ON THE GALOIS MODULE STRUCTURE OF EXTENSIONS OF LOCAL FIELDS

by

Lara Thomas

Abstract. — We present a survey of the theory of Galois module structure for extensions of local fields. Let L/K be a finite Galois extension of local fields, with Galois group G. We denote by $O_K \subset O_L$ the corresponding extension of valuation rings. The associated order of O_L is the full set, $\mathfrak{A}_{L/K}$, of all elements of $K[G]$ that induce endomorphisms on O_L. It is an O_K-order of $K[G]$ and the unique one over which O_L might be free as a module. When the extension is at most tamely ramified, the equality $\mathfrak{A}_{L/K} = O_K[G]$ holds, and O_L is $\mathfrak{A}_{L/K}$-free. But when ramification is permitted, the structure of O_L as an $\mathfrak{A}_{L/K}$-module is much more difficult to determine. Recent progress has been made on this subject and motivates an exposition of this theory.

Résumé. — Le sujet de cet article est la théorie des modules galoisiens pour les extensions de corps locaux. Précisément, soit L/K une extension galoisienne finie de corps locaux, de groupe G. Notons $O_K \subset O_L$ les anneaux de valuation correspondants. L'ordre associé à l'anneau O_L dans l'algèbre de groupe $K[G]$ est l'ensemble, noté $\mathfrak{A}_{L/K}$, des éléments $\lambda \in K[G]$ tels que λO_L est contenu dans O_L. Cet ensemble est le seul O_K-ordre de $K[G]$ sur lequel O_L puisse être libre comme module. Lorsque l'extension est modérément ramifiée, on a l'égalité $\mathfrak{A}_{L/K} = O_K[G]$ et O_L est libre sur $\mathfrak{A}_{L/K}$. Dans le cas contraire, la structure de O_L comme $\mathfrak{A}_{L/K}$-module est connue uniquement pour des extensions particulières et son étude donne lieu à de nombreuses questions ouvertes. Des progrès récents viennent d'être réalisés et sont exposés dans cet article.

2000 ***Mathematics Subject Classification.*** — 11R33, 11S15, 11S20, 20C05.

Key words and phrases. — Galois module structure, Normal bases, Local fields, Number fields, Associated orders, Representation theory of finite groups, Ramification.

The author is very grateful to Nigel Byott, Philippe Cassou-Noguès and Jacques Martinet for enriching discussions and fruitful correspondence. She wishes to thank Erik Pickett for his suggestions in the English writing of this paper, and she is indebted to Christian Maire for his constant support and encouragement. The author would also like to thank Christophe Delaunay, Christian Maire and Xavier Roblot for making possible the captivating conference "Fonctions L et Arithmétique" in June 2009. The author was supported by a postdoctoral fellowship at the École Polytechnique Fédérale de Lausanne in Switzerland.

Introduction

In its origin, the theory of Galois modules covered classical questions of algebraic number theory. For example, let L/K be a finite Galois extension of number fields, with Galois group G, and let O_K and O_L denote the integer rings of K and L respectively. The ring O_L is naturally endowed with the structure of an $O_K[G]$-module, and a deep question is concerned with the freeness of this module. It is well known that a necessary condition for O_L to be free over $O_K[G]$ is for the extension to be at most tamely ramified, however this is not sufficient. In 1981, Taylor proved the conjecture of Fröhlich: when the extension L/K is tame, he established an explicit connection between the algebraic structure of O_L as a $\mathbb{Z}[G]$-module with some analytic invariants attached to certain characters of G [**151**].

Since this discovery, the subject has developed considerably into several directions, including the study of Galois modules over their associated order when ramification is permitted. Precisely, when the extension L/K is wildly ramified, one natural question is to determine the structure of the valuation ring O_L as a module over its associated order in $K[G]$, i.e., over the full set $\mathfrak{A}_{L/K}$ of elements of $K[G]$ that induce endomorphisms on O_L:

$$\mathfrak{A}_{L/K} = \{\lambda \in K[G] \,:\, \lambda O_L \subset O_L\}.$$

This is a subring of $K[G]$ which contains $O_K[G]$, with equality if and only if the extension is at most tamely ramified.

The most canonical way to attack the problem is via localization, i.e., by transition to local completions. Thus, we now suppose that L/K is a finite Galois extension of local fields, with Galois group G, and we denote by O_K and O_L the valuation rings of K and L. The previous considerations apply to this context as well. In this paper, we shall investigate the following three problems through the survey of previous articles, and outline the main contributions to them since the works of Leopoldt and Fröhlich:

1. to give an explicit description of the associated order $\mathfrak{A}_{L/K}$ of O_L in $K[G]$;
2. to describe the structure of O_L as an $\mathfrak{A}_{L/K}$-module, and in particular to determine whether O_L is free over, i.e., is isomorphic to, $\mathfrak{A}_{K[G]}$;
3. if O_L is $\mathfrak{A}_{K[G]}$-free, to give an explicit generator of O_L over its associated order.

It should be stressed that at present there is still no complete theory for associated orders, their structure being essentially known for prescribed extensions only. Also, there are still partial general criteria for determining whether a valuation ring is free over its associated order in some extension of local fields. However, several advances have recently been made, especially in positive characteristic, and it is our main goal to expose most of these results.

The paper is organised as follows. In Section 1, we begin with a brief survey of the theory of Galois modules for number fields, including associated orders of integer rings. This will give motivation for the rest of the paper. We then restrict to the algebraic structure of valuation rings as modules over their associated order in extensions of local fields. Since this study depends on the ramification of the extension, Section 2 comprises a short preliminary chapter of definitions and properties on the ramification theory for local fields. Sections 3 and 4 are then concerned with the questions of describing the associated order of the top valuation ring in certain extensions of local fields and determining whether the valuation ring is a free module over it, in both mixed (Section 3) and equal (Section 4) characteristic cases. Lastly, Section 5 exposes further comments towards these investigations.

1. Classical Galois module theory for number fields

To give context for what follows, we first recall the classical theory of Galois modules, i.e., for extensions of number fields. For more details about this section, we refer the reader, e.g., to Chapter 1 of [**92**], as well as to the articles [**34**], [**70**], [**122**] and [**126**].

1.1. Normal integral bases in tame extensions. — Let L/K be a finite Galois extension of number fields, with Galois group G. We denote by O_K (resp. O_L) the ring of integers of K (resp. L).

The normal basis theorem asserts that the field L is free of rank 1 as a left module over the group ring $K[G]$ (see [**18**] for two recent short proofs). A more delicate problem is the analogue question for the study of the Galois module structure of the ring O_L. Precisely, the natural action of G on L induces on O_L an $O_K[G]$-module structure: understanding this structure and determining whether O_L is a free module are deeper questions. Note that if O_L is free over $O_K[G]$, it is of rank one and the Galois conjugates of any generator form a K-basis of L that is called a normal integral basis. The existence of normal integral bases for the extension L/K is thus equivalent to the freeness of O_L over $O_K[G]$.

There are many obstructions to studying the $O_K[G]$-module structure of O_L. In particular, when $K \neq \mathbb{Q}$, the ring O_K might not be principal. Moreover, O_L might not even be free over O_K, and, even if it is free, O_L might not be $O_K[G]$-free. Some examples will be given below. In fact, the freeness of O_L over $O_K[G]$ is closely related to the ramification of the extension.

A necessary condition for O_L to be free over $O_K[G]$ is for it to be $O_K[G]$-projective, i.e., to be a direct summand of a free $O_K[G]$-module. The following theorem characterizes $O_K[G]$-projective modules in a more general context (see e.g. Theorem II.I of [**126**]). Recall that the extension L/K is said to be at most tamely ramified ("tame") if every prime ideal that ramifies has a ramification index prime to the characteristic of its residue field.

Theorem 1.1. — *Let A be a Dedekind domain, with field of fractions K. Let L/K be a finite Galois extension with Galois group G. We denote by B the integral closure of A in L, and by $Tr_{L/K} = \sum_{\sigma \in G} \sigma$ the trace map of L/K. The following conditions are equivalent.*

1. *B is a projective $A[G]$-module ;*
2. *$Tr_{L/K}(B) = A$;*
3. *L/K is at most tamely ramified.*

Note that the equivalence $2 \Leftrightarrow 3$ is a consequence of the characterisation of the different $\mathcal{D}_{L/K}$ of the extension L/K. Indeed, $\mathrm{Tr}_{L/K}(B) \neq A$ if and only if $\mathrm{Tr}_{L/K}(B)$ is contained in a prime ideal $\mathfrak{p}$ of A, i.e., if and only if $\mathcal{D}_{L/K} \subset \mathfrak{p}B$. Thus, according to ([**143**], Chap. III, Prop. 13), this is equivalent to the existence of prime ideals of O_L above $\mathfrak{p}$ that are not tamely ramified. As for $1 \Rightarrow 2$, it is essentially the statement that, since B is an A-module of finite type which is torsion-free, if B is projective then it is cohomologically trivial, i.e., $\hat{H}^0(G,B) = A/\mathrm{Tr}_{L/K}B = 0$.

When applied to extensions of number fields, Theorem 1.1 provides necessary conditions for O_L to be free as an $O_K[G]$-module, but they are not sufficient. On the other hand, a theorem of Swan [**147**] asserts that every projective $O_K[G]$-module M of finite type is locally free: for each prime ideal $\mathfrak{p}$ of O_K, the localization of M at $\mathfrak{p}$, that is $M_{\mathfrak{p}} = M \otimes_{O_K} O_{K_{\mathfrak{p}}}$, is free over $O_{K_{\mathfrak{p}}}[G]$, where $K_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic completion of K (for a complete proof, see also Theorem 32.11 of [**74**]). In particular, if M is such a module, its rank is well defined: it is given by the rank of the free $K[G]$-module $M \otimes_{O_K} K$. This rank is finite and also equals the rank of $M_{\mathfrak{p}}$ as an $O_{K_{\mathfrak{p}}}[G]$-module, for every $\mathfrak{p}$.

Therefore, Theorem 1.1 implies the following criterion which is usually known as Noether's criterion, part of which goes back to Speiser [**146**] (he proved the necessary condition), and which is presented as the basic starting point of Galois module structure theory:

***Theorem 1.2* (Noether's criterion).** — *Let L/K be a finite Galois extension of number fields, with Galois group G. Let $O_K \subset O_L$ be the corresponding integer rings. Then O_L is locally free over $O_K[G]$ if and only if the extension is tamely ramified.*

In particular, when the extension L/K is tame, the ring O_L determines an element in the class group $\mathrm{Cl}(O_K[G])$ of locally free $O_K[G]$-modules, and one is interested in understanding this class in terms of the arithmetic of the extension L/K. Recall that this group is defined as the kernel of the rank map from $\mathcal{K}_0(O_K[G])$ to $\mathbb{Z}$, where $\mathcal{K}_0(O_K[G])$ is the Grothendieck group of the category of locally free $O_K[G]$-modules with addition given by direct sums. If M is a locally free $O_K[G]$-module, we denote by $\{M\}$ its class in $\mathcal{K}_0(O_K[G])$ and by $[M]$ the element $\{M\} - m\{O_K[G]\}$ of $\mathrm{Cl}(O_K[G])$, where m is the rank of M. Since every locally free $O_K[G]$-module of rank ≥ 2 has the cancellation property ([**96**], result IV), we have $\{M\} = \{N\}$ in $\mathcal{K}_0(O_K[G])$ if and only if $M \oplus O_K[G] \simeq N \oplus O_K[G]$, which implies $M \simeq N$ whenever the ranks are strictly greater than 1. Finally, $\mathrm{Cl}(O_K[G])$ is a finite abelian group whose neutral element is formed by the classes of all stably free $O_K[G]$-modules, and in fact by the classes of all locally free $O_K[G]$-modules M of rank 1 such that $M \oplus O_K[G] \simeq O_K[G] \oplus O_K[G]$, as a consequence of ([**96**], results I and IV). Algorithms for explicit computations of the locally free class group $\mathrm{Cl}(O_K[G])$ were recently worked out in [**20, 22**].

1.1.1. Extensions over $\mathbb{Q}$.— We first suppose $K = \mathbb{Q}$, consider a tame extension $L/\mathbb{Q}$ with Galois group G, and address the question of determining whether O_L is free over $\mathbb{Z}[G]$. When the extension $L/\mathbb{Q}$ is abelian, a result of Hilbert, as part of the well-known Hilbert-Speiser theorem, implies that O_L is $\mathbb{Z}[G]$-free (originally, this result was restricted to abelian extensions $L/\mathbb{Q}$ whose degree is relatively prime to the discriminant of L, and Leopoldt extended it to abelian tame extensions [**117**]). The proof is based on the Kronecker-Weber theorem: L is a subfield of a cyclotomic field $\mathbb{Q}(e^{\frac{2i\pi}{n}})$ with n squarefree, and the trace of $e^{\frac{2i\pi}{n}}$ in L generates a normal integral basis for $L/\mathbb{Q}$. Now, this argument does not apply when G is not abelian or when $K \neq \mathbb{Q}$.

The existence of normal integral bases in tame non-abelian extensions over $\mathbb{Q}$ was widely investigated during the 1970's by several authors, including Armitage, Cassou-Noguès, Cougnard, Fröhlich, Martinet, Queyrut and Taylor. In particular, Martinet first proved that the ring O_L is free over $\mathbb{Z}[G]$ when G is a dihedral group of order $2p$, for some odd prime number p [**126**]. But then, in 1971, he constructed tamely ramified extensions $L/\mathbb{Q}$ whose Galois group G is a quaternion group of order 8 and such that O_L is not free over $\mathbb{Z}[G]$ [**124**]. This provided the first known counter-example for the existence of normal integral bases, and motivated to a very large extent the conjecture of Fröhlich. Several contributions and computations led to the proof, by Taylor, of this conjecture, in 1981 [**151**]. A precise account of them is given in Chapter 1 of [**92**].

The conjecture of Fröhlich determines the class of O_L in the locally free class group $\mathrm{Cl}(\mathbb{Z}[G])$ in terms of some analytic invariant. Taylor's proof is based on the combination of several ingredients: a generalization to non-abelian characters of the classical Lagrange resolvent and Galois Gauss sums, the logarithm for local group rings which was first introduced by Taylor himself, as well as the famous Fröhlich's Hom-description of the class group $\mathrm{Cl}(\mathbb{Z}[G])$ allowing much of the work to be conducted at a local level (see e.g. Chapter II of [**92**], or [**34**]).

Precisely, for any character χ of the Galois group G, there is an extended Artin L-function $\Lambda(s,\chi)$ attached to $L/\mathbb{Q}$ and which satisfies a functional equation $\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\bar{\chi})$, where $\bar{\chi}$ is the complex conjugate character and $W(\chi)$ is a constant called the Artin root number attached to χ. Fröhlich's conjecture is related to the equality $[O_L] = t(W_{L/\mathbb{Q}})$ in $\mathrm{Cl}(\mathbb{Z}[G])$, where $t(W_{L/\mathbb{Q}})$ is the so-called analytic root number class. This invariant was first defined by Cassou-Noguès [**50**] solely in terms of the values of Artin root numbers of symplectic characters of G. As these values are ± 1, $t(W_{L/\mathbb{Q}})$ is an element of order 1 or 2. The theorem of Taylor can thus be stated as follows.

Theorem 1.3 **(Taylor, 1981)**. — *Let $L/\mathbb{Q}$ be a finite Galois extension of number fields, with Galois group G. Denote by $O_K \subset O_L$ the corresponding integer rings. If the extension is at most tamely ramified, then:*

1. *$[O_L \oplus O_L] = 1$ in $Cl(\mathbb{Z}[G])$;*
2. *the only obstructions to the vanishing of the class of O_L are the signs of the Artin root numbers of symplectic characters. In particular, if G has no irreducible symplectic character, then $[O_L] = 1$ in $Cl(\mathbb{Z}[G])$.*

Equivalently, assertion 1 states that the module $O_L \oplus O_L$ is stably free over $\mathbb{Z}[G]$, and thus free since it is of rank 2. This means that we always have $O_L \oplus O_L \simeq \mathbb{Z}[G] \oplus \mathbb{Z}[G]$. If, moreover, $t(W_{L/\mathbb{Q}}) = 1$, then $O_L \oplus \mathbb{Z}[G] \simeq \mathbb{Z}[G] \oplus \mathbb{Z}[G]$ and O_L is stably free. This happens in particular when G has no irreducible symplectic characters (assertion 2): in this case, O_L is in fact free because $\mathbb{Z}[G]$ satisfies Jacobinski's cancellation theorem since no simple component of $\mathbb{Q}[G]$ is a totally definite quaternion algebra (see e.g. [**96**], Par. 3).

More generally, Theorem 1.3 can be applied to determine the $\mathbb{Z}[G]$-structure of O_L in some relative tame extension L/K with Galois group G: in this case, the module $O_L \oplus O_L$ is isomorphic to $\mathbb{Z}[G]^{2[K:\mathbb{Q}]}$. In particular, O_L is $\mathbb{Z}[G]$-free whenever $[O_L] = 1$ in $\mathrm{Cl}(\mathbb{Z}[G])$ and $\mathbb{Z}[G]$ has the cancellation property. Specifically, O_L is $\mathbb{Z}[G]$-free in the following supplementary cases: when the order of G is odd [**151**] or not divisible by 4 [**51, 70**], when G is symmetric, or when K contains the m-th roots of unity if m is the exponent of G [**93**]. In particular, for $K = \mathbb{Q}$, this provides new examples of tame extensions of $\mathbb{Q}$ with integral normal bases. Note also that, in 1978, Taylor already proved the analogue of the Hilbert-Speiser theorem in this context: if L/K is tame, then O_L is $\mathbb{Z}[G]$-free. Now, Theorem 1.3 cannot be extended to determine the relative Galois structure of O_L in general, i.e., as an $O_K[G]$-module when $K \neq \mathbb{Q}$ (see next paragraph).

On the opposite side, the conjecture of Fröhlich has given rise to the construction of new tame extensions $L/\mathbb{Q}$ without integral normal basis, among them certain quaternion extensions. For instance, if $L/\mathbb{Q}$ has Galois group $G = H_{32}$, Fröhlich had proved that O_L is stably free over $\mathbb{Z}[G]$. However, this doesn't necessarily imply that O_L is free. Indeed, Cougnard constructed such an extension without integral normal basis [**69**]. Note that on H_8 and H_{16}, every stably free module is free. In particular, in [**124**], the quaternion extensions $L/\mathbb{Q}$ with Galois group H_8 and without integral normal basis are such that O_L is not stably free over $\mathbb{Z}[G]$.

To conclude this section, we should stress the fact that Theorem 1.3 does not lead to any description of generators when O_L is free over $O_K[G]$. However, explicit generators or algorithms to find them when $K = \mathbb{Q}$ and $G = A_4$, D_{2p} (with p odd prime), H_8, H_{12}, H_{32} or $H_8 \times C_2$ are given in [**65, 67, 73, 68, 126**]. More recently, in 2008, Bley and Johnston implemented an algorithm which, amongst other things, determines such generators for other groups G; in particular, abelian or dihedral D_{2n} with “small" orders [**21**].

1.1.2. Relative extensions of number fields.— The case of relative extensions is much more difficult, even for abelian extensions. In 1999, Greither et al. proved that the field $\mathbb{Q}$ is the only base field over which all tame abelian extensions have a normal integral basis [**104**].

In fact, the question of the existence of normal integral bases for tame relative extensions is solved for prescribed extensions only, including e.g. certain cyclic extensions. For example, one key argument in [**104**] is that for any number field $K \neq \mathbb{Q}$, there exists a prime number p and a tame cyclic extension L/K of degree p without normal integral basis. In 2001, Cougnard gave other examples of relative cyclic extensions without normal integral basis, generalizing results of Brinkhuis [**29, 30**]. Furthermore, in 2009, Ichimura proved that when $K/\mathbb{Q}$ is unramified at some odd prime number p, any tame cyclic extension L/K of degree p has a normal integral basis if the extension $L(\zeta_p)/K(\zeta_p)$ has a normal integral basis, where ζ_p is a p-th root of unity [**108**].

Kummer extensions of number fields have been investigated by several authors, such as Fröhlich [**99**], Kawamoto [**113, 114, 115**], Okutsu, Gomez-Ayala [**101**], Ichimura [**109**], and very recently Corso and Rossi [**75**]. Gomez-Ayala gave an explicit criterion for the existence of normal integral bases in tame Kummer extensions of prime degree, along with explicit generators. Del Corso and Rossi (2010) have just generalized this result to cyclic Kummer extensions of arbitrary degree, precising [**109**]. Their result is based on an explicit formula for the ramification index of prime ideals in such extensions. As an application, Ichimura proved that, given an integer $m \geq 2$ and a number field K, there exists a finite extension L/K depending on m and K such that for any abelian extension M/K of exponent dividing m, the extension LM/L has a normal integral basis.

Other relative extensions without normal integral basis have been investigated (see e.g. [**115**]). Among several contributions, one could cite Brinkhuis' result for CM fields [**29**]: if L/K is an unramified abelian extension of number fields, each of which is either CM or totally real, and if the Galois group of L/K is not 2-elementary, then L/K has no normal integral basis.

We conclude this section with the notion of weak normal integral bases whose non existence is a further obstruction to the existence of normal integral bases [**30**]: if L/K is a tame finite abelian extension of number fields with Galois group G, we say that L/K has a weak normal integral basis if the projective $\mathfrak{M}$-module $\mathfrak{M} \otimes_{O_K[G]} O_L$ is in fact free, where $\mathfrak{M}$ is the unique maximal O_K-order of $K[G]$. The investigation of this notion has just led Greither and Johnston to establish a necessary and sufficient condition for the existence of normal integral bases ([**102**], Theorem 5.5]):

Proposition 1.4 **(Greither & Johnston, 2009)**. — *Let L/K be a tame finite extension of number fields such that $L/\mathbb{Q}$ is abelian of odd degree. Suppose that either $[L : K]$ is not divisible by 3 or that for all primes q dividing $[K : \mathbb{Q}]$ the field $L(\zeta_{3^\infty})$ contains no q-th root of unity. Then L/K has a normal integral basis if and only if the tower $L/K/\mathbb{Q}$ is arithmetically split.*

Here, a tower of number fields $K \subset M \subset L$ is said to be arithmetically split if there exists an extension L'/K such that $L = L'M$ and the extensions L'/K and M/K are arithmetically disjoint, i.e., they are linearly independant and no finite prime $\mathfrak{p}$ ramifies both in L'/K and M/K.

1.2. Wildly ramified extensions. — When the extension L/K is wildly ramified, i.e., not tamely ramified, we are faced with a very different situation since the integer ring O_L is not locally free over $O_K[G]$. We also note another failure concerned with the following result due to Fröhlich (which was a key argument in Theorem 1.3): suppose $L/\mathbb{Q}$ is a tame extension with Galois group G and let $\mathfrak{M}$ be a maximal order in $\mathbb{Q}[G]$ containing $\mathbb{Z}[G]$, then the locally free $\mathfrak{M}$-module $O_L\mathfrak{M}$ is stably free over $\mathfrak{M}$. This result was first conjectured by Martinet, and Cougnard proved that it does not hold in general for wild extensions [**71**]. There are a number of approaches to circumventing these difficulties, and we present some of them here (see also Appendix C of [**92**]).

We can first investigate which results from the classical tame theory can be generalized to the wild case, by adapting the framework. For example, Queyrut developed a K-theoretic approach, replacing the locally free class group $\mathrm{Cl}(\mathbb{Z}[G])$ with the class group of another category of $\mathbb{Z}[G]$-modules (see e.g. [**52**], [**139**]). One should cite [**53**] as well, where the class of O_L in $\mathrm{Cl}(\mathbb{Z}[G])$ is replaced with the class of a certain submodule of O_L.

We can also consider the Ω-conjectures of Chinburg which extend and generalize Fröhlich's conjecture [**63, 145**], and their relations with Equivariant Tamagawa Number conjectures in special cases (see e.g. [**31**]). Chinburg's conjectures give equalities between new invariants in the class group $\mathrm{Cl}(\mathbb{Z}[G])$ that involve the Galois structure of O_L.

Another approach is concerned with the indecomposable $\mathbb{Z}[G]$-modules or $O_K[G]$-modules that can occur in O_L as well as the question of the decomposability of O_L as an $O_K[G]$-module. In this direction, one should cite the contributions for certain p-extensions of Yokoi, Miyata (e.g. [**132**]), Bertrandias [**14**], Bondarko & Vostokov (e.g. [**27**]), Rzedowski Calderon, Villa Salvador & Madan [**141**], as well as Elder & Madan (e.g. [**78, 79, 80, 81**]). Note that the question depends very much on ramification invariants of the extension, and most of the results are stated under some technical restrictions on ramification numbers.

In this paper, the approach we consider is due to Leopoldt [**117**]; it was initiated by Leopoldt, Fröhlich [**99**] and Jacobinski [**111**]. The idea is to replace the group ring $O_K[G]$ by a larger subring of $K[G]$, namely the associated order of O_K in $K[G]$:

$$\mathfrak{A}_{L/K} = \mathfrak{A}_{L/K}(O_L) = \{\lambda \in K[G] \,:\, \lambda O_L \subset O_L\},$$

with the idea that O_L may have better properties as a module over $\mathfrak{A}_{L/K}$ than over $O_K[G]$. The Galois module structure of O_L over its associated order, for extensions of global or local fields, is our main topic of interest in the rest of the paper.

1.3. The associated order of integer rings in extensions of number fields. —

1.3.1. General properties.— Let L/K be a finite Galois extension of number fields, with Galois group G. In this section, we give an account of the general properties of the associated order of O_L in $K[G]$. They all hold in more general Galois extensions L/K, e.g. when K is the field of fractions of some Dedekind domain O_K and O_L is the integral closure of O_L in L. However, to simplify the exposition of the paper, we describe them in the number field case. For further details, we refer to [**7**], [**8**], [**11**] and [**125**].

The associated order $\mathfrak{A}_{L/K}$ of O_L in L/K is an O_K-order in $K[G]$, i.e., it is a subring of $K[G]$ and a finitely generated module over O_K which contains a K-basis of $K[G]$. It is also a free O_K-module of rank $[L:K]$ over O_K, since it is a subring of the endomorphism ring $\mathrm{End}_{O_K}(O_L)$ with O_K a principal ideal domain.

The ring O_L is a module over its associated order which is torsion free and finitely generated. One can thus define its rank as the dimension over K of $O_L \otimes_{\mathfrak{A}_{L/K}} L$, and see that it is equal to 1, by the normal basis theorem. Moreover, the associated order $\mathfrak{A}_{L/K}$ is the only O_K-order of $K[G]$ over which O_L can be free as a module (Par. 4 of [**125**], Prop. 12.5 of [**60**] or Par. 5.8 of [**154**]).

In [**11**], Bergé described some further general results about $\mathfrak{A}_{L/K}$ obtained by Jacobinski, in particular when viewed as a subring of the ring $\mathrm{End}_{O_K}(O_L)$ of O_K-endomorphisms of O_L. Note that, when the extension L/K is abelian, the associated order $\mathfrak{A}_{L/K}$ is isomorphic to the ring $\mathrm{End}_{O_K[G]}(O_L)$ of $O_K[G]$-endomorphisms of O_L.

Finally, the equality $\mathfrak{A}_{L/K} = O_K[G]$ holds if and only if the extension L/K is at most tamely ramified (see e.g. [**11**], Theorem 1), in which case O_L is locally free as an $O_K[G]$-module. However, the question of determining whether O_L is locally free (or even free) over its associated order is much more delicate in the wildly ramified case than in the tame case. First, O_L might not be projective over its associated order [**17**]. Moreover, there exist projective $\mathfrak{A}_{L/K}$-modules that are not locally free (see [**122**], Par. 3). Also, the algebraic structure of $\mathfrak{A}_{L/K}$ is known for prescribed extensions of global and local fields only and still yields open questions.

Remark 1.5. — One could address the question of whether Artin root numbers of real characters of G can be related to the structure of O_L over its associated order, generalizing Fröhlich's conjecture in this setting. However, as far as we know, this idea fails. In [**122**] (Par. 3.3), Martinet raised several obstructions to such a connection and gave a counter-example for quaternion extensions of degree 8, citing a result of Fröhlich [**98**].

1.3.2. Extensions over $\mathbb{Q}$.— Again, when $K = \mathbb{Q}$, some partial results are known. First, in 1959, Leopoldt proved that for any abelian extension $L/\mathbb{Q}$ the ring O_L is free over its associated order [**117**], generalizing in this way the Hilbert-Speiser theorem. Once more, the proof is based on the Kronecker-Weber theorem but the arguments are much more difficult. In 1964, Jacobinski [**111**] gave an alternate proof to this theorem, extending the explicit description of the associated order in terms of the ramification structure to a larger class of extensions (see Subsection 3.2). A simplified proof was also given by Lettl in [**120**]. Note that the theorem of Leopoldt is very explicit, in the sense that it determines $\mathfrak{A}_{L/K}$ and provides an explicit Galois generator in terms of the classical abelian Galois Gauss sums. See ([**54**], Chapter I) for further details.

In 1972, generalizing a theorem of Martinet, Bergé [**10**] proved that O_L is free over its associated order when $L/\mathbb{Q}$ is a dihedral extension of order $2p$ when p is an odd prime. But dihedral extensions over $\mathbb{Q}$ of order $\neq 2p$ give counter-examples of the projectivity of O_L over its associated order. At the same time, Martinet proved that every quaternion extension of degree 8 over $\mathbb{Q}$ that is wildly ramified is such that O_L is free over its associated order [**123**], which is not always true when the extension is tamely ramified [**124**].

1.3.3. Leopoldt extensions.— Let L/K be an extension of number fields where $L/\mathbb{Q}$ is abelian; it is said to be Leopoldt if the ring of integers O_L is free over its asociated order. A field is said to be Leopoldt if every finite extension L/K with $L/\mathbb{Q}$ abelian is such that O_L is free over its associated order. Results of Leopoldt [**117**], Cassou-Noguès & Taylor ([**54**], Chap. 1, Thm. 4.1), Chan & Lim [**57**], Bley [**19**], and Byott & Lettl [**48**] culminated in the proof that the n-th cyclotomic field $\mathbb{Q}(\zeta_n)$ is Leopoldt for every n. See also [**100**] for another type of Leopoldt extensions. Johnston has generalized these results by giving more examples of Leopoldt fields, along with explicit generators [**112**]. He has also obtained some freeness result in intermediate finite layers of certain cyclotomic $\mathbb{Z}_p$-extensions ([**112**], Cor.8.4).

The result of Chan and Lim is the following [**57**]: let m and m' be positive integers with $m|m'$, let $K = \mathbb{Q}(\zeta_m)$ and $L = \mathbb{Q}(\zeta_{m'})$, where ζ_n denotes a primitive n-th root of unity. Then, the ring of integers $\mathbb{Z}[\zeta_{m'}]$ of L is free over its associated order in $K[G]$ and the authors give explicit generators (Aiba investigated an analogue of this result for function fields, see Subsection 4.3). As noticed by Byott, this order is in fact the maximal order in $K[G]$. Later, for an extension

L/K with $L/\mathbb{Q}$ abelian, Byott and Lettl [**48**] gave an explicit description of the associated order of O_L when K is a cyclotomic field, and proved that O_L is free over it. Their paper contains some intermediate results about maximal orders in $K[G]$ (see Subsection 5.1).

1.3.4. Other extensions.— One should also mention the reference ([**54**], Chaper XI) where Cassou-Noguès and Taylor determine the Galois structure of rings of integers of certain abelian extensions over quadratic imaginary number fields, by evaluating suitable elliptic functions at singular values. See also [**5**] where Bayad considers the Galois module structure of rings of integers attached to elliptic curves without complex mutliplication and admitting a rational point of finite order: this contains a freeness result over associated orders, with explicit generators.

1.3.5. Intermediate results.— The paper of Johnston [**112**] is interesting also because it gathers several properties of associated orders that might be very useful, some of them are originally issued from [**48**] and [**57**]. For example, the next two propositions show how associated orders in composite fields and subfields can be determined under certain additional assumptions, which sometimes permits the reduction of the problem to simpler extensions:

Proposition 1.6 **([48], Lemma 5)**. — *If L/K and M/K are arithmetically disjoint extensions of number fields, then $\mathfrak{A}_{LM/M} = \mathfrak{A}_{L/K} \otimes_{O_K} O_M$ and $\mathfrak{A}_{LM/K} = \mathfrak{A}_{L/K} \otimes_{O_K} \mathfrak{A}_{M/K}$. Moreover, if $O_L = \mathfrak{A}_{L/K} \cdot \alpha_1$ and $O_M = \mathfrak{A}_{M/K} \cdot \alpha_2$, then $O_{LM} = \mathfrak{A}_{LM/K} \cdot (\alpha_1 \otimes \alpha_2)$.*

More generally, Greither & Johnston recently obtained an arithmetically disjoint capitulation result for certain extensions of number fields ([**103**], Cor. 1.2), generalizing [**109**]. As noticed by the authors ([**103**], Remark 5), there is no "arithmetically disjoint capitulation" for finite Galois extensions of p-adic fields ([**119**], Proposition1.b). Moreover, one can prove that if L/K is a finite Galois extension of number fields such that O_L is not locally free over its associated order $\mathfrak{A}_{L/K}$, then there exists no extension M/K arithmetically disjoint from L/K such that $O_{LM} = O_L \otimes_{O_K} O_M$ is free over $\mathfrak{A}_{LM/K} = \mathfrak{A}_{L/K} \otimes_{O_K} O_M$.

An interesting result for certain intermediate extensions is the following:

Proposition 1.7 **([48], Lem. 6 - [112], Cor. 2.5)**. — *Let L/K and M/K be Galois extensions of number fields with $K \subset M \subset L$ and L/M at most tamely ramified. Put $G = Gal(L/K)$ and $H = Gal(M/K)$. Let $\pi : K[G] \to K[H]$ denote the K-linear map induced by the natural projection $G \to H$. If $O_L = \mathfrak{A}_{L/K} \cdot \alpha$ for some $\alpha \in O_L$, then $\mathfrak{A}_{M/K} = \pi(\mathfrak{A}_{L/K})$ and $O_M = \mathfrak{A}_{M/K} \cdot Tr_{L/M}(\alpha)$.*

Another line of attack is to reduce the problem of the existence of elements α such that $O_L = \mathfrak{A}_{L/K} \cdot \alpha$ to the computation of certain discriminants, based on explicit computation of resolvents;

Proposition 1.8 **([112], Cor. 4.4)**. — *Let L/K be a finite extension of number fields, with Galois group G, and let $\hat{G}$ denote the group of characters of G. Suppose that O_L is locally free over $\mathfrak{A}_{L/K}$. Then, for any $\alpha \in O_L$, $O_L = \mathfrak{A}_{L/K} \cdot \alpha$ if and only if $\prod_{\chi \in \hat{G}} < \alpha | \chi >$ divides*

$\prod_{\chi\in\hat{G}} <\beta|\chi>$ *for all* $\beta \in O_L$, *where* $<\alpha,\chi>= \sum_{g\in G}\chi(g^{-1})g(\alpha)$ *is the resolvent attached to* α *and* χ.

This result has to be compared with Lemma 1 of **[3]** in the case of function fields, where Galois generators over associated order when they exist are characterized by a minimality condition on discriminants.

Finally, let us mention the article **[6]** in which Bergé investigated the genus of the ring of integers of an extension of number fields. She analyzed the obstacles for projectivity encountered at various stages of reduction, linking them to a bad functorial behavior of the associated order.

1.3.6. From local freeness to global freeness.— Other examples are derived from the local case. Mathematicians rapidly considered Galois module structure of rings of integers for extensions of local fields, mainly motivated by Noether's theorem and because the local context is easier to deal with. We should also mention the following proposition which allows us to reduce to the local case (see Prop. 1 of **[8]**, as well as Prop. 2 of **[17]**):

Proposition 1.9. — *Let* L/K *be a finite Galois extension of number fields, with Galois group* G. *Let* $\mathfrak{P}$ *be a prime ideal of* O_L *whose decomposition group coincides with* G *and write* $\mathfrak{p} = \mathfrak{P} \cap O_K$. *Then, the associated order of* $O_{L_\mathfrak{P}}$ *in* $K_\mathfrak{p}[G]$ *is the* $\mathfrak{p}$*-adic completion of* $\mathfrak{A}_{L/K}$. *Moreover, if* O_L *is free (resp. projective) over* $\mathfrak{A}_{L/K}$, *then* $O_{L_\mathfrak{P}}$ *is free (resp. projective) over* $U_{K_\mathfrak{p}[G]}$.

One can generalize this to all prime ideals $\mathfrak{p}$ of O_K, i.e., without the condition on the decomposition group, and prove that O_L is projective over its associated order in $K[G]$ if and only if it is locally projective (see **[8]**, Chap. I, Par. 1 & 2, where $\mathfrak{p}$-adic completions correspond to tensor products over $O_{K_\mathfrak{p}}[D]$, D being the decomposition group of an ideal above $\mathfrak{p}$). However, being locally free is not a sufficient condition for O_L to be free over $\mathfrak{A}_{L/K}$. Nevertheless, recent results of Johnston and Greither & Johnston show that local freeness is close to global freeness in the following sense;

Proposition 1.10 **(Johnston, 2008 ([112], Proposition 3.1))**
If O_L *is locally free over* $\mathfrak{A}_{L/K}$, *then, given any non-zero ideal* $\mathfrak{a}$ *of* O_K, *there exists* $\beta \in O_L$ *such that* $\mathfrak{a} + [O_L : \mathfrak{A}_{L/K} \cdot \beta] = O_K$, *where* $[O_L : \mathfrak{A}_{L/K} \cdot \beta]$ *denote the* O_K*-module index of* $\mathfrak{A}_{L/K} \cdot \beta$ *in* O_L.

Proposition 1.11 **(Bley & Johnston, 2008 ([21], Prop. 2.1))**
Let L/K *be a finite Galois extension of number fields with Galois group* G. *Let* $\mathfrak{M}$ *be a maximal order in* $K[G]$ *containing* $\mathfrak{A}_{L/K}$. *Then,* O_L *is* $\mathfrak{A}_{L/K}$*-free if and only if:*

1. O_L *is locally free over* $\mathfrak{A}_{L/K}$, *and;*
2. *there exists* $\alpha \in O_L$ *such that* $\mathfrak{M} \otimes_{\mathfrak{A}_{L/K}} O_L = \mathfrak{M} \cdot \alpha$.

When this is the case, then $O_L = \mathfrak{A}_{L/K} \cdot \alpha$.

In fact, Proposition 1.11 is stated in a more general context. Furthermore, when the Wedderburn decomposition of $K[G]$ is explicitly computable and under certain extra hypothesis, Bley and Johnston derive from this proposition an algorithm that either determines a $\mathfrak{A}_{L/K}$-generator of O_L or determines that no such element exists ([**21**], Par. 8).

In what follows, we then restrict to finite Galois extensions of local fields and consider the structure of the top valuation rings over their associated order.

2. Local setup

From now on, we suppose that K is a local field, i.e., a complete field with respect to a discrete valuation $v_K : K^* \to \mathbb{Z}$ (with $v_K(0) = +\infty$). Let O_K be its valuation ring, i.e., $O_K = \{x \in K \; : \; v_K(x) \geq 0\}$, and let $\mathfrak{p}_K$ denote the unique maximal ideal of O_K. We then define the residue field of K as the quotient $k := O_K/\mathfrak{p}_K$, and we shall always suppose that it is perfect.

Let p be a prime number. When k has characteristic p, this leads to the following cases;

- equal characteristic case (p, p): K has characteristic p, in which case it can be identified with the field of formal power series $k((T))$ for some element $T \in K$ with $v_K(T) = 1$;

- unequal characteristic case $(0, p)$: K has characteristic 0, i.e., it is an extension of the field $\mathbb{Q}_p$ of p-adic numbers.

Next, we fix a separable closure K^{sep} of K and we consider a finite Galois extension L/K with Galois group G. Let $O_K \subset O_L$ denote the corresponding valuation rings. In our setup, i.e., when K is a local field, the ring O_L is always free as an O_K-module, since it is of finite type over a principal ring ([**143**], Chap. 2, Prop. 3).

2.1. Galois module theory for extensions of local fields.— The more general Hattori's approach to Swan's theorem ([**74**], 32.A) enables us to derive again, from Theorem 1.1, a Noether's criterion for extensions of local fields:

Proposition 2.1. — *If L/K is a finite Galois extension of local fields, with Galois group G, then O_L is $O_K[G]$-free if and only if the extension is at most tamely ramified.*

When the extension is ramified, we introduce the associated order $\mathfrak{A}_{L/K}$ of O_L in $K[G]$, given by $\mathfrak{A}_{L/K} = \{\lambda \in K[G] \; : \; \lambda O_L \subset O_L\}$. The classical considerations described in the first section, and specifically in Subsection 1.3, apply to this local context as well.

In particular, it is a ring containing $O_K[G]$, with equality if and only if L/K is tame, and O_L is an $\mathfrak{A}_{L/K}$-module. Moreover, since $K[G]$ acts faithfully on L, $\mathfrak{A}_{L/K}$ is an O_K-order in $K[G]$ and we address the question of whether O_L is free over $\mathfrak{A}_{L/K}$. If it is, and if we can find an explicit generator, then we can say that we have determined the structure of the $O_K[G]$-module O_L. If, on the other hand, O_L is not free over $\mathfrak{A}_{L/K}$, then we have at least obtained one information about the Galois structure of O_L: its structure is too complicated to be rendered free by enlarging $O_K[G]$. In both cases, the question is difficult, not least because it is difficult to describe $\mathfrak{A}_{L/K}$ as an O_K-module since it requires a detailed understanding of the action of G on O_L. Many answers are in fact given without an explicit determination of this order.

This question is solved for prescribed extensions of local fields only, and our goal is to expose most of the known answers in what follows.

2.2. Ramification of local fields.— The description of the associated order of the valuation ring in any extension of local fields involves higher ramification invariants. We thus recall some facts about the ramification theory of local fields with perfect residue field, and precisely the notion of ramification groups and jumps. For further details, see for example ([**143**], Chap. IV), and for a complete investigation of the possible values of ramification jumps in p-extensions of local fields, we refer the reader to [**116**] and [**90**], as well as the works of Marshall, Maus, Miki and Wyman.

Let L/K be a finite Galois extension, with group G. The ramification groups G_i, for $i \in \mathbb{Z}_{\geq -1}$, of L/K are defined by:

$$G_i := \{\sigma \in G \,:\, \sigma(x) - x \in \mathfrak{p}_L^{i+1}\}.$$

In particular, the ramification groups form a decreasing filtration of normal subgroups of G:

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m \neq \; G_{m+1} = 1,$$

for some integer $m \geq -1$. Note that, for $i = 0$, the ramification group G_0 is the inertia group of L/K, and the ramification index of the extension is defined as $e_{L/K} = \mathrm{card}(G_0)$.

The extension L/K is said to be unramified if $G_0 = 1$; tamely ramified if $G_1 = 1$, equivalently if its ramification index is prime to the residue characteristic of K; and totally ramified if $G_0 = G$. Moreover, when the residue field k of K has characteristic 0, the group G_1 is trivial and G_0 is cyclic; when $\mathrm{char}(k) = p$, G_1 is a p-group and the quotient group G_0/G_1 is cyclic of order prime to p. In particular, if $\mathrm{char}(k) = 0$, then the extension L/K is at most tamely ramified. This is the reason why we exclude this case and only consider local fields with positive residue characteristic p, since we are interested in wild extensions. In this context, if L/K is a p-extension, then $G_0 = G_1$: in particular, tamely ramified implies unramified.

A notion that arises naturally is that of ramification jumps, which are defined as the integers $b \geq -1$ such that $G_b \neq G_{b+1}$. They form an increasing sequence: $b_1 < \cdots < b_r$ (with $b_r = m$ with regards to the previous notation). When the residue characteristic of K is some prime number p and L/K is a totally ramified p-extension, i.e., $b_1 \geq 1$, jumps are all congruent modulo p ([**143**], IV.2, Proposition 11) :

$$\forall i, j, \quad b_i \equiv b_j \bmod p.$$

Furthermore, when the extension is abelian, the Hasse-Arf theorem induces more advanced congruences (see e.g. [**153**], Proposition 5).

If L/K is a totally ramified p-extension, we have the following. When $\mathrm{char}(K) = p$, i.e., in the context of Artin-Schreier theory, one can prove that all ramification jumps of L/K are relatively prime to p whenever the residue field of K is perfect. Moreover, in this case, ramification jumps are not bounded.

When $\mathrm{char}(K) = 0$, things are rather different: jumps are bounded and might be divisible by p. Precisely, suppose L/K be of degree p^n and let $b_1 \leq b_2 ... \leq b_m$ denote its ramification jumps. Let $e_K = v_K(p)$ be the absolute ramification index of K. Then, $b_m \leq \frac{e_K[L:K]}{p-1}$, and so $b_m - \lfloor \frac{b_m}{p} \rfloor \leq p^{n-1}e_K$. Moreover, if $b_m < \frac{p^n e_K}{p-1}$ then $p \not| b_i$ for all i, and if $b_m = \frac{p^n e_K}{p-1}$, then all jumps are divisible by p and L/K is a Kummer cyclic extension (see [**143**], Chap. IV, Exercise 3).

3. Local Galois module structure in mixed characteristic

Let K be a local field of characteristic $(0, p)$, for some fixed prime number p. We seek to determine $\mathfrak{A}_{L/K}$ and the module structure of O_L as an $\mathfrak{A}_{L/K}$-module, where the action is induced by that of $K[G]$ acting on L. We will often suppose that K is in fact a finite extension of $\mathbb{Q}_p$ (and say it is a p-adic field), equivalently, that its residue field k is finite, since most of the known results are stated in this setting even if they can be generalized to local fields with perfect residue field.

3.1. On the p-adic version of Leopoldt's theorem. — The archetypal result is that of Leopoldt. For extensions of p-adic fields, it says that O_L is $\mathfrak{A}_{L/K}$-free whenever $K = \mathbb{Q}_p$ and G is abelian. However, it is proved that the field $\mathbb{Q}_p$ is the only base field which satisfies this property (see e.g. Subsections 3.2 and3.3).

In 1998, Lettl strengthened the local version of Leopoldt's theorem as follows [**119**]. He proved that if $L/\mathbb{Q}_p$ is abelian, then O_L is again free over $\mathfrak{A}_{L/K}$ for any intermediate field K of the extension $L/\mathbb{Q}_p$. Moreover, writing G_0 for the inertia group of L/K, and $\mathfrak{M}_0$ for the maximal order in $K[G_0]$, the author shows that if $p \neq 2$, then $\mathfrak{A}_{L/K} = O_K[G] \otimes_{O_K[G_0]} \mathfrak{M}_0$. Unfortunately, his argument does not give an explicit generator of O_L over its associated order in general. As a corollary, Lettl deduced a global result: if L/K is an extension of number fields with $L/\mathbb{Q}$ abelian, then O_L is locally free over $\mathcal{A}_{L/K}$.

In fact, the property of Lettl characterises $\mathbb{Q}_p$ among its finite extensions, as a local analogue of [**104**]. If $F \neq \mathbb{Q}_p$, then there exist fields $F \subset K \subset L$ with L/F abelian but O_L not free over $\mathfrak{A}_{L/K}$. An example is given by Lubin-Tate extensions in ([**42**] Theorem 5.1): let K be a finite extension of $\mathbb{Q}_p$ and write $K^{(n)}$ for the n-th division field of K with respect to a Lubin-Tate formal group, then $K^{(n)}$ is an abelian extension of K, but $O_{K^{m+r}}$ fails to be free over its associated order in $K^{(m+r)}/K^{(r)}$ whenever $m > r \geq 1$ and $K \neq \mathbb{Q}_p$.

Another extension of the p-adic Leopoldt's theorem is due to Byott. If L/K is an abelian extension of p-adic fields, then O_L is $\mathfrak{A}_{L/K}$-free whenever L/K is at most weakly ramified, i.e., its second ramification group is trivial ([**41**], Cor. 4.3).

3.2. Extensions with cyclic inertia group (Bergé). — According to the local version of Leopoldt's theorem, if $L/\mathbb{Q}_p$ is a finite abelian extension with Galois group G and ramification groups G_i, the associated order $\mathfrak{A}_{L/K}$ of O_L is the subring of $\mathbb{Q}_p[G]$ obtained by adjoining to

$\mathbb{Z}[G]$ the idempotents

$$e_i = \frac{1}{\mathrm{card}(G_i)} \sum_{\sigma \in G_i} \sigma,$$

and O_L is free over this subring. In [**7**], Bergé investigated the analogue of this property for extensions over any absolutely unramified p-adic field with cyclic inertia group, extending results of [**111**]. In this section, we shall describe most of her results.

Let K be a p-adic field which is absolutely unramified, i.e., $e_K = 1$. Let L/K be a finite Galois extension, with Galois group G and cyclic inertia group G_0. Bergé described explicitly the associated order $\mathfrak{A}_{L/K}$ of such an extension, and investigated criteria for the top valuation ring to be free over its associated order. However, in her more general setting, Bergé did not consider the problem of giving explicit generators for those cases in which O_L is free over its associated order.

As another consequence of her investigation, she constructed extensions for which the valuation ring is not free. This fact was already surprising since the conditions imposed on K and on G by Bergé are merely the abstraction of conditions satisfied by all abelian extensions of $\mathbb{Q}_p$, and these extensions satisfy Leopoldt's result.

Using a result of Jacobinski [**111**], Bergé first reduced the problem to totally ramified extensions. So, let L/K be a totally ramified cyclic extension of order rp^n, with $p \nmid r$ and $e_K = 1$. The cyclic group G/G_1 has order r. Let $\mathfrak{C}$ be the multiplicative group of characters of G/G_1 of degree 1. For each $\chi \in \mathfrak{C}$, we write e_χ for the idempotent

$$e_\chi = \frac{1}{r} \sum_{\sigma \in G/G_1} \chi(\sigma^{-1})\sigma$$

of the group algebra $K[G/G_1]$. For each ramification group G_i of L/K, we also write

$$e_i = \frac{1}{\mathrm{card}(G_i)} \sum_{\sigma \in G_i} \sigma$$

which is an idempotent of $K[G]$. According to Leopoldt's result, if $K = \mathbb{Q}_p$ and L/K is abelian, all e_i belong to $K[G]$. This does not hold in general, and Bergé provided explicit counter examples in her setting. Her main result is the following ([**7**], Thm. 1);

Proposition 3.1 **(Bergé, 1978)**. — *Let K be a p-adic field such that $K/\mathbb{Q}_p$ is unramified. Let L/K be a totally ramified cyclic extension of degree rp^n with $p \nmid r$. Let σ be a generator of its highest non trivial ramification group, and write $f = \sigma - 1$. Then $\mathfrak{A}_{L/K}$ is the subring of $K[G]$ generated by $O_K[G]$, the elements $e_i f$ for $1 \le i \le n$, and the idempotents $e_\chi e_i$ for all $\chi \in \mathfrak{C}$ and all i such that $e_\chi e_i \in \mathfrak{A}_{L/K}$.*

Bergé then investigated the existence of a criterion for O_L to be free over its associated order. This yields the following criterion ([**7**], Cor. of Thm. 3);

Proposition 3.2 **(Bergé, 1978)**. — *Under the assumptions of Proposition 3.1, and if t_1 denotes the first ramification jump of L/K, the ring O_L is free as a $\mathfrak{A}_{L/K}$-module if and only if $\frac{rp}{p-1} - t_1 < \frac{p^n}{p^{n-1}-1}$, with $\frac{p^n}{p^{n-1}-1} = +\infty$ if $n = 1$.*

In particular, if the property "O_L is free over its associated order" is true for L/K, then it is true for subextensions L'/K.

Bergé then derived from these investigations the structure of $\mathfrak{A}_{L/K}$, as well as certain criteria for freeness, for non totally ramified extensions (see e.g. [**7**], Cor. of Thm 2). For example, if L/K has cyclic inertia group and if $e_K = 1$, she proved that $\mathfrak{A}_{L/K}$ is included in the O_K-order of $K[G]$ generated by $O_K[G]$ and all the idempotents e_i attached to the ramification groups G_i. Moreover, the equality holds if and only if $\frac{rp}{p-1} - 1 \leq t_1$, where t_1 is the first ramification jump of L/K ([**7**], Cor. of Prop. 3 and Cor. 3 of Thm. 1). When this is the case, we say that the extension is almost maximally ramified. We shall come back on this notion in Subsection 5.1.

Finally, note that most of Bergé's results have been extended by Burns in [**33**].

3.3. Cyclic p-extensions. — We now consider a general p-adic field K, i.e., without any assumption on e_K. On such a field, there are several results for cyclic p-extensions, but only the case of extensions of degree p is completely solved.

3.3.1. Cyclic extensions of degree p.— Let L/K be a totally ramified cyclic extension of degree p. Contributions of Bergé, Bertrandias (F. and J.-P.) and Ferton in the 1970's culminated in a complete answer for such an extension: they determined an explicit description of the associated order $\mathfrak{A}_{L/K}$, obtained full criteria for O_L to be free over it, and described generators.

First, Bergé [**12**] and Bertrandias & Ferton [**17**] obtained independently and by different methods an explicit description of $\mathfrak{A}_{L/K}$ when L/K is a totally ramified cyclic extension of degree p;

Theorem 3.3 **(Bergé - Bertrandias & Ferton, 1972)**. — *Let K be a p-adic field, with uniformizing element π_K. Let L/K be a totally ramified extension of degree p. Let t be its unique ramification jump, and let σ be a generator of its Galois group. Write $f = \sigma - 1$. Then, the associated order of O_L in $K[G]$ is the O_K-submodule of $K[G]$ generated by the elements $\dfrac{f^i}{\pi_K^{n_i}}$ for $i = 0, ..., p-1$, where the integers n_i are given by:*

$$n_i = \lfloor \frac{it + \rho_i}{p} \rfloor,$$

with r_j the least non-negative residue of $-jt$ modulo p, and $\rho_i = inf_{i \leq j \leq p-1} r_j$.

Moreover, Bertrandias (F. and J.-P.) and Ferton ([**16, 17**]) determined explicitly when O_L is free over its associated order;

Theorem 3.4 **(F. Bertrandias - J.P. Bertrandias - M. J. Ferton, 1972)**
Let K be a finite extension of $\mathbb{Q}_p$. Let L/K be a totally ramified extension of degree p with ramification jump t.

1. *If $p|t$, then O_L is free over $\mathfrak{A}_{L/K}$.*
2. *If $p \not| t$, write $t = pk + a$ with $1 \leq a \leq p-1$, we have:*
   (a) *if $1 \leq t < \frac{pe_K}{p-1} - 1$, then O_L is $\mathfrak{A}_{L/K}$-free if and only if $a|p-1$;*
   (b) *if $t \geq \frac{pe_K}{p-1} - 1$, then O_L is $\mathfrak{A}_{L/K}$-free if and only if $N \leq 4$, where N denotes the length of the continued fraction expansion:*

$$\frac{t}{p} = a_0 + \cfrac{1}{a_1 + \dots \cfrac{1}{\dots + \cfrac{1}{a_N}}},$$

with $a_N \geq 2$.

Note that cases 2.(a) and 2.(b) are treated differently. Moreover, case 2.(b) is precisely when the extension is said to be almost maximally ramified (see Subsection 5.1 for further details). For an extension of degree p, this is equivalent to the condition where the idempotent $\frac{1}{p}\sum_{\sigma \in G} \sigma$ belongs to $\mathfrak{A}_{L/K}$.

When $e_K = 1$, then $t = 1 = a$ if $p \neq 2$, and $t = a = 1$ or $p|t$ if $p = 2$. In particular, case 2.(a) never happens. Therefore, if K is an absolutely unramified p-adic field, extensions of degree p over K are almost maximally ramified whenever $p \neq 2$, and they are such that O_L is $\mathfrak{A}_{L/K}$-free, according to cases 1 and 2.(b). In particular, we recover Leopoldt's theorem for cyclic extensions of degree p over $\mathbb{Q}_p$.

Moreover, the authors determined explicitly Galois generators for O_L, when it is free over $\mathfrak{U}_{L/K}$, in terms of t, p and a generator of G. They also deduced conditions of projectivity for integer rings in cyclic extensions of degree p of number fields ([**17**], Cor. 1).

3.3.2. Cyclic extensions of degree p^n.— Following these results, Bergé, Bertrandias (F.) and Ferton attacked the problem for cyclic extensions of degree p^n with $n \geq 2$, but this situation is more difficult. For $p = 3$, Bergé described the O_K-generators for the associated order in a particular extension of degree 9 with prescribed ramification jumps [**12**]. In parallel, Ferton obtained partial results for cyclic extensions of degree p^2 ([**86**], Par. 3).

In 1978 and 1979, Bertrandias (F.) generalized case 2.(b) of Theorem 3.4 to cyclic extensions of degree p^n when $p \not| e_K$[**15, 13**];

Proposition 3.5 **(Bertrandias, 1979 ([13], Thm. 4))**. — *Let K be a p-adic local field, with $p \not| e_K$. Let L/K be a totally ramified cyclic extension of degree p^n, with $p \geq 1$. Let t_i denote its ramification jumps, for $i = 1, \dots, n$. We suppose that the ramification is almost maximally ramified, i.e., that $t_i \geq \frac{p^i e_K}{p-1} - 1$, for all i. Then O_L is free over $\mathfrak{A}_{L/K}$ if and only if $N \leq 4$, where N is the length of the continued fraction expansion of t_1/p.*
Moreover, the structure of $\mathfrak{A}_{L/K}$, and Galois generators, are determined explicitly.

More than twenty years later, case 2.(a) of Theorem 3.4 was partially generalized to certain Kummer extensions by Miyata [**133**], with improvements by Byott in 2008 [**36**]. For such an extension L/K of degree p^n, the ramification jumps all lie in the same residue class modulo p^n. Write b for the least non negative residue of these jumps modulo p^n. In [**36**], Byott introduced a set

$$\mathcal{S}(p^n) \subset \{c \,:\, 1 \leq c \leq p^n - 1,\ p \nmid c\}.$$

The precise definition of this set is a little elaborate. However, a more easily defined set closely related to $\mathcal{S}(p^n)$ is $\mathcal{S}_0(p^n)$, with

$$\mathcal{S}_0(p^n) = \bigcup_{m=1,\ldots,n} \{c \,:\, c \text{ divides } p^m - 1\}.$$

In particular, $\mathcal{S}_0(p^n) \subset \mathcal{S}(p^n)$, with equality if $n \leq 2$, and in most cases when $n \geq 3$. The criterion of Miyata, reformulated by Byott, is then that O_L is free over $\mathfrak{A}_{L/K}$ if and only if $b \in \mathcal{S}(p^n)$.

Note also that Nigel Byott [**38**] had dealt with cyclic extensions of degree p^2 when $\mathrm{char}(K) = 0$ in 2002, in the language of Hopf algebras.

3.4. Lubin-Tate extensions. — Another extension of local fields for which the structure of the valuation ring over its associated order has been investigated are Lubin-Tate extensions. For background on Lubin-Tate theory, see for example [**142**].

Let K be a finite extension of $\mathbb{Q}_p$, and let q be the cardinality of its residue field. Let π be a uniformizing element of K. Let $f(X)$ be a Lubin-Tate series for K, corresponding to the parameter π, and let $F(X,Y)$ be the formal group admitting $f(X)$ as an endomorphism. Let $\mathfrak{m}$ be the maximal ideal of the valuation ring of a fixed algebraic closure of K, and, for all $n \geq 0$, set

$$G^{(n)} = \{\lambda \in \mathfrak{m} \,:\, f^{(n)}(\lambda) = 0\},$$

where $f^{(0)}(X) = X$ and $f^{(n)}(X) = f(f^{(n-1)}(X))$ for $n \geq 1$. Then, the division fields $K^{(n)}$ are defined by $K^{(n)} = K(G^{(n)})$. For every $n \geq 1$, the extension $K^{(n)}/K$ is totally ramified and abelian, of degree $q^{n-1}(q-1)$, and every element of $G^{(n)} \backslash G^{(n-1)}$ generates the maximal ideal of $O_{K^{(n)}}$. Furthermore, $K^{(1)}/K$ is cyclic of order $q-1$.

Just as the cyclotomic theory allows an explicit constructive treatment of class field theory for $\mathbb{Q}_p$, so the extensions K_n provide a constructive treatment of class field theory of totally ramified extensions for K [**142**]. This is probably the main motivation to consider the fields $K^{(n)}$ as good candidates for an investigation of integral Galois module structure, in the light of the theorem of Leopoldt. Interest in these questions arose from the work of Taylor [**150**], and its subsequent applications to CM fields.

Example 3.6. — Take $K = \mathbb{Q}_p$ and $\pi = p$. Consider $f(X) = (1+X)^p - 1$. Then $F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$, so the group operation is the usual multiplication with a change of variable to shift the identity from 1 to 0. Thus $F^{(n)} = \mathbb{Q}_p(\zeta_{p^n})$ for some primitive p^n-th root of unity ζ_{p^n}. In this sense, Lubin-Tate extensions can be presented as generalized cyclotomic extensions.

The integral Galois module structure of extensions of the form $K^{(m+r)}/K^{(r)}$ was considered in some detail ([**40, 41, 42, 55, 56, 149, 150**]), and there is now a complete theory for the Galois structure of the top valuation ring over its associated order in such an extension:

Theorem 3.7 **(Lubin-Tate extensions).** — *Let $m, r \geq 1$ be two integers. Let $O_{m,r}$ denote the valuation ring of $K^{(m+r)}$ and write $G_{m,r} := Gal(K^{(m+r)}/K^{(r)})$ for $m, r \geq 1$. We have:*

1. *if $m \leq r$, then $O_{m,r}$ is free over $\mathfrak{A}_{K^{(r)}}[G_{m,r}]$* [**150**] *;*
2. *if $m > r$ and $K = \mathbb{Q}_p$, then O_L is free over $\mathfrak{A}_{K^{(r)}}[G_{m,r}]$* [**55, 56**] *;*
3. *if $m > r$ and $K \neq \mathbb{Q}_p$, then O_L is not free over $\mathfrak{A}_{K^{(r)}}[G_{m,r}]$* [**42**].

Case 1 corresponds to the Kummer case. In cases 1 and 2, an explicit Galois generator is given, as well as the determination of the associated order (in case 2, $\mathfrak{A}_{K^{(r)}}[G_{m,r}]$ is determined by a "transport of structure" from the cyclotomic case [**56**]). Note also that if one take $\pi = p$ in case 2, we have a relative extension of cyclotomic fields, and the result was already proved in [**57**].

The proof of case 3 uses a study of the ramification jumps of the extension, and it doesn't provide any explicit determination of the associated order. However, in [**41**], Byott gives an explicit description of $\mathfrak{A}_{K^{(r)}}[G_{m,r}]$ when $r = 1$ and $m = 2$, under the additional assumption that the field K has absolute ramification index $e_K > q^2$. Similarly for the works of Bergé, Bertrandias and Ferton for certain cyclic p-extensions, this thus provides an infinite family of totally ramified extensions over local fields in which the valuation ring is not free over its associated order, but for which this order is known explicitly. This is worth noting, since orders and freeness are usually established simultaneously.

The investigation of the extensions $K^{(n)}/K$, with K itself as base field, probably started with the work of Byott [**39**]. In particular, for $n = 2$, he proved that O_L is not free over $\mathfrak{A}_{K^{(2)}/K}$, whenever $K/\mathbb{Q}_p$ is ramified and the residue field of K has cardinality at least 3. Byott also considered the integral Galois module structure of intermediate fields of $K^{(2)}/K$. He determined explicitly the associated orders in all cases, and when freeness holds he gave a generator. Today, we do not know whether this result has been generalized to other extensions $K^{(n)}/K$ with $n \geq 2$.

We close this section with the following remark. As noticed by Byott, there is a striking similarity to R. Miller's work [**129**], who considered the corresponding problem for function fields in characteristic p, where Lubin-Tate formal groups are replaced with Carlitz modules. We shall come back on this setting in subsection 4.3.

3.5. Elementary abelian extensions. — In characteristic 0, few results are known for elementary abelian extensions. In 2007, Miyata gave conditions for the valuation ring not to be free over its associated order when L/K is a totally ramified abelian Kummer extension of the type $L = K(\alpha, \beta)$, where α and β are suitably normalized elements with $\alpha^p, \beta^p \in K$ and such that $K(\alpha)/K$ and $K(\beta)/K$ have ramification numbers t in the range $2p < t < pe_K/(p-1)$ ([**130**], Theorem 5).

3.6. Dihedral extensions. — We suppose now that $L/\mathbb{Q}_p$ is a dihedral extension of degree $r2p$, with $p \neq 2$ and $p \not| r$. We suppose that the inertia group is cyclic, which happens whenever $r \geq 3$. In [**9**], Bergé proved that O_L is free over its associated order if and only if $r < p$. In [**86**], Ferton investigated the case of dihedral extensions of degree $2p$. This case is also derived from works of Bergé (see e.g [**7**] and [**10**],).

4. Local Galois module structure in equal characteristic

When the local field K is of characteristic p and the extension L/K is of order a power of p, the group algebra $K[G]$ is a local ring whose maximal ideal is its augmentation ideal, i.e., the left ideal generated by all $\sigma - 1$ when σ runs through G (Thm. 19.1 of [**121**]). Moreover, it has a unique minimal left ideal, which is generated by the trace element $\sum_{\sigma \in G} \sigma$ (see e.g. [**153**], Chap. 3).

In this setting, the associated order $\mathfrak{A}_{L/K}$ is a local ring as well, and there exists a canonical isomorphism between $\mathfrak{A}_{L/K}/\mathfrak{m}\mathfrak{A}_{L/K}$ and the residue field k of K, if $\mathfrak{m}$ denotes the unique maximal ideal of $\mathfrak{A}_{L/K}$ ([**154**], Prop. 5.10 and Cor. 5.2).

4.1. Cyclic extensions of formal power series fields. — Over a local field K of characteristic p, the Galois module structure of the top valuation ring has been entirely solved for cyclic extensions of degree p. Precisely, let L/K be a totally ramified extension of degree p. We denote by t its unique ramification jump: it is prime to p and we write $t = pk + a$ with $1 \leq a \leq p-1$. Recall that, by Artin-Schreier theory, one can find $A \in K$ such that $L = K(\alpha)$ with $\alpha^p - \alpha = A$ and $v_K(A) = -t$.

In 2003, Aiba established the following criterion [**1**], which was precised by Lettl [**118**]:

Proposition 4.1 **(Aiba, 2003 - Lettl, 2005)**. — *The valuation ring O_L is $\mathfrak{A}_{L/K}$-free if and only if a divides $p-1$.*

This criterion is the same as the one given by Bertrandias (F.) and Ferton [**17**] for the corresponding problem in characteristic 0. Note also that it is based on the following property derived from ([**3**], Lemma 1) and ([**1**], Lemma 2), and which characterises p-extensions in characteristic p:

Lemma 4.2 **(Aiba, 2003)**. — *Suppose L/K is an abelian p-extension with Galois group G. If O_L is $\mathfrak{A}_{L/K}$-free, then $O_L = \mathfrak{A}_{L/K} \cdot \alpha$ if and only if $Tr_{L/K}(\alpha)$ divides $Tr_{L/K}(\beta)$ for any $\beta \in O_L$.*

Then, in 2005, Proposition 4.1 was made more explicit and reinterpreted in algebraic terms by the author in her Ph.D. [**154**]. Precisely, let $\mathrm{edim}(\mathfrak{A}_{L/K}) := \dim_k \mathfrak{m}/\mathfrak{m}^2$ denote the embedding dimension of $\mathfrak{A}_{L/K}$. She proved that O_L is $\mathfrak{A}_{L/K}$-free if and only if $\mathrm{edim}(\mathfrak{A}_{L/K}) \leq 3$ ([**154**], Thm. 5.2, Prop. 5.23).

Finally, de Smit and the author [**144**] generalized these criteria by computing efficiently the minimal number of $\mathfrak{A}_{L/K}$-module generators of O_L from p and t with a continued fraction expansion. In particular, this provides an algorithm that given p and a computes d in polynomial time, i.e., in time bounded by a polynomial in $\log(p)$. The main result is the following. Note that, in this case, the continued fraction expansion of $-a/p$, instead of $+a/p$ (comparing with Theorem 3.4), codes the Galois structure of the ring O_L; moreover, the criterion is based on the values of the coefficients of this expansion, instead of its length.

***Theorem 4.3* (de Smit & Thomas, 2007).** — *Let K be a local field of characteristic p, and let L/K be a totally ramified cyclic extension of degree p. Let t be the unique ramification jump of L/K, and write $t = pk + a$ with $1 \leq a \leq p-1$. Let d be the minimal number of $\mathfrak{A}_{L/K}$-generators of O_L. Then $d = 1$ if and only if O_L is $\mathfrak{A}_{L/K}$-free, and we have;*

1. *if $a = p-1$, then $d = 1$ and $edim(\mathfrak{A}_{L/K}) = 2$;*
2. *if $a < p-1$, then $edim(\mathfrak{A}_{L/K}) = 2d+1$ and $d = \sum_{i\ odd, i<n} a_i$, where the coefficients a_i's are the unique integers given by*

$$-\frac{a}{p} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \, \cfrac{\ddots}{a_{n-1} + \cfrac{1}{a_n}}}}$$

with $a_1, ..., a_n \geq 1$ and $a_n \geq 2$. In particular, O_L is $\mathfrak{A}_{L/K}$-free if and only if $a|(p-1)$.

Moreover, in all cases, a set of O_K-generators for $\mathfrak{A}_{L/K}$ and a minimal set of $\mathfrak{A}_{L/K}$-generators for O_L are given explicitly.

The proof has two basic ingredients: graded rings and balanced sequences. Precisely, the associated order $\mathfrak{A}_{L/K}$ is given the structure of a graded ring and O_L the structure of a graded module over it. The proof is then based on an explicit combinatorial description of the gradings on $\mathfrak{A}_{L/K}$ and O_L in terms of the balanced sequence associated to the fraction $\frac{a}{p}$.

It is worth noting that this result is probably the first one where the minimal number of $\mathfrak{A}_{L/K}$-generators of O_L is given in the case of non freeness, whereas previous works in this direction had concentrated only on determining when O_L is $\mathfrak{A}_{L/K}$-free. Moreover, the explicit use of combinatorics, through subtle properties of the sequence $\{\lceil \frac{ia}{p} \rceil\}_{i\geq 1}$, is very intriguing and constitutes another novel approach of the authors.

These contributions also prove that there is no Leopoldt type result over $\mathbb{F}_p((T))$ since one can derive infinitely many cyclic extensions over $\mathbb{F}_p((T))$ for which the valuation ring is not free over its associated order. Indeed, for any prime number p, if $t > 0$ is a positive integer such that $p \nmid t$ and $a \nmid (p-1)$ (a is the least non negative residue of t modulo p), then the extension $L/\mathbb{F}_p((T))$ given by $L = \mathbb{F}_p((T))(\alpha)$ with $\alpha^p - \alpha = T^{-t}$ is cyclic of order p and such that O_L is not free over its associated order.

The consideration of cyclic p-extensions of higher degree in positive characteristic is still in progress.

4.2. Elementary abelian extensions. — In parallel, Byott and Elder have obtained results for a family of elementary abelian extensions [**44**], and obtained a criterion which agrees with the condition found by Miyata for certain Kummer extensions in characteristic 0 [**36, 133**]).

For these extensions, it is the existence of a particularly well-behaved "Galois scaffold" that allows the structure of the top valuation ring over its associated order to be determined. Such structure was introduced by Elder [**77**], it corresponds to some variant of a normal basis that allows for an easy determination of valuation and thus has implications for the questions of the Galois module structure. Byott and Elder develop the idea to use it to determine a necessary and sufficient condition for O_L to be free over its associated order for larger classes of extensions in mixed and equal characteristic.

4.3. Note on the function Field case. — Since function fields can be viewed as the globalisation of local fields of positive characteristic, it is natural to consider analogue Galois module structure questions for extensions of such fields.

Let p be a prime number, and let q be a power of p. Let $K = k(T)$ be a global function field over the finite field $k = \mathbb{F}_q$ of characteristic p. One can think of K as being the set of functions defined over k of a certain projective nonsingular curve $\mathcal{C}$ defined over k. In general, there is no canonical way to define a ring of integers O_K for K. To study integral Galois module structure, we fix a finite non-empty set S of places of K, and we let $O_K = O_{K,S}$ be the set of all $x \in K$ having no pole outside S. If L is a finite extension of K, then we let O_L be the integral closure of O_K in L. Let L/K be a finite Galois extension with Galois group G; we can consider O_L as an $O_K[G]$-module and investigate its structure. We can also be interested in the existence of analogue results between the number field case and the function field case, when $\mathbb{F}_q(T)$ plays the same role as $\mathbb{Q}$.

Recall that we derived Noether's criterion from Theorem 1.1 and Swan's Theorem. Now, Swan's theorem was originally stated for modules over group algebras $A[G]$, when e.g. G is abelian or the ring A has characteristic 0. According to Martinet, in a private communication, this also holds in positive characteristic once the order of the group G is prime to $\mathrm{char}(A)$. However, for general extensions of function fields of characteristic p, we can derive a Noether's criterion from the local case. Indeed, the ring of integers O_L is locally free over its associated order $\mathfrak{A}_{L/K}$ if and only if each completion $O_{L,\mathfrak{p}}$ is free over its associated order in the corresponding local extension. Then, using the characterisation of tameness of the trace being surjective at integral level, and since taking the trace commutes with completion, we deduce that O_L is locally free over $O_K[G]$ if and only if the extension is at most tamely ramified.

First, if G has order prime to p, tameness is automatic and Chapman gave a version of the "Hom-description" of Fröhlich for the class group of locally free $O_K[G]$-modules [**58**]. Furthermore, if G is cyclic, Chapman used class field theory and Kummer theory to calculate the isomorphism classes explicitly.

Then, Ichimura proved the converse of Noether's criterion, in the particular case where G is an abelian p-group. Precisely, if L/K is a finite abelian p-extension, then Ichimura proves that O_L is free over $O_K[G]$ if and only if L/K is unramified outside S. The method of the proof is quite explicit. Since the problem reduces to the case where G is cyclic, one can suppose L/K

to be cyclic, in which case it can be described explicitly in terms of Witt vectors. This allows a free generator of O_L as an $O_K[G]$-module to be written down.

In the particular case where $O_K = \mathbb{F}_q[T]$, i.e., $S = \{\infty_T\}$, Chapman gave a constructive proof of an analogue of the Hilbert-Speiser theorem ([**59**],Theorem 1). This result is based on an analogue of the Kronecker-Weber theorem for function fields due to Carlitz and Hayes [**107**]: all abelian extensions of $\mathbb{F}_q(T)$ can be obtained by adjoining roots of unity, division points of the Carlitz module for $\mathbb{F}_q[T]$, and division points of the Carlitz module for $\mathbb{F}_q[\frac{1}{T}]$. The result of Chapman is the following;

Theorem 4.4 **(Chapman, 1991)**. — *If $L/\mathbb{F}_q(T)$ is a finite abelian extension which is wildly ramified at no prime of $O_K = \mathbb{F}_q[T]$, then O_L is a free module of rank 1 over the group ring $O_K[G]$. Moreover, a generator can be constructed explicitly.*

Note that normal integral bases can be afforded by Thakur's analogue of Gauss sums, using a Carlitz module.

When raising the bottom field K to a finite extension, the situation is more difficult. In [**4**], Anglès investigated the existence of integral normal bases for intermediate extensions of a tame cyclotomic extension over $\mathbb{F}_q[T]$. Precisely, let $K \subset M \subset N \subset L$ be a tower of extensions over the function field $K = \mathbb{F}_q(T)$. Suppose that the field L is obtained by adjoining to K the P-division points of the Carlitz module, for some irreducible polynomial $P \in \mathbb{F}_q[T]$ (we say that L is a cyclotomic function field). Anglès gave several sufficient conditions for N/M to be without normal integral basis. In particular, if $p \neq 2$ and if M is the quadratic subfield of L/K, then N/M has a normal integral basis if and only if the polynomial $P \in \mathbb{F}_q[T]$ defining L/K has degree at most 2. This provides some analogue of results of Brinkhuis and Cougnard for cyclotomic extensions of number fields.

Finally, for wild extensions of function fields, the analogue of Leopoldt's theorem on $\mathbb{F}_q(T)$ is no longer true for function fields since it is not true for wild extensions of the local field $\mathbb{F}_p((T))$ (see Subsection 4.1). Aiba obtained another counter example which is more elaborate. Let L/K be a finite Galois extension of function fields with Galois group G, and let O_L be the integral closure of O_K in L. One can define the associated order of O_L in $K[G]$ as $\mathfrak{U}_{L/K} = \{\lambda \in K[G] \ : \ \lambda O_L \subset O_L\}$, and study the structure of O_L as a module over it. If $K = \mathbb{F}_q(T)$ and $O_K = \mathbb{F}_q[T]$, Aiba constructed examples of extensions $L/\mathbb{F}_q(T)$ for which O_L is not free over its associated order using Hayes modules [**3**]. Moreover, for certain extensions of cyclotomic function fields L/K, Aiba also investigated an analogue of a result of Chan and Lim [**57**] on cyclotomic number fields. In particular, in [**2**], he found the existence of conditions for O_L not to be free over its associated order, contrary to the characteristic 0 case.

5. Further comments

5.1. On the maximality of associated orders. — Let K be a local field of residue characteristic p and L/K be a finite abelian p-extension over K, with Galois group G. In this section, we consider the question of whether the associated order of O_L in $K[G]$ is a maximal order, which might help in the investigation of the Galois module structure of O_L. Most of the required information about maximal orders is contained in [**140**].

If K has characteristic p, the algebra $K[G]$ has no maximal order. This is due to the fact that the K-algebra is not separable (see e.g. [**154**], Prop. 5.9).

When K has characteristic 0, and since G is abelian, the algebra $K[G]$ contains a unique maximal O_K-order $\mathfrak{M}$; it is the integral closure of O_K in $K[G]$([**140**], remark after Theorem 8.6). The Wedderburn decomposition of $K[G]$ into simple K-algebras is $K[G] = \oplus K[G]e_\chi$, where the e_χ are primitive idempotents indexed by a set of representatives for the classes of characters of G which are conjugate under the action of the absolute Galois group of K. This yields the decomposition $\mathfrak{M} = \oplus \mathfrak{M}e_\chi$ and each $\mathfrak{M}e_\chi$ is the maximal order of $K[G]e_\chi$. Therefore, $\mathfrak{M}$ is the O_K-module generated by the group ring $O_K[G]$ and idempotents of $K[G]$.

Moreover, each summand $K[G]e_\chi$ is isomorphic to a cyclotomic field K_χ, with $K_\chi = K(\zeta_m)$ if m is the order of χ and ζ_m a primitive mth root of unity. Therefore, $\mathfrak{M} \simeq \prod_{\chi\in\Gamma_K} \mathfrak{M}_\chi$, where $\mathfrak{M}_\chi$ is the valuation ring of K_χ. In particular, the components $\mathfrak{M}_\chi$ are principal ideal domains, so that, if the associated order $\mathfrak{A}_{L/K}$ equals $\mathfrak{M}$, then O_L is free over it. The equality $\mathfrak{A}_{L/K} = \mathfrak{M}$ thus provides a condition of freeness.

5.1.1. Criteria for $\mathfrak{A}_{L/K} = \mathfrak{M}$.— Since L/K is abelian, the associated order $\mathfrak{A}_{L/K}$ can only equal the maximal order $\mathfrak{M}$ if the extension is cyclic. As noticed by Byott, this can be shown using Frohlich's notion of "factorisability" [**91**]. See also Corollary 1.8 of [**33**]. One can also prove it in a more restrictive context, using some other criteria to determine whether O_L is $O_K[G]$-indecomposable.

Indeed, one necessary condition for $\mathfrak{A}_{L/K}$ to coincide with $\mathfrak{M}$ is that it must contain some nontrivial idempotents. On the other hand, the ring O_L is indecomposable as an $O_K[G]$-module if it cannot be written as a direct sum of two non-zero $O_K[G]$-submodules. This amounts to the fact that the ring of $O_K[G]$-endomorphisms of O_L contains no nontrivial idempotents. But since G is supposed to be abelian, this ring is precisely the associated order $\mathfrak{A}_{L/K}$. Hence, if $\mathfrak{A}_{L/K} = \mathfrak{M}$, then O_L is $O_K[G]$-decomposable. Vostokov and Miyata have investigated criteria for O_L to be $O_K[G]$-indecomposable [**131, 159**].

For example, if L/K is an abelian p-extension, and if the order of the first ramification group G_1 does not divide the different, then O_L is $O_K[G]$-indecomposable, and so $\mathfrak{A}_{L/K} \neq \mathfrak{M}$. This comes from the fact that if the order of G_1 divides the different, then the associated order contains the central idempotent attached to the trace element for G_1. In particular, if L/K has ramification index p^n, and if its biggest ramification jump t_m satisfies $t_m - \lfloor \frac{t_m}{p} \rfloor \leq p^{n-1}e_K$, then O_L is indecomposable as an $O_K[G]$-module ([**160**], Theorem 4). For $p \geq 3$, Byott proved that if this condition does not hold, then L/K is cyclic ([**42**], Prop. 3.7).

5.1.2. Link with almost maximal ramification.— Bertrandias investigated the $O_K[G]$-decomposability of O_L when L/K is a cyclic extension of degree p [**13**]. In particular, she proved that O_L is $O_K[G]$-decomposable if and only if the idempotent $\frac{1}{p}\mathrm{Tr}_{L/K}$ belongs to

$\mathfrak{A}_{L/K}$, and, when this is true, she described the decomposition of O_L into indecomposable $O_K[G]$-submodules in terms of the value of the ramification jump t modulo p ([**13**], Thm. 2 and Thm. 3). Moreover, she proved that the condition is actually equivalent to the double inequality $\frac{p}{p-1}e_K - 1 \leq t \leq \frac{p}{p-1}e_K$: we say that the extension is almost maximally ramified.

The notion of almost maximal ramification is due to Jacobinski [**111**]. An extension L/K with Galois group G is said to be almost maximally ramified if all idempotents $e_H = \frac{1}{|H|}\sum_{\sigma\in H}\sigma$ belong to the associated order $\mathfrak{U}_{L/K}$, when H run over all subgroups of G included between two consecutive ramification groups of the extension.

When L/K is a totally ramified cyclic extension of degree p^n, this is equivalent to the following conditions (see e.g. [**7**], Cor. of Prop. 3, and [**13**], Prop. 1). For each integer i, $0 \leq i \leq n$, write H_i for the subgroup of G of order p^i, and put $e_i = e_{H_i}$. Clearly, the groups $H_i's$ are the ramification groups of the extension. Moreover, each e_i is an idempotent of $K[G]$, and $p^i e_i$ coincides with the trace of the extension $L/L^{H_{n-i}}$. We also write $t_1 < t_2 < ... < t_n$ for the n ramification jumps of L/K.

Proposition 5.1. — *The extension L/K is almost maximally ramified if and only if it satisfies one of the following equivalent conditions:*

1. *$e_H \in \mathfrak{A}_{L/K}$ for all subgroups $H \subset G$ included between two consecutive ramification groups;*
2. *$e_i \in \mathfrak{A}_{L/K}$ for all $i \in \{1, ..., n\}$;*
3. *$\dfrac{p^i e_K}{p-1} - 1 \leq t_i \leq \dfrac{p^i e_K}{p-1}$ for all $i = 1, 2, ..., n$;*
4. *$t_i = \dfrac{p^i e - a}{p-1}$ for all i, where a is the least non-negative residue modulo p of t_1.*

Note that, in this context, if we set $e'_0 = e_n$ and $e'_i = e_{n-i} - e_{n-i+1}$, then the e'_i are orthogonal idempotents whose sum is 1, and $K[G] = \oplus_{0\leq i\leq n} K[G]e'_i$.

Suppose now that K is absolutely unramified ($e_K = 1$), and that the extension L/K is cyclic and totally ramified, of order rp^n with $p \not| r$. In 1978, Bergé obtained an explicit description of the maximal order $\mathfrak{M}$ of $K[G]$: this is the O_K-module generated by $O_K[G]$ and the idempotents e_i ([**7**], Proposition 5). Moreover, the equality $\mathfrak{A}_{L/K} = \mathfrak{M}$ holds if and only if the extension is almost maximally ramified ([**7**], Corollary 3 of Theorem 1).

When K is not absolutely unramified, almost maximal ramification is not sufficient for $\mathfrak{A}_{L/K}$ to equal the maximal order $\mathfrak{M}$. If L/K is cyclic of order p^n, this is due to the fact that, in this setting, the idempotents e_i defined above are not sufficient to generate the maximal order $\mathfrak{M}$ of $K[G]$. As a consequence of Theorem 3.4, Bertrandias (F. and J.-P.) and Ferton obtained the following criterion for a cyclic extension of degree p ([**16**], Theorem 2);

Proposition 5.2 **(Bertrandias & Bertrandias & Ferton, 1972)**
Let K be a local field of mixed characteristic $(0, p)$. Let L/K be a totally ramified extension of degree p, with Galois group G. Let t be its ramification jump; let a be its least non-negative residue modulo p. Then $\mathfrak{A}_{L/K}$ coincides with the maximal order $\mathfrak{M}$ in $K[G]$ if and only if the

extension is almost maximally ramified and a satisfies one of the following conditions :

$$a = 0 \quad ou \quad a|(p-1) \quad ou \quad a|p-2 \quad ou \quad a|2p-1.$$

5.1.3. Number field case.— These considerations still hold for extensions of number fields. As an illustration, let us mention the following criterion due to Byott and Lettl, where the assumption on linear disjointness is crucial;

***Proposition 5.3* (Byott-Lettl, 1996 [48]).** — *Let L/K be a cyclic and totally ramified extension of number fields. Suppose it is linearly disjoint to $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, where m denotes the conductor of K. Then $\mathfrak{A}_{L/K}$ is the maximal order of $K[G]$.*

Is the associated order a local ring ? The previous consideration also lead us to the question whether the associated order is a local ring. For an abelian p-extension L/K, this always holds when $\mathrm{char}(K) = p$ (see e.g. [**154**], Prop. 5.10). In zero characteristic, this is related to the existence of nontrivial idempotents as well, and one can prove that if O_L is $O_K[G]$-indecomposable, then $\mathfrak{A}_{L/K}$ is a local ring. According to ([**42**], Prop. 3.7),the condition that $\mathfrak{A}_{L/K}$ is a local ring is thus very weak.

5.2. Hopf structures in Galois module theory. — The use of Hopf theory is another one of the most innovative approaches to the wild situation in recent years. This idea, initiated by Fröhlich, was developed by Taylor and Childs in the mid 1980's to solve Galois module questions for extensions of local fields of unequal characteristic. Hopf orders had first been considered by people studying group schemes (Tate, Oort, Raynaud, Larson). Most of the contributions towards the connection between Hopf orders and Galois module structure are due to Byott, Childs, Greither, Pareigis and Taylor. For more details about this theory, we refer the reader to [**60**]. Among other investigations of the relation between Hopf orders and Galois module structure, one should cite, e.g., the recent contributions of Agboola, Bley & Boltje, Miyata and Truman.

If R is a commutative ring, a Hopf R-algebra is an R-bialgebra with antipode. It is said to be finite if it is finitely generated and projective as an R-module. If L/K is a finite Galois extension of number fields or of local fields of mixed characteristic $(0, p)$, the group ring $K[G]$ provides the easiest example of a Hopf algebra. We then call a Hopf order any sub Hopf algebra of $K[G]$ which is also an O_K-order in $K[G]$.

In 1985, Taylor considered local extensions constructed using division points of Lubin-Tate formal groups [**150**]: using the formal group structure, he gave an explicit description of the associated order, and showed that the top valuation ring was free over it. Then, in 1987, he generalised and reinterpreted this in terms of Kummer theory with respect to the formal group [**149**]. In particular, he made it explicit that the construction works because the associated order is a Hopf order.

More generally, Childs and Moss proved the following criterion [**61, 62**];

***Theorem 5.4* (Childs - Moss, 1994).** — *Let L/K be a finite Galois extension of p-adic fields or of number fields, with Galois group G. If the associated order $\mathfrak{A}_{L/K}$ of O_L is a Hopf order in $K[G]$, then O_L is $\mathfrak{A}_{L/K}$-free of rank one.*

The converse is false. Indeed, there are many wildly ramified Galois extensions L/K whose valuation rings are free over their associated order $\mathfrak{A}_{L/K}$ but $\mathfrak{A}_{L/K}$ is not a Hopf order (see Theorem 5.1 of [**61**] and its corollaries).

In parallel, Greither and Pareigis [**106**] proved that L is also an H-Hopf Galois extension of K for various K-Hopf algebras H (the terminology means that L is an H-module algebra); one of them is the group algebra $K[G]$. If the field extension is one of p-adic fields, one can define the associated order in each Hopf-Galois structure, prove that Theorem 5.4 still holds, and compare freeness results between them. For example, Childs did this for cyclic extensions of degree p^2; Byott then did the same for elementary abelian extensions of degree p^2 [**38**]. It can happen that the valuation ring is free over its associated order with respect to some non-classical Hopf-Galois structure, whereas it is not free in the classical case.

In 1992, Greither essentially classified most of the Hopf orders in the group algebra $K[\mathbb{Z}/p^2\mathbb{Z}]$ for a p-adic field K, and found which of them occur as associated orders of valuation rings. Independently to this, Byott found almost all the Hopf orders in both $K[\mathbb{Z}/p^2\mathbb{Z}]$ and $K[\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}]$, including some excluded by Greither's hypothesis. Furthermore, in 2004, Byott determined all Hopf-Galois structures on Galois extensions of fields of degree pq, where p, q are distinct primes such that $q \equiv 1 (\mathrm{mod}\ p)$ [**37**].

Moreover, for an abelian p-extension of p-adic fields, Bondarko proved that if the top valuation ring is free over its associated order, then the associated order must be a Hopf order and the extension can be produced from a one-dimensional formal group [**25**]. In [**42**], Byott investigates the ramification numbers of abelian p-extensions L/K for which the associated order of O_L is a Hopf order in $K[G]$.

Finally, Hopf structures have been investigated in certain p-extensions of degree p^n by Miyata [**131**] and Byott (see e.g. [**36, 38, 42**]). One recent result is the following;

***Theorem 5.5* (Byott, 2008).** — *If K is a p-adic field and L/K a Kummer extension of degree p^n of the form $L = K(\alpha)$ with $\alpha^{p^n} \in K$ and $v_K(\alpha - 1) > 0$, $v_K(\alpha - 1)$ coprime to p. Then $\mathfrak{A}_{L/K}$ is a Hopf order if and only if $a = p^n - 1$, where a denotes the least non-negative residue of the first ramification jump modulo p^n.*
Moreover, if $p^n/2 < a < p^n - 1$, then O_L is not free over its associated order.

5.3. Valuation criteria for normal basis generators. — Investigating the algebraic structure of the top valuation ring over its associated order in abelian elementary p-extensions, Byott and Elder [**45**] raised the question of the existence of a valuation criterion for normal basis generators of some extension L/K of local fields, i.e., of the existence of an integer v such that every element $x \in L$ with valuation v generates a normal basis for L/K.

If $\mathrm{char}(K) = p$, Elder and the author proved that every totally ramified p-extension of K satisfies such a valuation criterion, for a prescribed value of v;

***Theorem 5.6* (Thomas 2008, Elder 2010).** — *Let K be a local field of characteristic p and let L/K be a totally ramified p-extension. Write d for the valuation of the different of the extension. Then each element $x \in L$ with valuation congruent to $-d-1$ modulo $[L:K]$ is a normal basis generator for L/K.*

Nigel Byott has reinterpreted this result in terms of Hopf-Galois structures [**35**].

Florence, de Smit and the author have just solved the question entirely in all characteristics [**89**]. Let L/K be a finite Galois extension of local fields. To simplify, say that $VC(L/K)$ holds if L/K satisfies a valuation criterion for normal basis generators. They first proved that $VC(L/K)$ holds if and only if the tamely ramified part of the extension L/K is trivial and every non-zero $K[G]$-submodule of L contains a unit. Moreover, the integer v can take one value modulo $[L:K]$ only, namely $-d_{L/K}-1$, where $d_{L/K}$ is the valuation of the different of L/K. When K has positive characteristic, they recover the result of Elder and the author. When $\mathrm{char}(K)=0$, they identify all abelian extensions L/K for which $VC(L/K)$ is true, using algebraic arguments. These extensions are determined by the behaviour of their cyclic Kummer subextensions.

Therefore, one can then address the question of the existence of a valuation criterion for Galois generators of valuation rings over their associated orders, when they are free. Several results in this direction have now been obtained, and the existence of such a criterion can also provide arguments to determine non-freeness results. Note also that the $\mathfrak{U}_{L/K}$-generators of O_L founded for cyclic extensions L/K of degree p in both characteristic cases 0 and p (according to the results of Subsection 3.3 and 4.1) satisfy the valuation criterion of Florence, de Smit and the author.

5.4. Galois module structure of ambiguous ideals. — Let L/K be a finite Galois extension of number fields or local fields, with Galois group G. Instead of investigating the Galois module structure of the integer ring O_L, one can consider ambiguous ideals, i.e., fractional ideals of L that are stable under the action of G. In particular, if $\mathfrak{a}$ is such an ideal, one may define its associated order in $K[G]$ by:

$$\mathfrak{A}_{L/K}(\mathfrak{a}) = \{\alpha \in K[G] \;:\; \alpha\mathfrak{a} \subset \mathfrak{a}\}.$$

Similarly to the ring O_L, $\mathfrak{a}$ is a module over $\mathfrak{A}_{L/K}(\mathfrak{a})$ and one can address the question of whether it is free. In what follows, we give a brief account of the investigation that has been done on this subject when K is a p-adic field. In this case, every fractional ideal of L is ambiguous.

If the extension L/K is tame, then $\mathfrak{A}_{L/K}(\mathfrak{a}) = O_K[G]$ ([**11**], Thm. 1). Now, whereas the relation $\mathfrak{A}_{L/K}(O_L) = O_K[G]$ characterizes tamely ramified extensions (see Subsection 1.3), this is false if we replace O_L with another ambiguous ideal. Indeed, in ([**11**], Par. I.3), Bergé gives the following counter-example. If $L = \mathbb{Q}_2(i)$ with $i^2 = -1$, and if $\mathfrak{a} = (1+i)O_L$, then the extension $L/\mathbb{Q}_2$ is wildly ramified whereas $\mathfrak{A}_{L/K}(\mathfrak{a}) = \mathbb{Z}_2[G]$.

Moreover, when K is a local field, Ullom proved that if he extension L/K is tame, then every ambiguous ideal of L is a free $O_K[G]$-module [**155**]. An explicit set of generators for each ideal can be derived from the construction of normal integral bases by Kawamoto [**113**].

If L/K is wild, the situation is very different, and only special cases are known. First, Ullom showed that the freeness of any ambiguous ideal $\mathfrak{a}$ of L over $O_K[G]$ is a strong restriction on both the ramification of L/K and the L-valuation of $\mathfrak{a}$ ([**156**], Theorem 2.1). He also proved that if an ambiguous ideal in L is free over $O_K[G]$, then L/K must be weakly ramified, i.e., its second ramification group is trivial [**156**].

The Galois module structure of ambiguous ideals over their associated orders has been investigated for cyclic extensions. Suppose first that L/K is an extension of degree p. Write t for the unique ramification jump of L/K, and $\mathfrak{P}_L$ for the maximal ideal of O_L. In [**87**], Ferton characterized the ideals $\mathfrak{P}_L^r$ of O_L which are free over their associated order, in terms of the values of t and r. Her results generalized Theorem 3.4. In particular, answering a question of Jacobinski, she proved that every ideal $\mathfrak{P}_L^r$ such that $r \equiv t \bmod(p)$ is free over its associated order. Note that two ideals $\mathfrak{P}_L^r$ and $\mathfrak{P}_L^{r'}$ have the same associated order if $r \equiv r' (\bmod\ p)$. Later, in [**33**], and under the assumption that $e_K = 1$, Burns proved that if L/K is a cyclic extension of order $p^n r$ with $p \nmid n$, then O_L is free over its associated order if and only if there exists a fractional ideal of L which is free over its associated order, and this happens if and only if $n = 1$, or $n = 2$ and $r < p^2$, or $n > 2$ and $r < p(p-1)$ (Thm. 3 of [**33**]). See also Lemma 1.1 of [**32**].

Finally, in [**32**], Burns gave an almost complete answer to the question when L/K is a finite totally ramified abelian extension of p-adic fields, for an odd prime p, extending [**7**], [**155**] and [**33**]. A key tool is the notion of factorisability introduced by Fröhlich [**91**], as well as the factorisable quotient function, introduced by Burns in 1991 [**33**] and which allows the question of whether $\mathfrak{a}$ is free over its associated order to be answered by computing module indices. Note that an appendix by W. Bley describes an algorithm to determine whether an ambiguous ideal in the ring of algebraic integers in a number field is locally or globally free over its associated order.

In particular, denoting by G the Galois group of L/K, Burns investigated the structure of fractional ideals of L, $\mathfrak{a}$, over their associated order in $\mathbb{Q}_p[G]$, i.e., over $\mathfrak{A}_{\mathbb{Q}_p[G]}(\mathfrak{a}) := \{\lambda \in \mathbb{Q}_p[G] \ : \ \lambda\mathfrak{a} \subset \mathfrak{a}\}$. When K is ramified over $\mathbb{Q}_p$, there are only two types of extensions for which there is an ideal free over its associated order in $\mathbb{Q}_p[G]$: the weakly ramified extensions, and the cyclic extensions that are almost maximally ramified. When $K/\mathbb{Q}_p$ is unramified, the result is much more complicated, and Burns investigated necessary conditions on the existence of ideals free over their associated orders in $\mathbb{Q}_p[G]$ in terms of the ramification jumps.

We now develop two examples of the Galois module structure of ambiguous ideals.

5.4.1. Galois module structure of the inverse different.— Let L/K be a totally ramified abelian extension of degree p^n with Galois group G. We denote by $b_1 \leq b_2 \leq \dots \leq b_n$, with $b_1 \geq 1$ and possibly $b_i = b_{i+1}$ for some i, the ramification jumps of L/K, and let $e_K = v_K(p)$ be the absolute ramification index of K. Let $\mathcal{D}_{L/K}^{-1}$ be the inverse different of L/K, defined by:

$$\mathcal{D}_{L/K}^{-1} = \{x \in L \ : \ \mathrm{Tr}_{L/K}(xO_L) \subset O_L\}.$$

In ([**42**], Theorem 3.10), Byott proved the following:

***Theorem 5.7* (Byott,1997).** — *If $b_n - \lceil \frac{b_n}{p} \rceil \neq p^{n-1}e_K$, and if $b_i \not\equiv -1 \pmod{p^n}$ for some i, then $\mathcal{D}_{L/K}^{-1}$ is not free over its associated order.*

5.4.2. Square root of the inverse different.— In the global case, the study of the $\mathbb{Z}[G]$-structure of other G-stable ideals of O_L began in a special case in [**85**], where Erez studied the square root of the inverse difference of some extensions of number fields answering a question of Conner and Perlis. Let L/K denote an odd degree Galois extension of number fields. By Hilbert's formula for the valuation of the different $\mathcal{D}_{L/K}$ of L/K, there exists a fractional ideal $\mathcal{A}_{L/K}$ of the ring of integers O_K of K such that:

$$\mathcal{A}_{L/K}^2 = \mathcal{D}_{L/K}^{-1} \ .$$

This ideal is known as the square root of the inverse different. It is an ambiguous ideal. As an analogue of Noether's criterion, Erez showed $\mathcal{A}_{L/K}$ to be locally free if and only if L/K is weakly ramified, i.e., if the second ramification group of any prime ideal $\mathfrak{p}$ of O_L is trivial [**83**]. Moreover, in [**82**], Erez and Taylor proved that when L/K is at most tamely ramified, then $\mathcal{A}_{L/K}$ is always free over $\mathbb{Z}[G]$. For a precise account on the Galois module structure of the square root of the inverse different until 1991, see [**84**].

The question of whether $\mathcal{A}_{L/K}$ is free as a $\mathbb{Z}[G]$-module when L/K is wildly but weakly ramified is still open. Pickett and Vinatier [**138**] have recently proved that $\mathcal{A}_{L/K}$ is a free $\mathbb{Z}[G]$-module when L/K is an odd degree weakly ramified Galois extension of number fields such that, for any wildly ramified prime $\mathfrak{p}$ of O_L, the decomposition group is abelian, the ramification group is cyclic and the localised extension $F_\wp/\mathbb{Q}_p$ is unramified, where $\wp = \mathfrak{p} \cap F$ and $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$. This result generalises Theorem 1.2 of [**158**], which is the natural analogue in the absolute case $K = \mathbb{Q}$. The proof of this result uses Lubin-Tate theory and the explicit descriptions by Pickett of self-dual normal basis generators for cyclic weakly ramified extensions of an unramified extension of $\mathbb{Q}_p$ [**137**]. These generators are constructed with the help of Lubin-Tate theory and Dwork's p-adic exponential power series.

It should be interesting to pursue this investigation and determine the Galois structure of $\mathcal{A}_{L/K}$ as a module over its associated order, when higher ramification is permitted. In this direction, one result is due to Burns whose proof is given in Appendix A of [**84**]:

***Proposition 5.8* (Burns, 1991).** — *If $L/\mathbb{Q}$ is a finite abelian extension such that the square root of the inverse different $\mathcal{A}_{L/K}$ exists, then $\mathcal{A}_{L/K}$ is locally free over its associated order.*

5.4.3. Existence of valuation criteria.— Finally, one can also consider the question of the existence of valuation criterion for Galois generators of ambiguous ideals when they are free over their associated order, and partial answers are already obtained. For example, if L/K is an abelian and weakly ramified extension of p-adic fields with Galois group G of odd order, the square root of the inverse different exists and is a free module over $O_K[G]$. Generalizing a result of Byott, Vinatier proved that every element $\beta \in L$ with valuation $v_L(\beta) = 1 - e_K$ generates $\mathcal{A}_{L/K}$ over $O_K[G]$ ([**157**], Cor. 2.5).

5.5. On the sufficiency of the ramification invariants. — We close this paper by the following remark. Let L/K be a finite extension of local fields of residue characteristic p. Results about the Galois module structure of ideals of L (e.g. [**42**], [**32**], [**87**]) indicate the possibility of nice general patterns governing some relationship with the ramification invariants of the extension, precisely its ramification jumps as well as the absolute ramification index of K. Moreover, when L/K is of degree p, the single ramification break determines whether or not O_L is free over its associated order in both mixed and equal characteristic cases. It seems that the ramification invariants actually control the question of freeness to a considerable extent, and Byott and Elder have noticed that they are sufficient to determine the structure of ideals when their number is maximal [**46**].

Nevertheless, we do not expect that such invariants will give the required information for all extensions. For instance, in ([**12**], Chap. 4), Bergé constructed two wild extensions over a fixed 3-adic field K with the same ramification jumps but such that the associated orders of their top valuation rings are different. More recently, this insufficiency was also observed for biquadratic extensions of 2-adic fields with one ramification jump [**47**]. These observations have led Byott and Elder to introduce a refined ramification filtration for some totally ramified elementary abelian p-extensions, i.e., one with more ramification jumps [**44, 46**], and then investigate whether they are sufficient. It will be interesting to address the question of which invariants determine the Galois module structure of ideals for more general extensions.

References

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

[2] A. Aiba, *Carlitz modules and Galois module structure II*, J. Number Theory **68** (1998), no. 1, 29-35.

[3] A. Aiba, *Carlitz modules and Galois module structure*, J. Number Theory **62** (1997), no. 1, 213-219.

[4] B. Anglès, *Bases normales relatives en caractéristique positive*, J. Thèorie des Nombres de Bordeaux **14** (2002), no. 1, 1-17.

[5] A. Bayad, *Structure galoisienne d'anneaux d'entiers et courbes elliptiques sans multiplication complexe*, Journal of number theory **52** (1995), 267-279.

[6] A.-M. Bergé, *À propos du genre de l'anneau des entiers d'une extension*, Number theory, 1979-1980 and 1980-1981, Exp. No. 1, 9 pages, Publ. Math. Fac. Sci. Besançon, Univ. Franche-Comté, Besançon, 1981.

[7] A.-M. Bergé, *Arithmétique d'une extension à groupe d'inertie cyclique*, Ann. Inst. Fourier **28, 4** (1978), 17-44.

[8] A.-M. Bergé, *Projectivité des anneaux d'entiers sur leurs ordres associés*, Astérisque **61** (1979), 15-28.

[9] A.-M. Bergé, *Extensions galoisiennes d'un corps local à groupes d'inertie cycliques*, Sémianire de Théorie des Nombres de Bordeaux, exposé no 2 (1976/1977).

[10] A.-M. Bergé, *Sur l'arithmétique d'une extension diédrale*, Annales de l'Institut Fourier **22**, no 2 (1972), 31-59.

[11] A.-M. Bergé, *À propos de l'ordre associé à l'anneau des entiers d'une extension, d'après H. Jacobinski*, Séminaire de Théorie des Nombres de Bordeaux, Exposé no 8 (1971-1972), 1-12.

[12] A.-M. Bergé, *Quelques résultats relatifs à l'ordre associé à une extension*, Publ. Math. Bordeaux **5** (1972-1973), 9-24.

[13] F. Bertrandias, *Sur les extensions cycliques de degré p^n d'un corps local*, Acta Arithmetica **34** (1979), 4, 361-377.

[14] F. Betrandias, *Décomposition du Galois-module des entiers d'une extension cyclique de degré premier d'un corps de nombres ou d'un corps local*, Ann. Inst. Fourier, **29** (1979), no. 1, xiv, 33-48.

[15] F. Bertrandias, *Entiers d'une p-extension cyclique d'un corps local*, C. R. Acad. Sc. Paris **286** (1978), Série A, 1083 - 1086.

[16] 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.

[17] 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.

[18] D. Blessenohl, *On the normal basis theorem*, Note di Matematica **27**, n. 1 (2007), 5-10.

[19] W. Bley, *A Leopoldt-type result for rings of integers of cyclotomic extensions*, Canad. Math. Bull. **38** (1995), 141-148.

[20] W. Bley, R. Boltje, *Computation of locally free class groups*, in F. Hess, S. Pauli, M. Pohst (Eds.), Algorithmic Number Theory, Lecture Notes in Computer Science **4076** (2006), 72-86.

[21] W. Bley, H. Johnston, *Computing generators of free modules over orders in group algebras*, Journal of Algebra **320** (2008), 836-852.

[22] W. Bley, S:M.J. Wilson, *Computations in relative algebraic K-groups*, LMS J. Comput. Math. **12** (2009), 166-194.

[23] M. V. Bondarko, *The Leopoldt problem for totally ramified abelian extensions of complete discrete valuation fields* (Russian), Algebra i Analiz 18 (2006), no. 5, 99–129; translation in St. Petersburg Math. J. **18** (2007), no. 5, 757–778

[24] M. V. Bondarko, *Local Leopoldt's problem for ideals in totally ramified p-extensions of complete discrete valuation fields*, Algebraic Number Theory and Algebraic Geometry: Papers Dedicated to A. N. Parshin on the Occasion of his Sixtieth Birthday, Contemp. Math., vol. 300, Amer. Math. Soc., Providence, RI, 2002, pp. 27-57.

[25] M. V. Bondarko, *Local Leopoldt's problem for rings of integers in abelian p-extensions of complete discrete valuation fields*, Doc. Math. **5** (2000), 657-693.

[26] M. V. Bondarko, *Additive Galois modules in Dedekind rings. Decomposability* (Russian), Algebra i Analiz 11 (1999), no. 6, 103-121; translation in St. Petersburg Math. J. **11** (2000), no. 6, 1019-1033.

[27] M. V. Bondarko, S. V. Vostokov, *Decomposability of ideals as Galois modules in complete discrete valuation fields* (Russian), Algebra i Analiz, **11** (1999), no. 2, 41-63; translation in St. Petersburg Math. J., **11** (2000), no. 2, 233-249

[28] M. V. Bondarko, S. V. Vostokov, and I. B. Zhukov, *Additive Galois modules in complete discrete valuation fields*, Algebra i Analiz 9 (1997), no. 4, 28-46; English transl., St.-Petersburg Math. J. **9** (1998), no. 4, 675-693.

[29] J. Brinkhuis, *Normal integral bases and complex conjugation*, J. reine angew. Math., **375/376** (1987), 157-166.

[30] J. Brinkhuis, *Galois modules and embedding problems*, J. Reine Angew. Math., **346** (1984), 141-165.

[31] D. Burns, *Equivariant Tamagawa numbers and Galois module theory I*, Compositio Math., **129** (2001), 203-237.

[32] D. Burns, *On the equivariant structure of ideals in abelian extensions of local fields (with an appendix by W. Bley)*, Comment. Math. Helv. **75** (2000), 1-44.

[33] D. Burns, *Factorisability and wildly ramified Galois extensions*, Ann. Inst. Fourier **41, 2** (1991), 393-430.

[34] D. Burns, N. P. Byott, *L-functions and Galois modules*, in: L-functions and arithmetic (J. Coates, M. J. Taylor, eds.), Cambridge University Press, 1991, 75-139.

[35] N. P. Byott, *A valuation criterion for normal basis generators of Hopf-Galois extensions in characteristic* p, preprint 2009.

[36] N.P. Byott, *On the integral Galois module structure of cyclic extensions of p-adic fields*, Quart. J. Math. **59** (2008), 149-162.

[37] N. P. Byott, *Hopf-Galois structures on Galois field extensions of degree pq*, J. Pure Appl. Algebra **188** (2004), no. 1-3, 45-57.

[38] N. P. Byott, *Integral Hopf Galois structures on degree* p^2 *extensions of p-adic fields*, J. Algebra **248** (2002), 334-365.

[39] N. P. Byott, *Integral Galois Module Structure of some Lubin-Tate extensions*, J. Number Theory **77** (1999), 252 - 273.

[40] N. P. Byott, *Galois module structure and Kummer theory for Lubin-Tate formal groups*, Algebraic number theory and Diophantine analysis (Graz, 1998), 55–67, de Gruyter, Berlin, 2000.

[41] N.P. Byott, *Associated orders of certain extensions arising from Lubin-Tate formal groups*, J. Théorie des Nombres de Bordeaux **9**, no 2 (1997), 449 - 462.

[42] N. P. Byott, *Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications*, J. Théor. Nombres Bordeaux **9** (1997), no. 1, 201-219.

[43] N. P. Byott, G. G. Elder, *Integral Galois module structure for elementary extensions with a Galois scaffold*, preprint 2009.

[44] N. P. Byott, G. G. Elder, *On the necessity of new ramification breaks*, Journal of Number Theory **129** (2009), 84-101.

[45] N. P. Byott, G. G. Elder, *A valuation criterion for normal bases in elementary abelian extensions*, Bull. London Math. Soc. **39** (2007), 5, 705-708.

[46] N. P. Byott, G. G. Elder, *New ramification breaks and additive Galois structure*, J. Théor. Nombres Bordeaux **17** (2005), no. 1, 87-107.

[47] N. P. Byott, G. G. Elder, *Biquadratic extensions with one break*, Canad.Math. Bull. **45** (2002), no. 2, 168-179.

[48] N. P. Byott, G. Lettl, *Relative Galois module structure of integers of Abelian fields*, J. Th. Nombres, Bordeaux **8** (1996), 125-141.

[49] N. P. Byott and M. J. Taylor, *Hopf orders and Galois module structure*, in DMV Seminar 18, *Group Rings and Class Groups*, Birkhauser, basel, 1992, 154-210.

[50] Ph. Cassou-Noguès, *Quelques théorèmes de base normale d'entiers*, Ann. Inst. Fourier **28** (1978), 1-33.

[51] Ph. Cassou-Noguès, *Quelques théorèmes de bases normales*, Soc. Math. de France, Astérisque **41-42** (1977), 183-189.

[52] Ph. Cassou-Noguès, J. Queyrut, *Structure galoisienne des anneaux d'entiers d'extensions sauvagement ramifiées. II*, Ann. Inst. Fourier **32** no 1 (1982), 7-27.

[53] Ph. Cassou-Noguès, M. J. Taylor, *Galois module structure for wild extensions*, Algebraic number theory and Diophantine analysis (Graz, 1998), 69-91, de Gruyter, Berlin, 2000.

[54] Ph. Cassou-Noguès, M. J. Taylor, *Elliptic functions and rings of integers*, Progress in Mathematics, Vol. 66, Birkhäuser, Basel, 1987.

[55] S. P. Chan, *Galois module structure of non-Kummer extensions*, Arch. Math. **70** (1998), 286-292.

[56] S. P. Chan, C.-H. Lim, *The associated orders of rings of integers in Lubin-Tate division fields over the p-adic nu,ber field*, Illinois J. Math. **39** (1995), 30-38.

[57] S. P. Chan, C.-H. Lim, *Relative Galois module structure of rings of integers of cyclotomic fields*, J. Reine Angew. Math. **434** (1993), 205-220.

[58] R. Chapman, *Kummer theory and Galois module structure in global function fields*, Math. Z. **208** (1991), 375 - 388.

[59] R. Chapman, *Carlitz modules and normal integral bases*, J. London Math. Soc. **44** (1991), 250-260.

[60] L. N. Childs, *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*, in: Math. Surveys Monogr., vol. 80, Amer. Math. Soc., Providence, RI, 2000.

[61] L. N. Childs, *Taming wild extensions with Hopf algebras*, Trans. Amer. Math. Soc. **304** (1987), 111-140.

[62] L. N. Childs, D. J. Moss, *Hopf algebras and local Galois module theory*, Advances in Hopf Algebras (J. Bergen, S. Montgomery, eds), Marcel Dekker, Inc., New York, 1994, 1-24.

[63] T. Chinburg, *Exact sequences and Galois module structure*, Ann. of Math. **121** (1985), 351-376. 10. H. Cohen, A course in computational

[64] L. N. Childs, D. J. Moss, *Hopf algebras and local Galois module theory*, Advances in Hopf Algebras (J. Bergen, S. Montgomery, eds.), Marcel Dekker, Inc., New York, 1994, 1-24.

[65] J. Cougnard, *Normal integral bases for A_4 extensions of the rationals*, Math. Comp. **75** (253) (2006), 485-496.

[66] J. Cougnard, *Nouveaux exemples d'extensions relatives sans base normale*, Ann. Fac. Sci. Toulouse Math. (6) 10 (2001), no. 3, 493-505.

[67] J. Cougnard, *Construction de base normale pour les extensions de $\mathbb{Q}$ à groupe D_4*, J. Théor. Nombres Bordeaux **12** (2) (2000), 399-409.

[68] J. Cougnard, *Anneaux d'entiers stablement libres sur $\mathbb{Z}[H_8 \times C_2]$*, J. Théor. Nombres Bordeaux **10** (1) (1998), 163-201.

[69] J. Cougnard, *Un anneau d'entiers stablement libre et non libre*, Experimental Mathematics **3** Vol. 2 (1994), 129-136.

[70] J. Cougnard, *Les travaux de Fröhlich, Ph. Cassou-Noguès et M. J. Taylor sur les bases normales*, Séminaire N. Bourbaki, 1982-1983, exp. no 598, 25-38.

[71] J. Cougnard, *Un contre-exemple à une conjecture de Martinet*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 539–560. Academic Press, London, 1977.

[72] J. Cougnard, *Propriétés galoisiennes des anneaux d'entiers des p-extensions*, Composition Math. **33** (1976), 303-336.

[73] J. Cougnard, J. Queyrut, *Construction de bases normales pour les extensions galoisiennes absolues à groupe de Galois quaternionien d'ordre* 12, J. Théor. Nombres Bordeaux **14** (1) (2002), 87-102.

[74] C. W. Curtis, I. Reiner, *Methods of Representation Theory: With Applications to Finite Groups and Orders*, Wiley-Interscience, 1990.

[75] I. Del Corso, L. Paolo Rossi, *Normal integral bases for cyclic Kummer extensions*, Journal of Pure and Applied Algebra **214** (2010), 385-391.

[76] G. G. Elder, *A valuation criterion for normal basis generators in local fields of characteristic p*, Arch. Math. **94** (2010), 43-47.

[77] G. G. Elder, *Galois scaffolding in one-dimensional elementary abelian extensions*, Proc. Amer. Math. Soc. **137** (2009), no. 4, 1193–1203.

[78] G. G. Elder, *On Galois structure of the integers in cyclic extensions of local number fields*, Journal de Théorie des Nombres de Bordeaux **14** (2002), 113-149.

[79] G. G. Elder, *Galois module structure of ideals in wildly ramified cyclic extensions of degree* p^2, Ann. Inst. Fourier **45** (1995), no. 3, 625-647.

[80] G. G. Elder, M. L. Madan, *Galois module structure of the integers in wildly ramified* $C_p \times C_p$ *extensions*, Canad. J. Math. **49** (1997), no. 4, 722-735.

[81] G. G. Elder, Madan, *Galois module structure of the integers in widly ramified cyclic extensions*, J. Number Theory **47** (1994), no. 2, 138-174.

[82] B. Erez, M. J. Taylor, *Hermitian modules in Galois extensions of number fields and Adams operations*, Anns of Math. **135** (1992), 271-296.

[83] B. Erez, *The Galois structure of the square root of the inverse different*, Math. Z. **208** (1991), 239-255.

[84] B. Erez, *A survey of recent work on the square root of the inverse different*, S.M.F. Astérisque **198-200** (1991), 198-199-200.

[85] B. Erez, *The Galois structure of the trace form in extensions of odd prime degree*, J. Algebra **118** (1988), no. 2, 438-446.

[86] M.-J. Ferton, *Sur l'anneau des entiers de certaines extensions cycliques d'un corps local*, Mémoires de la SMF **37** (1974), 69-74.

[87] M.-J. Ferton, *Sur les idéaux d'une extension cyclique de degré premier d'un corps local*, C.R. Acd. Sc. Paris **276** Série A (1973), 1483-1486.

[88] M.-J. Ferton, *Sur l'anneau des entiers d'une extension diédrale de degré* $2p$ *d'un corps local.* (French) C. R. Acad. Sci. Paris Sér. A-B **274** (1972), A1529–A1532.

[89] M. Florence, B. de Smit, L. Thomas, *Normal basis generators in p-extensions of local fields*, preprint 2010, submitted.

[90] J.-M. Fontaine, *Groupes de ramification et représentations d'Artin*, Ann. Scient. Sc. Norm. Sup., 4ème série **4, 3** (1971).

[91] A. Fröhlich, *Module defect and factorisability*, Illinois J. Math. **32** (1988), no. 3, 407-421.

[92] A. Fröhlich, *Galois module structure of algebraic integers*, Springer Verlag, Berlin, 1983.

[93] A. Fröhlich, *Value distributions of symplectic root numbers*, Proc. London Math. Soc. **(3) 46** (1983), no. 1, 83-99.

[94] A. Fröhlich, *Arithmetic and Galois module structure for tame extensions*, J. Reine Agew. Math., **286/287** (1976), 380-440.

[95] A. Fröhlich, *A normal integral basis theorem*, J. of Algebra **39** (1976), no 1.

[96] A. Fröhlich, *Locally free modules over arithmetic orders*, Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III. J. Reine Angew. Math. **274/275** (1975), 112-124.

[97] A. Fröhlich, E. Keating, S.M.J. Wilson, *The class group of quaternion and 2-dihedral* 2*-groups*, Mathematika **21** (1974), no 41.

[98] A. Fröhlich, *Artin root numbers and normal integral bases for quaternion fields*, Invent. Math. **17** (1972), 143-166.

[99] A. Fröhlich, *The module structure of Kummer extensions over Dedekind domains*, J. Reine Angew. Math. **209** (1962), 39-53.

[100] E.J. Gomez Ayala, *Normal bases for quadratic extensions inside cyclotomic fields*, Arch. Math. **66** (1996), no. 2, 123-125.

[101] E.J. Gomez-Ayala, *Bases normales d'entiers dans les extensions de Kummer de degré premier*, Journal de Théorie des Nombres de Bordeaux, **6** (1994), 95-116.

[102] C. Greither, H. Johnston, *Non-existence and splitting theorems for normal integral bases*, preprint 2009.

[103] C. Greither, H. Johnston, *Capitulation for locally free class groups of orders of group algebras over number fields*, Bull. London Math. Soc. **41** (2009), 541-548.

[104] C. Greither, D. Replogle, K. Rubin, A. Srivastav, *Swan modules and Hilbert Speiser number fields*, J. Number Theory **79** (1999), 164-173.

[105] C. Greither, *Constructing monogenic Hopf algebras over p-adic rings of integers*, J. Algebra **174**(1995), 794-800.

[106] C. Greither, B. Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106**(1987), 239-258.

[107] D. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. soc. *189* (1974), 77-91.

[108] H. Ichimura, *Note on Galois descent of a normal integral basis of a cyclic extension of degree p*, Proc. Japan Acad. **85**, Ser. A (2009), 160-162.

[109] H. Ichimura, *On the ring of integers of a tame Kummer extension over a number field*, Journal of Pure and Applied Algebra **187** (2004), 169-182.

[110] H. Ichimura, *On normal integral bases of unramified abelian p-extensions over a global function field of characteristic p*, Finite Fields and Their Applications **10** (2004), 432-437.

[111] H. Jacobinski, *Über die Hauptordnung eines Körpers als gruppen modul.*, Jour. reine angew. Math. **213** (1964).

[112] H. Johnston, *Relative Galois module structure of rings of integers of absolutely abelian number fields*, J. reine angew. Math. **620** (2008), 85-103.

[113] F. Kawamoto, *On normal integral bases of local fields*, J. of Algebra **98** (1986), 197-199.

[114] F. Kawamoto, *Remark on "On normal integral bases*, Tokyo Journal Mathematics **8** (1985), 275.

[115] F. Kawamoto, *On normal integral bases*, Tokyo Journal Mathematics **7** (1984), 221-231.

[116] F. Laubie, *Ramification des séries formelles*, Canad. Math. Bull. **47** (2004), no. 2, 237-245.

[117] H. W. Leopoldt, *Über die Hauptordnung der ganzen Elementen eines abelschen Zahlkörpers*, J. Reine Angew. Math. **201** (1959), 119-149.

[118] G. Lettl, *Note on a theorem of A. Aiba*, Journal of Number Theory **115** (2005), 87-88.

[119] G. Lettl, *Relative Galois module structure of integers of local abelian fields*, Acta Arith. **85** (1998), no. 3, 235-248.

[120] G. Lettl, *The ring of integers of an abelian number field*, J. reine angew. Math. **404** (1990), 162-170.

[121] T. Y. Lam, *A first course in noncommutative rings*, Graduate Texts in Mathematics, Springer, Second Edition, 2001.

[122] J. Martinet, *Bases normales et constante de l'équation fonctionnelle des fonctions L d'Artin*, Séminaire Bourbaki (1974), exp. 450.

[123] J. Martinet, *Sur les extensions à groupe de Galois quaternionien*, C.R. Acad. Sc. Paris **274-A** (1972), 933-935.

[124] J. Martinet, *Modules sur l'algèbre du groupe quaternionien*, Ann. Sc. de l'ENS, 4ème série **4** (1971), 299-308.

[125] J. Martinet, *Anneau des entiers d'une extension galoisienne considérée comme module sur l'algèbre du groupe de Galois*, Colloque de Théorie des Nombres de Bordeaux (1969), Bull. Soc. math. Fr., Mémoire **25** (1971), 123-126.

[126] J. Martinet, *Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre* $2p$, Annale de l'Institut Fourier, tome **19**, no 1 (1969), 1-80.

[127] L. McCulloh, *Galois module structure of abelian extensions*, J. Reine Angew. Math. **375-376** (1987), 259-306.

[128] H. Miki, *On the ramification numbers of cyclic p-extensions over local fields*, J. Reine Angew. Math. **328** (1981), 99-115.

[129] R. Miller, *Galois module structure in wild extensions of the rational function field*, Ph.D. thesis, University of Exeter, 1997.

[130] Y. Miyata, *On Galois structure of the integers in elementary abelian extensions of local number fields*, J. Number Theory **125** (2007), no. 2, 442-458.

[131] Y. Miyata, *Maximal tame extensions over Hopf orders in rings of integers of a* $\mathfrak{p}$*-adic number fields*, J. Algebra **274** (2004), 794-825.

[132] Y. Miyata, *Indecomposability of ideals of* $\mathfrak{p}$*-adic number fields*, Journal of number theory **107** (2004), 1-7.

[133] Y. Miyata, *On the module structure of rings of integers in* $\mathfrak{p}$*-adic number fields over associated orders*, Math. Proc. Camb. Phil. Soc. **123** (1998), 199-212.

[134] Y. Miyata, *On the Galois module structure of ideals and rings of all integers of* $\mathfrak{p}$*-adic number fields*, J. Alg. **177** (1995), 627-646.

[135] E. Noether, *Normal basis bei Körpern ohn höhere Verzweigung*, J. Reine Angew. Math. **167** (1932), 147-152.

[136] E. J. Pickett *Construction of Self-Dual Integral Normal Bases in Abelian Extensions of Finite and Local Fields*, Int. J. Number Th., to appear.

[137] E.J. Pickett *Explicit Construction of Self-Dual Integral Normal Bases for the Square-Root of the Inverse Different*, J. Number Th. **129** (2009) 1773-1785.

[138] E. J. Pickett and S. Vinatier, *Self-Dual Integral Normal Bases and Galois Module Structure*, in preparation.

[139] J. Queyrut, *Structure galoisienne de anneaux d'entiers d'extensions sauvagement ramifiées I*, Annales de l'Institut Fourier **31**, no 3 (1981), 1-35.

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

[141] M. Rzedowski-Calderon, G.D. Villa Salvador, M.L. Madan, *Galois module structure of rings of integers*, Math. Z. **204** (1990), 401-424.

[142] J.-P. Serre, *Local class field theory*, in "Algebraic Number Theory", J.W. Cassels and A. Fröhlich Eds, Academic Press, London, 1967.

[143] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1968.

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

[145] V. P. Snaith, *Galois module structure*, Fields Institute Monographs, vo.. 2, American Mathematical Society, Providence, 1994. (see also the review written by Agboola in the Bulletin of the American Mathematical Society **35**, 3 (1998), 249-252)

[146] A. Speiser, *Gruppendeterminante und Körperdiskriminante*, Math. Ann. **77** (1916), 546-562.

[147] R. G. Swan, *Induced representations and projective modules*, Ann. of Math. **71** (1960), 552-578.

[148] M. J. Taylor, *Hopf orders and Galois module structure*, with contributions by N. P. Byott. DMV Sem., 18, Group rings and class groups **153-210**, Birkhäuser, Basel, 1992

[149] M. J. Taylor, *Hopf structure and the Kummer theory of formal groups*, J. Reine Angew. Math. **375/376** (1987), 1-11.

[150] M. J. Taylor, *Formal groups and the Galois module structure of local rings of integers*, J. Reine Angew. Math. **358** (1985), 97-103.

[151] M. J. Taylor, *On Fröhlich's Conjecture for Rings of Integers of Tame Extensions*, Inventiones Mathematicae **63** (1981), 41-79.

[152] M. J. Taylor, *Galois module structure of integers of relative abelian extensions*, J. Reine Angew. Math. **303-304** (1978), 97-101.

[153] L. Thomas, *Valuation of normal basis generators in characteristic* p, Journal of Algebra **320** (2008), 3811-3820.

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

[155] S. Ullom, *Integral normal bases in Galois extensions of local fields*, Nagoya Math. J. **39** (1970), 141-146.

[156] S. Ullom, *Normal bases in Galois extensions of number fields*, Nagoya Math. J., Vol. **34** (1969), 153-167.

[157] S. Vinatier, *Galois module structure in weakly ramified* 3*-extensions*, Acta Arithmetica **119.2** (2005), 171-186.

[158] S. Vinatier *Structure galoisienne dans les extensions faiblement ramifiées de* $\mathbb{Q}$. J. Number Theory, 91(1), 2001.

[159] S.V. Vostokov, *Decomposability of ideals in splitting p-extensions of local fields*, Vestnik St. Peterburg Univ. Math. **26** (1993), 15-22. Translaton in Vestnik St.Petersburg Univ. Math. **26(2)** (1993), 10-16.

[160] S. V. Vostokov, *Ideals of an abelian p-extensions of a local field as Galois modules*, Journal of Soviet Math. **11** (1979), 567-584.

[161] B. F. Wyman, *Wildly ramified Gamma extensions*, Amer. J. Math. **91** (1969), 135-152.

[162] H. Yokoi, *On the ring of integers in an algebraic number field as a representation module of Galois group*, Nagoya Math. J. **16** (1960), 83-90.

May 27, 2010

Lara Thomas, Ecole Polytechnique Fédérale de Lausanne - Chaire de Structures Algébriques et Géométriques - FSB - IMB - Station 8, Bureau 594 CH - 1015 Lausanne • *E-mail :* `lara.thomas@epfl.ch`