ไดกราฟของการส่งกำลังเคบนริงสลับที่จำกัดบางริง

นายอิทธิวัฒน์ โตเจริญนิรัติศัย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรดุษฎีบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2558

DIGRAPHS OF THE kTH POWER MAPPING OVER SOME FINITE COMMUTATIVE RINGS

Mr. Ittiwat Tocharoennirattisai

A Dissertation Submitted in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosophy of Science Program in Mathematics

Department of Mathematics and Computer Science

Faculty of Science

Chulalongkorn University

Academic Year 2015

Thesis Title	DIGRAPHS OF THE kTH POWER MAPPING OVER SOME FINITE COMMUTATIVE RINGS
By	Mr. Ittiwat Tocharoenirattisai
Field of Study	Mathematics
Thesis Advisor	Associate Professor Yotsanan Meemark, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Doctoral Degree

.... Dean of the Faculty of Science

(Associate Professor Polkit Sangvanich, Ph.D.)

THESIS COMMITTEE

.... Chairman

(Associate Professor Ajchara Harnchoowong, Ph.D.)

.... Thesis Advisor

(Associate Professor Yotsanan Meemark, Ph.D.)

.... Examiner

(Assistant Professor Tuangrat Chaichana, Ph.D.)

.... Examiner

(Assistant Professor Ouamporn Phuksuwan, Ph.D.)

.... External Examiner

(Associate Professor Nittiya Pabhapote, Ph.D.)

อิทธิวัฒน์ โตเจริญนิรัติศัย : ไดกราฟของการส่งกำลังเคบนริงสลับที่จำกัดบางริง. (DIGRAPHS OF THE kTH POWER MAPPING OVER SOME FINITE COMMUTATIVE RINGS) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: รศ.ดร.ยศนันต์ มีมาก, 46 หน้า.

ดุษฎีนิพนธ์นี้พิจารณาภาคขยายเฉพาะที่ของริงกาลัวในรูป $GR(p^n,d)[x]/(f(x)^a)$, โดยที่ n, d และ a เป็นจำนวนเต็มบวก p เป็นจำนวนเฉพาะ และ $f(x)$ เป็นพหุนามโมนิกใน $GR(p^n,d)[x]$ ที่มีลำดับขั้นเป็น r ซึ่ง $\overline{f}(x)$ ใน $\mathrm{F}_{p^d}[x]$ เป็นพหุนามลดทอนไม่ได้ เราคำนวณเลขชี้กำลังของ R โดยไม่อาศัยโครงสร้างของกรุปยูนิตของ R และเราวิเคราะห์ไดกราฟ $G^{(k)}(R)$ ซึ่งเกิดจากการส่งกำลัง k ได้ดีขึ้นพร้อมทั้งได้เงื่อนไขของการเป็นไดกราฟสมมาตร นอกจากนี้เราศึกษาไดกราฟเหนือริงลูกโซ่จำกัด R ซึ่งโครงสร้างของ $G_2^{(k)}(R)$ เช่น $\mathrm{indeg}^{(k)}\ 0$ และระยะทางไกลสุดสำหรับ $G_2^{(k)}(R)$ จะเป็นผลที่ได้จากนิรพลของไอดีลใหญ่สุดเฉพาะกลุ่ม M ของ R

ภาควิชา คณิตศาสตร์และ วิทยาการคอมพิวเตอร์ ลายมือชื่อนิสิต ....

ลายมือชื่อ อ. ที่ปรึกษาหลัก..

สาขาวิชา.........คณิตศาสตร์........................

ปีการศึกษา..........2558..........................

5472869723 : MAJOR MATHEMATICS

KEYWORDS : kTH POWER MAPPING / LOCAL RINGS / SYMMETRIC DIGRAPHS

ITTIWAT TOCHAROENNIRATTISAI : DIGRAPHS OF THE kTH POWER MAPPING OVER SOME FINITE COMMUTATIVE RINGS. ADVISOR : ASSOC. PROF. YOTSANAN MEEMARK, Ph.D., 46 pp.

In this dissertation, we consider a local extension R of the Galois ring of the form

$$GR(p^n, d)[x]/(f(x)^a),$$

where n, d and a are positive integers, p is a prime and $f(x)$ is a monic polynomial in $GR(p^n, d)[x]$ of degree r such that the reduction $\overline{f}(x)$ in $\mathbb{F}_{p^d}[x]$ is irreducible. We establish the exponent of R without completely determination of its unit group structure. We obtain better analysis of the iteration graphs $G^{(k)}(R)$ induced from the kth power mapping including the conditions on symmetric digraphs. In addition, we work on the digraph over a finite chain ring R. The structure of $G_2^{(k)}(R)$ such as $\text{indeg}^{(k)}\,0$ and maximum distance for $G_2^{(k)}(R)$ is determined by the nilpotency of maximal ideal M of R.

Department : ....Mathematics.... Student's Signature : ....

..and Computer Science..

Field of Study : ....Mathematics.... Advisor's Signature : ....

Academic Year : ....2015...........

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to Associate Professor Dr. Yotsanan Meemark, my thesis advisor, for motivation and encouragement to accomplish this thesis. I also wish to thank the Science Achievement Scholarship of Thailand, SAST, which supports me during my undergraduate and graduate studies. Next, I expresses my gratitude to the Graduate School of Chulalongkorn University which gave me an opportunity to present my research at the Fq12 conference last year. Moreover, I would also like to express my appreciation to my thesis committee: Associate Professor Dr. Ajchara Harnchoowong, the chairman, Assistant Professor Dr. Tuangrat Chaichana, Assistant Professor Dr. Ouamporn Phuksuwan, and Associate Professor Dr. Nittiya Pabhapote, for their valuable comments and suggestions.

Finally, I would like to express my greatly gratitude to my family for their love and encouragement during my study.

CONTENTS

page

CHAPTER I

INTRODUCTION

1.1 Digraph of the kth power mapping

Let R be a finite commutative ring with identity $1 \neq 0$. For an integer $k \geq 2$, the **kth power mapping digraph over** R, denoted by $G^{(k)}(R)$, is the digraph whose vertex set is R and there is a directed edge from a to b if and only if $a^k = b$.

A **component** of a digraph is a subdigraph which is a maximal connected subgraph of the associated nondirected graph. We consider two disjoint subdigraphs $G_1^{(k)}(R)$ and $G_2^{(k)}(R)$ of $G^{(k)}(R)$ induced on the set of vertices which are in the unit group $R^\times$ and induced on the remaining vertices which are not invertible, respectively. They are called the **unit subdigraph** and the **zero divisor subdigraph**, respectively. Observe that there are no edges between $G_1^{(k)}(R)$ and $G_2^{(k)}(R)$, that is, $G^{(k)}(R) = G_1^{(k)}(R) \mathbin{\dot{\cup}} G_2^{(k)}(R)$.

A cycle of length $t \geq 1$ is said to be a **t-cycle** and we assume that all cycles are oriented counterclockwise. We call a cycle of length one a **fixed point**. The **distance** from a vertex $g \in R$ to a cycle is the length of the directed path from g to a vertex in the cycle.

The **indegree** (respectively, **outdegree**) of a vertex $a \in R$ of $G^{(k)}(R)$, is the number of directed edges entering (respectively, leaving) to a, and denoted by

$\operatorname{indeg}^{(k)} a$ (respectively, $\operatorname{outdeg}^{(k)} a$). The definition of $G^{(k)}(R)$ implies that the outdegree of each vertex is equal to 1. This result implies the next result that each component of the digraph $G^{(k)}(R)$ has exactly one cycle.

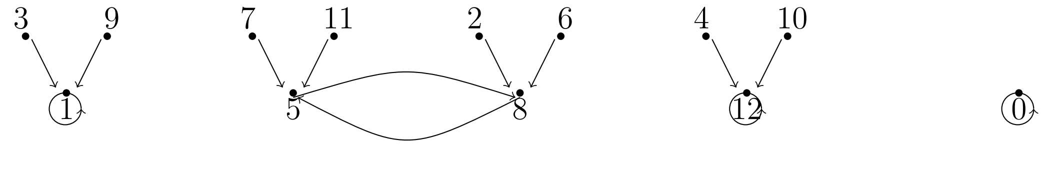
Theorem 1.1.1. *Let R be a finite commutative ring with identity, and let $k \geq 2$. Each component of the digraph $G^{(k)}(R)$ has exactly one cycle. Therefore, the number of components of this digraph is equal to the number of its cycles.*

Proof. Let g be a vertex in a component C of $G^{(k)}(R)$. Consider

$$g \to g^k \to g^{k^2} \to \cdots \to g^{k^i} \cdots .$$

If there is no cycle, then the above path is infinite, contradicting the finiteness of R. Thus, C contains a cycle. Moreover, if C has more than one cycle, then there is a vertex with outdegree greater than one, which is impossible. Hence, each component contains exactly one cycle. □

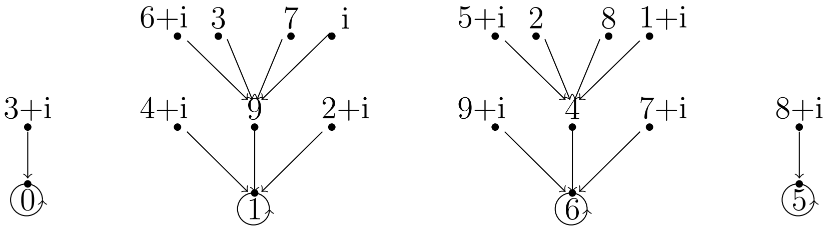
Example 1.1.2. Consider the digraph $G^{(3)}(\mathbb{Z}_{13})$.



$G_1^{(3)}(\mathbb{Z}_{13})$ $G_2^{(3)}(\mathbb{Z}_{13})$

We see that the digraph $G^{(3)}(\mathbb{Z}_{13})$ contains three components for $G_1^{(3)}(\mathbb{Z}_{13})$ and one component for $G_2^{(3)}(\mathbb{Z}_{13})$. This digraph has three fixed points and one 2-cycle. Moreover, $\operatorname{indeg}^{(3)} 1 = \operatorname{indeg}^{(3)} 5 = \operatorname{indeg}^{(3)} 8 = \operatorname{indeg}^{(3)} 12 = 3$, $\operatorname{indeg}^{(3)} 0 = 1$ and the indegree of the other vettices is 0.

Example 1.1.3. (Example 3 in Section 5 of [7]) Consider the digraph $G^{(2)}(\mathbb{Z}[i]/(2+4i))$.



We see that the digraph $G^{(2)}(\mathbb{Z}[i]/(2+4i))$ contains four fixed points. Moreover, this digraph is symmetric (see definition in Chapter IV) of order 2.

For a finite commutative ring R with identity and $a \in R$, the component of $G^{(k)}(R)$ containing a is denoted by $\mathrm{Com}(a)$.

The kth power mapping digraph is defined by using the idea of Somer and Křížek [5] who studied the structure of digraphs $G^{(2)}(\mathbb{Z}_n)$. Later, they worked on the kth power mapping digraph $G^{(k)}(\mathbb{Z}_n)$ [6]. Y. Meemark and N. Wiroonsri ([10, 11], respectively) worked on digraphs $G^{(2)}(\mathbb{F}_{p^n}[x]/(f(x)))$ and $G^{(k)}(\mathbb{F}_{p^n}[x]/(f(x)))$, respectively, where $f(x)$ is a monic polynomial of degree ≥ 1 in $\mathbb{F}_{p^n}[x]$, where $\mathbb{F}_{p^n}$ is the field with p^n elements and gave some conditions for symmetric digraphs. Again, Y. Meemark and N. Maingam [7] studied the digraphs $G^{(2)}(\mathbb{Z}[i]/(\gamma))$, where $\mathbb{Z}[i]$ is the ring of Gaussian integers and $\gamma = a + bi$ be a nonzero element in $\mathbb{Z}[i]$. Next, Y.J. Wei, G.H. Tang, H.D. Su [13] considered the digraphs $G^{(2)}(R)$, where R is a finite commutative ring with identity and determined the structure of R when the digraphs have only two, three and four components. Later, Y.J. Wei, G.H. Tang, J.H. Nan [12] investigated the structure of digraphs $G^{(k)}(\mathbb{F}_{p^r}C_n)$ for the group ring $\mathbb{F}_{p^r}C_n$, where $\mathbb{F}_{p^r}$ is a field with p^r elements, and C_n is a cyclic group of order n. They explained some conditions for symmetric digraphs. G. Deng, L. Somer [3] worked on the digraphs $G^{(k)}(R)$, where R is a finite commutative ring of characteristic p. Recently, Y.J. Wei and G.H. Tang [14] generalized the results on cycles, components and semiregularity to finite commutative rings. They also continued working more on symmetric digraphs.

1.2 Exponent

Let G be a finite group. The **exponent** of G, denoted by $\exp G$, is the least positive integer n such that $g^n = e$ for all $g \in G$. For example, $\exp \mathbb{Z}_n = n$ and $\exp S_4 = 12$. It gives some information on the order of an element of G. The exponent plays the role of universal order for a group. Note that $\exp G$ divides $|G|$ When G is abelian, the exponent of G also serves as an important tool to explore deeper into its Sylow p-subgroup which results in the structure theorem for finite abelian groups. We briefly discuss some properties of exponent of a group in the following theorem.

Theorem 1.2.1. (Theorem 1.1 of [7]) *Let G be a finite group and H a subgroup of G.*

(1) $\exp G = \operatorname{lcm}\{o(a) : a \in G\}$, *where $o(a)$ is the order of a in G.*

(2) $\exp H$ *divides* $\exp G$.

(3) *If $G = G_1 \times G_2$, then* $\exp G = \operatorname{lcm}\{\exp G_1, \exp G_2\}$.

(4) *If G is abelian, then there exists an element g in G such that $o(g) = \exp G$.*

Proof. (1)–(3) are clear. To prove (4), assume that G is abelian. By the elementary divisor theorem, there exist positive integers $n_1, n_2, \dots, n_t \geq 1$ such that $n_1 \mid n_2 \mid \cdots \mid n_t$ and

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t}.$$

Thus, $\exp G = n_t$ and $(0, 0, \dots, 0, 1)$ in the rightmost group has order n_t. □

For a finite commutative ring R with identity, its **exponent** is defined to be the exponent of the group of units of R. We write $\lambda(R)$ for the exponent of R and $R^\times$ for the group of units of R. That is, $\lambda(R) = \exp(R^\times)$. For example, $\lambda(\mathbb{Z}_{12}) = \exp(\mathbb{Z}_{12}^\times) = 2$. We can easily determine the exponent of R if the structure of the group of units is known, such as when R is the ring of integers modulo m, finite fields, Galois rings, and finite chain rings. The exponent of the ring of integers modulo m is also known as the Carmichael λ-function [5, 6], which is defined by a modification of the Euler's φ-function as follows:

(1) $\lambda(1) = 1 = \varphi(1)$, $\lambda(2) = 1 = \varphi(2)$, $\lambda(4) = 2 = \varphi(4)$.

(2) $\lambda(2^k) = 2^{k-2} = \frac{1}{2}\varphi(2^k)$, for $k \geq 3$.

(3) $\lambda(p^k) = (p-1)p^{k-1} = \varphi(p^k)$, for any odd prime p and $k \geq 1$.

(4) $\lambda(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = \operatorname{lcm}(\lambda(p_1^{k_1}), \lambda(p_2^{k_2}), \dots, \lambda(p_r^{k_r}))$, where $p_1, p_2, \dots, p_r$ are distinct primes and $k_i \geq 1$ for $i \in \{1, \dots, r\}$.

The exponent of the quotient rings over the Gaussian integers is completely determined in the next theorem.

Theorem 1.2.2. (Lemma 2.2 and Proposition 2.3 of [7])

(1) *Up to multiplication by units, the primes in $\mathbb{Z}[i]$ are of three types.*

(a) *p, where p is a prime in $\mathbb{Z}$ satisfying $p \equiv 1 \pmod 4$.*

(b) *π or $\bar{\pi}$, where $q = \pi\bar{\pi}$ is a prime in $\mathbb{Z}$ satisfying $q \equiv 1 \pmod 4$.*

(c) *$\alpha = 1 + i$.*

(2) *Let p and q be positive primes in $\mathbb{Z}$ satisfying $p \equiv 3 \pmod 4$, and $q \equiv 1 \pmod 4$, π denote a prime factor of q in $\mathbb{Z}[i]$, and $\alpha = 1 + i$. Then:*

(a) *$\lambda(\pi^n) = |(\mathbb{Z}[i]/(\pi^n))^\times| = q^{n-1}(q-1)$ for all positive integers n.*

(b) *$\lambda(p^n) = \frac{1}{p^{n-1}}|(\mathbb{Z}[i]/(p^n))^\times| = p^{n-1}(p^2-1)$ for all positive integers n.*

(c) *$\lambda(\alpha^j) = |(\mathbb{Z}[i]/(\alpha^j))^\times| = 2^{j-1}$ for $j \in \{1,2,3\}$, $\lambda(\alpha^4) = \frac{1}{2}|(\mathbb{Z}[i]/(\alpha^4))^\times| = 4$, $\lambda(\alpha^5) = \frac{1}{4}|(\mathbb{Z}[i]/(\alpha^5))^\times| = 4$, and*

$$\lambda(\alpha^n) = \begin{cases} \frac{1}{2^m}|(\mathbb{Z}[i]/(\alpha^n))^\times| = 2^{m-1}, & \text{if } n = 2m; \\ \frac{1}{2^{m+1}}|(\mathbb{Z}[i]/(\alpha^n))^\times| = 2^{m-1}, & \text{if } n = 2m+1, \end{cases}$$

for all $n \geq 6$.

(d) *$\lambda(\sigma_1^{j_1}\sigma_2^{j_2}\ldots\sigma_s^{j_s}) = \operatorname{lcm}(\lambda(\sigma_1^{j_1}), \lambda(\sigma_2^{j_2}), \ldots, \lambda(\sigma_s^{j_s}))$, where $\sigma_1, \sigma_2, \ldots, \sigma_s$ are distinct primes in $\mathbb{Z}[i]$ for $j_l \geq 1$ and $l \in \{1, 2, \ldots, s\}$.*

1.3 Local rings and Galois rings

A **local ring** is a commutative ring with identity which has a unique maximal ideal. Note that for a local ring R, its unique maximal ideal is given by

$M = R \smallsetminus R^{\times}$ (Proposition 1.2.11 of [1]) and we call the field R/M, **the residue field of** R.

For example, $\mathbb{Z}_{p^n}$, where p is a prime and $n \in \mathbb{N}$, is a local ring with unique maximal ideal $p\mathbb{Z}_{p^n}$ and residue field $\mathbb{Z}_{p^n}/p\mathbb{Z}_{p^n} \cong \mathbb{Z}_p$. Moreover, every field is a local ring with maximal ideal $\{0\}$.

We recall some properties of a finite local ring in the next theorem.

Theorem 1.3.1. (Theorem 6.1.2 of [1] and Theorem XVIII.2 of [8]) *Let R be a finite local ring with unique maximal ideal M. Then*

(1) $|R| = p^{nr}$ *and* $|M| = p^{(n-1)r}$, *for some prime p and some $n, r \in \mathbb{N}$.*

(2) $M^n = \{0\}$. *Moreover, for the least positive integer s such that $M^s = \{0\}$, it is called the* ***nilpotency of*** M.

(3) $R^{\times} \cong (1 + M) \times (R/M)^{\times}$.

Next, let n, d be positive integers and p a prime. Then there exists a monic polynomial $g(t)$ in $\mathbb{Z}_{p^n}[t]$ of degree d such that the reduction $\overline{g}(t)$ in $\mathbb{Z}_p[t]$ is irreducible (Theorem 13.9 of [15]). Consider the ring extension $\mathbb{Z}_{p^n}[t]/(g(t))$ of $\mathbb{Z}_{p^n}$. This is given by

$$\{a_0 + a_1 t + \cdots + a_{d-1}t^{d-1} + (g(t)) : a_i \in \mathbb{Z}_{p^n} \text{ for all } i \in \{0, 1, \ldots, d-1\}\}.$$

It is called a **Galois extension** of $\mathbb{Z}_{p^n}$.

Theorem 1.3.2. (Theorem 5.1.8 of [1]) *Up to isomorphism the Galois extension with parameters n, d and p is unique.*

Hence, we may denote $\mathbb{Z}_{p^n}[t]/(g(t))$ by $GR(p^n,d)$, and call it the **Galois ring**. Observe that $GR(p^n,1)=\mathbb{Z}_{p^n}$ and $GR(p,d)=\mathbb{F}_{p^d}$, the field of p^d elements.

We record some properties of $GR(p^n,d)$ in the next theorem.

Theorem 1.3.3. (Section 6.2 of [1]) *Let n, d be positive integers and p a prime. Let $g(t)\in\mathbb{Z}_{p^n}[t]$ be a monic polynomial of degree d such that the reduction $\overline{g}(t)$ in $\mathbb{Z}_p[t]$ is irreducible. Let $R=GR(p^n,d)=\mathbb{Z}_{p^n}[t]/(g(t))$. Then*

(1) *R is a finite local ring of order p^{nd} with maximal ideal $M=p(\mathbb{Z}_{p^n}[t]/(g(t)))$, which is principal, and residue field $R/M\cong\mathbb{F}_{p^d}$. Moreover, the characteristic of R is p^n.*

(2) *The unit group $R^\times$ consists of cosets $a_0+a_1t+\cdots+a_{d-1}t^{d-1}+(g(t))$, where $a_i\in\mathbb{Z}_{p^n}$ for all $i\in\{0,1,\ldots,d-1\}$ and $p\nmid a_i$ for some $i\in\{0,1,\ldots,d-1\}$.*

An extension ring R of a local ring S is called a **local extension** if R is a local ring. Hence, the Galois ring $GR(p^n,d)$ is a local extension of $\mathbb{Z}_{p^n}$.

The structure of the unit group of $GR(p^n,d)$ is well studied and presented with its exponent below.

Theorem 1.3.4. (Theorem XVI.9 of [8]) *The unit group $GR(p^n,d)^\times\cong H\times\mathbb{F}_{p^d}^\times$, where H is a group of order $p^{(n-1)d}$ such that:*

(1) *If (p is odd) or ($p=2$ and $n\leq 2$), then H is a direct product of d cyclic groups each of order p^{n-1}, and so the exponent of $GR(p^n,d)$ in this case is $p^{n-1}(p^d-1)$.*

(2) *If $p=2$ and $n\geq 3$, then H is a direct product of a cyclic group of order 2, a cyclic group of order 2^{n-2} and $d-1$ cyclic groups each of order 2^{n-1}, and*

so the exponent of $GR(2^n, d)$ in this case is $2^{n-1}(2^d - 1)$ for $d \geq 2$ and 2^{n-2} for $d = 1$, respectively.

1.4 Finite chain rings

A **finite chain ring** R is a finite commutative ring with identity such that for any two ideals I and J of R, we have $I \subseteq J$ or $J \subseteq I$. For example, for a prime p and $n \in \mathbb{N}$, $\mathbb{Z}_{p^n}$ is a finite chain ring and all ideals form the chain

$$\{0\} \subsetneq p^{n-1}\mathbb{Z}_{p^n} \subsetneq \cdots \subsetneq p\mathbb{Z}_{p^n} \subsetneq \mathbb{Z}_{p^n}.$$

Moreover, the nilpotency of $p\mathbb{Z}_{p^n}$ is n.

It can be shown that (Section XVII of [8]) a finite chain ring is a finite local ring with maximal principal ideal. Thus, a Galois ring is a finite chain ring.

Example 1.4.1. The ring $\mathbb{F}_{2^2}[x]/((x+3)^2)$ is a finite chain ring (maximal ideal $(x+3)/(x+3)^2)$, but it is not a Galois ring.

We recall the characterization of a finite chain ring in the next theorem.

Theorem 1.4.2. (Theorem XVII.5 of [8]) *Let R be a finite chain ring with unique maximal ideal M with nilpotency s, and residue field $R/M \cong \mathbb{F}_{p^d}$. Then a finite chain ring R is isomorphic to an extension ring*

$$GR(p^n, d)[x]/(z(x), p^{n-1}x^{s-(n-1)e})$$

*for some positive integers n, e, and $z(x) = x^e + p(a_{e-1}x^{e-1} + \cdots + a_0)$, $a_0 \in GR(p^n, d)^{\times}$, $a_1, \cdots, a_{e-1} \in GR(p^n, d)$, called an **Eisenstein polynomial of***

degree *e. Furthermore, $|R| = p^{ds}$, $|M| = p^{d(s-1)}$ and R is a local extension of $GR(p^n, d)$.*

Moreover, the group of units of a finite chain ring is explicitly determined by Hou et al. [4]. (The results are complicated and consist of several cases and many new symbols, so they are not included in this dissertation.) Therefore, the exponent of a finite chain ring is known. Recently, Chen et al. [2] studied the structure of the Gauss extension of a Galois ring and its unit group.

Besides the characteristic of the unit group, the exponent of the ring can be used to study the digraph of the kth power mapping [3, 7, 10, 11]. This motivated Dang and Somer [3] to compute without the explicit structure of the unit group, the exponent of the quotient ring $\mathbb{F}_q[x]/(f(x)^a)$, where $a \geq 1$, $\mathbb{F}_q$ is the field of q elements and $f(x)$ is a monic irreducible polynomial in $\mathbb{F}_q[x]$.

A deeper result for local ring extensions is as follows.

Theorem 1.4.3. (Corollary 4.3.3 of [1]) *Let R be a finite local ring, and $f(x)$ be a monic irreducible polynomial in $R[x]$. Then $R[x]/(f(x)^a)$ is a finite local ring for any positive integer a.*

In this dissertation, we consider a local extension R of the Galois ring $GR(p^n, d)$ of the form

$$GR(p^n, d)[x]/(f(x)^a),$$

where $a \geq 1$ and $f(x)$ is a monic polynomial in $GR(p^n, d)[x]$ of degree r such that the reduction $\overline{f}(x)$ in $\mathbb{F}_{p^d}[x]$ is irreducible. We compute the exponent of R without completely determination of its group structure in Chapter II. In Chapter III, we study the existence of a t-cycle and the number of t-cycles in $G_1^{(k)}(R)$ where R is a finite commutative ring with identity. Moreover, in Section 3.2, the maximum distance from any vertex to the unique cycle in the component of the digraph $G_1^{(k)}(R)$ and the trees attached to it are determined. Furthermore, we investigate indegree of 0 and the maximum distance from any vertex to the fixed point 0 in $G_2^{(k)}(R)$ for a finite chain ring R. For Chapter IV, we discuss semiregular digraphs and determine the indegree of any vertex in $R^{\times}$ in Section 4.1. Then, in Section 4.2, we work on symmetric digraphs. The final chapter gives five examples of the kth power mapping digraphs demonstrating the results in the previous chapters. The work in this dissertation will appear in Turkish Journal of Mathematics [9].

CHAPTER II

EXPONENT OF $GR(p^n, d)[x]/(f(x)^a)$

In this chapter, we compute the exponent of the local extension R of the Galois ring $GR(p^n, d)$ of the form

$$GR(p^n, d)[x]/(f(x)^a),$$

where $a \geq 1$ and $f(x)$ is a monic polynomial in $GR(p^n, d)[x]$ of degree r such that the reduction $\overline{f}(x)$ in $\mathbb{F}_{p^d}[x]$ is irreducible. From Section 4.3 of [1], we have that R is a local ring of characteristic p^n with maximal ideal

$$\begin{aligned} M &= (p, f(x))/(f(x)^a) \\ &= \{h(x) + f(x)l(x) + (f(x)^a) : h(x) \in pGR(p^n, d)[x],\, l(x) \in GR(p^n, d)[x], \\ &\qquad \deg h < r,\, \deg l < r(a-1)\}. \end{aligned}$$

Then $|R| = p^{ndra}$, $|M| = p^{dr(na-1)}$ and $R/M \cong \mathbb{F}_{p^{dr}}$.

When $a = 1$, it turns out that R is still a Galois ring as a result of the next theorem.

Theorem. (Theorem 14.23 of [15]) *Let $f(x) \in GR(p^n, d)[x]$ be a monic polynomial of degree r such that the reduction $\overline{f}(x)$ in $\mathbb{F}_{p^d}[x]$ is irreducible. Then the ring $GR(p^n, d)[x]/(f(x))$ is isomorphic to a Galois ring $GR(p^n, dr)$.*

Hence, $R = GR(p^n, d)[x]/(f(x)) \cong GR(p^n, dr)$ and the exponent R is presented in Theorem 1.3.4.

Now, we assume that $a \geq 2$ and proceed to compute the exponent of R.

2.1 Some lemmas

Since R is a local ring with maximal ideal M, by Theorem 1.4.3 (3) we have $R^\times \cong (1+M) \times \mathbb{F}_{p^{dr}}^\times$ and $\mathbb{F}_{p^{dr}}^\times$ is cyclic of order $p^{dr}-1$, so it suffices to determine the exponent of the p-group $1+M$.

Deng and Somer [3] considered the exponent of the ring $\mathbb{F}_{p^n}[x]/(f(x)^a)$, where $a \geq 1$ and $f(x)$ is an irreducible polynomial in $\mathbb{F}_{p^n}[x]$ of degree r in the following theorem.

Theorem 2.1.1. (Lemma 3.3 of [3]) *Let $f(x)$ be an irreducible polynomial in $\mathbb{F}_{p^n}[x]$ of degree r and $a \geq 1$. Then*

$$\lambda(\mathbb{F}_{p^n}[x]/(f(x)^a)) = p^s(p^{nr}-1),$$

where $p^{s-1} < a \leq p^s$ for some $s \in \mathbb{N} \cup \{0\}$.

Following Deng and Somer, let s be the positive integer such that $p^{s-1} < a \leq p^s$. We shall show that every element in $1+M$ is of order not exceeding p^{s+n-1} and the order of $1+f(x)+(f(x)^a)$ is p^{s+n-1}, so the exponent of the group $1+M$ is p^{s+n-1}. However, our computation is more complicated because the characteristic of the ring R is p^n and the binomial coefficients do not disappear easily like in the extension of fields case where it is of characteristic p.

For any $m \in \mathbb{N}$, we write $e_p(m)$ for **the maximum power of p in m**, that is, $p^{e_p(m)} \mid m$ but $p^{e_p(m)+1} \nmid m$.

The proof is started by deriving some facts on the maximum power of p is binomial coefficients using de Polignac formula.

Theorem 2.1.2. (de Polignac formula) *Let $m \in \mathbb{N}$ and p be a prime. Then*

$$e_p(m!) = \sum_{i=1}^{\infty}[\frac{m}{p^i}].$$

We divide the computation into four lemmas as follows.

Lemma 2.1.3. $e_p(\binom{p^n}{l_1}) = e_p(\binom{p^n}{l_2})$, *where $1 \le l_1, l_2 \le p-1$ and $n \in \mathbb{N}$. Moreover, $e_p(\binom{p^n}{l_1}) = n$.*

Proof. Note that $e_p(p^n!) = p^{n-1} + p^{n-2} + \cdots + p + 1$. Since $1 \le l_1, l_2 \le p-1$, $e_p(l_1!) = e_p(l_2!) = 0$ and

$$\begin{aligned} e_p((p^n - l_1)!) &= [\frac{p^n - l_1}{p}] + [\frac{p^n - l_1}{p^2}] + \cdots + [\frac{p^n - l_1}{p^n}] \\ &= [\frac{p^n - l_2}{p}] + [\frac{p^n - l_2}{p^2}] + \cdots + [\frac{p^n - l_2}{p^n}] \\ &= e_p((p^n - l_2)!). \end{aligned}$$

On the other hand,

$$\begin{aligned} e_p((p^n - l_1)!) &= (p^{n-1} - 1) + \cdots + (p - 1) \\ &= (p^{n-1} + \cdots + p + 1) - n \\ &= e_p((p^n)!) - n. \end{aligned}$$

Hence,

$$e_p(\binom{p^n}{l_1}) = e_p(\binom{p^n}{l_2}) = e_p(p^n!) - e_p((p^n - l_1)!) = n,$$

as desired. □

Lemma 2.1.4. *Let $a \geq 2$, and s, $n \in \mathbb{N}$, where $p^{s-1} < a \leq p^s$. For, $0 \leq i \leq s-2$, $1 \leq k \leq (p-1)p^{s-2-i} - 1$. Then:*

(1) $e_p(\binom{p^{s+n-1}}{p^{s-1-i}}) \geq n$.

(2) $e_p(\binom{p^{s+n-1}}{p^{s-1-i}+l_1}) = e_p(\binom{p^{s+n-1}}{p^{s-1-i}+l_2})$, *where* $1 \leq l_1, l_2 \leq p-1$. *Moreover,* $e_p(\binom{p^{s+n-1}}{p^{s-1-i}+l_1}) \geq n$.

(3) $e_p(\binom{p^{s+n-1}}{p^{s-1-i}+kp}) \geq n$.

(4) $e_p(\binom{p^{s+n-1}}{p^{s-1-i}+kp+l_1}) = e_p(\binom{p^{s+n-1}}{p^{s-1-i}+kp+l_2})$, *where* $1 \leq l_1, l_2 \leq p-1$. *Moreover,* $e_p(\binom{p^{s+n-1}}{p^{s-1-i}+kp+l_1}) \geq n$.

Proof. Note that $e_p((p^{s+n-1})!) = p^{s+n-2} + p^{s+n-3} + \cdots + p + 1$. For (1), we compute

$$\begin{aligned}
&e_p((p^{s+n-1} - p^{s-1-i})!) \\
&= [\frac{p^{s+n-1} - p^{s-1-i}}{p}] + [\frac{p^{s+n-1} - p^{s-1-i}}{p^2}] + \cdots + [\frac{p^{s+n-1} - p^{s-1-i}}{p^{s-2-i}}] + \\
&\quad [\frac{p^{s+n-1} - p^{s-1-i}}{p^{s-1-i}}] + [\frac{p^{s+n-1} - p^{s-1-i}}{p^{s-i}}] + \cdots + [\frac{p^{s+n-1} - p^{s-1-i}}{p^{s+n-2}}] \\
&= (p^{s+n-2} - p^{s-2-i}) + (p^{s+n-3} - p^{s-3-i}) + \cdots + (p^{n+1+i} - p) + \\
&\quad (p^{n+i} - 1) + (p^{n-1+i} - 1) + \cdots + (p - 1) \\
&= (p^{s+n-2} + \cdots + p + 1) - (p^{s-2-i} + \cdots + p + 1 + (n+i))
\end{aligned}$$

and

$$e_p((p^{s-1-i})!) = p^{s-2-i} + \cdots + p + 1.$$

Thus

$$e_p(\binom{p^{s+n-1}}{p^{s-1-i}}) = e_p((p^{s+n-1})!) - e_p((p^{s+n-1} - p^{s-1-i})!) - e_p((p^{s-1-i})!)$$

$$= n + i \geq n.$$

Observe that

$$\begin{aligned}
&e_p((p^{s+n-1} - p^{s-1-i} - l_1)!) \\
&= [\frac{p^{s+n-1} - p^{s-1-i} - l_1}{p}] + [\frac{p^{s+n-1} - p^{s-1-i} - l_1}{p^2}] + \cdots + [\frac{p^{s+n-1} - p^{s-1-i} - l_1}{p^{s-2-i}}] + \\
&\quad [\frac{p^{s+n-1} - p^{s-1-i} - l_1}{p^{s-1-i}}] + [\frac{p^{s+n-1} - p^{s-1-i} - l_1}{p^{s-i}}] + \cdots + [\frac{p^{s+n-1} - p^{s-1-i} - l_1}{p^{s+n-2}}] \\
&= [\frac{p^{s+n-1} - p^{s-1-i} - l_2}{p}] + [\frac{p^{s+n-1} - p^{s-1-i} - l_2}{p^2}] + \cdots + [\frac{p^{s+n-1} - p^{s-1-i} - l_2}{p^{s-2-i}}] + \\
&\quad [\frac{p^{s+n-1} - p^{s-1-i} - l_2}{p^{s-1-i}}] + [\frac{p^{s+n-1} - p^{s-1-i} - l_2}{p^{s-i}}] + \cdots + [\frac{p^{s+n-1} - p^{s-1-i} - l_2}{p^{s+n-2}}] \\
&= e_p((p^{s+n-1} - p^{s-1-i} - l_2)!).
\end{aligned}$$

Moreover,

$$\begin{aligned}
&e_p((p^{s+n-1} - p^{s-1-i} - l_1)!) \\
&= (p^{s+n-2} - p^{s-2-i} - 1) + (p^{s+n-3} - p^{s-3-i} - 1) + \cdots + (p^{n+1+i} - p - 1) + \\
&\quad (p^{n+i} - 1 - 1) + (p^{n-1+i} - 1) + \cdots + (p - 1) \\
&= (p^{s+n-2} + \cdots + p + 1) - (p^{s-2-i} + \cdots + p + 1 + (n + i + 1) + (s - 2 - i)) \\
&= e_p((p^{s+n-1})!) - (p^{s-2-i} + \cdots + p + 1 + (n + i + 1) + (s - 2 - i))
\end{aligned}$$

and

$$e_p((p^{s-1-i} + l_1)!) = [\frac{p^{s-1-i} + l_1}{p}] + \cdots + [\frac{p^{s-1-i} + l_1}{p^{s-1}}]$$

$$= p^{s-2-i} + \cdots + p + 1.$$

Hence,

$$\begin{aligned} e_p(\binom{p^{s+n-1}}{p^{s-1-i}+l_1}) &= e_p((p^{s+n-1})!) - e_p((p^{s+n-1}-p^{s-1-i}-l_1)!) \\ &\quad - e_p((p^{s-1-i}+l_1)!) \\ &= n+s-1 \geq n. \end{aligned}$$

This proves (2). Next, we compute

$$\begin{aligned} & e_p((p^{s+n-1}-p^{s-1-i}-kp)!) = \\ & [\frac{p^{s+n-1}-p^{s-1-i}-kp}{p}] + [\frac{p^{s+n-1}-p^{s-1-i}-kp}{p^2}] + \cdots + [\frac{p^{s+n-1}-p^{s-1-i}-kp}{p^{s-2-i}}] + \\ & [\frac{p^{s+n-1}-p^{s-1-i}-kp}{p^{s-1-i}}] + [\frac{p^{s+n-1}-p^{s-1-i}-kp}{p^{s-i}}] + \cdots + [\frac{p^{s+n-1}-p^{s-1-i}-kp}{p^{s+n-2}}] \\ & = (p^{s+n-2}-p^{s-2-i}-k) + (p^{s+n-3}-p^{s-3-i}+[-\frac{k}{p}]) + \cdots + \\ & \quad (p^{n+1+i}-p+[-\frac{k}{p^{s-3-i}}]) + (p^{n+i}-1+[-\frac{k}{p^{s-2-i}}]) + \\ & \quad (p^{n-1+i}+[-\frac{1}{p}-\frac{k}{p^{s-1-i}}]) + \cdots + (p+[-\frac{1}{p^{n-1+i}}-\frac{k}{p^{s+n-3}}]) + \\ & = (p^{s+n-2}+\cdots+p+1) - (p^{s-2}+\cdots+p+1+k+1) + \\ & \quad ([-\frac{k}{p}] + \cdots + [-\frac{k}{p^{s-2-i}}]) + ([-\frac{1}{p}-\frac{k}{p^{s-1-i}}] + \cdots + [-\frac{1}{p^{n-1+i}}-\frac{k}{p^{s+n-3}}]) \end{aligned}$$

and

$$\begin{aligned} e_p((p^{s-1-i}+kp)!) &= [\frac{p^{s-1-i}+kp}{p}] + \cdots + [\frac{p^{s-1-i}+kp}{p^{s-1-i}}] \\ &= (p^{s-2-i}+\cdots+p+1) + k + ([\frac{k}{p}] + \cdots + [\frac{k}{p^{s-2-i}}]). \end{aligned}$$

Thus

$$
\begin{aligned}
&e_p(\binom{p^{s+n-1}}{p^{s-1-i}+kp}) \\
&= e_p((p^{s+n-1})!) - e_p((p^{s+n-1}-p^{s-1-i}-kp)!) - e_p((p^{s-1-i}+kp)!) \\
&\geq (n-1+i)+1-((([\frac{k}{p}]+[-\frac{k}{p}])+\cdots+([\frac{k}{p^{s-2-i}}]+[-\frac{k}{p^{s-2-i}}])) \\
&\geq n,
\end{aligned}
$$

and so we have (3). To prove the final statement, we compute

$$
\begin{aligned}
&e_p((p^{s+n-1}-p^{s-1-i}-kp-l_1)!) \\
&= [\frac{p^{s+n-1}-p^{s-1-i}-kp-l_1}{p}]+[\frac{p^{s+n-1}-p^{s-1-i}-kp-l_1}{p^2}]+\cdots+ \\
&\quad [\frac{p^{s+n-1}-p^{s-1-i}-kp-l_1}{p^{s-2-i}}]+[\frac{p^{s+n-1}-p^{s-1-i}-kp-l_1}{p^{s-1-i}}]+ \\
&\quad [\frac{p^{s+n-1}-p^{s-1-i}-kp-l_1}{p^{s-i}}]+\cdots+[\frac{p^{s+n-1}-p^{s-1-i}-kp-l_1}{p^{s+n-2}}] \\
&= [\frac{p^{s+n-1}-p^{s-1-i}-kp-l_2}{p}]+[\frac{p^{s+n-1}-p^{s-1-i}-kp-l_2}{p^2}]+\cdots+ \\
&\quad [\frac{p^{s+n-1}-p^{s-1-i}-kp-l_2}{p^{s-2-i}}]+[\frac{p^{s+n-1}-p^{s-1-i}-kp-l_2}{p^{s-1-i}}]+ \\
&\quad [\frac{p^{s+n-1}-p^{s-1-i}-kp-l_2}{p^{s-i}}]+\cdots+[\frac{p^{s+n-1}-p^{s-1-i}-kp-l_2}{p^{s+n-2}}] \\
&= e_p((p^{s+n-1}-p^{s-1-i}-kp-l_2)!).
\end{aligned}
$$

Also,

$$\begin{aligned}
&e_p((p^{s+n-1}-p^{s-1-i}-kp-l_1)!)\\
&=(p^{s+n-2}-p^{s-2-i}-k-1)+(p^{s+n-3}-p^{s-3-i}+[-\frac{k}{p}-\frac{l_1}{p^2}])+\cdots+\\
&\quad(p^{n+1+i}-p+[-\frac{k}{p^{s-3-i}}-\frac{l_1}{p^{s-2-i}}])+(p^{n+i}-1+[-\frac{k}{p^{s-2-i}}-\frac{l_1}{p^{s-1-i}}])+\\
&\quad(p^{n-1+i}+[-\frac{1}{p}-\frac{k}{p^{s-1-i}}-\frac{l_1}{p^{s-i}}])+\cdots+(p+[-\frac{1}{p^{n-1+i}}-\frac{k}{p^{s+n-3}}-\frac{l_1}{p^{s+n-2}}])\\
&=(p^{s+n-2}+\cdots+p+1)-(p^{s-2-i}+\cdots+p+1+k+1)+\\
&\quad(-1+[-\frac{k}{p}-\frac{l_1}{p^2}]+\cdots+[-\frac{k}{p^{s-2-i}}-\frac{l_1}{p^{s-1-i}}])+\\
&\quad([-\frac{1}{p}-\frac{k}{p^{s-1-i}}-\frac{l_1}{p^{s-i}}]+\cdots+[-\frac{1}{p^{n-1+i}}-\frac{k}{p^{s+n-3}}-\frac{l_1}{p^{s+n-2}}])
\end{aligned}$$

and

$$\begin{aligned}
e_p((p^{s-1-i}+kp+l_1)!)&=[\frac{p^{s-1-i}+kp+l_1}{p}]+\cdots+[\frac{p^{s-1-i}+kp+l_1}{p^{s-1-i}}]\\
&=(p^{s-2-i}+\cdots+p+1)+(k)+\\
&\quad([\frac{k}{p}+\frac{l_1}{p^2}]+\cdots+[\frac{k}{p^{s-2-i}}+\frac{l_1}{p^{s-1-i}}]).
\end{aligned}$$

Therefore,

$$\begin{aligned}
&e_p(\binom{p^{s+n-1}}{p^{s-1-i}+kp+l_1})\\
&\quad=e_p((p^{s+n-1})!)-e_p((p^{s+n-1}-p^{s-1-i}-kp-l_1)!)-e_p((p^{s-1-i}+kp+l_1)!)\\
&\quad\geq(n+i)+1-(([\frac{k}{p}+\frac{l_1}{p^2}]+[-\frac{k}{p}-\frac{l_1}{p^2}])+\cdots+\\
&\qquad([\frac{k}{p^{s-2-i}}+\frac{l_1}{p^{s-1-i}}]+[-\frac{k}{p^{s-2-i}}-\frac{l_1}{p^{s-1-i}}]))\\
&\quad\geq n.
\end{aligned}$$

This completes the lemma. □

Lemma 2.1.5. *Let $a \geq 2$, and $s, n \in \mathbb{N}$, where $p^{s-1} < a \leq p^s$. Let $f(x)$ be a monic polynomial in $GR(p^n, d)[x]$ such that the reduction $\overline{f}(x)$ in $\mathbb{F}_{p^d}[x]$ is irreducible. Then:*

(1) $e_p(\binom{p^{s+n-1-t}}{p^{s-1}}) = n - t$ *for all* $t \in \mathbb{N}$.

(2) $(1 + f(x) + (f(x)^a))^{p^{s+n-1-t}} \neq 1 + (f(x)^a)$ *for all* $t \in \mathbb{N}$.

Proof. Note that $e_p((p^{s+n-1-t})!) = p^{s+n-2-t} + \cdots + p + 1$,

$$\begin{aligned}
&e_p((p^{s+n-1-t} - p^{s-1})!) \\
&= [\frac{p^{s+n-1-t} - p^{s-1}}{p}] + [\frac{p^{s+n-1-t} - p^{s-1}}{p^2}] + \cdots + [\frac{p^{s+n-1-t} - p^{s-1}}{p^{s-2}}] + \\
&\quad [\frac{p^{s+n-1-t} - p^{s-1}}{p^{s-1}}] + [\frac{p^{s+n-1-t} - p^{s-1}}{p^{s}}] + \cdots + [\frac{p^{s+n-1-t} - p^{s-1}}{p^{s+n-2}}] \\
&= (p^{s+n-2-t} - p^{s-2}) + (p^{s+n-3-t} - p^{s-3}) + \cdots + (p^{n+1-t} - p) + \\
&\quad (p^{n-t} - 1) + (p^{n-1-t} - 1) + \cdots + (p - 1) \\
&= (p^{s+n-2-t} + \cdots + p + 1) - (p^{s-2} + \cdots + p + 1 + (n - t))
\end{aligned}$$

and

$$e_p((p^{s-1})!) = p^{s-2} + \cdots + p + 1.$$

Thus

$$\begin{aligned}
e_p(\binom{p^{s+n-1-t}}{p^{s-1}}) &= e_p((p^{s+n-1-t})!) - e_p((p^{s+n-1-t} - p^{s-1})!) - e_p((p^{s-1})!) \\
&= n - t.
\end{aligned}$$

which implies (1). For (2), we compute

$$\begin{aligned}
&(1 + f + (f^a))^{p^{s+n-1-t}} \\
&= 1 + \binom{p^{s+n-1-t}}{1} f + \cdots + \binom{p^{s+n-1-t}}{p^{s-1}} f^{p^{s-1}} + \cdots + \binom{p^{s+n-1-t}}{a-1} f^{a-1} + (f^a).
\end{aligned}$$

Since $a \geq 2$ and $p^{s-1} < a \leq p^s$, we have $(1 + f + (f^a))^{p^{s+n-1-t}} \neq 1 + (f^a)$ for all $t \in \mathbb{N}$ by (1). □

Lemma 2.1.6. *$e_p(m!) < \frac{m}{p-1}$ for all $m \in \mathbb{N}$.*

Proof. Let $t \in \mathbb{N}$ be such that $p^t \leq m < p^{t+1}$. For $i \geq t+2$, we have $0 < \frac{m}{p^i} < \frac{p^{t+1}}{p^i} < 1$, so $[\frac{m}{p^i}] = 0$. Hence,

$$e_p(m!) = \sum_{j=1}^{\infty}[\frac{m}{p^j}] = \sum_{j=1}^{t+1}[\frac{m}{p^j}] + \sum_{j=t+2}^{\infty}[\frac{m}{p^j}] = \sum_{j=1}^{t+1}[\frac{m}{p^j}] \leq \sum_{j=1}^{t+1}\frac{m}{p^j} < \sum_{j=1}^{\infty}\frac{m}{p^j} = \frac{m}{p-1}$$

as desired. □

2.2 Exponent of $GR(p^n, d)[x]/(f(x)^a)$, $a \geq 2$

Now, we are ready to compute the exponent of $GR(p^n, d)[x]/(f(x)^a)$, when $a \geq 2$.

Theorem 2.2.1. *Let $f(x) \in GR(p^n, d)[x]$ be a monic polynomial of degree r such that the reduction $\overline{f}(x)$ in $\mathbb{F}_{p^d}[x]$ is irreducible, and $a \geq 2$. If s is the positive integer such that $p^{s-1} < a \leq p^s$, then*

$$\lambda(GR(p^n, d)[x]/(f(x)^a)) = p^{s+n-1}(p^{dr} - 1).$$

Proof. Let $h(x) \in pGR(p^n, d)[x]$, and $l(x) \in GR(p^n, d)[x]$, where $\deg h < r$, and $\deg l < r(a-1)$. Then

$$\begin{aligned}(1 + h + fl + (f^a))^{p^{s+n-1}} = (1 + fl)^{p^{s+n-1}} + \binom{p^{s+n-1}}{1}(1 + fl)^{p^{s+n-1}-1}h + \cdots + \\ \binom{p^{s+n-1}}{p^{s+n-1} - 1}(1 + fl)h^{p^{s+n-1}-1} + h^{p^{s+n-1}} + (f^a).\end{aligned}$$

Since $h(x) \in pGR(p^n, d)[x]$, we have $h(x)^j \in p^j GR(p^n, d)[x]$ for all $j \in \mathbb{N}$. By Lemma 2.1.6, $e_p(j!) < j$ and $s + n - 1 \geq n$, so $\binom{p^{s+n-1}}{j}h^j \in p^{s+n-1}GR(p^n, d)[x] =$

$\{0\}$ for all $1 \leq j \leq p^{s+n-1}$. It follows that

$$\binom{p^{s+n-1}}{1}h = \cdots = \binom{p^{s+n-1}}{p^{s+n-1}-1}h^{p^{s+n-1}-1} = h^{p^{s+n-1}} = 0.$$

Thus,

$$\begin{aligned}(1+h+fl+(f^a))^{p^{s+n-1}} &= (1+fl)^{p^{s+n-1}} + (f^a) \\ = 1 + \binom{p^{s+n-1}}{1}fl + \cdots + \binom{p^{s+n-1}}{p^{s-1}}(fl)^{p^{s-1}} &+ \cdots + \binom{p^{s+n-1}}{a-1}(fl)^{a-1} + (f^a).\end{aligned}$$

Lemmas 2.1.3 and 2.1.4 show that $p^n \mid \binom{p^{s+n-1}}{i}$ for all $i \in \{1, 2, \cdots, a-1\}$. Hence, $(1+h+fl+(f^a))^{p^{s+n-1}} = 1+(f^a)$. Thus, Lemma 2.1.5 implies that p^{s+n-1} is the order of $1+f+(f^a) \in 1+M$, so $\exp(1+M) = p^{s+n-1}$. Therefore, $\lambda(GR(p^n,d)[x]/(f(x)^a)) = \operatorname{lcm}(\exp(1+M), \exp \mathbb{F}_{p^{dr}}^{\times}) = p^{s+n-1}(p^{dr}-1)$. □

Taking $d = 1$ and $n = 1$ in Theorem 2.2.1, respectively, we conclude the following corollaries.

Corollary 2.2.2. *Let $f(x) \in \mathbb{Z}_{p^n}[x]$ be a monic polynomial of degree r such that the reduction $\overline{f}(x)$ in $\mathbb{F}_p[x]$ is irreducible, and $a \geq 2$. Then*

$$\lambda(\mathbb{Z}_{p^n}[x]/(f(x)^a)) = p^{s+n-1}(p^r-1),$$

where $p^{s-1} < a \leq p^s$ for some $s \in \mathbb{N}$.

Corollary 2.2.3. *Let $f(x) \in \mathbb{F}_{p^d}[x]$ be a monic irreducible polynomial of degree r, and $a \geq 2$. Then*

$$\lambda(\mathbb{F}_{p^d}[x]/(f(x)^a)) = p^s(p^{dr}-1),$$

where $p^{s-1} < a \leq p^s$ for some $s \in \mathbb{N}$.

CHAPTER III

CYCLES AND DISTANCE

In this chapter, we find necessary and sufficient conditions for the existence of t-cycles with $t \geq 1$ in $G_1^{(k)}(R)$, and find the number of t-cycles in $G_1^{(k)}(R)$ for a finite commutative ring R with identity. Later, we compute the indegree of the fixed point 0 and maximum distance from a vertex in the component containing 0 to 0 in $G_2^{(k)}(R)$ over a finite local ring R.

3.1 Number of cycles

Let R be a finite commutative ring with identity $1 \neq 0$ and $k \geq 2$. We set $\lambda(R) = uv$, where u is the largest divisor of $\lambda(R)$ relatively prime to k. Let t be a positive integer.

Theorem 3.1.1. *The following statements are equivalent.*

(1) *There exists a t-cycle, where $t \geq 1$, in $G_1^{(k)}(R)$.*

(2) *There exists $b \in R^\times$ where t is the least positive integer such that $o(b) \mid k^t - 1$.*

(3) *$t = \operatorname{ord}_d k$ for some divisor d of u.*

Proof. (1) $\Rightarrow$ (2). Let a be a vertex of a t-cycle. Then t is the least positive integer such that $a^{k^t} = a$, so $a(a^{k^t-1} - 1) = 0$. Since $a \in R^\times$, $a^{k^t-1} - 1 = 0$. Thus,

t is the least positive integer such that $a^{k^t-1} = 1$, and we set $b = a$. Hence, we have (2) as required.

(2) $\Rightarrow$ (3). Suppose there exists $b \in R^\times$ such that $o(b) \mid k^t - 1$, but $o(b) \nmid k^l - 1$, for all $1 \leq l < t$. Then t is the least positive integer such that $b^{k^t-1} = 1$, and $\gcd(o(b), k) = 1$, so $o(b) \mid u$. Set $d = o(b)$. Thus, $t = \operatorname{ord}_d k$ for some divisor d of u.

(3) $\Rightarrow$ (1). Suppose $t = \operatorname{ord}_d k$ for some divisor d of u. Since $R^\times$ is abelian, then there exists $a \in R^\times$ such that $o(a) = \lambda(R)$. Set $b = a^{\frac{\lambda(R)}{d}}$. Since $t = \operatorname{ord}_d k$, t is the least positive integer such that $b^{k^t-1} = a^{\frac{\lambda(R)(k^t-1)}{d}}$ and so $b \in R^\times$. This means that $b^{k^t} = b$, that is, there exists a t-cycle, where $t \geq 1$, in $G_1^{(k)}(R)$. □

Corollary 3.1.2. *If $k \equiv 1 \pmod u$, then every cycle in $G_1^{(k)}(R)$ is a fixed point.*

Proof. Assume that $k \equiv 1 \pmod u$. Hence for any divisor d of u, $d \mid k-1$. This means that $1 = \operatorname{ord}_d k$ for all divisors d of u. By Theorem 3.1.1, every cycle in $G_1^{(k)}(R)$ is a fixed point. □

Let R be a finite commutative ring with identity. The number of t-cycles in $G^{(k)}(R)$ is denoted by $A_t(G^{(k)}(R))$. For a finite local ring R with unique maximal ideal M, let p^{nr} be the order of R and the residue field $R/M \cong \mathbb{F}_{p^r}$ We have known that $R^\times \cong (1+M) \times \mathbb{F}_{p^r}^\times$, where $1+M$ is a p-group of order $p^{r(n-1)}$. Assume that

$$1 + M \cong \mathbb{Z}_{p^{s_1}} \times \mathbb{Z}_{p^{s_2}} \times \cdots \times \mathbb{Z}_{p^{s_q}},$$

for some $q \in \mathbb{N}$, and $0 \leq s_1 \leq s_2 \leq \cdots \leq s_q$ such that $s_1 + s_2 + \cdots + s_q = r(n-1)$. Then we can find the number of t-cycles in $G_1^{(k)}(R)$ by the following theorem.

Theorem 3.1.3. *Let R be a finite local ring of order p^{nr} with unique maximal ideal M and residue field $R/M \cong \mathbb{F}_{p^r}$. Assume that $R^\times$ as in the above set up, and let $k \geq 2$, $t \in \mathbb{N}$. Then*

$$A_t(G_1^{(k)}(R)) = \frac{1}{t}\Big((\prod_{i=1}^{q} \gcd(p^{s_i}, k^t - 1))(\gcd(p^r - 1, k^t - 1)) - \sum_{d \mid t, d \neq t} dA_d(G_1^{(k)}(R))\Big).$$

Proof. Let $g \in R^\times$ be a vertex in a t-cycle. Then t is the least positive integer such that $g^{k^t} = g$, so $g^{k^t - 1} = 1$. Notice that h in $G_1^{(k)}(R)$ satisfies $h^{k^t} = h$ if and only if h is a vertex in a d-cycle of $G_1^{(k)}(R)$ for some $d \mid t$ and the number of vertices in a d-cycle is $dA_d(G_1^{(k)}(R))$. Then the number of vertices in $G_1^{(k)}(R)$ that satisfy equation $g^{k^t-1} = 1$ is equal to $(\prod_{i=1}^{q} \gcd(p^{s_i}, k^t - 1))(\gcd(p^r - 1, k^t - 1)) - \sum_{d \mid t, d \neq t} dA_d(G_1^{(k)}(R))$. Consequently,

$$A_t(G_1^{(k)}(R)) = \frac{1}{t}\Big((\prod_{i=1}^{q} \gcd(p^{s_i}, k^t - 1))(\gcd(p^r - 1, k^t - 1)) - \sum_{d \mid t, d \neq t} dA_d(G_1^{(k)}(R))\Big),$$

as required. □

The group of units of the Galois ring $GR(p^n, r)$ presented in Theorem 1.3.4 gives us the next result.

Theorem 3.1.4. *Let $R = GR(p^n, r)$ be a Galois ring, where n, r are positive integers and p is a prime. Let $k \geq 2$ and $t \in \mathbb{N}$. Then:*

(1) *If (p is an odd prime) or ($p = 2$, and $n \leq 2$), then*

$$A_t(G_1^{(k)}(R)) = \tfrac{1}{t}\Big(\gcd(p^r - 1, k^t - 1)(\gcd(p^{n-1}, k^t - 1))^r - \sum_{d \mid t, d \neq t} dA_d(G_1^{(k)}(R))\Big).$$

(2) *If $p = 2$, and $n \geq 3$, then*

$$A_t(G_1^{(k)}(R)) = \frac{1}{t}\Big(ABCD - \sum_{d \mid t, d \neq t} dA_d(G_1^{(k)}(R))\Big),$$

where $A = \gcd(2^r - 1, k^t - 1)$, $B = \gcd(2, k^t - 1)$, $C = \gcd(2^{n-2}, k^t - 1)$ *and* $D = (\gcd(2^{n-1}, k^t - 1))^{r-1}$.

3.2 Distance

Let R be a finite commutative ring with identity. In this section, we work on the distance from any vertex to the unique cycle in the component of the digraph $G_1^{(k)}(R)$ and the trees attached to it. The proofs are similar to Theorems 3.6–3.8 of Meemark's [11].

Theorem 3.2.1. *Let R be a finite commutative ring with identity, and write $k = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, where $p_1, p_2, \dots, p_r$ are distinct primes, $k_i \geq 1$ for all i. Suppose that $\lambda(R) = \exp(R^\times) = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} m$, $a_i \geq 0$ for all i and $\gcd(p_1 \dots p_r, m) = 1$. For each component of $G_1^{(k)}(R)$, the maximum distance from a vertex in the component to the unique cycle of the component is equal to $l = \max\limits_{1 \leq i \leq r} \lceil \dfrac{a_i}{k_i} \rceil$.*

Proof. Let $g \in R^\times$. Since $o(g) \mid \lambda(R)$, $o(g) = p_1^{b_1} p_2^{b_2} \dots b_r^{a_r} s$ where $b_i \leq a_i$ for all i and $s \mid m$. Since $\frac{a_i}{k_i} \leq \lceil \frac{a_i}{k_i} \rceil$, $b_i \leq a_i \leq k_i \lceil \frac{a_i}{k_i} \rceil \leq k_i l$ where $l = \max\limits_{1 \leq i \leq r} \lceil \dfrac{a_i}{k_i} \rceil$. Then $o(g^{k^l}) = \frac{o(g)}{\gcd(o(g), k^l)} = s$. Since $s \mid m$ and $\gcd(k, m) = 1$, $\gcd(k, s) = 1$. Since $s \mid k^{\varphi(s)} - 1$, $g^{k^l (k^{\varphi(s)} - 1)} = 1$, and so $g^{k^l (k^{\varphi(s)})} = g^{k^l}$. Hence, g^{k^l} is on a cycle, and the distance from a vertex in the component of $G_1(R)$ to the unique cycle of the component is at most l.

Next, we assume that $g \in R^\times$ is a vertex on a t-cycle. Let $o(g) = d$. Then t is the least positive integer such that $d \mid k^t - 1$, so $\gcd(k, d) = 1$. We shall find a vertex in the component to g of distance l. Since $R^\times$ is abelian, there is an

$h \in R^{\times}$ such that $o(h) = \lambda(R)$. Choose $w = h^m$. Then

$$o(w) = o(h^m) = \frac{o(h)}{\gcd(o(h), m)} = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}.$$

Thus, $o(w) \mid k^l$, this means that $w^{k^l} = 1$. Since $\gcd(k, d) = 1$, for any $j \geq 0$

$$o(g^{k^j}) = \frac{o(g)}{\gcd(o(g), k^j)} = d.$$

Then $o(wg^{k^j}) = \operatorname{lcm}(o(w), o(g^{k^j})) = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} d$, and $(wg^{k^j})^{k^l} = w^{k^l} g^{k^{j+l}} = g^{k^{j+l}}$, for all $j \geq 0$. Hence, $wg^{k^{-l+t}}$ is the initial vertex of a directed path of length l to g. □

Theorem 3.2.2. *Let R be a finite commutative ring with identity, and let $k \geq 2$. Write k and $\lambda(R)$ as in Theorem 3.2.1. Then the set*

$$H = \{w \in R^{\times} : w^{k^j} = 1 \textit{ for some } j \in \{0, 1, \dots, l\}\}$$

consists of all vertices of the component containing 1. *Moveover, every vertex in H is on the tree attached to the fixed point* 1.

Proof. For any $x \in H$, we have $x^{k^j} = 1$ for some $j \in \{0, 1, \dots, l\}$, and so x is a vertex in the component containing 1.

Conversely, let y be a vertex in the component containing 1. Then $y^{k^j} = 1$, for some $j \in \{0, 1, \dots, l\}$, this means that $y \in H$. Thus, H consists of all vertices of the component containing 1. Finally, it is clear that every vertex in H is on the tree attached to the fixed point 1. □

Corollary 3.2.3. *Let R be a finite commutative ring with identity. Let $k \geq 2$ and $t \in \mathbb{N}$. Let $g \in R^{\times}$ be a vertex on a t-cycle. Then the tree attached to g is* *isomorphic to the tree attached to* 1*. Moreover, any two components in* $G_1^{(k)}(R)$ *containing* t*-cycle are isomorphic.*

Proof. Let $g \in R^\times$ be a vertex on a t-cycle. The proof of Theorem 3.2.1 gives that

$$H_g = \{wg^{k^{-j+t}} : w \in R^\times,\ and\ w^{k^j} = 1\ for\ some\ j \in \{0, 1, \dots, l\}\}$$

is a vertex on the tree attached to g.

Next, we show that $|H_g| = |H|$. Let $h \in R^\times$ be a vertex on this tree pointing to g. Then $h^{k^i} = g$ for some $i \in \{0, 1, \dots, l\}$. Note that $s \in R^\times$ is a root of $x^{k^i} = g$ if and only if sh^{-1} is a root of $x^{k^i} = 1$. Hence, we obtain a one-to-one correspondence between H and H_g preserving the tree structure. Hence, this proof is complete. □

For the graph $G_2^{(k)}(R)$, let R be a finite local ring of order p^{nr} with unique maximal ideal M, residue field $R/M \cong \mathbb{F}_{p^r}$, and let $s \in \mathbb{N}$ be the nilpotency of M. It is clear that there is only one cycle in $G_2^{(k)}(R)$, that is, the cycle of the fixed point 0, so $A_1(G_2^{(k)}(R)) = 1$ and $A_t(G_2^{(k)}(R)) = 0$ for $t \geq 2$.

For the unique component of $G_2^{(k)}(R)$, we shall study $\text{indeg}^{(k)}\, 0$ and the maximum distance from a vertex in the component to the unique cycle of the component by looking at the chain

$$\{0\} \subseteq M^{s-1} \subseteq \cdots \subseteq M \subseteq R,$$

and calculating $|M^j|$, where $1 \leq j \leq s$. Note that M^i/M^{i+1} is an R/M-vector space where the action of R/M on M^i/M^{i+1} is given by $(\alpha + M)(\eta + M^{i+1}) =$

$\alpha\eta + M^{i+1}$ for all $\alpha \in R$ and $\eta \in M^i$. Assume that $\dim_{R/M}(M^i/M^{i+1}) = t_i$ for all $1 \leq i \leq s-1$. Since $|M| = p^{r(n-1)}$ and $|R/M| = p^r$, $|M/M^2| = p^{rt_1}$, so $|M^2| = p^{r(n-1-t_1)}$. Continuing this calculation gives $|M^j| = p^{r(n-1-t_1-t_2-\cdots-t_{j-1})}$ for all $1 \leq j \leq s$.

Theorem 3.2.4. *Let R be a finite local ring of order p^{nr} with unique maximal ideal M, residue field $R/M \cong \mathbb{F}_{p^r}$ and let s be the nilpotency of M. Let* $\dim_{R/M}(M^i/M^{i+1}) = t_i$ *for all $1 \leq i \leq s-1$. For the unique component of $G_2^{(k)}(R)$, let l be the maximum distance from a vertex in the component to the unique cycle of the component and let $k \geq 2$. Then* $\operatorname{indeg}^{(k)} 0 \geq p^{r(n-1-T)}$, *where $T = \displaystyle\sum_{i=1}^{\lceil \frac{s}{k} \rceil - 1} t_i$ and $l = \lceil \log_k s \rceil$. In particular, if $k \geq s$, then $G_2^{(k)}(R)$ has one component and* $\operatorname{indeg}^{(k)} 0 = |M| = p^{r(n-1)}$, *that is, every directed edge terminates at* 0.

Proof. First, we assume that $k < s$. Clearly, $M^{\lceil \frac{s}{k} \rceil} \subseteq \{x \in M : x^k = 0\}$. Thus, $\operatorname{indeg}^{(k)} 0 = |\{x \in M : x^k = 0\}| \geq |M^{\lceil \frac{s}{k} \rceil}| = p^{r(n-1-T)}$, where $T = t_1 + t_2 + \cdots + t_{\lceil \frac{s}{k} \rceil - 1}$.

Next, let $l = \lceil \log_k s \rceil$ and let $x \in M$. Since $l = \lceil \log_k s \rceil$, so $k^l \geq s$. Then $x^{k^l} = 0$. Let j be the distance from x to 0. Then $x^{k^j} = 0$ and hence $j \leq l$. Let y be any element in $M \smallsetminus M^2$. Then $y^{k^l} = 0$. Since $l = \lceil \log_k s \rceil$, $l - 1 < \log_k s$, $k^{l-1} < s$. Since $y \in M \smallsetminus M^2$, $y^{k^{l-1}} \neq 0$. Hence, $l = \lceil \log_k s \rceil$ is the maximum distance from a vertex in the component to the unique cycle of the component.

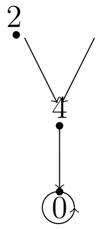
If $k \geq s$, then $x^k = 0$ for all $x \in M$. Thus, $\operatorname{indeg}^{(k)} 0 = |M| = p^{r(n-1)}$ and every directed edge terminates at 0. □

In particular, for a finite chain ring R with unique maximal ideal M and residue field $R/M \cong \mathbb{F}_{p^d}$, we have for any $\theta \in M \setminus M^2$, $M = R\theta$ and $M^j = R\theta^j$ for all $1 \leq j \leq s$, where s is the nilpotency of M. Since $\dim_{R/M}(M^i/M^{i+1}) = t_i = 1$ for all $1 \leq i \leq s-1$, it follows that $|M^i/M^{i+1}| = p^d$ for all $1 \leq i \leq s-1$, so $|R| = p^{ds}$, $|M| = p^{d(s-1)}$ and $|M^j| = p^{d(s-j)}$ for all $1 \leq j \leq s$. Therefore, the above theorem implies the next corollary.

Corollary 3.2.5. *Let R be a finite chain ring with unique maximal ideal M, residue field $R/M \cong \mathbb{F}_{p^d}$ and let s be the nilpotency of M. For the unique component of $G_2^{(k)}(R)$, let l be the maximum distance from a vertex in the component to the unique cycle of the component and let $k \geq 2$. Then* $\operatorname{indeg}^{(k)} 0 = p^{d(s-\lceil \frac{s}{k} \rceil)}$ *and $l = \lceil \log_k s \rceil$. In particular, if $k \geq s$, then $G_2^{(k)}(R)$ has one component and* $\operatorname{indeg}^{(k)} 0 = |M| = p^{d(s-1)}$*, that is, every directed edge terminates at* 0*. Moreover, if $R = GR(p^n, d)$ is a Galois ring, the result holds with $s = n$.*

Proof. If $k \geq s$, then the result is immediate. Suppose that $k < s$. Clearly, $M^{\lceil \frac{s}{k} \rceil} \subseteq \{x \in M : x^k = 0\}$. Let $x \in M$ be such that $x^k = 0$ and assume that x does not belong to $M^{\lceil \frac{s}{k} \rceil}$ Suppose that $x \notin M^{\lceil \frac{s}{k} \rceil}$. Then $x = r\theta^j$ for some $r \in R^\times$ and $j < \lceil \frac{s}{k} \rceil$. This implies that $kj < s$ and so $x^k = r^k\theta^{kj} \neq 0$ which is a contradiction. Hence, $\operatorname{indeg}^{(k)} 0 = |\{x \in M : x^k = 0\}| = |M^{\lceil \frac{s}{k} \rceil}| = p^{d(s-\lceil \frac{s}{k} \rceil)}$. By Theorem 3.2.4, the maximum distance from a vertex in the component to the unique cycle of the component is $\lceil \log_k s \rceil$. □

Example 3.2.6. Let $R = GR(2^3, 1)[x]/(x + 2, 2^{3-1}x)$ and $k = 2$. Then $s = (3 - 1) + 1 = 3$ is the nilpotency of maximal ideal M of R and $|M| = p^{s-1} = 4$. By Corollary 3.2.5, $\operatorname{indeg}^{(2)} 0 = 2$ and the maximum distance from a vertex in the component to the unique cycle of the component is $l = 2$. The digraph $G_2^{(2)}(R)$ is shown below.



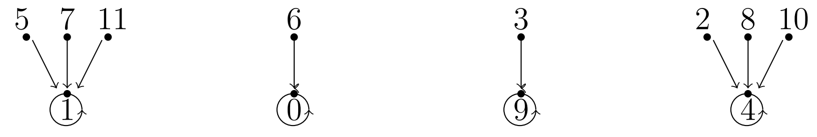
CHAPTER IV

SYMMETRIC DIGRAPHS

In this chapter, we present some conditions when the digraphs are symmetric using the exponents discovered in Chapter II.

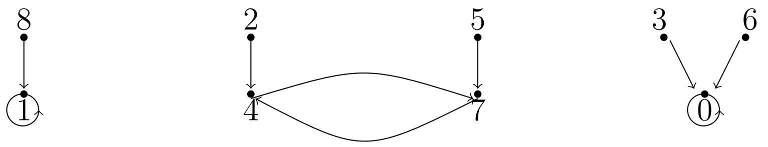
Let $N \geq 2$ be an integer. The digraph G is said to be **symmetric** of order N if its set of components can be partitioned into subsets of size N and each containing N isomorphic components.

For example, we consider the digraph $G^{(2)}(\mathbb{Z}_{12})$.



We see that its components can be partitioned into subsets of size two and each containing two isomorphic components. Hence, the digraph $G^{(2)}(\mathbb{Z}_{12})$ is symmetric of order 2.

Next, we consider the digraph $G^{(2)}(\mathbb{Z}_9)$.



It follows that its components cannot be partitioned into subsets of any size $N \geq 2$ and each containing $N \geq 2$ isomorphic components. Hence, the digraph $G^{(2)}(\mathbb{Z}_9)$

is not symmetric of any order $N \geq 2$.

An important tool for investigating the symmetric digraphs is semiregularity. Hence, we study semiregularity and then we determine conditions on symmetric digraphs.

4.1 Semiregularlity

A digraph G is called **semiregular** if there is a positive integer d such that each vertex of G either has indegree 0 or d. We know the outdegree of each vertex of $G^{(k)}(R)$ is equal to 1. We investigate the indegree of vertices in $G^{(k)}(R)$ and show that $G_1^{(k)}(R)$ is semiregular.

For a finite local ring R with unique maximal ideal M, let p^{nr} be an order of R and the residue field $R/M \cong \mathbb{F}_{p^r}$. In Section 3.1, we assume that

$$R^\times \cong (1+M) \times \mathbb{F}_{p^r}^\times \cong \mathbb{Z}_{p^{s_1}} \times \mathbb{Z}_{p^{s_2}} \times \cdots \times \mathbb{Z}_{p^{s_q}} \times \mathbb{F}_{p^r}^\times,$$

for some $q \in \mathbb{N}$, and $0 \leq s_1 \leq s_2 \leq \cdots \leq s_q$ such that $s_1 + s_2 + \cdots + s_q = r(n-1)$. Then we have the indegree of 1 in $G_1^{(k)}(R)$ in the next theorem. We also need the $\operatorname{indeg}^{(k)} 1$ recalled in the next theorem.

Theorem 4.1.1. (Theorem 2.3 of [14]) *Let R be a finite local ring of order p^{nr} with maximal ideal M and residue field $R/M \cong \mathbb{F}_{p^r}$, and let $k \geq 2$. Assume that*

$$R^\times \cong (1+M) \times \mathbb{F}_{p^r}^\times \cong \mathbb{Z}_{p^{s_1}} \times \mathbb{Z}_{p^{s_2}} \times \cdots \times \mathbb{Z}_{p^{s_q}} \times \mathbb{F}_{p^r}^\times,$$

for some $q \in \mathbb{N}$, and $0 \leq s_1 \leq s_2 \leq \cdots \leq s_q$ such that $s_1 + s_2 + \cdots + s_q = r(n-1)$. Then $\operatorname{indeg}^{(k)} 1 = \Big(\prod_{i=1}^{q} \gcd(p^{s_i}, k)\Big)\Big(\gcd(p^r - 1, k)\Big).$

Proof. Note that the indegree of 1 in $G_1^{(k)}(R)$ is the number of solutions of $x^k = 1$ in $R^\times$, so we find $\operatorname{indeg}^{(k)} 1$ by consider the number of solutions of $kx = 0$ in right hand side. Since a cyclic group of order m contains exactly $\gcd(m, k)$ solutions of $x^k = 1$, so there are $\Big(\prod_{i=1}^{q} \gcd(p^{s_i}, k)\Big)\Big(\gcd(p^r - 1, k)\Big)$ directed edges entering to 1 in $R^\times$. □

Theorem 4.1.2. *Let R be a finite commutative ring with identity and let $k \geq 2$. Then for any $g \in R^\times$, $\operatorname{indeg}^{(k)} g = 0$ or $\operatorname{indeg}^{(k)} g = \operatorname{indeg}^{(k)} 1$. Hence, $G_1^{(k)}(R)$ is semiregular.*

Proof. Assume that $\operatorname{indeg}^{(k)} g > 0$. Then there exists $h \in R^\times$ such that $h^k = g$. Since $s \in R^\times$ is a root of $x^k = g$ if and only if sh^{-1} is a root of $x^k = 1$. Hence, $\operatorname{indeg}^{(k)} g = \operatorname{indeg}^{(k)} 1$. □

Together with Theorem 1.3.4, we have:

Corollary 4.1.3. *Let $R = GR(p^n, r)$ be a Galois ring, where n, r are positive integers, p is a prime and let $k \geq 2$.*

(1) *If (p is odd) or ($p = 2$ and $n \leq 2$), then*

$$\operatorname{indeg}^{(k)} 1 = \gcd(p^r - 1, k)(\gcd(p^{n-1}, k))^r.$$

(2) *If $p = 2$ and $n \geq 3$, then*

$$\operatorname{indeg}^{(k)} 1 = \gcd(2^r - 1, k)\gcd(2, k)\gcd(2^{n-2}, k)(\gcd(2^{n-1}, k))^{r-1}.$$

4.2 Symmetry

For any finite local ring, we have the following results.

Theorem 4.2.1. *Let R be a finite local ring and let $k \geq 2$. If $G_1^{(k)}(R)$ is a symmetric of order $N \geq 2$, then $G^{(k)}(R)$ is not symmetric of order N.*

Proof. Since $G_2^{(k)}(R)$ has only one component and $N \geq 2$, $G^{(k)}(R)$ is not symmetric of order N. □

Theorem 4.2.2. *Let R be a finite local ring and let $k \geq 2$, and $t_i \in \mathbb{N}$.*

(1) *If $A_{t_i}(G_1^{(k)}(R)) = Nl_i$ for some $N \geq 2$, and $l_i \geq 1$ for any i such that there are t_i-cycle in $G_1^{(k)}(R)$, then $G_1^{(k)}(R)$ is symmetric of order N.*

(2) *If $A_1(G_1^{(k)}(R)) = Nl_1 - 1$ for some $N \geq 2$, $l_1 \geq 1$ and $A_{t_i}(G_1^{(k)}(R)) = Nl_i$ for some $l_i \geq 1$ for any i such that there are t_i-cycle in $G_1^{(k)}(R)$ and* $\mathrm{Com}(0) \cong \mathrm{Com}(1)$, *then $G^{(k)}(R)$ is symmetric of order N.*

Proof. Assume that $A_{t_i}(G_1^{(k)}(R)) = Nl_i$ for some $N \geq 2$, $l_i \geq 1$ for any i such that there are t_i-cycle in $G_1^{(k)}(R)$. By Theorem 4.1.2 and Corollary 3.2.3, $G_1^{(k)}(R)$ is symmetric of order N. Hence, (1) is completed.

Next, we assume that $A_1(G_1^{(k)}(R)) = Nl_1 - 1$ for some $N \geq 2$, $l_1 \geq 1$, and $A_{t_i}(G_1^{(k)}(R)) = Nl_i$ for some $l_i \geq 1$ for any i such that there are t_i-cycle in $G_1^{(k)}(R)$ and $\mathrm{Com}(0) \cong \mathrm{Com}(1)$. By Theorem 4.1.2 and Corollary 3.2.3, $G^{(k)}(R)$ is symmetric of order N. Hence, we have (2). □

First, we study symmetric digraphs over Galois rings.

Theorem 4.2.3. *Let $R = GR(p^n, r)$ be a Galois ring, where n, r are positive integers, p is a prime and let $k \geq 2$. If $k = p^j m$, where $j \geq n-1$, $p \nmid m$ and $p^r - 1 \mid k - 1$, then $G^{(k)}(R)$ is symmetric of order p^r.*

Proof. First we consider the case when p is an odd prime. From Theorem 1.3.4 (1), $\lambda(R) = p^{n-1}(p^r - 1)$. Since $k = p^j m$ and $p^r - 1 \mid k - 1$, we have $\gcd(k, p^r - 1) = 1 = \gcd(m, p^r - 1)$. Then $u = p^r - 1$ and $k \equiv 1 \pmod{u}$. By Corollary 3.1.2, every cycle in $G_1^{(k)}(R)$ is a fixed point. Also, Theorem 3.1.4 (1) implies that $A_1(G_1^{(k)}(R)) = p^r - 1$. Since $k = p^j m$, $j \geq n - 1$ and $\gcd(m, p^r - 1) = 1$, $l = \lceil \frac{n-1}{j} \rceil = 1$ by Theorem 3.2.1 if $j > 0$. Because $j \geq n - 1$, $k = p^j m \geq n$ and by Theorem 3.2.4, $G_2^{(k)}(R)$ has one component and $\operatorname{indeg}^{(k)} 0 = |R| - |R^\times|$. Corollary 4.1.3 (1) gives

$$\operatorname{indeg}^{(k)} 1 = p^{(n-1)r} = |R| - |R^\times| = \operatorname{indeg}^{(k)} 0.$$

Since $l = 1$, $\operatorname{Com}(0) \cong \operatorname{Com}(1)$. Corollary 3.2.3 and $A_1(G_1^{(k)}(R)) = p^r - 1$ allow us to conclude that $G^{(k)}(R)$ is symmetric of order p^r. For $j = 0$, we have $n = 1$, so $\operatorname{indeg}^{(k)} 1 = 1 = \operatorname{indeg}^{(k)} 0$ and $A_1(G_1^{(k)}(R)) = p^r - 1$. Hence, $G^{(k)}(R)$ is also symmetric of order p^r. The proof of the case $p = 2$ can be done in a similar way. □

Theorem 4.2.4. *Let $R = GR(2^n, r)$ be a Galois ring, where n, r are positive integers and let $k \geq 2$. If $2^r - 1$ is a prime for some $r \geq 3$, $k = 2^j$, where $j \geq n - 1$ and $\gcd(j, r) = 1$, then $G^{(k)}(R)$ is symmetric of order 2.*

Proof. From Theorem 1.3.4, $\lambda(R) = 2^{n-1}(2^r - 1)$, so $u = 2^r - 1$, and is an odd prime. So, the divisors d of u are 1 and u. If $d = 1$, then $t = 1$ ($\operatorname{ord}_1 2^j = 1$), so $A_1(G_1^{(k)}(R)) = 1$ by Theorem 3.1.4. Assume that $d = u$. Then $t = \operatorname{ord}_u 2^j$ which is the least positive integer such that $u = d = 2^r - 1 \mid 2^{jt} - 1$. Since $\gcd(j, r) = 1$, $r \mid t$. Since $2^r - 1$ is a prime for some $r \geq 3$, r is an odd prime. Let $t = 2^i m$ for some integer $i \geq 0$ and some positive odd integer m. If $i > 0$, then $r \mid 2^i m$ and $r \mid m$ which is a contradiction because $m < t$. Thus, t is odd. By Theorem 3.1.4,

$$A_t(G_1^{(k)}(R)) = \frac{1}{t}(\gcd(2^r - 1, 2^{jt} - 1) - 1) = \frac{1}{t}(2)(2^{r-1} - 1).$$

Since $A_t(G_1^{(k)}(R))$ is a positive integer and t is odd, $A_t(G_1^{(k)}(R))$ is even. From $j \geq n - 1$, so $k = 2^j \geq n$. This implies that $G_2^{(k)}(R)$ has one component and $\operatorname{indeg}^{(k)} 0 = |R| - |R^\times|$ by Theorem 3.2.4. Theorem 3.2.1 gives $l = \lceil \frac{n-1}{j} \rceil = 1$. Thus, it follows from Corollary 4.1.3 that

$$\operatorname{indeg}^{(k)} 1 = 2^{(n-1)r} = |R| - |R^\times| = \operatorname{indeg}^{(k)} 0.$$

Since $l = 1$, $\operatorname{Com}(0) \cong \operatorname{Com}(1)$. By Corollary 3.2.3 and $A_t(G_1^{(k)}(R))$ is an even $(t > 1)$, we finally have $G^{(k)}(R)$ is symmetric of order 2. □

Next, we study symmetry for digraphs of the kth power mapping over local rings $R = GR(p^n, d)[x]/(f(x)^a)$, $a \geq 2$, in Theorems 4.2.5–4.2.7. To use the exponent of R discovered in Section 2.2, let s be the positive integer such that $p^{s-1} < a \leq p^s$.

Theorem 4.2.5. *If $k = p^j m$, where $0 \leq j < s + n - 1$, $p \nmid m$ and $k \geq na$, then $G^{(k)}(R)$ is not symmetric of any order $N \geq 2$.*

Proof. The result is clear for $j = 0$ because $p \nmid \operatorname{indeg}^{(k)} 1$ by Theorem 4.1.1 but $p \mid \operatorname{indeg}^{(k)} 0$ by Theorem 3.2.4. Assume that $j \geq 1$. By Theorem 2.2.1, $\lambda(R) = p^{s+n-1}(p^{dr} - 1)$. By Theorem 3.2.1, for each component of $G_1^{(k)}(R)$ has maximum distance $l \geq \lceil \frac{s+n-1}{j} \rceil \geq 2$. Since $k \geq na$, $G_2^{(k)}(R)$ has one component and the maximum distance is 1 by Theorem 3.2.4. Hence, $G^{(k)}(R)$ is not symmetric of any order $N \geq 2$. □

Theorem 4.2.6. *If $k \geq na$ and $p \nmid k$, then $G^{(k)}(R)$ is not symmetric of any order $N \geq 2$.*

Proof. Since $k \nmid p$, by Theorem 4.1.1, $\operatorname{indeg}^{(k)} 1 = \gcd(p^{dr} - 1, k)$ which is not a power of p. However, because $k \geq na$, it follows from Theorem 3.2.4 that $G_2^{(k)}(R)$ has one component and $\operatorname{indeg}^{(k)} 0 = |R| - |R^{\times}| = p^{dr(na-1)}$ which is a power of p. Hence, $G^{(k)}(R)$ is not symmetric of any order $N \geq 2$. □

Theorem 4.2.7. *If $k = p^j m$, where $j \geq s + n - 1$, $p \nmid m$ and $p^{dr} - 1 \mid k - 1$, then $G^{(k)}(R)$ is symmetric of order p^{dr}.*

Proof. By Theorem 2.2.1, $\lambda(R) = p^{s+n-1}(p^{dr} - 1)$. Since $k = p^j m$ and $p^{dr} - 1 \mid k-1$, $\gcd(k, p^{dr}-1) = 1 = \gcd(m, p^{dr}-1)$. Then $u = p^{dr}-1$. Since $k \equiv 1 \pmod{u}$, every cycle in $G_1^{(k)}(R)$ is a fixed point by Corollary 3.1.2. Also, $A_1(G_1^{(k)}(R)) = p^{dr} - 1$ by Theorem 3.1.3. Since $j \geq s + n - 1$, $k \geq na$, and so $G_2^{(k)}(R)$ has one component and $\operatorname{indeg}^{(k)} 0 = |R| - |R^{\times}| = p^{dr(na-1)}$ by Theorem 3.2.4. In addition, $l = \lceil \frac{s+n-1}{j} \rceil = 1$ by Theorem 3.2.1. Recall that $|R^{\times}| = p^{dr(na-1)}(p^{dr} - 1)$ and $A_1(G_1^{(k)}(R)) = p^{dr} - 1$, so

$$\operatorname{indeg}^{(k)} 1 = p^{dr(na-1)} = |R| - |R^{\times}| = \operatorname{indeg}^{(k)} 0.$$

Hence, $\operatorname{Com}(0) \cong \operatorname{Com}(1)$. Since there are $p^{dr} - 1$ component with 1-cycles in $G_1^{(k)}(R)$ and they are all isomorphic by Corollary 3.2.3, together with $\operatorname{Com}(0) \cong \operatorname{Com}(1)$, we can conclude that $G^{(k)}(R)$ is symmetric of order p^{dr}. □

Finally, let $R = GR(p^n, d)[x]/(z(x), p^{n-1}x^{s-(n-1)e})$ be a finite chain ring with $s \geq 2$. We end this work by giving some results for symmetric digraphs over R.

Theorem 4.2.8. *If $k = p^j m$, where $p \nmid m$ and $\gcd(m, p^d - 1) \neq 1$, then $G^{(k)}(R)$ is not symmetric of any order $N \geq 2$.*

Proof. Since $k = p^j m$ and $\gcd(m, p^d - 1) \neq 1$, it follows from Theorem 4.1.1 that $\operatorname{indeg}^{(k)} 1$ is not a power of p. However, $\operatorname{indeg}^{(k)} 0$ is a power of p by Corollary 3.2.5. Hence, Corollary 3.2.3 implies that $G^{(k)}(R)$ is not symmetric of any order $N \geq 2$. □

Theorem 4.2.9. *If $p \nmid k$, then $G^{(k)}(R)$ is not symmetric of any order $N \geq 2$.*

Proof. Clearly, $A_1(G_1^{(k)}(R)) \geq 1$. Recall that $\operatorname{indeg}^{(k)} 1 = \gcd(p^d - 1, k)$ and $p \nmid \gcd(p^d - 1, k)$. By Corollary 3.2.5, we have $p \mid \operatorname{indeg}^{(k)} 0$. Hence, it follows from Corollary 3.2.3 that $G^{(k)}(R)$ is not symmetric of any order $N \geq 2$. □

Theorem 4.2.10. *If $k = p^j m$, where $p \nmid m$, $p^d - 1 \mid k - 1$ and $\operatorname{Com}(1) \cong \operatorname{Com}(0)$, then $G^{(k)}(R)$ is symmetric of order p^d.*

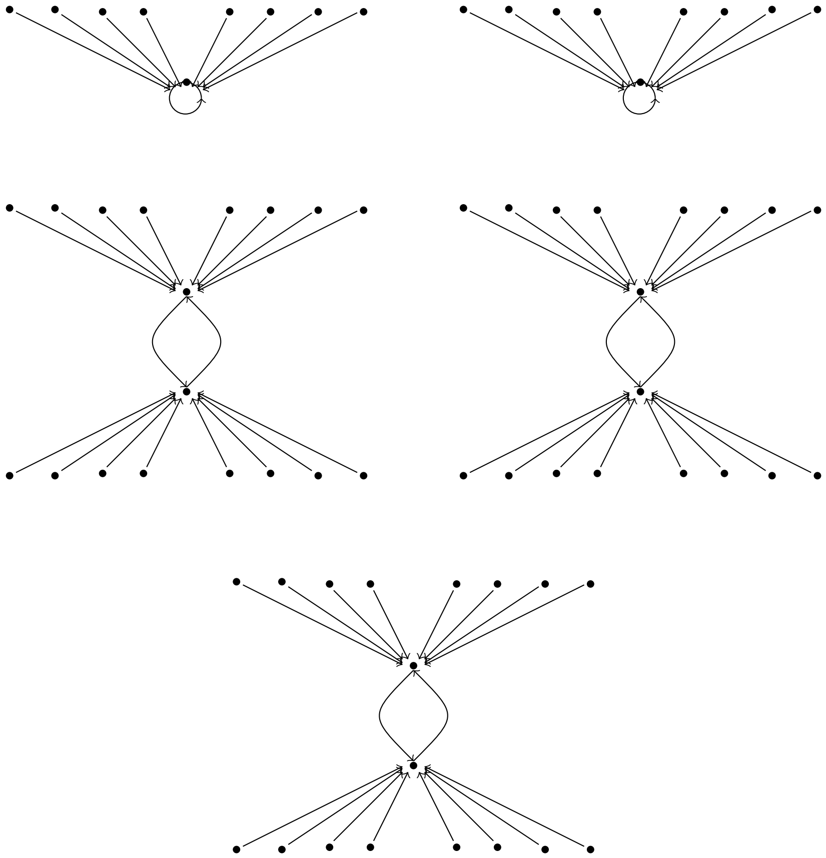
Proof. Its proof is similar to Theorem 4.2.3 and omitted. □

CHAPTER V

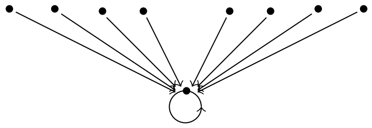
EXAMPLES

We illustrate the results of the previous chapters by the following five examples.

(1) Let $R = GR(3^2, 2)$ and $k = 3$. Then $|R^\times| = 3^{(2-1)2}(3^2 - 1) = 72$. It follows from Theorem 1.3.4 (1) that $\lambda(R) = 3^{2-1}(3^2 - 1) = 3(8)$. We have $u = 8$, so all divisors d of u are 1, 2, 4, 8. By Theorem 3.1.1, $G_1^{(3)}(R)$ contains 1-cycles and 2-cycles. From Theorem 3.1.4 (1), $A_1(G_1^{(3)}(R)) = 2$ and $A_2(G_1^{(3)}(R)) =\ 3$. For each component of $G_1^{(3)}(R)$, the maximum distance from a vertex in the component to the unique cycle of the component is $l = \lceil \frac{1}{1} \rceil = 1$ by Theorem 3.2.1. It follows from Corollary 4.1.3 (1) that $\operatorname{indeg}^{(3)} 1 = \gcd(3^2 - 1, 3)(\gcd(3^{2-1}, 3))^2 = 9$. Since $k = 3 \geq n = 2$, by Theorem 3.2.4, $G_2^{(3)}(R)$ has one component and $\operatorname{indeg}^{(3)} 0 = |R| - |R^\times| = 81 - 72 = 9$. Observe that $l = 1$ and $\operatorname{indeg}^{(3)} 1 = \operatorname{indeg}^{(3)} 0 = 9$, so $\text{Com}(1) \cong \text{Com}(0)$. Thus, set $N = 3$, $l_1 = 1 = l_2$, and so by Theorem 4.2.2 (2), we have $G^{(3)}(R)$ is symmetric of order 3. We display the digraph $G^{(3)}(R)$ below.

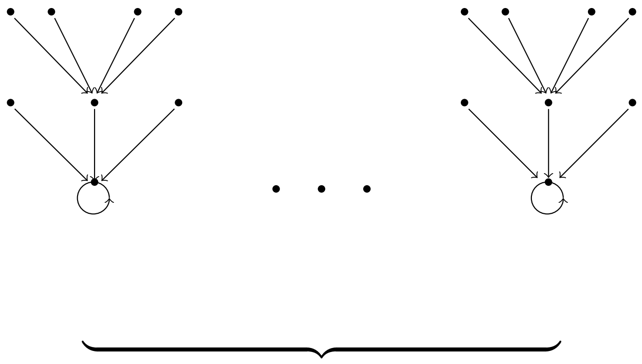


$G_1^{(3)}(R)$

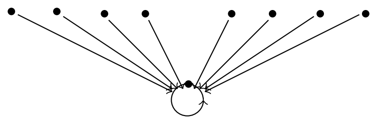


$G_2^{(3)}(R)$

(2) Let $R = GR(3^2, 2)$ and $k = 4$. Then $|R^{\times}| = 3^{(2-1)2}(3^2 - 1) = 72$. By Theorem 1.3.4 (1), $\lambda(R) = 3(8)$. Then $u = 3$ and all divisors d of u are 1 and 3. By Theorem 3.1.1, $G_1^{(4)}(R)$ contains only 1-cycles. From Theorem 3.1.4 (1), $A_1(G_1^{(4)}(R)) = \gcd(3^2-1, 4-1)(\gcd(3^{2-1}, 4-1))^2 = 9$, By Theorem 3.2.1, any component of $G_1^{(4)}(R)$ has maximum distance $l = \lceil \frac{3}{2} \rceil = 2$. By Corollary 4.1.3 (1), $\operatorname{indeg}^{(4)} 1 = \gcd(3^2 - 1, 4)(\gcd(3^{2-1}, 4))^2 = 4$. Observe that $k = 4 \geq n = 2$, by Theorem 3.2.4, $G_2^{(4)}(R)$ has one component and $\operatorname{indeg}^{(4)} 0 = 9$. Since $4 = \operatorname{indeg}^{(4)} 1 \neq \operatorname{indeg}^{(4)} 0 = 9$, Com(1) and Com(0) are not isomorphic. Thus, set $N = 3$, $l_1 = 3$, by Theorem 4.2.2 (1), $G_1^{(4)}(R)$ is symmetric of order 3, but by Theorem 4.2.1, $G^{(4)}(R)$ is not symmetric of order 3. The digraph $G^{(4)}(R)$ is shown below.



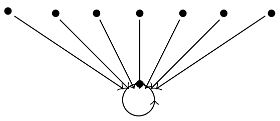
$G_1^{(4)}(R)$



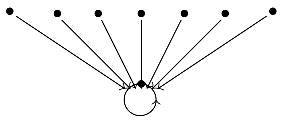
$G_2^{(4)}(R)$

(3) Let $R = \mathbb{Z}_{2^2}[x]/((x+1)^2)$ and $k = 4$. From Theorem 2.2.1, we have $s = 1$ and $\lambda(R) = 2^{1+2-1}(2^1 - 1) = 4$. Then $u = 1$ and all divisors d of u is 1. By Theorem 3.1.1, $G_1^{(4)}(R)$ contains 1-cycles. It follows from Theorem 3.1.3 that $A_1(G_1^{(4)}(R)) = \gcd(2^1 - 1, 4 - 1) = 1$. For each component of $G_1^{(4)}(R)$, the maximum distance from a vertex in the component to the unique cycle of the component is $l = \lceil \frac{2}{2} \rceil = 1$ by Theorem 3.2.1. Then $\operatorname{indeg}^{(4)} 1 = |R^\times| = 8$.

Since $k = 2^2$ and $r = 1$, by Theorem 4.2.7, $G^{(4)}(R)$ is symmetric of order 2 and we can draw the digraph $G^{(4)}(R)$ below.

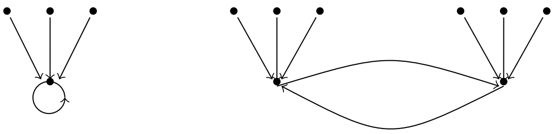


$G_1^{(4)}(R)$

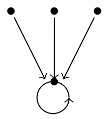


$G_2^{(4)}(R)$

(4) Let $R = \mathbb{F}_{2^2}[x]/((x+3)^2)$ and $k = 2$. From Theorem 2.2.1, $s = 1$ and $\lambda(R) = 2(2^2-1) = 2(3)$. Then $u = 3$ and all divisors d of u are 1, 3. By Theorem 3.1.1, $G_1^{(2)}(R)$ contains 1-cycles and 2-cycles. It follows from Theorem 3.1.3 that $A_1(G_1^{(2)}(R)) = 1$ and $A_2(G_1^{(2)}(R)) = 1$. For each component of $G_1^{(2)}(R)$, the maximum distance from a vertex in the component to the unique cycle of the component is $l = \lceil \frac{1}{1} \rceil = 1$ by Theorem 3.2.1. Since $|R^\times| = 4(3)$ and by Corollary 3.2.3, $\mathrm{indeg}^{(2)}\, 1 = 4$. Since $k = 2 \geq a = 2$, by Theorem 3.2.4, $G_2^{(2)}(R)$ has one component and $\mathrm{indeg}^{(2)}\, 0 = 4$. The digraph $G^{(2)}(R)$ is shown below.

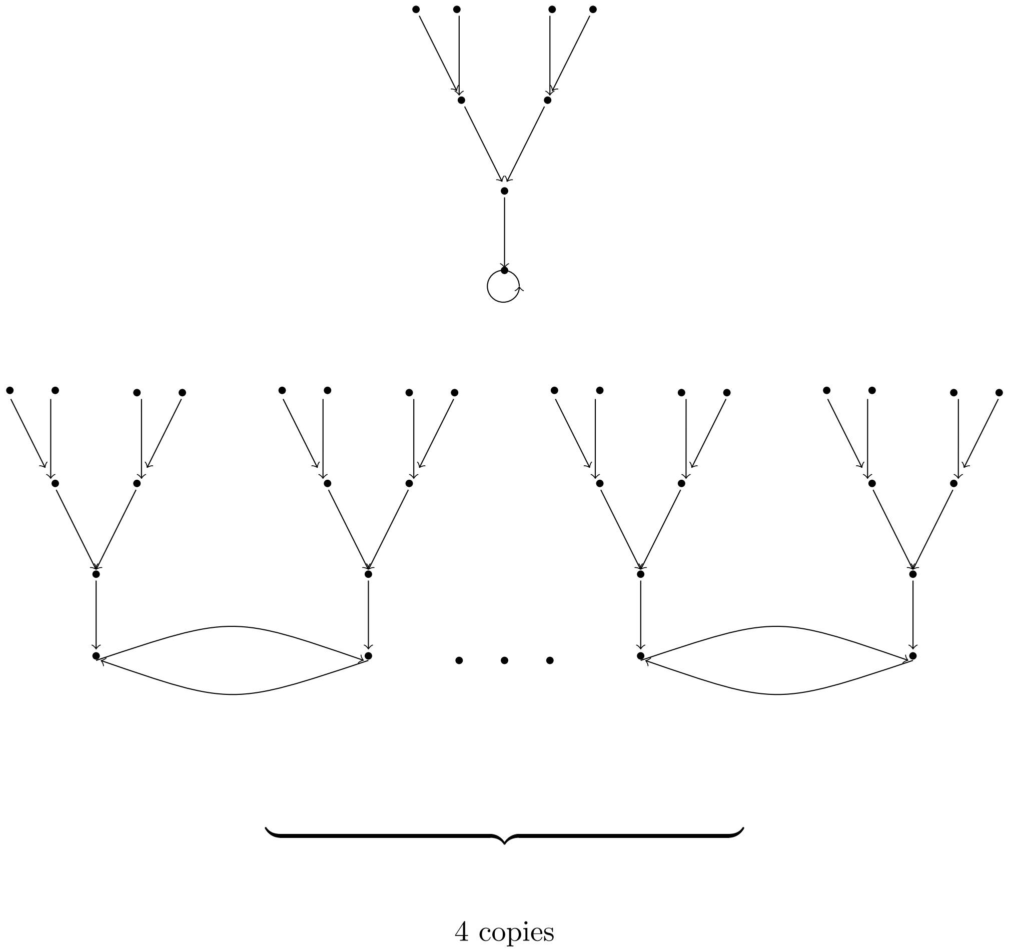


$G_1^{(2)}(R)$

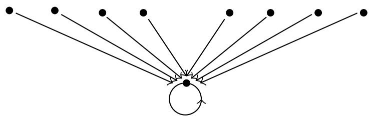


$G_2^{(2)}(R)$

(5) Let $R = GR(3^2,1)[x]/(x^2+1)$ and $k = 2$. Then by Theorem 2.3 (2) in [2], $R = GR(3^2,2)$. Then it suffices to consider the digraph over $GR(3^2,2)$. By Theorem 1.3.4 (1), $\lambda(R) = 3(8)$. We have $u = 3$, so all divisors d of u are 1 and 3. By Theorem 3.1.1, $G_1^{(2)}(R)$ contains 1-cycles and 2-cycles. From Theorem 3.1.4 (1), $A_1(G_1^{(2)}(R)) = 1$ and $A_2(G_1^{(2)}(R)) = 4$. For each component of $G_1^{(2)}(R)$, the maximum distance from a vertex in the component to the unique cycle of the component is $l = \lceil \frac{3}{1} \rceil = 3$ by Theorem 3.2.1. It follows from Corollary 4.1.3 (1) that $\text{indeg}^{(2)}\, 1 = \gcd(3^2 - 1, 2)(\gcd(3^{2-1}, 2))^2 = 2$. Since $k = 2 \geq n = 2$, by Theorem 3.2.4, $G_2^{(2)}(R)$ has one component and $\text{indeg}^{(2)}\, 0 = 9$. The digraph $G^{(2)}(R)$ is displayed below.



$G_1^{(2)}(R)$



$G_2^{(2)}(R)$

REFERENCES

[1] Bini G., Flamini F.: *Finite Commutative Rings and Their Applications*, Kluwer Academic Publishers, Massachusetts, 2002.

[2] Chen W., Su H., Tang G.: Units on the Gauss extension of a Galois ring, *Algebra and Its Appl.* Vol. 15, No. 2 (2016), 1–9.

[3] Deng G., Somer L.: On the symmetric digraphs from the kth power mapping on a finite commutative ring, *Discrete Math., Algorithms and Appl.*, Vol. 7, No. 1 (2015), 1–15.

[4] Hou X.D., Leung K.H., Ma S.L.: On the group of units of finite commutative chain rings, *Finite Fields Appl.* **9** (2003), 20–38.

[5] Křížek M., Somer L.: On a connection of number theory with graph theory, *Czechoslovak Math. J.* **54** (2004), 465–485.

[6] Křížek M., Somer L.: On symmetric digraphs of the congruences $x^k \equiv y \pmod{n}$, *Discrete Math.* **309** (2009), 1999–2009.

[7] Maingam N., Meemark Y.: The digraphs of the square mapping on quotient rings over the Gaussian integers, *Int. J. Number Theory.* **7** (2011), 835–852.

[8] McDonald B.R.: *Finite Rings with Identity*, Marcel Dekker, New York, 1974.

[9] Meemark Y., Tocharoenirattisai I.: Exponent of local ring extension of Galois rings and digraphs of the kth power mapping, *Turk. J. Math.*, to appear.

[10] Meemark Y., Wiroonsri N.: The quadratic digraph on polynomial rings over finite fields, *Finite Fields Appl.* **16** (2010), 334–346.

[11] Meemark Y., Wiroonsri N.: The digraphs of the kth power mapping of the quotient ring of polynomial ring over finite fields, *Finite Fields Appl.* **18** (2012), 179–191.

[12] Nan J.H., Tang G.H., Wei Y.J.: The iteration digraphs of group rings over finite fields, *Algebra and Its Appl.* **5** (2014), 1–19.

[13] Su H.D., Tang G.H., Wei Y.J.: The square mapping graphs of finite commutative rings, *Algeb. Collo.* **19** (3) (2012), 569–580.

[14] Tang G.H., Wei Y.J.: The iteration digraphs of finite commutative rings, *Turk. J. Math.* **39** (2015), 872–883.

[15] Wan Z.X.: *Lectures on Finite Fields and Galois Rings*, World Scientific Publishing, River Edge, NJ, 2003.

VITA

Name	Mr. Ittiwat Tocharoennirattisai
Date of Birth	3 December 1988
Place of Birth	Bangkok, Thailand
Education	B.Sc. (Mathematics, Second Class Honours), Mahidol University, 2011
Scholarship	Science Achievement Scholarship of Thailand, (SAST), and Graduate School