DISCRETE MATHEMATICS AND APPLICATIONS

Abstract Algebra 2

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

Faculty of Industrial Sciences & Technology

Chapter Description

Chapter Outline

5.3 Semigroups and Monoid

5.4 Subgroups

5.5 Cyclic Groups

Aims

- Define extra properties semigroup and monoid.
- Define extra properties for subgroups.
- Define extra properties for cyclic groups

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

Adam Shariff Adli Aminuddin

Semigroup & Monoid

Definition (Semigroup)

Let G be a nonempty set with a binary operation $*$. G is a semigroup under operation $*$ and in which the multiplication operation is associative.

Definition (Monoid)

A monoid is a semigroup that has identity element for the binary operation.

Semigroup & Monoid: Example

(1) $\mathbb{R}$ is a semigroup under the binary operation +, since + is associative.

(2) $\mathbb{R}$ is also a semigroup under multiplication.

(3) $\mathbb{R}$ is not a semigroup under subtraction.

(4) $\mathbb{R}^n$ is a semigroup under +. More generally, any vector space V is a semigroup under vector addition +.

(5) $\mathbb{R}^3$ has another binary operation, the cross product $\times$ i.e. $(\mathbb{R}^3, \times)$ is not a semigroup

Subgroup

If a subset H of a group G is itself a group under the same operation as in G, we say H is a subgroup of G.

We use the notation $H \leq G$ to mean H is a subgroup of G. If we want to indicate that H is a subgroup of G, but not equal to G itself, we write $H < G$.

Some terminologies:

proper subgroup – a subgroup H when $H < G$ is called a proper subgroup.

trivial subgroup - the subgroup $\{e\}$ is called the trivial subgroup of G

nontrivial subgroup - a subgroup H when $H \neq \{e\}$ is called a nontrivial subgroup of G.

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

Subgroup Test

Theorem (One-Step Subgroup Test)

Let G be a group and H a nonempty subset of G. Then, H is a subgroup of G if H is closed under multiplication (i.e. $ab^{-1} \in H$ whenever $a, b \in H$).

Theorem (Two-Step Subgroup Test)

Let G be a group and H a nonempty subset of G. Then, H is a subgroup of G if

1. $ab \in H$ whenever $a, b \in H$ (H is closed under multiplication).
2. $a^{-1} \in H$ whenever $a \in H$ (each element in H has an inverse).

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

Subgroup Test: Example 1

Let G be an Abelian group with the identity e. Then $H = \{x \in G | x^2 = e\}$ is a subgroup of G.

Proof

1. Since $e^2 = e$, then $e \in H$. Thus $H \neq \phi$.
2. Let $a, b \in H$ which give $a^2 = b^2 = e$. We must show that $ab^{-1} \in H$.

$$\begin{aligned}(ab^{-1})^2 &= ab^{-1}ab^{-1} \\ &= (aa)(b^{-1}b^{-1}) \\ &= a^2(b^2)^{-1} \\ &= ee^{-1} \\ &= e\end{aligned}$$

This gives $ab^{-1} \in H$.

We can also define a subgroup H where elements in H are generated by any element of group G**.**

Adam Shariff Adli Aminuddin

Cyclic Subgroup

Let $a \in G$. Then $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{e, a, a^2, a^3, \ldots\}$ is called a cyclic subgroup of G generated by a.

1. Let $G = U(8) = \{1,3,5,7\}$. All cyclic subgroups of G are listed as follows:

$$\langle 1 \rangle = \{1\} \quad , \quad \langle 3 \rangle = \{3,1\} \quad , \quad \langle 5 \rangle = \{5,1\} \quad , \quad \langle 7 \rangle = \{7,1\} .$$

2. Let $G = U(5) = \{1,2,3,4\}$. All cyclic subgroups of G are listed as follows:

$$\langle 1 \rangle = \{1\} \quad , \quad \langle 2 \rangle = \{2,4,3,1\} \quad , \quad \langle 3 \rangle = \{3,4,2,1\} \quad , \quad \langle 4 \rangle = \{4,1\}$$

Note that $U(5) = \langle 2 \rangle = \langle 3 \rangle$.

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

Centre & Centralizer

Definition (Center of a Group)

The center $Z(G)=\{a\in G \mid ax=xa,\ \forall x\in G\}$ of a group G which is the set of elements in G that commute with every element of G.

Definition (Centralizer of *a* in G)

Let a be a fixed element of a group G. The centralizer of a in G, $C_G(a)=\{g\in G \mid ga=ag\}$ which is the set of all elements in G that commute with a.

Note that $Z(G)=\bigcap_{a\in G} C_G(a)$.

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

Centre & Centralizer: Example 1

Let $G=\{1,a,b,c,d,e\}$ and the multiplication table is given as follows:

$\bullet$	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	b	1	e	c	d
b	b	1	a	d	e	c
c	c	d	e	1	a	b
d	d	e	c	b	1	a
e	e	c	d	b	a	1

Thus,

$$C_G(1)=G,\quad C_G(a)=\{1,a,b\},\quad C_G(b)=\{1,a,b\},\quad C_G(d)=\{1,d,e\},\quad C_G(e)=\{1,c,d,e\},$$

and $Z(G)=\bigcap_{a\in G} C_G(a)=\{1\}$.

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

Cyclic Group

A group G is called cyclic if there is an element a in G such that $G = \{a^n \mid n \in \mathbb{Z}\}$.
Such an element a is called a *generator* of G.

Example:
Let $G = U(5) = \{1, 2, 3, 4\}$. All cyclic subgroups of G are listed as follows:

$\langle 1 \rangle = \{1\}$, $\langle 2 \rangle = \{2, 4, 3, 1\}$, $\langle 3 \rangle = \{3, 4, 2, 1\}$, $\langle 4 \rangle = \{4, 1\}$

Since $U(5) = \langle 2 \rangle = \langle 3 \rangle$, thus $U(5)$ is a cyclic group.

Cyclic Group: Example 1

Let $G = U(8) = \{1,3,5,7\}$. All cyclic subgroups of G are listed as follows:

$\langle 1 \rangle = \{1\}$, $\langle 3 \rangle = \{3,1\}$, $\langle 5 \rangle = \{5,1\}$, $\langle 7 \rangle = \{7,1\}$.

Thus, $U(8)$ is not cyclic group since there is no generator.

Cyclic Group: Example 2

Let $G = \mathbb{Z}_6 = \{0,1,2,3,4,5\}$. All cyclic subgroups of G are listed as follows:

$\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \{1,2,3,4,5\}$, $\langle 2 \rangle = \{2,4,0\}$, $\langle 3 \rangle = \{3,0\}$
$\langle 4 \rangle = \{4,2,0\}$, $\langle 5 \rangle = \{5,4,3,2,1,0\}$

Since $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$, thus $U(5)$ is a cyclic group.

*Note that, for any $G = \mathbb{Z}_n$, the generator are any $a < n$ and relatively prime with n. i.e. $\gcd(a,n) = 1$

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