DISCRETE MATHEMATICS AND APPLICATIONS

Abstract Algebra 1

Mohd Sham Mohamad (mohdsham@ump.edu.my)
Adam Shariff Adli Aminuddin (adamshariff@ump.edu.my)

Faculty of Industrial Sciences & Technology

Chapter Description

Chapter Outline

5.1 Groups

5.2 Abelian Group

Aims

- Define properties of a group .
- Define extra properties for abelian group

Adam Shariff Adli Aminuddin

http://ocw.ump.edu.my/course/view.php?id=443

References

1. Rosen K.H., Discrete Mathematics & Its Applications, (Seventh Edition), McGraw-Hill, 2011
2. Epp S.S, Discrete Mathematics with Applications, (Fourth Edition), Thomson Learning, 2011
3. Ram Rabu, Discrete Mathematics, Pearson, 2012
4. Walls W.D., A beginner's guide to Discrete Mathematics, Springer, 2013
5. Chandrasekaren, N. & Umaparvathi, M., Discrete Mathematics, PHI Learning Private Limited, Delhi, 2015

Binary Operation

Definition (Binary Operation)

A binary operation on a non-empty set A is a map $f : A \times A \to A$ such that

(i) f is defined for every pair of elements in A

(ii) f uniquely associates each pair of elements in A to some element of A

i.e. $f : (a,b) \to a * b = c \in A, \ \forall a,b \in A$

Adam Shariff Adli Aminuddin

Group: Definition

Definition (Group)

Let G be a nonempty set with a binary operation $*$. G is a group if **closed under operation** $*$ and satisfies the following properties:

(i) Associativity

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

(ii) Identity

There exist a unique identity $e \in G$ such that $a*e = e*a = a\,,\ \forall a \in G$

(iii) Inverse

$\forall a \in G$ there exist a unique $b \in G$ such that $a*b = b*a = e$ (denote as $b = a^{-1}$)

Adam Shariff Adli Aminuddin

Group: Example 1

The set of integers $\mathbb{Z}$, the set of rational numbers $\mathbb{Q}$ and the set of real numbers $\mathbb{R}$ are all groups under ordinary addition.

- **Closed Operation**: Addition – Closed
- **Associative**

  $(a+b)+c=a+(b+c)$, $\forall a,b,c\in G$ by properties of addition in $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.
- **Identity**

  There exist a unique identity $0\in G$ such that $a+0=0+a=a$, $\forall a\in G$.
- **Inverse**

  $\forall a\in G$ there exist a unique $b\in G$ such that $a+(-a)=(-a)+a=0$

Adam Shariff Adli Aminuddin

Group: Example 2

The set of positive rational numbers $\mathbb{Q}^+$ under multiplication is a group.

- **Closed Operation**: Multiplication – Closed
- **Associative** `

  $(ab)c = a(bc)$, $\forall a, b, c \in G$ by properties of multiplication $\mathbb{R}$.

- **Identity**

  There exist a unique identity $1 \in G$ such that $a1 = 1a = a$, $\forall a \in G$.

- **Inverse**

  $\forall a \in G$ there exist a unique $b = \frac{1}{a} \in G$ such that $a\left(\frac{1}{a}\right) = \left(\frac{1}{a}\right)a = 1$

Adam Shariff Adli Aminuddin
http://ocw.ump.edu.my/course/view.php?id=443

Group: Example 3

The subset $\{1,-1,i,-i\}$ of the complex numbers is a group under complex multiplication.

- **Closed Operation**: Multiplication

  Closed (Multiplication Table)

$*$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

- **Associative**

  $(ab)c = a(bc)\ ,\ \forall a,b,c \in G$

  since commutative $ab = ba$.

- **Identity:** There exist a unique identity $1 \in G$ such that $a1 = 1a = a\ ,\ \forall a \in G$.

- **Inverse:** $1^{-1} = 1, (-1)^{-1} = -1, i^{-1} = i, (-i)^{-1} = i$.

Commutative

Let G be a group with a binary operation $*$. Two elements g and h of a group G is said to be commutative if $g*h=h*g$.

Example

1. Let $3,4\in\mathbb{Z}_{10}$. Then, $3+4=7=4+3$ which means 3 and 4 are commutative.

2. $\begin{bmatrix}1&2\\2&2\end{bmatrix},\begin{bmatrix}2&3\\3&3\end{bmatrix}\in GL(2,\mathbb{R})$. Then

$$\begin{bmatrix}1&2\\2&2\end{bmatrix}\begin{bmatrix}2&3\\3&3\end{bmatrix}=\begin{bmatrix}8&9\\10&12\end{bmatrix}\neq\begin{bmatrix}8&10\\9&12\end{bmatrix}=\begin{bmatrix}2&3\\3&3\end{bmatrix}\begin{bmatrix}1&2\\2&2\end{bmatrix}$$ which means

$\begin{bmatrix}1&2\\2&2\end{bmatrix}$ and $\begin{bmatrix}2&3\\3&3\end{bmatrix}$ are not commutative.

Adam Shariff Adli Aminuddin
http://ocw.ump.edu.my/course/view.php?id=443

Abelian Group

Definition (Abelian Group)

Let G be a group with a binary operation $*$.

A group G is **abelian** if $a*b=b*a, \quad \forall a,b\in G$.

Example: $GL(2,\mathbb{R})$ is not abelian group since $\begin{bmatrix}1 & 2\\ 2 & 2\end{bmatrix}\begin{bmatrix}2 & 3\\ 3 & 3\end{bmatrix}\neq\begin{bmatrix}2 & 3\\ 3 & 3\end{bmatrix}\begin{bmatrix}1 & 2\\ 2 & 2\end{bmatrix}$.

Adam Shariff Adli Aminuddin
http://ocw.ump.edu.my/course/view.php?id=443

Abelian Group: Example 1

Consider $\mathbb{Z}_4 = \{0,1,2,3\}$. The Cayley table for $\mathbb{Z}_4$ is given as follows:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4$ is abelian group since $a+b=b+a, \ \ \forall a,b \in \mathbb{Z}_4$.

Abelian Group: Example 2

$U(n) = \{$ All positive integers greater than or equal to 1, relatively prime to n and less than n $\}$

$U(5) = \{1, 2, 3, 4\}$

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$U(8) = \{1, 3, 5, 7\}$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$U(5)$ and $U(8)$ are abelian groups.

Adam Shariff Adli Aminuddin
http://ocw.ump.edu.my/course/view.php?id=443