Chapter 6:
THE GROUP CONCEPT

Mphako-Banda

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG
SCHOOL OF MATHEMATICS

LEARNING OUTCOMES FOR THE LECTURE

By the end of this lecture, students will be able to:

- define a group
- define a unit, unity
- show that the sets Z,R and the set of complex numbers are groups under addition
- show that the set R excluding zero and the set of complex numbers excluding zero are groups under multiplication
-

Definition (6.1.1)

A set G with an associative binary operation $\star$, written $\langle G, \star\rangle$ is called a group if

(i) *G is closed under $\star$*

for any a, b in G we have that the product of a and b is in G

(ii) *$\star$ is associative on G*

for any a,b,c in G (ab)c=(ab)c

(iii) *there exists a unique element e (sometimes 0 or1) called identity or unity with $e \star g = g \star e = g$ for each $g \in G$ and*

(iv) *for each $g \in G$ there is an inverse $g^{-1} \in G$ such that $g \star g^{-1} = g^{-1} \star g = e$.*

Definition (6.1.2) (abelian group)

If $g \star h = h \star g$ for each $g, h \in G$, then G is an abelian group.

NOTE: The words or concepts of "‘binary operation,"’ "‘unity or identity"’, "‘inverse"’ and "‘closed"’ need to be fully explored.

Definition (6.1.3 Binary operation $\star$ acting on S.)

[Recall from Chapter 5] A binary operation $\star$ acting on S is a well defined mapping $\star : S \times S \to S$ that assigns each pair of elements $(a, b) \in S \times S$ with a unique element $a \star b \in S$. i.e $\star(a, b) = a \star b \in S$.

Definition (6.2.1 (1)) (closure of a set S under a given binary operation)

Let $\star : S \times S \to S$ be well defined binary mapping or operation Since $\star(a, b) = a \star b \in S \quad \forall a, b \in S$, we say that S is closed under $\star$.

Definition (6.2.1 (2)) (well defined property on SxS)

Since for each $(a, b) \in S \times S$ *there is a unique* $\star(a, b) = a \star b \in S$ *we have* $(a_1, b_1) = (a_2, b_2) \Rightarrow \star(a_1, b_1) = \star(a_2, b_2)$ *or* $a_1 \star b_1 = a_2 \star b_2$. *We call this the well defined property of* $\star$ *on* S.

Definition (6.2.1 (3)) (commutativity under a given binary operation)

If $a \star b = b \star a \quad \forall a, b \in S$, *then we say a and b are commutative under* $\star$. *If* S *is an abelian group then* $a \star b = b \star a \quad \forall a, b \in S$.

***All** elements* $\in S$ *commute with each other.*

Definition (6.2.1 (4)) (associativity of a given binary operation)

$\star$ *is an associative map if*

$a \star (b \star c) = (a \star b) \star c \quad \forall a, b, c \in S.$

Definition (6.2.1 (5)) (Identity element in a group G is unique)

The unity or identity element in G is unique and leaves each element of S unchanged under $\star$

i.e $\star(e, a) = \star(a, e) = a \quad \forall a \in S$ *or*

$e \star a = a \star e = a \quad \forall a \in S.$

Definition (6.2.1 (6)) (a unit or invertible element in S is an element that has an inverse in S)

An element $a \in S$ *is called a unit or invertible in S if we can find* $b \in S$ *such that* $a \star b = b \star a = e.$

NOTE: We will show if b exists then b is unique and can be written as a^{-1}, the inverse of a.

NOTE: The inverse of a always commutes with a. These invertible elements are referred to as Units.

NOTE: unity e is unique, some elements in S may be units. Unity is a unit,
BUT not all units are unity. Unity is unique.

Example (6.2.2 (1))

$\star$ *ordinary addition on* $\mathbb{Z}$, $\mathbb{R}$, *or* $\mathbb{C}$, *then* $\langle \mathbb{Z}, \star \rangle$, $\langle \mathbb{R}, \star \rangle$, $\langle \mathbb{C}, \star \rangle$ *are groups.*

- (i) $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, *are closed under addition.*
- (ii) *addition in* $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, *is associative.*
- (iii) *identity:* $e = 0$ *in* $\mathbb{Z}$, $\mathbb{R}$, *or* $\mathbb{C}$, *since*

$$x + 0 = 0 + x = x \quad \forall x \in \mathbb{Z}, \mathbb{R}, \mathbb{C}.$$

- (iv) *For any* $x \in \mathbb{Z}, \mathbb{R}, \mathbb{C}$, $-x$ *is the inverse of* x *since* $x + (-x) = -x + x = 0$.

the 4 properties to check in order to show that a given set with a given binary operation is a group

- (v) *Indeed* $\mathbb{Z}, \mathbb{R}, \mathbb{C}$ *are abelian groups under addition* $\forall x, y \in \mathbb{Z}, \mathbb{R}, \mathbb{C}$ *since* $x + y = y + x$. *Thus* $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{C}, + \rangle$ *are abelian groups*.

Example (6.2.2 (2))

⋆ *ordinary multiplication on* $\mathbb{Z}, \mathbb{R}, \mathbb{C}$

(i) $\mathbb{Z}, \mathbb{R}, \mathbb{C}$ *are closed under multiplication.*

(ii) *Multiplication is associative on* $\mathbb{Z}, \mathbb{R}, \mathbb{C}$.

(iii) *Multiplicative identity or unity is 1, since* $x \bullet 1 = 1 \bullet x = x \quad \forall x \in \mathbb{Z}, \mathbb{R}, \mathbb{C}$.

(iv) $\forall x \in \mathbb{R}\backslash\{0\}, \mathbb{C}\backslash\{0\}, \quad x^{-1} = \frac{1}{x}$, *since* $\frac{1}{x} \bullet x = x \bullet \frac{1}{x} = 1$.

Exercise: (i) Show that the set of rational numbers is a group under addition
(ii) Show that the set of rational numbers excluding zero is a group under multiplication

Please do this exercise

Note:

- 1 and -1 are the only invertible elements in $\mathbb{Z}$, since $1.1 = 1$ and $(-1).(-1) = 1$. Thus $1^{-1} = 1$ and $(-1)^{-1} = (-1)$.
- Let $m \in \mathbb{Z}, \quad m \neq 0, 1, -1$. If m^{-1} exists say n, then $mn = 1 \Rightarrow n = \frac{1}{m} \notin \mathbb{Z}$.
- Thus $m \in \mathbb{Z}, \quad m \neq 1, -1$ is not invertible, hence $\langle \mathbb{Z}, . \rangle$ is not a group. the set of integers under multiplication is not a group
- $\langle \mathbb{R}, \bullet \rangle$, $\langle \mathbb{C}, \bullet \rangle$ are not groups since 0 does not have an inverse.
- Hence $\langle \mathbb{R} \backslash \{0\}, \bullet \rangle, \langle \mathbb{C} \backslash \{0\}, \bullet \rangle$ are groups under multiplication.
- $\langle \mathbb{Z} \backslash \{0\}, \bullet \rangle$ not a group. Not all elements $m \in \mathbb{Z}$ are units (invertible).