Chapter 3
Elementary Group Theory

Exercise 3.1

1. a. No, the operation $*$ on the set of positive odd numbers 0^+ defined by $x * y = x+y$ is not a binary operation because for all $x, y \in 0^+$, $x * y = x + y \notin 0^+$.
e.g. $1, 3 \in 0^+$ but $1*3 = 1 + 3 = 4 \notin 0^+$.

b. Yes, since $\forall$ $x, y \in R$, $x + y = 2^{xy} \in R$

c. Yes, Here Z = {..., –3, –2, –1, 0, 1, 2, 3, ...}
$\forall$ $x, y \in Z$, $2x – y$ is also an integer and uniquely belongs to Z. So, it is a binary operation.

d. No, let $2, 3 \in N$ then $2*3 = 2+3 – 2.3$
$= 5 – 6$
$= –1 \notin N$
Therefore $*$ defined by $x * y = x + y – xy$ on the set of natural number is not a binary.

e. Yes, $\forall$ $A, B \in M$ = {set of 2×2 matrix}
$A*B = AB$ is also a 2×2 matrix and uniquery belongs to M. So, it is a binary.

3. Let S = {–1, 0, 1}
For any $a, b \in S$ $\quad a*b = a.b \in S$
$\therefore$ multiplication operation on S = {–1, 0, 1} is a binary operation.

4. Given S = {–1, 0, 1}
Operation $*$ defined by $a*b = a\times b$
a. $\forall$ $a, b \in S$, $\quad a*b = a.b = b.a = b*a$
$\therefore$ $*$ is commutative on S.

b. $\forall$ $a, b, c \in S$
$(a*b) * c = (a\times b) * c$
$= a\times b\times c$
$= a\times(b*c)$
$= a*(b*c)$
$\therefore$ '$*$' is an associative on S.

5. Let e be an identify element of $a \in Z$ then
$a*e = a$ and $e*a = a$
$2a + e = a$ $\quad 2e + a = a$
$e = –a \in z$ $\quad e = 0 \in z$
identify is not uniquely.
Let a' be inverse of $a \in z$ then $a * a' = e$
$2a + a' = –a$
$a^1 = –3a \in z$

6. Let $a, b, c \in Q$ be any elements.
Then, $(a * b) * c = (a + b + ab) * c$
$= a + b + ab + c + (a + b + ab) c$
$= a + b + ab + c + ac + bc + abc$
$= a + b + c + bc + ca + ab + abc$
$= a + (b + c + bc) + a(c + b + bc)$
$= (b + c + bc) + a + (b + c + bc) a$
$= a + (b + c + bc) + (b + c + bc) a$
$= a * (b + c + bc)$
$= a * (b*c)$
$\therefore$ '$*$' is an associative.

7. $\forall$ a, b $\in$ z
   a$*$b = 3a + 2b is also an integers and uniquely belongs to z. So, $*$ is a binary operation.
   But a$*$b = 3a + 2b $\neq$ 3b + 2a = b$*$a
   $\therefore$ a$*$b $\neq$ b$*$a
   $\therefore$ '$*$' is not a commutative.
8. Given, P = power set of a non–empty set X.
a. Let A, B $\in$ P with A$*$B = A$\cup$B
   Here, A$\cup$B must belong to set P. So, union operation on P is a binary.
b. Let A, B $\in$ P with A$*$B = A–B
   Here, A–B or B–A must belong to the power set P.
   $\therefore$ difference operation is a binary.
c. $\forall$ A, B $\in$ P A$\cap$B $\in$ P. So, intersection is a binary.
9. Given, set S = {1, ω, ω^2} where ω is the cube root of unity operation; multiplication.
   $1 \times \omega = \omega \in S$
   $\omega \times \omega^2 = \omega^3 = 1 \in S$
   $1 \times 1 = 1 \in S$
   $\omega^2 \times \omega^2 = \omega^4 = \omega^3.\ \omega = 1.\ \omega = \omega \in S$
   So, $\forall$ a, b $\in$ S   a $*$b = a, b $\in$ S
   $\therefore$ multiplication operation is binary on S.
a. Commutative
   $1 \times \omega = \omega \times 1$
   $\omega^2 \times \omega = \omega^3 = \omega \times \omega^2$
   $\therefore$ $\forall$ a, b $\in$ S   a$*$b = ab = ba = b$*$a
   $\therefore$ multiplication is commutative on S.
b. Associative
   $1 \times (\omega \times \omega^2) = 1\times\omega^3$
   $= 1\times\omega\times\omega^2$
   $= (1 \times \omega) \times \omega^2$
   $\therefore$ $\forall$ a, b, c $\in$ s. (a$*$b)$*$c = (ab) $*$ c
   = abc
   = a(bc)
   = a(b$*$c)
   = a$*$(b$*$c)
   $\therefore$ multiplication operation is association.

Exercise 3.2

1. If x, y $\in$ z and n is positive integer
   Then, x is said to be the congruent to y with modulo n if x–y is exactly divisible by n.
   It can be expressed as x $\equiv$ y modulo n.
   e.g. 7 $\equiv$ 1 modulo 3 $\Rightarrow$ 7 – 1 is divisible by 3
   i.e. when 7 is divided by 3 the remainder is 1.
   Similarly, 9 $\equiv$ 1 modulo 4 $\Rightarrow$ 9 – 1 is divisible by 4 i.e. when 9 is divided by 4 leaves remainder 1.
   a $\equiv$ b modulo n $\Rightarrow$ a – b is divisible by n.
   i.e. when a is divided by n, remainder is b.
2. **Addition Modulo 'n'**
   Let x, y $\in$ z and n be a positive integer. The addition modulo 'n' is written as ($+_n$), defined as x $+_n$y = r ($0 \leq r < n$) where r is remainder when x + y is divided by n.
   e.g.
   4 $+_2$3 = 1 i.e. when 4+3 = 7 is divided by 2, leaves remainder 1.
   12 $+_3$4 = 1 i.e. when 12+4 = 16 is divided by 3, remainder 1.
   18 $+_4$4 = 2 i.e. when 18+4 = 22 is divided by 4 remainder 2.

Multiplication Modulo 'n'

Let x, y $\in$ z and n is a positive integer. Then multiplication modulo n is denoted by (x_n), is defined by

$x \times_n y = r$, $(0 \le r < n)$ where r is remainder when $x \times y$ is divided by n.

e.g. $3 x_2\, 2 = 0$ i.e. when $3 \times 2 = 6$ is divided by 2, remainder is 0.

$7 \times_3 5 = 2$ when $7 \times 5 = 35$ is divided by 3, reminder is 2.

3.

x	1	–1	i	–i
1	1	–1	i	–i
–1	–1	1	–i	i
i	i	–i	–1	1
–i	–i	i	1	–1

$(i^2 = -1)$

Since, it is closed, the operation is a binary operation.

4. Given $z_3 = \{0, 1, 2\}$

We need to prepare a Caleys table for multiplication modulo 3.

x_3	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Since, it is closed, the multiplication modulo 3 on the set z = {0, 1, 2,} is a binary.

5. An operation '$*$' is said to be a binary on a set S if $\forall$ a, b $\in$ S then $a * b \in S$. In other words, an operation $*$ is said to be binary if it is closed.

x	**0**	**1**
0	0	0
1	0	1

Here, $0 \times 0 = 0$

$0 \times 1 = 0$

$1 \times 0 = 0$

$1 \times 1 = 1$

i.e. $\forall$ a, b $\in$ S $\qquad a \times b \in S$

'x' is a binary operation on S.

6. $\forall$ x, y $\in$ Z

$x * y = x + y - 2$ also belongs to Z

i.e. $\forall x, y \in Z \Rightarrow x * y = x + y - 2 \in Z$

$\therefore$ '$*$' is closed.

Since it is closed, it is a binary.

$x * y = x + y - 2$

$= y + x - 2$

$= y * x$

$\therefore$ $\forall$ x, y $\in$ Z, $x*y = y*x$ is proved.

'$*$' is commutative.

Finally, let x, y, z $\in$ Z then

$x*(y*z) = x * (y + z - 2)$

$= x + y + z - 2 - 2$

$= x + y + z - 4$

$= x + y - 2 + z - 2$

$= (x*y) + z - 2$

$= (x*y) * z$

$\therefore$ This proves that '$*$' also associative.

7. Given, M = {set of all 3×2 matrices}

Operation: addition

$\forall$ A, B $\in$ M, A + B $\in$ M

because addition of two matrices of order 3×2 is also 3×2 matrix.

Addition operation on set M is closed. It means it is a binary.

Let A, B, C $\in$ M then,

(A + B) + C = A + (B + C)

$\therefore$ Associative

Let I be an identify element of A$\in$M. Then,

A + I = A

I = A = A

I = null matrix

$\therefore \quad I = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$

$\therefore \quad A^1 = -A \in M$

8. $2x + 1 = 6$ in Z_7

or, $2\times_7 x +_7 1 = 6$

or, $2\times_7 x +_7 1 +_7 6 = 6 +_7 6$

or, $2\times_7 x = 5$

or, $7\times_7 (2\times_7 x) = 4\times_7 5$

or, $(4\times_7 2) \times_7 x = 4\times_7 5$ (By associative law)

or, $1\times_7 x = 6$

or, $x = 6$

Exercise 3.3

1.a. Set N (Natural number) Operation: Multiplication 'x'

(N, x) is not a group because there doesn't exist inverse element.

b. (Z, +) is a group

c. (Q – {0}, X) is a group

d. Yes

e.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

It is closed, so binary

$(1*2)$ r $* 4 = 3*4 = 2$

$1*(2*4) = 1*1 = 2$

$\forall$ a, b, c $\in$ S, $(a*b) \times c = a*(b*c$

$\therefore$ associative holds

0$\in$s is an identity element $\forall$ a$\in$S.

$\forall$ x $\in$ S, $\exists$ inverse element y$\in$ S such that

$x +_5 y = 0$

Here, Inverse of 0 is 0

Inverse of 1 is 4

Inverse of 2 is 3

Inverse of 3 is 2

Inverse 4 is 1

$\therefore$ (S, $+_5$) is a group

f. S = {1, –1, i, –i}

$(S, \times)$ is a group

g. yes

h. yes

i. no, identity does not exist.

j. yes

k. yes

2.

$\times_3$	**0**	**1**	**2**
0	0	0	0
1	0	1	2
2	0	2	1

Closure Property: $\forall$ a, b $\in$ s $a x_3 b \in s$

$0x_2\ 0 = 9$ $0x_3\ 1 = 1$ $0x_3\ 2 = 0$

$1x_3\ 0 = 0$ $1x_3\ 1 = 1$ $1x_3\ -2 = -2$

$2x_3\ 0 = 0$ $2x_3\ 1 = 2$ $2x_3\ 2 = 1$

Associative Property

$0x_3\ (1\times_3 2) = 0\times_3 2 = 0$

$(0x_3 1)\times_3 2 = (0\times_3 2) = 0$

$(2x_3\ 1)\times_3 2) = 2\times_3 2 = 1$

$\therefore$ $\forall$ a, b, c $\in$ S, $(a*b) * c = a*(b*c)$

Existence of identity

$\forall a \in S, \exists e \in S$ s.t. $a \times_3 e = a$

Existence of inverse:

$\forall a \in S, \exists a' \in S$ s.t. $a*a' = e$

$a * a^1 = e$

$\therefore$ $(S, \times_3)$ is a group.

3. Given $(S, \times)$ where s = {1, –1, 1, –1}

For closure

For any a, b $\in$ s $a*b = ab \in s$

e.g. $1\times1 = 1\in s$

$-1\times-1 = 1 \in s$

$-1\times i = -i\in s$

$i\times i = i^2 = -1\in s$

$-i\times i = -i^2 = 1\in s$

So, for any two elements of S, the new element after operating also must belong to sets. So it is closed.

For associatively,

$(1\times1 \times - i = 1\times-i = -i$

$1\times(1 \times -i) = 1 \times - i = -1$

$\therefore (1 \times 1) \times -i = 1\times (1 \times - i)$

Similarly others follows

That is $\forall$ a, b, c $\in$ s $\Rightarrow (a\times b) \times c = a\times(b\times c)$

$\therefore$ It is associative.

For existence of identify:

Let $1\in s$ then $1\times1 = 1$

Let $-i\in s$ then $-i\times1 = -i$

Let $i\in s$ then $i\times1 = i$

Let $-1\in s$ then $-1\times1 = -1$

$\therefore$ -1 is an identify element of any element $\in s$.

For existence of inverse:

For $1 \in s$	$1 \times 1 = 1$	$\therefore$ 1 is inverse of 1
For $-1 \in s$	$-1 \times -1 = 12$	$\therefore$ -1 is inverse of -1
For $i \in s$	$i \times -i = 1$	$\therefore$ $-i$ is inverse of i
For $-i \in s$	$-i \times i = 1$	$\therefore$ i is inverse of $-i$

Therefore, $\forall$ a $\in$ s $\exists$ a'$\in$ s.t. a$\times$a' = e

Hence, the algebraic structure (S, $\times$) satisfies all the properties (i.e. closure, associativity, existence of identity and existence of inverse)

$\therefore$ (S, $\times$) is a group

4.a. Algebraic Structure:

An structure of the form (G, $*$) is known as an algebraic structure. Where G is a non-empty set and '$*$' is a binary operation.

e.g. (G, +), (G, x), (Z, –) (Q, +) etc are some examples of an algebraic structure.

b. Semi-group:

An algebraic structure (G, $*$) is said to be a semi–group. It satisfies the associative property.

e.g. (z^+, +) is a semi-group but (z, +) is not.

c. Group: An algebraic structure (G, $*$) is said to be a group if it satisfies the following for properties.

- Closure
- Associative
- Existence of identity
- Existence of inverse

d. Monoid: An algebraic structure (G, $*$) is said to be a monoid if it satisfies associativity and existence of an identity. e.g. (Z, $\times$)

e. Abelian group: A group (G, $*$) is said to be an abelian of it satisfies the commutative property.

f. Trivial group: A group (G, $*$) is said to be a trivial group if G consists of a single element.

5. Let M = $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R \text{ and } ad - bc \neq 0\right\}$ be the set of 2$\times$2 real non-singular matrices.

i. $\forall$ A, B $\in$ M, AB is again 2$\times$2 real non-singular matrix. So, M is closed.

ii. $\forall$ A, B, C $\in$ M, A(BC) = (AB) C by matrix algebra. So M is associative under multiplication.

iii. $\forall$ A$\in$M, we get I = $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ even that AI = IA = A. So the identify matrix I exists.

iv. $\forall$ A$\in$M, we get A^{-1} (Since A is non–singular) set. $AA^{-1} - A^{-1}A = I$ where $A^{-1} = \frac{\text{Adj.(A)}}{|A|}$, is known as inverse of A. Hence M is a group.

6. Show that (Z, +) is a group.

i. Closure property: $\forall$ a, b $\in$ z, a + b $\in$ Z

$\therefore$ z is closed

ii. Associative: $\forall$ a, b, c $\in$ Z

(a + b) + c = a + (b + c)

$\therefore$ z is associative

iii. Existence of identify: $\forall$a $\in$ z, the must exist 0 $\in$ z s.t. a+0 = a

$\therefore$ 0 $\in$ Z is an identify element.

iv. Existence of inverse: $\forall$a$\in$Z there must –a$\in$Z s.t. a + (–a) = 0

$\therefore$ –a is inverse of a

Hence (Z, +) is a group.

7.

×	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

From the above table, s is closed
$(1\times\omega) \times \omega^2 = \omega\times\omega^2 = \omega^3 = 1$
$1\times(\omega\times\omega^2) = 1\times\omega^3 = 1\times1 = 1$
$\therefore$ $(1\times\omega) \times \omega^2 = 1\times(\omega\times\omega^2)$
Again, $\omega\times(\omega^2 \times \omega^2) = \omega \times \omega^4 = \omega\times\omega = \omega^2$
$(\omega\times\omega^2) \times \omega^2 = \omega^3\times\omega^2 = 1\times\omega^2 = \omega^2$
$\therefore$ $\omega\times(\omega^2 \times \omega^2) = (\omega \times \omega^2) \times \omega^2$
That is
$\forall$ a, b, c $\in$ S
$(a\times b) \times c = a\times(b\times c)$
$\therefore$ S is associative.
From the table, 1 is an identity element of any element of S.
i.e. $1\times1 = 1$
$\omega\times1 = \omega$
$\omega^2\times1 = \omega^2$
$\therefore$ identity element 1 exist.
Since, $1\times1 = 1$
$\omega\times\omega^2 = 1$
$\omega^2\times\omega = 1$
$\therefore$ Inverse of 1 is 1
Inverse of w is ω^2
Inverse of w^2 is ω
So, there is an existence of an inverse element.
Finally, $1\times\omega = \omega\times1 = \omega$
$\forall$ a, b $\in$ s $\quad$ $a\times b = b \times a$
Comutative property satisifies.

Hence, (S, ×) is an abelian group.

8. The set: Z
Operation '∗' defined by $a*b = a+b+2ab$
a. Since, a, b $\in$ Z
$a + b + 2ab$ is also belongs to Z.
$\therefore$ z is closed
b. $\forall$ a, b, c $\in$ Z
$a * (b * c) = a * (b + c + 2bc)$
$= a + b + c + 2bc + 2a(b + c + 2bc)$
$= a + b + c + 2bc + 2ab + 2ca + 4abc$
$= a + b + c + 2ab + 2bc + 2ca + 4abc$
Again, $(a*b) * c = (a + b + 2ab) * c$
$= a + bb + 2ab + c + 2(a + b + 2ab) c$
$= a + b + 2ab + c + 2ca + 2bc + 4abc$
$= a + b + c + 2ab + 2bc + 2ca + 4abc$
$\therefore$ $a*(b*c) = (a*b) * c$
$\therefore$ z is associative
c. Since $a*0 = a + 0 + 2a0 = a$
$\forall$ a$\in$z, the identity element 0$\in$ Z exists.
d. Let d be inverse of a such that $a*d = 0$ (identify)

$a + d + 2ad = 0$

$d + 2ad = -a$

$d(1 + 2a) = -a$

$d = \frac{-a}{1 + 2a} \notin Z$

Even through

$a \neq -\frac{1}{2}$, if a = 1 then

$d = \frac{1}{3} \notin Z$

∴ inverse element may not exist. Therefore, (Z, ∗) is not a group.

9. For definition of group look at 4(c)

From the given Calyes table,

S is closed.

$\forall$ a, b, c $\in$ S

$a * (b * c) = a * a = a$

$(a * b) * c = b * c = a$

∴ $a * (b * c) = (a * b) * c$

∴ S is associative

From the table, $a * a = a$

$b * a = b$

$c * a = c$

∴ a is identity element.

From the table,

$a * a = a$

$b * c = a$

$c * b = a$

∴ inverse of a is itself a

inverse of b is itself c

Therefore, inverse elements exists.

Since, S satisfies closure property, associative property, existence of identity and existence of inverse, (S, ∗) is a group.

10.

a. Set: Z

Operation: –

Now, we check (Z, –) is a group or not.

$\forall$ a, b $\in$ Z, $a * b = a - b \in Z$

∴ z is closed.

$\forall$ a, b, c $\in$ Z, $(a - b) - c \neq a - (b - c)$

e.g. let a = –1, b = –3 and c = 5

Then, $(a - b) - c = (-1 + 3) - 5 = 2 - 5 = -3$

$a - (b - c) = -1 - (-3 - 5) = -1 + 8 = 7$

∴ $(a - b) - c \neq a - (b - c)$

∴ Z is not associative

Since associative property is not satisfied.

The set of integers with subtraction operation is not a group.

b. (z, x) $\Rightarrow$ Group (check)

$\forall$ a, b $\in$ z, $a \times b \in z$ so, closure is satisfied.

$\forall$ a, b, c $\in$ z, $(a \times b) \times c = a \times (b \times c)$

∴ z is associative.

Let $a \in z$ then $a \times 1 = a$

∴ so there must exist $1 \in z$ s.t. $a \times 1 = a$ so identify element 1 exists.

If b is inverse of $a \in z$ then $a \times b = 1$

$b = \frac{1}{a} \notin Z$

Since, if a = 2 then $b = \frac{1}{2} \notin Z$

Therefore, there is no existence of inverse element.

$\therefore$ $(Z, \times)$ is not a group.

11. Let $V = \{(a_1, a_2, a_3) : a_1\, a_2\, a_3 \in R\}$ be a set of 3 dimensional vectors.
Now, we have to show that (v, +) is a group.
$\forall v_1\, v_2 \in v \qquad v_1 + v_2 \in V$
Since addition of two 3–dimention vectors is also 3–dimentional
$\therefore$ v is closed.
$\forall\, v_1, v_2, v_3 \in V$, then it is obvious that $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$
$\therefore$ associative property also holds.
$\forall\, v_1 \in v$ of 3 dimensional null vector
(0, 0, 0) s.t. $v_1 + (0, 0, 0) = v_1$
$\therefore$ Identity element (0, 0, 0) exists.
$\forall v_1 \in V, \exists -v_1 \in V$ s.t. $v_1 + (-v_1) = (0, 0, 0)$
$\therefore$ inverse element also exists.
Hence, (V, +) is a group.

12. Solution:

i. Closure property:

$\forall\, a, b \in Q^+, \qquad a*b = \frac{ab}{4} \in Q^+$

$\therefore$ Q^+ is closed.

ii. Associative property:

$\forall\, a, b, c \in Q^+$ then $(a*b) * c = \left(\frac{ab}{4}\right) * c = \frac{abc}{\frac{4}{4}} = \frac{abc}{16}$

$a*(b*c) = a*\left(\frac{bc}{4}\right) = \frac{abc}{\frac{4}{4}} = \frac{abc}{16}$

$\therefore$ $(a*b) * c = (b * c)$

$\therefore$ associative property holds

iii. Existence of identity

Let e be an identify of $a \in Q^+$

Then, $a*e = a$

$\frac{ae}{4} = a$

$ae = 4a$

$ae - 4a = 0$

$a(e - 4) = 0$

$e = 4 \in Q^+$ since $a \neq 0$

Identify element exists.

iv. Existence of inverse:

let b be an inverse of $a \in Q^+$

such that, $a * b = e$

$\frac{ab}{4} = 4$

$ab = 16$

$b = \frac{16}{a} \in Q^+$

$\therefore$ inverse element $b \in Q^+$ exists.

Hence, $(Q^+, *)$ is a group.

Where $*$ is defined by $a*b = \frac{ab}{4}$

Further, $\forall$ a, b $\in Q^+$

$a*b = \frac{ab}{4} = \frac{ba}{4} = b*a$

$\therefore$ commutative property is also satisfied. Therefore, $(Q^+, *)$ is an abelian group.

13. Given,

P = {non empty subsets of X}

Is (P, U) is a group?

$\forall P_1 P_2 \in P$ then $P_1*P_2 = P_1UP_2 \in P$

$\therefore$ P is closed.

$\forall P_1, P_2, P_3 \in P, (P_1UP_2) U P_3 = P_1U(P_2UP_3)$

$\therefore$ P is associative.

$\forall P_1 \in P$ then $P_1U\phi = P_1$ but $\phi \notin P$.

$\therefore$ identity element does not exist.

$\therefore$ this is not a group.