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:

- (i)prove the cancellation law in a group G
- (ii)define a subgroup H of a group G.
- (iii)show that a given subset H of a group G is a group.
- (iv)prove Theorem 6.3.6
- (v)define order of an element g in G.

(vi)present small finite groups in multiplication tables.

(vii)determine unity, inverses of elements in a given multiplication table.
(viii)determine whether a given a multiplication table of a set M represent a group or not.

Proposition (6.3.3 Cancellation laws)

Let $g, h, f \in G$ then

(i) *If $gh = gf$, then $h = f$.*
PROOF: *$g, h, f \in G$ so $g^{-1} \in G$ as G is a group.*
$gh = gf \Rightarrow g^{-1}(gh) = g^{-1}(gf) \Rightarrow (g^{-1}g)h = (g^{-1}g)f \Rightarrow eh = ef \Rightarrow h = f$.

(ii) *if $hg = fg$ then $h = f$. (Proof same as above with right multiplication.)*

note that we would not cancel out g if we had gh=fg. we would cancel out if and only G is abelian hence fg=gf and gh=fg⇒gh=gf⇒h=f.

Proposition (6.3.4)

Let $g, h, f \in G$ then

for any g in G, the inverse of g is unique in G

(i) *the equation $gx = h$ has a unique solution $x = g^{-1}h$ in G.*
PROOF: $g, h \in G$ *so* $g^{-1} \in G$ *as G is a group and* $g^{-1}g = gg^{-1} = e$

multiply both sides by the inverse of g

$gx = h \Rightarrow g^{-1}(gx) = g^{-1}h \Rightarrow (g^{-1}g)x = g^{-1}h \Rightarrow ex = g^{-1}h \Rightarrow x = g^{-1}h.$

(ii) *the equation $xg = h$ has a unique solution $x = hg^{-1}$.*
(Proof is similar with Right multiplication.)

Subgroup of a group G

Definition (6.3.5)

H is a subgroup of G under $\star$ *if* $H \neq \emptyset$, $H \subseteq G$ *and* $\langle H, \star \rangle$ *is a group.*

non empty

subset

same binary operation as in G

We write $H \leq G$.

$\{e\} = H \leq G$; called trivial group.

$G \leq G$ improper subgroup.

if $H \subset G$ and $\langle H, \star \rangle$ is a group, then H is a proper subgroup of G.

{e} is the trivial subgroup of G

H is a non trivial proper subset of G that is a group under the same binary operation as on G

For H to be a subgroup of G, H has to satisfy three conditions: (i)H is non empty, (ii)H is subset of G, (iii)H is a group under the same binary operation as on G.

Below we give some examples of subgroups of a group G

Example

Let $H = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} | a, b \in \mathbb{R}, a \neq 0 \right\}$.

a different from zero so that det(A) a matrix in H is not equal to zero and hence A an invertible matrix (A has an inverse)

G is a group under multiplication of matrices, with $G = GL(2, \mathbb{R})$

(i) $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix} \in G$

matrix entries from the set os real numbers and the entries of the product matrix are real numbers (ac, ad+bc real)

since $ac, ad+bc \in \mathbb{R}$, $ac \neq 0$, since $a \neq 0$ and $c \neq 0$.

(ii) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$ is the identity. H

note that the identity matrix is of the form of matrices from H since the entries are real and

entries must be the same

entry equal to zero

(iii) $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ has an inverse since $det \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = a^2 \neq 0$.

(iv) Multiplication of matrices is associative.

$\therefore$ H is a group and $H \leq GL(n, \mathbb{R})$, the general linear group.

Example

$\langle \mathbb{R}\backslash\{0\}, \bullet\rangle \leq \langle \mathbb{C}\backslash\{0\}, \bullet\rangle$ the set of real numbers excluding zero under multiplication is a subgroup of the set complex numbers excluding zero under multiplication

EXERCISE

H subset of G

Let G be an abelian group. Consider $H = \{g \in G | g^2 = e\}$. Show that $H \leq G$.

elements g of H are all elements g in G that satisfy the condition that g^2 =e

(i) $H \subseteq G$

(ii) $H \neq \emptyset$, $\cancel{gh^{-1} \in H \quad \forall\, g, h \in H \text{ since } g = g^{-1} \text{ and } h = h^{-1}}$. (ii) Show that H is a group

Theorem (6.3.6)

Let H be a non empty subset of G. Then $H \leq G$ iff $ab^{-1} \in H \quad \forall a, b \in H$.

The above theorem(Theorem 6.3.6) enables us to prove that a subset H of a group G is a subgroup without having to check all group axioms

(i)$\Rightarrow$show that, given that H is a non-empty subset of G, for any a, b in H we have that $ab^{-1} \in H$
(ii)$\Longleftarrow$ show that if H is a non-empty subset of G with the condition that for any
a, b $\in$ H we have that $ab^{-1} \in H$ then H is a group(in red is the assumption for the reverse implic.)

PROOF

$\Rightarrow$: $H \leq G$ then $\langle H, \star \rangle$ is a group. If $a, b \in H$ then $a, b^{-1} \in H$ and so $ab^{-1} \in H$. H is closed under the binary operation

$\Leftarrow$: Assume $ab^{-1} \in H \quad \forall a, b \in H$ and H is non empty subset . So we have at least one element $a \in H$. By assumption $aa^{-1} \in H$. But $aa^{-1} = e$ in G. So $e \in H$.
If $a \in H$ and $e \in H$ then by assumption $ea^{-1} \in H$.
That is $a^{-1} \in H$ for each $a \in H$
If $a, b \in H$ then by above $a, b^{-1} \in H$ so $(a)(b^{-1})^{-1} = ab \in H$ by Proposition 6.3.1 [$(b^{-1})^{-1} = b$] and assumption.
Finally, $\star$ on G is associative thus $\star$ on H must be associative too. [We say a property is inherited by H]
Therefore H is a group.

we show that H is a subgroup by showing (i)H non empty, (ii)for any A,B∈H we should have that $AB^{-1} \in H$

Example

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, b \in \mathbb{R} \right\}$$

is a subgroup of G.

$H \neq \emptyset$ since $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$

B A

Let $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \in H$

B^{-1}

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \in H \quad (-b \in \mathbb{R})$$

$$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & -b+c \\ 0 & 1 \end{pmatrix}}_{AB^{-1}} \in \text{H}$$

$\cancel{H}$

$(-b + c) \in \mathbb{R}$. Thus $H \leq G$.

Definition (6.3.7)

The order of a group G is the number of elements in G written $|G|$. Order of $g \in G$ is the smallest positive integer n such that $g^n = e$. We write $|g|$ or $o(g)$. Order might be finite or infinite. We say a finite group if $|G| < \infty$ and G is infinite group when G has infinitely many elements.

$\mathbb{Z}$ has infinite elements

Example: $\langle \mathbb{Z}, + \rangle$ group $|\mathbb{Z}| = \infty$ thus $\mathbb{Z}$ is an infinite group. $\langle \mathbb{Z}_n, + \rangle$ is a finite group, $|\mathbb{Z}_n| = n$.

Order of g in G. If $|g| = m$ then $\overbrace{g \star g \star \cdots \star g}^{m} = e$. Recall $g^0 = e \; \forall g \in G$

Thus $|g| = m$, m smallest positive integer such that $g^m = e$.

example: $G=\mathbb{Z}_4$. G is a group under addition of residue classes modulo 4. The unity is the class of 0.
We have that 3^4= 3+3+3+3=0 modulo 4.Thus |3| =4.
Question: What is the order of the classes 2, 1, and 0? That is find |2|, |1|, |0|

Part 3

E.M.B

Note that order of an element is the smallest positive integer as you can see that $3^8=0$ modulo 4 but order of 3 modulo 4 is 4 since 4 is the smallest positive integer such that $3^4=0$ modulo 4

CAYLEY TABLES or MULTIPLICATION TABLES

Small finite groups can be displayed on multiplication table.

M	e	a	b	c
e	e	a	b	c
a	a	a	b	e
b	b	b	c	c
c	c	e	c	e

each cell of the table contains the product of an element in column containing M and the row containing M. eg

e=a*c

(i) *M* not a group.

(ii) Binary operation not associative. Repetition of elements in rows and columns.

(iii) $(ab)c = bc = c$ but $a(bc) = ac = e$ [not associative]

if any one of the group axioms does not hold then the set M with the given binary operation * is not a group

M	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

a*a=e, thus a^{-1}=a
Question: confirm that b^{-1}=b and c^{-1}=c

(i) M is an abelian group. [Symmetric about main diagonal $\Rightarrow$ commutative.]

(ii) All elements appear in each row and column, all appear once.

(iii) Identity is e. All elements are invertible
$a^{-1} = a, \quad b^{-1} = b \quad c^{-1} = c.$

M	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

a*c=e thus a^{-1}=c

(i) M is an abelian group.

(ii) Identity is e.

(iii) All elements have inverses

$$a^{-1} = c \quad b^{-1} = b \quad c^{-1} = a \quad e^{-1} = e.$$

Question: confirm that b^{-1}=b, e^{-1}=e

Associativity? (ab)c = cc = b
a(bc) = aa = b

NOTE:

- **Closure:** Table contains only listed in *M* and appearing exactly once in each row and each column.
- **Unity :** Exactly one row and exactly one column in the table are the same as the leading row and column.
- **Inverse :** Unity appear exactly once in each row and each column.
- **Abelian :** Symmetric about main diagonal.

Exercise: Construct the multiplication table of $M=\mathbb{Z}_4$
Consider the binary operation of addition of classes modulo 4.