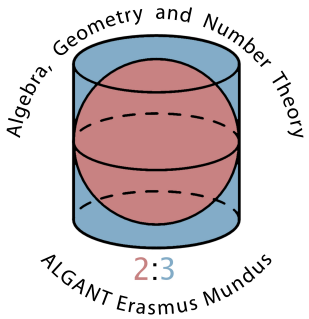

Universiteit Leiden
Mathematisch Instituut

Master thesis

On local Galois module structure for cyclic extensions of prime degree

Candidate: **Marta Lucchini**
Thesis Advisor: **Dr. Bart de Smit**

Academic year: 2011-2012

Come sarà
un giorno prendere
la strada e andare via,
incontro alla realtà,
farsi travolgere
da un vento di follia,
come sarà?

Claudio Baglioni
Noi no

Contents

Introduction

Let A be a complete discrete valuation ring with residue characteristic $p > 0$, and K the field of fractions of A. Let L be a finite Galois extension of K of Galois group G, and B the integral closure of A in L.

The associated order R of B is defined as the subring of the group ring $K[G]$,

$$R := \{x \in K[G] : xB \subseteq B\}.$$

An important question in Galois module theory is concerned with the structure of B as an R-module. Although the theory is complete for tamely ramified extensions, when we know $R = A[G]$ and B is R-free (see Theorem 1.1.3), there is still no general answer about the freeness of B over R for wildly ramified extensions (see [17] for a survey about this field of study).

Our work deals with a particular aspect of this problem. Assume L/K is totally ramified of degree $p > 0$ equal to the residue characteristic of K (hence the extension has ramification index p and the corresponding extension of residue fields is of degree 1). We denote by σ a generator of the Galois group G.

In [3] and [4], F. Bertrandias, J.-P. Bertrandias and M.-J. Ferton give a criterion for B to be R-free, in the unequal characteristic case, i.e. when $\mathrm{char}K = 0$. On the other hand, in the equal characteristic setting, namely when $\mathrm{char}K = p$, a criterion for freeness is achieved by A. Aiba in [1]; his result is then extended in [6] by B. de Smit and L. Thomas: after defining combinatorial objects related to certain properties of the ramification of the extension, they give a combinatorial description of B and R as modules over A, and determine explicit generators for B over R, even in the non-free case.

In this thesis, we shall investigate whether the same approach is applicable in the unequal characteristic framework and adapt, as much as possible, the results achieved in [6] to our context.

There are two main issues which distinguish the two cases and do not allow a complete standardization of the theory. First, when $\mathrm{char}K = p$, we have $(\sigma - 1)^p = \sigma^p - 1 = 0$, which permits to equip L (resp. B) with the

structure of a graded module over $K[G]$ (resp. $A[G]$); this property, which we have to give up in the unequal characteristic case, simplifies a lot the nature of the objects at issue. Secondly, depending on the characteristic of K, the ramification groups and jumps of the extension (see Chapter 1.2) have completely different properties. In particular, when $\mathrm{char}K = 0$ the unique ramification jump t of the extension is bounded in terms of the absolute ramification index of K, and the case in which it is "very close" to the bound ("almost maximally ramified case") turns out to be more delicate and requires to be treated separately.

The thesis has four chapters.

The first one recalls some preliminary notions about Galois module structure theory and ramification theory; moreover, it introduces the combinatorial tools we need, and discusses some of their properties.

In the second chapter, we describe the structure of B and R considered as A-modules. We will see that, despite the deep differences between the equal and unequal characteristic settings, it is possible to give similar A-bases for B and R, in the two cases. Until this point indeed, we quite manage to control the divergence related to the characteristic of the base field.

The third chapter is concerned with the nature of R as a ring; in particular we wonder whether it is local. This question plays a crucial role when attacking the problem of the R-freeness of B: de Smit and Thomas, in [6], use the fact that, when $\mathrm{char}K = p$, the associated order is a local ring. In characteristic 0, this does not need to be true, and it is exactly at this point that the notion of almost maximal ramification intervenes: in the chapter we prove that R is local if and only if the extension L/K is not almost maximally ramified, and we determine the nature of $R/J(R)$, where $J(R)$ denotes the Jacobson radical of R, for almost maximally ramified extensions.

In the last chapter, we eventually investigate the structure of B over R, assuming $\mathrm{char}K = 0$. We will see that, in the not almost maximally ramified case, the same criterion for B to be R-free holding in the equal characteristic setting is still valid: B is R-free if and only if $s|p-1$, where s is the remainder of the division by p of the ramification jump t (see Definition 1.2.2). We also determine a minimal set of R-generators for B when it is not free. When the extension is almost maximally ramified instead, s dividing $p-1$ is a sufficient but not necessary condition for B to be R-free. The following theorem combines Proposition 4.1.1, Theorem 4.5.1 and Theorem 4.6.1, which contain our main result; the set $\mathcal{D}'$ appearing in the statement is a set of integers contained in $\{1, \dots, p\}$ and it is defined by combinatorial objects which only depend on s (see (4.7)).

Theorem. *Assume the extension L/K is almost maximally ramified;*

i) if $s|p-1$ or $s=0$, then B is free over R;

ii) if $s \nmid p-1$, then the cardinality d of a minimal set of R-module generators for B is $d = \#\mathcal{D}' - 1$. In particular, B is R-free if and only if $\#\mathcal{D}' = 2$.

Hence, by extending to the unequal characteristic setting the techniques exploited by de Smit and Thomas, we manage not only to give a criterion for freeness, but also to compute an explicit basis, or a minimal set of generators, for B over its associated order.

Chapter 1

Preliminaries

In this chapter, we shall review some definitions and results concerning Galois module structure theory and the ramification theory of local fields. Further, we are going to introduce some combinatorial objects which will play an essential role in the development of our study.

1.1 Galois module structure theory: first definitions and results

We start from a classical result, for the proof of which we refer to [11, VI.13, Theorem 13.1].

Theorem 1.1.1 (Normal Basis Theorem)**.** *Let L/K be a finite Galois extension of fields with Galois group G. There exists $x \in L$ such that a basis for L over K is given by the Galois conjugates of x; in other words, L is a free $K[G]$-module of rank 1. Such an x is called a normal basis generator of L over K.*

Before introducing the concept of normal integral basis, let us recall few notions about local fields.

By a local field we mean a field K which is complete with respect to a discrete valuation v_K, that is a surjective group morphism $v_K : K^\times \to \mathbb{Z}$, and whose residue field is perfect. The ring of integers of K is the valuation ring $A = \{x \in K : v_K(x) \geq 0\}$, whose fraction field is K, and the residue field of K is $A/\mathfrak{p}$, where $\mathfrak{p}$ denotes the unique maximal ideal of A, i.e. $\mathfrak{p} = \{x \in K : v_K(x) > 0\}$. An element $\pi_K \in K$ such that $v_K(\pi_K) = 1$ is called a uniformizer of K.

Let L/K be a finite Galois extension of number fields or local fields with Galois group G; let A and B be the rings of integers of K and L respectively;

then the action of G induces on B a natural structure of $A[G]$-module (in this sense, B is referred to as a Galois module).

From now on, if L/K is a finite Galois extension of number fields or local fields, $A \subset B$ will indicate the associated rings of integers, G the Galois group.

Definition 1.1.2. *A finite Galois extension L/K of number fields or local fields is said to admit an integral normal basis if there exists an element $\alpha \in L$ such that an A-basis for B is given by the Galois conjugates of α, or equivalently, if B is a free $A[G]$-module of rank 1.*

The existence of an integral normal basis turns out to be tightly related to the ramification properties of the extension. Several results have been achieved concerning the conditions an extension must satisfy in order to admit an integral normal basis. We refer to [17], for a complete survey of this broad theory.

However, in the context of local fields in which our work develops, the following result, due to Emily Noether (see [12]), deserves to be mentioned. We remind that a finite extension L/K of local fields is said to be tamely ramified when its ramification index is prime to the residue characteristic of K.

Theorem 1.1.3 (Noether's criterion)**.** *Let L/K be a finite Galois extension of local fields, with Galois group G. Then B is a free $A[G]$-module if and only if the extension is tamely ramified.*

Remark that for an extension L/K of number fields, if B is free as an $A[G]$-module, then necessarily the extension L/K is tamely ramified, although this condition is not sufficient. Indeed several examples of tame extensions $L/\mathbb{Q}$ without integral normal basis have been explicitly given, among which certain quaternion extensions. We refer again to [17] for more details.

Noether's criterion suggests that another strategy is required in order to determine the Galois module structure of B when the extension is wildly ramified. One possible approach consists in considering B as a module over a larger subring of $K[G]$ than the group ring $A[G]$. This object is called the associated order of B, that is why it seems appropriate to recall few notions about orders.

Definition 1.1.4. *Let A be a noetherian integral domain and F its quotient field. Let E be a finite-dimensional F-algebra, V a finite-dimensional F-vector space. A full A-lattice in V is a finitely-generated A-submodule M in V such that $F \cdot M = V$, where $F \cdot M$ is the set of finite sums $\sum x_i m_i$, $x_i \in F, m_i \in M$. An A-order in E is a subring Λ of E such that Λ is a full A-lattice in E.*

With the same notations as in the previous definition, for a full A-lattice M in E, we define the left order of M as

$$\mathcal{A}_l(E, M) := \{y \in E : \ yM \subseteq M\}$$

This is indeed an order (see [13, II.8]) and leads us to the next definition:

Definition 1.1.5. *Let L/K be a finite Galois extension of number fields or local fields; the associated order R of the ring of integers B of L is*

$$R := \mathcal{A}_l(K[G], B) = \{y \in K[G] : \ yB \subseteq B\}.$$

By Theorem 1.1.1, B can be identified with an A-lattice in $K[G]$ via the isomorphism of $K[G]$-modules $L \cong K[G]$. Hence, R is an A-order and, as an A-module, it is free or rank $[L : K]$. Note that if G is abelian, R is isomorphic to the ring $\mathrm{End}_{A[G]}B$ of $A[G]$-endomorphisms of B.

The following proposition shows that R is the only A-order over which B can possibly be free, which explains why it makes sense to consider R instead of $A[G]$ in the wildly ramified case. Of course, when B is R-free, it is of rank 1 and the element α such that $B = R \cdot \alpha$ is a normal basis generator for L/K.

Proposition 1.1.6. *Let L/K be a finite Galois extension of number fields or local fields. If B is free over an A-order Γ in $K[G]$, then $\Gamma = R$.*

Proof. First note that, if B is a Γ-module, automatically $\Gamma \subseteq R$, by definition of R. Suppose B is free over Γ with $B = \Gamma \cdot \alpha$ for some $\alpha \in B$. If x is in R, then $x\alpha$ is in B by definition of R; hence $x\alpha = y\alpha$ for some $y \in \Gamma$. We must have $x = y$ as α generates L as a free $K[G]$-module of rank 1, so $x \in \Gamma$. □

In general, we have $A[G] \subseteq R$, with equality if and only if the extension L/K is tamely ramified. This can be easily seen in the local case. Indeed, by Theorem 1.1.3, if L/K is tamely ramified, it admits an integral normal basis, which is equivalent to say that B is $A[G]$-free. By Proposition 1.1.6, R is the only A-order over which B can be free; we deduce that $R = A[G]$. On the other hand, if L/K is wildly ramified, one can show that the maximal ideal $\mathfrak{p}$ of A divides the ideal $\mathrm{Tr}_{L/K}(B)$ of A, (here Tr denotes the usual trace map $L \to K$ and $\mathrm{Tr}_{L/K}(B) = \{\mathrm{Tr}_{L/K}(x), \ x \in B\}$). Therefore, if π_K is a uniformizer of K, we have $\frac{1}{\pi_K} \sum_{g \in G} g \in R$, which implies $R \neq A[G]$.

The problem of determining the structure of R and discussing the freeness of B over R in the wildly ramified case arises then naturally. These are the questions that, in a certain specific context, will be mainly dealt with in this thesis.

The following notions about ramification are also useful to our purposes.

1.2 Ramification groups and jumps

For a complete treatment of this theory we refer to [14, Chapter IV].

Let L/K be a finite Galois extension of local fields with Galois group G; assume that the extension of the associated residue fields is separable. Let $\mathfrak{p}_L$ denote the maximal ideal of the ring of integers B of L.

Definition 1.2.1. *For $i \in \mathbb{Z}_{\geq -1}$ we define the i-th ramification group of L/K as*

$$G_i = \{\sigma \in G \text{ such that } \sigma(x) - x \in \mathfrak{p}_L^{i+1} \text{ for all } x \in B\},$$

or equivalently

$$G_i = \{\sigma \in G \text{ such that } \sigma(x)/x \in 1 + \mathfrak{p}_L^{i} \text{ for all } x \in L^{\times}\}. \tag{1.1}$$

Note that we have a decreasing filtration of normal subgroups of G,

$$G_{-1} = G \supseteq G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n \neq G_{n+1} = \{1\}, \tag{1.2}$$

for some $n \geq -1$.

The group G_0 is called the inertia group and its order is the ramification index $e_{L/K}$: one can prove that, if K^{unr} is the largest unramified subextension of L over K, and H the subgroup of G fixing K^{unr}, then $H = G_0$ (see [14, IV.1, Corollary to Prop. 2]). Therefore the extension L/K is unramified (totally ramified) if and only if the inertia group is trivial (G itself).

Further L/K is tamely ramified if and only if $G_1 = \{1\}$. This is easy to prove after considering two facts: first, G_1 is a p-group, with p characteristic of the residue field $\bar{L}$ of L ([14, IV.2, Corollary 3]); secondly, the group morphism $G_0 \to \bar{L}^{\times}$ given by $\sigma \mapsto u$ with u such that $\sigma(\pi_L) = u\pi_L$ for a uniformizer π_L of L, induces an injection $G_0/G_1 \hookrightarrow \bar{L}^{\times}$.

Finally, the case $\mathrm{char}\bar{L} = 0$ deserves a remark: for $i \geq 1$, consider the map $G_i \to \bar{L}$, $\sigma \mapsto a$, where $a \in B$ is such that $\sigma(\pi_L) - \pi_L = a\pi_L^{i+1}$: this is a group morphism which induces an injection $G_i/G_{i+1} \hookrightarrow \bar{L}$; if $\mathrm{char}\bar{L} = 0$, then $\bar{L}$ has no trivial finite subgroups, which yields $G_i = G_{i+1}$. As we must get $G_i = \{1\}$ at a certain i, we deduce $G_1 = \{1\}$. Hence, if $\mathrm{char}\bar{L} = 0$, the extension L/K is at most tamely ramified, which explains why we do not consider such a context when interested in certain behaviors of wild ramification.

Instead, throughout this thesis, we will deal with local fields whose residue field has characteristic $p > 0$. If K is such a field, then either K is a finite extension of the p-adic numbers $\mathbb{Q}_p$, or it is a finite extension of the field of formal power series $\mathbb{F}_p((t))$, over the field of p elements. Call $\bar{K}$ the residue

field of K; the first case is referred to as the "unequal characteristic case", as $\mathrm{char}K = 0$ and $\mathrm{char}\bar{K} = p$, whereas by "equal characteristic case" we indicate the second context, since $\mathrm{char}K = \mathrm{char}\bar{K} = p$.

In the framework of ramification theory, we shall also introduce the concept of ramification jump.

Definition 1.2.2. *Consider the filtration in (1.2); the integers $t \geq -1$ such that $G_t \neq G_{t+1}$ are called ramification jumps.*

One can prove a number of results concerning the ramification jumps of a totally ramified p-extension of local fields L/K, where p is the residue characteristic of K; however, as we will only deal with extensions of degree p, we will not need but some properties of the (unique) ramification jump in this setup. The following proposition, for which we give here a sketch of proof, fixes an upper bound for the ramification jump, whenever $\mathrm{char}K = 0$.

Proposition 1.2.3. *Suppose the extension L/K is totally ramified of degree $p > 0$ equal to the residue characteristic of K. If the characteristic of K is 0, the unique ramification jump t of the extension L/K satisfies*

$$-1 \leq t \leq \frac{ap}{p-1},$$

where $a := v_K(p)$ is the absolute ramification index of K.

Proof. Let π_L be a uniformizer for the ring of integers B of L. Then, as L/K is totally ramified, B is generated by π_L over A, i.e. $B = A[\pi_L]$ (see [14, I.6, Prop. 18]). Further, let $\mathcal{D}_{L/K}$ denote the different of L/K and $f = X^p + a_1X^{p-1} + \ldots + a_p$ the minimal polynomial of π_L over K, with $a_i \in A$. We have

$$\mathcal{D}_{L/K} = (f'(\pi_L))$$

([14, III.6, Corollary 2]). Now, $f'(\pi_L) = \sum_{i=1}^{p} i a_{p-i} \pi_L^{i-1}$, with $a_0 = 1$; as the terms $ia_{p-i}\pi^{i-1}$ have all different valuations v_L modulo p, we get

$$\begin{aligned} v_L(\mathcal{D}_{L/K}) = v_L(f'(\pi_L)) &= inf\{v_L(ia_{p-i}\pi_L^{i-1}), i = 1, \ldots, p\} \\ &\leq v_L(p\pi_L^{p-1}) = ap + p - 1. \end{aligned} \tag{1.3}$$

On the other hand, one can also prove

$$v_L(\mathcal{D}_{L/K}) = \sum_{i=0}^{\infty} (\#G_i - 1) = (p-1)(t+1), \tag{1.4}$$

(see [14, IV.2, Prop. 4]). The lemma follows by combining (1.3) and (1.4). □

We have also seen that, if L/K is wildly ramified, $G_{-1} = G_0 = G_1 = G$. Hence we will always take the set $\{1, 2, \ldots, ap/(p-1)\}$ as a range for t.

The proposition above together with the following one justify the definitions of maximal and almost maximal ramification, which are due to Jacobinski (see [9]). The setting assumed is the same as in Proposition 1.2.3.

Proposition 1.2.4. *If $p|t$, then $t = ap/(p-1)$; further K contains the p-th roots of unity and there exists a uniformizer π of K, such that $L = K(\pi^{1/p})$.*

Proof. See [8, III.2, Prop. 2.3]. □

Definition 1.2.5. *Let K be a local field of characteristic 0. The extension L/K is said to be maximally ramified if $t = ap/(p-1)$; further, it is called almost maximally ramified when t satisfies*

$$\frac{ap}{p-1} - 1 \leq t \leq \frac{ap}{p-1}.$$

Chapter 3 will clarify the importance of this notion with respect to the questions we pose, and will give a characterization for this kind of extensions.

Before concluding this chapter, some combinatorial definitions.

1.3 The combinatorics involved

The description of the associated order that will be proposed in the next chapter makes use of the same combinatorial objects introduced and exploited by de Smit and Thomas in [6]. We redefine them here and recall some easy properties of theirs.

Let $x \in \mathbb{R}$, $0 \leq x < 1$. For any integer i we define a_i, ϵ_i as follows:

$$\begin{aligned} a_i &= \lceil ix \rceil = \inf\{n \in \mathbb{Z} : n \geq ix\} \\ \epsilon_i &= a_i - a_{i-1} \end{aligned}$$

The sequences $(a_i)_{i\in\mathbb{Z}}$ and $(\epsilon_i)_{i\in\mathbb{Z}}$ satisfy the following properties:

Lemma 1.3.1. *For all $i, j, n \in \mathbb{Z}$, $n \geq 0$, we have*

$$|(\epsilon_{i+1} + \ldots + \epsilon_{i+n}) - (\epsilon_{j+1} + \ldots + \epsilon_{j+n})| \leq 1 \tag{1.5}$$

$$a_n = \epsilon_1 + \ldots + \epsilon_n = sup\{\epsilon_{i+1} + \ldots + \epsilon_{i+n}, i \in \mathbb{Z}\} \tag{1.6}$$

Proof. Remark that, for $i \in \mathbb{Z}$, $n \in \mathbb{Z}_{\geq 0}$, we have $\epsilon_{i+1} + \ldots + \epsilon_{i+n} = a_{i+n} - a_i$. On the one hand, $a_i + a_n \geq ix + nx$, hence $a_i + a_n \geq \lceil (i+n)x \rceil = a_{i+n}$. On

the other hand, $a_{i+n} - a_i \geq (i+n)x - ix - 1 = nx - 1$, so $a_{i+n} - a_i \geq a_n - 1$. It follows that

$$a_n - 1 \leq a_{i+n} - a_i \leq a_n, \tag{1.7}$$

which yields (1.5). Finally, proving (1.6) amounts to seeing that

$$0 \leq (\epsilon_1 + \ldots + \epsilon_n) - (\epsilon_{i+1} + \ldots + \epsilon_{i+n}) \leq 1,$$

or equivalently $0 \leq a_n - (a_{i+n} - a_i) \leq 1$, which is clear by (1.7). □

The following lemma holds for the sequence (ϵ_i) associated to a rational number $s/p \in [0,1)$ with $\gcd(s,p)$=1.

Lemma 1.3.2. *The sequence $\epsilon_2, \ldots, \epsilon_{p-1}$ is a palindrome.*

Proof. Remark that, as $a_j = j\frac{s}{p} + 1 - \{j\frac{s}{p}\}$ for all $j \in \mathbb{Z}$, we have $a_i + a_{p-i} = s + 1$ for any integer i, $0 < i < p$.
Hence, for $1 < i < p$,

$$\epsilon_i = a_i - a_{i-1} = a_{p-i+1} - a_{p-i} = \epsilon_{p-i+1},$$

which proves the lemma. □

We can also associate to s/p a third sequence $m_1, \ldots, m_{p-1}$ defined by

$$m_j = \inf\{\epsilon_{i+1} + \ldots + \epsilon_{i+j} : 0 \leq i < p - j\}; \tag{1.8}$$

notice that by Lemma 1.3.1, for $0 \leq i < p$, we have $a_i - m_i \in \{0, 1\}$. In particular, if $a_n = m_n$ for some $n \in \{1, 2, \ldots, p-1\}$, then by Lemma 1.3.1 we must have

$$\epsilon_1 + \ldots + \epsilon_n = \epsilon_{i+1} + \ldots \epsilon_{i+n}$$

for all i with $0 \leq i < p - n$. This easily yields the following

Lemma 1.3.3. *For every $n \in \{1, \ldots, p-1\}$, we have $a_n = m_n$ if and only if $\epsilon_i = \epsilon_j$ for all i, j with $0 < i, j < p$ and $i \equiv j$ modulo n. Then we call n a sub-period of (ϵ); further, n is called a minimal sub-period of (ϵ), if no proper divisor of n is a sub-period.*

To conclude, it is worth mentioning a few other properties about sub-periods. These are stated and proved in [6, Prop. 4]. For $x \in \mathbb{Q}$, $0 < x < 1$, let $\mathcal{M}(x)$ be the set of minimal sub-periods of the sequence (ϵ) associated to x.

Proposition 1.3.4. *Let $x = s/p$. If s divides $p-1$, then $\mathcal{M}(x) = \{(p-1)/s\}$; otherwise we have $p - 1 \in \mathcal{M}(x)$.*

We are now ready to get into the core of our work, starting with a description of the ring of integers B of L and its associated order R as A-modules.

Chapter 2

Bases for the ring of integers and its associated order

Throughout all this chapter, K denotes a local field of characteristic 0 and residue characteristic $p > 0$; let $\pi = \pi_K$ be a uniformizer of K. Further, L is a totally ramified Galois extension of K, whose Galois group G is cyclic of order p (hence the ramification index of the extension is p, and the corresponding extension of residue fields is of degree 1). We denote by A and B the valuation rings of K and L respectively, by R the associated order of B, according to Definition 1.1.5. Call t the unique ramification jump of L/K, a the absolute ramification index of K (i.e. $a = v_K(p)$), σ a generator of G. Let $s \in \{0, \dots, p-1\}$ and $k \in \mathbb{Z}_{\geq 0}$ be such that $t = pk + s$.

The goal of this chapter is to give bases for B and R as A-modules: we want these bases to be as close as possible to the ones given by de Smit and Thomas in [6, Prop. 3] in the equal characteristic setup.

2.1 A normal basis generator

By Theorem 1.1.1, we know that L is free of rank 1 as a $K[G]$-module. Our first step consists in finding a suitable normal basis generator of L. We first recall a criterion for any $x \in L$ to be a normal basis generator.

Proposition 2.1.1. *Suppose $p \nmid t$. In the setting described above, any element $x \in L$ of valuation $v_L(x) \equiv t \bmod p$ is a normal basis generator of L/K.*

The proof requires two preliminary lemmas. For the first one we include here the proof given in [8, III.2, Lemma 2.2]; the second one is proved below by adapting an argument given by Thomas in [16, Lemma 8]. The notation in the lemmas is the same as above.

Lemma 2.1.2. *For any $\alpha \in L$, there exists $a \in K$ such that*

$$v_L((\sigma-1)\alpha) = v_L(\alpha - a) + t.$$

Proof. Let π_L be a uniformizer for L; since L/K is totally ramified, π_L generates L over K; so let $a_0, \ldots, a_{p-1} \in K$ be such that $\alpha = a_0 + a_1\pi_L + \ldots + a_{p-1}\pi_L^{p-1}$. Set now $\beta = \sigma(\pi_L)/\pi_L - 1$; we have

$$\sigma(\alpha) - \alpha = \sum_{i=1}^{p-1} a_i \pi_L^i ((1+\beta)^i - 1)$$

Further, from $v_L(\beta) = t > 0$, we deduce that $v_L(a_i\pi_L^i((1+\beta)^i - 1))$ are all distinct, as $v_L((1+\beta)^i - 1) \equiv i\beta \bmod \pi_L^{t+1}$. Therefore,

$$\begin{aligned} v_L(\sigma(\alpha) - \alpha) &= inf\{v_L(a_i\pi_L^i((1+\beta)^i - 1)), i = 1, \ldots, p-1\} \\ &= inf\{v_L(a_i\pi_L^i\beta), i = 1, \ldots, p-1\} \\ &= v_L((\alpha - a_0)\beta) = v_L(\alpha - a_0) + t. \end{aligned}$$

The lemma holds with $a := a_0$. □

Lemma 2.1.3. *For any $\alpha \in L$ such that $p \nmid v_L(\alpha)$, we have*

$$v_L((\sigma-1)\alpha) = v_L(\alpha) + t$$

Proof. Let π_L be a uniformizer of L. For $i \geq 1$ consider the i-th ramification group G_i of L/K as defined in (1.1). We have that $\sigma \in G_t$ if and only if $\frac{\sigma x}{x} - 1 \equiv 0$ modulo π_L^t, for all $x \in L^\times$. As $G_t = G$ be definition of t,

$$v_L((\sigma-1)\alpha) = v_L\Big(\alpha\Big(\frac{\sigma\alpha}{\alpha} - 1\Big)\Big) \geq v_L(\alpha) + t.$$

We now show that this is actually an equality. Let $a_0, \ldots, a_{p-1} \in K$ be such that $\alpha = a_0 + a_1\pi_L + \ldots + a_{p-1}\pi_L^{p-1}$. By Lemma 2.1.2, we have

$$v_L((\sigma-1)\alpha) = v_L(\alpha - a_0) + t$$

Since $p|v_L(a_0)$ and $p \nmid v_L(\alpha)$, the valuation v_L takes different values on a_0 and α, so that $v_L(\alpha - a_0)$ is either $v_L(\alpha)$ or $v_L(a_0)$. It suffices to notice that $v_L(\alpha - a_0) = v_L(a_1\pi_L + \ldots + a_{p-1}\pi_L^{p-1})$ is not divisible by p, to conclude $v_L(\alpha - a_0) = v_L(\alpha)$. □

Proof. (Proposition 2.1.1.) By assumption p does not divide $v_L(x)$; hence Lemma 2.1.3 yields $v_L((\sigma-1)x) = v_L(x) + t$. Moreover $v_L((\sigma-1)^i x) =$

$v_L(x)+it$, while $v_L((\sigma-1)^{i-1}x)$ is not a multiple of p. Now, if $v_L(x) \equiv t \neq 0 \mod p$, and in this case only, we can write

$$v_L((\sigma-1)^i x) = v_L(x) + it \qquad \text{for } 0 \leq i \leq p-1.$$

To conclude, consider the set

$$\mathcal{N} = \{x, (\sigma-1)x, \ldots, (\sigma-1)^{p-1}x\};$$

its elements are linearly independent since $\{v_L((\sigma-1)^i x), 0 \leq i \leq p-1\}$ is a complete set of residues modulo p. Hence $\mathcal{N}$ is a normal basis for the extension L/K. □

2.2 The ring of integers

Assume p does not divide the ramification jump t. Let $x \in L$ be such that $v_L(x) = -t(p-1)$. By Proposition 2.1.1, we have $L = K[G] \cdot x$.

We intend to determine a basis for B as an A-module, by exploiting the normal basis just found for L over K.

Proposition 2.2.1. *Consider the set*

$$\mathcal{B} = \{e_i = \pi^{\lceil t(p-i)/p \rceil}(\sigma-1)^{i-1}x, \quad 1 \leq i \leq p\},$$

where $\lceil r \rceil$ denotes the smallest integer n such that $n \geq r$, for any real r. Then $\mathcal{B}$ is a basis for B as an A-module.

Proof. By our choice of x and by Lemma 2.1.3,

$$v_L((\sigma-1)^{i-1}x) = -t(p-i).$$

Now we would like to write $-t(p-i)$ in the shape $a_i p + b_i$ for suitable integers a_i, b_i, with $0 \leq b_i \leq p-1$. If $\lfloor r \rfloor$ denotes denotes the largest integer n such that $n \leq r$, after dividing by p we get

$$\begin{aligned} -t(p-i) &= p\lfloor -t(p-i)/p \rfloor + b_i \quad \text{for some } b_i \\ &= -p\lceil t(p-i)/p \rceil + b_i \end{aligned}$$

as $\lfloor -r \rfloor = -\lceil r \rceil$. It follows that $v_L(\pi^{\lceil t(p-i)/p \rceil}(\sigma-1)^{i-1}x) = b_i$. Note that $\{b_i, 0 \leq i \leq p-1\} = \{0, \ldots, p-1\}$, so that the $v_L(e_i)$ are all different residues modulo p. This implies that $\{e_i\}_{1 \leq i \leq p}$ is a basis for the $A/\mathfrak{p}$-vector space $B/\mathfrak{p}B$, where $\mathfrak{p}$ is the maximal ideal of A. As a consequence of Nakayama's Lemma (see [2, II, Prop. 2.8]), this yields the statement. □

The result in Proposition 2.2.1 can be reformulated in terms of the combinatorial sequences described in the previous chapter.

Write $t = pk + s$, with $1 \leq s \leq p$ (we are still assuming that p does not divide t). We introduce here the sequences (ϵ_i), (a_i), (m_i) associated to s/p. Then

$$\lceil t(p-i)/p \rceil = k(p-i) + \lceil (p-i)s/p \rceil = k(p-i) + a_{p-i};$$

from now on we will work on $\mathcal{B}$, expressed as follows:

$$\mathcal{B} = \{e_i = \pi^{k(p-i)+a_{p-i}}(\sigma - 1)^{i-1}x, \quad 1 \leq i \leq p\} \tag{2.1}$$

Remark that the choice we made for the valuation of the generator x has allowed us to give for B over A an analogous basis to the one given in [6], in the equal characteristic case. In that framework, a normal basis generator of valuation v_L equal to $-t(p-1)$ came up after manipulating the Artin-Schreier generator of the extension L/K; further, in $K[G]$ with K of characteristic p, we have $(\sigma - 1)^p = \sigma^p - 1 = 0$, so L and B could be equipped with the structure of graded $K[G]$-module and graded $A[G]$-module respectively. Of course, this is what we cannot reproduce in the unequal characteristic case.

2.3 The associated order

Consider now the associated order R of B, as we defined it in Chapter 1:

$$R = \{y \in K[G] : yB \subseteq B\}$$

We would like to give a description of R as an A-module. As an intermediate result, we prove the following

Lemma 2.3.1. *Assume $p \nmid t$. For a and σ as before, for $x \in L$ with $v_L(x) = -(p-1)t$, we have*

$$v_L((\sigma - 1)^i x) = \begin{cases} -(p-1-i)t & \text{if } 0 \leq i \leq p-1, \\ ap - (2p-2-i)t & \text{if } p \leq i \leq 2p-2 \end{cases}$$

Proof. The case $0 \leq i \leq p-1$ is an immediate consequence of Lemma 2.1.3, so we are interested in the second part of the statement. First, we shall compute the valuation v_L of $(\sigma - 1)^p x$. Set $z = \sigma - 1$; then $(z+1)^p = 1$, so

$$z^p = -pz(1 + n_1 z + n_2 z^2 + \ldots + n_{p-3} z^{p-3} + z^{p-2}),$$

where each n_i is a positive integer. By Lemma 2.1.3, $v_L(zx) = v_L(x) + t > v_L(x)$; hence

$$v_L(z^p x) = v_L(-pzx) = ap + t + v_L(x)$$

which is equal to $2t$ modulo p. Thus, for $p \neq 2$, we have $2t \neq 0$ modulo p and we are allowed to write $v_L(z^{p+i}x) = ap + (i+1)t + v_L(x) = ap - (p-i-2)t$, for $0 \leq i \leq p-2$, whence the result announced. If instead $p = 2$, then the lemma is still true, since $p \leq i \leq 2p-2$ only includes $i = 2$. □

As before, s denotes the residue of t modulo p.

Theorem 2.3.2. *Assume $0 < s < p$; let $(m_i)_{0<i<p}$ be the sequence defined in (1.8), associated to s/p. Put $m_0 := 0$. Then the set*

$$\mathcal{R} = \{f_i = \frac{(\sigma-1)^i}{\pi^{ik+m_i}} \quad 0 \leq i \leq p-1\}, \tag{2.2}$$

is a basis for the associated order R as an A-module.

Proof. First of all, we shall show that indeed $f_i e_j$ is in B, for all $0 \leq i \leq p-1$, $1 \leq j \leq p$ and e_j as in (2.1). If $i + j \leq p$, the proof is the same as in the equal characteristic case: set $\varphi = (\sigma - 1)/\pi^k$ and remark

$$\begin{aligned} \varphi e_j &= \pi^{k(p-j-1)+a_{p-j}}(\sigma-1)^j(x) \\ &= \pi^{k(p-j-1)+a_{p-j-1}+\epsilon_{p-j}}(\sigma-1)^j(x) \\ &= \pi^{\epsilon_{p-j}} e_{j+1} \end{aligned}$$

It follows that $\varphi^i e_j = \pi^{\epsilon_{p-i-j+1}+\ldots+\epsilon_{p-j}} e_{i+j}$. Therefore by definition of the sequence (m_i), we get that

$$f_i e_j \in \{e_{i+j}, \pi e_{i+j}\}. \tag{2.3}$$

Of course then $f_i e_j \in B$.

On the other hand, the case $i + j > p$ is more tricky and peculiar of the characteristic 0 environment. Assume then $i + j > p$, say $i + j = p + l$, with $1 \leq l \leq p-1$; we have

$$f_i e_j = \frac{(\sigma-1)^{i+j-1}(x)}{\pi^{(i+j-p)k+m_i-a_{p-j}}} = \frac{(\sigma-1)^{p+l-1}(x)}{\pi^{lk+m_i-a_{i-l}}}.$$

By Lemma 2.3.1, we can compute the valuation v_L of $f_i e_j$:

$$\begin{aligned} v_L(f_i e_j) &= ap - (2p-2-(p+l-1))t - p(lk + m_i - a_{i-l}) \\ &= ap - (p-1)t + ls - p(m_i - a_{i-l}) \end{aligned} \tag{2.4}$$

Since char$K = 0$, we have $(p-1)t \leq ap$ (see Proposition 1.2.3) and, under our initial assumption that p does not divide t, the inequality is strict, by Proposition 1.2.4. So we can write $ap = (p-1)t + n$, with $n \equiv s$ modulo p. We find

$$v_L(f_i e_j) = n + ls - p(m_i - a_{i-l}) \geq (l+1)s - p(m_i - a_{i-l})$$

Our purpose is to show that the quantity on the RHS is non-negative (we will actually see it is positive). First, we prove that $m_i - a_{i-l} \leq a_{l+1} - 1$. Indeed, if $m_i = a_i$, then $\epsilon_{i+1} = \epsilon_1 = 1$ (according to the terminology of Lemma 1.3.3, i is a sub-period of (ϵ)), and $a_i + 1 = a_{i+1}$; hence

$$\begin{aligned} m_i + 1 &= a_{i+1} = \epsilon_1 + \ldots \epsilon_{l+1} + \epsilon_{l+2} + \ldots + \epsilon_{i+1} \\ &\leq a_{l+1} + a_{i-l} \end{aligned}$$

by Lemma 1.3.1, (1.6). If instead $m_i + 1 = a_i$, then

$$m_i + 1 \leq a_{i+1} \leq a_{l+1} + a_{i-l}$$

Further, $a_{l+1} - 1 = \lceil (l+1)s/p \rceil - 1 < (l+1)s/p$. Therefore

$$m_i - a_{i-l} \leq a_{l+1} - 1 < (l+1)s/p, \tag{2.5}$$

which gives what we wanted. This proves that, for every i, j, we have $v_L(f_i e_j) \geq 0$, or in other words,

$$\bigoplus_{i=0}^{p-1} A f_i \subseteq R. \tag{2.6}$$

It remains to prove this inclusion is an equality. For this, let

$$\theta := \sum_{i=0}^{p-1} x_i f_i, \qquad x_i \in K$$

and suppose $\theta \in R$; we want to show that x_i is in A for all i. Let i_0 be the largest index i for which x_i is non-zero; assume first $i_0 \neq 0, p-1$. Consider $v \in \{0, \ldots, p-1-i_0\}$ such that

$$m_{i_0} = \epsilon_{v+1} + \ldots + \epsilon_{v+i_0}$$

In fact, we can assume $v \in \{1, \ldots, p-1-i_0\}$: if $v = 0$, then $a_{i_0} = m_{i_0}$, hence i_0 is a sub-period for (ϵ) and $\epsilon_1 + \ldots + \epsilon_{i_0} = \epsilon_2 + \ldots + \epsilon_{i_0+1}$.

We shall consider the action of θ on ϵ_v. We have

$$\begin{aligned}\theta e_v &= \sum x_i f_i e_v \qquad \text{(remark } i+v<p \text{ for all i)} \\ &= \sum x_i \pi^{k(p-v-i)+a_{p-v}-m_i} z^{v+i-1} x \\ &= \sum x_i \pi^{a_{p-v}-a_{p-v-i}-m_i} \pi^{k(p-v-i)+a_{p-i-v}} z^{v+i-1} x \\ &= \sum \pi^{\epsilon_{p-v-i+1}+\ldots+\epsilon_{p-v}-m_i} x_i e_{v+i}\end{aligned}$$

Now, by Lemma 1.3.2, $\epsilon_j = \epsilon_{p+1-j}$ for all j with $2 \leq j \leq p-1$. Hence we get

$$\begin{aligned}\theta e_v &= \sum \pi^{\epsilon_{v+i}+\ldots+\epsilon_{v+1}-m_i} x_i e_{v+i} \\ &= \sum_{i<i_0} \pi^{\epsilon_{v+i}+\ldots+\epsilon_{v+1}-m_i} x_i e_{v+i} + x_{i_0} e_{v+i_0}\end{aligned}$$

Since the e_j, $1 \leq j \leq p$, form an A-basis for B, we deduce $x_{i_0} \in A$. By (2.6), we know $x_{i_0} f_{i_0} \in R$; thus we can reproduce the same argument for $\theta - x_{i_0} f_{i_0}$ and eventually conclude $x_i \in A$ for all i.

Finally, let us show that we can assume $i_0 \neq 0, p-1$. If $i_0 = 0$, then $\theta = x_0$, which is obviously in R if and only if $x_0 \in A$; on the other hand, if $i_0 = p-1$, then

$$\begin{aligned}\theta e_1 &= \sum_{i<p-1} x_i f_i e_1 + x_{p-1} f_{p-1} e_1 \\ &= \sum_{i<p-1} x_i f_i e_1 + x_{p-1} e_p\end{aligned}$$

This implies $x_{p-1} \in A$ and for $\theta' := \theta - x_{p-1} f_{p-1}$ we have $i_0 < p-1$.

The proof is now complete.

□

Provided that $p \nmid t$ if $\mathrm{char} K = 0$, we have obtained that $\mathcal{R}$ is an A-basis for R both if the characteristic of K is 0 and p (see [6, Prop. 3]). Again, the same remark we made for B holds: when passing to the characteristic 0 case, we lose the grading on R.

We are now going to investigate the structure of the associated order R as a ring.

Chapter 3

The structure of the associated order as a ring

We consider the same setting as at the beginning of Chapter 2. Besides the notation already introduced, we shall denote by $\mathfrak{p}$ the maximal ideal of A and by $\bar{K} = A/\mathfrak{p}$ the residue field of A.

In [6, Theorem 4], De Smit and Thomas find the minimal number of R-module generators for B, in the equal characteristic environment in which they work. The proof of this theorem exploits the fact that the associated order R is a local ring (see [15, Prop. 5.10]).

Our goal now is to prove an analogous result, in the unequal characteristic framework. It is then natural to wonder whether R is local in this case too. We will find out that it is local if and only if the extension L/K is not almost maximally ramified, which will make possible, at least under this assumption, to generalize in a way the results holding when char$K = p$.

We recall that the extension L/K is said to be almost maximally ramified (a.m.r.) when the unique ramification jump t satisfies

$$\frac{ap}{p-1} - 1 \leq t \leq \frac{ap}{p-1}, \tag{3.1}$$

with $a := v_K(p)$ the absolute ramification index of the extension.

3.1 Is R a local ring?

Theorem 3.1.1. *The associated order R is a local ring if and only if the extension L/K is not a.m.r..*

Different strategies will be applied to prove the two directions of the equivalence: the non-localness of R when L/K is a.m.r. will follow from the existence of nontrivial idempotents in R, which will make of R a disconnected

ring; on the other hand, when the extension is not a.m.r., we will exploit the basis for R as an A-module, which we have previously determined, and conclude that R is local as all its A-module generators, except $f_0 = 1$, are topologically nilpotent.

The following lemmas contribute to the proof of Theorem 3.1.1.

Lemma 3.1.2. *Let*

$$e = \frac{1}{p} \sum_{i=0}^{p-1} \sigma^i$$

Then $e \in K[G]$ is idempotent, and R contains it if and only if (3.1) holds.

Proof. It is easy to check that e satisfies $e^2 = e$, namely that e is idempotent. Consider the usual A-basis for R:

$$\mathcal{R} = \left\{ f_i = \frac{(\sigma - 1)^i}{\pi^{ik+m_i}}, \text{ for } 0 \leq i \leq p-1 \right\}$$

Remark that $f_{p-1} = (\sigma - 1)^{p-1}/\pi^{n_{p-1}}$, where $n_{p-1} = (p-1)k + s$. Therefore e belongs to R if and only if the absolute ramification index $a = v_K(p)$ is at most n_{p-1}. This condition is equivalent to (3.1): indeed,

$$\begin{aligned} (3.1) &\iff ap \leq t(p-1) + p - 1 \iff ap \leq (pk + s + 1)(p-1) \\ &\iff a \leq k(p-1) + (s+1)(1 - 1/p) \\ &\iff a \leq k(p-1) + s = n_{p-1}. \end{aligned}$$

□

Remark 3.1.3. In fact, the condition $a \leq n_{p-1}$ implies $a = n_{p-1} = k(p-1)+s$; indeed, as $ap \geq (p-1)t$ (Proposition 1.2.3), we also have

$$a \geq (p-1)k + (p-1)s/p \Longrightarrow a \geq (p-1)k + s;$$

hence we have $a = k(p-1) + s$ if and only if L/K is a.m.r..

Our next step consists in establishing a link between the existence of non-trivial idempotents in a ring and the connectedness of its spectrum (for this topic, we refer the reader to [7, p. 54, 85]). Let us remind few definitions.

Definition 3.1.4. *Let R be a commutative ring with identity (as we will always assume here). The spectrum of R, denoted $Spec(R)$, is the set of all prime ideals of R. Moreover, for any ideal I of R, we define*

$$Z(I) := \{\textit{prime ideals of } R \textit{ containing } I\}.$$

It is well-known that $Spec(R)$ can be given a topological structure, whose closed sets are the $Z(I)$, for I ideal of R. This topology is called the Zariski topology.

Definition 3.1.5. *A ring R is said to be disconnected if its spectrum $Spec(R)$ is disconnected with respect to the Zariski topology.*

These items are enough to prove the following

Lemma 3.1.6. *If a ring R contains a nontrivial idempotent, then R is disconnected. Furthermore, R is not local.*

Remark 3.1.7. The reverse implication of the first statement in Lemma 3.1.6 is true as well. Nevertheless, it is a result we will not need.

Proof. Let $e \in R$ be such that $e \neq 0, 1$ and $e^2 = e$. Of course, $1 - e \in R$ has these properties too. Set then

$$\begin{aligned} X_1 &= \{\text{prime ideals of } R \text{ containing } e\} \\ X_2 &= \{\text{prime ideals of } R \text{ containing } 1 - e\} \end{aligned}$$

We claim that, for $i = 1, 2$, we have $X_i \neq \varnothing, X_i \neq Spec(R)$ and $Spec(R)$ is the disjoint union of the X_i.

It is clear that the sets X_1 and X_2 are disjoint, since an ideal containing both e and $1-e$ coincides with the whole ring R, which is not a prime ideal, by definition. Further, both X_1 and X_2 are nonempty: by Zorn's Lemma, every ideal is contained in a maximal ideal; so the maximal ideal containing Re (respectively $R(1-e)$) is an element of X_1 (resp. X_2).

It remains to show that the union of X_1 and X_2 gives the entire spectrum of R. For this, take a prime ideal P of R. Since $0 = e(1 - e)$ is in P, either e or $1 - e$ must be in P by definition of prime ideal. This gives $Spec(R) = X_1 \bigsqcup X_2$.

The last assertion is then trivial. □

Lemmas 3.1.2 and 3.1.6 prove one direction of the equivalence announced in Theorem 3.1.1. The following definitions and intermediate results aim to prove the remaining implication.

Definition 3.1.8. *Let R be a topological ring. An element $x \in R$ is said to be topologically nilpotent if the sequence $(x^n)_{n\geq 0}$ converges to 0.*

We shall now introduce a topology on the associated order R.

In general, if I is an ideal of a commutative ring A and M is an A-module, one can equip M with a topology, called I-adic, such that a basis for the open

sets is given by the $m + I^n M$, for $m \in M$ and $n \geq 0$ (see [2, Chapter X]).

In our setting, we take $I = \mathfrak{p}$, the maximal ideal of A; we equip the A-module R with the $\mathfrak{p}$-adic topology. We remark that R is complete with respect to this topology, since it is finitely-generated as an A-module and A is noetherian (see [2, X, Prop. 10.13]).

Lemma 3.1.9. *If $f_i \in \mathcal{R}$ is topologically nilpotent for $1 \leq i \leq p-1$, then R is a local ring.*

Proof. Suppose $f_i^n \longrightarrow 0$ as $n \longrightarrow \infty$. By definition, this means that for all positive integer N, there exists $n_0 > 0$ such that $f_i^n \in \mathfrak{p}^N R$ for all $n > n_0$. As it is easy to see, this is equivalent to say that the power series $\sum_{n=0}^{\infty} f_i^n$ converges. We now have

$$(\sum_{n=0}^{\infty} f_i^n)(1 - f_i) = 1,$$

from which we deduce $1 - f_i \in R^\times$ (here $R^\times$ denotes the set of units of R). Analogously, for any $r \in R$ we get $1 - r f_i \in R^\times$.

We claim that f_i belongs to all maximal ideals of R. Suppose there exists a maximal ideal M of R such that $f_i \notin M$. Hence $R = M + Rf_i$, and $m = 1 - r f_i$ for some $m \in M$ and $r \in R$. This is not possible since $1 - r f_i$ is a unit. Therefore, for all $i \in \{1, \ldots, p-1\}$, for all maximal ideal $M \subset R$, we have $Af_i \subset M$.

Since $R = \oplus_{i=0}^{p-1} Af_i$ and A local, it turns out that R admits a unique maximal ideal

$$\mathfrak{m} := \mathfrak{p} \oplus Af_1 \oplus \ldots \oplus Af_{p-1};$$

thus R is a local ring. □

It remains to verify that the assumption of Lemma 3.1.10 holds when the extension L/K is not a.m.r.; this is accomplished by the next lemma.

Lemma 3.1.10. *When the extension L/K is not almost maximally ramified, for $0 < i < p$, the generators f_i of the A-module R are topologically nilpotent.*

Proof. Let $x \in L$ be our favorite element of valuation $v_L(x) = -t(p-1)$. We are going to show that, under (3.1),

$$v_L(f_i^n x) \longrightarrow \infty, \quad \text{as } n \longrightarrow \infty.$$

First, we are interested in determining the valuation $v_L((\sigma - 1)^m x)$ for any positive integer m. This has already been done, in Lemma 2.3.1, for $0 \leq m \leq$

$p-1$ and for $p \leq m \leq 2(p-1)$, and these two cases were treated distinctly.

To extend this result, a similar argument will be useful: set $z = \sigma - 1$; therefore $(z+1)^p = 1$, which yields

$$z^p = -pz(1 + n_1 z + \ldots + n_{p-3} z^{p-3} + z_{p-2}), \tag{3.2}$$

where each n_i is a positive integer. Now, let us raise both sides of (3.2) to the n-th power, for $n \in \mathbb{Z}_{\geq 2}$:

$$\begin{aligned} & z^{np} &=& (-p)^n z^n (1 + n_1 z + \ldots + n_{p-3} z^{p-3} + z_{p-2})^n \\ \Longrightarrow \quad & z^{np-n+1} &=& (-p)^n z (1 + n_1 z + \ldots + n_{p-3} z^{p-3} + z_{p-2})^n \end{aligned}$$

Note this passage is allowed since $K[G] = K[\sigma]/(\sigma^p - 1)$ is a reduced ring. Then

$$v_L(z^{np-n+1}x) = nap + v_L(zx) = nap - t(p-1) + t,$$

which implies, for $j \in \{0, \ldots, p-2\}$

$$\begin{aligned} v_L(z^{np-n+1+j}x) &= nap + v_L(z^{j+1}x) \\ &= nap - t(p-1) + (j+1)t \end{aligned}$$

Remark that for $j = p-2$ we have $v_L(z^{np-n+1+j}x) \equiv 0$ modulo p.

So for any positive integer m, if j is the unique integer verifying $(j-1)(p-1) < m \leq j(p-1)$, we get

$$v_L(z^m x) = (j-1)ap - (j(p-1) - m)t$$

Suppose now $i \in \{1, \ldots, p-1\}$ and $n \in \mathbb{Z}_{\geq 0}$; let $l \in \mathbb{Z}$ be such that $(l-1)(p-1) < in \leq l(p-1)$. Then

$$\begin{aligned} v_L(f_i^n x) &= v_L\Big(\frac{z^{in}}{\pi^{n(ik+m_i)}} x\Big) \\ &= (l-1)ap - (l(p-1) - in)t - pn(ik + m_i) \\ &= l(ap - (p-1)t) + n(is - pm_i) - ap \\ &\geq in\Big(\frac{ap}{p-1} - t + s - p\frac{m_i}{i}\Big) + \alpha, \qquad \text{as } l \geq in/(p-1), \end{aligned}$$

with α a quantity independent of n. Now, the extension L/K is a.m.r. if and only if $ap = (p-1)t + s$ (see Remark 3.1.3); otherwise, $ap \geq (p-1)t + p + s$. Thus, in this latter case,

$$\begin{aligned} v_L(f_i^n x) &\geq in\Big(\frac{p+s}{p-1} + s - p\frac{m_i}{i}\Big) + \alpha \\ &= inp\Big(\frac{s+1}{p-1} - \frac{m_i}{i}\Big) + \alpha. \end{aligned}$$

We wonder whether

$$\frac{s}{p-1} - \frac{m_i}{i} \geq 0, \tag{3.3}$$

or equivalently, if $is \geq (p-1)m_i$. This is true, and it can be seen combinatorially: view is as the number of ϵ_i equal to 1 in the string

$$S' : \quad \underbrace{\epsilon_1, \ldots, \epsilon_{p-1}}_{1}, \underbrace{\epsilon_1, \ldots, \epsilon_{p-1}}_{2}, \ldots, \underbrace{\epsilon_1, \ldots, \epsilon_{p-1}}_{\text{i}}$$

Then reread S' as made of $p-1$ substrings of length i: such substrings can be either of the shape $\epsilon_{n+1}, \ldots, \epsilon_{n+i}$ with $0 \leq n \leq p-1-i$, or of the shape $\epsilon_r, \ldots, \epsilon_{p-1}, \epsilon_1, \ldots, \epsilon_s$, with $s+p-r=i$. In the first case, the weight of the substring is at least m_i, where by weight of a string we mean the sum of its terms. In the second case, by Lemma 1.3.2,

$$\begin{aligned} \epsilon_r + \ldots \epsilon_{p-1} + \epsilon_1 + \ldots + \epsilon_s &= a_s + \epsilon_2 + \ldots + \epsilon_{p+1-r} \\ = a_s + a_{p+1-r} - 1 &\geq a_s + \epsilon_{s+1} + \ldots + \epsilon_{i+1} - 1 \\ = a_{i+1} - 1 &= \epsilon_2 + \ldots + \epsilon_{i+1} \geq m_i \end{aligned}$$

This explains (3.3). Therefore, for all $i \in \{1, \ldots, p-1\}$

$$v_L(f_i^n x) \geq in + \alpha \longrightarrow \infty, \quad \text{as } n \longrightarrow \infty,$$

which proves the lemma. □

The four lemmas build the proof of Theorem 3.1.1. We can finally remark that in the a.m.r. case, we would have,

$$v_L(f_i^n x) = inp\Big(\frac{s}{p-1} - \frac{m_i}{i}\Big) + \alpha,$$

and, in particular, $v_L(f_{p-1}^n x) = \alpha$ does not tend to infinity.

3.2 When R is not local, first part: p does not divide t

In this section and in the next one, we would like to discuss the ring R, in the almost maximally ramified case, when we know it is not local. In particular we shall say something more about the maximal ideals of R and the structure of the $A/\mathfrak{p}$-algebra $R/J(R)$, where $J(R)$ denotes the Jacobson radical of R (that is the intersection of all its maximal ideals).

Throughout this section, assume the extension L/K is almost maximally ramified, but not maximally ramified, i.e. $t \neq ap/(p-1)$, or equivalently, p does not divide t. Hence $s \neq 0$.

We just remarked that in this case at least two elements of the A-basis of R, namely f_0 and f_{p-1}, turn out not to be topologically nilpotent. We wonder if, and in which case, f_0 and f_{p-1} are the only such elements. The answer is given in Proposition 3.2.2, which is preceded by a combinatorial lemma.

Lemma 3.2.1. *If s does not divide $p-1$, then the identity*

$$\frac{s}{p-1} = \frac{m_i}{i} \tag{3.4}$$

occurs only at $i = p-1$.

Proof. In Lemma 3.1.10, we saw that $is \geq (p-1)m_i$ for any i with $0 < i < p$. If $gcd(s, p-1) = 1$, of course (3.4) cannot be achieved except at $p-1$. Suppose then $1 < g := gcd(s, p-1) < s$ and write

$$\frac{s}{p-1} = \frac{r}{q} \quad \text{with } r = \frac{s}{g},\ q = \frac{p-1}{g}$$

We shall exclude (3.4) for $i \in \{q, 2q, \ldots, (g-1)q\}$.

Assume that (3.4) does not hold for $i = q$, i.e. $s/(p-1) > m_q/q$; hence $r/q > m_q/q$ and $m_q < r$. This would suffice if $g = 2$, so suppose $g \geq 3$.

Consider a substring of (ϵ), say $\epsilon_{j+1}, \ldots, \epsilon_{j+q}$, with $1 < j < p-q$, summing to $m_q < r$. If $j + 2q < p$, consider $\epsilon_{j+1}, \ldots, \epsilon_{j+q}, \epsilon_{j+q+1}, \ldots \epsilon_{j+2q}$ (otherwise take $\epsilon_{j-(q-1)}, \ldots, \epsilon_j, \epsilon_{j+1}, \ldots, \epsilon_{j+q}$). We have

$$\epsilon_{j+1} + \ldots + \epsilon_{j+2q} \leq m_q + a_q < r + r = 2r.$$

This implies that $m_{2q} < 2r$ and $m_{2q}/2q \lneq r/q = s/(p-1)$. We can iterate this argument and conclude that if (3.4) does not hold at $i = q$ then $m_{tq}/tq < s/(p-1)$ for all $t \in \{2, \ldots, g-1\}$.

Therefore it remains to prove that the assumption about q is true. Remark that, if we prove $a_q \neq m_q$, then $s/(p-1) > m_q/q$ will follow. Indeed, $a_q \neq m_q$ yields

$$\begin{aligned} qs &= \text{number of 1s occurring in } \epsilon_1, \ldots, \epsilon_{p-1} \text{ repeated } q \text{ times} \\ &\geq a_q + (p-2)m_q > m_q + (p-2)m_q = (p-1)m_q \end{aligned}$$

(this is obtained by applying the same argument used to show $is \leq (p-1)m_i$, see (3.3)). By Lemma 1.3.3, $a_q = m_q$ if and only if q is a sub-period for (ϵ).

On the other hand, by Proposition 1.3.4, $p-1$ is a minimal sub-period for the sequence (ϵ) associated to s/p, i.e. no proper divisor of $p-1$ is a sub-period. So $a_q \neq m_q$.

Another argument can be given to prove $a_q \neq m_q$, without using Proposition 1.3.4. Assume first $s < (p-1)/2$; then (ϵ) associated to s is made up of words $1, 0, \ldots, 0$ of either length $\lfloor \frac{p-1}{s} \rfloor$ ("short words") or $\lceil \frac{p-1}{s} \rceil$ ("long words").

Two remarks build up the proof. The first one: by definition of a_i and ϵ_i, one can see that the longest block of sequential short words in (ϵ) is at the beginning of the sequence; secondly, if q, that divides $p-1$, is a sub-period, then (ϵ) is obtained by repeating g times the word $W := \epsilon_1, \ldots, \epsilon_q$. In particular $\epsilon_{p-q}, \ldots, \epsilon_{p-1} = W$. By Lemma 1.3.2, this implies that $\epsilon_1, \epsilon_2 \ldots, \epsilon_{q+1}$ is itself palindrome, hence it starts and terminates with the longest block of sequential short words. This yields a contradiction: by repeating W, a longer block of sequential short words than the one opening the sequence (ϵ) will appear.

If instead $s > (p-1)/2$, consider $s' < (p-1)/2$ such that $s = p - s'$; then, if (ϵ) is associated to s and (ϵ') to s', we have

$$\epsilon_i = \begin{cases} \epsilon'_i = 1 & \text{if } i = 1, \\ 1 - \epsilon'_i & \text{otherwise.} \end{cases}$$

So q dividing $p-1$ cannot be a sub-period: indeed the longest string of sequential ones in (ϵ) is at the beginning of the sequence; if (ϵ) is a repetition of the word W defined as before, with W, ϵ_{q+1} palindrome, then we can find a longer sequence of ones than at the beginning.

We conclude that $m_q/q < s/(p-1)$ for all $i \in \{q, 2q, \ldots, (g-1)q\}$, and (3.4) only holds for $i = p-1$. □

It is now easy to prove the following

Proposition 3.2.2. *If s does not divide $p-1$, then f_i is topologically nilpotent if and only if $0 < i < p-1$.*

Assume instead s divides $p-1$, let $q = (p-1)/s$; then $f_{jq} = f_q^j$ is not topologically nilpotent, for $j \in \{0, 1, \ldots, s\}$.

Proof. Let $n \geq 1$ and $i \geq 1$. In the proof of Lemma 3.1.10, we computed $v_L(f_i^n x)$ and in the a.m.r. case we got

$$v_L(f_i^n x) = inp\Big(\frac{s}{p-1} - \frac{m_i}{i}\Big) + \alpha,$$

where α is a quantity that does not depend on n. Then, f_{p-1} is not topologically nilpotent, as $s/(p-1) = m_{p-1}/(p-1)$, and f_0, f_{p-1} are the only element with this property, by Lemma 3.2.1.

On the other hand, if s does divide $p-1$, then $q = (p-1)/s$ and $\{q, 2q, \ldots, sq = p-1\}$ is the set of sub-periods of (ϵ): indeed, (ϵ) is obtained by repeating s times the string $1, 0, \ldots, 0$, of length q.

This yields that the non-nilpotent elements of R in the almost maximally ramified case are $\{f_q, f_{2q}, \ldots, f_{sq}\}$. Moreover, if we let $z = \sigma - 1$, for $0 < j < s+1$,

$$\begin{aligned} f_{jq} &= \frac{z^{jq}}{\pi^{jqk+m_{jq}}} = \frac{z^{jq}}{\pi^{jqk+a_{jq}}} \\ &= \frac{z^{jq}}{\pi^{jqk+j}} = \frac{z^{jq}}{\pi^{jqk+ja_q}} = \frac{z^{jq}}{\pi^{jqk+jm_q}} \\ &= f_q^j. \end{aligned}$$

This completes the proof. □

Our next goal consists in determining the structure of $R/J(R)$ as a $\bar{K}$-algebra, with $\bar{K}$ residue field of A. In particular, we are going to prove the following

Theorem 3.2.3. *We have isomorphisms of $\bar{K}$-algebras:*

$$R/J(R) \simeq \begin{cases} \bar{K} & \text{if } L/K \text{ is not a.m.r.,} \\ \bar{K}[X]/(X^2 - \alpha X) & \text{if } L/K \text{ is a.m.r., } s \nmid p-1 \text{ and } s \neq 0, \\ \bar{K}[X]/(X^{s+1} - \alpha X) & \text{if } L/K \text{ is a.m.r. and } s|p-1 \text{ and } s \neq 0, \end{cases} \quad (3.5)$$

where $\alpha = -p/\pi^{(p-1)k+s} \in \bar{K}$.

Proof. Remark that the first case of (3.5) has already been proved: if the extension L/K is not a.m.r., then $\mathfrak{p} + Af_1 + \ldots + Af_{p-1}$ is the only maximal ideal of R and obviously $R/J(R) = \bar{K}$.

Let us start discussing the case in which L/K is a.m.r. and s does not divide $p-1$. By Proposition 3.2.2, if $f_i \notin J(R)$, then $i \in \{0, p-1\}$. Hence R has at most two maximal ideals; since R is not local (see Lemmas 3.1.2 and 3.1.6), we conclude that it has exactly two maximal ideals, and in particular, for the Jacobson radical $J(R)$ we have

$$J(R) \supseteq \mathfrak{p} \oplus Af_1 \oplus \ldots \oplus Af_{p-2} \oplus \mathfrak{p}f_{p-1}. \quad (3.6)$$

Since $R/J(R)$ has dimension at least 2 as a $\bar{K}$-vector space, (3.6) is actually an equality, and

$$R/J(R) = \bar{K} \oplus \bar{K}f_{p-1}.$$

We shall investigate the behavior of f_{p-1} in $R/J(R)$; the following computation will lead to the definition of the constant α appearing in the statement. Let us recall that we can write

$$z^p = -pz(1 + n_1 z + \dots n_{p-3} z^{p-3} + z^{p-2}),$$

where the n_i are positive integers; to simplify notation, put

$$\gamma(z) := 1 + n_1 z + \dots n_{p-3} z^{p-3} + z^{p-2}; \tag{3.7}$$

further, we will use the fact that the absolute ramification index $v_K(p)$ of the extension is equal to $(p-1)k + s$ if and only if L/K is a.m.r. (see Remark 3.1.3). We have

$$\begin{aligned} f_{p-1}^2 &= \frac{z^{2p-2}}{\pi^{2(p-1)k+2s}} = \frac{-p}{\pi^{(p-1)k+s}} \frac{z^{p-1}}{\pi^{(p-1)k+s}} \gamma(z) \\ &= \frac{-p}{\pi^{(p-1)k+s}} f_{p-1} \gamma(z); \end{aligned}$$

Set now $\alpha := \frac{-p}{\pi^{(p-1)k+s}}$; note that $\alpha \neq 0$ in $\bar{K}$. Hence

$$f_{p-1}^2 = \alpha f_{p-1} + f$$

where $f := \alpha(\gamma(z) - 1) f_{p-1}$.

Now, if $p \neq 2$, then $f \in J(R)$: indeed $\gamma(z) - 1$ is a polynomial in z with zero constant term and $z = \pi^{k+m_1} f_1$ is in $J(R)$; moreover, as an ideal of R, the Jacobson radical is closed under multiplication by f_{p-1}. If instead $p = 2$, then we could have $z \notin J(R)$, if $z = f_1 = f_{p-1}$. Nevertheless, our assumptions exclude $p = 2$, since in this case the only possible values of s are 0 and $1 = p - 1$.

It follows that

$$\begin{aligned} \bar{K}[X]/(X^2 - \alpha X) &\longrightarrow R/J(R) = \bar{K} \oplus \bar{K} f_{p-1} \\ X &\longmapsto f_{p-1} \end{aligned}$$

is an isomorphism of $\bar{K}$-algebras, which completes the first part of (3.5).

Assume now L/K is a.m.r. and $s|p-1$; let $q = (p-1)/s$. By Proposition 3.2.2, if $f_i \notin J(R)$, then i must be a multiple of q. Let $\mathfrak{m}$ be a maximal ideal of R. Since $f_{jq} = f_q^j$ for $j \in \{1, \dots, s\}$, it turns out that f_{p-1} belongs to $\mathfrak{m}$ if and only if f_q^j does, for all j. Hence, if we put

$$I := \Big(\bigoplus_{\substack{0 \leq i \leq p-1 \\ q \nmid i}} A f_i \Big) \oplus \Big(\bigoplus_{\substack{0 \leq i \leq p-1 \\ q | i}} \mathfrak{p} f_i \Big).$$

we get $J(R) \supseteq I$. Let us look at

$$f_q^{s+1} = \frac{z^{(s+1)q}}{\pi^{(s+1)qk+(s+1)m_q}};$$

as $sq = p-1$ and $m_q = 1$,

$$\begin{aligned} f_q^{s+1} &= \frac{1}{\pi^{(p-1)k+s}} \frac{z^{p-1+q}}{\pi^{qk+m_q}} = \frac{-p}{\pi^{(p-1)k+s}} \frac{z^q}{\pi^{qk+m_q}} \gamma(z) \\ &= \alpha f_q \gamma(z) = \alpha f_q + h, \end{aligned} \tag{3.8}$$

where $h := \alpha(\gamma(z) - 1) f_q$.

Now, if $q \neq 1$, then h is in I as $\gamma(z) - 1$ is a polynomial in z with zero constant term and $z \in I$. If $q = 1$, then $s = p - 1$, which yields $m_1 = 1$, so that $z f_q = \pi^{k+1} f_1 f_q$ is in $\mathfrak{p}R \subseteq I$. In all cases, we conclude

$$f_q^{s+1} - \alpha f_q = 0 \quad \text{in } R/I$$

Hence we get an isomorphism of $\bar{K}$-algebras:

$$\begin{aligned} \bar{K}[X]/(X^{s+1} - \alpha X) &\longrightarrow R/I \\ X &\longmapsto f_q \end{aligned} \tag{3.9}$$

Note that, since $\alpha \neq 0$ and $p \nmid s$, the polynomial $X^{s+1} - \alpha X \in \bar{K}[X]$ is separable; so the ring $\bar{K}[X]/(X^{s+1} - \alpha X)$ is reduced and its Jacobson radical is trivial. From (3.9), it follows that $J(R/I) = 0$, which implies

$$I = \bigcap_{\substack{\mathfrak{m} \text{ max. ideal of } R \\ \mathfrak{m} \supseteq I}} \mathfrak{m} \quad \supseteq \bigcap_{\mathfrak{m} \text{ max. ideal of } R} \mathfrak{m} \quad = J(R)$$

Finally, $I = J(R)$ and (3.9) is the isomorphism announced. □

Remark 3.2.4. The isomorphisms proved in the previous theorem have the following important consequences. When $s \nmid p - 1$, the factorization of the polynomial $X^2 - \alpha X = X(X - \alpha)$ determines the two maximal ideals $\mathfrak{m}_1$, $\mathfrak{m}_2$ of R:

$$\begin{aligned} \mathfrak{m}_1 &= \mathfrak{p} \oplus A f_1 \oplus \ldots \oplus A f_{p-1} \\ \mathfrak{m}_2 &= \mathfrak{p} \oplus A f_1 \oplus \ldots \oplus A(f_{p-1} - \alpha) \end{aligned}$$

Likewise, when $s|p-1$, the maximal ideals are determined by the factorization of $X^{s+1} - \alpha X$ in $\bar{K}[X]$.

3.3 When R is not local, second part: p divides t

So far we have discussed the case in which p does not divide t. We shall now assume that p does divide t and describe the associated order R in this case.

By Proposition 1.2.4, we know that $p|t$ if and only if $t = ap/(p-1)$, i.e. L/K is maximally ramified. Moreover, in this case K contains the p-th roots of unity and there exist uniformizers π, ω of K and L respectively such that

$$L = K[\omega], \qquad \omega^p = \pi. \tag{3.10}$$

Let us rewrite (3.10) as $L = \bigoplus_{i=0}^{p-1} K\omega^i$. With respect to the K-basis $1, \omega, \ldots, \omega^{p-1}$ of L, the Galois group G acts diagonally on L: if $G = \langle\sigma\rangle$, with σ defined by $\sigma(\omega) = \zeta_p\omega$ and $\zeta_p \in K$ a p-th root of unity, the action of σ^i on any $y \in L$ is described by a diagonal $p \times p$-matrix. Hence via the isomorphism

$$\psi : End_K L \longrightarrow M_p(K),$$

where $M_p(K)$ is the ring of $p \times p$-matrices with coefficients in K, the group ring $K[G] \subset End_K L$ is mapped injectively to the subring of diagonal matrices $D_p(K) = K \times \ldots \times K = K^p \subset M_p(K)$. In fact, as it is easy to check, ψ induces an isomorphism

$$\psi_{|K[G]} : K[G] \longrightarrow K^p; \tag{3.11}$$

further, $A[G] \subset K[G]$ is mapped injectively via ψ to $A \times \ldots \times A = A^p$; now, A is the maximal A-order in K since it is integrally closed in K (see [13, Theorem 8.6]); hence it follows that A^p is an A-order in K^p and it is maximal.

As $A[G] \subset R \subset K[G]$, the image via ψ of R in K^p is an A-order containing A^p. Therefore $R \simeq A^p$. We have proved the following

Lemma 3.3.1. *If L/K is a maximally ramified extension, the associated order R coincides with the maximal order in $K[G]$, and via ψ defined above, we have*

$$R \simeq A^p.$$

Chapter 4

The ring of integers as a module over its associated order

In the same setting and with the same notations given at the beginning of Chapter 2 and 3, we shall approach in this chapter some questions concerning the freeness of B as a module over its associated order. The arguments used will exploit the results previously achieved about the structure of R as a ring.

4.1 A first result about the freeness of B

As usual, we write $t = pk + s$, where t is the unique ramification jump of the extension L/K. Here we assume $0 < s < p$.

The description of B as an A-module given in chapter 2 already allows us to give a partial answer to the question concerning the freeness of B over its associated order.

Proposition 4.1.1. *If s divides $p-1$, then B is free as an R-module with generator e_1.*

Proof. Let $(\epsilon_i)_{0<i<p}$, $(a_i)_{0<i<p}$, $(m_i)_{0<i<p}$ be the combinatorial sequences defined in the first chapter, associated to s/p.

Assuming that s divides $p-1$, it is easy to see that

$$\epsilon_1, \ldots, \epsilon_{p-1} = 1, 0 \ldots, 0, 1, 0, \ldots, 0, \quad \ldots \quad 1, 0, \ldots, 0$$

where each string $1, 0, \ldots, 0$ has length $\frac{p-1}{s}$. In particular, if $i = l(p-1)/s$ for some integer $l \leq s$, then $\epsilon_i = 0$ (except for $s = p-1$, in which case $\epsilon_i = 1$ for all i); further $m_i = a_i = l$ and $\epsilon_{i+1} = 1$ for $l \neq s$.

We proved that $\{f_i = (\sigma-1)^i/\pi^{ik+m_i},\ 0 \leq i \leq p-1\}$ is an A-basis for the associated order R; we consider the first element of our A-basis of B, i.e. $e_1 = \pi^{k(p-1)+a_{p-1}}x$. We have

$$\begin{aligned} f_i e_1 &= \pi^{k(p-1)-ik+a_{p-1}-m_i}(\sigma-1)^i x \\ &= \pi^{a_{p-1}-a_{p-i-1}-m_i}\pi^{k(p-i-1)+a_{p-i-1}}(\sigma-1)^i x \\ &= \pi^{\epsilon_{p-1}+\epsilon_{p-2}+\ldots+\epsilon_{p-i}-m_i}e_{i+1} \end{aligned} \tag{4.1}$$

Now, by Lemma 1.3.2,

$$\epsilon_{p-1} + \ldots + \epsilon_{p-i} = \epsilon_2 + \ldots + \epsilon_{i+1}$$

If $\epsilon_{i+1} = 0$, then $\epsilon_2, \ldots, \epsilon_{i+1}$ is a string of length i whose sum equals $a_i - 1$; so we must have $m_i = a_i - 1 = \epsilon_2 + \ldots + \epsilon_{i+1}$. Otherwise, by the previous remark, i must be a multiple of $\frac{p-1}{s}$, in which case $\epsilon_2 + \ldots + \epsilon_{i+1} = a_i = m_i$.

Therefore, in any case, $f_i e_1 = e_{i+1}$ and e_1 generates B as an R-module. □

Now, one can wonder whether the converse is also true. It is precisely at this point that almost maximally ramified extensions intervene and require to be treated separately. Before clarifying this point, let us give a brief overview on the equal characteristic setting.

4.2 The main result about R-module generators for B, in the equal characteristic case

In this section we recall de Smit and Thomas' result about a minimal set of R-module generators for B, in the equal characteristic case. It seems convenient to include it here, as we are going to prove an analogous result in the unequal characteristic setup, for extensions which are not almost maximally ramified.

Throughout this section, assume K has characteristic p. The notation is the usual one.

Remark that, by [6, Prop. 2], the ring of integers B of L can be given the structure of a graded $A[G]$-submodule of L, whose homogeneous part of degree i is the free A-module of rank 1

$$B_i = \mathfrak{p}^{k(p-i)+a_{p-i}}(\sigma-1)^{i-1}w,$$

where w is a suitable element of valuation $v_L(w) = -t(p-1)$, obtained by Artin-Schreier theory.

The main result on the minimal number of generators for B as an R-module (Theorem 4 of [6]) is stated below. As usual, the sequences (a_i) and

(m_i) appearing in the statement are associated to s/p, with s remainder of the division of t by p.

Theorem 4.2.1. *Let*

$$\mathcal{D} = \{i : 1 \leq i \leq p \text{ and } a_j + m_{i-j} < a_i \text{ for all } j \text{ with } 0 < j < i\}; \quad (4.2)$$

let d be the minimal number of R-module generators of B.

Then we have $d = \#\mathcal{D}$ and a set of homogeneous elements in B forms a set of R-module generators of B if and only if for each i in $\mathcal{D}$ it contains an A-module generator of B_i, where B_i is the homogeneous part of degree i of B as an $A[G]$-module.

As already remarked, the proof exploits the fact that R is local.

4.3 A set of R-module generators for B, in the not almost maximally ramified case

From now on, assume K has characteristic 0. Further, in this section, L/K is supposed to be not almost maximally ramified; by Theorem 3.1.1, we know R is local in this case.

We want to determine the cardinality of a minimal set of R-module generators for B, similarly to what de Smit and Thomas achieved (Theorem 4.2.1 above). Since in the unequal characteristic case we are not allowed to talk about graded rings and homogeneous elements anymore, we need to rephrase and adapt their statement to our setting. What we are going to prove is the following

Theorem 4.3.1. *Suppose the extension L/K is not almost maximally ramified. Let d and $\mathcal{D}$ be defined as above. Let $\mathcal{B} = \{e_i, 1 \leq i \leq p\}$ be the usual basis for B as an A-module.*

Then $d = \#\mathcal{D}$ and a subset X of $\mathcal{B}$ forms a set of R-module generators of B if and only if for each i in $\mathcal{D}$, e_i is in X.

Proof. By Theorem 2.3.2, we know

$$R = A \oplus Af_1 \oplus \ldots \oplus Af_{p-1},$$

where, as usual, $f_i = \frac{(\sigma-1)^i}{\pi^{ik+m_i}}$ for $0 \leq i \leq p-1$. Under our assumption, R is a local ring whose maximal ideal is

$$\mathfrak{m} = \mathfrak{p} \oplus Af_1 \oplus \ldots \oplus Af_{p-1}.$$

In other words, if we put $f'_0 = \pi$, $f'_i = f_i$ for $1 \leq i \leq p-1$, the set $\mathcal{M} = \{f'_i, 0 \leq i \leq p-1\}$ is a set of A-module generators of $\mathfrak{m}$.

First, we claim that

$$\mathfrak{m}B = \bigoplus_{i=1}^{p} A^{(i)} e_i, \qquad \text{with } A^{(i)} = \begin{cases} \mathfrak{p} & \text{if } i \in \mathcal{D}, \\ A & \text{otherwise.} \end{cases} \tag{4.3}$$

For this, let us look at

$$B/\mathfrak{p}B = \bigoplus_{i=1}^{p} (A/\mathfrak{p}) e_i \supseteq \mathfrak{m}B/\mathfrak{p}B,$$

and consider the $f'_i e_j \in \mathfrak{m}B$, with $0 \leq i \leq p-1$ and $1 \leq j \leq p$. Suppose $i+j > p$: of course this occurs for values of i greater than 0, so we can simply write $f_i e_j$; say $i + j = p + l$, with $1 \leq l \leq p-1$. We have already computed $v_L(f_i e_j)$, which turned out to be

$$v_L(f_i e_j) = ap - (p-1)t + ls - p(m_i - a_{i-l})$$

(see (2.4)). As we are dealing with the not almost maximally ramified case, we must have $ap - (p-1)t = ph + s$ for some integer $h \geq 1$ (see Remark 3.1.3), so that

$$v_L(f_i e_j) = ph + (l+1)s - p(m_i - a_{i-l}) > ph \geq p$$

(indeed, $(l+1)s - p(m_i - a_{i-l})$ is positive: see (2.5)). This implies that $f_i e_j$ is in $\mathfrak{p}B$. Moreover, for all $j \in \{1, \ldots, p\}$, we have $f'_0 e_j = \pi e_j \in \mathfrak{p}B$.

Assume now $i + j \leq p$ and $i \geq 1$ (so again, let us simply write $f_i e_j$). By (2.3), in such case we get

$$f_i e_j = \pi^{a_{p-j} - m_i - a_{p-i-j}} e_{i+j} \in \{e_{i+j}, \pi e_{i+j}\}$$

Then Ae_l is contained in $\mathfrak{m}B$ if and only if l satisfies the following:

$$f_i e_j = e_l \text{ for some } i, j \text{ such that } i + j = l \text{ and } i \geq 1. \tag{4.4}$$

We find

$$\mathfrak{m}B/\mathfrak{p}B = \bigoplus_{\substack{1 \leq l \leq p, \\ l \text{ satisfies (4.4)}}} (A/\mathfrak{p}) e_l$$

It remains to translate this result in terms of the sequences (m_i), (a_i): consider then the condition $a_{p-j} - m_i - a_{p-i-j} = 0$ or, equivalently

$$a_{p-j} - m_{i-j} - a_{p-i} = 0 \text{ for } j < i. \tag{4.5}$$

By properties of the sequence (a_i), for $1 \leq i < j < p$ we have $a_i + a_{p-i} = s + 1 = a_j + a_{p-j}$ which allows us to rewrite (4.5) as

$$a_i - m_{i-j} - a_j = 0$$

Finally, with respect to the $A^{(i)}$ defined in (4.3), for $1 \leq i \leq p$, we have the following equivalences:

$$\begin{aligned} A^{(i)} = A &\Leftrightarrow a_j + m_{i-j} = a_i, \quad \forall j \text{ with } 1 \leq j < i \\ A^{(i)} = \mathfrak{p} &\Leftrightarrow a_j + m_{i-j} < a_i, \quad \forall j \text{ with } 1 \leq j < i, \end{aligned}$$

i.e. $A^{(i)} = \mathfrak{p}$ if and only if i is in $\mathcal{D}$, which proves (4.3).

To conclude, consider the quotient $B/\mathfrak{m}B$: by Nakayama's Lemma, a subset of B is a minimal set of generators for B as an R-module if and only if it generates $B/\mathfrak{m}B$ as a $\bar{K}$-vector space ($\bar{K} = A/\mathfrak{p}$) and its cardinality is equal to the $\bar{K}$-dimension of $B/\mathfrak{m}B$.

From

$$B/\mathfrak{m}B = (B/\mathfrak{p}B)/(\mathfrak{m}B/\mathfrak{p}B) = \bigoplus_{\substack{1 \leq i \leq p \\ i \in \mathcal{D}}} \bar{K} e_i,$$

we deduce that $\{e_i, i \in \mathcal{D}\}$ is a minimal set of R-module generators for B. $\square$

4.4 Freeness of B in the not almost maximally ramified case

At the beginning of this chapter, we posed the question of determining if or in which cases the converse of Proposition 4.1.1 holds as well. We deduce, from what we have just proved, that if the extension L/K is not a.m.r., we can conclude the same results about the structure of R and B, no matter if the characteristic of K is 0 or p.

Therefore, we have the following characterization of the extensions L/K for which the ring of integers B of L is free over its associated order; the proof is the same as the one given by De Smit and Thomas in their corollary to Theorem 4, in [6]. We include it here for convenience.

Theorem 4.4.1. *If the extension L/K is not a.m.r., then B is free over R if and only if s divides $p - 1$, where, as before, s is the residue of the ramification jump t modulo p.*

Proof. The "if" part is exactly what Proposition 4.1.1 consists of. So assume that B is R-free, i.e. $\mathcal{D} = \{1\}$. Suppose $0 < s < p$, which yields $m_1 = 0$, and call l the smallest integer $1 < l < p$, such that $m_l = 1$; then $a_i = 1$ for all $i < l$ since $1 \leq a_i \leq m_i + 1 = 1$. Further, for some $j < l$ we have $a_l = a_j + m_{l-j} = 1 = m_l$, as $l \notin \mathcal{D}$. Hence l is a subperiod of (ϵ) and by Lemma 1.3.3, we have that $\epsilon_1, \ldots, \epsilon_{p-1}$ is an s-fold repetition of a sequence $1, 0 \ldots 0$, which only occurs for s dividing $p - 1$. □

Further, all the combinatorial results holding in the equal characteristic case are still true in our unequal characteristic framework, if the extension is not a.m.r.. In particular, in both context we are provided with an easy procedure to compute the number $d = \#\mathcal{D}$ of R-generators for B, based on the continued fraction expansion of $-s/p$ (see [6, Theorem 3]).

4.5 Freeness of B in the maximally ramified case

Assume now L/K is maximally ramified: the ramification jump equals $ap/(p-1)$, where $a = v_K(p)$; further K contains the p-th roots of unity and there are uniformizers π, ω of K and L respectively such that $L = K[\omega]$ and $\omega = \pi^{1/p}$ (Proposition 1.2.4).

Theorem 4.5.1. *If p divides t, then B is a free R-module generated by $1 + \omega + \ldots + \omega^{p-1}$.*

Proof. By Lemma 3.3.1, the associated order R is isomorphic to the ring A^p of diagonal $p \times p$ matrices on the A-basis $\{1, \omega, \ldots, \omega^{p-1}\}$ of B. So the R-module B is identified with the A^p-module M spanned by all columns of matrices in A^p. As M is generated over A^p by the column vector $(1, \ldots, 1)^T$, we deduce that B is generated over R by $1 + \omega + \ldots + \omega^{p-1}$.

□

4.6 The almost maximally ramified case

In this last section, we are going to discuss the freeness of the R-module B in the almost maximally ramified case, assuming $s \neq 0$. Recall that, in this framework, the ring R is not local (Theorem 3.1.1), so we cannot apply the same strategies that were successful in the equal characteristic context of [6] and that we managed to reproduce here, provided that L/K is not a.m.r..

However, Theorem 3.2.3 gives a description of $R/J(R)$. Since the cases in which $s|p-1$ and $s=0$ are already solved (we know B to be free over R by Proposition 4.1.1 and by Theorem 4.5.1), we are only interested in the behavior of B over R when s does not divide $p-1$ and $s \neq 0$. In this case we know, by Theorem 3.2.3,

$$J(R) = \mathfrak{p} \oplus Af_1 \oplus \ldots \oplus Af_{p-2} \oplus \mathfrak{p}f_{p-1} \tag{4.6}$$

and

$$R/J(R) \simeq \bar{K}[X]/(X^2 - \alpha X) \simeq \bar{K} \oplus \bar{K}f_{p-1},$$

with $\alpha = -p/\pi^{(p-1)k+s} \in \bar{K}^\times$ (recall that in the a.m.r. case, $v_K(p) = (p-1)k + s$ by Remark 3.1.3).

Our purpose now is to state a combinatorial condition for B to be R-free and give generators. For $\mathcal{D}$ defined as in (4.2), let

$$\mathcal{D}' = \{1\} \cup \{l \in \mathcal{D} \setminus \{1\} : m_i - a_{i-l+1} < a_l - 1, \text{ for } l < i < p-1\}. \tag{4.7}$$

We are going to prove the following

Theorem 4.6.1. *Assume L/K is a.m.r., $s \nmid p-1$ and $s \neq 0$. Let d denote the minimal number of R-module generators of B. Then we have $d = \#\mathcal{D}' - 1$.*

The proof of Theorem 4.6.1 requires two intermediate results. Before stating them, set $z := \sigma - 1$ and

$$M := \bigoplus_{i \in \mathcal{D}'} \mathfrak{p}e_i \oplus \bigoplus_{i \in \{1,\ldots,p\} \setminus \mathcal{D}'} Ae_i. \tag{4.8}$$

Note that, in the next two lemmas, α is viewed as an element of A rather than as a class in $A/\mathfrak{p}$.

Lemma 4.6.2. *Assume L/K is a.m.r., $s \nmid p-1$ and $s \neq 0$. Let M as in (4.8). For any $i \in \{1, \ldots, p-1\}$ and $j \in \{2, \ldots, p\}$ with $i + j > p$, let $l \in \{2, \ldots, p\}$ be such that $i + j = p + l - 1$. Then*

$$f_i e_j \equiv \pi^\delta \alpha e_l \bmod M \cap J(R)B, \qquad \text{where } \delta = \begin{cases} 0 & \text{if } m_i - a_{i-l+1} = a_l - 1, \\ 1 & \text{if } m_i - a_{i-l+1} < a_l - 1. \end{cases}$$

Proof. We have $f_i = \frac{z^i}{\pi^{ik+m_i}}$ and $e_j = \pi^{(p-j)k+a_{p-j}} z^{j-1} x$. Let $\gamma(z)$ be defined as in (3.7). Therefore

$$\begin{aligned} f_i e_j &= \frac{z^{i+j-1}x}{\pi^{(i+j-p)k+m_i-a_{p-j}}} = \frac{z^{p+l-2}x}{\pi^{(l-1)k+m_i-a_{i-l+1}}} \qquad (4.9) \\ &= \frac{-p}{\pi^{(l-1)k+m_i-a_{i-l+1}}} z^{l-1}\gamma(z)x = \alpha \frac{\pi^{(p-1)k+s}}{\pi^{(l-1)k+m_i-a_{i-l+1}}} z^{l-1}\gamma(z)x \\ &= \alpha \frac{\pi^{(p-l)k+a_{p-l}}}{\pi^{m_i-a_{i-l+1}+a_{p-l}-s}} z^{l-1}\gamma(z)x \\ &= \frac{\alpha}{\pi^{m_i-a_{i-l+1}+a_{p-l}-s}} e_l + \frac{\alpha}{\pi^{m_i-a_{i-l+1}+a_{p-l}-s}} (\gamma(z)-1)e_l \end{aligned}$$

Now, set $\delta := -(m_i - a_{i-l+1} + a_{p-l} - s)$. In the proof of Theorem 2.3.2, (2.5), we remarked that

$$a_l - 2 \leq m_i - a_{i-l+1} \leq a_l - 1$$

Moreover, as it is easy to check, $a_l + a_{p-l} = s + 1$, whence

$$0 \leq \delta = -m_i + a_{i-l+1} - 1 + a_l \leq 1.$$

In particular, $\delta = 0$ if $m_i - a_{i-l+1} = a_l - 1$ and $\delta = 1$ if $m_i - a_{i-l+1} < a_l - 1$, as desired.

It remains to prove that $\eta := \pi^\delta \alpha(\gamma(z)-1)e_l$ is in $M \cap J(R)B$. Of course, this is true if $\delta = 1$, as both M and $J(R)B$ contain $\mathfrak{p}B$. Suppose then $\delta = 0$.

As $\gamma(z) - 1$ is a polynomial in $z = \pi^{k+m_1} f_1 = \pi^k f_1$ (note $m_1 = 1$ only at $s = p-1$) with zero constant term, and since f_1 is in the Jacobson radical (by assuming $s \neq 0$ and $s \nmid p-1$ we avoid the case $p = 2$), we must have $\eta \in J(R)B$.

To prove $\eta \in M$, it suffices to verify that $zB \subseteq M$. Clearly, if $k > 0$, the lemma holds, as $z = \pi^k f_1$ and $M \supset \mathfrak{p}B$. So assume $k = 0$.

Let $j \in \{1, \ldots, p-1\}$; we have $ze_j = f_1 e_j \in \{e_{j+1}, \pi e_{j+1}\}$ (see (2.3)). If $f_1 e_j = \pi e_{j+1}$, clearly $f_1 e_j \in M$; otherwise, $j+1 \notin \mathcal{D}$, hence $j+1 \notin \mathcal{D}'$ and, by definition of M, it follows $f_1 e_j \in M$.

Consider now $ze_p = f_1 e_p$; by computation (4.9) applied with $i = 1$ and $l = 2$, we get $ze_p = \alpha\pi^\delta \gamma(z) e_2$; let us assume $\delta = 0$. Note that $z^i e_2 = f_1(f_1^{i-1} e_2)$ lies in $\{f_1 e_{i+1}, \pi f_1 e_{i+1}, \ldots, \pi^{i-1} f_1 e_{i+1}\}$ for every $i = 0, \ldots, p-2$. Therefore $ze_p \in M$ follows as a consequence of the fact that $ze_j \in M$ for all j with $0 < j < p$. This shows that $\eta \in M$ and completes the proof. □

Lemma 4.6.3. *With the same assumptions and notations as in Lemma 4.6.2, we have $J(R)B = M$.*

Proof. Let us first check $J(R)B \subseteq M$. For this, we shall consider all products $f_i e_j$ with $f_i \in J(R)B$: by (4.6), we take $i \in \{1, \ldots, p-2\}$ and $j \in \{1, \ldots, p\}$.

Suppose first $i + j \leq p$; if $f_i e_j = \pi e_{i+j}$, then $f_i e_j \in M$ because $M \supset \mathfrak{p}B$; otherwise $f_i e_j = e_{i+j}$ and $f_i e_j \in M$ because $i + j \notin \mathcal{D}$.

Suppose now $i+j > p$ and let $l \in \{2, \ldots, p\}$ be such that $i+j = p+l-1$. By Lemma 4.6.2, we know

$$f_i e_j \equiv \pi^\delta \alpha e_l \bmod M$$

If $\delta = 1$, then $f_i e_j \in M$; otherwise we have $m_i - a_{i-l+1} = a_l - 1$, which implies $l \notin \mathcal{D}'$ and $e_l \in M$. This proves $f_i e_j \in M$, from which it follows $J(R)B \subseteq M$.

For the remaining inclusion, we shall verify that $e_l \in J(R)B$ for all $l \notin \mathcal{D}'$.

For $l \notin \mathcal{D}$, there must exist (i, j) with $1 \leq i, j < l$ and $i + j = l$ such that $f_i e_j = e_l$. If $l < p$, of course $i < p-1$. Then, let $l = p$; it is easy to check that $f_{p-1} e_1 = e_p$, so $p \notin \mathcal{D}$. We wonder whether e_p can also be obtained as $f_i e_j$ with $i < p-1$ and $j = p-i$. In fact, this is true provided that $m_i = a_{p-j} = a_i$ for some i with $1 < i < p-1$, or equivalently, there must exist a sub-period $i < p-1$ of (ϵ): as a consequence of Lemma 1.3.2, the index i corresponding to the zero preceding the last 1 of the sequence (ϵ) satisfies this property. So we indeed have

$$e_p \in J(R)B. \tag{4.10}$$

Finally, if $l \in \mathcal{D} \setminus \mathcal{D}'$, there exists i with $l < i < p-1$ and $m_i - a_{i-l+1} = a_l - 1$; set $j = p + l - i - 1$; hence, by Lemma 4.6.2

$$f_i e_j \equiv \alpha e_l \bmod J(R)B$$

Since $f_i e_j \in J(R)B$, we have $e_l \in J(R)B$. The lemma follows. □

Proof. (Theorem 4.6.1) The result achieved in Lemma 4.6.3 implies

$$B/J(R)B = \bigoplus_{i \in \mathcal{D}'} \bar{K} e_i.$$

We have that the minimal number n of generators for any module V over $R/J(R) = \bar{K}[X]/(X^2 - \alpha X) = \bar{K} \oplus \bar{K} f_{p-1}$ is

$$n = \max\left(\dim_{\bar{K}} \ker(\psi_1),\ \dim_{\bar{K}} \ker(\psi_2)\right),$$

where ψ_1, ψ_2 are the endomorphism of V defined by $\psi_1 : w \mapsto f_{p-1} w$ and $\psi_2 : w \mapsto (f_{p-1} - \alpha) w$. We shall compute n for $V = B/J(R)B$; remark that,

for this choice of V, Nakayama's Lemma implies $n = d$, with d as in the statement.

To compute n, first notice that $\mathcal{D}' \setminus \{1\} \neq \varnothing$: indeed, the $\bar{K}$-dimension of $B/J(R)B$ is at least 2, as $B/J(R)B$ is a module over $R/J(R) = \bar{K} \oplus \bar{K} f_{p-1}$.

Further, we see that f_{p-1} acts as multiplication by 0 on e_1 and as multiplication by α on $e_j \neq e_1$, in $B/J(R)B$. Indeed, we have $f_{p-1}e_1 = e_p$, which belongs to $J(R)B$, by (4.10); so $f_{p-1}e_1 = 0$ in $B/J(R)B$. On the other hand, (4.9) applied to $i = p-1$ and $j \in \{2, \dots, p\}$ gives

$$f_{p-1}e_j \equiv \pi^{\delta} \alpha e_j \bmod J(R)B \cap M = J(R)B,$$

where $\delta = -(m_{p-1} - a_{p-j} + a_{p-j} - s) = 0$ as $m_{p-1} = s$. So for $j \in \mathcal{D}' \setminus \{1\}$, we get $f_{p-1}e_j = \alpha e_j$ in $B/J(R)B$.

As a consequence, we find

$$\ker(\psi_1) = \bar{K} e_1, \qquad \ker(\psi_2) = \bigoplus_{i \in \mathcal{D}' \setminus \{1\}} \bar{K} e_i,$$

and

$$d = \max(1, \#\mathcal{D}' - 1) = \#\mathcal{D}' - 1,$$

as desired. □

We deduce a criterion for B to be free over R.

Corollary 4.6.4. *Assume L/K is a.m.r. and $s \neq 0$. Then B is free over its associated order if and only if $\#\mathcal{D}' \leq 2$.*

Proof. If s does not divide $p-1$, then B is free over R if and only if $\#\mathcal{D}' = 2$ by Theorem 4.6.1.

If $s | p-1$, we know B is R-free and $\mathcal{D} = \{1\} = \mathcal{D}'$ (indeed, B is generated by e_1 over R by Proposition 4.1.1). □

Remark 4.6.5. In [3, Theorem 1], Bertrandias, Bertrandias and Ferton give a criterion for B to be R-free in terms of the continued fraction expansion of s/p. In particular, they prove that, when the extension L/K is a.m.r., B is R-free if and only if the length of the continued fraction expansion of s/p is at most 4, where by length they mean the integer N such that

$$\frac{s}{p} = [0, x_1, \dots, x_N] := \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{\ddots \cfrac{}{x_{N-1} + \cfrac{1}{x_N}}}}}$$

It is easy to check that $N \leq 2$ if and only if $s|p-1$.

The combination of our result with theirs gives

Theorem 4.6.6. *For an a.m.r. extension L/K such that $s \neq 0$, the following are equivalent:*

i) B is free over R;

ii) the length of the continued fraction expansion of s/p is at most 4;

iii) $\#\mathcal{D}' \leq 2$.

Remark 4.6.7. Theorem 4.6.1 also permits to give explicit generators for B over R.

Suppose $\#\mathcal{D}' = 2$, say $\mathcal{D}' = \{1, j\}$, $1 < j < p$. Then $B/J(R)B$ is free over $R/J(R)$, generated by $e_1 + e_j$; indeed, any element $ae_1 + be_j \in B/J(R)B$ can be written as $(a + ((b-a)/\alpha)f_{p-1})(e_1 + e_j)$, with $(a + ((b-a)/\alpha)f_{p-1}) \in \bar{K} \oplus \bar{K}f_{p-1} = R/J(R)$. With Nakayama's Lemma, it follows that B is free over R, generated by $e_1 + e_j$.

More generally, as a consequence of Theorem 4.6.1, we can state

Theorem 4.6.8. *With the same assumptions as in Theorem 4.6.1, if $\mathcal{D}' = \{j_0 = 1, j_1, \ldots, j_d\}$, with $\{j_1, \ldots, j_d\} \subseteq \{2, \ldots, p-1\}$ all distinct, then $\{e_1 + e_{j_1}, e_{j_2}, \ldots, e_{j_d}\}$ is a set of R-module generators for B.*

Finally, one can see that the computation of the continued fraction expansion of s/p only gives a criterion for the R-freeness of B, but does not allow to compute the cardinality of a minimal set of generators. The example below underlines that, when the length N of the continued fraction expansion is larger than 4, the cardinality of $\mathcal{D}'$, and so d, is not apparently related to N. For a fixed p, we shall denote by N_s the length of the continued fraction expansion of s/p and by $\mathcal{D}'_s$, the set $\mathcal{D}'$ associated to s.

Example 4.6.9. Let $p = 29$.

1) Take $t = s = 8$ (remark that, if $t = s$, the extension L/K is a.m.r. with $a = t$); we have $s/p = [0, 3, 1, 1, 1, 2]$ and $\mathcal{D}'_8 = \{1, 4, 11\}$.

2) Take $t = s = 17$; then $s/p = [0, 1, 1, 2, 2, 2]$ and $\mathcal{D}'_{17} = \{1, 2, 7, 12\}$.

3) Take finally $t = s = 18$; we have $s/p = [0, 1, 1, 1, 1, 1, 3]$ and $\mathcal{D}'_{18} = \{1, 2, 5\}$.

Note that $N_8 = N_{17}$ but $\#\mathcal{D}'_8 \neq \#\mathcal{D}'_{17}$; on the contrary, $N_8 \neq N_{18}$ whereas $\#\mathcal{D}'_8 = \#\mathcal{D}'_{18}$.

We conclude with two questions, that remain open.

First, we still do not have a direct proof of the equivalence of the combinatorial conditions *ii)* and *iii)* in Theorem 4.6.6, which would give a new proof of Theorem 1 in [3].

Further, we wonder whether we can find an easy way to compute $\#\mathcal{D}'$: in the equal characteristic case, the cardinality of $\mathcal{D}$ can be easily computed in terms of the continued fraction expansion of $-s/p$ (see [6, Theorem 3]); in our context, we saw that, despite a criterion for the R-freeness of B can be given in terms of the length of the continued fraction expansion of s/p, this method cannot be extended to determine the minimal number d of R-module generators of B.

Bibliography

[1] A. Aiba, *Artin-Schreier extensions and Galois module structure*, J. Number Theory **102** (2003), 118–124.

[2] M.F. Atiyah, I.G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969.

[3] F. Bertrandias, J.-P. Bertrandias, M.-J. Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, C.R. Acad. Sc., Paris **274** (1972), 1388–1391.

[4] F. Bertrandias, M.-J. Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, C.R. Acad. Sc., Paris **274** (1972), 1330–1333.

[5] J.W.S. Cassels, A. Fröhlich, *Algebraic Number Theory*, Academic Press, 1967.

[6] B. de Smit, L. Thomas, *Local Galois module structure in positive characteristic and continued fractions*, Archiv der Mathematik **88** (2007), 207–219.

[7] D. Eisenbud, *Commutative algebra with a view towards algebraic geometry*, Springer-Verlag, 1995

[8] I.B. Fesenko, S.V. Vostokov, *Local Fields and Their Extensions*, Second Edition, AMS 2001.

[9] H. Jacobinski, *Über die Hauptordnung eines Körpers als Gruppenmodul*, J. Reine Angew. Math. **213** (1964), 151–164.

[10] H. Johnston, *Notes on Galois Modules*, Notes accompanying the course *Galois Modules* given in Cambridge in 2011.

[11] S. Lang, *Algebra*, Springer-Verlag, 2002.

[12] E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. reine angew. Math. **167** (1932), 147–152.

[13] I. Reiner, *Maximal Orders*, Clarendon Press, 2003.

[14] J.-P. Serre, *Local Fields*, Springer-Verlag, 1979.

[15] L. Thomas, *Arithmétique des extensions d'Artin-Schreier-Witt*, Ph.D. thesis, Université Toulouse 2 le Mirail, 2005.

[16] L. Thomas, *A valuation criterion for normal basis generators in equal positive characteristic*, Journal of Algebra **320** (2008), 3811–3820.

[17] L. Thomas, *On the Galois module structure of extensions of local fields*, Actes de la Conférence "Fonctions L et Arithmétique", Publ. Math. Besançon Algèbre Théorie Nr. (2010), 157–194.

Acknowledgements

Thanks to my thesis advisor, Bart de Smit, for his help and constant support.

Grazie ai miei e a Chiara, once again.

Grazie agli amici storici: Emilio e i miei compagni di Torino, le ragazze milanesi, Martina, Stefano, Francesco.

Grazie ad Andrea, per tutto.

Thanks to Natalia, for true friendship, wisest advice in all situations, and great time spent together.

Grazie a Jacopo, per la disponibilità all'ascolto e la compagnia. Grazie anche ad Andrea, per l'ospitalità e l'affetto.

A Dino.