Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2017) 41: 223 – 234
© TÜBİTAK
doi:10.3906/mat-1601-134

Exponent of local ring extensions of Galois rings and digraphs of the kth power mapping

Ittiwat TOCHAROENIRATTISAI, Yotsanan MEEMARK*
Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok, Thailand

Received: 30.01.2016 • **Accepted/Published Online:** 18.04.2016 • **Final Version:** 03.04.2017

Abstract: In this paper, 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 complete 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 $G_2^{(k)}(R)$ are determined by the nilpotency of maximal ideal M of R.

Key words: Finite chain rings, Galois rings, symmetric digraphs

1. Introduction

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 $g \in G$. It gives some information on the order of an element of G. Note that $\exp G$ divides $|G|$. In particular, $\exp G = \text{lcm}\{o(a) : a \in G\}$, where $o(a)$ is the order of a in G. Moreover, if $G = G_1 \times G_2$, then $\exp G = \text{lcm}(\exp G_1, \exp G_2)$. 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.

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, $\lambda(R) = \exp(R^\times)$. We can easily determine the exponent of R if the structure of the group of units is known. That is the case for 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 [4, 5]. A *local ring* is a commutative ring with identity that has a unique maximal ideal.

Let n and d be positive integers and let p be a prime. Then there exists a monic polynomial $f(x)$ in $\mathbb{Z}_{p^n}[x]$ of degree d such that the reduction $\overline{f}(x)$ in $\mathbb{Z}_p[x]$ is irreducible. Consider the ring extension $\mathbb{Z}_{p^n}[x]/(f(x))$, called a *Galois ring*. It can be proved that up to isomorphism this Galois ring is unique and hence we may denote it by $GR(p^n, d)$. Observe that $GR(p^n, 1) = \mathbb{Z}_{p^n}$ and $GR(p, d) = \mathbb{F}_{p^d}$, the field of p^d elements. The Galois ring $GR(p^n, d)$ is a local ring of characteristic p^n with maximal ideal

*Correspondence: yotsanan.m@chula.ac.th
2010 *AMS Mathematics Subject Classification:* 11R58.

$pGR(p^n, d)$ and residue field isomorphic to $\mathbb{F}_{p^d}$. Its unit group is well studied and is presented with its exponent below.

Theorem 1.1 (Theorem XVI.9 of [6]) *$GR(p^n, d)^\times \cong H \times \mathbb{F}_{p^d}^\times$, 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.*

A *finite chain ring* R is a finite commutative ring such that for any two ideals I and J of R, we have $I \subseteq J$ or $J \subseteq I$. It is a finite local ring with maximal principal ideal. Thus, a Galois ring is a finite chain ring. By Theorem XVII.5 of [6], any finite chain ring R of nilpotency s is isomorphic to an extension ring

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

for some positive integers n, d, and e; a prime p; and $z(x) = x^e + p(a_{e-1}x^{e-1} + \cdots + a_0)$, $a_0 \in GR(p^n, d)^\times$, $a_1, \ldots, a_{e-1} \in GR(p^n, d)$, called an Eisenstein polynomial of degree e. Moreover, the group of units of a finite chain ring was explicitly determined by Hou et al. [3]. Therefore, the exponent of a finite chain ring is known. Recently, Chen et al. [1] 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 [2, 7–9]. This motivated Dang and Somer [2] to compute without the explicit structure of 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 over $\mathbb{F}_q[x]$.

Let R be a finite commutative ring with identity 1. For $k \geq 2$, let $G^{(k)}(R)$ be the kth power mapping digraph over R 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 that 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 that are in the unit group $R^\times$ and induced on the remaining vertices that 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, $G^{(k)}(R) = G_1^{(k)}(R) \ \dot{\cup} \ G_2^{(k)}(R)$.

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) a and is denoted by $\text{indeg}^{(k)} a$ (respectively, $\text{outdeg}^{(k)} a$). 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 1.2 *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.*

This functional digraph is defined using the idea of Somer and Křížek [4], who studied the structure of digraphs $G^{(2)}(\mathbb{Z}_n)$. Later, they worked on the kth power mapping digraph $G^{(k)}(\mathbb{Z}_n)$ [5]. Meemark and Wiroonsri [8, 9] 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, Meemark and Maingam [7] studied the digraphs $G^{(2)}(\mathbb{Z}[i]/(\gamma))$, where $\mathbb{Z}[i]$ is the ring of Gaussian integers and $\gamma = a + bi$ is a nonzero element in $\mathbb{Z}[i]$. Next, Wei et al. [11] 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 2, 3, and 4 components. Later, Wei et al. [10] 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. Deng and Somer [2] worked on the digraphs $G^{(k)}(R)$, where R is a finite commutative ring of characteristic p. Recently, Wei and Tang [12] generalized results on cycles, components, and semiregularity to finite commutative rings. They also continued working more on symmetric digraphs.

In what follows, 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 complete determination of its group structure in Section 2. Applying this result leads to better analysis of the iteration graphs $G^{(k)}(R)$ including the conditions on symmetric digraphs in the last two sections.

2. The exponent

In this section, 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. It is a local ring of characteristic p^n with maximal ideal

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

Then $|R| = p^{ndra}$, $|M| = p^{dr(na-1)}$, and $R/M \cong \mathbb{F}_{p^{dr}}$. If $a = 1$, then it follows from Theorem 14.23 of [13] that R is isomorphic to $GR(p^n, dr)$, so its exponent is presented in Theorem 1.1. Now we assume that $a \geq 2$ and proceed to compute the exponent of R. Recall that $R^\times \cong (1 + M) \times \mathbb{F}_{p^{dr}}^\times$ and $\mathbb{F}_{p^{dr}}^\times$ is cyclic of order $p^{dr} - 1$, so it suffices to determine the exponent of the p-group $1 + M$. Following Deng and Somer [2], we 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 the field 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 starts by deriving some facts on the maximum power of p that is binomial coefficients using the de Polignac formula. We divide them into four lemmas as follows. The proofs of the first two lemmas are routine and hence are omitted.

Lemma 2.1 $e_p(\binom{p^n}{l_1}) = e_p(\binom{p^n}{l_2})$, *where* $1 \le l_1, l_2 \le p-1$ *and* $n \in \mathbb{N}$. *Moreover,* $e_p(\binom{p^n}{l_1}) = n$.

Lemma 2.2 *Let* $a \ge 2$, *and* $s, n \in \mathbb{N}$, *where* $p^{s-1} < a \le p^s$. *For* $0 \le i \le s-2$, $1 \le k \le (p-1)p^{s-2-i}-1$. *Then:*

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

(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* $1 \le l_1, l_2 \le p-1$. *Moreover,* $e_p(\binom{p^{s+n-1}}{p^{s-1-i}+l_1}) \ge n$.

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

(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* $1 \le l_1, l_2 \le p-1$. *Moreover,* $e_p(\binom{p^{s+n-1}}{p^{s-1-i}+kp+l_1}) \ge n$.

Lemma 2.3 (1) $e_p(\binom{p^{s+n-1-t}}{p^{s-1}}) = n-t$ *for all* $t \in \mathbb{N}$.

(2) $(1+f+(f^a))^{p^{s+n-1-t}} \ne 1+(f^a)$ *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

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

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 2.4 *$e_p(m!) < \frac{m}{p-1}$ 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,

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

□

Now we are ready to compute the exponent.

Theorem 2.5 *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 $h(x) \in pGR(p^n,d)[x]$, $l(x) \in GR(p^n,d)[x]$, $\deg h < r$, $\deg l < r(a-1)$. Then

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

Since $h(x) \in pGR(p^n,d)[x]$, we have $h(x)^j \in p^jGR(p^n,d)[x]$ for all $j \in \mathbb{N}$. By Lemma 2.4, $e_p(j!) < j$ 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 and 2.2 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 2.3 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, $\lambda(GR(p^n,d)[x]/(f(x)^a)) = \mathrm{lcm}(\exp(1+M), \exp\mathbb{F}_{p^{dr}}^{\times}) = p^{s+n-1}(p^{dr}-1)$. □

3. Cycles and components

In this section, we find necessary and sufficient conditions for the existence of a t-cycle with $t \geq 1$ in $G_1^{(k)}(R)$, and we find the number of t-cycles in $G_1^{(k)}(R)$ for a finite commutative ring R with identity. Later, we present some properties in $G_2^{(k)}(R)$ over a finite local ring R.

3.1. Number of cycles

For a finite commutative ring R with identity, we set $\lambda(R) = uv$, where u is the largest divisor of $\lambda(R)$ relatively prime to k.

Theorem 3.1 *Let R be a finite commutative ring with identity. Let t be a positive integer, and $k \geq 2$. The following statements are equivalent:*

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

(2) *There exists $b \in R^\times$ with t 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 t-cycle, and 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 3.2 *Let R be a finite commutative ring with identity, and let $k \geq 2$. If $k \equiv 1 \pmod u$, then every cycle in $G_1^{(k)}(R)$ is a fixed point.*

Proof Assume that $k \equiv 1 \pmod u$. Since $d \mid u$, $d \mid k - 1$. This mean that $1 = \operatorname{ord}_d k$ for all divisors d of u. By Theorem 3.1, 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 $1 + M \cong \mathbb{Z}_{p^{s_1}} \times \mathbb{Z}_{p^{s_2}} \times \cdots \times \mathbb{Z}_{p^{s_q}}$, where 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 3.3 *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 setup, and let $k \geq 2$, $t \in \mathbb{N}$. Then*

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

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

Consequently,

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

as required. □

The group of units of the Galois ring $GR(p^n, r)$ presented in Theorem 1.1 gives us the next result.

Theorem 3.4 *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*
$A_t(G_1^{(k)}(R)) = \frac{1}{t}[\gcd(p^r - 1, k^t - 1)(\gcd(p^{n-1}, k^t - 1))^r - \sum_{d|t, d\neq t} dA_d(G_1^{(k)}(R))]$.

(2) *If $p = 2$, and $n \geq 3$, then $A_t(G_1^{(k)}(R)) =$*
$\frac{1}{t}[\gcd(2^r - 1, k^t - 1)\gcd(2, k^t - 1)\gcd(2^{n-2}, k^t - 1)(\gcd(2^{n-1}, k^t - 1))^{r-1} - \sum_{d|t, d\neq t} dA_d(G_1^{(k)}(R))]$.

3.2. Distance

Let R be a finite commutative ring with identity. First, 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 [9].

Theorem 3.5 *Let R be a finite commutative ring with identity, and let $k = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, where $p_1, p_2, \dots, p_r$ are distinct primes, $k_i \geq 1$ for all i. Write $\lambda(R) = \exp(R^\times) = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} m$, $a_i \geq 0$ 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 $l = \max_{1\leq i\leq r} \lceil \frac{a_i}{k_i} \rceil$.*

Theorem 3.6 *Let R be a finite commutative ring with identity, and let $k \geq 2$. The set*

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

where l is given in Theorem 3.5, consists of all vertices of the component containing 1. Moreover, every H is on the tree attached to the fixed point 1.

Corollary 3.7 *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 a t-cycle are isomorphic.*

For the graph $G_2^{(k)}(R)$, we 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 $(r + M)(\eta + M^{i+1}) = r\eta + M^{i+1}$ for all $r \in R$ 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 3.8 *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 $\text{indeg}^{(k)}\, 0 \geq p^{r(n-1-T)}$, where $T = \sum_{i=1}^{\lceil \frac{s}{k} \rceil - 1} t_i$ and $l = \lceil \log_k s \rceil$. In particular, if $k \geq s$, then $G_2^{(k)}(R)$ has one component and $\text{indeg}^{(k)}\, 0 = |M| = p^{r(n-1)}$; that is, every directed edge terminates at 0.*

Proof If $k \geq s$, then the result is immediate. Next, we assume that $k < s$. Clearly, $M^{\lceil \frac{s}{k} \rceil} \subseteq \{x \in M : x^k = 0\}$. Thus, $\text{indeg}^{(k)}\, 0 = |\{x \in M : x^k = 0\}| \geq |M^{\lceil \frac{s}{k} \rceil}| = p^{r(n-1-T)}$, 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. □

In particular, for a finite chain ring R with unique maximal ideal M and residue field $R/M \cong \mathbb{F}_{p^r}$, we have for any $\theta \in M \smallsetminus M^2$, $M = R\theta$ 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 $|M^i/M^{i+1}| = p^r$ for all $1 \leq i \leq s-1$, so

$|R| = p^{rs}$, $|M| = p^{r(s-1)}$ and $|M^j| = p^{r(s-j)}$ for all $1 \le j \le s$. Therefore, the above theorem implies the next corollary.

Corollary 3.9 *Let R be a finite chain ring with unique maximal ideal M 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 $k \ge 2$. Then $\operatorname{indeg}^{(k)} 0 = p^{r(s-\lceil \frac{s}{k} \rceil)}$ and $l = \lceil \log_k s \rceil$. In particular, if $k \ge s$, then $G_2^{(k)}(R)$ has one component and $\operatorname{indeg}^{(k)} 0 = |M| = p^{r(s-1)}$; that is, every directed edge terminates at 0. Moreover, if $R = GR(p^n, r)$ is a Galois ring, the result holds with $s = n$.*

Proof If $k \ge s$, 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, $\operatorname{indeg}^{(k)} 0 = |\{x \in M : x^k = 0\}| = |M^{\lceil \frac{s}{k} \rceil}| = p^{r(s-\lceil \frac{s}{k} \rceil)}$. By Theorem 3.8, the maximum distance from a vertex in the component to the unique cycle of the component is $\lceil \log_k s \rceil$. □

4. Symmetric digraphs

In this section, we present some conditions when the digraphs are symmetric using the exponents discovered in the previous sections. Let R be a finite commutative ring with identity. Let $N \ge 2$ be an integer. The digraph $G^{(k)}(R)$ 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 any $a \in R$, the component contains vertex a, which is denoted by $\operatorname{Com}(a)$. The following results are immediate.

Theorem 4.1 *Let R be a finite local ring and let $k \ge 2$. If $G_1^{(k)}(R)$ is symmetric of order $N \ge 2$, then $G^{(k)}(R)$ is not symmetric of order N.*

Theorem 4.2 *Let R be a finite local ring and let $k \ge 2$, $t_i \in \mathbb{N}$.*

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

We also need the $\operatorname{indeg}^{(k)} 1$ recalled in the next theorem.

Theorem 4.3 (Theorem 2.3 of [12]) *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 $k \ge 2$. Assume that*

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

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

Together with Theorem 1.1, we have:

Corollary 4.4 *Let $R = GR(p^n, r)$ be a Galois ring, where n, r are positive integers and 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* $\operatorname{indeg}^{(k)} 1 = \gcd(2^r - 1, k)\gcd(2, k)\gcd(2^{n-2}, k)(\gcd(2^{n-1}, k))^{r-1}$.

First, we study symmetric digraphs over Galois rings.

Theorem 4.5 *Let $R = GR(p^n, r)$ be a Galois ring, where n, r are positive integers and 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 1.1 (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 3.2, every cycle in $G_1^{(k)}(R)$ is a fixed point. Also, Theorem 3.4 (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 3.5 if $j > 0$. Because $j \geq n - 1$, $k = p^j m \geq n$ and by Theorem 3.8, $G_2^{(k)}(R)$ has one component and $\operatorname{indeg}^{(k)} 0 = |R| - |R^\times|$. Corollary 4.4 (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 3.7 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 4.6 *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 1.1, $\lambda(R) = 2^{n-1}(2^r - 1)$, so $u = 2^r - 1$, and odd prime. 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 3.4. 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 3.4,

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

Since $A_t(G_1^{(k)}(R))$ is a positive integer and t is odd, $A_t(G_1^{(k)}(R))$ is even. From $j \geq n - 1$, $k = 2^j \geq n$. This implies that $G_2^{(k)}(R)$ has one component and $\operatorname{indeg}^{(k)} 0 = |R| - |R^\times|$ by Theorem 3.8. Theorem 3.5 gives $l = \lceil \frac{n-1}{j} \rceil = 1$. Thus, it follows from Corollary 4.4 that

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

Since $l = 1$, $\mathrm{Com}(0) \cong \mathrm{Com}(1)$. By Corollary 3.7 and $A_t(G_1^{(k)}(R))$ being even ($t > 1$), we finally have that $G^{(k)}(R)$ is symmetric of order 2. $\square$

Next, we study symmetric digraphs over local extension rings $R = GR(p^n, d)[x]/(f(x)^a)$, $a \geq 2$, in Theorems 4.7–4.9. To use the exponent, we let s be a positive integer such that $p^{s-1} < a \leq p^s$.

Theorem 4.7 *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 $p \nmid \mathrm{indeg}^{(k)}\, 1$ but $p \mid \mathrm{indeg}^{(k)}\, 0$. Assume that $j \geq 1$. By Theorem 2.5, $\lambda(R) = p^{s+n-1}(p^{dr} - 1)$. By Theorem 3.5, 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 3.8. Hence, $G^{(k)}(R)$ is not symmetric of any order $N \geq 2$. $\square$

Theorem 4.8 *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 4.3, $\mathrm{indeg}^{(k)}\, 1 = \gcd(p^{dr} - 1, k)$, which is not a power of p. However, because $k \geq na$, it follows from Theorem 3.8 that $G_2^{(k)}(R)$ has one component and $\mathrm{indeg}^{(k)}\, 0 = |R| - |R^\times| = p^{dr(na-1)}$, which is a power of p. Hence, $G^{(k)}(R)$ is not symmetric of any order $N \geq 2$. $\square$

Theorem 4.9 *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 2.5, $\lambda(R) = p^{s+n-1}(p^{dr} - 1)$. 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 3.2. Also, $A_1(G_1^{(k)}(R)) = p^{dr} - 1$ by Theorem 3.3. Since $j \geq s + n - 1$, $k \geq na$, and so $G_2^{(k)}(R)$ has one component and $\mathrm{indeg}^{(k)}\, 0 = |R| - |R^\times| = p^{dr(na-1)}$ by Theorem 3.8. In addition, $l = \lceil \frac{s+n-1}{j} \rceil = 1$ by Theorem 3.5. Recall that $|R^\times| = p^{dr(na-1)}(p^{dr} - 1)$ and $A_1(G_1^{(k)}(R)) = p^{dr} - 1$, so

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

Hence, $\mathrm{Com}(0) \cong \mathrm{Com}(1)$. Since there are $p^{dr} - 1$ components with 1-cycles in $G_1^{(k)}(R)$ and they are all isomorphic by Corollary 3.7, together with $\mathrm{Com}(0) \cong \mathrm{Com}(1)$, we can conclude that $G^{(k)}(R)$ is symmetric of order p^{dr}. $\square$

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 4.10 *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 4.3 that $\mathrm{indeg}^{(k)}\, 1$ is not a power of p. However, $\mathrm{indeg}^{(k)}\, 0$ is a power of p by Corollary 3.9. Hence, Corollary 3.7 implies that $G^{(k)}(R)$ is not symmetric of any order $N \geq 2$. $\square$

Theorem 4.11 *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 $\text{indeg}^{(k)} 1 = \gcd(p^d - 1, k)$ and $p \nmid \gcd(p^d - 1, k)$. By Corollary 3.9, we have $p \mid \text{indeg}^{(k)} 0$. Hence, it follows from Corollary 3.7 that $G^{(k)}(R)$ is not symmetric of any order $N \geq 2$. □

Theorem 4.12 *If $k = p^j m$, where $p \nmid m$, $p^d - 1 \mid k - 1$ and $\text{Com}(1) \cong \text{Com}(0)$, then $G^{(k)}(R)$ is symmetric of order p^d.*

Proof Its proof is similar to that of Theorem 4.5 and omitted. □

Acknowledgment

The first author wishes to thank his adviser (the second author) for motivation and encouragement to write this paper. He also wishes to thank the Science Achievement Scholarship of Thailand, SAST, which supported him during his undergraduate and graduate studies. Next, he expresses his gratitude to the Graduate School of Chulalongkorn University, which gave him an opportunity to present this research at the Fq12 conference last year.

References

[1] Chen W, Su H, Tang G. Units on the Gauss extension of a Galois ring. J Algebra Appl 2016; 15: 1-9.

[2] Deng G, Somer L. On the symmetric digraphs from the kth power mapping on a finite commutative ring. Discrete Math 2015; 7: 1-15.

[3] Hou XD, Leung KH, Ma SL. On the group of units of finite commutative chain rings. Finite Fields Appl 2003; 9: 20-38.

[4] Křížek M, Somer L. On a connection of number theory with graph theory. Czech Math J 2004; 54: 465-485.

[5] Křížek M, Somer L. On symmetric digraphs of the congruences $x^k \equiv y \pmod{n}$. Discrete Math 2009; 309: 1999-2009.

[6] McDonald BR. Finite Rings with Identity. New York, NY, USA: Marcel Dekker, 1974.

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

[8] Meemark Y, Wiroonsri N. The quadratic digraph on polynomial rings over finite fields. Finite Fields Appl 2010; 16: 334-346.

[9] Meemark Y, Wiroonsri N. The digraphs of the kth power mapping of the quotient ring of polynomial ring over finite fields. Finite Fields Appl 2012; 18: 179-191.

[10] Nan JH, Tang GH, Wei YJ. The iteration digraphs of group rings over finite fields. J Algebra Appl 2014; 5: 1-19.

[11] Su HD, Tang GH, Wei YJ. The square mapping graphs of finite commutative rings. Algeb Collo 2012; 19: 569-580.

[12] Tang GH, Wei YJ. The iteration digraphs of finite commutative rings. Turk J Math 2015; 39: 872-883.

[13] Wan ZX. Lectures on Finite Fields and Galois Rings. River Edge, NJ, USA: World Scientific Publishing, 2003.