The 3rd International Conference on Mathematics and Technology in Mathematics Education
5-7 March 2014, Royal University of Phnom Penh, Campus II (Pochentong)

Mr. Yim Ayuvathana Vichea
- Mathematical Researcher at RAC
- Editor of Magazine of Cambodian Mathematics and Education
- Member of Cambodian Mathematical Society
E-mail: ayuvathana.kvichea@yahoo.com
Tel: 077 53 11 48
Outline

1- Definitions of Group and Subgroup
2- Special Groups
3- Group of Integers Modulo n
4- Quaternion Group
5- Cyclic Group
6- Permutation Group
7- Conclusion

References
1- Definitions of Group and Subgroup
(នពយាប័ណ្ឌក្តីខ្មែរ លិខិនទៀត)

• As early as **200BC**, mathematicians have studied structures (តំណាង) that we now call groups: structures, symmetries, numbers, permutations and more.

• In the **19th century British mathematicians** took the lead in the study of **Abstract Algebra** (ពីជគណិតអរូបី).

• The **group** (ពុ្រក) is a part of the abstract algebra.

• There are three historical roots of **group theory**: the theory of **algebraic equations**, **number theory** and **geometry**.

• **Lagrange, Abel** and **Galois** were early researchers in the field of group theory.
Definitions of Group and Subgroup

Definition of Group (រឿងមន័យ្រករ)

• A non-empty set $G$ equipped with a binary operation ($បបណាិវីធទេទតធ$) $*$ is called a group (កុួត) if the following properties are satisfied:

(i). $(G, *)$ has the closure property (ស្រួសស្រួល៖ គ្រឿង); i.e. for every $x, y \in G$, $x * y \in G$

(ii). $(G, *)$ has the associative property (គ្រឿង៖ ំសោះ); i.e. for every $x, y, z \in G$, $(x * y) * z = x * (y * z)$
Definitions of Group and Subgroup

(iii). \((G, \ast)\) has a both-sided identity (ទាករឹតឈើត), i.e. there exists \(e \in G\) such that
\[
x \ast e = e \ast x = x \text{ for every } x \in G
\]

(iv). every element \(x\) of \(G\) has a both-sided inverse (ទាករឹតឈើត) \(x^{-1}\) in \(G\), i.e. for every \(x \in G\), there exists \(x^{-1} \in G\) such that
\[
x \ast x^{-1} = x^{-1} \ast x = e.
\]
Definitions of Group and Subgroup

Note

- If \((G, \ast)\) satisfies (i) only, it is called a **groupoid** ( កូន្តីបូពិសោះ ).

- If \((G, \ast)\) satisfies (i) and (ii) only, it is called a **semi-group** ( រណរី្រករ ).

- If \((G, \ast)\) satisfies (i), (ii) and (iii) only, it is called a **monoid** ( របូណូអធីត ).

Example \((\mathbb{Z}, +)\) and \((\mathbb{Q}, +)\) are groups.
Definitions of Group and Subgroup

Abelian Group (ក្នុងការប្រការបើកង្មេះ)
A group \((G, \ast)\) is said to be abelian or commutative (ក្នុងការប្រការបើកង្មេះប្រការបើករដ្ឋបាល) if \(G\) possesses the commutative property with respect to the operation \(\ast\), i.e. if for every \(x, y \in G\), \(x \ast y = y \ast x\).

Example
Groups \((\mathbb{Z}, +)\) and \((\mathbb{Z}, \times)\) are abelian.

Niels Henrik Abel (5 August 1802 – 6 April 1829 (aged 26)) was a Norwegian mathematician.
Definitions of Group and Subgroup

**Quasi-group** (ករណីគំនូរ)

- A non-empty set $G$ equipped with a binary operation $*$ is called a **quasi-group** if it satisfies the following properties:
  
  (i). $(G, *)$ has the closure property ( សរុបសិនបាន ), i.e. for every $x, y \in G$, then $x * y \in G$

  (ii). The equations $a * x = b$ and $y * a = b$ have unique solutions ( បននធរមីយអតរមយគតង ).

**Examples**

1. The system $(\mathbb{Z}, +)$ is a quasi-group.
2. The system $(\mathbb{Z}, \times)$ is not a quasi-group.
Definitions of Group and Subgroup

Finite Group (កុមារការងារជាក់)

- A group \((G, \ast)\) is **finite** (កុមារការងារជាក់) if \(G\) is a finite set. It is **infinite** (កុមារការងារជាក់នឹងអនុសាសន៍) if \(G\) is an infinite set.

- The **order** (រងាស់) of a finite group \((G, \ast)\) is the number of its elements and denoted by \(O(G)\) or \(|G|\). The order of an infinite group is defined to be zero.

Examples
1. The system \((\mathbb{Z}, +)\) is an infinite group.
2. The system \((S = \{1, w, w^2\}, \times)\) is a finite group, where \(w\) is a cube root of unity (បីបីទីបីៃន១).
Definitions of Group and Subgroup

Subgroup (ក្មេងការ៉េ)

- Let $H \subseteq G$. A non-empty set $H$ of a group $G$ is called a subgroup (ក្មេងការ៉េ) of $(G, \ast)$ if $(H, \ast)$ is a group.

- For every group $(G, \ast)$ has at least two (trivial) subgroups, i.e. $(G, \ast)$ and $\{e\}$, $\ast$, where $e$ is the identity of $G$.

Examples 1. The system $(\mathbb{Z}, +)$ is a subgroup of a group $(\mathbb{Q}, +)$.

2. The system $(\mathbb{Q}^*, \times)$ is a subgroup of a group $(\mathbb{R}^*, \times)$.

Theorem (ត្រូវៈពីចារ់)

A necessary and sufficient condition for a non-empty subset $H$ to be a subgroup of a group $(G, \ast)$ is $a \ast b^{-1} \in H$ for every $a, b \in H$. 
2- Special Groups (ឃ្លេសអនាគត)

- Group of Integers Modulo n (ពិសោធន៍សត្វមុំមើលជាទិន n)
- Quaternion Group (អគ្គីសម្រាប់កីឡា)
- Cyclic Group (ពិសោធន៍សត្វមុំ)
- Permutation Group (ពិសោធន៍នាង)
- Klein’s Group (ពិសោធន៍ Klein)
- ...
3- Group of Integers Modulo $n$

Let $n$ be a positive integer that $n > 1$ and let $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$ or $\mathbb{Z}(n)$ is a set of classes: $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$.

We define a binary relation $\oplus$ as

$$[a] \oplus [b] = [a + b]$$

where $a, b = 0, 1, 2, 3, \ldots, n-1$. The system $(\mathbb{Z}_n, \oplus)$ is an abelian group. This group is called the group of integers modulo $n$ or the group of residue classes modulo $n$ (កុំព្យូទ័រសន្ទឹមសតិចិនសមារនីតិកម្ម $n$ ឬកុំព្យូទ័រសន្ទឹមសតិចិនសមារនីតិកម្ម $n$).
Group of Integers Modulo n

The complete addition tables (or Cayley tables) for $(\mathbb{Z}_2, \oplus)$, $(\mathbb{Z}_3, \oplus)$ and $(\mathbb{Z}_4, \oplus)$ are given below.

$\begin{array}{c|cc}
\oplus & 0 & 1 \\
\hline
0 & 0 & 1 \\
1 & 1 & 0 \\
\end{array}$

$\begin{array}{c|cccc}
\oplus & 0 & 1 & 2 \\
\hline
0 & 0 & 1 & 2 \\
1 & 1 & 2 & 0 \\
2 & 2 & 0 & 1 \\
\end{array}$

$\begin{array}{c|cccc}
\oplus & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}$

Arthur Cayley (16 August 1821–26 January 1895 (aged 73)) was a British mathematician.
4- Quaternion Group

Let $Q_8 = \{1, i, j, k, -1, -i, -j, -k\}$ whose elements satisfy the conditions with multiplication:

\((-1)^2 = 1, \ i^2 = j^2 = k^2 = -1, \ ij = -ji = k, \ jk = -kj = i, \ ki = -ik = j, \)

and \(-x = (-1)x = x(-1)\) for all $x$ in $Q_8$.

The system $(Q_8, \times)$ is a group of order 8. This group is called the **quaternion group**.
Quaternion Group (ក្រុមមុខមូលរយៈ)

- The complete multiplication table (or Cayley table) for \((Q_8, \times)\).

<table>
<thead>
<tr>
<th>\times</th>
<th>1</th>
<th>i</th>
<th>j</th>
<th>k</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>i</td>
<td>j</td>
<td>k</td>
</tr>
<tr>
<td>i</td>
<td>i</td>
<td>-1</td>
<td>k</td>
<td>-j</td>
</tr>
<tr>
<td>j</td>
<td>j</td>
<td>-k</td>
<td>-1</td>
<td>i</td>
</tr>
<tr>
<td>k</td>
<td>k</td>
<td>j</td>
<td>-i</td>
<td>-1</td>
</tr>
</tbody>
</table>

Quaternion multiplication

Sir William Rowan Hamilton (midnight, 3-4 August 1805 – 2 September 1865) was an Irish physicist, astronomer, and mathematician, who made important contributions to classical mechanics, optics, and algebra.
Quatertion Group (ក្រុមសេសត្រូវបាក់)

• The quaternion set Q₈ are equal to R⁴, a four-dimensional vector space over the real numbers. Q₈ has three operations: addition, scalar multiplication, and quaternion multiplication.

• The elements of this basis are customarily denoted as 1, i, j, and k. Every element of Q₈ can be uniquely written as a linear combination of these basis elements, that is, as a₁ + bi + cj + dk, where a, b, c, and d are real numbers.

• Then the basis elements are:

  \[
  1 = (1, 0, 0, 0),
  i = (0, 1, 0, 0),
  j = (0, 0, 1, 0),
  k = (0, 0, 0, 1),
  \]

Quateregion Group

Graphical representation of quaternion units product as 90°-rotation in 4D-space

$ij = k$
$ji = -k$
$ij = -ji$
5- Cyclic Group (កុំព្យូទ័រធីគមីរ)

• Let G be a group. For any $a \in G$, the subgroup
  \[ H = \{ x \in G / x = a^n \text{ for } n \in \mathbb{Z} \} \]
is the **subgroup generated by a** (កុំព្យូទ័រធីគមីរ) and is
denoted by $\langle a \rangle$.

A given subgroup $K$ of $G$ is a **cyclic subgroup** (កុំព្យូទ័រធីគមីរ) if there exists an element $b$ in $G$ such that
  \[ K = \langle b \rangle = \{ y \in G / y = b^n \text{ for some } n \in \mathbb{Z} \} \]
In particular, $G$ is a **cyclic group** (កុំព្យូទ័រធីគមីរ) if there is an
element $a \in G$ such that $G = \langle a \rangle$.

• Any element $a$ of the group $G$ such that $G = \langle a \rangle$ is a
  **generator** (សត្វ់រីក) of $G$. 
Cyclic Group (កុំព្យូទ័រ)

• Examples

1. The system \((\mathbb{Z}, +)\) is a cyclic group. We have \(\mathbb{Z} = \langle 1 \rangle\) and \(\mathbb{Z} = \langle -1 \rangle\). These numbers -1 and 1 are generators of \(\mathbb{Z}\).

2. Let \(E\) be a set of all even integers. The system \((E, +)\) is the cyclic subgroup generated by 2 of the group \((\mathbb{Z}, +)\). Hence \(E = \langle 2 \rangle\).

3. The set \(H = \{[2], [4], [6], [8]\} \subseteq \mathbb{Z}_{10}\) is an abelian group with respect to multiplication. Since \([2]^2 = [4]\), \([2]^3 = [8]\), \([2]^4 = [6]\), then \(H = \langle [2] \rangle\) i.e. \((H, \otimes)\) is a cyclic group and that [2] is a generator of \(H\).
Cyclic Group (ធនិះជីបុំ)

- Example cyclic groups in 2 dimensional symmetry
• A permutation (សមាគភាព) of a set A is a function from A to A that is both one-to-one and onto (មេដាយទី១មួយ និងទី២មួយ). A permutation group (សមាគភាព) $S(A)$ of a set A is a set of permutation of A that forms a group under function composition (ប្រភេទនិយមនិយមរួមគឺ).

• Let $A = \{a_1 , a_2 , ..., a_n\}$. Any permutation $f$ on A is determined by the choices for the n values $f(a_1), f(a_2), ..., f(a_n)$.

There are $n(n – 1) ... (2)(1) = n!$ different ways in which $f$ can be defined, and $S(A)$ has $n!$ elements. Each element $f$ in $S(A)$ can be represented by a matrix:

$$f = \begin{bmatrix} a_1 & a_2 & \ldots & a_n \\ f(a_1) & f(a_2) & \ldots & f(a_n) \end{bmatrix}$$
Permutation Group (ព្រះសម្រាប់វិធីសាស្រ្ត)

• Each permutation $f$ on $A$ can be made to correspond to a permutation $f'$ on $B = \{1, 2, 3, \ldots, n\}$ by replacing $a_k$ with $k$ for $k = 1, 2, 3, \ldots, n$:

$$f' = \begin{bmatrix} 1 & 2 & \ldots & n \\ f'(1) & f'(2) & \ldots & f'(n) \end{bmatrix}.$$ 

The mapping $f \rightarrow f'$ is an isomorphism (សម្រាប់វិធីសាស្រ្ត) from $S(A)$ to $S(B)$, and the groups are the same except for notation. The group $S(B)$ is called as the symmetric group (ព្រះសម្រាប់វិធីសាស្រ្ត) on $n$ elements, and it is denoted by $S_n$. 
Permutation Group (កូនប្រមូល)

Examples

1. The notation \( f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{bmatrix} \) indicates that \( f \) is an element of \( S_5 \) and that \( f(1) = 3, f(2) = 1, f(3) = 5, f(4) = 4, \) and \( f(5) = 2. \)

2. If \( f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{bmatrix} \) and \( g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{bmatrix} \) are two elements of \( S_5 \), then

\[ fg = f \circ g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 5 \\ 2 & 5 & 1 \end{bmatrix}. \]
The Rectangle (តូចការ៉េក្រុង)

The rectangle has 4 symmetries, where 
\( f_0 = I = \) identity motion, \( f_1 = \) rotation through 180°, 
\( f_2 = \) reflection about the horizontal axis or A-axis, 
and \( f_3 = \) reflection about the vertical axis or B-axis.

We have,

\[
I = f_0 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}
\]

\[
f_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}
\]

\[
f_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix}
\] and \( f_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \).

Then the set \( S_4 = \{ I, f_1, f_2, f_3 \} \).
Permutation Group (ក្រុមតំបន់)

The Rectangle (ត្រីកោណកោណាលុង)

- complete composition table (or Cayley table) for \((S_4, \circ)\).

<table>
<thead>
<tr>
<th></th>
<th>(0)</th>
<th>(I)</th>
<th>(f_1)</th>
<th>(f_2)</th>
<th>(f_3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0)</td>
<td>(0)</td>
<td>(I)</td>
<td>(f_1)</td>
<td>(f_2)</td>
<td>(f_3)</td>
</tr>
<tr>
<td>(I)</td>
<td>(I)</td>
<td>(I)</td>
<td>(f_1)</td>
<td>(f_2)</td>
<td>(f_3)</td>
</tr>
<tr>
<td>(f_1)</td>
<td>(f_1)</td>
<td>(I)</td>
<td>(f_3)</td>
<td>(f_2)</td>
<td>(f_1)</td>
</tr>
<tr>
<td>(f_2)</td>
<td>(f_2)</td>
<td>(f_3)</td>
<td>(I)</td>
<td>(f_1)</td>
<td>(f_2)</td>
</tr>
<tr>
<td>(f_3)</td>
<td>(f_3)</td>
<td>(f_2)</td>
<td>(f_1)</td>
<td>(I)</td>
<td>(f_3)</td>
</tr>
</tbody>
</table>

From the above Cayley table, then \((S_4, \circ)\) is a group. It is called the symmetric group of rectangle (ក្រុមតំបន់ត្រីកោណកោណាលុង).
Permutation Group (ពរាចារណ៍)

The equilateral triangle (តីកណ្តាលមុន)

The equilateral triangle has 6 symmetries, where $f_0 = I = \text{identity motion}$, $f_1 = \text{rotation through } 120^0$, $f_2 = \text{rotation through } 240^0$, $f_3 = \text{reflection about the A-axis}$, $f_4 = \text{reflection about the B-axis}$, and $f_5 = \text{reflection about the C-axis}$. We have,

$I = f_0 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$, \quad $f_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$,

$f_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$, \quad $f_3 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$,

$f_4 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$, and \quad $f_5 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$.

Then the set $S_3 = \{ I, f_1, f_2, f_3, f_4, f_5 \}$. 
Permutation Group (គឺប្រាប់អំពីការឈឺ)

The equilateral triangle (គឺការឈឺតំបន់)

- complete composition table (or Cayley table) for \((S_3, \circ)\).

<table>
<thead>
<tr>
<th></th>
<th>I</th>
<th>f₁</th>
<th>f₂</th>
<th>f₃</th>
<th>f₄</th>
<th>f₅</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>f₃</td>
<td>f₄</td>
<td>f₅</td>
</tr>
<tr>
<td>f₁</td>
<td>f₁</td>
<td>f₂</td>
<td>I</td>
<td>f₄</td>
<td>f₅</td>
<td>f₃</td>
</tr>
<tr>
<td>f₂</td>
<td>f₂</td>
<td>I</td>
<td>f₁</td>
<td>f₅</td>
<td>f₃</td>
<td>f₄</td>
</tr>
<tr>
<td>f₃</td>
<td>f₃</td>
<td>f₅</td>
<td>f₄</td>
<td>I</td>
<td>f₂</td>
<td>f₁</td>
</tr>
<tr>
<td>f₄</td>
<td>f₄</td>
<td>f₃</td>
<td>f₅</td>
<td>f₃</td>
<td>I</td>
<td>f₂</td>
</tr>
<tr>
<td>f₅</td>
<td>f₅</td>
<td>f₄</td>
<td>f₃</td>
<td>f₂</td>
<td>f₁</td>
<td>I</td>
</tr>
</tbody>
</table>

From the above Cayley table, then \((S_3, \circ)\) is a group. It is called the symmetric group of equilateral triangle (ការអំពីការឈឺតំបន់).
Permutation Group (ពរុមបៃតង)
Permutation Group (ក្រុមត្រីកោណ)
7- Conclusion

- The aim of this paper is to show some special groups in algebra, particularly in abstract algebra (or modern algebra).

- This paper provides the definition of the group and some special groups, and shows a proof to be a group by using Cayley table especially for symmetric groups.
References

References


