

The pre-periods of all endomorphisms of a finite cyclic group

Aveya Charoenpol [‡]

Napaporn Sarasit [†]

Division of Mathematics

Faculty of Engineering

Rajamangala University of Technology

Isan Khonkaen Campus

40000

Thailand

Pongsaphat Prachumdang [§]

Udom Chotwattakawanit ^{*}

Department of Mathematics

Faculty of Science

Khon Kaen University

40002

Thailand

Abstract

Let $\mathbf{G}$ be a group. By Fitting's lemma, if $\mathbf{G}$ is finite abelian and t is the pre-period of $\mathbf{G}$, then $\mathbf{G}$ can be represented as the direct sum of $\ker f^t$ and $f^t(\mathbf{G})$ for all endomorphisms f of $\mathbf{G}$. In this paper, we will show that the pre-period of a cyclic group of order n is the maximum of $v_p(n)$ (the p -adic valuation of n) for all prime p with $p \mid n$. Indeed, the pre-periods of all endomorphisms of a finite cyclic group are determined in terms of the p -adic valuations.

Subject Classification: 08A60, 08A35, 20E34.

Keywords: Pre-period, Endomorphism, Monounary algebra, Cyclic group.

[‡] E-mail: aveya.ch@rmuti.ac.th

[†] E-mail: napaporn.sr@rmuti.ac.th

[§] E-mail: pong_sa_phat@kkumail.com

^{*} E-mail: udomch@kku.ac.th (Corresponding Author)

1. Introduction

An endomorphism plays a crucial role to solve many problems not only in algebraic structures [1, 2] but also in many categories [3-5]; especially, in groups [6-9].

Let $\mathbf{G}$ be a group and f be an its endomorphism. As we know that $\ker f^t \subseteq \ker f^{t+1}$ and $f^t G \supseteq f^{t+1}(G)$ for all $t \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$ where f^0 is the identity map. If G is finite, there exist $m, n \in \mathbb{N}_0$ such that $\ker f^m = \ker f^{m+1}$ and $f^n(G) = f^{n+1}(G)$. Such n was studied and known in a monounary algebra [10-12] as the pre-period (or stabilizer) of f , denoted by $\lambda(f)$. We can show by the basic facts (Theorem 4) in group theory that $m = n$. Moreover by Fitting's lemma [13], if $\mathbf{G}$ is abelian, then $\mathbf{G} = \ker f^n \oplus f^n(G)$. It is interesting to study the pre-period of an endomorphism of any finite abelian group.

In the present work, we describe the pre-periods of all endomorphisms of a finite cyclic group by applying some facts in a monounary algebra.

A monounary algebra is an algebra which is extensively studied [14, 15]. There are closed connections between monounary algebras and all algebraic structures. One of the connections is the monounary algebra induced by an endomorphism (see e.g. in [9]). A *monounary algebra* is a set A equipped with a unary operation $f: A \rightarrow A$ and it is denoted by (A, f) . Monounary algebras have the benefit that they are comparatively simple to visualize; especially, they can be represented as digraphs whose vertices are the elements of A with a directed edge from a to $f(a)$ for all $a \in A$. A digraph connecting with group theory has been studied in [16-18] and etc.

The height $ht(A, f)$ of (A, f) where A is finite is mentioned by the means of the height of the digraph via the concepts of the cyclic element and the height $ht(x)$ of element x . Although the height of (A, f) has known and extensively studied (see e.g. in [19, 20]), we will show in Proposition 1 that it is equal to $\lambda(f)$.

The pre-period of a finite algebra was defined in [21, 22] and studied for a finite lattice. In this work, we will study the pre-periods of the cyclic group of order n in the terms of the p -adic valuations $v_p(n)$ of n defined by

$$v_p(n) = \begin{cases} \max\{b \in \mathbb{N}_0 | p^b | n\} & \text{if } n \neq 0, \\ \infty & \text{if } n = 0 \end{cases}$$

for all prime number p .

2. Basic concepts in a monounary algebra

This section will begin with an examination of some fundamental properties of (A, f) where A is finite. For $B \subseteq A$, observe that if $f(B) = B$ then f^1_B is a permutation and so all elements in B are cyclic. Denote

$$C(A, f) := \{x \in A | x \text{ is cyclic}\}.$$

One see that $C(A, f)$ is the maximum subset B of A with $f(B) = B$ as the following proposition which can be proven directly.

Proposition 1: 1Let (A, f) be finite. Then

1. 1 $f(C(A, f)) = C(A, f)$;
2. 2 for each $B \subseteq A$, if $f(B) = B$ then $B \subseteq C(A, f)$;
- 3 $ht(A, f) = \lambda(f)$.

Proof: The statements 1 and 2 can be easy proven. Suppose that $ht(A, f) = n$. Since for each $\alpha \in A$, $f^n(\alpha)$ is cyclic, $f^n(A) \subseteq C(A, f)$. Since $C(A, f) \subseteq A$ and by the statement 1, we get $f^n(A) = f^{n+1}(A) = C(A, f)$. Since $f^{n-1}(\alpha)$ is not cyclic for all $\alpha \in A$ with $ht(\alpha) = n$, the set $f^n(A) = C(A, f)$ is proper of $f^{n-1}(A)$ and so $\lambda(f) = n$.

Proposition 2: 2Let ϕ, φ be unary operations on a finite set A such that $\phi \circ \varphi = \varphi \circ \phi$. Then

$$\lambda(\phi \circ \varphi) \leq \max\{\lambda(\phi), \lambda(\varphi)\}.$$

Proof: Let $m = \max\{\lambda(\phi), \lambda(\varphi)\}$. Then $\phi^m(A) = \phi^{m+1}(A)$ and $\varphi^m(A) = \varphi^{m+1}(A)$. By $\phi \circ \varphi = \varphi \circ \phi$, we get $(\phi \circ \varphi)^m(A) = (\phi \circ \varphi)^{m+1}(A)$ and so, $\lambda(\phi \circ \varphi) \leq m$.

Proposition 3: 3Let A be a finite set and $f: A \rightarrow A$. Then

$$\lambda(f^k) = \left\lceil \frac{\lambda(f)}{k} \right\rceil$$

for all $k \in \mathbb{N}$ where $\lceil x \rceil$ is the ceiling function of a real number x .

Proof: Let $k \in \mathbb{N}$, $t = \lambda(f)$ and $s = \lambda(f^k)$. Observe that $f^r(A) = f^t(A)$ for all nonnegative integers $r \geq t$. Since $t < t + 1 \leq t + k \leq k\left(\left\lceil \frac{t}{k} \right\rceil + 1\right)$, we get

$$\begin{aligned} (f^k)^{\left\lceil \frac{t}{k} \right\rceil}(A) &= f^{k\left\lceil \frac{t}{k} \right\rceil}(A) \\ &= f^t(A) \\ &= (f^k)^{\left\lceil \frac{t}{k} \right\rceil + 1}(A) \end{aligned}$$

which implies $s \leq \left\lceil \frac{t}{k} \right\rceil$. Since

$$\begin{aligned} f^{ks}(A) &= (f^k)^s(A) \\ &= (f^k)^{s+1}(A) \\ &= f^{ks+k}(A), \end{aligned}$$

we have $f^{ks}(A) = f^{ks+1}(A)$ and $t \leq ks$. Hence, $\left\lceil \frac{t}{k} \right\rceil \leq s$.

3. Main results

Theorem 4: 4Let G be a finite group and f be an its endomorphism. Then

$$\ker f^n = \ker f^{n+1} \text{ if and only if } f^n(G) = f^{n+1}(G)$$

for all $n \in \mathbb{N} \cup \{0\}$. Moreover,

$$\lambda(f) = \min\{n \in \mathbb{N} \cup \{0\} \mid \ker f^n = \ker f^{n+1}\}.$$

Proof: Let $n \in \mathbb{N} \cup \{0\}$.

($\Rightarrow$) It is clear by the First Isomorphism Theorem.

($\Leftarrow$) Assume that $f^n(G) = f^{n+1}(G)$. Observe that $\ker f^n \subseteq \ker f^{n+1}$. Since G is finite, the Isomorphism Theorem and Lagrange's Theorem imply $|\ker f^n| = |\ker f^{n+1}|$. Hence, $\ker f^n = \ker f^{n+1}$.

As we know, an n -element cyclic group is the group $\mathbb{Z}_n$ of integers modulo n under the additive operation. It is clear that for each $m \in \mathbb{Z}$, the operation $f_m: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ defined by

$$f_m(\bar{x}) = \overline{mx}$$

for all $\bar{x} \in \mathbb{Z}_n$ is an endomorphism of $\mathbb{Z}_n$; moreover, $f_m = f_i$ for some $1 \leq i \leq n$. It is easy to see that all endomorphisms of $\mathbb{Z}_n$ are exactly $f_1, \dots, f_n$ and $f_m \circ f_k = f_{mk}$ for all $m, k \in \mathbb{Z}$.

Lemma 5: 5 Let $n \in \mathbb{N}$. Then

1. 3 all endomorphisms of $\mathbb{Z}_n$ are exactly $f_1, \dots, f_n$ and
2. 4 the set of all endomorphisms of $\mathbb{Z}_n$ is a commutative monoid under the composition; moreover, $f_m \circ f_k = f_{mk}$ for all $m, k \in \mathbb{Z}$.

Remark 1: 6 For each $m, n \in \mathbb{Z}$, $k \in \mathbb{N} \cup \{0\}$ and prime number p , one can see that $v_p(mn) = v_p(m) + v_p(n)$ and if $n \neq 0$ then $v_p(n^k) = kv_p(n)$.

Corollary 6: 7 Let $n, m \in \mathbb{N}$. Then

$$\lambda(f_m) \leq \max \left\{ \left\lceil \frac{\lambda(f_p)}{v_p(m)} \right\rceil \mid p \text{ is prime and } p \mid m \right\}.$$

Proof: Suppose that $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ for some $k \in \mathbb{N}$, $a_1, a_2, \dots, a_k \in \mathbb{N}$ and prime numbers $p_1, p_2, \dots, p_k$. Then $v_{p_i}(m) = a_i$ for all $1 \leq i \leq k$. By Proposition 2, Proposition 3 and Lemma 5 (2),

$$\begin{aligned} \lambda(f_{p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}}) &= \lambda(f_{p_1}^{a_1} \circ f_{p_2}^{a_2} \circ \dots \circ f_{p_k}^{a_k}) \\ &\leq \max \left\{ \left\lceil \frac{\lambda(f_{p_i})}{a_i} \right\rceil \mid 1 \leq i \leq k \right\}. \end{aligned}$$

Lemma 7: 8 Let $n, m \in \mathbb{N}$ and $d = \gcd(m, n)$. Then $\bar{0}, \frac{\bar{n}}{d}, \frac{2\bar{n}}{d}, \dots, \frac{(d-1)\bar{n}}{d}$ are all distinct elements in $\ker f_m$.

Proof: For each $0 \leq r \leq d-1$, we see that

$$f_m\left(\frac{rn}{d}\right) = m\left(\frac{rn}{d}\right) = n\left(\frac{rm}{d}\right) = \bar{0}$$

and for each $0 \leq s \leq d-1$, if $\frac{\overline{rn}}{d} = \frac{\overline{sn}}{d}$, then $d|r-s$ which implies by $1-d \leq r-s \leq d-1$ that $r=s$. Hence, the elements $\overline{0}, \frac{\overline{n}}{d}, \frac{\overline{2n}}{d}, \dots, \frac{\overline{(d-1)n}}{d}$ are distinct in $\ker f_m$. Assume that $\overline{x} \in \ker f_m$. Then $n|mx$ and $x = \frac{n}{d}a$ for some $a \in \mathbb{Z}$. By Division Algorithm,

$$x = \frac{n}{d}(dq+r) = nd + \frac{n}{d}r$$

for some $q, r \in \mathbb{Z}$ with $0 \leq r \leq d-1$.

Theorem 8: 9 Let $n, m \in \mathbb{N}$. Then

$$\lambda(f_m) = \max \left\{ \left\lfloor \frac{v_p(n)}{v_p(m)} \right\rfloor \mid p \text{ is prime and } p|m \right\}.$$

Proof: Let p be prime and $p|m$. Suppose that $a = v_p(m)$ and $b = v_p(n)$. By Lemma 7, $|\ker f_p^i| = |\ker f_{p^i}| = \gcd(n, p^i)$ for all $i \in \mathbb{N} \cup \{0\}$. Hence, if $i \leq b$, then $|\ker f_p^i| = p^i$ and if $i > b$, then $|\ker f_p^i| = p^b$. These imply by Theorem 4 that $\lambda(f_p) = b$. We will show that $\lambda(f_m) \geq \left\lfloor \frac{b}{a} \right\rfloor$. It is clear if $b=0$. Suppose that $b \in \mathbb{N}$. By $b \leq a \left\lfloor \frac{b}{a} \right\rfloor$, we get $p^b | p^{a \left\lfloor \frac{b}{a} \right\rfloor}$ and by $p^a | m$, $p^{a \left\lfloor \frac{b}{a} \right\rfloor} | m^{\left\lfloor \frac{b}{a} \right\rfloor}$ which imply that $p^b | m^{\left\lfloor \frac{b}{a} \right\rfloor}$. Since p^b is a divisor of n , $\frac{n}{p^b} \in \mathbb{N}$ and

$$f_m^{\left\lfloor \frac{b}{a} \right\rfloor} \left(\overline{\frac{n}{p^b}} \right) = \overline{m^{\left\lfloor \frac{b}{a} \right\rfloor} \frac{n}{p^b}} = \overline{0}.$$

Hence, $\frac{\overline{n}}{p^b} \in \ker f_m^{\left\lfloor \frac{b}{a} \right\rfloor}$. Observe that

$$v_p \left(m^{\left\lfloor \frac{b}{a} \right\rfloor - 1} \right) = \left(\left\lfloor \frac{b}{a} \right\rfloor - 1 \right) v_p(m) = \left(\left\lfloor \frac{b}{a} \right\rfloor - 1 \right) a.$$

Since $\left\lfloor \frac{b}{a} \right\rfloor < \frac{b}{a} + 1$, we get $a \left(\left\lfloor \frac{b}{a} \right\rfloor - 1 \right) < b$ and $p^b m^{\left\lfloor \frac{b}{a} \right\rfloor - 1}$. So, $nm^{\left\lfloor \frac{b}{a} \right\rfloor - 1} \frac{n}{p^b}$ which implies that

$$f_m^{\left\lfloor \frac{b}{a} \right\rfloor - 1} \left(\overline{\frac{n}{p^b}} \right) = \overline{m^{\left\lfloor \frac{b}{a} \right\rfloor - 1} \frac{n}{p^b}} \neq \overline{0}.$$

Thus $\ker f_m^{\left\lfloor \frac{b}{a} \right\rfloor - 1} \subsetneq \ker f_m^{\left\lfloor \frac{b}{a} \right\rfloor}$. By Theorem 4, $\lambda(f_m) \geq \left\lfloor \frac{b}{a} \right\rfloor$. Since p is arbitrary such that p is prime with $p|m$ and by Corollary 6, the proof is complete.

Corollary 9: 10 For each $n \in \mathbb{N}$, the pre-period $\lambda(\mathbb{Z}_n)$ of the cyclic group $\mathbb{Z}_n$ of order n is $\max\{v_p(n) \mid p \text{ is prime and } p|n\}$.

Proof: Let $n, m \in \mathbb{N}$ and p be prime that $p|m$ and $\lambda(f_m) = \left\lfloor \frac{v_p(n)}{v_p(m)} \right\rfloor$. Then $\lambda(f_m) \leq v_p(n)$. If $p \nmid n$, then $\lambda(f_m) = \left\lfloor \frac{0}{v_p(m)} \right\rfloor = 0$; and if $p|n$, we are done. And by Theorem 8, the proof is complete.

Acknowledgment

This research project is supported by Rajamangala University of Technology Isan. Contract No. ENG 13/67.

References

- [1] G. Fang and J. Fang, "The strong endomorphism kernel property in distributive p-algebras," *Southeast Asian Bulletin of Mathematics*, vol. 37, no. 4 (2013).
- [2] Y. Susanti and J. Koppitz, "On endomorphisms of power-semi-groups," *Asian-European Journal of Mathematics*, vol. 10, no. 03, p. 1750058 (2017).
- [3] M. Böttcher and U. Knauer, "Endomorphism spectra of graphs," *Discrete Mathematics*, vol. 109, no. 1-3, pp. 45--57 (1992).
- [4] U. Knauer, "Endomorphism types of trees," *Words, Languages, and Combinatorics*, *World Scientific, Singapore*, pp. 273-287 (1992).
- [5] K. Grant, R. Nowakowski, and I. Rival, "The endomorphism spectrum of an ordered set," *Order*, vol. 12, pp. 45-55 (1995).
- [6] J. Konieczny, "Automorphism groups of endomorphism monoids of free g-sets," *Asian-European Journal of Mathematics*, vol. 7, no. 01, p. 1450015 (2014).
- [7] H. Ghumashyan and J. Gurić an, "Endomorphism kernel property for finite groups," *Mathematica Bohemica*, vol. 147, no. 3, pp. 347-358 (2022).
- [8] J. Fang and Z. J. Sun, "Finite abelian groups with the strong endomorphism kernel property," *Acta Mathematica Sinica, English Series*, vol. 36, pp. 1076-1082 (2020).
- [9] M. Sha, "Digraphs from endomorphisms of finite cyclic groups," *J. Combin. Math. Combin. Comp*, vol. 83, p. 105-120 (2012).
- [10] K. Denecke and C. Ratanaprasert, "N-ary operations with long pre-periods," *Asian-European Journal of Mathematics*, vol. 2, no. 02, pp. 201-212 (2009).

- [11] C. Ratanaprasert and K. Denecke, "Unary operations with long pre-periods," *Discrete Mathematics*, vol. 308, pp. 4998-5005 (2008).
- [12] D. Zupnik, "Cayley functions," in *Semigroup Forum*, vol. 3, pp. 349-358 (1971).
- [13] N. Jacobson, "Basic algebra ii: Second edition, (2009).
- [14] E. Halušková, "Strong endomorphism kernel property for monounary algebras," *Mathematica Bohemica*, vol. 143, no. 2, pp. 161-171 (2018).
- [15] I. Pozdnyakova, "Semigroups of endomorphisms of some infinite monounary algebras," *Journal of Mathematical Sciences*, vol. 190, no. 5, pp. 658--668 (2013).
- [16] U. Ahmad, "The power digraphs associated with generalized dihedral groups," *Discrete Mathematics, Algorithms and Applications*, vol. 7, no. 04, p. 1550057 (2015).
- [17] E. Brown, "Directed graphs defined by arithmetic (mod n)," *Fibonacci Quarterly*, vol. 35, pp. 346-351 (1997).
- [18] M. H. Mateen, M. K. Mahmmod, D. Alghazzawi, and J.-B. Liu, "Structures of power digraphs over the congruence equation $x^p \equiv y \pmod{m}$ and enumerations," *AIMS Math*, vol. 6, no. 5, pp. 4581-4596 (2021).
- [19] U. Ahmad and H. Syed, "On the heights of power digraphs modulo n ," *Czechoslovak mathematical journal*, vol. 62, pp. 541--556 (2012).
- [20] D. Jakubikova-Studenovska and J. Pócs, *Monounary algebras* (2009).
- [21] A. Charoenpol and U. Chotwattakawanit, "The pre-period of the glued sum of finite modular lattices." *Discussiones Mathematicae: General Algebra & Applications*, vol. 43, no. 2, pp. 223-231 (2023).
- [22] A. Charoenpol and U. Chotwattakawanit, "The maximum pre-period property of the direct product of chains," *Asian-European Journal of Mathematics*, vol. 16, no. 09, p. 2350155 (2023).

Received November, 2024