ЧЕБЫШЕВСКИЙ СБОРНИК
Том 26. Выпуск 4.

УДК: 512.623.27; 512.625 DOI: 10.22405/2226-8383-2025-26-4-71-87

Базисы ассоциированных модулей Галуа в общих дико разветвленных расширениях и в элементарных абелевых расширениях степени p^2

М. В. Бондарко, К. С. Ладный, К. И. Пименов

Бондарко Михаил Владимирович — Санкт-Петербургский государственный университет (г. Санкт-Петербург).
e-mail: m.bondarko@spbu.ru
Ладный Кирилл Сергеевич — Национальный исследовательский университет «Высшая школа экономики» (г. Москва).
e-mail: kladnyy@hse.ru
Пименов Константин Игоревич — Санкт-Петербургский государственный университет (г. Санкт-Петербург).
e-mail: k.pimenov@spbu.ru

Аннотация

Данная статья посвящена исследованию ассоциированных модулей и порядков Галуа для вполне разветвленных расширений полей дискретного нормирования. Основное внимание уделяется явным вычислениям и построению базисов для этих модулей, в частности в случае элементарных абелевых расширений степени p^2. Авторы вводят и развивают теорию градуированно-независимых множеств и диагональных базисов, которые позволяют явно описывать модули γ_i и соответствующие ассоциированные порядки. Центральный результат работы — теорема 3.3.2, которая дает явное описание модулей γ_i для расширений с группой Галуа $(\mathbb{Z}/p\mathbb{Z})^2$ и различными по модулю p^2 скачками ветвления. В работе исследованы свойства введенных конструкций, в том числе их поведение относительно подъема на ручные расширения и связь с классическими ассоциированными порядками. Полученные результаты обобщаются на случай относительных ассоциированных модулей $\gamma_i^0 = \gamma_i \cap k_0[G]$, где $k_0 \subset k$. В работе используется построенный ранее первым автором изоморфизм между между $K \otimes_k K$ и $K[G]$, и представлен детальный анализ фильтраций на тензорных квадратах и их связи со структурой модулей Галуа. Статья может представлять интерес для специалистов по теории чисел и арифметической геометрии.

Ключевые слова: ассоциированные модули Галуа, ассоциированные порядки, дикий тип ветвления, расширения полей дискретного нормирования, элементарные абелевы расширения, градуированные базисы, скачки ветвления.

Библиография: 8 названий.

Для цитирования:
Бондарко М. В., Ладный К. С., Пименов К. И. Базисы ассоциированных модулей Галуа в общих дико разветвленных расширениях и в элементарных абелевых расширениях степени p^2 // Чебышевский сборник, 2025, т.26, вып.4, с. 71–87.

CHEBYSHEVSKII SBORNIK
Vol. 26. No. 4.

UDC: 512.623.27; 512.625 DOI: 10.22405/2226-8383-2025-26-4-71-87

Bases of associated Galois modules in general wildly ramified extensions and in elementary abelian extensions of degree p^2

M. V. Bondarko, K. S. Ladny, K. I. Pimenov

Bondarko Mikhail Vladimirovich — Saint Petersburg State University (St. Petersburg).
e-mail: m.bondarko@spbu.ru
Ladny Kirill Sergeevich — National Research University "Higher School of Economics" (Moscow).
e-mail: kladnyy@hse.ru
Pimenov Konstantin Igorevich — Saint Petersburg State University (St. Petersburg).
e-mail: k.pimenov@spbu.ru

Abstract

The paper provides a comprehensive investigation of associated Galois modules and orders for totally ramified extensions of complete discrete valuation fields. The authors focus on explicit computations and systematic construction of bases for these modules, with particular emphasis on elementary abelian extensions of degree p^2. The study introduces and develops the theory of graded-independent sets and diagonal bases, which enable constructive description of the modules γ_i and related associated orders. The central achievement is Theorem 3.3.2, which provides an explicit computation of the modules γ_i for extensions with Galois group $(\mathbb{Z}/p\mathbb{Z})^2$ and ramification jumps distinct modulo p^2. The paper thoroughly examines properties of the introduced constructions, including their relationship with classical associated orders and the behaviour under tame lifts. The obtained results are generalized to the case of relative associated modules $\gamma_i^0 = \gamma_i \cap k_0[G]$, where $k_0 \subset k$. The paper extensively utilizes the isomorphism between $K \otimes_k K$ and $K[G]$ constructed by the first author, and presents a detailed analysis of filtrations on tensor squares and their connection to Galois module structure. Respectively, the text can be interesting to specialists in algebraic number theory and arithmetic geometry.

Keywords:
associated Galois modules, associated orders, wild ramification, discrete valuation field extensions, elementary abelian extensions, graded bases, ramification jumps.

Bibliography: 8 titles.

For citation:
Bondarko, M. V., Ladny, K. S., Pimenov, K. I. 2025, "Bases of associated Galois modules in general wildly ramified extensions and in elementary abelian extensions of degree p^2" , *Chebyshevskii sbornik*, vol.26, no.4, pp. 71–87.

The paper is dedicated to Sergei Vladimirovich Vostokov,
who was an outstanding mathematician and also
a wonderful scientific advisor of the first author
that inspired him to study additive Galois modules.
Your memories will live on long after you've passed.

The research of Mikhail V. Bondarko was supported by the Leader (Leading scientist Math) grant no. 22-7-1-13-1 of the Theoretical Physics and Mathematics Advancement Foundation "BASIS".
The research of Kirill S. Ladny was supported within the framework of the project "International academic cooperation" HSE University.

1. Introduction

1.1. History and motivation

This paper is devoted to the calculation of certain associated Galois modules. Those are closely related to associated Galois orders (and we compute some of those as well). Let us recall some history and motivation for studying these matters.

Starting from [7], the ring of integers $\mathfrak{O}$ of a global or a local field K is studied as a module over its associated order

$$\gamma(\mathfrak{O}) = \{f \in k[G] : \ f(\mathfrak{O}_K) \subset \mathfrak{O}_K\};$$

here G is the Galois group of an extension K/k. The main results of ibid. says that $\mathfrak{O}$ is free over $\gamma(\mathfrak{O})$ (and hence isomorphic to $\gamma(\mathfrak{O})$ as a Galois module) whenever $k = \mathbb{Q}$ and G is abelian.

Since 1959, dozens of papers computing associated orders (of rings of integers and fractional ideals) were written. Yet the main subject of this paper are so-called associated Galois modules that are somewhat distinct from associated orders, even though closely related to them. First we define them, and then discuss the relation to associated orders.

Throughout this paper K/k is a totally ramified extension of complete discrete valuation fields of degree n.

We set

$$\mathfrak{C}_i = \{f \in K[G] : \ \min_{x \in K^*}(v(f(x)) - v(x)) \geqslant i\}; \ \gamma_i = \mathfrak{C}_i \cap k[G],$$

where v is the discrete valuation on K and $i \in \mathbb{Z}$. The main question we studied is to find a specific description of all γ_i. Our main result is Theorem 3.3.2 below that gives a simple expression for γ_i for all $i \in \mathbb{Z}$ assuming that K/k is an elementary abelian extension of degree $n = p^2$ whose ramification jumps are distinct modulo n.

Remark 1.1.1. 1. Obviously $\gamma_0 \subset \gamma(\mathfrak{O}) \subset \gamma_{1-n}$ and $\gamma_{1-n} \subset \gamma_{-n} = \pi_k^{-1}\gamma_0$, where π_k is an uniformizing element of k.

Hence the computation of γ_i does give some information on the associated order.

2. In certain cases we have Galois module isomorphisms $\gamma_i \to \mathfrak{M}^{i-d}$ (where d is the ramification depth on K/k; see §2.1 below); see Theorem 4.3.2(5) of [2]. However, we probably don't have any isomorphisms of this sort in the setting of our Theorem 3.3.2; cf. Theorem 3.10 of [4].

So, to add some motivation, we will now recall an interesting statement that relates associated Galois modules to the arithmetic of the extension.

We will never apply this theorem in the paper; respectively, the reader who does not need additional motivation for studying associated Galois modules may skip it.

Let F be a commutative m-dimensional formal group law with coefficients in $\mathfrak{o}$. We will write $F(\mathfrak{M})$ for the corresponding value of the commutative group functor coming from F (here $\mathfrak{M}$ is the maximal ideal of the valuation field K); note that there exists a canonical (forgetful) bijection of sets $F(\mathfrak{M}) \to \mathfrak{M}^m$.

Theorem 1.1.2 (Theorem 2.3.1 of [3]). Take $w > 0$; let a map

$$A : G \to F(\mathfrak{M}), \ \sigma \to a_\sigma = (a_{1\sigma}, \dots, a_{m\sigma})$$

(here $a_{i\sigma} \in \mathfrak{M}$) belong to $Z^1(G, F(\mathfrak{M}))$ (that is, an inhomogeneous Galois 1-cocycle). Then the following statements are equivalent.

1. For any i, $1 \leqslant i \leqslant m$, the element $f_i = \sum_{\sigma \in G} a_{i\sigma}\sigma$ lies in the module $\mathfrak{C}_{w+d}$; here d is the ramification depth of K/k (see §2.1 below).

2. $f \in B^1(G, F(\mathfrak{M}))$ (a 1-coboundary) and there exists an $x = (x_i) \in F(\mathfrak{M})$ such that

$$x \underset{F}{-} \sigma(x) = a_\sigma \ \forall \sigma \in G$$

and $v(x_i) \geqslant w$ for all i.

Remark 1.1.3. 1. We are mainly interested in the case where the values of A belong to $F(\mathfrak{M}_0) = F(\mathfrak{M} \cap k)$. Then A is a homomorphism $G \to F(\mathfrak{M}_0)$. Moreover, in this case condition 1 of the theorem depends on the modules γ_i only and condition 2 translates into a Kummer-type condition on the corresponding formal modules; see Definition 4.1.1 and Theorem 4.2 of [3].

2. Moreover, the theorem demonstrates that in the case where all $a_{i\sigma}$ belong to a subfield k_0 of k it suffices to know the modules $\gamma_i^0 = \gamma_i \cap k_0[G]$ only to apply the theorem. For this reason (and also to extend Theorem 1.2.1 below to more general extensions) we develop some theory of associated Galois modules of this type.

1.2. The contents of the paper

The main specific result of the paper is the following one.

Theorem 1.2.1. Assume K/k is a totally ramified Galois extension with Galois group p $G \cong (\mathbb{Z}/p\mathbb{Z})^2$, with ramification jumps that are distinct modulo p^2, and σ_1, σ_2 are elements of G corresponding to distinct ramification jumps.

Then there exists a piecewise linear function $H : \mathbb{Z}^2 \to \mathbb{Z}$ such that for any $i \in \mathbb{Z}$ we have $\gamma_l = \langle \pi_k^{[(l-d-H(i,j)-1)/n]+1}(\sigma_1 - 1)^i(\sigma_2 - 1)^j \mid 0 \leqslant i, j \leqslant p-1 \rangle_0$.

Proof. Immediate from Theorem 3.3.2(2) combined with Proposition 3.1.2(2). □

Remark 1.2.2. 1. The function H is piecewise linear; it is calculated in §3.3 as well.

2. It suffices to assume that σ_1 and σ_2 generate G to compute the smallest l such that $(\sigma_1 - 1)^i(\sigma_2 - 1)^j \in \gamma_l$ for each $(i, j) : \ 0 \leqslant i, j \leqslant p-1$; see Theorem 3.3.2(1) and Remark 3.3.3(3).

Now, let us say something about the general results and methods of this paper.

We develop much general theory for specifying "nice" bases of various associated Galois modules (and orders). Whereas most of this theory is inspired by the examples considered in [2], our definitions and statements related to these *graded-independent* and *diagonal* bases appear to be completely new.

However, some of the statements and methods that we use for studying these bases have much in common with [2]. In particular, some of the calculations are based on the isomorphism $\phi : K \otimes_k K \to K[G]$ introduced in [1], and we prove some new statements related to it.

In §2 we introduce some notation and recall some theory of associated Galois modules. Most of the statements in this section are related to ϕ and $K \otimes_k K$.

In §3 we develop the theory of graded bases; they allow us to construct "compatible" bases for all γ_i. We also make some general calculations and prove Theorem 1.2.1.

In §4 we define and study relative Galois modules of the sort γ_i^0 (see Remark 1.1.3(2)). They allow us to extend Theorem 1.2.1; see Theorem 4.1.3(2).

Next we define some more associated Galois modules (and orders; we define $\gamma^0(i, j) = \{f \in k_0[G] : \ f(\mathfrak{M}^i) \subset \mathfrak{M}^j\}$). Next we study those (graded) bases that are convenient for constructing bases of modules of this type; we call them *diagonal bases*. We describe an algorithm that allows to describe bases of all $\gamma^0(i, j)$ in terms of a diagonal base, and also prove that certain tame lifts of Galois extensions contain graded bases.

Some more information on the contents can be found in the beginnings of sections.

Remark 1.2.3. It appears that computation of associated orders in the cases where no freeness results are known to hold (cf. Remark 1.1.1(2)) are rather rare. The only example of this sort known to the authors is the (main) Theorem 2.4 of [5].

2. Some notation and basic associated Galois module theory

In this section we recall some basics of the theory of associated Galois modules.

In §2.1 we mostly introduce notation.

In §2.2 we recall the theory of the isomorphism $\phi : K \otimes_k K \to K[G]$. The results of this section do not differ much from the corresponding statements of [2]; yet the exposition is new. We will not really need the results of this section till §3.3.

2.1. Basic notation and definitions

K/k is a totally ramified Galois extension of complete discrete valuation fields, G is its Galois group, and n is its degree.

We set $d = v(\mathfrak{D}^{K/k}) - n + 1$ be the *ramification depth* of K/k; here $\mathfrak{D}^{K/k}$ is the different of this extension.

We will write $\mathfrak{M}_\mathfrak{o} \subset \mathfrak{o}$ (resp. $\mathfrak{M} \subset \mathfrak{O}$) for the maximal ideal and the rings of integers of k and K, respectively.

$\overline{k} = \mathfrak{o}/\mathfrak{M}_\mathfrak{o} \cong \mathfrak{O}/\mathfrak{M}$ is the residue field both of k and K. Denote by r the canonical epimorphism $\mathfrak{O} \to \overline{k}$.

$p > 0$ is the characteristic of $\overline{k}$, v is the discrete valuation on K.

The characteristic of K may be either p or 0.

$\mathrm{tr}_{E/L}$ is the trace operator corresponding to a finite extension E/L (of complete discrete valuation fields); we will mostly need $\mathrm{tr} = \mathrm{tr}_{K/k}$.

π will be a fixed uniformizing element of K.

LEMMA 2.1.1. $r \circ \mathrm{tr}$ yields a $\overline{k}$-linear isomorphism $\mathfrak{M}^{-d}/\mathfrak{M}^{1-d} \to \overline{k}$.

PROOF. Essentially by the definition of the different, $\mathrm{tr}(\mathfrak{M}^{1-d}) = \mathfrak{M}_\mathfrak{o}$ and $\mathrm{tr}(\mathfrak{M}^{-d}) = \mathfrak{o}$. Hence we get a non-zero map which is obviously $\overline{k}$-linear. Since the multiplication by π^{-d} gives an isomorphism $\mathfrak{M}^{-d}/\mathfrak{M}^{1-d} \to \overline{k}$, $r \circ \mathrm{tr}$ is an isomorphism indeed. □

Consequently, the element $c_\pi = \mathrm{tr}(\pi^{-d})$ belongs to $\mathfrak{o}^*$.

Now let us define some associated Galois modules; we will define more of them in §4 below.

For $i \in \mathbb{Z}$ we set

$$\mathfrak{C}_i = \{f \in K[G] : \min_{x \in K^*}(v(f(x)) - v(x)) \geqslant i\};\ \gamma_i = \mathfrak{C}_i \cap k[G];$$

here we take the obvious action of the set $K[G]$ on K.[1] Obviously, $\mathfrak{C}_i$ (resp. γ_i) give a separated exhaustive filtration on $K[G]$ (resp. $k[G]$).

Clearly, for $\sigma \in G$ we have $\sigma - 1 \in \gamma_i$ if and only if $i \geqslant h$, where h is the (lower) ramification jump for σ (see Definition II.4.5 of [6]); cf. the proof of Theorem 3.2.2(1) below.

We will write $d(f) = i$ whenever $f \in K[G] \setminus \{0\}$ and $f \in \mathfrak{C}_{i+d} \setminus \mathfrak{C}_{i+d+1}$; we will justify this shift by d (along with the $r(c_\pi)^{-1}$ multiplier below) in §2.2. Obviously, this definition gives a well-defined function $K[G] \setminus \{0\} \to \mathbb{Z}$.

Let us also describe functions corresponding to factors of the filtration $\mathfrak{C}_i$.

For $i \in \mathbb{Z}$ and $f \in \mathfrak{C}_i$ we set

$$p_i(f) = r(c_\pi)^{-1} \sum_{j=0}^{n-1} r(f(\pi^{j-i})/\pi^j) X^j \in R_{K/k} = \overline{k}[X]/(X^n - 1). \tag{1}$$

[1] Note that the usual group algebra multiplication in $K[G]$ does not correspond to the composition of endomorphisms of K. Yet this problem does not occur if one multiplies elements of $k[G]$ only; thus $k[G]$ acts on K as a ring.

We will write $p_i(f) \sim g \in R_{K/k}$ if there exists $c \in \overline{k} \setminus \{0\}$ such that $p_i(f) = cg$.

Moreover, if $f \in \mathfrak{C}_i \setminus \mathfrak{C}_{i+1}$ then we set $\rho(f) = p_i(f)$. Thus ρ gives a well-defined function $K[G] \setminus \{0\} \to \mathbb{Z}$.

LEMMA 2.1.2. p_i gives a $\overline{k}$-linear isomorphism $\mathfrak{C}_i/\mathfrak{C}_{i+1} \to R_{K/k}$ (of $\overline{k}$-vector spaces).

PROOF. Immediate from our definitions. □

2.2. Definitions and statements related to $K \otimes_k K$

The algebra $K \otimes_k K$ is really important for our paper. Some of its properties extend to more general field extensions, and we will start from statements of this type.

For this purpose we introduce the following notation.

We will always assume below that K'/k' is a totally ramified extension of complete discrete valuation fields,[2] n' is its degree, $\mathfrak{O}_{K'}$ (resp. $\mathfrak{o}'$) is the ring of integers of K' (resp. k'), $\mathfrak{M}'$ is the valuation ideal of K', $\overline{k'}$ is the residue field of K' and k', and $\pi' \in \mathfrak{M}'$ is an uniformizing element.

For $i \in \mathbb{Z}$ we set $X_i^{K' \otimes_{k'} K'} = \sum_{j \in \mathbb{Z}} \mathfrak{M}'^j \otimes \mathfrak{M}' \subset K' \otimes_{k'} K'$.

Below we will omit the upper index $K' \otimes_{k'} K'$ in all the notation in the case $K'/k' = K/k$. We write just t for the automorphism of $K' \otimes_{k'} K'$ (or of $K \otimes_k K$) that swaps the factors of the tensor square.

By default, all tensor products below are that over the ring $\mathfrak{o}$. Yet when we will write $\otimes$ when treating subsets and elements of $K' \otimes_{k'} K'$ then we will assume that this symbol means $\otimes_{\mathfrak{o}'}$.

PROPOSITION 2.2.1. Assume $i, j \in \mathbb{Z}$.

1. $X_i^{K' \otimes_{k'} K'} \cdot X_j^{K' \otimes_{k'} K'} \subset X_{i+j}^{K' \otimes_{k'} K'}$.

Consequently, $X_0^{K' \otimes_{k'} K'}$ is a subring of $K' \otimes_{k'} K'$ and $X_i^{K' \otimes_{k'} K'}$ is an $X_0^{K' \otimes_{k'} K'}$-module.

2. Moreover, $X_i^{K' \otimes_{k'} K'}/X_{i+1}^{K' \otimes_{k'} K'}$ is a one-dimensional free module over the ring $X_0^{K' \otimes_{k'} K'}/X_1^{K' \otimes_{k'} K'}$.

3. $X_i^{K' \otimes_{k'} K'} = \bigoplus_{l=0}^{n'-1} \pi'^l \otimes \mathfrak{M}'^{i-l}$.

4. For any $\varepsilon \in \mathfrak{O}_{K'}^*$ we have $\varepsilon \otimes \varepsilon^{-1} \in 1 + X_1^{K' \otimes_{k'} K'}$.

Consequently, for $x \in K'^*$ and $\varepsilon_1, \varepsilon_2 \in \mathfrak{O}_{K'}^*$ the class of $\varepsilon_1 x \otimes \varepsilon_2 x^{-1}$ in $X_0^{K' \otimes_{k'} K'}/X_1^{K' \otimes_{k'} K'}$ equals that of $\varepsilon_1 \varepsilon_2 (\pi' \otimes \pi'^{-1})^{v'(x)}$, where v' is the discrete valuation on K', and the class of $x \otimes x^{-1}$ is 1 if $n' \mid v'(x)$.

5. There exist a unique isomorphism

$$r^{K' \otimes_{k'} K'} : X_0^{K' \otimes_{k'} K'}/X_1^{K' \otimes_{k'} K'} \to R_{K'/k'} = \overline{k'}[X]/(X^{n'} - 1)$$

of $\overline{k'}$-algebras with a unit that sends $\pi' \otimes \pi'^{-1}$ into X. Moreover, this element of $X_0^{K' \otimes_{k'} K'}/X_1^{K' \otimes_{k'} K'}$ along with the aforementioned isomorphism do no not depend on the choice of π'.

6. t is a ring automorphism that restricts to $X_i^{K' \otimes_{k'} K'}$.

Moreover, for any $\alpha \in X_0^{K' \otimes_{k'} K'}$ we have $r^{K' \otimes_{k'} K'}(t(\alpha)) = r^{K' \otimes_{k'} K'}(\alpha)(X^{-1})$; note here that X is invertible in $R_{K'/k'}$.

PROOF. 1. Obvious.

2. The previous assertion implies that $X_i^{K' \otimes_{k'} K'}/X_{i+1}^{K' \otimes_{k'} K'}$ is a module over $X_0^{K' \otimes_{k'} K'}/X_1^{K' \otimes_{k'} K'}$ indeed. It remains to note that the multiplications by $1 \otimes \pi'^i$ and $1 \otimes \pi'^{-i}$ give

[2] In several statements we don't need K'/k' to be Galois. Note however that we don't really need non-Galois extensions in this paper.

mutually inverse $X_0^{K'\otimes_{k'}K'}/X_1^{K'\otimes_{k'}K'}$-module isomorphisms between $X_0^{K'\otimes_{k'}K'}/X_1^{K'\otimes_{k'}K'}$ and $X_i^{K'\otimes_{k'}K'}/X_{i+1}^{K'\otimes_{k'}K'}$.

3. Since $\{\pi'^{l+a},\ 0\leqslant a\leqslant n'-1\}$, give a $\mathfrak{o}'$-base of $\mathfrak{M}'^l$ for any $l\in\mathbb{Z}$, and $\mathfrak{M}'\subset K'$, $\bigoplus_{0\leqslant a\leqslant n'-1}\pi'^{l+a}\otimes_{\mathfrak{o}'}\mathfrak{M}'^{i-l}=\mathfrak{M}'^l\otimes_{\mathfrak{o}'}\mathfrak{M}'^{i-l}\subset K'\otimes_{k'}K'$. Summing up these equalities for all $l,\ 0\leqslant l\leqslant n'-1$, we easily deduce the statement in question.

4. Firstly, K'/k' is totally ramified; hence ε can be presented as $\varepsilon'(1+\delta)$, where $\varepsilon\in k'$ and $\delta\in\mathfrak{M}'$. Hence $\varepsilon\otimes\varepsilon^{-1}=\varepsilon'\otimes\varepsilon'^{-1}\cdot(1+\delta)\otimes(1+\delta)^{-1}=(1+\delta)\otimes(1+\delta)^{-1}\in 1+X_1^{K'\otimes_{k'}K'}$ indeed. This immediately implies $\varepsilon_1(x\otimes\varepsilon_2x^{-1}-\varepsilon_2(\pi'\otimes\pi'^{-1})^{v'(x)})\in X_1^{K'\otimes_{k'}K'}$

Lastly, if $v'(x)$ is divisible by n' then $x=x'\varepsilon_x$ for some $x'\in k'$ and $\varepsilon_x\in\mathfrak{O}_{K'}^*$; hence the images of $x\otimes x^{-1}$ and $x'\otimes x'^{-1}=1$ in $X_0^{K'\otimes_{k'}K'}/X_1^{K'\otimes_{k'}K'}$ coincide.

5. Assertion 3 easily implies that $X_0^{K'\otimes_{k'}K'}/X_1^{K'\otimes_{k'}K'}$ is generated by the classes of $\pi'^l\otimes\pi'^{-l}$, $l\geqslant 0$, as an $\overline{k'}$-vector space, and the classes of $1,\pi'\otimes\pi'^{-1},\dots,\pi'^{n'-1}\otimes\pi'^{1-n'}$ are $\overline{k'}$-independent in it. Hence to construct the isomorphism in question it suffices to verify that $\pi'^n\otimes\pi'^{-n}\in 1+X_1^{K'\otimes_{k'}K'}$. Now, this statement is given by the previous assertion, that also immediately implies the independence statments in our assertion.

6. All the statements in question except the last one are obvious.

The equality is easy as well. We clearly can present α as $\sum_{0\leqslant l\leqslant n'-1}a_l\pi'^l\otimes\pi'^{-l}+\alpha'$ for some $a_j\in\mathfrak{o}'$ and $\alpha'\in X_1^{K'\otimes_{k'}K'}$; see assertions 3 and 5. Hence it suffices to verify the statement for $\alpha=\pi'^l\otimes\pi'^{-l}$, and in this case it is obvious.

□

Now we return to the extension K/k and relate $K\otimes_k K$ to $K[G]$. We recall a definition that is important for our arguments.

THEOREM 2.2.2. Assume $i,j\in\mathbb{Z}$.

1. The k-vector space homomorphism $K\otimes_k K\to K[G]$ that sends $x\otimes y$ (for $x,y\in K$) into $x\sum_{\sigma\in G}\sigma(y)\sigma$, is bijective.[3]

2. For any $\sum x_i\otimes y_i\in K\otimes_k K$ and $z\in K$ we have $\phi(\sum x_i\otimes y_i)(z)=\sum_i x_i\operatorname{tr}(y_iz)$.

3. For any $\alpha,\beta\in K\otimes_k K$ we have $\phi(\alpha)*\phi(\beta)=\phi(\alpha\beta)$, where we set $\sum_{\sigma\in G}a_\sigma\sigma*\sum_{\sigma\in G}b_\sigma\sigma=$ $=\sum_{\sigma\in G}a_\sigma b_\sigma\sigma$.

4. $\mathfrak{C}_{i+d}=\phi(X_i)$.

5. For any $i\in\mathbb{Z}$ the following two functions on X_i coincide: $r_i^{K\otimes_kK}=x\mapsto r^{K\otimes_kK}(x\cdot(1\otimes\pi^{-i}))$ and $p_{d+i}\circ\phi$.

6. $\phi(t(\alpha))=\sum_{\sigma\in G}\sigma(a_{\sigma^{-1}})\sigma$, where $\phi(\alpha)=\sum_{\sigma\in G}a_\sigma\sigma$.

PROOF. Assertions 1—4 are given by Lemma 1.1.1, Proposition 1.3.1, and Proposition 2.4.4 of [2], respectively.

5. Both of these functions are clearly additive and annihilate X_{d+i+1}. Moreover, they are obviously $\overline{k}$-linear if considered as functions from X_{d+i}/X_{d+i+1}. Hence it suffices to compare their values on $\pi^j\otimes\pi^{i-j}$ for $0\leqslant j\leqslant n-1$. Now, $r^{K\otimes_kK}(\pi^j\otimes\pi^{-j})=X^j$; see Proposition 2.2.1(4). Next,

$$p_{d+i}(\phi(\pi^j\otimes\pi^{i-j}))=r(c_\pi)^{-1}\sum_{l=0}^{n-1}r(\pi^j\operatorname{tr}(\pi^{l-j-d})\pi^{-l})X^l.$$

Applying Lemma 2.1.1 we easily obtain $p_{d+i}(\phi(\pi^j\otimes\pi^{i-j}))=X^j$, and this concludes the Proof.

6. Obviously, it suffices to verify this equality for $\alpha=x\otimes y$, where $x,y\in K$. Now, $\phi(y\otimes x)=y\sum_{\sigma\in G}\sigma(x)\sigma=\sum_{\sigma\in G}\sigma(x\sigma^{-1}(y))\sigma=\sum_{\sigma\in G}\sigma(a_{\sigma^{-1}})\sigma$ indeed.

□

[3] And ϕ is also K-linear if we multiply elements on K by the first component in $K\otimes_k K$.

Remark 2.2.3. 1. In [2, Definition 2.8.1] $d_i(f)$ for $f \in \mathfrak{C}_{i+d}$ was essentially defined as $r_i^{K\otimes_k K}$ (see Theorem 2.2.2(5)). Thus we have just checked the compatibility of the two definitions.

2. Now we will study the relations between distinct extensions and the corresponding $K'\otimes_{k'}K'$'s. We are mainly interested in the case of Galois extensions, and it will be convenient for us to denote the bigger extension by K/k. Note hower, that Proposition 2.2.4(1,2) below is clearly valid without assuming that the extension K/k is Galois.

Proposition 2.2.4. Assume $k' \subset K' \subset K$, $k' \subset k \subset K$, k/k' is a finite extension, and $\alpha' \in X_i^{K'\otimes_{k'}K'}$ for some $i \in \mathbb{Z}$.

Denote the ramification index of K/K' by e and the image of α' in $K \otimes_k K$ by α.

1. Assume that $\alpha' = \sum_{0\leqslant l\leqslant n'-1} a_l \pi'^j \otimes \pi'^{i-l} + \beta$ for some $\beta \in X_{i+1}^{K'\otimes_{k'}K'}$ and $a_{ij} \in \mathfrak{o}'$ (cf. Proposition 2.2.1(3)). Then $\alpha \in X_{ie}$ and $r_{ie}^{K\otimes_k K}(\alpha) = c^i \sum r(a_l) X^{le}$, where $c = r(\pi'/\pi^e)$.

2. Assume $p \nmid [k : k']$, n is a power of p, and $K = K'k$. Then $n = n'$ and $\alpha' \in X_{i+1}^{K'\otimes_{k'}K'}$ if and only if $\alpha \in X_{(i+1)e}$.

3. Assume that $k = k'$ and K'/k is a Galois subextension of K/k.
Then $\phi(\alpha) = \phi^{K'\otimes_{k'}K'}(\alpha') \circ \mathrm{tr}_{K/K'}$.

Proof. 1. Once again, it clearly suffices to verify this statement in the case $\alpha' = \pi'^l \otimes \pi'^a$ for $0 \leqslant l < n, a \geqslant i-l$. Now, if $a > i-l$ then we obviously have $\alpha \in X_{(i+1)e}$; thus we can assume $a = i-l$. In this case $\alpha \in X_{ie}$ and $r_{ie}^{K\otimes_k K}(\alpha) = r^{K\otimes_k K}(\pi'^l \otimes (\pi'^{i-l}/\pi^{ei})) = r^{K\otimes_k K}((\pi'/\pi^e)^i \otimes 1 \cdot \pi^{le} \otimes \pi^{-le} \cdot \cdot (\pi'/\pi^e)^{l-i} \otimes (\pi'/\pi^e)^{i-l} = c^i X^{le}$ indeed; see Proposition 2.2.1(4).

2. Since the degrees of K'/k' and k/k' are coprime, these extensions are linearly disjoint. Hence $n = n'$ indeed.

To verify the equivalence in question is suffices to apply the previous assertion and note that the corresponding homomorphism $X_0^{K'\otimes_{k'}K'}/X_1^{K'\otimes_{k'}K'} \to X_0/X_1$ is injective.

3. Clearly, it suffices to verify that for any $z \in K$ we have $\phi(\alpha')(z) = \phi^{K'\otimes_{k'}K'}(\alpha')(\mathrm{tr}_{K/K'})$.

Now if $\alpha' = \sum x_i \otimes y_i$ for $x_i, y_i \in K'$ then (by Theorem 2.2.2(2)),

$$\phi(\alpha')(z) = \sum x_i \,\mathrm{tr}(y_i z) = \sum x_i \,\mathrm{tr}_{K/K'}(y_i \,\mathrm{tr}_{K/K'} z) = \phi^{K'\otimes_{k'}K'}(\alpha')(\mathrm{tr}_{K/K'} z)$$

indeed.

□

3. Main associated Galois modules calculations

This section is devoted to constructing $\mathfrak{o}$-bases of the modules γ_i.

In §3.1 we introduce some new and rather simple theory for constructing bases of this sort; we call the corresponding notions *graded-independent sets* and *graded bases*.

In §3.2 we study the graded independence and the values of the functions d and ρ for elements of the form $\prod_{i=1}^a (\sigma_i - 1)$ for $a \leqslant p-1$.

In §3.3 we apply all the earlier theory to the study extensions with Galois group $(\mathbb{Z}/p\mathbb{Z})^2$. We are able to construct a ("simple") graded base in the case where the ramification jumps of K/k are distinct modulo p^2; see Theorem 3.3.2.

3.1. On graded-independent sets and bases

Let us give some more simple definitions related to associated Galois modules.

Definition 3.1.1. Assume $B \subset K[G] \setminus \{0\}$.

1. For $i \in \mathbb{Z}$ we set $B_i = \{f \in B,\ d(f) \equiv i \bmod n\}$.

2. We will say that B is *graded-independent* if for any $i \in \mathbb{Z}$ the set $\rho(B_i) \subset R_{K/k}$ is linearly independent over $\overline{k}$.

3. We call B a *graded base* for K/k whenever B is graded-independent and generates $k[G]$ as a k-module (so, $B \subset k[G]$).

PROPOSITION 3.1.2. Assume $B \subset K[G] \setminus \{0\}$ is a graded-independent set.

1. Chose a non-zero function $c : B \to k$ and set $m = \min_b(v(c_b) + d(b))$.

Then $d(\sum_{b\in B} c_b b) = m$ and $\rho(\sum_b c_b b) = \sum_{b\in B_m} r(c_b)\rho(b)$.

2. For any $i \in \mathbb{Z}$ we have $\mathfrak{C}_i \cap (\bigoplus_{b\in B} k \cdot b) = \bigoplus_{b\in B} \pi_k^{[(i-d-d(b)-1)/n]+1} b \cdot \mathfrak{o}$.

Moreover, if B contains n elements and $B \subset k[G]$ then B is a graded base for K/k.

PROOF. 1. Both equalities are easy. Obviously, $d(\sum_{b\in B} c_b b) \geqslant m$ and $d(\sum_{b\in B\setminus B_m} c_b b) > m$. Thus it remains to apply Lemma 2.1.2.

2. Follows from assertion 1 immediately. □

REMARK 3.1.3. Consequently, if B is a graded base for K/k then the restriction of the function d (resp. ρ) to B completely determines the values of these functions on $k[G] \setminus \{0\}$.

3.2. Simple calculations for "short compositions" of $(\sigma_i - 1)$

Starting from this moment we will always assume that n is a power of p.

First we recall a statement on ramification jumps in this case.

LEMMA 3.2.1. [[8, Proposition IV.11]]

All ramification jumps of K/k are congruent modulo p.

So we set $\overline{h},\ 0 \leqslant \overline{h} < p$, to be the common residue of the ramification jumps of K/k modulo p.

THEOREM 3.2.2. Let $\sigma_i,\ 1 \leqslant i \leqslant a$, belong to G (we do not assume σ_i to be distinct). We will write $h(\sigma_i)$ for the ramification jumps corresponding to σ_i, $\sum = \sum_{i=1}^a h(\sigma_i)$, $\prod = \prod_{i=1}^a (\sigma_i - 1) \in k[G]$.

Then the following statements are valid.

1. $\prod \in \gamma_{\sum}$ and $p_{\sum}(\prod) \sim \sum_{j=0}^{n-1} (\prod_{l=1}^a (j - l\overline{h}))X^j$ (see (1)).

2. Assume in addition that $a < p$. Then $(X-1)^{n-a-1} \mid p_{\sum}(\prod)$ and $(X-1)^{n-a} \nmid p_{\sum}(\prod)$; hence $d(\prod) = \sum -d$.

Moreover, if $\overline{h} \neq 0$ then $p_{\sum}(\prod) \sim (X^{\overline{h}} - 1)^{n-a-1}$.

3. Assume that $p^a \leqslant n$, $\overline{h} \neq 0$, and for any $i,\ 1 \leqslant i \leqslant a-1$ we have $h(\sigma_{i+1}) - h(\sigma_i) = p^i s_i$, where $s_i \in \mathbb{Z} \setminus p\mathbb{Z}$. Set B to be the set of $\prod (\sigma_i - 1)^{n_i}$ for (n_i) running through all sets of non-negative integers such that $\sum n_i < p$.

Then for any $s \in \mathbb{Z}$ the corresponding set B_s consists of at most one element. Consequently, B is graded-indepent.

PROOF. 1. Assume $(\sigma_i - 1)(\pi) = c_i \pi^{h(\sigma_i)+1} \varepsilon_i$ for some $c_i \in \mathfrak{o}^*$ and $\varepsilon_i \in 1 + \mathfrak{M}$. Then for any $j \in \mathbb{Z}$ we obviously have $(\sigma_i - 1)(\pi^j) = c_i^j \pi^{h(\sigma_i)+j} \varepsilon_{ij}$ for some $\varepsilon_{ij} \in 1 + \mathfrak{M}$; recall here that $h(\sigma_i) > 0$ since K/k is wildly ramified. Combining this statements for all powers of π and all σ_i we easily obtain $p_{\sum}(\prod) = r(\prod c_i) \sum_{j=1}^a (j - l\overline{h}) X^j$. Since $r(\prod c_i) \neq 0$, we obtain the result.

2. Since $X^n - 1 = (X-1)^n$ in $\overline{k}[X]$, for $b \geqslant 0$ we have $(X-1)^{n-b} \mid p_{\sum}(\prod)$ if and only if $(X-1)^b p_{\sum}(\prod) = 0$. Now, the previous assumption implies that the coefficient of $p_{\sum}(\prod)$ at X^j is a non-zero polynomial in $r(j)$ of degree $\sum < p$. Next, in R we have $(X-1)(\sum_{i=0}^{n-1} g(i) X^i) = \sum_{i=0}^{n-1} (g(i-1) - g(i)) X^i$. Hence the well-known formula for the sth difference of a polynomial of degree s gives the divisibility statements in question.

The "moreover" statement is just a simple calculation of coefficients.

3. According to Proposition 3.1.2, if all the sets B_s consist of at most one element then B is graded-independent indeed.

Thus for two sets of non-negative integers (n_i) and (n'_i) whose sums do not exceed $p-1$ it suffices to verify that $\sum n_i h(\sigma_i) \equiv \sum n'_i h(\sigma_i) \bmod n$ implies $(n_i) = (n'_i)$.

Now, for any numbers o_i we have $\sum_{i=1}^{a} o_i h(\sigma_i) = q_1 h(\sigma_1) + \sum_{j=1}^{a-1} q_{j+1} p^j s_j$, where $q_l = \sum_{r=l}^{a} o_i$ for any l, $1 \leqslant l \leqslant a$. Now we take $o_i = n'_i - n_i$; then for any $j \geqslant 0$ clearly $q_j$is an integer that is zero if it is divisible by p. Applying obvious induction we obtain that all q_j vanish; hence $(n_i) = (n'_i)$ and we obtain a contradiction. □

Remark 3.2.3. The case $\overline{h} = 0$ is rather "rare". This can only happen if $\operatorname{char} K = 0$ and G is cyclic; see Proposition III.2.3 of [6] and Exercises IV.2.3(c,f) of [8].[4] Moreover (see Proposition III.2.3 of [6] once again), if $G = \mathbb{Z}/p\mathbb{Z}$ and $\overline{h} = 0$ then for any other Galois extension K'/k with Galois group $\mathbb{Z}/p\mathbb{Z}$ the ramification jump in it is at most p.

3.3. Calculations in the case $G = (\mathbb{Z}/p\mathbb{Z})^2$

Now we pass to to more specific statements. We assume that $K = K_1K_2$, where K_i/k are degree p extensions whose ramification jumps are $h_2 > h_1 > 0$. Thus $n = p^2$, $G = (\mathbb{Z}/p\mathbb{Z})^2$, and simple ramification theory calculations give the following statement.

Proposition 3.3.1. Set σ_1 (resp. σ_2) to be a non-trivial element of G whose restriction to K_2 (resp. K_1) is trivial.

1. Then $p \nmid h_1$.

2. The ramification jumps corresponding to σ_1 and σ_2 equal h_1 and $\tilde{h_2} = ph_2 - (p-1)h_1$, respectively. Moreover, these ramification jumps are prime to p and $h_1 \not\equiv h_2 \bmod p$ if and only if $h_1 \not\equiv \tilde{h_2} \bmod p^2$.

3. $d = (p-1)(ph_2 + h_1)$, and the ramification depths of K_1/k and K_2/k equal $(p-1)h_1$ and $(p-1)h_2$, respectively.

Proof. 1. h_1 is prime to p since $h_1 < h_2$; see Remark 3.2.3.

2. The calculation of jumps in this case is really easy; see Exercise III.3.2b of [6]. It immediately yields the equivalence in questions.

3. We apply the (definition of the depth of ramification along with the) well-known formula for the different given by Proposition 4 in [8, §IV.1]. We immediately obtain the values of ramification depths of K_1/k and K_2/k, and it remains to note that $d = (p-1)(ph_2 - (p-1)h_1) + (p^2-p)h_1$. □

Now we pass to the main specific theorem of this paper. We set $a = i + j$ (for integer i, j, $0 \leqslant i, j \leqslant p-1$) and define the following (piecewise linear) function: we set $H(i,j) = h_1 i + \tilde{h_2} j - d$ whenever $a < p-1$ and $H(i,j) = (pi - (p-1)^2)h_1 + ph_2 j$ otherwise.

We also define the following $P(i,j) \in R_{K/k}$ for (integer) $i, j \geqslant 0$: we set $P(i,j) = (X^{h_1} - 1)^{n-a-1}$ if $a < p-1$. Next, for $i + j \geqslant p-1$ we set $P(i,j) = (\sum_{s=0}^{p-1} (\prod_{l=1}^{i} (s - lh_1)) X^{ps})(\sum_{t=0}^{p-1} (\prod_{l=1}^{j} (t - lh_2)) X^{pt})$.

Theorem 3.3.2. Adopt the notation and assumptions of the previous proposition. For $0 \leqslant i, j \leqslant p-1$ we set $f_{ij} = (\sigma_1 - 1)^i (\sigma_2 - 1)^j \in k[G]$, $a = i + j$.

1. Then for $0 \leqslant i, j \leqslant p-1$ we have $d(f_{ij}) = H(i,j)$ and $\rho(f_{ij}) \sim P(i,j)$.

Consequently, $p \mid d(f_{ij})$ if and only if $a \geqslant p-1$.

2. Moreover, if $p \nmid h_2 - h_1$ then $B = \{f_{ij} : 0 \leqslant i, j \leqslant p-1\}$ is a graded base of K/k.

Proof. 1. We start from the study of $d(f_{ij})$ and $\rho(f_{ij})$.

In the case $a < p-1$ the corresponding statements are given by Theorem 3.2.2(2).

[4] Here we also use the well-known fact that there exists a degree p subextension in K/k whose ramification jump equals the smallest ramification jump of K/k.

Now assume $a \geqslant p-1$. This calculation is the main application of the multiplication $*$ (and of the other statements related to $K \otimes_k K$) in our paper. We note that $f_{ij} = (\overline{\sigma}_1 - 1)^i \circ \mathrm{tr}_1 * (\overline{\sigma}_2 - 1)^j \circ \mathrm{tr}_2$, where $\overline{\sigma}_1$ (resp. $\overline{\sigma}_2$) is the restriction of σ_1 (resp. σ_2) to K_1 (resp. K_2), $tr_{1,2}$ are the trace operators from K into K_1 and K_2, respectively, and $*$ is the coefficientwise multiplication on $K[G]$ introduced in Theorem 2.2.2(3). Next, Theorem 3.2.2(2) allows us to make the corresponding computations in K_1/k and K_2/k easily. We obtain $d^{K_1/k}(\overline{\sigma}_1 - 1)^i = (i-p+1)h_1$ (see Proposition 3.3.1(3)), $\rho^{K_1/k}(\overline{\sigma}_1 - 1)^i \sim \sum_{s=0}^{p-1}(\prod_{l=1}^{i}(s - lh_1))X^s$, $d^{K_2/k}(\overline{\sigma}_2 - 1)^j = (j-p+1)h_2$, $\rho^{K_2/k}(\overline{\sigma}_2 - 1)^j \sim \sum_{s=0}^{p-1}(\prod_{l=1}^{j}(s - lh_2))X^s$. Hence Theorem 2.2.2(3,4) along with Proposition 2.2.4(1,3) imply that $f_{ij} \in \gamma_{H(i,j)}$ and $p_{H(i,j)+d}(f_{ij}) \sim P(i,j)$. It remains to note that $P(i,j) \neq 0$ (in R) since it is not divisible by $(X-1)^n$; see Theorem 3.2.2(2).

Lastly, if $a < p-1$ then $H(i,j) = h_1 i + \tilde{h_2} j - d \equiv h_1 a - d \equiv h_1(p-1-d) \not\equiv 0 \bmod p$; see Proposition 3.3.1. It remains to note that p obviously divides $H(i,j)$ if $a \geqslant p-1$.

2. Firstly, f_{ij} obviously give a k-base of $k[G]$. So, it remains to verify that for any $s \in \mathbb{Z}$ the set $\rho(B_s) \subset R_{K/k}$ is linearly independent over $\overline{k}$, where $B_s = \{f \in B : \ d(f) \equiv s \bmod n\}$.

We consider two cases.

First assume $p \nmid s$. By assertion 1 the corresponding B_s is contained inside the set $B = \{f_{ij} : \ 0 \leqslant i,j, \ i+j < p-1\}$; hence the set B_s consists of at most one element according to Theorem 3.2.2(3).

Now we pass to the case $p \mid s$. The argument is similar to the Proof of Theorem 3.2.2(3). According to assertion 1, $B_s = \{f_{ij} : \ 0 \leqslant i,j \leqslant p-1, \ i+j \geqslant p-1, \ (pi-(p-1)^2)h_1 + ph_2 j \equiv s \bmod n\}$. Hence if (i_1,j_1) and (i_2,j_2) are distinct elements of B_s then $s - p(h_2-h_1)j_1 \not\equiv s - p(h_2-h_1)j_2 \bmod n$. Consequently, $ph_1(i_1+j_1) \not\equiv ph_1(i_2+j_2) \bmod s$. Since $p \nmid h_1$, it follows that for distinct elements of B_s the corresponding values of $i+j$ are distinct; hence $P(i,j)$ are divisible by distinct powers of $X^p - 1$ (see assertion 1). This immediately implies the $\overline{k}$-independence in question.

□

Remark 3.3.3. 1. It is easily seen that the argument used for the computing of $d(f_{ij})$ and $\rho(f_{ij})$ for $i+j \geqslant p-1$ can be vastly generalized. Indeed, assume that totally ramified field extensions K_s/k, $1 \leqslant s \leqslant m$ (for $m > 1$), are linearly disjoint, that is, $K = K_1 \otimes_k K_2 \otimes_k \cdots \otimes_k K_m$ is a field (and their composite). Then the same argument as above implies for any $\alpha_s \in X_{c_s}^{K_s \otimes_k K_s}$ we have $\prod \alpha_s \in X_c$ and $r_c^{K \otimes_k K}(\prod \alpha_s) = g$, where $c = n \sum c_s/n_s$, $n_s = [K_s : k]$, and $g = \prod r_{c_s}^{K_s \otimes_k K_s}(\alpha_s)(X^{n/n_s})$. Moreover, one can easily express $\phi(\prod \alpha_s)$ in terms of $\phi^{K_s/k}(\alpha_s)$.

2. The main question here is whether this g is not zero. Moreover, one would certainly like a large collection of elements of this sort to be graded-independent and their images with respect to ϕ to belong to $k[G]$. We note that $n/n_s \mid d^{K/k}(\phi(\alpha_s))$ and $\rho^{K/k}(\phi(\alpha_s))$ is a polynomial in X^{n/n_s}. Thus, if n_s are powers of p then one doesn't have much chance to obtain a big graded-independent set if $m > 2$.

Now let us describe a setting generalizing that considered in Theorem 3.3.2(2). We assume $m = 2$, $n_1 \geqslant n_2$, $\alpha_s \in X_{c_s}^{K_s \otimes_k K_s}$ for $c_1 \not\equiv c_2 \bmod p$ and both $\prod r_{c_s}^{K_s \otimes_k K_s}(\alpha_s)$ are divisible by $(X-1)$ but not divisible by $(X-1)^2$. Then a straightforward generalization of the arguments used in the Proof of Theorem 3.3.2(2) yields that the set $\phi(\alpha_1^i \cdot \alpha_2^j)$ is graded-independent if (i,j) runs through non-negative integers such that $n_2 i + n_1 j < n$. This set consists of $(n+n_1)/2$ elements. Unfortunately, the authors have no idea how to complete these elements to a graded-independent base (unless $n_1 = p$).

Recall that a vast class of extensions K_s/k that contain α_s satisfying the properties in question was introduced in [2, §3]; these extensions were called *semistable* extensions. Moreover, Theorem 3.5 and Proposition 3.4.1 of ibid. can be used to construct semistable extensions explicitly (for $p \nmid c_s$)

Alternatively, if $\mathrm{char}\, k = 0$, k contains all roots of 1 of degree p^r ($r > 0$), and $K_1 = K(\pi_1)$, where $\pi_1 = \sqrt[p^r]{\pi_k}$ (cf. Remark 3.2.3) then for $\alpha^1 = \pi_1 \otimes \pi_1^{-1} - 1$ one can easily check that $\phi^{K_1/k}(\alpha^1)$ belongs to $k[G]$ as well, $\alpha^1 \in X_0^{K_1 \otimes_k K_1}$, and $r_0^{K_1 \otimes_k K_1}(\alpha^1) = X - 1$.

3. Note that the elements $\phi(\alpha_1^i \cdot \alpha_2^j)$ can be expressed as products of $\phi(\alpha_1)$ and $\phi(\alpha_2)$ with respect to the multiplication $*$; see Theorem 2.2.2(3). It appears that one can replace the elements f_{ij} in Theorem 3.3.2 by elements that can be computed similarly (for certain $\phi(\alpha_1)$ and $\phi(\alpha_2)$ of a rather simple form). Yet we do not use bases of this form in this paper since they are not compatible with (the general) Theorem 3.2.2.

4. Some more associated modules and orders

Throughout this section we will assume that $k_0 \subset k$, k/k_0 is a totally ramified extension of complete discrete valuation fields (yet cf. 4.1.4 below).

In §4.1 we develop the theory of the modules $\gamma_i^0 = \gamma_i \cap k_0[G]$. This enables us to prove an analogue of Theorem 3.3.2(2) in the case where the two ramification jumps are distinct but congruent modulo p.

In §4.2 we consider various associated orders and some more associated Galois modules (we define $\gamma^0(i,j) = \{f \in k_0[G] : \ f(\mathfrak{M}^i) \subset \mathfrak{M}^j\}$). We define and study those graded bases that are convenient for constructing bases of modules of this type; we call them *diagonal bases*. Moreover, we prove that a graded base becomes a diagonal base if we lift the original extension by a tamely ramified extension of degree that is at least $n-1$.

4.1. On relative associated Galois modules

We set $e_0 = [K : k_0]$, $\mathfrak{o}_0 = \mathfrak{o} \cap k_0$ is the ring of integers of k_0, $\pi_0 \in \mathfrak{o}_0$ is an uniformizing element.

Now we define associated Galois modules inside $k_0[G]$.

Definition 4.1.1. Assume $i \in \mathbb{Z}$, $B \subset K[G] \setminus \{0\}$.

1. We set $\gamma_i^0 = \mathfrak{C}_i \cap k_0[G]$.

2. For $i \in \mathbb{Z}$ we set $B_i^0 = B_0^i(K/k_0) = \{f \in B : \ d(f) \equiv i \bmod e_0\}$.

3. We will say that B is k_0-*graded independent* if for any $s \in \mathbb{Z}$ the set $\rho(B_s^0) \subset R_{K/k}$ is linearly independent over $\overline{k}$.

4. We call B a *graded base* for $(K/k, k_0)$ whenever B is k_0-independent and generates $k_0[G]$ as a k_0-module (so, $B \subset k_0[G]$).

Proposition 4.1.2. I. Assume $B \subset K[G] \setminus \{0\}$ is a k_0-graded independent set.

1. Chose a non-zero function $c : B \to k_0$ and set $m = \min_b(v(c_b) + d(b))$.

Then $d(\sum_{b\in B} c_b b) = m$ and $\rho(\sum_b c_b b) = \sum_{b\in B_m} r(c_b)\rho(b)$.

2. For any $i \in \mathbb{Z}$ we have $\mathfrak{C}_i \cap (\bigoplus_{b\in B} k_0 \cdot b) = \bigoplus_{b\in B} \pi_0^{[(i-d-d(b)-1)/n]+1} b \cdot \mathfrak{o}_0$.

II. Assume that L is a k_0-vector subspace of $K[G]$.

Then there exists a k_0-graded independent set $B \subset L$ such that $L = \bigoplus_{b\in B_m} k_0 \cdot b$.

Proof. I. The Proof is easy; it suffices to generalize the Proof of Proposition 3.1.2 in the obvious way.

II. We take B to be the union B_s^0, $0 \leqslant s < e_0$. Here we set each B_s^0 to be a lift to L of any $\overline{k}$-base of $(L \cap \mathfrak{C}_s)/(L \cap \mathfrak{C}_{s+1})$.

Obviously, B is k_0-independent. The number of elements in it clearly equals the length of the $\overline{k}$-module $L \cap \mathfrak{C}_0 / L \cap \mathfrak{C}_{e_0} = (L \cap \mathfrak{C}_0)/\pi_0(L \cap \mathfrak{C}_0)$. Hence it also equals the k_0-dimension of L, and we obtain the result in question. □

Now we are able to generalize Theorem 3.2.2(3) and extend Theorem 3.3.2(2).

Once again we assume that n is a power p. We will use the notation v_p of the p-adic valuation of integers; $w = v_p(e_0)$.

THEOREM 4.1.3. I. In each of the following two cases and for any $s \in \mathbb{Z}$ the corresponding set $B_s^0 \subset \mathbb{Z}[G]$ consists of at most one element.

1. σ_i, $1 \leqslant i \leqslant a$, belong to G, and for the corresponding ramification jumps we have $v_p(h(\sigma_2) - h(\sigma_1)) < v_p(h(\sigma_3) - h(\sigma_2)) < \dots < v_p(h(\sigma_a) - h(\sigma_{a-1})) < w$. We take B to be the set of $\prod(\sigma_i - 1)^{n_i}$, where (n_i) run through all sets of non-negative integers such that $\sum n_i < p$.

2. The assumptions of Theorem 3.3.2(1) are fulfilled and $0 < v_p(h_2 - h_1) < w - 1$. We take $B = \{(\sigma_1 - 1)^i(\sigma_2 - 1)^j : \ 0 \leqslant i, j \leqslant p - 1\}$.

II. Consequently, in case I(2) the set B is a k_0-graded base of $(K/k, k_0)$.

PROOF. I. The Proofs of both assertions are easy and similar to that of Theorem 3.2.2(3). The corresponding values of $\prod(\sigma_i - 1)^{n_i}$ were calculated in Theorem 3.2.2(2) and 3.3.2(1). Now we proceed to our cases using simple modifications of the corresponding arguments above.

1. According to Theorem 3.2.2(2) (and similarly to part 3 of that theorem), it suffices to verify for two sets of non-negative integers (n_i) and (n_i') whose sums do not exceed $p - 1$ that if $\sum n_i h(\sigma_i) \equiv \sum n_i' h(\sigma_i) \bmod e_0$ then $(n_i) = (n_i')$.

Once again, for any numbers o_i we have $\sum_{i=1}^{a} o_i h(\sigma_i) = q_1 h(\sigma_1) + \sum_{j=1}^{a-1} q_{j+1} p^j s_j$, where $q_l = \sum_{r=l}^{a} o_i$ for any l, $1 \leqslant l \leqslant a$. We take $o_i = n_i' - n_i$; then for any $j \geqslant 0$ clearly q_j is an integer that is zero if it is divisible by p. Applying obvious induction we obtain that all q_j vanish; hence $(n_i) = (n_i')$ and we obtain a contradiction.

2. Once again, if $p \nmid s$ then the corresponding values of $i + j$ are less than $p - 1$; see Theorem 3.3.2(1). Hence the statement in question is given by the previous assertion.

Now assume $p \mid s$. According Theorem 3.3.2(1), we should count the pairs $(0 \leqslant i < p, \ 0 \leqslant j < p)$ such that $i + j \geqslant p - 1$ and $(pi - (p-1)^2)h_1 + ph_2 j \equiv s \bmod e_0$. Now, if we have two pairs (i, j) and (i', j') satisfying this congruence then $p^{w-1} \mid h_1(i - i') + h_2(j - j')$. Since $h_1 \equiv h_2 \bmod p$, we obtain $i - i' = j - j$. Lastly, if $p^{w-1} \mid (i - i')(h_1 - h_2)$ then $p \mid i - i'$; hence $i = i'$ and $j = j'$.

II. Immediate from (case 2 of) assertion I combined with Proposition 4.1.2(I). □

REMARK 4.1.4. It can make sense to modify Definition 4.1.1 to obtain more general results. Yet the authors did not check the details here.

1. Firstly, one can try to avoid the assumption that k/k_0 is totally ramified. Then one should take the corresponding base field extension into account; this does not seem to be hard.

2. Secondly, one can probably extend the results of this section to the case where k_0 does not lie in k (but lies in K). The main difficulty here is our definition of the function ρ; note that $\rho(\pi^s f) = X^s \rho(f)$ for any $s \in \mathbb{Z}$ and $f \in K[G] \setminus \{0\}$. It appears that this problem can be avoided if one considers the function $\rho' : \ f \mapsto \rho(\phi(t(\phi^{-1}(f))))$ instead of ρ[5] and applies Proposition 2.2.1(6) (and possibly Theorem 2.2.2(6)).

4.2. Some more associated modules (and orders) and their relation to tame lifts

Unfortunately, the associated order $\gamma(\mathfrak{O}_K) = \{f \in k[G] : \ f(\mathfrak{O}_K) \subset \mathfrak{O}_K\}$ does not have to be equal to any of the γ_i. For this reason, we introduce some more types of associated modules. We modify slightly the notation of [2]. We also extend it to relative modules; however, the reader may ignore this (and assume $k_0 = k$ till the end of this paper).

Below a, b, a', b', i, j will always denote arbitrary integers.

We set $\mathfrak{C}(i, j) = \{f \in K[G] : \ f(\mathfrak{M}^i) \subset \mathfrak{M}^j\}$; $\gamma(i, j) = \mathfrak{C}(i, j) \cap k[G]$ and $\gamma^0(i, j) = \mathfrak{C}(i, j) \cap$ $\cap\, k_0[G]$.

PROPOSITION 4.2.1. 1. $\mathfrak{C}(i, j) = \phi(\mathfrak{M}^j \otimes \mathfrak{M}^{i-d-n+1})$.

2. $\mathfrak{C}_{j-i} \subset \mathfrak{C}(i, j) \subset \mathfrak{C}_{j-i+1-n}$.

[5] Recall that t is the automorphism of $K \otimes_k K$ that swaps the factors of this tensor square

Proof. 1. Recall that the following well-known statement: the different of K/k equals $\mathfrak{M}^{d+n-1}$. Combining it with Theorem 1.2.1 of [2] we obtain the result.

2. Obvious. □

Remark 4.2.2. 1. Consequently, $\gamma^0(i,j)/\gamma^0(j-i)$ is an $\overline{k}$-vector space; it obviously equals the kernel of the $\overline{k}$-linear map $\gamma^0_{j-i+1-n}/\gamma^0_{j-i} \to \mathfrak{C}_{j-i+1-n}/\mathfrak{C}(i,j)$. Now, a graded base B for $(K/k, k_0)$ yields an explicit base of $\gamma^0_{j-i+1-n}/\gamma^0_{j-i}$ (see Proposition 4.1.2(I.2)) and to compute the values on this map on this base. The authors do not think that there exists any nice way for doing this in general. However, if B is "nice enough" then the function ρ is sufficient for this computation.

Below we will essentially demonstrate this in Propositions 4.2.4 and Propositions 4.2.6(1,3). Yet we will work in $K \otimes_k K$ instead of $K[G]$; thus one has to apply the map ϕ^{-1} (along with Theorem 2.2.2(4) and Proposition 4.2.1(1)) to make the corresponding "translation".

2. One may call $\gamma^0(i,i) \subset \gamma(i,i)$ the associated orders of the ideal $\mathfrak{M}^i$. The "most traditional" of them is the ring $\gamma(0,0)$.

Now we study the filtration on $K \otimes_k K$ corresponding to $\mathfrak{M}^a \otimes \mathfrak{M}^b$ for $a, b \in \mathbb{Z}$. The first simple observation here is the following one.

Lemma 4.2.3. Define the following two relations of $\mathbb{Z}^2$: $(a,b) \leqslant^{\mathbb{Z}^2} (a',b')$ if and only if $a \leqslant a'$ and $b \leqslant b'$ and $(a,b) \sim^{\mathbb{Z}^2} (a',b')$ if and only if $a - a' = b' - b = nc$ for some $c \in \mathbb{Z}$.

Then the following statements are valid.

1. $\leqslant^{\mathbb{Z}^2}$ is a partial order relation, and $\sim^{\mathbb{Z}^2}$ is an equivalence relation.

2. Set $X = \mathbb{Z}^2/\sim^{\mathbb{Z}^2}$; we will write $[(a,b)]$ for the $\sim^{\mathbb{Z}^2}$-equivalence class of (a,b). Then $\leqslant^{\mathbb{Z}^2}$ induces a well-defined partial order relation $\leqslant^X$ on X; here we set $[(a,b)] \leqslant^X [(a',b')]$ if and only if $(a,b) \leqslant^{\mathbb{Z}^2} (a'',b'')$ for some $(a'',b'') \sim^{\mathbb{Z}^2} (a',b')$.

3. $\mathfrak{M}^a \otimes \mathfrak{M}^b \supset \mathfrak{M}^{a'} \otimes \mathfrak{M}^b$ if and only if $[(a,b)] \leqslant^X [(a',b')]$.

Proof. Assertions 1 and 2 are obvious. Assertion 3 is very easy as well; cf. the Proof of Proposition 2.2.1(4). □

We will write p^X for the projection $\mathbb{Z}^2 \to X$.

Now we associate certain subsets of X to elements and "ideals" of $K \otimes_k K$.

Proposition 4.2.4. 1. Then α can be presented as $\sum_{(i,j)\in G'(\alpha)} \varepsilon_{ij} \cdot \pi^i \otimes \pi^j$, where $\varepsilon_{ij} \in (\mathfrak{O} \otimes \mathfrak{O})^*$ and $G'(\alpha)$ is a subset of $\mathbb{Z}^2$ such that the images of any two its distinct elements in X are (distinct and) incomparable.

2. The set $G(\alpha) = p^X(G'(\alpha))$ is canonically determined by α.

3. $\alpha \in \mathfrak{M}^a \otimes \mathfrak{M}^b$ if and only if $(a,b) \leqslant (a',b')$ for each $(a',b') \in G(\alpha)$.

Proof. All these statements are rather simple and easily follow from the results of [2, S2.4]; see also Proposition 2.5.2 of ibid. □

Now we define sets that are "graded independent in a strong sense".

Definition 4.2.5. 1. We say that α is *diagonal* if the number $a + b$ is constant on the set $G(\alpha) = \{([a,b])\}$.

Moreover, if this is the case then we will also say that $\phi(\alpha)$ is diagonal.

2. We say that a set $B \subset k[G] \setminus \{0\}$ is k_0-*diagonal* whenever it is k_0-graded independent (see Definition 4.1.1) and for any $s \in \mathbb{Z}$ any non-zero k_0-linear combination of elements of B^0_s is diagonal.

3. For a totally ramified extension K'/k' and $\alpha \in K' \otimes_{k'} K'$ we will write $d^{K'\otimes_{k'}K'}(\alpha) = i$ whenever $\alpha \in X_i \setminus X_{i+1}$.

Proposition 4.2.6. Assume α is diagonal and $d^{K\otimes_k K}(\alpha) = i \in \mathbb{Z}$.

1. Assume $r_i^{K\otimes_k K}(\alpha) = \sum_{l=0}^{n-1} a_l X^l$ (see Theorem 2.2.2(5)). Then $G(\alpha) = \{\ ([(l, i-l)])|\ a_l \neq 0\}$.

2. Assume $\beta \in X_{i+n-1}$. Then $G(\alpha) = G(\alpha+\beta)$.

3. If B is k_0-diagonal and $c : B \to k_0$ is a non-zero function.

Set G' to be the union of $G(\sum_{b\in B_s^0} c(b)b)$ for s running through all those integers such that not all $c(b)$ are zero for $b \in B_s^0$.

Then $G(\sum_{b\in B} c(b)b)$ equals the set of $\leqslant^X$-minima of G'.

Proof. 1. Immediate from our definitions.

2. The statement easily follows from the following simple observation: if $a+b \geqslant n-1$ then $\pi^a \otimes \pi^b \in \mathfrak{O} \otimes \mathfrak{O}$.

3. Choose a representative in $\mathbb{Z}^2$ for each $v \in G'$; denote the set of these representatives by $\tilde{G}'$. Then we can present $\sum_{b\in B} c(b)b = \sum_{(i,j)\in\tilde{G}'} \varepsilon_{ij} \cdot \pi^i \otimes \pi^j$, where $\varepsilon_{ij} \in (\mathfrak{O}\otimes\mathfrak{O})^*$; Lemma 4.2.3(3). Moreover, if $\tilde{G} \subset \tilde{G}'$ is the subset corresponding to all $\leqslant^X$-minima then this lemma allows to convert this expresion into $\sum_{(i,j)\in\tilde{G}} \varepsilon'_{ij} \cdot \pi^i \otimes \pi^j$, where $\varepsilon'_{ij} \equiv \varepsilon \bmod \mathfrak{M}\otimes\mathfrak{O} + \mathfrak{O}\otimes\mathfrak{M}$. According to Proposition 4.2.6(2), this yields $G(\sum_{b\in B} c(b)b) = p_X(\tilde{G})$, and this concludes the Proof. □

Now relate these notions to tame lifts.

Theorem 4.2.7. Assume that K'/k'_0 is a totally ramified extension of complete discrete valuation fields whose degree is a power of p, $k'_0 \subset k' \subset K$, K'/k' is a Galois extension of degree n with Galois group G, k_0/k'_0 is a tamely ramified extension of degree e, and $B \subset K'[G]$ is a k'_0-graded independent set. We take $k = k_0k'$, $K = k_0K'$.

1. Then K'/k'_0 is linearly disjoint with k_0/k'_0.

2. B is also a k_0-independent set in $K[G]$. Consequently, it is a k_0-graded base for $(K/k, k_0)$ if it is a k'_0-graded base of $(K'/k', k'_0)$.

3. Assume in addition that $e \geqslant n-1$. Then B is also k_0-diagonal in $K[G]$.

Proof. 1. Obvious.

2. Immediately follows from Proposition 2.2.4(1,2).

3. Clearly, it suffices to consider the case $B = B_s^0(K'/k'_0)$ for some $s \in \mathbb{Z}$. Moreover, we can clearly assume that $d^{K'\otimes_{k'}K'}(b) = s$ for all $b \in B$. Fix a non-zero linear combination $\alpha = \sum_{b\in B} c_b b$, where $c_b \in k_0$.

Set m to be the minimum of $v(c_b)$. Then Proposition 4.2.6(2) allows us to replace c_b by any c'_b such that $c_b - c'_b \in \mathfrak{M}^{em+n} \cap k_0$. Consequently, we can take $c'_b = \pi_k^{em/n} o_b$ for some $o_b \in \mathfrak{o}_0$. Now, if $b \in B$ and $b = b' + \sum_{0\leqslant l\leqslant n-1} c_{bl}\pi'^l \otimes \pi'^{s-l}$ for some $b' \in X_{s+1}^{K'\otimes_{k'}K'}$ then $d^{K\otimes_k K}(b') \geqslant se+e \geqslant se+n-1$; see Proposition 2.2.4(2). Thus it remains to verify that the element $\alpha = \pi_0^{em/n} \sum_{b\in B,\ 0\leqslant l\leqslant n-1} c_{bl}\pi'^l \otimes \pi'^{s-l}$ is diagonal (in $K\otimes_k K$). Now, applying Proposition 2.2.4(2) one again we obtain that $G(\alpha)$ (is non-empty and) consists of all those $[(me+le, -le)]$ such that $v(\sum_{b\in B} c_{bl}) > 0$, and this concludes the Proof. □

Remark 4.2.8. 1. Combining Theorem 4.2.7 with Theorems 3.2.2(3), 3.3.2(3) and 4.1.3 we obtain certain k_0-diagonal set of elements in extensions that can be obtained as tame lifts of large enough degrees. In particular, this gives an explicit algorithm for computing all associated orders whenever $G = (\mathbb{Z}/p\mathbb{Z})^2$, the ramification jumps in K'/k' are distinct, and the degree of k_0/k'_0 is at least p^2-1; see Remark 4.2.2.

2. However, the authors suspect that the elements $(\sigma_1-1)^i(\sigma_2-1)^j$, $0 \leqslant i,j \leqslant p-1$ give a diagonal base "much more often". Yet we doubt that these elements are "optimal" in all cases; they possibly fail to be diagonally independent if the ramification jumps are "too large" (and $\operatorname{char} k = 0$). Moreover, there probably exist totally ramified Galois extensions such that no diagonal bases exist for them (in contrast to Proposition 4.1.2(II)).

3. Checking that any non-zero k_0-linear combination of elements of B_s^0 is diagonal is rather simple if B_s^0 consists of at most one element. However, it appears that k-diagonal bases satisfying

this assumptions for all s are rather rare. The only family of examples of this sort known to the authors is the one of *stable* extensions introduced in [2, 4.1]. This is a rather big subclass of that of semistable extensions (cf. Remark 3.3.3(2)), and one can easily construct examples of extensions of this sort.

Respectively, our Theorem 4.2.7 essentially generalizes the implication (1) $\Longrightarrow$ (5) in Theorem 4.4 of ibid.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Bondarko M.V., Local Leopoldt's problem for rings of integers in abelian p-extensions of complete discrete valuation fields// Doc. Math. 2000, vol. 5, 657-693.

2. Bondarko M.V., Local Leopoldt's problem for ideals in p-extensions of complete discrete valuation fields// In book: Algebraic Number Theory and Algebraic Geometry: Papers Dedicated to A. N. Parshin on the Occasion of his Sixtieth Birthday, 2002, Contemporary Mathematics, Providence, 27-57.

3. Bondarko M.V., Links between associated additive Galois modules and computation of H^1 for local formal group modules// J. of Number Theory 2003, vol. 101, 74-104.

4. Byott N., Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications// Journal de Theorie des nombres de Bordeaux 1997. vol. 9(1), 201-219.

5. Byott N., Associated orders of certain extensions arising from Lubin-Tate formal groups// Journal de Theorie des nombres de Bordeaux 1997. vol. 9, 449-462.

6. Fesenko I.B., Vostokov S.V., Local Fields and their extensions. A constructive approach/ - Second edition - AMS - Providence - RI - 2002.

7. Leopoldt H.-W., Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers. (German), J. Reine Angew. Math. 201 (1959), 119–149.

8. Serre, J.-P., Local fields/ J.-P. Serre - Springer - 1979.

REFERENCES

1. Bondarko, M.V., 2000, "Local Leopoldt's problem for rings of integers in abelian p-extensions of complete discrete valuation fields", *Documenta Mathematica*, 5, pp. 657–693.

2. Bondarko, M.V., 2002, "Local Leopoldt's problem for ideals in p-extensions of complete discrete valuation fields", in *Algebraic Number Theory and Algebraic Geometry: Papers Dedicated to A. N. Parshin on the Occasion of his Sixtieth Birthday*, Providence: American Mathematical Society, pp. 27–57.

3. Bondarko, M.V., 2003, "Links between associated additive Galois modules and computation of H^1 for local formal group modules", *Journal of Number Theory*, 101, pp. 74–104.

4. Byott, N., 1997, "Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications", *Journal de Théorie des Nombres de Bordeaux*, 9(1), pp. 201–219.

5. Byott, N., 1997, "Associated orders of certain extensions arising from Lubin-Tate formal groups", *Journal de Théorie des Nombres de Bordeaux*, 9, pp. 449–462.

6. Fesenko, I.B., and Vostokov, S.V., 2002, *Local Fields and Their Extensions: A Constructive Approach*, 2nd ed., Providence: American Mathematical Society.

7. Leopoldt, H.W., 1959, "Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers", *Journal für die reine und angewandte Mathematik*, 201, pp. 119–149.

8. Serre, J.P., 1979, *Local Fields*, Springer.

Получено: 14.06.2025
Принято в печать: 17.10.2025