

Chapter 6: THE GROUP CONCEPT

Mphako-Banda



LEARNING OUTCOMES FOR THE LECTURE

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

- ♣ prove that a given set G is a group under a given binary operation
- ♣ prove uniqueness of an inverse for each element of g of G
- ♣ prove the group properties for inverses and inverses of products in a group G
- ♣
- ♣

In the following example we show that the power set $\mathcal{P}(U)$ is a group under the binary operation symmetric difference

Example (6.2.2 (3))

Let U be a set, $\mathcal{P}(U) = \{X | X \subseteq U\}$ under symmetric difference Δ

 recall power set: eg. $U = \{1, 2, 3\}$, $\mathcal{P}(U) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

$\langle \mathcal{P}(U), \Delta \rangle$ $X, Y \subseteq U$ all possible subsets of U

$$X \Delta Y = (X - Y) \cup (Y - X) = (X \cup Y) - (X \cap Y)$$

(i) $X \Delta \emptyset = X$, \emptyset is identity.

(ii) $X \Delta X = \emptyset$ that is X its own inverse. $X \cap X - X \cup X = \emptyset$

(iii) $\mathcal{P}(U)$ closed under Δ i.e.

$$X \Delta Y = (X - Y) \cup (Y - X) \subseteq U \therefore X \Delta Y \in \mathcal{P}(U).$$

(iv) $\mathcal{P}(U)$ abelian under Δ ,

$$X \Delta Y = (X \cup Y) - (X \cap Y) = (Y \cup X) - (Y \cap X) = Y \Delta X.$$

(v) $\mathcal{P}(U)$ associative under Δ .

Students to try show $X \Delta (Y \Delta Z) = T$ and where $T \in \mathcal{P}(U)$

$$(X \Delta Y) \Delta Z = T. \quad \text{Thus, we conclude that } \mathcal{P}(U) \text{ is an abelian group under } \Delta$$

in this example we consider the power set under the binary operation of intersection of sets

Example (6.2.2 (4))

$\langle \mathcal{P}(U), \cap \rangle$

- (i) $\mathcal{P}(U)$ closed under \cap for any $X, Y \in \mathcal{P}(U)$, $X \cap Y \in \mathcal{P}(U)$
- (ii) $\mathcal{P}(U)$ associative under \cap for any $X, Y, Z \in \mathcal{P}(U)$, $(X \cap Y) \cap Z = X \cap (Y \cap Z)$
- (iii) $\mathcal{P}(U)$ commutative under \cap
- (iv) Unity or identity, $X \cap U = X$, $e = U$ unity
- (v) $X \cap Y = U$, $Y = ?$ if $\mathcal{P}(U)$ is a group then all elements in $\mathcal{P}(U)$ should have an inverse
only $U \cap U = U$ so only U has inverse, thus $\langle \mathcal{P}(U), \cap \rangle$ is not a group.

in this example, we consider the set of mappings from X to X and the binary operation is the composition of mappings

Example (6.2.2 (5))

$M = \{f : X \rightarrow X \mid f \text{ mapping}\}$ under composition of mappings, \circ .

- (i) $\langle M, \circ \rangle$ closed under \circ .
 - (ii) $\langle M, \circ \rangle$ associative under \circ .
 - (iii) unity $e = 1_X$ identity mapping.
 - (iv) not all $f : X \rightarrow X$ are bijective/ invertible. Not all f have an inverse.
- $\langle M, \circ \rangle$ not a group.

Example (6.2.2 (6))

$M_n(\mathbb{R})$, $M_n(\mathbb{C})$, $n \times n$ matrices over \mathbb{R} and \mathbb{C} respectively.

$\langle M_n(\mathbb{R}), + \rangle$, $\langle M_n(\mathbb{C}), + \rangle$

- closed, associative, commutative under $+$
- unity $e = 0$, zero $n \times n$ matrix of size n .
- $A \in M_n(\mathbb{R})$ or $A \in M_n(\mathbb{C})$, $-A$ is the inverse of A .

$\langle M_n(\mathbb{R}), + \rangle$, $\langle M_n(\mathbb{C}), + \rangle$ abelian groups.

If A, B are $n \times n$ matrices with real entries then we have $A+B$ is a $n \times n$ matrix with real entries

Matrix addition is associative and commutative

The unity under addition of $n \times n$ matrices is a $n \times n$ with all entries being zeros

The inverse of a $n \times n$ matrix A under addition is the negative of the matrix A since $A+(-A)=0$

a similar reasoning holds for $n \times n$ matrices with entries in the set of complex numbers.

In this example we consider square matrices of order n with entries in the set of real and complex numbers

Example (6.2.2 (7))

$\langle M_n(\mathbb{R}), \bullet \rangle, \langle M_n(\mathbb{C}), \bullet \rangle$

(i) *closed, associative under \bullet*

(ii) $e = I_n$

(iii) *Multiplication of matrices not commutative.*

(iv) *not all matrices are invertible.*

$\langle M_n(\mathbb{R}), \bullet \rangle, \langle M_n(\mathbb{C}), \bullet \rangle$ are *not groups*.

However $GL(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$ is a group under matrix multiplication. This is called the *general linear group*. $GL(n, \mathbb{R})$ is the set of all $n \times n$ invertible matrices with real entries

If A and B are square matrices of order n with real entries, then AB is a square matrix of order n with real entries. Multiplication of matrices is associative.

The unity e is the identity matrix of order n .

Some square matrices are not invertible, for example the matrices whose determinant is equal to zero, thus not all square matrices have an inverse.

similar reasoning as above for square matrices of order n with entries in the set of complex numbers.

In this example, we consider the set of all non zero residue classes modulo p , where p is a prime number.

Example (6.2.2 (8))

$\langle \mathbb{Z}_p^*, \bullet \rangle$ is a group p prime.

the binary operation is multiplication of residue classes modulo p

(i) $e = \bar{1}$,

(ii) $\forall a \in \mathbb{Z}_p, a \neq 0 \quad \gcd(a, p) = 1$
 $\Rightarrow \bar{a}$ has an inverse in \mathbb{Z}_p .

(iii) \mathbb{Z}_p^* is closed under multiplication.

can you check this property
 $p=3$.

(iv) multiplication is associative.

for (iii) please note that we exclude the residue class of zero modulo p

In the following section we give some fundamental properties of groups

Group Properties

iv) for each a in G there is an inverse b in G such that $a*b = b*a = e$

Proposition (6.3.1 (i))

Let G be a group with binary operation \star . If e is unity, then $e^{-1} = e$. e is self inverse

PROOF:

recall: b is the inverse of a iff $a*b=b*a=e$
now $e*e=e*e=e$ ($b=e$)

Let e be unity in G . Since $e \star a = a \star e = a \quad \forall a \in G$ we have $e \star e = e$ by definition, e is its own inverse.

Proposition (6.3.1 (ii))

Let G be a group with binary operation \star . If $a \in G$ then, the inverse is unique. We write this unique element as a^{-1} . Further $(a^{-1})^{-1} = a$.

uniqueness: assume that a has two inverses b and c and prove that indeed $b=c$. thus inverse of a is unique

PROOF: Let $a \in G$ with $b, c \in G$ and $a \star b = b \star a = e$ and $a \star c = c \star a = e$ (We assume a has 2 inverses.)

Then $c \star (a \star b) = c \star e = c$ so $(c \star a) \star b = c$ since \star is associative and e is unity in G . Thus $e \star b = c$ and since e is unity on b we have $b = c$. Thus if a has invers, it is unique and so $b = c = a^{-1}$. $(c \star a) \star b = c \star (a \star b) \Rightarrow e \star b = c \star e \Rightarrow b = c$ ← please note


Further, since we have just shown that if an inverse exist, it is unique, we have

$$(a) \star (a^{-1}) = (a^{-1}) \star (a) = e \text{ and } e = e^{-1}.$$

Thus $(a^{-1})^{-1} = a$ since a satisfies the necessary condition to be the inverse of a^{-1} .

Note: to prove that y is the inverse of x we should show that $xy=yx=e$

Proposition (6.3.1 (iii))

Let G be a group with binary operation \star . If $a, b \in G$ then so is $(a \star b)$ and $(a \star b)^{-1} = b^{-1} \star a^{-1}$.  note the reversal

PROOF: Inverses exist and are unique, so $b^{-1}, a^{-1} \in G$ we have that

$$a^{-1} \star a = a \star a^{-1} = e; \quad b^{-1} \star b = b \star b^{-1} = e \text{ and}$$

$$\begin{aligned} (b^{-1} \star a^{-1}) \star (a \star b) &= b^{-1} \star (a^{-1} \star a) \star b \\ &= b^{-1} \star e \star b = b^{-1} \star b = e \\ &= (a \star b) \star (b^{-1} \star a^{-1}) = e \end{aligned}$$

Therefore $(b^{-1} \star a^{-1}) = (a \star b)^{-1}$ as it satisfies the requirement of the inverse of $(a \star b)$.

Proposition (6.3.1 (iv))

Let G be a group with binary operation \star . If a_1, a_2, \dots, a_n are units so is $a_1 \star a_2 \star \dots \star a_n$ and

$$(a_1 \star a_2 \star \dots \star a_n)^{-1} = a_n^{-1} \star \dots \star a_2^{-1} \star a_1^{-1}.$$

PROOF: Given $a_1^{-1}, a_2^{-1}, \dots, a_n^{-1} \in G$, as above we have

$$(a_n^{-1} \star a_{n-1}^{-1} \star \dots \star a_2^{-1} \star a_1^{-1}) \star (a_1 \star a_2 \star \dots \star a_n) = e$$

$$(a_1 \star a_2 \star \dots \star a_n) \star (a_n^{-1} \star a_{n-1}^{-1} \star \dots \star a_2^{-1} \star a_1^{-1}) = e$$


$$\text{So } a_n^{-1} \star \dots \star a_2^{-1} \star a_1^{-1} = (a_1 \star a_2 \star \dots \star a_n)^{-1}.$$

Proposition (6.3.1 (v))

Let G be a group with binary operation \star . If a is a unit so is a^n for any $n \in \mathbb{Z}$ where $a^0 = e$, and $(a^n)^{-1} = (a^{-1})^n$.

PROOF: In part (iv) if $a_1 = a_2 = \dots = a_n = a$, then $a_1 \star a_2 \star \dots \star a_n = a \star a \star \dots \star a = a^n$ and $(a^n)^{-1} = a^{-1} \star a^{-1} \star \dots \star a^{-1} = (a^{-1})^n$ where a^{-1} is the inverse of a .

NOTE 6.3.2

We define $a^0 = e$ and $a^n = a \star a \star \dots \star a$ $n \in \mathbb{Z}$. 

By above $(a^n)^{-1} = (a^{-1})^n$ so a^m is defined for all $m \in \mathbb{Z}$.

All indices laws follows:

$a^m \star a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$ where $m, n \in \mathbb{Z}$.

We write $a \star b$ as ab .