


Finite Fields and Their Applications 7, 382–396 (2001)

doi:10.1006/fta.2000.0317, available online at <http://www.idealibrary.com> on 

Finite Commutative Chain Rings

Xiang-dong Hou

Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435
E-mail: xhou@euler.math.wright.edu

Communicated by Dieter Jungnickel

Received January 21, 2000; revised October 19, 2000; published online June 11, 2001

A commutative ring with identity is called a chain ring if all its ideals form a chain under inclusion. A finite chain ring, roughly speaking, is an extension over a Galois ring of characteristic p^n using an Eisenstein polynomial of degree k . When $p \nmid k$, such rings were classified up to isomorphism by Clark and Liang. However, relatively little is known about finite chain rings when $p \mid k$. In this paper, we allowed $p \mid k$. When $n = 2$ or when $p \parallel k$ but $(p - 1) \nmid k$, we classified all pure finite chain rings up to isomorphism. Under the assumption that $(p - 1) \nmid k$, we also determined the structures of groups of units of all finite chain rings. © 2001 Academic Press

Key Words: finite chain ring; Galois ring; group of units.

1. INTRODUCTION

All rings considered in this paper are commutative with identity unless specified otherwise. A ring is called a chain ring if all its ideals form a chain under inclusion. Finite chain rings are precisely finite local rings whose maximal ideals are principal. As pointed out by Clark and Liang [3], finite chain rings arise in algebraic number theory as quotient rings of rings of integers in number fields [10] and in geometry as coordinatizing rings of Hjelmslev planes [9]. More references on the role of finite chain rings in Hjelmslev planes and Klingenberg planes can be found in [2, 15]. Recently, finite chain rings have been used in various constructions of partial difference sets, relative difference sets, and bent functions [6, 7, 11, 12]. One of the properties of finite chain rings that make them useful in those combinatorial constructions is that every finite chain ring has a “non-degenerate” character [7]. Chain rings (without the finiteness condition), also known as valuation rings, play a central role in module theory [4, 5]. Noncommutative chain



rings (defined in the same way) are useful in the structure of certain types of noncommutative rings. (See, for example, [1].)

The main concerns of this paper are two basic questions about finite chain rings: their classification and their groups of units.

All finite chain rings can be obtained through the following construction. We refer the reader to [13, pp. 307–308, 339–349] for the proofs of the claims in the construction. Let p be a prime, $n, r > 0$, and $f \in \mathbb{Z}_{p^n}[x]$ a monic polynomial of degree r whose image in $\mathbb{Z}_p[x]$ is irreducible. Then $GR(p^n, r) = \mathbb{Z}_{p^n}[x]/(f)$ is a ring whose structure depends only on p, n , and r . $GR(p^n, r)$ is called a Galois ring of characteristic p^n and rank r [8, 14]. $GR(p^n, r)$ is a local ring whose maximal ideal is $pGR(p^n, r)$. Every finite chain ring is of the form

$$GR(p^n, r)[x]/(g, p^{n-1}x^t), \quad (1.1)$$

where $g \in GR(p^n, r)[x]$ is an Eisenstein polynomial of degree k , i.e., $g = x^k - p(a_{k-1}x^{k-1} + \cdots + a_0)$ ($a_i \in GR(p^n, r)$ and a_0 is a unit of $GR(p^n, r)$), $t = k$ when $n = 1$, and $1 \leq t \leq k$ when $n \geq 2$. The integers p, n, r, k, t are called the invariants of the chain ring in (1.1) [3]. A basic problem, which seems to be very difficult, is to classify finite chain rings with fixed invariants up to isomorphism. We call the finite chain ring in (1.1) a pure finite chain ring if $g = x^k - pa_0$. When $p \nmid k$, Clark and Liang [3] classified all pure finite chain rings with fixed invariants p, n, r, k, t up to isomorphism. Moreover, they showed that when $p \nmid k$, every finite chain ring is pure [3]. Thus all finite chain rings with invariants p, n, r, k, t are classified up to isomorphism when $p \nmid k$. However, when $p|k$, little is known about the isomorphism classes of finite chain rings, even if the finite chain rings are pure. In this paper, we will allow $p|k$. The first main result of this paper is a classification of pure finite chain rings with invariants p, n, r, k, t up to isomorphism when $n = 2$ or when $p \parallel k$ but $(p-1) \nmid k$. ($p \parallel k$ means $p|k$ but $p^2 \nmid k$.) In particular, the numbers of isomorphism classes of pure finite chain rings in these cases are given.

The group of units of a finite commutative local ring is an essential piece of information about the structure of the ring. In general, the structure of such a group of units is difficult to determine. For Galois rings, the structures of their groups of units are known [13, pp. 322–323]. But for finite chain rings, such structures are not known. As the second main result of this paper, we will determine the structure of the group of units of a finite chain ring with invariants p, n, r, k, t under the assumption $(p-1) \nmid k$.

The paper is organized as follows. In Section 2, we review some basic facts about Galois rings and finite chain rings to be used in the sequel. In Section 3, we classify all pure finite chain rings under the assumptions described earlier. Section 4 deals with multiplicative orders of elements in $1 + m$, where m is the maximal ideal of a finite chain ring. In Section 5, we determine the structure of the group of units of an arbitrary finite chain ring with $(p-1) \nmid k$.

2. GALOIS RINGS AND FINITE CHAIN RINGS

We refer the reader to [13, pp. 322–323, 339–349] for the proofs of the facts about Galois rings and finite chain rings quoted in this section.

The Galois ring $GR(p^n, r)$ is a local ring with maximal ideal $pGR(p^n, r)$ and $GR(p^n, r)/pGR(p^n, r) = GF(p^r)$. Its multiplicative group (group of units) $GR(p^n, r)^*$ contains a unique cyclic subgroup T^* of order $p^r - 1$. $T = T^* \cup \{0\}$ is called the Teichmüller set of $GR(p^n, r)$ and it forms a system of coset of representatives of $GR(p^n, r)/pGR(p^n, r)$. Every element $a \in GR(p^n, r)$ has a unique p -adic expansion

$$a = \xi_0 + p\xi_1 + \dots + p^{n-1}\xi_{n-1} \quad (\xi_i \in T). \tag{2.1}$$

The map

$$\begin{aligned} \sigma: \quad GR(p^n, r) &\rightarrow GR(p^n, r) \\ \xi_0 + p\xi_1 + \dots + p^{n-1}\xi_{n-1} &\mapsto \xi_0^p + p\xi_1^p + \dots + p^{n-1}\xi_{n-1}^p \end{aligned} \tag{2.2}$$

is called the Frobenius map of $GR(p^n, r)$. σ is an automorphism of $GR(p^n, r)$ of order r and $\text{Aut}(GR(p^n, r)) = \langle \sigma \rangle$. We have

$$GR(p^n, r)^* = T^* \cdot (1 + pGR(p^n, r)) \cong T^* \times (1 + pGR(p^n, r)), \tag{2.3}$$

where

$$1 + pGR(p^n, r) \cong \begin{cases} \mathbb{Z}_{p^{r-1}}, & \text{if } p \text{ is odd, or if } p = 2 \text{ and } n \leq 2, \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_{2^{r-1}}, & \text{if } p = 2 \text{ and } n \geq 3. \end{cases} \tag{2.4}$$

It follows easily from (2.4) that if p is odd or if $p = 2$ and $n \leq 2$,

$$(1 + pGR(p^n, r))^{p^i} = 1 + p^{i+1}GR(p^n, r), \quad i \geq 0. \tag{2.5}$$

Let R be the finite chain ring in (1.1) with invariants p, n, r, k, t . The maximal ideal of R is xR and the nilpotency of x is $(n - 1)k + t$. R has the same residue field as $GR(p^n, r)$: $R/xR = GR(p^n, r)/pGR(p^n, r) = GF(p^r)$. Every element $y \in R$ can be written as

$$y = a_0 + a_1x + \dots + a_{k-1}x^{k-1}, \quad a_i \in GR(p^n, r), \tag{2.6}$$

where a_0, \dots, a_{t-1} are unique and a_t, \dots, a_{k-1} are unique modulo $p^{n-1}GR(p^n, r)$. The group of units R^* of R also has a similar decomposition:

$$R^* = T^* \cdot (1 + xR) \cong T^* \times (1 + xR). \tag{2.7}$$

However, the structure of the multiplicative group $1 + xR$ is more interesting than that of $1 + pGR(p^n, r)$, as we will see in Section 5. Note that when $n = 1$, $R = GF(p^r)[x]/(x^k)$. Such rings need no classification.

3. CLASSIFICATION OF PURE FINITE CHAIN RINGS

LEMMA 3.1. *Let*

$$R = GR(p^n, r) [x]/(x^k - pu, p^{n-1} x^t) \tag{3.1}$$

$$S = GR(p^n, r) [x]/(x^k - pv, p^{n-1} x^t) \tag{3.2}$$

be two pure finite chain rings, where $n \geq 2, 1 \leq t \leq k, u, v \in GR(p^n, r)^*$, and let \bar{u}, \bar{v} be the images of u, v in $GR(p^n, r)/\text{ann}(p) = GR(p^{n-1}, r)$. Then $R \cong S$ if and only if there exists a $\rho \in \text{Aut}(GR(p^{n-1}, r))$ such that in the ring $R/\text{ann}(p) = GR(p^{n-1}, r) [x]/(x^k - p\bar{u}, p^{n-2} x^t)$, the equality

$$\bar{u}^{-1} \rho(\bar{v}) = z^k \tag{3.3}$$

holds for some $z \in GR(p^{n-1}, r) [x]/(x^k - p\bar{u}, p^{n-2} x^t)$.

Proof. By Lemma 4 of [3], $R \cong S$ if and only if there is a $\psi \in \text{Aut}(GR(p^n, r))$ such that $x^k - p\psi(v)$ has a root in R .

Necessity. Since $R \cong S$, there exists an automorphism ψ of $\text{Aut}(GR(p^n, r))$ and an element $w \in R$ with $w^k = p\psi(v)$. Write $w = xz$ for $z \in R$. Then

$$p\psi(v) = x^k z^k = puz^k. \tag{3.4}$$

There is a natural isomorphism $\bar{(\)} : \text{Aut}(GR(p^n, r)) \rightarrow \text{Aut}(GR(p^{n-1}, r))$ such that for any $f \in \text{Aut}(GR(p^n, r))$, the diagram

$$\begin{array}{ccc} GR(p^n, r) & \xrightarrow{f} & GR(p^n, r) \\ \downarrow & & \downarrow \\ GR(p^{n-1}, r) & \xrightarrow{\bar{f}} & GR(p^{n-1}, r) \end{array} \tag{3.5}$$

commutes, where the vertical maps are the natural homomorphisms. Let $\rho = \bar{\psi}$. Then (3.4) implies that in $R/\text{ann}(p), \bar{u}^{-1} \rho(\bar{v}) = z^k$.

Sufficiency. Trace back the proof of necessity. ■

LEMMA 3.2. *Let*

$$R = GR(p^n, r)[x]/(x^k - pu, p^{n-1} x^t), \tag{3.6}$$

where $n \geq 2, 1 \leq t \leq k, u \in GR(p^n, r)^*$.

(i) *if* $p \nmid k$, *then*

$$(R^*)^k \cap GR(p^n, r)^* = (GR(p^n, r)^*)^k. \tag{3.7}$$

(ii) *If* $p \parallel k, (p - 1) \nmid k$ *and* $n \geq 3$ *or* $n = 2$ *but* $t > k/p$, *then*

$$(R^*)^k \cap GR(p^n, r)^* = (GR(p^n, r)^*)^k. \tag{3.8}$$

(iii) If $p \parallel k$, $(p - 1) \nmid k$, $n = 2$, and $t \leq k/p$, then

$$(R^*)^k \cap GR(p^2, r)^* = (T^*)^k \cdot (1 + pGR(p^2, r)), \tag{3.9}$$

where T^* is a the unique cyclic subgroup of order $p^r - 1$ of $GR(p^2, r)^*$

Proof. (i) By (2.3) and (2.7), it suffices to show that $(1 + xR)^k \cap (1 + pGR(p^n, r)) = (1 + pGR(p^n, r))^k$. But since $1 + xR$ and $1 + pGR(p^n, r)$ are p -groups and $p \nmid k$, we have

$$\begin{aligned} (1 + xR)^k \cap (1 + pGR(p^n, r)) &= (1 + xR) \cap (1 + pGR(p^n, r)) \\ &= 1 + pGR(p^n, r) = (1 + pGR(p^n, r))^k. \end{aligned} \tag{3.10}$$

(ii) Again, by (2.3) and (2.7), it suffices to show that

$$(1 + xR)^p \cap (1 + pGR(p^n, r)) = (1 + pGR(p^n, r))^p. \tag{3.11}$$

Assume that $(1 + x^b \varepsilon)^p \in 1 + pGR(p^n, r)$, where $b > 0$, $\varepsilon \in R^*$. We want to show that $(1 + x^b \varepsilon)^p \in (1 + pGR(p^n, r))^p$. If $b \geq k$, we have $(1 + x^b \varepsilon)^p \in (1 + pR)^p \subset 1 + p^2R$. Thus $(1 + x^b \varepsilon)^p \in (1 + p^2R) \cap (1 + pGR(p^n, r)) = 1 + p^2GR(p^n, r) = (1 + pGR(p^n, r))^p$. Therefore, we may assume that $0 < b < k$. Under this assumption, we will show that $(1 + x^b \varepsilon)^p = 1$. Writing

$$\begin{aligned} (1 + x^b \varepsilon)^p &= 1 + px^b \varepsilon + \frac{p(p-1)}{2} x^{2b} \varepsilon^2 + \dots + x^{pb} \varepsilon^p \\ &= 1 + px^b \left(\varepsilon + \frac{(p-1)}{2} x^b \varepsilon^2 + \dots \right) + x^{pb} \varepsilon^p \\ &= 1 + px^b \varepsilon' + x^{bp} \varepsilon^p \quad (\varepsilon' \in R^*) \\ &= 1 + x^{b+k} \eta + x^{bp} \varepsilon^p \quad (\eta \in R^*) \end{aligned} \tag{3.12}$$

it suffices to show that $x^{b+k} \eta + x^{bp} \varepsilon^p = 0$. Note that $x^{b+k} \eta + x^{bp} \varepsilon^p \in pGR(p^n, r)$, since $(1 + x^b \varepsilon)^p \in 1 + pGR(p^n, r)$. Also note that $b + k \neq bp$ since $(p - 1) \nmid k$.

Case 1. $b + k < bp$. Then

$$pGR(p^n, r) \ni x^{b+k} \eta + x^{bp} \varepsilon^p = px^b \eta' \quad \text{for some } \eta' \in R^*. \tag{3.13}$$

We must have $px^b = 0$ since $0 < b < k$.

Case 2. $b + k > bp$.

Case 2.1. $bp \neq k$. Then $bp = ak + c$, where $a \geq 0$, $0 < c < k$, and

$$pGR(p^n, r) \ni x^{b+k} \eta + x^{bp} \varepsilon^p = x^{bp} \eta' = p^a x^c \eta'' \quad (\eta', \eta'' \in R^*). \tag{3.14}$$

Thus $p^a x^c = 0$ since $0 < c < k$.

Case 2.2. $bp = k$. Then we have

$$pGR(p^n, r) \ni x^{b+k} \eta + x^{bp} \varepsilon^p = pu(x^b \eta + \varepsilon^p). \quad (3.15)$$

Write $\varepsilon = z + x^i \delta$, $z \in GR(p^n, r)^*$, $\delta \in R^*$, $i > 0$. Then

$$\begin{aligned} pGR(p^n, r) &\ni pu(x^b \eta + \varepsilon^p) \\ &= pu(x^b \eta + z^p + px^i \delta^i + x^{ip} \delta^p) \quad (\delta^i \in R^*) \\ &= puz^p + pu(x^b \eta^i + x^{ip} \delta^p) \quad (\eta^i \in R^*). \end{aligned} \quad (3.16)$$

Note that $b \neq ip$. (Otherwise, $k = bp = ip^2$, which is a contradiction.) Thus

$$pGR(p^n, r) \ni pu(x^b \eta^i + x^{ip} \delta^p) = px^{\min(b, ip)} \eta'', \quad \eta'' \in R^*. \quad (3.17)$$

Since $0 < \min(b, ip) < k$, (3.17) happens only when $n = 2$ and $\min(b, ip) \geq t$. In particular, $k/p = b \geq t$, which is contradictory to the assumption.

(iii) Also by (2.3) and (2.7), it suffices to show that

$$(1 + xR)^p \supset 1 + pGR(p^2, r). \quad (3.18)$$

Every element of $1 + pGR(p^2, r)$ is of the form $1 + pu\varepsilon^p$ for some $\varepsilon \in T$, where T is the Teichmüller set of $GR(p^2, r)$. We have

$$\begin{aligned} (1 + xR)^p &\ni (1 + x^{k/p} \varepsilon)^p \\ &= 1 + px^{k/p} \varepsilon' + x^k \varepsilon^p \quad (\varepsilon' \in R) \\ &= 1 + pu\varepsilon^p, \end{aligned} \quad (3.19)$$

where $px^{k/p} = 0$ since $k/p \geq t$. ■

THEOREM 3.3. *Let*

$$R(u) = GR(p^n, r)[x]/(x^k - pu, p^{n-1} x^t), \quad (3.20)$$

where $n \geq 2$, $1 \leq t \leq k$, $u \in GR(p^n, r)^*$. Assume that one of the following conditions holds.

- (i) $n = 2$;
- (ii) $p \nmid k$, $n \geq 3$;
- (iii) $p \parallel k$, $(p-1) \nmid k$, and $n \geq 4$ or $n = 3$ but $t > k/p$;
- (iv) $p \parallel k$, $(p-1) \nmid k$, $n = 3$, and $t \leq k/p$.

Define a subgroup $G \subset GR(p^{n-1}, r)^*$ as

$$G = \begin{cases} (GR(p^{n-1}, r)^*)^k, & \text{if (i) or (ii) or (iii) holds,} \\ (T^*)^k \cdot (1 + pGR(p^2, r)), & \text{if (iv) holds,} \end{cases} \quad (3.21)$$

where T^* is the unique cyclic subgroup of $p^r - 1$ of $GR(p^{n-1}, r)$. Let $\text{Aut}(GR(p^{n-1}, r))$ act on $GR(p^{n-1}, r)^*/G$ in the obvious way. Then the natural

homomorphism

$$\overline{(\)}: GR(p^n, r)^* \rightarrow GR(p^{n-1}, r)^*/G \tag{3.22}$$

induces a bijection

$$[R(u)] \mapsto [\bar{u}], \quad u \in GR(p^n, r)^* \tag{3.23}$$

between the isomorphism classes of pure finite chain rings with invariants p, n, r, k, t , and the $\text{Aut}(GR(p^{n-1}, r))$ -orbits in $GR(p^{n-1}, r)^*/G$.

Proof. Under conditions (ii), (iii), or (iv), the conclusion follows from Lemmas 3.1 and 3.2. To be more specific, assume, for example, condition (iii). By Lemma 3.1, $R(u) \cong R(v)$ ($u, v \in GR(p^n, r)^*$) if and only if there is a $\rho \in \text{Aut}(GR(p^{n-1}, r))$ such that in $GR(p^{n-1}, r)$,

$$\bar{u}^{-1} \rho(\bar{v}) \in [GR(p^{n-1}, r)[x]/(x^k - p\bar{u}, p^{n-2}x^t)]^k \cap GR(p^{n-1}, r)^*, \tag{3.24}$$

where \bar{u} and \bar{v} are the images of u and v in $GR(p^{n-1}, r)$. According to Lemma 3.2, the right hand side of (3.24) is $(GR(p^{n-1}, r)^*)^k$. Thus $R(u) \cong R(v)$ if and only if \bar{u} and \bar{v} are in the same $\text{Aut}(GR(p^{n-1}, r))$ -orbit of $GR(p^{n-1}, r)^*/(GR(p^{n-1}, r)^*)^k$.

Under condition (i), the conclusion follows from Lemma 3.1 and the fact that

$$[(GR(p, r)[x]/(x^t))^k] \cap GR(p, r)^* = (GR(p, r)^*)^k. \quad \blacksquare \tag{3.25}$$

COROLLARY 3.4. *Let p, n, r, k, t be as in Theorem 3.3 and let $d = (k, p^r - 1)$. Then the number of isomorphism classes of pure finite chain rings with invariants p, n, r, k, t is*

$$\begin{aligned} & \frac{1}{r} \sum_{i=0}^{r-1} (p^i - 1, d), && \text{under conditions (i), (ii), or (iv),} \\ & \frac{1}{r} \sum_{i=0}^{r-1} (p^i - 1, d)p^{(i, r)}, && \text{under condition (iii).} \end{aligned} \tag{3.26}$$

Here conditions (i)–(iv) are the ones in Theorem 3.3.

Proof. Let T and σ be the Teichmüller set and Frobenius map of $GR(p^{n-1}, r)$ respectively. First assume condition (iii). In the notation of Theorem 3.3, we have

$$\begin{aligned} GR(p^{n-1}, r)^*/G &= (T^*/(T^*)^k) \times [(1 + pGR(p^{n-1}, r))/(1 + pGR(p^{n-1}, r))^k] \\ &= (T^*/(T^*)^k) \times [(1 + pGR(p^{n-1}, r))/(1 + p^2GR(p^{n-1}, r))]. \end{aligned} \tag{3.27}$$

(Note that since $p \parallel k$, $(1 + pGR(p^{n-1}, r))^k = (1 + pGR(p^{n-1}, r))^p = 1 + p^2GR(p^{n-1}, r)$.) Identify $T^*/(T^*)^k$ as \mathbb{Z}_d and identify

$(1 + pGR(p^{n-1}, r))/(1 + p^2 GR(p^{n-1}, r))$, as a set, as T . Then the action of σ on $GR(p^{n-1}, r)^*/G = \mathbb{Z}_d \times T$ is given by

$$\sigma(a, \xi) = (pa, \xi^p), \quad (a, \xi) \in \mathbb{Z}_d \times T. \quad (3.28)$$

For each $0 \leq i < r - 1$, the number of elements in $\mathbb{Z}_d \times T$ fixed by σ^i is

$$(p^i - 1, d) \cdot [(p^i - 1, p^r - 1) + 1] = (p^i - 1, d)p^{(i,r)}. \quad (3.29)$$

Thus by the Burnside Lemma, the number of $\langle \sigma \rangle$ -orbits in $\mathbb{Z}_d \times T$ is

$$\frac{1}{r} \sum_{i=0}^{r-1} (p^i - 1, d)p^{(i,r)}. \quad (3.30)$$

The proof of (3.26) under conditions (i), (ii), and (iv) is similar. One only has to note that in these cases,

$$GR(p^{n-1}, r)^*/G = T^*/(T^*)^k. \quad \blacksquare \quad (3.31)$$

Remark. Let $d|(p^r - 1)$. By a result of [3],

$$\frac{1}{r} \sum_{i=0}^{r-1} (p^i - 1, d) = \sum_{c|d} \frac{\phi(c)}{\tau(c)}, \quad (3.32)$$

where $\phi(c)$ is the Euler function and $\tau(c)$ is the smallest number $m > 0$ such that $p^m - 1 \equiv 0 \pmod{c}$. Both sides of (3.32) are the number of orbits when \mathbb{Z}_r acts on \mathbb{Z}_d through

$$\begin{aligned} \mathbb{Z}_r \times \mathbb{Z}_d &\rightarrow \mathbb{Z}_d \\ (i, a) &\mapsto p^i a. \end{aligned} \quad (3.33)$$

The left hand side of (3.32) is independent of r as long as $d|(p^r - 1)$. This fact can also be seen directly without using (3.32). Actually, for any integers $s > 0$, $(1/sr) \sum_{i=0}^{sr-1} (p^i - 1, d) = (1/r) \sum_{i=0}^{r-1} (p^i - 1, d)$.

4. THE ORDER OF AN ELEMENT IN $1 + xR$

Let

$$R = GR(p^n, r)[x]/(g, p^{n-1}x^t) \quad (4.1)$$

be a finite chain ring with invariants p, n, r, k, t , where $t = k$ when $n = 1$, $1 \leq t \leq k$ when $n \geq 2$, and

$$g = x^k - p(a_{k-1}x^{k-1} + \cdots + a_0), \quad a_i \in GR(p^n, r), \quad a_0 \in GR(p^n, r)^*. \quad (4.2)$$

The invariants p, n, r, k, t will be fixed throughout this section. For $c \geq 1$ and $l \geq 0$, let

$$h_{c,l} = \min \{cp^i + (l - i)k : 0 \leq i \leq l\}. \quad (4.3)$$

Clearly, $h_{c,l}$ is increasing with respect to both c and l .

Lemma 4.1. Let $c \geq 1$.

(i) If k is not of the form $c(p - 1)p^s$ ($s \geq 0$) and $\varepsilon \in R^*$, then for all $l \geq 0$,

$$(1 + x^c \varepsilon)^{p^l} = 1 + x^{h_{c,l}} \varepsilon_l, \quad \varepsilon_l \in R^*. \tag{4.4}$$

(ii) If k is not of the form $c(p - 1)p^s$ ($s \geq 0$), or if $r > 1$, or if $a_0 \not\equiv -1 \pmod{pGR(p^n, r)}$, where a_0 is as in (4.2), then the exponent of the multiplicative group $1 + x^c R$ is p^L where L is the smallest l such that $h_{c,l} \geq (n - 1)k + t$.

Proof. (i) We use induction on l . Condition (4.4) trivially holds for $l = 0$. Assuming (4.4), we have

$$\begin{aligned} (1 + x^c \varepsilon)^{p^{l+1}} &= (1 + x^{h_{c,l}} \varepsilon_l)^p \\ &= 1 + px^{h_{c,l}} \varepsilon_l + \frac{p(p-1)}{2} x^{2h_{c,l}} \varepsilon_l^2 + \dots + x^{ph_{c,l}} \varepsilon_l^p \\ &= 1 + px^{h_{c,l}} \left(\varepsilon_l + \frac{p-1}{2} x^{h_{c,l}} \varepsilon_l^2 + \dots \right) + x^{ph_{c,l}} \varepsilon_l^p \\ &= 1 + px^{h_{c,l}} \varepsilon' + x^{ph_{c,l}} \varepsilon'' \quad (\varepsilon', \varepsilon'' \in R^*) \\ &= 1 + x^{k+h_{c,l}} \varepsilon''' + x^{ph_{c,l}} \varepsilon'' \quad (\varepsilon''' \in R^*). \end{aligned} \tag{4.5}$$

Note that $k + h_{c,l} \neq ph_{c,l}$. (Otherwise, $k = (p - 1)h_{c,l}$, which force $h_{c,l} = cp^l$ according to (4.3). Then $k = c(p - 1)p^l$, which contradicts the assumption on k .) Therefore,

$$(1 + x^c \varepsilon)^{p^{l+1}} = 1 + x^{\min\{k + h_{c,l}, ph_{c,l}\}} \varepsilon_{l+1}, \quad \varepsilon_{l+1} \in R^*. \tag{4.6}$$

Since

$$\begin{aligned} &\min\{k + h_{c,l}, ph_{c,l}\} \\ &= \min\{cp^0 + (l + 1)k, \quad cp^1 + lk, \dots, cp^l + k, \\ &\quad p(cp^0 + lk), \dots, p(cp^{l-1} + k), cp^{l+1}\} \\ &= \min\{cp^0 + (l + 1)k, cp^1 + lk, \dots, cp^l + k, cp^{l+1}\} \\ &= h_{c,l+1}, \end{aligned} \tag{4.7}$$

we have proved (4.4) for $l + 1$.

(ii) From the proof of (i), it is easy to see that

$$(1 + x^c R)^{p^l} \subset 1 + x^{h_{c,l}} R \quad \text{for all } l \geq 0. \tag{4.8}$$

Thus $(1 + x^c R)^{p^L} \subset 1 + x^{h_{c,L}} R = \{1\}$, since $h_{c,L} \geq (n - 1)k + t$ and $(n - 1)k + t$ is the nilpotency of x . It remains to prove that there is a $u \in R$

such that

$$(1 + x^c u)^{p^{l-1}} \neq 1. \quad (4.9)$$

If k is not of the form $c(p-1)p^s$, (4.9) follows from (4.4) with $u = 1$. Now assume that $k = c(p-1)p^s$ for some $s \geq 0$. Because of the assumption on r and a_0 , the inequality $a_0^{-1}y + y^p \neq 0$ in $GR(p^n, r)/pGR(p^n, r) = GF(p^r)$ has a solution $y \in GF(p^r)^*$. Lift y to $\bar{y} \in T^* = T \setminus \{0\}$, where T is the Teichmüller set of $GR(p^n, r)$. Then $a_0^{-1}\bar{y} + \bar{y}^p \in GR(p^n, r)^*$. Let σ be the Frobenius map of $GR(p^n, r)$ and choose $u = \sigma^{-s}(\bar{y})$. We will show that for all $l \geq 0$,

$$(1 + x^c u)^{p^l} = 1 + x^{h_{c,l}} \varepsilon_l, \quad \varepsilon_l \in R^*. \quad (4.10)$$

(Note that (4.9) follows from (4.10) immediately.) It is easy to see that for $0 \leq l \leq s+1$, $h_{c,l} = cp^l$ and that

$$(1 + x^c u)^{p^l} = 1 + x^{cp^l} \varepsilon_l, \quad \varepsilon_l \equiv u^{p^l} \pmod{xR}, \quad 0 \leq l \leq s. \quad (4.11)$$

(The proof of (4.11) is the same as that of (i).) We then have

$$\begin{aligned} (1 + x^c u)^{p^{s+1}} &= (1 + x^{cp^s} \varepsilon_s)^p \\ &= 1 + px^{cp^s} \eta + x^{cp^{s+1}} \varepsilon_s^p \quad (\eta \equiv \varepsilon_s \pmod{xR}) \\ &= 1 + x^{cp^s+k} a_0^{-1} \eta' + x^{cp^{s+1}} \varepsilon_s^p \quad (\eta' \equiv \varepsilon_s \pmod{xR}) \\ &= 1 + x^{cp^{s+1}} (a_0^{-1} \eta' + \varepsilon_s^p). \end{aligned} \quad (4.12)$$

In R/xR ,

$$\begin{aligned} a_0^{-1} \eta' + \varepsilon_s^p &= a_0^{-1} \varepsilon_s + \varepsilon_s^p \\ &= a_0^{-1} u^{p^s} + u^{p^{s+1}} \\ &= a_0^{-1} \bar{y} + \bar{y}^p \\ &\neq 0. \end{aligned} \quad (4.13)$$

Thus

$$(1 + x^c u)^{p^{s+1}} = 1 + x^{cp^{s+1}} \varepsilon_{s+1} = 1 + x^{h_{c,s+1}} \varepsilon_{s+1}, \quad \varepsilon_{s+1} \in R^*. \quad (4.14)$$

For $l > s+1$, starting with (4.14) and again by the same proof as that of (i), one can show that

$$(1 + x^c u)^{p^l} = 1 + x^{h_{c,l}} \varepsilon_l, \quad \varepsilon_l \in R^*. \quad (4.15)$$

The proof of (ii) is now complete. ■

For $c \geq 1$, let

$$\alpha(c) = \text{the smallest } l \text{ such that } h_{c,l} \geq (n-1)k + t. \quad (4.16)$$

Then we have the following corollary.

COROLLARY 4.2. *Let $c \geq 1$,*

(i) *If k is not of the form $c(p - 1)p^s$ ($s \geq 0$) and $\varepsilon \in R^*$, then the multiplicative order of $1 + x^c\varepsilon$ is $p^{\iota(c)}$.*

(ii) *If k is not of the form $c(p - 1)p^s$ ($s \geq 0$), or if $r > 1$, or if $a_0 \not\equiv -1 \pmod{xR}$, then the exponent of the multiplicative group $1 + x^cR$ is $p^{\iota(c)}$.*

In the next two lemmas, we calculate $h_{c,l}$ and $\alpha(c)$ explicitly.

Lemma 4.3. *For $c \geq 1$, let*

$$\iota(c) = \max \left\{ 0, \left\lceil \log_p \left(\frac{k}{(p-1)c} \right) \right\rceil \right\}. \tag{4.17}$$

Then

$$h_{c,l} = \begin{cases} cp^l, & \text{if } 0 \leq l \leq \iota(c), \\ cp^{\iota(c)} + (l - \iota(c))k, & \text{if } l > \iota(c). \end{cases} \tag{4.18}$$

Proof. The proof relies on the fact that the function $f(x) = cp^x + (l - x)k$ is decreasing for x to the left of a certain point and is increasing for x to the right of the point. (The critical number, which is of no use in this proof, is actually $\log_p k - \log_p(c \ln p)$.) Note that (4.18) is obvious for $l = 0$. Thus we assume $l \geq 1$.

Case 1. $\iota(c) = 0$. Then $k \leq (p - 1)c$. For $l \geq 1$, we have

$$cp^0 + lk \leq cp^1 + (l - 1)k. \tag{4.19}$$

Thus

$$h_{c,l} = \min \{cp^i + (l - i)k : 0 \leq i \leq l\} = cp^0 + lk. \tag{4.20}$$

Case 2. $\iota(c) > 0$. Then

$$(p - 1)cp^{\iota(c)-1} < k \leq (p - 1)cp^{\iota(c)}. \tag{4.21}$$

For $1 \leq l \leq \iota(c)$, $cp^l \leq cp^{l-1} + k$. Then

$$h_{c,l} = \min \{cp^i + (l - i)k : 0 \leq i \leq l\} = cp^l. \tag{4.22}$$

For $l > \iota(c)$,

$$cp^{\iota(c)} + (l - \iota(c))k < cp^{\iota(c)-1} + (l - \iota(c) + 1)k, \tag{4.23}$$

and

$$cp^{\iota(c)} + (l - \iota(c))k \leq cp^{\iota(c)+1} + (l - \iota(c) - 1)k. \tag{4.24}$$

Thus

$$h_{c,l} = \min \{cp^i + (l - i)k : 0 \leq i \leq l\} = cp^{\iota(c)} + (l - \iota(c))k. \tag{4.25}$$

Lemma 4.4.

$$\alpha(c) = \begin{cases} \iota(c) + n - 1 + \left\lceil \frac{t - cp^{(c)}}{k} \right\rceil, & \text{if } 1 \leq c < (n-1)k + t, \\ 0 & \text{if } c \geq (n-1)k + t. \end{cases} \quad (4.26)$$

Proof. The conclusion is obvious for $c \geq (n-1)k + t$. Thus assume $1 \leq c < (n-1)k + t$. First, we claim that

$$cp^{(c)-1} < (n-1)k + t. \quad (4.27)$$

If $\iota(c) = 0$, (4.27) is obvious. If $\iota(c) > 0$, by (4.17),

$$(p-1)cp^{(c)-1} < k, \quad (4.28)$$

which implies (4.27). By (4.27) and (4.18), we see that $h_{c,l} \geq (n-1)k + t$ implies $l \geq \iota(c)$. Thus by (4.18),

$$\begin{aligned} h_{c,l} &\geq (n-1)k + t \\ \Leftrightarrow l &\geq \iota(c) \text{ and } cp^{(c)} + (l - \iota(c))k \geq (n-1)k + t \\ \Leftrightarrow l &\geq \iota(c) \text{ and } l \geq \iota(c) + n - 1 + \left\lceil \frac{t - cp^{(c)}}{k} \right\rceil. \end{aligned} \quad (4.29)$$

The proof will be complete after proving

$$n - 1 + \frac{t - cp^{(c)}}{k} > -1. \quad (4.30)$$

Assume the contrary of (4.30). Then

$$cp^{(c)} \geq nk + t. \quad (4.31)$$

In particular, $\iota(c) > 0$ since $c < (n-1)k + t$. Then by (4.28), $cp^{(c)} < kp/(p-1) \leq 2k$, which is a contradiction to (4.31) ■

5. THE GROUP OF UNITS

Let

$$R = GR(p^n, r)[x]/(g, p^{n-1}x^t) \quad (5.1)$$

be a finite chain ring with invariants p, n, r, k, t , where $t = k$ when $n = 1$ and $1 \leq t \leq k$ when $n \geq 2$, and $g \in GR(p^n, r)[x]$ is an Eisenstein polynomial of degree k . Since $R^* \cong T^* \times (1 + xR)$ ((2.7)), to determine the structure of the

group of units of R^* of R , it suffices to determine that of the multiplicative group $1 + xR$.

Let $\alpha(c)$ ($c \geq 1$) be defined by (4.16). Since $h_{c,l}$ (defined in (4.3)) is increasing with respect to c , $\alpha(c)$ is decreasing with respect to c . From the definitions of $\alpha(c)$ and $h_{c,b}$, it is also clear that $\alpha((n - 1)k + t) = 0$ and $\alpha((n - 1)k + t - 1) > 0$. Thus

$$\alpha(1) \geq \alpha(2) \geq \dots \geq \alpha((n - 1)k + t - 1) > \alpha((n - 1)k + t) = 0. \tag{5.2}$$

For each $0 \leq j \leq \alpha(1)$, let

$$e_j = |\{c : 1 \leq c \leq (n - 1)k + t, \alpha(c) = j\}|. \tag{5.3}$$

Note that $e_0 = 1$ and $e_0 + \dots + e_{\alpha(1)} = (n - 1)k + t$.

THEOREM 5.1. *Assume that $(p - 1) \nmid k$, Then*

$$1 + xR \cong \mathbb{Z}_p^{r(e_1 - e_2)} \times \mathbb{Z}_{p^2}^{r(e_2 - e_3)} \times \dots \times \mathbb{Z}_{p^{\alpha(1)-1}}^{r(e_{\alpha(1)-1} - e_{\alpha(1)})} \times \mathbb{Z}_{p^{\alpha(1)}}^{r e_{\alpha(1)}}. \tag{5.4}$$

(Note that (5.4) implies that $e_1 \geq e_2 \geq \dots \geq e_{\alpha(1)}$.)

Proof. For each $c \geq 1$ and $\varepsilon \in R^*$, by Corollary 4.2, $o(1 + x^c \varepsilon) = p^{\alpha(c)}$. Thus for each $0 \leq j \leq \alpha(1)$,

$$\begin{aligned} \{y \in 1 + xR : y^{p^j} = 1\} &= \{1 + x^c \varepsilon : \alpha(c) \leq j, \varepsilon \in R^*\} \\ &= 1 + x^{1 + e_{\alpha(1)} + \dots + e_{j+1}} R, \end{aligned} \tag{5.5}$$

since the smallest integer c such that $\alpha(c) \leq j$ is $1 + e_{\alpha(1)} + \dots + e_{j+1}$. In particular,

$$\begin{aligned} |\{y \in 1 + xR : y^{p^j} = 1\}| &= p^{r[(n - 1)k + t - (1 + e_{\alpha(1)} + \dots + e_{j+1})]} \\ &= p^{r[e_1 + \dots + e_j]}, \quad \text{for } 0 \leq j \leq \alpha(1). \end{aligned} \tag{5.6}$$

Isomorphism (5.4) follows from (5.6) through straightforward counting arguments. ■

Theorem 5.1 shows that the group of units of a finite chain ring is more interesting than that of a Galois ring (cf. (2.4)). Next, we look at some concrete examples of Theorem 5.1.

EXAMPLE 5.2. Let $(p, n, r, k, t) = (5, 3, r, 5, 1)$. $(n - 1)k + t = 11$. Using (4.26), one can quickly determine that

$$(\alpha(1), \dots, \alpha(11)) = (3, 2, 2, 2, 2, 1, 1, 1, 1, 0). \tag{5.7}$$

Thus $e_1 = 5, e_2 = 4, e_3 = 1$, and

$$R^* \cong \mathbb{Z}_{5^{r-1}} \times \mathbb{Z}_5^r \times \mathbb{Z}_{5^2}^{3r} \times \mathbb{Z}_{5^3}^r. \tag{5.8}$$

EXAMPLE 5.3. Let $(p, n, r, k, t) = (3, 2, r, 19, 3)$. $(n - 1)k + t = 22$. By (4.26),

$$(\alpha(1), \dots, \alpha(22)) = (3, 3, 2, 2, 2, 2, 2, 1, \dots, 1, 0). \tag{5.9}$$

Thus $e_1 = 14, e_2 = 5, e_3 = 2$, and

$$R^* \cong \mathbb{Z}_{3^{r-1}} \times \mathbb{Z}_3^{9r} \times \mathbb{Z}_{3^{3r}} \times \mathbb{Z}_3^{2r}. \tag{5.10}$$

Theorem 5.1 also shows that when $(p - 1) \nmid k$, the structure of the group of units of a finite chain ring is completely determined by its invariants p, n, r, k, t . However, this is not the case when $(p - 1) \mid k$.

EXAMPLE 5.4. Let

$$R = \mathbb{Z}_{3^2} [x]/(x^2 - 3), \tag{5.11}$$

$$S = \mathbb{Z}_{3^2} [x]/(x^2 - 6). \tag{5.12}$$

Both R and S are finite chain rings with invariants $(p, n, r, k, t) = (3, 2, 1, 2, 2)$. $(n - 1)k + t = 4$. For each $a \in R$,

$$(1 + xa)^3 = 1 + 3xa + x^3a^3 = 1 + 3x(a + a^3), \tag{5.13}$$

$$(1 + xa)^{3^2} = 1. \tag{5.14}$$

Thus

$$\begin{aligned} |\{y \in 1 + xR : y^3 = 1\}| &= |\{1 + xa : a + a^3 \equiv 0 \pmod{xR}\}| \\ &= |\{1 + xa : a \equiv 0 \pmod{xR}\}| \\ &= |1 + x^2R| \\ &= 3^2. \end{aligned} \tag{5.15}$$

(Note that $1 + a^2 \neq 0$ in $R/xR = GF(3)$.) Therefore

$$1 + xR \cong \mathbb{Z}_3 \times \mathbb{Z}_{3^2}. \tag{5.16}$$

Similarly, for each $b \in S$,

$$(1 + xb)^3 = 1 + 3xb + x^3b^3 = 1 + 3x(b - b^3) = 1, \tag{5.17}$$

since $b - b^3 = 0$ in $S/xS = GF(3)$. Thus

$$1 + xS \cong \mathbb{Z}_3^3. \tag{5.18}$$

ACKNOWLEDGMENT

The author thanks the anonymous referees for the valuable comments and additional references.

REFERENCES

1. Y. Al-Khamees, Finite almost chain rings, *Math. Japon.* **36** (1991), 883–890.
2. B. Artmann, G. Dorn, D. Drake, and G. Törner, Hjelmlev'sche Inzidenzgeometrie und verwandte Gebiete—Literaturverzeichnis, *J. Geom.* **7** (1976), 175–191.
3. W. E. Clark and J. J. Liang, Enumeration of finite commutative chain rings, *J. Algebra* **27** (1973), 445–453.
4. C. Faith, “Rings and Things and a Fine Array of Twentieth Century Associative Algebra,” Amer. Math. Soc., Providence, 1999.
5. L. Fuchs and L. Salce, “Modules over Valuation Domains,” Dekker, New York, 1985.
6. X. Hou, q -ary bent functions constructed from chain rings, *Finite Fields Appl.* **4** (1998), 55–61.
7. X. Hou, Bent functions, partial difference sets and quasi-Frobenius local rings, *Dec. Codes Cryptogr.* **20** (2000), 251–268.
8. G. J. Janusz, Separable algebras over commutative rings, *Trans. Amer. Math. Soc.* **122** (1966), 461–479.
9. W. Klingenberg, Projective und affine Ebenen mit Nachbarelementen, *Math. Z.* **60** (1960), 384–406.
10. W. Krull, “Idealtheorie,” 2nd ed., Springer-Verlag, Berlin/New York, 1968.
11. K. H. Leung and S. L. Ma, Constructions of partial difference sets and relative difference sets on p -groups, *Bull. London Math. Soc.* **22** (1990), 533–539.
12. K. H. Leung and S. L. Ma, Partial difference sets with Paley parameters, *Bull. London Math. Soc.* **27** (1995), 553–564.
13. B. R. McDonald, “Finite Rings with Identity,” Dekker, New York, 1974.
14. R. Raghavendran, Finite associative rings, *Composition Math.* **21** (1969), 195–229.
15. G. Törner and F. D. Veldkamp, Literature on geometry over rings, *J. Geom.* **42** (1991), 180–200.