NON-ISOMORPHIC PURE GALOIS-EISENSTEIN RINGS

ALEXANDRE FOTUE TABUE AND CHRISTOPHE MOUAHA

ABSTRACT. Let \( n, r, e, s \) be positive integers and the prime \( p \), the finite local principal ideals ring of parameters \((p, n, r, e, s)\)

\[ GR(p^n, r)[x]/(x^r - pu^e) \]

is defined by an invertible element \( u \) of the Galois ring \( GR(p^n, r) \) of characteristic \( p^e \) of order \( p^m \). It is called Galois-Eisenstein ring of parameters \((p, n, r, e, s)\). A basic problem, which seems to be very difficult is to determine all non-isomorphism pure Galois-Eisenstein rings of parameters \((p, n, r, e, s)\). In this paper, this isomorphism problem for pure Galois-Eisenstein rings of parameters \((p, n, r, e, s)\) is investigated.

Keywords: Galois field, Galois ring.

AMS Subject Classification: 13Exx, 13M05, 13M10, 13Hxx, 13B05

1. Introduction

Throughout this paper, all rings are finite, associative, commutative with \( 1 \neq 0 \). For a ring \( R \), we denote by \( R^\times \) the set of invertible elements of \( R \), and \( J(R) \) the Jacobson radical of \( R \). Let \( r, n \), and \( p \) denote positive integers, \( p \) a prime, the residue class ring \( \mathbb{Z}/p^n\mathbb{Z} \) of integers modulo \( p^n \) with \( p \) prime and \( n > 1 \) and let \( GR(p^n, r) \) denote the (unique up to isomorphism) Galois extension of degree \( r \) of the ring \( \mathbb{Z}/p^n\mathbb{Z} \) of integers \( \text{mod} \ p^n \). To begin, let \( f \in (\mathbb{Z}/p^n\mathbb{Z})[x] \) be a primitive irreducible polynomial of degree \( r \). Then there is a unique monic polynomial \( f_n \in (\mathbb{Z}/p^n\mathbb{Z})[x] \) of degree \( r \) such that \( f \equiv f_n(\text{mod} \ p) \), and \( f_n \) divides \( x^{p^r-1} - 1 \) in \( (\mathbb{Z}/p^n\mathbb{Z})[x] \). Let \( \xi \) be a root of \( f_n \), so that \( \xi^{p^r-1} = 1 \). The Galois ring \( GR(p^n, r) \) is defined to be \((\mathbb{Z}/p^n\mathbb{Z})[\xi] \). Moreover, \( GR(p^n, r) \) is local ring with \( J(\text{GR}(p^n, r)) = (p) \) and the order of multiplicative subgroup \( \Gamma_p(r)^* := \langle \xi \rangle \) of \( \text{GR}(p^n, r)^* \) is \( p^r - 1 \). The set \( \Gamma_p(r) := \Gamma_p(r)^* \cup \{0\} \) is called \textit{Teichmüller set} of \( \text{GR}(p^n, r) \). The Galois ring \( \text{GR}(p^n, r) \) depends only on \( p, n \) and \( r \).

A ring \( R \) is a Galois-Eisenstein ring of parameters \((p, n, r, e, s)\) if \( GR(p^n, r) \) is the largest Galois ring contained in \( R \) and all ideals form the chain

\[ \{0\} = (\theta^e) \subseteq (\theta^{e-1}) \subseteq \cdots \subseteq (\theta) = J(R) \subseteq R. \]  

(1.1)

Since \( J(\text{GR}(p^n, r)) = (p) \), there exists an integer \( e \) such that \((\theta^e) = pR\). The integer \( s \) the nilpotency index of \( J(R) \), the Jacobson radical of \( R \), the integer
e ramification index of $R$. According to the Theorem 17.5 of [4], a GE-ring of parameters $(p, n, r, e, s)$ is isomorphic to the ring

$$GR(p^n, r)[x]/(x^e - pu(x); x^r)$$

(1.2)

where $u(x) := u_{e-1}x^{e-1} + \cdots + u_1x + u_0 \in GR(p^n, r)[x]$, with $u_0 \in GR(p^n, r)^\times$. The polynomial $x^e - pu(x)$ is an associated Eisenstein polynomial to the GE-ring (1.2). W. Clark and J. Liang shown in Lemma 2. of [1] that when $n > 1$, an element $\theta$ in $R$ is a root of an Eisenstein polynomial of degree $e$ over $GR(p^n, r)$ if and only if $J(R) = (\theta)$. We say that a GE-ring of the form (1.2) is pure if $u(x) = u_0 \in GR(p^n, r)^\times$.

Clark and Liang shown in [1] that, if $p \nmid e$ then pure GE-rings in the form (1.2) are pure and they enumerate all non-isomorphic pure GE-rings and when $p \mid e$, Clark and Liang shown in [1] that there are GE-rings which are not pure. Moreover, Xiang-Dong Hou in [2] gave the number of all non-isomorphic pure GE-rings, when $n = 2$ or $p \mid e, p^2 \nmid e$ and $(p - 1) \nmid e$. In this paper, the main goal is the determination all non-isomorphic pure GE-ring of parameters $(p, n, r, e, s)$, when $(p - 1) \nmid e$.

The paper is organized as follows. In Section 2, we review some basic facts about Galois rings and pure GE-rings of parameters $(p, n, r, e, s)$ to be used in sequel. In Section 3, we determine all non-isomorphic pure GE-rings of parameters $(p, n, r, e, s)$.

2. Preliminaries

Let $R$ be a pure GE-ring of parameters $(p, n, r, e, s)$. Let

$$L_e(R) := (R^\times)^e \cap (GR(p^n, r))^\times$$

be a multiplicative subgroup of $GR(p^n, r)^\times$, where $(R^\times)^e := \{u^e : u \in R^\times\}$. The aim of this section is the determination of the integer $b(e) \in \{1; 2; \cdots; n\}$ such that

$$L_e(R) = (\Gamma_p(r)^e)^e \cap (1 + p^b(e)GR(p^n, r)).$$

(2.1)

2.1. Galois Rings. The theory of Galois Rings was firstly developed by W. Krull (1924) and the reader will find in the monograph [7], more information about on Galois rings quoted. For this subsection, we gather the results on Galois rings allowing to determine the integer $b(e)$. A finite local ring of characteristic $p^n$ is called Galois ring $GR(p^n, r)$ of characteristic $p^n$ of rank $r$, if its Jacobson radical is generated by $p$. It is obvious that $GR(p^n, 1) = \mathbb{Z}/p^n\mathbb{Z}$ and $GR(p, r) = GF(p^r)$, where $GF(p^r)$ is the Galois field of the size $p^r$.

Let $f_n \in (\mathbb{Z}/p^n\mathbb{Z})[x]$ be a monic polynomial of degree $r$ such that

$$f_n \mod p \in (\mathbb{Z}/p\mathbb{Z})[x]$$
is irreducible over $\mathbb{Z}/p\mathbb{Z}$ and $f_n$ divides $x^{p^\ell-1} - 1 \pmod{p^n}$. In [5], an algorithm allows to compute the polynomial $f_n$ is given. Let $\xi$ be a root of $f_n$. Then $\text{GR}(p^n, r) = (\mathbb{Z}/p^n\mathbb{Z})[\xi]$ and $\Gamma_p(r)^* := \langle \xi \rangle$ is the unique cyclic subgroup of order $p^\ell - 1$ of multiplicative group $\text{GR}(p^n, r)^*$ isomorphic to cyclic multiplicative group $\text{GF}(p^n)^*$. The Teichmüller set $\Gamma_p(r)$ of $\text{GR}(p^n, r)$ forms a complete system of representatives modulo $p$ in $\text{GR}(p^n, r)$.

The following proposition gives the immediate properties of the Teichmüller set of the Galois ring $\text{GR}(p^n, r)$.

**Proposition 1.** Let $\xi$ be a generator of $\Gamma_p(r)^*$. Then

1. $\text{GR}(p^n, r) \subseteq \text{GR}(p^n, r')$ if and only if $\Gamma_p(r) \subseteq \Gamma_p(r')$

   if and only if $r$ devises $r'$;

2. $\Gamma_p(r) \cap \Gamma_p(r') = \Gamma_p(\gcd(r; r'))$;

3. $(\Gamma_p(r)^*)^{p^\ell-1} = \langle \xi^{p^\ell-1} \rangle$ and the order of $\langle \xi^{p^\ell-1} \rangle$ is $\frac{p^\ell-1}{\gcd(p^\ell-1, x)}$.

**Example 1.** The monic polynomials $f := x^2 + x + 2$ is irreducible over $\text{GF}(3)$. We denote by $\alpha$ the root of $f$. Then $\text{GF}(3)(\alpha)$ is the Galois field with 9 elements. Moreover, the monic polynomial $f_2 := x^2 - 5x - 1 \in (\mathbb{Z}/9\mathbb{Z})[x]$ such $f_2 \mod = f$ and $f_2$ devises $x^8 - 1 \in (\mathbb{Z}/9\mathbb{Z})[x]$. We then construct the Galois ring $\text{GR}(9, 2)$ and $\text{GR}(9, 2) = (\mathbb{Z}/9\mathbb{Z})[\xi]$, where $\xi^2 = 5\xi + 1$. Thus the Teichmüller set of the Galois ring $\text{GR}(9, 2)$ is $\Gamma_3(2) = \{0, 1, \xi, \xi^2(= 5\xi+1), \xi^3(= 8\xi+5), \xi^4(= 8\xi), \xi^5(= 4\xi+8), \xi^6(= \xi+4)\}$, and $(\Gamma_3(2)^*)^{18} = (\Gamma_3(2)^*)^2 = \langle \xi^2 \rangle = \{1, 5\xi + 1, 8\}$.

The following lemma gives the immediate properties of a complete residue system modulo $p^\ell$, where $\ell \in \{0, 1, \cdots, n\}$.

**Lemma 2.1.** Let $\xi$ be a generator of $\Gamma_p(r)^*$ and $\ell \in \{0, 1, \cdots, n\}$, we consider the set

$$\mathcal{R}_\ell := \left\{ \sum_{i=0}^{\ell-1} \xi_i p^i \in \text{GR}(p^n, r) : \xi_i \in \Gamma_p(r) \right\}$$

and by convention, we adopt $\mathcal{R}_0 := \{0\}$. Then

1. $\mathcal{R}_0 = \Gamma_p(r)$ and $\mathcal{R}_\ell(n) = \text{GR}(p^n, r)$;

2. $\mathcal{R}_\ell$ forms a complete residue system modulo $p^\ell$ in $\text{GR}(p^n, r)$;

3. for each $\alpha \in \text{GR}(p^n, r)$, for each $\ell \in \{0; 1; 2; \cdots ; n\}$, there exists a unique $(\gamma; \beta) \in \mathcal{R}_\ell \times \mathcal{R}_\ell(n-\ell)$, such that $\alpha = \gamma + p^\ell \beta$.

We remark that

$$\mathcal{R}_\ell(0) \subseteq \mathcal{R}_\ell(1) \subseteq \cdots \subseteq \mathcal{R}_\ell(n).$$
Proposition 2. The automorphism group of the ring $\text{GR}(p^n, r)$ is
\[
\text{Aut}(\text{GR}(p^n, r)) := \langle \sigma_p : \xi \mapsto \xi^p \rangle,
\]
and for all $\xi_i \in \Gamma_p(r)$,
\[
\sigma \left( \sum_{i=0}^{n-1} \xi_i p^i \right) = \sum_{i=0}^{n-1} \sigma(\xi_i)p^i.
\]

Moreover, the groups $\text{Aut}(\text{GR}(p^n, r))$ and \{0; 1; \ldots; r - 1\}, are isomorphic and for all $j \in \{0; 1; \ldots; r - 1\}$,
\[
\{x \in \Gamma_p(r) : \sigma_p^j(x) = x\} = \Gamma_p(\gcd(r, j)).
\]

We remark that if $\gcd(r, j) = 1$ then \[
\{x \in \Gamma_p(r) : \sigma_p^j(x) = x\} = \mathbb{Z}/p^n\mathbb{Z}.
\]

Example 2. Consider the Galois ring
\[
\text{GR}(9, 2) = (\mathbb{Z}/9\mathbb{Z})[\xi],
\]
where $\xi^2 = 5\xi + 1$. Thus the Teichmüller set of the Galois ring $\text{GR}(9, 2)$ is
\[
\Gamma_3(2) = \{0, 1, \xi, 5\xi + 1, 8\xi + 5, 8, 8\xi + 8, \xi + 4\}.
\]

The Galois group of of the ring $\text{GR}(p^n, r)$ is
\[
\text{Aut}(\text{GR}(9, 2)) = \{\text{Id}, \sigma_3 : \xi \mapsto \xi^3\}
\]
and
\[
\{x \in \Gamma_3(2) : \sigma_3(x) = x\} = \Gamma_3(\gcd(2, 1)) = \mathbb{Z}/9\mathbb{Z}.
\]

The structure of group of invertible elements of $\text{GR}(p^n, r)$ is given by the following theorem.

Theorem 2.2. ([7] Theorem 14.11) Let $\text{GR}(p^n, r)^\times$ be the group of invertible elements of $\text{GR}(p^n, r)$. Then $\text{GR}(p^n, r)^\times$ is the internal direct product of subgroups $\Gamma_p(r)^\times$ and $1 + p\text{GR}(p^n, r)$. Moreover,

(1) If $p$ is odd or if $p = 2$ and $n \leq 2$, then
\[
1 + p\text{GR}(p^n, r) \cong (\mathbb{Z}/(p^n))^\times,
\]
(2.4)

(2) if $p = 2$ and $n \geq 3$, then
\[
1 + p\text{GR}(p^n, r) \cong \text{GF}(2) \times \left(\mathbb{Z}/(2^{n-2})\right)^{-1} \times \left(\mathbb{Z}/(2^{n-1})\right)^{-1}.
\]

Theorem 2.2 has as a consequence the following corollary and this corollary gives a simple expression of the subgroup $(1 + p\text{GR}(p^n, r))^\times$ of $1 + p\text{GR}(p^n, r)$.
Corollary 1. Let \( i \) be an integer and \( p \) is a prime. If \( p \) odd or if \( p = 2 \) and \( n \leq 2 \), then

\[
(1 + p\mathcal{GR}(p^n, r))^\omega / q = 1 + q^{\omega+1}\mathcal{GR}(p^n, r).
\] (2.6)

2.2. Pure Galois-Eisenstein Rings. Let \( R \) be a pure Galois-Eisenstein ring (short: pure GE-ring) of parameters \((p, n, r, e, s)\). Then there exists \( u \in \mathcal{GR}(p^n, r)^\times \) such that \( R = \mathcal{GR}(p^n, r)[x]/(x^e - pu; x^s) \). The writing

\[
\mathcal{GE}(u) := \mathcal{GR}(p^n, r)[x]/(x^e - pu; x^s)
\] (2.7)
means that \( \mathcal{GE}(u) \) is a GE-ring of parameters \((p, n, r, e, s)\) defines by the invertible element \( u \in \mathcal{GR}(p^n, r)^\times \). In the sequel, we write \( \mathcal{GE}(u) = \mathcal{GR}(p^n, r)[\theta] \), such that \( \omega = pu \) and \( \omega^s = 0 \), but \( \omega^{s-1} \neq 0 \), for denote the pure Galois-Eisenstein ring of parameters \((p, n, r, e, s)\). We obvious that the Jacobson radical of \( \mathcal{GE}(u) \) is \((\theta)\).

Lemma 2.3. Let \( R \) be a pure Galois-Eisenstein ring of parameters \((p, n, r, e, s)\). Then the group of invertible elements \( R^\times \) of \( R \) is the internal direct product of subgroups \( \Gamma_p(r)^\times \) and \( 1 + J(R) \).

The following theorem gives the structure of subset

\[
\mathcal{L}_e(R) := (R^\times)^e \cap (\mathcal{GR}(p^n, r)^\times)
\] (2.8)
of group of invertible elements \( \mathcal{GR}(p^n, r)^\times \). This is the main result in this section.

Theorem 2.4. Let \( R \) be a pure Galois-Eisenstein ring of parameters \((p, n, r, e, s)\) such that \( s = (n - 1)e + t, 0 \leq t \leq e \) and \((p - 1) \nmid e \). Then there exists an integer \([b(e)] \in \{1; 2; \cdots ; n\} \) such that

\[
\mathcal{L}_e(R) = \langle \eta \rangle \cdot (1 + p\mathcal{GR}(p^n, r)_{[b(e)]}^\times),
\]
where

\[
[b(e)] = \begin{cases} 
1, & \text{if } t \leq \frac{n}{p} \text{ and } n = 2; \\
\min\{\omega + 1; n\}, & \text{if } t > \frac{n}{p} \text{ and } n = 2 \text{ or } n \neq 2.
\end{cases}
\]

where \( \omega := \max\{i \in \mathbb{N}^+ : p^i | e\} \).

Proof 1. The size of the multiplicative group \( 1 + J(R) \) is a power of \( p \), therefore

\[
(1 + J(R))^\omega / q = 1 + J(R)^\omega
\]
and \([b(e)] = [b(\omega)]\).

By Theorem 2.2 and Lemma 2.3,

\[
\mathcal{L}_e(R) = \left((\Gamma_p(r) \cdot (1 + J(R))^\omega) \cap \left(\Gamma_p(r) \cdot (1 + p\mathcal{GR}(p^n, r)_{[b(e)]}^\times)\right)\right),
\]
It follows that

\[ \mathcal{L}_e(R) = \langle \eta \rangle \cdot \left( (1 + J(R))^{p^e} \cap (1 + p\text{GR}(p^n, r)) \right), \]

in according by Lemma 2.1., we have \( \left( \Gamma_p(r)^e \right)^e = \langle \eta \rangle \). It suffices to determine the integer \( b(e) \) such that

\[ (1 + J(R))^{p^e} \cap (1 + p\text{GR}(p^n, r)) = 1 + p^{b(e)}\text{GR}(p^n, r). \]

We write

\[ (1 + J(R))^{p^e} \cap (1 + p\text{GR}(p^n, r)) = \mathcal{L}_1 \cup \mathcal{L}_2, \]

where

\[ \mathcal{L}_1 = \left\{(1 + \theta^b \varepsilon)^{p^e} \in 1 + p\text{GR}(p^n, r) : \geq e \ ; \ \varepsilon \in R^\times \right\}, \]

\[ \mathcal{L}_2 = \left\{(1 + \theta^b \varepsilon)^{p^e} \in 1 + p\text{GR}(p^n, r) : 1 \leq b < e \ ; \ \varepsilon \in R^\times \right\}. \]

Let \( b \) be an integer and \( \varepsilon \in R^\times \). On the one hand, suppose that \( b \geq e \). We have

\[ 1 + \theta^b \varepsilon \in 1 + pR \]

and

\[ (1 + \theta^b \varepsilon)^{p^e} \in (1 + pR)^{p^e} \subseteq 1 + p^{e+1}R. \]

Thus

\[ (1 + \theta^b \varepsilon)^{p^e} \in (1 + p^{e+1}R) \cap (1 + p\text{GR}(p^n, r)) = 1 + p^{e+1}\text{GR}(p^n, r) = (1 + p\text{GR}(p^n, r))^{p^e}. \]

Since

\[ (1 + p\text{GR}(p^n, r))^{p^e} \subseteq \mathcal{L}_1, \]

we have

\[ \mathcal{L}_1 = (1 + p\text{GR}(p^n, r))^{p^e}. \]
on the other hand, suppose that \( b < e \), we develop the following expres-
sion \( (1 + \theta^b \varepsilon)^{p^{\omega}} \) and we obtain:

\[
(1 + \theta^b \varepsilon)^{p^{\omega}} = 1 + \sum_{l=1}^{p^{\omega}-1} \left( \frac{l}{p^{\omega}} \right) (\theta^b \varepsilon)^l + (\theta^b \varepsilon)^{p^{\omega}}, \text{ since } l = jp^i \text{ and } p \nmid j; \\
= 1 + \sum_{i=1}^{\omega-1} \sum_{jp^i \leq p^{\omega}-1 \atop p \nmid j} \left( \frac{jp^i}{p^{\omega}} \right) (\theta^b \varepsilon)^{jp^i} + (\theta^b \varepsilon)^{p^{\omega}};
\]

since

\[
p^{\omega-i} \left( \frac{jp^i}{p^{\omega}} \right)
\]

and

\[
p^{\omega-i+1} \left( \frac{jp^i}{p^{\omega}} \right);
\]

thus

\[
(1 + \theta^b \varepsilon)^{p^{\omega}} = 1 + \sum_{i=1}^{\omega-1} \eta^{(\omega-i)+bp^i} \varepsilon_i + \theta^{bp^{\omega}} \varepsilon^{p^{\omega}},
\]

where \( \varepsilon_i \in R^x \). We write \( h(b, i) := e(\omega - i) + bp^i \) and

\[
h(b) := \min\{e(\omega - i) + bp^i : 0 \leq i < \omega\}.
\]

If \((p - 1) \nmid e\), then \( h(b, i) \neq h(b, i + 1) \). Thus there exists a unique \( i \in \{0; \cdots; \omega - 1\} \) such that \( h(b) = h(b, i) \). Therefore, there exists \( \varepsilon_b \in R^x \) such that

\[
(1 + \theta^b \varepsilon)^{p^{\omega}} = 1 + \theta^{h(b)} \varepsilon_b + \theta^{bp^{\omega}} \varepsilon^{p^{\omega}}.
\]

This forces that \( h(b) \geq s \), and \( bp^{\omega} \equiv 0 \mod e \). We have \( a \in \mathbb{N}^* \) such that \((pu)^a \varepsilon^{p^{\omega}} \in pGR(p^n, r)\). We obtain,

\[
\mathcal{L}_2 = \left\{ \begin{array}{ll}
1 + pGR(p^n, r), & \text{if } n = 2 \text{ and } t \leq t' \varepsilon; \\
(1), & \text{if } n \neq 2 \text{ or } n = 2 \text{ and } t > t' \varepsilon, \end{array} \right.
\]

\[\blacksquare\]

**Example 3.** Let \( R \) be a GE-ring of parameters \((3, 2, 2, 18, 25)\). Then by **Theorem 2.2** \( \blacksquare(2) = 2 \). Thus

\[
\mathcal{L}_0(R) = \langle \xi^2 \rangle \cdot (1 + 3^3 GR(9, 2))
\]

\[= \{1, \xi^2, \xi^4\},\]

where \( \Gamma_3(2)' = \langle \xi \rangle \) and \( \xi^2 = 5\xi + 1 \).
3. Main result

In this section, we determine the pure GE-rings of parameters \((p, n, r, e, s)\). Note when \(n = 1\), \(R = GF(p^r)/(x^e)\). Such rings need no classification, so we will suppose that \(n \geq 2\). The isomorphism problem for pure GE-rings with given parameters \((p, n, r, e, s)\) mentions by A. A. Nechaev in [6] and T. G. Gazaryan in [3], shown that pure GE-rings \(GE(1)\) and \(GE(2)\) of parameters \((3, 2, 1, 2, 3)\) are non-isomorphic rings with isomorphic additive and multiplicative groups.

Let \(\sim\) be the equivalence relation defined on \(GR(p^n, r)^\times\) by

\[
\mathbf{u} \sim \mathbf{v} \iff GE(\mathbf{u}) \cong GE(\mathbf{v}),
\]

(3.1)

where \(\mathbf{u}, \mathbf{v} \in GR(p^n, r)^\times\).

Let \(\sigma\) be a generator of \(Aut(\mathbf{GR}(p^n, r))\), and the multiplicative subgroup

\[
\mathcal{L}_\sigma(R) = \langle \eta \rangle \cdot (1 + p^{\frac{\eta e}{GR(p^n, r)}})
\]

of \(\mathbf{GR}(p^n, r)^\times\) and \(\eta\) a generator of \((\Gamma_p(r)^*)^e\). Consider

\[
U, \langle \eta \rangle := \langle \chi \rangle + p\mathcal{R}_s(\partial(e) - 1),
\]

(3.2)

where \(\partial(e) = \text{min}\{\partial(e); n - 1\}\).

We write \(\chi := \xi^{\frac{e - 1}{p - 1}}\) and \(d := \text{gcd}(p^r - 1; e)\). Since \(\text{gcd}\left(d; \left(\frac{p^n - 1}{p - 1}\right)\right) = 1\), then \(\langle \chi \rangle \cdot \langle \eta \rangle = \Gamma_p(r)^*\).

The isomorphic GE-rings have the same parameters, but there are non-isomorphic GE-ring with the same parameters. The following example illustrates the isomorphism problem for the GE-rings.

**Example 4.** T. G. Gazaryan, given in [3], two GE-rings of parameters \((3, 2, 1, 2, 3)\) \(GE(1) = (\mathbb{Z}/9\mathbb{Z})[\theta]\) and \(GE(2) = (\mathbb{Z}/9\mathbb{Z})[\delta]\) as an example of non-isomorphic commutative chain rings. We have \(\theta^2 = 3, \delta^2 = 6,\) and \(\theta^3 = \delta^3 = 0\).

Then the radical Jacobson are:

\[
J(\mathbf{GE}(1)) = (\theta) = \{0; 3; 6; \theta; 3\theta\}
\]

and

\[
J(\mathbf{GE}(1)) = (\delta) = \{0; 3; 6; \delta; 3\delta\}.
\]

The Teichmüller set \(\Gamma_3(1) = \{0; 1; 8\}\), allows to write

\[
\mathbf{GE}(1) = \{a + b\theta : (a; b) \in \Gamma_3(1)\}
\]

and

\[
\mathbf{GE}(2) = \{a + b\delta : (a; b) \in \Gamma_3(1)\}.
\]
But \( J(\text{GE}(1)) \neq J(\text{GE}(2)) \). Indeed, if \( J(\text{GE}(1)) = J(\text{GE}(2)) \), then there exists \( z \in \text{GE}(1)^\times \) such that \( \theta = z\delta \). As

\[
3 = \theta^2 = z^2\delta^2 = 6z^2.
\]

It follows, \( z^2 = (a + \theta b)^2 = a^2 + 2\theta ab \). Therefore, the equation \( 3 = 6z^2 \) is equivalent to \( 3 = 6a^2 \). Now, for all \( a \in (\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\} \), we have \( 6a^2 = 6 \). It is absurd.

**Lemma 3.1.** Let \( R \) be the GE-ring of parameters \((p, n, r, e, s)\). Then there exists \( v \) in \( U_r(\mathfrak{p}(e)) \) such that \( R = \text{GE}(v) \).

**Proof 2.** Let \( R \) be the GE-ring of parameters \((p, n, r, e, s)\). Then there exists \( u \in \text{GR}(p^n, r)^\times \) such that \( R = \text{GE}(u) \). By the item 3 of Lemma 2.1., there exists \( (\gamma; \beta) \in \mathcal{R}_r(\mathfrak{b}(e)) \times \mathcal{R}_r(n - \mathfrak{b}(e)) \), such that \( u = \gamma + p\mathfrak{b}(e)\beta \) and \( \gamma \in \text{GR}(p^n, r)^\times \). Since \( \langle \delta \rangle \cdot \langle \eta \rangle = \Gamma_\rho(r)^\times \), there exists \( (a, v) \in (\langle \eta \rangle \times U_r(\mathfrak{b}(e)) \) such that \( \gamma = av \).

Now, \( u = v(\alpha + p\mathfrak{b}(e)\beta) \), where \( \beta = \beta v^{-1} \). We have

\[
g := \alpha + p\mathfrak{b}(e)\beta \in \mathcal{L}(R).
\]

By Theorem 2.4, there exists \( z \in R^\times \) such that \( g = z^e \).

Since

\[
\text{GE}(u) = \text{GR}(p^n, r)[\theta]
\]

with \( \theta^e = pv \) and \( s = \min\{i \in \mathbb{N} : \theta^i = 0\} \). Thus, \( J(\text{GE}(u)) = (\delta) \) where \( \delta := z\theta \).

We have \( \delta^e = pv \) and \( s = \min\{i \in \mathbb{N} : \delta^i = 0\} \). So \( \text{GE}(u) = \text{GE}(v) \). ■

The following lemma gives a fundamental condition for non-isomorphic pure GE-rings.

**Lemma 3.2.** For each \( u \) and \( v \) in \( U_r(\mathfrak{b}(e)) \). Then

\[
u \sim v \Leftrightarrow u = \sigma^i(v),
\]

for some \( i \in \{0; 1; \cdots ; r - 1\} \).

**Proof 3.** Let \( \theta := x + (x^e - pu : x^e) \) be a generator of \( J(\text{GE}(u)) \). Then pure GE-rings \( \text{GE}(u) \) and \( \text{GE}(v) \) are isomorphic means by Lemma. 4 of \([1]\), the existence of \((i; z) \in \{0; 1; \cdots ; r - 1\} \times \text{GE}(u)^\times \) such that \( (\theta z)^e = p\sigma^i(v) \) and \( \theta^e = pu \). Since \( uz^e = \sigma^i(v) \) and \( u, \sigma^i(v) \in U_r(\mathfrak{b}(e)) \), we have \( z^e \in 1 + p\mathfrak{b}(e)\text{GR}(p^n, r) \). Therefore,

\[
\begin{align*}
u \sim v & \quad \Leftrightarrow \quad \exists (i; \gamma) \in \{0; 1; \cdots ; r - 1\} \times (1 + p\mathfrak{b}(e)\text{GR}(p^n, r)) : u\gamma = \sigma^i(v), \text{ where } \gamma := z^e; \\
& \quad \Leftrightarrow \quad \exists (i; \gamma) \in \{0; 1; \cdots ; r - 1\} \times (1 + p\mathfrak{b}(e)\text{GR}(p^n, r)) : u\gamma = \sigma^i(v).
\end{align*}
\]

Now, \( \gamma \in (1 + p\mathfrak{b}(e)\text{GR}(p^n, r)) \cap U_r(\mathfrak{b}(e)) = \{1\} \). ■
Let \( u \in U_r(\mathfrak{b}(e)) \), we write \( C(u) = \{ \sigma^i(u) : i \in \{0; 1; \cdots ; r-1\} \} \), the Frobenius class of \( u \) and \( C_r(\mathfrak{b}(e)) \) a complete set of Frobenius representative of \( U_r(\mathfrak{b}(e)) \).

**Theorem 3.3.** Let \( \Xi^*(p, n, r, e, s) \) be the set of pure GE-rings of parameters \( (p, n, r, e, s) \) up to isomorphism. Suppose that \( (p-1) \not\mid e \). Then the mapping

\[
\begin{align*}
\text{GE} : & \quad C_r(\mathfrak{b}(e)) \\
& \quad \mapsto \quad \Xi^*(p, n, r, e, s) \\
& \quad \mapsto \quad \text{GE}(u)
\end{align*}
\]

is bijective. Moreover,

\[
|\Xi^*(p, n, r, e, s)| = \frac{1}{r} \sum_{i=1}^{r} \gcd(p^{\gcd(r,i)} - 1, e)p^{(\mathfrak{b}(e)-1)\gcd(i,r)}.
\]

**Proof 4.** By [Lemma 3.1](#), the mapping \( \text{GE} \) is bijection. Indeed, For each \( u \in U_r(\mathfrak{b}(e)) \), there exists a unique \( v \) in \( C_r(\mathfrak{b}(e)) \) such that \( \text{GE}(u) = \text{GE}(v) \).

Now, we determine the size of \( \Xi^*(p, n, r, e, s) \) such that \( \text{GE}(u) = \text{GE}(v) \).

By the Burnside’s Lemma, the number of \( \langle \sigma \rangle \)-orbits in \( U_r(\mathfrak{b}(e)) \) is

\[
\frac{1}{|\langle \sigma \rangle|} \sum_{i=1}^{r} |\text{fix}(\sigma^i)| = \frac{1}{r} \sum_{i=1}^{r} \gcd(p^n - 1, e)p^{(\mathfrak{b}(e)-1)n_i}.
\]

Thus, the mapping \( \text{GE} \) allows to determine up to isomorphism all pure GE-rings.

**Example 5.** Consider the pure GE-rings of parameters \( (3, 2, 1, 2, 3) \). In according by Theorem [2.3](#), \( b(2) = 1 \). Then

\[
C_1(1) = U_l(1) = \{1; 8\}.
\]

By formula of Theorem 3.3, there are two non-isomorphism pure GE-rings of parameters \( (3, 2, 1, 2, 3) \). Therefore, in the article [3](#), the GE-rings \( r(1) \) et \( r(8) \) are only non-isomorphism pure GE-rings of parameters \( (3, 2, 1, 2, 3) \).

**Example 6.** Consider the GE-rings \( \text{GR}(9, 2)[\theta] \) of parameters \( (3, 2, 2, 18, 25) \) and \( \text{GR}(9, 2) = (\mathbb{Z}/9\mathbb{Z})[\xi] \), with \( \xi^2 = 5\xi + 1 \).

In according by Theorem [2.3](#), \( b(18) = 2 \). Then

\[
C_2(18) = U_2(2) = \langle \xi^4 \rangle = \{1; 8\}.
\]
By formula of Theorem 3.3, there are 2 non-isomorphism pure GE-rings of parameters $(3, 2, 2, 18, 25)$, and the GE-rings of parameters $(3, 2, 2, 18, 25)$ up to isomorphism are $r(1)$, and $r(8)$

**Conclusion**

A pure Galois-Eisenstein ring of $(p, n, r, e, s)$ is constructed from an element of the complete set of Frobenius representative of $U_r([e])$ and this construction are unique up to isomorphism. In general, the isomorphism problem for Galois-Eisenstein Rings stays open.

**References**

[1] W. Clark and J. Liang, *Enumeration of Finite Commutative Chain Rings*, J. Algebra 27,(1973) 445-453.

[2] X. Hou, *Finite Commutative Chain Rings*, Finite Fields Appl. 7 (2001) 382 - 396

[3] T. G. Gazaryan, *An example of non-isomorphic commutative chain rings*, Uspekhi Mat. Nauk, 47:3(285) (1992), 155-156

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

[5] Gary McGuire, *An Approach to Hensel’s Lemma*, Irish Math. Soc. Buellentin 47 (2001), 15-21.

[6] A. A. Nechaev, *Finite Rings with Applications*, Handbook of Algebra, Vol. 5,(2008) 213-320.

[7] Zhe-Xian Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific, (2003) 342 pages.

Alexandre Fotue Tabue  
Department of mathematics, Faculty of Sciences, University of Yaounde 1, Cameroon  
E-mail address: alexfotue@gmail.com

Christophe Mouaha  
Department of mathematics, Higher Teachers Training College of Yaounde, University of Yaounde 1, Cameroon  
E-mail address: cmouaha@yahoo.fr