Degree project

Dynamical Systems Over Finite Groups

Author: Muhammad Badar
Date: 2012-02-28
Subject: Mathematics
Level: Master
Course code: 5MA12E
Dynamical systems over finite groups

Muhammad Badar

March 7, 2012
Abstract

In this thesis, the dynamical system is used as a function on a finite group, to show how states change. We investigate the 'number of cycles' and 'length of cycle' under finite groups. Using group theory, fixed point, periodic points and some examples, formulas to find 'number of cycles' and 'length of cycle' are derived. The examples used are on finite cyclic group $\mathbb{Z}_6$ with respect to binary operation '$+$'. Generalization using finite groups is made. At the end, I compared the dynamical system over finite cyclic groups with the finite non-cyclic groups and then prove the general formulas to find 'number of cycles' and 'length of cycle' for both cyclic and non-cyclic groups.

**keywords:** Cyclic group; Non-cyclic group; Dynamical system; Fixed point; Periodic point; Pre periodic point; Pure cycle structure.
Acknowledgments

This thesis is written as a part of the Master Program in Mathematics and Modelling at Linnaeus University, Sweden. It is written at the Department of Computer Science, Physics and Mathematics.

I am obliged to my supervisor Marcus Nilsson for accepting and giving me a chance to do my thesis under his kind supervision. I am also thankful to him for his work that set up a road map for me. I wish to thank Per-Anders Svensson for being in Linnaeus University and teaching me. He is really a cool, calm and has grip in his subject, as an educator should. I also want to thank of my head of department and teachers who time to time supported me in different subjects. I express my deepest gratitude to my parents and brothers who supported and encouraged me during my study. At the end I am very much thankful to Swedish Government for providing me the great opportunity by granting the permission to stay and study in Sweden.
# Contents

1 Introduction 6 

2 Preliminaries 7  
   2.1 Group 7  
   2.2 Dynamical systems over finite set 8  

3 Linear dynamical systems over finite cyclic group 10  

4 Linear dynamical systems over finite non-cyclic group 17  

5 Bibliography 23
1 Introduction

All the things having any relation with nature and society, and evolving in time are the part of a dynamical system. The solar system, the climatic, the economic system and the flow of ideas in our brains, are some of the examples of this system. This system can be classified into two groups, continuous and discrete, see for instance Fraleigh [1].

A continuous dynamical system is the one that evolves continuously. On the other hand, a discrete dynamical system is that phenomenon which evolves at specific moments. This system is shown by the iteration of a function, see for instance Khrennikov [4]. This thesis is meant to consider discrete dynamical systems.

The main objective behind the study of a dynamical system is to perceive and apprehend the future of a given phenomenon. Some time, we are not able to foretell what exactly will happen. Even then we are at least able to conclude something about the long term behavior of the system. This behavior can be classified by finding fixed points and cycles of the system and determine whether they are attractive, repulsive or natural, see for instance Khrennikov and Nilsson [3] and Edward [2].

I described some basic definitions of group theory and dynamical systems over finite set in Chapter 2, which are necessary to understand the concept of the thesis, see for instance Fraleigh [1] and Hua-Chieh [5].

In order to explain the linear dynamical systems over finite cyclic group, I solved some examples under addition in Chapter 3 and under multiplication in Chapter 4. On the behalf of these examples and definitions, I proved the general formula to find the length of cycle and number of cycles of the dynamical system.
2 Preliminaries

In this section, we shall define some basic definitions. There are many books which give a good introduction to the group theory, see for instance Fraleigh [1].

2.1 Group

Let \( G \) be a non empty set and \( * \) be a binary operation on \( G \). Then \( G \) is called a group if it satisfies the following axioms.

1) \( * \) is associative in \( G \), that is for all \( a, b, c \in G \), we have

\[
(a * b) * c = a * (b * c).
\]

2) \( G \) contains an identity element with respect to \( * \). For any \( a \in G \) there exist \( e \in G \) such that

\[
a * e = e * a = a
\]

3) Every element in \( G \) has its inverse in \( G \), with respect to \( * \). For any \( a \in G \) there exist \( a^{-1} \in G \) such that

\[
a * a^{-1} = a^{-1} * a = e
\]

If all above axioms are fulfilled then \( G \) is called group under the binary operation \( * \) and it is written as \( (G, *) \).

Definition 2.1. Let \( n \) be a positive integer. Integers \( a \) and \( b \) are said to be congruent modulo \( n \) if they have the same remainder when divided by \( n \). This is denoted by writing \( a \equiv b (\text{mod } n) \).

Definition 2.2. The set of integers modulo \( n \), \( Z_n = \{0, 1, 2, ..., n-1\} \), is a group under addition performed modulo \( n \).

Definition 2.3. Let \( n > 1 \) be an integer. The multiplicative group of integers modulo \( n \), denoted by \( Z_n^* \), is defined as follows. \( Z_n^* = \{k : 1 \leq k \leq n \text{ with } \gcd(k, n) = 1\} \).

Definition 2.4. A group which contains finite number of elements is called a finite group.

Definition 2.5. If in a group, the binary operation \( * \) is commutative that is for all \( a, b \in G \)

\[
a * b = b * a.
\]

Then \( (G, *) \) is called an abelian group.

Definition 2.6. A group \( G \) is called cyclic if its every element is generated by some element \( a \in G \), that is for some \( a \in G \) if \( G = \langle a \rangle = \{a^n | n \in \mathbb{Z}\} \) then, the element \( a \) is called generator of the cyclic group \( G \).
Example 2.1. Consider the group $\mathbb{Z}_5^*$ = \{1, 2, 3, 4\} we can see that
\[3^1 = 3, 3^2 = 4, 3^3 = 2 \quad \text{and} \quad 3^4 = 1.\]
This shows that group $\mathbb{Z}_5^*$ is cyclic and 3 is a generator. It can be written as $\mathbb{Z}_5^* = \langle 3 \rangle$.

Example 2.2. Let $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, we have
\[1 + 0 = 1, 1 + 1 = 2, 1 + 2 = 3, 1 + 3 = 4, 1 + 4 = 0\]
This shows that group $\mathbb{Z}_5$ is cyclic and 1 is a generator. It can be written as $\mathbb{Z}_5 = \langle 1 \rangle$.

Theorem 2.1. Let $G$ be a cyclic group with $n$ elements and generated by $a$. Let $b \in G$ and let $b = a^s$. Then $b$ generates a cyclic subgroup $H$ of $G$ containing $n/d$ elements, where $d$ is the greatest common divisor (abbreviated gcd) of $n$ and $s$.

Proof. It is given that $b$ generates a cyclic subgroup $H$ of $G$. We have to show that $H$ has $n/d$ elements. We know that $H$ has as many elements as the smallest positive power $m$ of $b$ that gives the identity. Since $b = a^s$, and $b^m = e$ iff $(a^s)^m = e$, or iff $n$ divides $ms$. Let $d$ be the gcd of $n$ and $s$. Then there exist integers $u$ and $v$ such that
\[d = un + vs.\]
Since $d$ divides both $n$ and $s$, we have
\[1 = u(n/d) + v(s/d).\]
Where both $n/d$ and $s/d$ are integers. This last equation shows that $n/d$ and $s/d$ are relatively prime, for any integer dividing both of them must also divide 1. We wish to find the smallest positive $m$ such that
\[\frac{ms}{n} = \frac{m(s/d)}{n/d},\]
is an integer. We conclude that $n/d$ must divide $m$. So, the smallest such $m$ is $n/d$. Thus the order of $H$ is $n/d$. \qed

2.2 Dynamical systems over finite set

It is a triple $(G, f, \gamma)$, where $G$ is a finite set, $f : G \to G$ is a map from $G$ to itself and $\gamma$ is the directed graph, whose vertices are the elements of $G$ and whose oriented edges (arrows) lead each vertex directly to its image (where it is sent by $f$), see for instance Edward [2] and Hua-Chieh [5].

Definition 2.7. A fixed point of a function is a point that is mapped to itself by the function. For example, if $f$ is defined on the finite set $G$ by
\[f(x) = x \quad \text{where,} \quad x \in G.\]
Then $x$ is called a fixed point.
Definition 2.8. Let \( g \in G \) is a fixed point to \( f \) if \( f(g) = g \), \( g \in G \) is a \( r \) - periodic point if \( r \) is the least number such that

\[
f^r(g) = g.
\]

The set \( \{g, f_a(g), f_a^2(g), ..., f_a^{r-1}(g)\} \) is called a \( r \) - cycle.

Example 2.3. Let \( G = (\mathbb{Z}_6, +) \) and \( f : G \to G \) is a function. The binary operation ‘+’ is defined in the following Cayley table.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 1: Cayley Table

Let \( f_1(x) = 1 + x \), for all \( x \in G \), where 1 is the fixed point of \( G \). Then find the number of cycles and length of each cycle.

First, we construct a table by putting values of \( x \) in \( f_1(x) \).

<table>
<thead>
<tr>
<th>x</th>
<th>f(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 2:

From table, 0 mapped to 1, 1 mapped to 2, 2 mapped to 3, 3 mapped to 4, 4 mapped to 5 and 5 mapped to 0.
so we can draw the figure.

Figure 1:

Here, the state space consists of one cycle of length 6.

3 Linear dynamical systems over finite cyclic group

Let \( f_a(g) = a \ast g \) for a fixed \( a \in G \), where \( \ast \) is the binary operation of the group \( G \). Consider the dynamical system

\[
 f_a : G \to G
\]

Example 3.1. Let \( f_2(x) = 2 + x \), for all \( x \in G \), where \( G = (\mathbb{Z}_6, +) \) and \( f : G \to G \) is a function, then find the number of cycles and length of each cycle.

First, we construct a table by putting values of \( x \) in \( f_2(x) \). See table 1 for the Cayley table.

<table>
<thead>
<tr>
<th>x</th>
<th>f(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 3:

From table, we can draw the figures.
Example 3.2. Let $f_3(x) = 3 + x$, for all $x \in G$, where $G = (\mathbb{Z}_6, +)$ and $f : G \to G$ is a function, then find the number of cycles and length of each cycle. First, we construct a table by putting values of $x$ in $f_3(x)$. See table 1 for the Cayley table.

<table>
<thead>
<tr>
<th>x</th>
<th>f(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 4:

From table, we can draw the figures.

Figure 3:

Here, the state space consists of three cycles of length 2.

Example 3.3. Let $f_4(x) = 4 + x$, for all $x \in G$, where $G = (\mathbb{Z}_6, +)$ and $f : G \to G$ is a function, then find the number of cycles and length of each cycle.
First, we construct a table by putting values of $x$ in $f_4(x)$. See table 1 for the Cayley table.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$f(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 5:

From table, we can draw the figures.

![Figure 4:](image)

Here, the state space consists of two cycles of length 3.

**Example 3.4.** Let $f_5(x) = 5 + x$, for all $x \in G$, where $G = (\mathbb{Z}_6, +)$ and $f : G \rightarrow G$ is a function, then find the number of cycles and length of each cycle.

First, we construct a table by putting values of $x$ in $f_5(x)$. See table 1 for the Cayley table.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$f(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 6:

From table, we can draw the figure.
Theorem 3.1. If $G$ is a group and $f : G \to G$ is a function, such that $f_a(x) = a \ast x$. Then $f_a$ is one-to-one and onto.

Proof. Given $f : G \to G$ is a function and $f_a(x) = a \ast x$.

We know that $f : G \to G$ is $1 - 1$ if and only if for every $x$ and $y$ in $G$, if $f(x) = f(y)$ then $x = y$.

Let $f_a(x) = f_a(y)$

then

$a \ast x = a \ast y$

$x = y$. by left cancellation law

So, $f_a$ is one-to-one.

Now, we prove that $f_a$ is onto.

We know that $f : G \to G$ is onto (or surjective) if and only if for every $y$ in $G$ there exists at least one $x$ in $G$ such that $f(x) = y$.

Let $y \in G$. We need to show there exist an $x \in G$ such that $f_a(x) = y$. Let $f_a(x) = a \ast x = y$. Since $G$ is a group, so $x = a^{-1} \ast y \in G$ for any $y \in G$. Hence this function is onto.

Corollary. Since $f_a$ is one-to-one and onto, so the dynamical system of $f_a$ will only contain periodic points (pure cycle structure).

Proof. We prove it by contradiction. Suppose that the dynamical system of $f_a$ has a pre periodic point $A$ such that
Figure 6:

then $f_a$ is not one-to-one, because $A \rightarrow B$ and $R \rightarrow B$, that is $A$ and $R$ have the same image $B$. So, our supposition was wrong. Hence the dynamical system of $f_a$ will only contain periodic points (pure cycle structure).

Here, we give an example $g(x) = x \ast x$ which is not one-to-one.

**Example 3.5.** Let $G = (\mathbb{Z}_5, \ast)$, consider the dynamical system defined by $g(x) = x \ast x$. The binary operation $\ast'$ is defined in the following Cayley table.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 7: Cayley Table

From Cayley Table, we have

- $g(1) = 1 \ast 1 = 1$
- $g(2) = 2 \ast 2 = 4$
- $g(3) = 3 \ast 3 = 4$
- $g(4) = 4 \ast 4 = 1$

Since, 1 mapped to 1, 2 mapped to 4, 3 mapped to 4 and 4 mapped to 1, so we can draw the figure as
Since 2 and 3 have the same image 4 and we also have a pre-periodic point 1 so, \( g(x) = x \ast x \) is not one-to-one.

By the above examples 3.1 to 3.4, if \( G = (\mathbb{Z}_6, +) \) and \( f : G \rightarrow G \) is a function such that \( f_a = x + a \), where \( a \) is given and \( x \) is any point of \( G \), then we have

Number of cycles = \( \gcd(a, n) \) and Length of each cycle = \( \frac{n}{\gcd(a, n)} \), where \( n = |G| = 6 \). We can formulate it in the form of a table as

<table>
<thead>
<tr>
<th>( a ) :</th>
<th>Number of cycles × Length of each cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 :</td>
<td>1 × 6</td>
</tr>
<tr>
<td>2 :</td>
<td>2 × 3</td>
</tr>
<tr>
<td>3 :</td>
<td>3 × 2</td>
</tr>
<tr>
<td>4 :</td>
<td>2 × 3</td>
</tr>
<tr>
<td>5 :</td>
<td>1 × 6</td>
</tr>
</tbody>
</table>

**Table 8:**

**Theorem 3.2.** Let \( a \) be any given point of a finite cyclic group \( (\mathbb{Z}_n, +) \) and \( f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n \) be a function. If \( a \) is the generator of \( \mathbb{Z}_n \), then \( d = \gcd(a, n) \) is the number of cycles and \( \frac{n}{\gcd(a, n)} \) is the length of each cycle.

**Proof.** Let \( a \in \mathbb{Z}_n \), where \( a \) is given point of \( \mathbb{Z}_n \) and \( x \) is any point of \( \mathbb{Z}_n \). Then, consider a function \( f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n \) as

\[
f_a(x) = x + a
\]

to create a dynamical system, we have to iterate \( f_a(x) \) again and again such that we could complete a pure cycle structure.

\[
f_a^r(x) = x + a + a + a + \ldots \quad (r \text{ times}).
\]
Hence
\[ f'_a(x) = x + ra. \]

Let \( r \) be the least integer, such that
\[ f'_a(x) = x \pmod{n}. \]

That is \( ra = 0 \), it is only possible if \( n \) divide \( ra \). Let \( d = \gcd(a, n) \) then \( n = d \cdot n' \), where \((a, n') = 1\). Since \( n \) divide \( ar \) so \( d \) divide \( ar \) and \( n' \) divide \( ar \) (because \( d \) and \( n' \) are factors of \( n \)).

This implies that
\[ n' \text{ divide } r, \text{ since } (a, n') = 1. \]

Here, \( r \) is least if
\[
\begin{align*}
  r &= n' \\
  \text{then } r &= \frac{n}{d}, \text{ since } n = d \cdot n' \\
  \text{that is } r &= \frac{n}{\gcd(a, n)}, \text{ since } d = \gcd(a, n)
\end{align*}
\]

We now generalize the theorem to any finite cyclic group.

**Theorem 3.3.** Let \( G \) be a finite cyclic group with \( n \) elements. Let \( f : G \rightarrow G \) be a function. If \( a = g^s \) is the given point and \( g \) is the generator of \( G \), then \( d = \gcd(s, n) \) is the number of cycles and \( \frac{n}{\gcd(s, n)} \) is the length of each cycle.

**Proof.** Let \( a \) be a given point of \( G \) and \( x \) is any point of \( G \). Then, consider a function \( f : G \rightarrow G \) defined as
\[ f_a(x) = x \ast a. \]

Since, we have proved in the Corollary of Theorem 3.1 that the dynamical system of \( f_a \) contains only periodic points. So, to create a dynamical system, we have to iterate \( f_a(x) \) again and again such that we could complete a pure cycle structure. That is
\[ f^r_a(x) = x \ast a \ast a \ast a \ast a \ast \ldots. \quad (r \text{ times}). \]

Hence
\[ f^r_a(x) = x \ast a^r = x \ast g^{sr}, \text{ since } a = g^s \]

Let \( r \) be the least integer such that
\[ f^r_a(x) = x \pmod{n}. \]
That is $g^e = e$, where $e$ is the identity of $G$. It is only possible if $n$ divide $sr$.

Let $d = \gcd(s, n)$, then $n = d \cdot n'$, where $(s, n') = 1$. Since $n$ divides $sr$, so $d$ and $n'$ also divide $sr$ (because $d$ and $n'$ are factors of $n$).

This implies that

$$n' \text{ divides } r, \text{ since } (s, n') = 1.$$ 

Here, $r$ is least if $r = n'$ then $r = \frac{n}{d}$ since $n = d \cdot n'$ that is $r = \frac{n}{\gcd(s, n)}$ since $d = \gcd(s, n)$.

## 4 Linear dynamical systems over finite non-cyclic group

Now, we consider a simple non-cyclic group and study a couple of examples of linear systems over it.

**Example 4.1.** Let $V = \{e, a, b, c\}$ is a non-cyclic group and $f : V \rightarrow V$ is a function. The binary operation $\cdot$ is defined in the following Cayley table. Let

\[
\begin{array}{cccc}
  \ast & e & a & b & c \\
  e & e & a & b & c \\
  a & a & e & c & b \\
  b & b & c & e & a \\
  c & c & b & a & e \\
\end{array}
\]

Table 9: Cayley Table

$f_a(x) = a \ast x$, for all $x \in V$. Then find the number of cycles and length of each cycle.

First, we construct a table by putting values of $x$ in $f_a(x)$.

\[
\begin{array}{ccc}
  x & f(x) \\
  e & a \\
  a & e \\
  b & c \\
  c & b \\
\end{array}
\]

Table 10:

From table, we can draw the figures.
Example 4.2. Let $f_e(x) = e \ast x$, for all $x \in V$. Then find the number of cycles and length of each cycle.

First, we construct a table by putting values of $x$ in $f_e(x)$. See table 9 for the Cayley table.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$f(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
</tr>
<tr>
<td>$c$</td>
<td>$c$</td>
</tr>
</tbody>
</table>

Table 11:

From table, we can draw the figures.

Figure 9:

Here, the state space consists of four cycles of length 1.

Example 4.3. Let $f_b(x) = b \ast x$, for all $x \in V$. Then find the number of cycles and length of each cycle.

First, we construct a table by putting values of $x$ in $f_b(x)$. See table 9 for the Cayley table.
Table 12:

<table>
<thead>
<tr>
<th>x</th>
<th>f(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>b</td>
</tr>
<tr>
<td>a</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>e</td>
</tr>
<tr>
<td>c</td>
<td>a</td>
</tr>
</tbody>
</table>

From table, we can draw the figures.

Figure 10:

Here, the state space consists of two cycles of length 2.

**Example 4.4.** Let $G = (\mathbb{Z}_{15}, \cdot)$ is a non-cyclic group and $f : G \rightarrow G$ is a function. The binary operation '$\cdot$' is defined in the following Cayley table.
Here $G = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>7</th>
<th>8</th>
<th>11</th>
<th>13</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
<td>8</td>
<td>11</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>14</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>13</td>
<td>2</td>
<td>14</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>14</td>
<td>13</td>
<td>4</td>
<td>11</td>
<td>2</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td>11</td>
<td>4</td>
<td>13</td>
<td>14</td>
<td>7</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>7</td>
<td>14</td>
<td>2</td>
<td>13</td>
<td>1</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>11</td>
<td>7</td>
<td>1</td>
<td>14</td>
<td>8</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>13</td>
<td>11</td>
<td>8</td>
<td>7</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 13: Cayley Table

Let $f_2(x) = 2 \cdot x$ for all $x \in G$, where 2 is the fixed point of $G$. Then find the number of cycles and length of each cycle.
First, we construct a table by putting values of $x$ in $f_2(x)$.
Table 14:

<table>
<thead>
<tr>
<th>x</th>
<th>f(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>14</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>13</td>
<td>11</td>
</tr>
<tr>
<td>14</td>
<td>13</td>
</tr>
</tbody>
</table>

From table, we can draw the figures.

Figure 11:

Here, the state space consists of two cycles of length 4.

**Example 4.5.** Let \( f_{14}(x) = 14 \cdot x \) for all \( x \in G \), where 14 is the fixed point of \( G \). Then find the number of cycles and length of each cycle.

First, we construct a table by putting values of \( x \) in \( f_{14}(x) \). See table 13 for the Cayley table.
From table, we can draw the figures.

<table>
<thead>
<tr>
<th>x</th>
<th>f(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td>2</td>
<td>13</td>
</tr>
<tr>
<td>4</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 15:

Here, the state space consists of four cycles of length 2.

Note that in example 4.5, $a = 14$, $n = 8$. Then, according to the formulas, which we have proved for cyclic groups,
number of cycles = $d = \gcd(a, n) = (14, 8) = 2$, length of cycle = $\frac{n}{d} = \frac{8}{2} = 4$.
But here, we have
number of cycles = 4, length of cycle = 2.

**Remark.** The formulas, which we have proved for cyclic groups can not be applied for the non-cyclic groups.

Now, we prove the general formulas to find 'number of cycles' and 'length of cycle' for both cyclic and non-cyclic groups.

**Theorem 4.1.** Let $G$ be a finite group with $n$ elements. Let $f : G \rightarrow G$ be a function such that

$$f_a(x) = x * a$$

21
where, $a$ is given point and $x$ is any point of $G$. Then the state space of $f_a(x) = x * a$, consists of $\frac{|G|}{|\langle a \rangle|}$ cycles of length $|\langle a \rangle|$.

**Proof.** Since, $G$ is a finite group having $n$ elements and $a \in G$, so $|\langle a \rangle| \leq |G|$. we have $f_a(x) = x * a$.

To create a dynamical system, we have to iterate $f_a(x)$ again and again such that, we could complete a pure cycle structure, that is

$$f_a^r(x) = x * a * a * a * \ldots \ldots \ (r \ times).$$

Hence

$$f_a^r(x) = x * a^r.$$

The cycle length $r$ is determined by

$$x * a^r = x.$$

We know that, if $a \in G$ is of finite order $r$, then $r$ is the smallest positive integer such that $a^r = e$ (the cycle length is independent of $x$). Then

the length of cycle $= r = |\langle a \rangle|$.

Since, order of an element of a group $G$ divides the order of the group $G$, so

$$\text{number of cycles} = \frac{|G|}{|\langle a \rangle|}.$$

\[\square\]

**Conjecture.** Since in example $4 \cdot 5$, $a = 14$, $n = 8$. Then, according to the general formulas.

number of cycles $= \frac{|G|}{|\langle a \rangle|} = \frac{8}{2} = 4$, length of cycle $= |\langle a \rangle| = 2$.

The result is same as in example $4 \cdot 5$, so the above formulas can be used to find number of cycles and length of cycle for both cyclic and non-cyclic groups.
5 Bibliography

References


