Journal de Mathématiques
Mathématiques et Applications
Fondamentales & Informatique
JMMAFI, ISSN 2411-7188, **vol.5**,
2018, pp.39-44

FINITE LOCAL RINGS AND THEIR GALOIS RINGS

H. ANDRIATAHINY[1], T.J. RABEHERIMANANA[2]

[1,2] Mention: Mathématiques et Informatique,
Domaine: Sciences et Technologies,
Université d' Antananarivo, B.P. 906 Ankatso,
101 Antananarivo, Madagascar

Résumé
Un anneau de Galois est décrit dans un anneau local fini à l'aide du système de représentation de Teichmüller. Les paramètres de l'anneau de Galois sont définis par l'anneau local fini.

Mots-clés. Anneau local fini, anneau de Galois, système de représentation de Teichmüller, corps fini.

abstract
A Galois ring is described in a finite local ring with the help of the Teichmüller representation system. The parameters of the Galois ring is defined by the finite local ring.

Keywords. finite local ring, Galois ring, Teichmüller representation system, finite field.

1 Introduction

The finite field $\mathbb{F}_{p^r}$ of p^r elements, where p is a prime number and $r \geq 1$ an integer, was introduced by Evariste Galois in 1830 (cf H. Lueneburg [5]). Wolfgang Krull (cf W. Krull [4]) introduced in 1924 the Galois ring as a common generalization of the finite field $\mathbb{F}_{p^r}$ and the prime ring $\mathbb{Z}/p^n\mathbb{Z}$, with $n \geq 1$ an integer. He studied the existence and the structure of these rings. Janusz (cf G.J. Janusz [2]) and Raghavendran (cf R. Raghavendran [3]) independently rediscovered the Galois rings. Since 1994, these rings were used in coding theory.
Local rings have an important geometric aspect. They are often associated with points on algebraic and analytic varieties and they give local properties of the varieties.
The presence of a Galois ring in a finite local ring R is a powerful tool in the study of the structure of R.

[1]hariandriatahiny@gmail.com [2]rabeherimanana.toussaint@yahoo.fr

In [6] (cf B.R. McDonald), a Galois ring is determined in a finite local ring by means of a property of regular polynomials.
The Teichmüller representation system is a system of representatives which has remarkable properties. We give a construction of a Galois ring in a finite local ring by using the Teichmüller representation system. The Galois ring is determined in such a way that its parameters and those of the local ring are the same.
This paper is organized as follows. In section 2, we recall a property of finite local rings. The section 3 is devoted to determine the parameters of a finite local ring. In section 4, the Teichmüller representation system is studied. And in section 5, we determine the Galois ring in a finite local ring.

2 Preliminaries

In this paper, all rings will be commutative with identity $1 \neq 0$. Ideals do not contain 1. A ring with only one maximal ideal is called local.

2.1 Proposition. *A finite ring* R *is local if and only if it has a nilpotent maximal ideal.*

Proof. Let R be local and $\mathfrak{P}$ its maximal ideal. If $x \in \mathrm{R}$, we get $x^l(1-x^k)=0$ for some $l \geq 0$ and $k > 0$. If $x \in \mathfrak{P}$, then $1-x^k$ is not in $\mathfrak{P}$ (otherwise $1 \in \mathfrak{P}$). So $1-x^k$ is a unit, and this implies that $x^l = 0$.
Conversely, let $\mathfrak{P},\mathfrak{P}'$ be different maximal ideals of R. Then there is an element $x \in \mathfrak{P} \setminus \mathfrak{P}'$. All powers x^n are outside $\mathfrak{P}'$, so x (and therefore $\mathfrak{P}$) is not nilpotent. □

The depth of the maximal ideal $\mathfrak{P}$ of a finite local ring is the smallest integer $\nu \geq 0$ such that $\mathfrak{P}^\nu = \{0\}$.

3 Parameters of a finite local ring

From now on, we consider the pair $(\mathrm{L}, \mathfrak{M})$ where L is a finite local ring and $\mathfrak{M}$ its maximal ideal with $\mathrm{Depth}(\mathfrak{M}) = \mu \geq 0$.
Consider the canonical ring homomorphisms

$$\begin{aligned} \alpha : \quad & \mathbb{Z} \longrightarrow \mathrm{L} \\ & z \longmapsto z \cdot 1_{\mathrm{L}} \end{aligned} \tag{1}$$

and

$$\begin{aligned} \pi : \quad & \mathrm{L} \longrightarrow \mathrm{L}/\mathfrak{M} \\ & x \longmapsto x + \mathfrak{M} \end{aligned} \tag{2}$$

We denote by K the residue class ring $\mathrm{L}/\mathfrak{M}$ ([1]). Clearly, K is a finite field, and we have the homomorphism

$$\begin{aligned} \pi \circ \alpha : \quad & \mathbb{Z} \longrightarrow K \\ & z \longmapsto z \cdot 1_K \end{aligned}$$

Since K is a domain, the kernel of $\pi \circ \alpha$ is generated by a prime number $p \geq 2$. The finite domain $\mathbb{Z}/p\mathbb{Z}$ is a field which we consider as embedded in K.
Since $\alpha(p)$ is in $\mathfrak{M}$, it is nilpotent, and we denote by $n \geq 1$ its depth, i.e. $p^n 1_L = 0$ and $p^{n-1}1_L \neq 0$. Then the kernel of α contains p^n, but not p^{n-1}. From this follows

$\ker(\alpha) = p^n\mathbb{Z}$. So we can suppose the local ring $\mathbb{Z}/p^n\mathbb{Z}$ as embedded in L.
Now consider

$$(x+y)^p = x^p + (\sum_{i=1}^{p-1} \binom{p}{i} x^{p-i}y^i) + y^p \quad , \quad x \in \mathrm{L} \quad , \quad y \in \mathfrak{M}^\lambda \quad , \quad \lambda \geq 0. \tag{3}$$

All binomial coefficients $\binom{p}{i}$ are divisible by p, so all middle terms are in $p \cdot \mathfrak{M}^\lambda \subseteq \mathfrak{M}^{\lambda+1}$.
In the special case $\mathfrak{M} = \{0\}$, $\mathrm{L} = K$, $\lambda = 0$ ($\mathfrak{M}^0 := \mathrm{L}$), we get

$$(x+y)^p = x^p + y^p,$$

and so the Frobenius map

$$\begin{aligned} \sigma : \quad K &\longrightarrow K \\ x &\longmapsto x^p \end{aligned} \tag{4}$$

is a ring homomorphism. Since σ is injective, it is also surjective, and so an automorphism of the field K.
Denote r the dimension of K as vector space over $\mathbb{Z}/p\mathbb{Z}$. Then $\mathrm{Card}(K) = p^r$, and the multiplicative group $K^* = K \setminus \{0\}$ has $p^r - 1 =: m$ elements. And it is well known that K^* is cyclic. Moreover, all elements of K satisfy the equation $X \cdot (X^m - 1) = X^{p^r} - X = 0$, but no such equation with $r' < r$. So the automorphism (4) has the order r.
The finite local ring $(\mathrm{L}, \mathfrak{M})$ is said to be of parameters (p, n, r).
A finite local ring R of parameters (p, n, r) is called a Galois ring of characteristic p^n and order r if pR is its maximal ideal. It is denoted by $GR(p^n, r)$. This means that a Galois ring is an unramified extension of the prime ring $\mathbb{Z}/p^n\mathbb{Z}$ ([6]).

4 Teichmüller representation system

If $\lambda \geq 1$ in (3), we get $y^p \in \mathfrak{M}^{p\cdot\lambda} \subseteq \mathfrak{M}^{\lambda+1}$. So $(x+y)^p = x^p + z$ with $z \in \mathfrak{M}^{\lambda+1}$. Continuing in this way, we have

$$(x+y)^{p^j} = x^{p^j} \quad , \quad \text{for } j \geq \mu - \lambda + 1 \quad , \quad x \in \mathrm{L} \quad , \quad y \in \mathfrak{M}^\lambda \quad , \quad \lambda \geq 1 \tag{5}$$

where $\mu = \mathrm{Depth}(\mathfrak{M})$.
In particular, for $j \geq \mu$ the power $(x+y)^{p^j}$ does not depend on the choice of $y \in \mathfrak{M}$.
Let $\Im \subseteq \mathrm{L}$ be a representation system for $(\mathrm{L}/\mathfrak{M})^* = K^*$.
Since (4) is an automorphism,

$$\Im^p := \{x^p \mid x \in \Im\} \tag{6}$$

is also a representation system for $(\mathrm{L}/\mathfrak{M})^*$, and so are all $\Im^{p^j} := \{x^{p^j} \mid x \in \Im\}$.
The Teichmüller representation system of $(\mathrm{L}/\mathfrak{M})^*$ (of L for simplicity) is defined by

$$\mathrm{T} := \{x^{p^\mu} \mid x \in \Im\}. \tag{7}$$

By (5), the Teichmüller representation system T does not depend on the choice of $\Im$.
Clearly, T is the only representation system of $(\mathrm{L}/\mathfrak{M})^*$ with $\mathrm{T}^p = \mathrm{T}$.
Since $x^{p^\mu} \cdot y^{p^\mu} = (x \cdot y)^{p^\mu}$ for $x, y \in \mathrm{L}$, the representation system T is also multiplicativly closed. So $\pi : \mathrm{L} \longrightarrow K$ induces a group isomorphism
$\overline{\pi} : \mathrm{T} \longrightarrow K^*$ where $\overline{\pi} = \pi|_{\mathrm{T}}$. In particular, T is also cyclic, i.e.

$$\mathrm{T} = (\eta) \tag{8}$$

with $\eta \in \mathrm{T}$. And we have $\mathrm{Card}(\mathrm{T}) = p^r - 1$.

5 Determination of the Galois ring in L

Now put $\mathrm{T}_0 := \mathrm{T} \cup \{0\}$ and consider the subsets of L

$$S_i := \mathrm{T}_0 \cdot p^i + \mathrm{T}_0 \cdot p^{i+1} + \ldots + \mathrm{T}_0 \cdot p^{n-1} + \mathrm{T}_0 \cdot p^n \tag{9}$$

with $i = 0, 1, \ldots, n-1, n$.

5.1 Lemma. *The S_i are additive subgroups of* L.

Proof. We will prove this by descending induction from n to 0.
This is clear for $S_n = \mathrm{T}_0 \cdot p^n = \{0\}$.
Suppose $i < n$ and that S_{i+1} is an additive subgroup of L. Let us show that S_i is also an additive subgroup of L. It is clear that $0 \in S_i$.
Let $u, v \in S_i$. We have $u = u_i p^i + u'$ and $v = v_i p^i + v'$ with $u_i, v_i \in \mathrm{T}_0$ and $u', v' \in S_{i+1}$. If $u_i = 0$ or $v_i = 0$ then $u + v \in S_i$. If $u_i \neq 0$ and $v_i \neq 0$, we can write $u_i = x^{p^\mu}$ and $v_i = y^{p^\mu}$ with $x, y \in \mathrm{T}$ by using $\mathrm{T} = \mathrm{T}^{p^\mu}$. It can be proved by induction from $j = 1$ to $j = \mu$ that $p^i \cdot (x+y)^{p^\mu} \equiv p^i \cdot (x^{p^\mu} + y^{p^\mu}) \bmod S_{i+1}$. But $(x+y)^{p^\mu} \in \mathrm{T}_0$ (whereas the sum may fall outside of T_0). So $p^i \cdot (x^{p^\mu} + y^{p^\mu}) \in p^i \cdot \mathrm{T}_0 + S_{i+1} = S_i$. Thus, $u + v \in S_i$. So S_i is additively closed.
Finally, let $w \in S_i$. Since $p^n w = 0$ and S_i is additively closed, then $-w \in S_i$.
Thus, S_i is an additive subgroup of L. □

5.2 Remark. Since T is multiplicatively closed, then S_i is also multiplicatively closed.

Now, put $S := S_0$.
Thus

$$S = \mathrm{T}_0 + \mathrm{T}_0 \cdot p + \ldots + \mathrm{T}_0 \cdot p^{n-1}. \tag{10}$$

5.3 Remark. Since $1 \in S$, then S is a subring of L.

5.4 Lemma. *S is a local ring with maximal ideal pS.*

Proof. If $\alpha + p \cdot \beta$, $\alpha \in \mathrm{T}$, $\beta \in S$ is in $S \setminus pS$, we get the multiplicative inverse $(\alpha + p \cdot \beta)^{-1}$ by $\alpha^{-1}(1 - p \cdot [-\frac{\beta}{\alpha}])^{-1}$ and the geometric series formula $(1 - p \cdot Y)^{-1} = 1 + p \cdot Y + \cdots + p^{n-1} \cdot Y^{n-1}$. □

5.5 Lemma. *We have $pS = \mathfrak{M} \cap S$.*

Proof. pS is the maximal ideal of S and $\mathfrak{M} \cap S$ is an ideal of S, then $\mathfrak{M} \cap S \subseteq pS$. Conversely, since $pS \subseteq S$ and $p \in \mathfrak{M}$, then $pS \subseteq \mathfrak{M}$ and $pS \subseteq \mathfrak{M} \cap S$. □

5.6 Lemma. *S/pS is isomorphic to $K = \mathbb{F}_{p^r}$.*

Proof. We see that S contains the whole Teichmüller representation system T of L and so a system of representatives of $\mathrm{L}/\mathfrak{M}$. Thus, from Lemma 5.5, the sequence of morphisms $S \longrightarrow \mathrm{L} \longrightarrow \mathrm{L}/\mathfrak{M}$ induces the isomorphism $S/pS \longrightarrow \mathrm{L}/\mathfrak{M}$, $x + pS \longmapsto x + \mathrm{M}$. □

5.7 Lemma. *Let $(\mathrm{L}', \mathfrak{M}')$ be a local ring with $\mathrm{L}' \subseteq \mathrm{L}$, $\mathfrak{M}' = \mathrm{L}' \cap \mathfrak{M}$ and such that the inclusion $\mathrm{L}' \hookrightarrow \mathrm{L}$ induces an isomorphism $\mathrm{L}'/\mathfrak{M}' \longrightarrow \mathrm{L}/\mathfrak{M}$. Then the Teichmüller representation system* T *of* L *is also the Teichmüller representation system* T′ *of* L′*, i.e.* $\mathrm{T} = \mathrm{T}'$.

Proof. A system of representatives of $\mathrm{L}'/\mathfrak{M}'$ becomes a system of representatives of $\mathrm{L}/\mathfrak{M}$ and $\mathrm{T}' = \mathrm{T}'^{p^{\mu-\mu'}} = \mathrm{T}$, with $\mu' = \mathrm{Depth}(\mathfrak{M}')$. □

5.8 Theorem. *S is the unique Galois ring of characteristic p^n and of order r contained in the finite local ring* L.

Proof. It is clear that $\mathrm{Card}(S) = p^{rn}$. Thus, from Lemmas 5.4 and 5.6, S is a finite local ring with parameters (p, n, r) and maximal ideal pS. So S is the Galois ring $GR(p^n, r)$. Furthermore, the morphism $S \hookrightarrow \mathrm{L}$ induces an isomorphism $S/pS \longrightarrow \mathrm{L}/\mathfrak{M}$. So from Lemma 5.7, (S, pS) is the smallest subring of $(\mathrm{L}, \mathfrak{M})$ of the above type. In particular, (S, pS) is unique in $(\mathrm{L}, \mathfrak{M})$. □

5.9 Theorem. *We have $S = (\mathbb{Z}/p^n\mathbb{Z})[\eta]$ where $\mathrm{T} = (\eta)$.*

Proof. It is clear that $S \subseteq (\mathbb{Z}/p^n\mathbb{Z})[\eta]$. Conversely, $(\mathbb{Z}/p^n\mathbb{Z})[\eta]$ is the smallest ring extension of $\mathbb{Z}/p^n\mathbb{Z}$ in L which contains η. And S is a subring of L containing η and $\mathbb{Z}/p^n\mathbb{Z}$. □

References

[1] S. Lang, Algebra, third ed., *Addison-Wesley*,1993.

[2] G.J. Janusz, Separable algebras over commutative rings, *Trans.AMS*, 122(1966), 461-479.

[3] R. Raghavendran, Finite Associative Rings, *Compos. Math.*, 21(1969), 195-229.

[4] W. Krull, Algebraische Theorie der RingeII, *Math.Ann.*, 91(1924), 1-46.

[5] H. Lueneburg, On the Early History of Galois Fields, *Finite Fields Appl.*, 341-355.

[6] B.R. McDonald, Finite Rings with identity, *Marcel Dekker Inc*, New York, 1974.