$ as $1 \in S$. Let $z_1, z_2 \in S \Rightarrow z_1^n = z_2^n = 1$; then $(z_1 z_2)^n = 1 \Rightarrow z_1 z_2 \in S$ [closure]
   Associativity is true as it is true $\forall z \in \mathbb{C}$
   again, $1 \in S$ and $z \,.\, 1 = 1 . z = z, \forall z \in S$ [Existence of identity]
   and finally, if $z \in S$, then $\frac{1}{z^n} = \frac{1}{1} = 1 \Rightarrow \frac{1}{z} \in S$ and $z . \frac{1}{z} = 1 \Rightarrow \frac{1}{z}$ is the inverse of $z \in S$ [Existence of inverse]
   Commutativity is true in $\mathbb{C} \Rightarrow S$ is an abelian group.
3. Yes, it is also abelian; associativity, commutativity and closure are obvious [do yourself]
   identity is $-1 \in \mathbb{Z}$ and inverse of $a \in \mathbb{Z}$ is $-a - 2 \in \mathbb{Z}$.
4. No, it is not. The inverse of a singular matrix [i.e. a matrix A s.t. $|A| = 0$] does not exist.
5. No, it is not. Let $A \in P(S)$; then $\nexists B \in S$, such that $A \cup B = \phi$; i.e. existence of inverse property fails to hold for any $A \in P(S)$.
   Note: Similarly, $(\boldsymbol{P(S)}, \cap)$ ***is also not a group as in this case there is no identity element.***

6. Let $a, b \in G \Rightarrow a = a^{-1}, b = b^{-1}$; also $a * b = (a * b)^{-1} = b^{-1} * a^{-1} = b * a$ [i.e. abelian].

7. Given, $(a * b)^2 = a^2 * b^2 \Rightarrow a * b * a * b = a * a * b * b \Rightarrow a * b = b * a$ [by Right & Left cancellation]. Hence the result.

8. Given, $a * b * c = e \Rightarrow b * c = a^{-1} \Rightarrow b * c * a = a^{-1} * a = e$[proved].

9. S is non-empty, as $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$
   Let $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in S$ & $B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \in S$; then $AB = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} \in S$ as $ac.bd \neq 0$ [closure]
   Associativity is true for all matrices.
   $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$ is the identity element.
   Let, $B = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ be the inverse of $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \Rightarrow \begin{pmatrix} ax & ay \\ bz & bt \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow x = \frac{1}{a}, y = 0, z = 0, t = \frac{1}{b}$
   Thus, $\begin{pmatrix} 1/a & 0 \\ 0 & 1/b \end{pmatrix}$ is the inverse of A and $\begin{pmatrix} 1/a & 0 \\ 0 & 1/b \end{pmatrix} \in S$ as $\frac{1}{a}.\frac{1}{b} = \frac{1}{ab} \neq 0 \because ab \neq 0$
   Hence the inverse of every matrix of S is in S.
   Hence S is a group. [Examine if it is abelian or not?]

10. $(\mathbb{Z}_{20}, +)$ is an additive group and $o(\bar{1}) = 20$ [$\because 20.1 = 20\ (modulo\ 20) = 0$]
    let, $\bar{m}$ has order 5.
    then, we have the result, $o(a^m) = \frac{n}{\gcd(m,n)}$
    for an additive group this can be written as $o(m.a) = \frac{n}{\gcd(m,n)}$ …(1)
    putting, $a = 1$, in (1) we get, $o(m) = \frac{20}{\gcd(m,20)}$ [$\because o(1) = 20$]
    by the given question, $o(m) = 5 \Rightarrow \frac{20}{\gcd(m,20)} = 5 \Rightarrow \gcd(m, 20) = 4$, giving $m = 4,8,12,16$
    Hence the required elements of Z_{20} which have the order 5 are $\bar{4}, \bar{8}, 1\bar{2}, 1\bar{6}$.

Assignments on Chapter 1:

1. Let $(G,\circ)$ be a group and $c \in G$. A binary composition $*$ is defined on G as $a * b = a \circ c \circ b,\ \ \forall a, b \in G$. Show that $(G,*)$ is a group with c^{-1} as its identity element.

2. Show that a group $(G,*)$ is abelian if and only if $(a * b)^{-1} = a^{-1} * b^{-1}$.

3. Examine if $(D,*)$ form an abelian group, where D is the set of all odd integers and $a * b = a + b - 1,\ \forall a, b \in D$.

4. Let $S = \{x \in \mathbb{Q} : 0 < x \leq 1\}$, examine if $(S, .)$ is a group.

5. Show that a group with three elements is necessarily abelian.