LEOPOLDT’S PROBLEM FOR ABELIAN TOTALLY RAMIFIED EXTENSIONS OF COMPLETE DISCRETE VALUATION FIELDS

M. V. BONDARKO

Abstract. By using methods described in earlier papers of the author, it is proved that, in many cases, if an Abelian totally ramified $p$-extension contains an ideal free over its associated order, then the extension is of the type described and completely classified in an earlier paper of the author (such extensions are said to be semistable). A counterexample to this statement is presented in the case where the conditions on the extension are not fulfilled. Several other properties of extensions in question are proved.

Introduction

The present paper is a continuation of the papers [B1] and [B2], where the ideals that are free over their associated orders (we call them Leopoldt ideals) were studied. The extensions that contain (at least one) Leopoldt ideal are called Leopoldt extensions.

In [B2], a wide class of totally ramified extensions of complete discrete valuation fields (we call them semistable extensions) was introduced. The Galois module structure of the ideals in these extensions was computed completely. It turned out that all such extensions are Leopoldt.

The extensions studied in the still earlier paper [B1] satisfy the following condition: their differents are generated by elements of smaller fields. It was proved that the ring of integers in such an extension is a Leopoldt ideal if and only if the extension is stable (cf. the definition in [B2]).

Our goal in this paper is to extend the result of [B1] to the general case. We prove that, under some conditions, any Leopoldt Abelian extension is semistable. An informal discussion in Subsection 2.3 shows that “most” extensions do satisfy these conditions. Thus, we may say that the Leopoldt problem (i.e., the problem of classifying the Leopoldt extensions) is solved for “most” of the local Abelian extensions.

In §1 we recall the main definitions and statements of the earlier papers. Since only complete discrete valuation fields are treated here, we restrict ourselves to this case only. The properties of the identification $\phi$ of $K \otimes_k K$ and $K[G]$ are crucially important. The proofs can be found in [B1]. We also recall the definition of a diagram and of a semistable extension. The details can be found in [B2].

In §2 we study the categorical properties of Leopoldt extensions. Also, we investigate the categorical properties of semistable extensions and construct bases of associated modules in intermediate extensions. The section finishes with the proof of the fact that, under some restrictions, the ramification jumps of a Leopoldt extension are congruent modulo $n = [K : k]$.

In §3, we formulate the main theorem for the general case. The statement is rather clumsy. However, it can be checked that most extensions satisfy the conditions of the

2000 Mathematics Subject Classification. Primary 12F99.

Key words and phrases. Semistable extension, Leopoldt ideal.
Theorem. The proof is by induction and requires investigation of the minimally unstable extensions, i.e., Leopoldt unstable extensions that contain semistable subextensions of index \(p\). We construct an element similar to \(\xi\) in [B2] and use its powers in the sense of the multiplication \(*\) to write out bases of associated modules.

In §4 we make some computations of diagrams (see the definitions in §1) in the minimally unstable case. That allows us to conclude the proof.

In §5 we discuss some alternatives to the main theorem. In particular, we formulate the theorem in the case where the \(p\)th root of unity \(\zeta_p\) belongs to \(k\). In that case, it is possible to get rid of the upper bounds on the ramification jumps. Since the proof of this theorem differs only slightly from the proof of the general case, it suffices to mention the main details. After that, we formulate and prove another version of the main lemma, which also can be used for the induction step. At the end of the section, we construct an example of an unstable extension that contains ideals that are free over their associated orders. This shows that the conditions on the main theorem are “almost best possible”.

The author is deeply grateful to professor S.V.Vostokov for his help and advice.

§1. Main definitions and statements of the papers [B1] and [B2]

1.1. Let \(K/k\) be a Galois extension of degree \(n\) of a complete discrete valuation field whose Galois group is \(G\). We assume that the characteristic of the residue field for \(k\) is equal to \(p\). The extension \(K/k\) will be a totally ramified \(p\)-extension of degree \(n = p^l\).

The trace map from \(K\) into \(k\) will be denoted by \(\text{tr}\). For any extension \(L/F\), we denote its ramification index by \(e(L/F)\). The normalized valuations on \(k\) and \(K\) are denoted by \(v_0\) and \(v\), respectively. Also, let \(v_0\) be the valuation on \(k_{\text{alg}}\) that coincides with \(v_0\) on \(k\); here \(k_{\text{alg}}\) is the algebraic closure of the field \(k\). We denote the integral closure of \(\mathfrak{o}\) in \(K\) by \(O_K\) and the different of the extension \(K/k\) by \(D\).

Usually, by a basis of an associated module we mean its \(\mathfrak{o}\)-basis. A primitive root of unity of degree \(p\) will be denoted by \(\zeta_p = \zeta_p\).

We consider the Galois algebra \(K \otimes_k K\). It is easily seen that, as a \(k\)-algebra, the tensor product \(K \otimes_k K\) is isomorphic to a direct sum of \(n\) copies of \(K\). More precisely, let \(K_\sigma, \sigma \in G\), denote a field isomorphic to \(K\).

Lemma 1.1.1. There is an isomorphism

\[
\psi : K \otimes_k K \rightarrow \bigoplus_{\sigma \in G} K_\sigma,
\]

where \(\psi = \sum_\sigma \psi_\sigma\), and the projection \(\psi_\sigma\) to the coordinate \(\sigma\) is defined by the formula

\[
\psi_\sigma(x \otimes y) = x\sigma(y) \in K_\sigma.
\]

Now we construct a map \(\phi\) from the Galois algebra \(K \otimes_k K\) into the group algebra \(K[G]\):

\[
\phi : K \otimes_k K \rightarrow K[G],
\]

\[
\alpha = \sum_i x_i \otimes y_i \rightarrow \phi(\alpha) = \sum_i x_i \left( \sum_{\sigma \in G} \sigma(y_i)\sigma \right).
\]

Clearly, the function \(\phi(\alpha)\) acts as follows:

\[
\phi(\alpha)(z) = \sum_i x_i \text{tr}(y_i z), \quad z \in K.
\]

In terms of \(\psi_\sigma\), the map \(\phi\) can be expressed as

\[
\phi(\alpha) = \sum_\sigma \psi_\sigma(\alpha)\sigma, \quad \alpha \in K \otimes_k K.
\]
Proposition 1.1.2. The map φ is an isomorphism of the k-vector spaces \( K \otimes_k K \) and \( K[G] \).

We need some properties of permutations of coordinates in \( K \otimes_k K \).

Proposition 1.1.3. Let i be the map that permutes the components in \( K \otimes_k K \).

1) For any \( \sigma \in G \) and \( \alpha \in K \otimes_k K \), we have

\[
\psi_\sigma(\alpha_1) = \sigma \psi_{\sigma^{-1}}(\alpha) = \psi_{\sigma^{-1}}(\alpha).
\]

2) If \( \phi(\alpha) \in k[G] \), then \( \phi(i(\alpha)) \in k[G] \).

The proof can be found in [B2], Subsection 3.2. We let i also denote the map \( \phi \circ i\phi^{-1} : K[G] \to K[G] \).

1.2. Modules of homomorphisms for a pair of ideals. For any pair of nonzero fractional ideals \( I_1, I_2 \) of the field \( K \), we define the following modules:

\[
\mathcal{C}_{K/k}(I_1, I_2) = \text{Hom}_\phi(I_1, I_2),
\]

\[
\mathfrak{A}_{K/k}(I_1, I_2) = \{ f \in k[G] \mid f(I_1) \subseteq I_2 \}.
\]

We call them the associated modules for \( I_1, I_2 \). Obviously, any \( \sigma \)-linear map from \( I_1 \) into \( I_2 \) extends to a \( k \)-linear homomorphism from \( K \) into \( K[G] \). Now we consider the group algebra \( K[G] \). This algebra acts on \( K \); each element of \( \text{Hom}_k(K, K) \) can be expressed uniquely as an element of \( K[G] \). Therefore, we assume that \( \mathcal{C}_{K/k}(I_1, I_2) \subseteq K[G] \).

An ideal \( J \) is called a Leopoldt ideal if it is free over \( \mathfrak{A}_{K/k}(I, I) \). An extension \( K/k \) is called a Leopoldt extension if \( K \) contains a Leopoldt ideal.

Following Hyodo [H], we define the depth of ramification of \( K/k \) with respect to \( K \) as the minimum of

\[
v(tr x) - v(x)
\]

over \( x \in K^* \). We denote this quantity by \( d = d_{K/k} \). It is well known that

\[
d = v_K(\mathfrak{D}) - e(K/k) + 1.
\]

We need a filtration on \( K[G] \), indexed by one parameter. We define

\[
\mathcal{C}_i = \{ f \in K[G] : \min_{x \in K^*} (v(f(x)) - v(x)) \geq i \},
\]

\[
\mathfrak{A}_i = \mathcal{C}_i \cap k[G] = \{ f \in k[G] : \min_{x \in K^*} (v(f(x)) - v(x)) \geq i \}.
\]

Also, we denote

\[
X_i = \sigma(a \otimes b \mid v(ab) \geq i), \quad X_i \subseteq K \otimes_k K.
\]

The associated modules can be described nicely with the help of the map \( \phi \).

Theorem 1.2. For the associated modules we have

\[
\mathcal{C}_{K/k}(I_1, I_2) = \phi(I_2 \otimes_k I_1^*),
\]

\[
\mathcal{C}_i = \phi(X_{i-d}),
\]

where \( I_1^* = \mathfrak{D}^{-1}I_1^{-1} \).

This statement is proved by applying the standard duality of ideals of complete discrete valuation fields.
1.3. Multiplication on $K[G]$. On the algebra $K \otimes_k K$, there is a natural multiplication: $(a \otimes b) \cdot (c \otimes d) = ac \otimes bd$. Using it and the bijection $\phi$, we can define a multiplication on $K[G]$. More precisely, if $f, g \in K[G]$, then we define

$$f \ast g = \phi(\phi^{-1}(f) \cdot \phi^{-1}(g)) \in K[G].$$

The identity below can be checked easily by direct computation.

Proposition 1.3.1. If $f = \sum_\sigma a_\sigma \sigma$ and $g = \sum_\sigma b_\sigma \sigma$, then

$$f \ast g = \sum_\sigma a_\sigma b_\sigma \sigma.$$

Remark 1.3.2. The above formula will be used in what follows as an alternative definition of the multiplication $\ast$.

Theorem 1.2 immediately implies the main result about the behavior of $\ast$ on associated modules.

Proposition 1.3.3. 1. For $f \in \mathcal{E}_{K/k}(I_1, I_2)$, $g \in \mathcal{E}_{K/k}(I_3, I_4)$ we have

$$f \ast g \in \mathcal{E}_{K/k}(I_1 I_3 \mathcal{O}, I_2 I_4).$$

2. For $f \in \mathcal{E}_i$, $g \in \mathcal{E}_j$ we have

$$f \ast g \in \mathcal{E}_{i+j-d}.$$

From this proposition, it is easy to deduce similar statements for the modules $\mathcal{A}_i$ and $\mathcal{A}_{K/k}(I_1, I_2)$.

1.4. The notion of a diagram. We supply $K[G]$ with the filtration generated by the modules $\mathcal{E}_{K/k}(I_1, I_2)$. It is convenient to describe this filtration with the use of the map $\phi$.

Consider the lattice $\mathbb{Z}^2$. We introduce a partial ordering on it: $(x_1, y_1) \leq (x_2, y_2) \iff x_1 \leq x_2, y_1 \leq y_2$. Now we define an equivalence relation on $\mathbb{Z}^2$: $(x_1, y_1) \sim (x_2, y_2) \iff (x_1 - x_2, y_1 - y_2) = k(n, -n), k \in \mathbb{Z}$. The ordering on $X = \mathbb{Z}^2/\sim$ obtained from $<$ will also be denoted by $\prec$. For notational convenience, we shall often indicate an element $x \in X$ by one element $z \in \mathbb{Z}^2$ such that $[z] = x$.

For an element $\omega \in K[G]$, we consider its preimage $\beta = \phi^{-1}(\omega) \in K \otimes_k K$ and write

$$\beta = \sum_{i \in \mathbb{Z}, 0 \leq j < n} a_{ij} \pi^i \otimes \pi^j, \quad a_{ij} \in \mathfrak{o}.$$

We demand that, in this expansion, $a_{ij} \in \mathfrak{o}^*$ or $a_{ij} = 0$. Consider the set $R = \{(i, j) : a_{ij} \neq 0\} \subset X$. We choose a set of minimums in $R$ with respect to the ordering $<$ and denote it by $G(\omega) = G(\beta)$. It is easily seen that $G(\omega)$ does not depend on our choice of $\pi$, because if an element $\pi^i \otimes \pi^j$ is written as a sum of $a_s \pi^{i_s} \otimes \pi^{j_s}, a_s \in \mathfrak{o}$, then some pair $(i_s, j_s)$ either is equal to $(i, j)$ or is smaller than $(i, j)$ with respect to $<$. For an element $\omega \in K[G]$, we consider its preimage $\beta = \phi^{-1}(\omega) \in K \otimes_k K$ and write

$$\beta = \sum_{i \in \mathbb{Z}, 0 \leq j < n} a_{ij} \pi^i \otimes \pi^j, \quad a_{ij} \in \mathfrak{o}.$$

We demand that, in this expansion, $a_{ij} \in \mathfrak{o}^*$ or $a_{ij} = 0$. Consider the set $R = \{(i, j) : a_{ij} \neq 0\} \subset X$. We choose a set of minimums in $R$ with respect to the ordering $<$ and denote it by $G(\omega) = G(\beta)$. It is easily seen that $G(\omega)$ does not depend on our choice of $\pi$, because if an element $\pi^i \otimes \pi^j$ is written as a sum of $a_s \pi^{i_s} \otimes \pi^{j_s}, a_s \in \mathfrak{o}$, then some pair $(i_s, j_s)$ either is equal to $(i, j)$ or is smaller than $(i, j)$ with respect to $<$. For an element $\omega \in K[G]$ we consider its preimage $\beta = \phi^{-1}(\omega) \in K \otimes_k K$ and write

$$\beta = \sum_{i \in \mathbb{Z}, 0 \leq j < n} a_{ij} \pi^i \otimes \pi^j, \quad a_{ij} \in \mathfrak{o};$$

we assume that for any $x \in X$ the set of $(i, j)$ such that $(i, j) \prec x$ and $a_{ij} \neq 0$ is finite. It is easily seen that for any $A \subset \mathbb{Z}^2$ such that $A/\prec = X$, any element $\beta$ can be written in the form (3) so that $a_{ij} \neq 0 \implies (i, j) \in A$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proposition 1.4.2. The following statements are equivalent:
1) \((u, v) \in G(\omega)\);
2) \(v(x) = -d - v \implies v(\omega(x)) = u\).

This proposition can be used for checking that \(G(\omega)\) is well defined.

1.5. Now we study the diagram of the \(*\)-product of two elements of \(K[G]\). For two sets \(A, B \subset X\), we denote their elementwise sum by \(A + B\).

Proposition 1.5.1.
\[
D(f * g) = D(f) + D(g).
\]

In order to refine this statement, we assign coefficients to the generators of diagrams.

Fixing a prime element \(\pi\) of the field \(K\), we introduce the function \(r : K^* \to \bar{k}\), \(r(x) = x\pi^{-v(x)} \mod \mathcal{M}\). Obviously, \(r(xy) = r(x)r(y)\).

Definition 1.5.2. For all \((i, j) \in G(\beta)\), define \(r(i, j)\): \(r(i, j) = a_{ij} \mod \mathcal{M} = r(a_{ij} \pi^i \pi^j) \in \bar{k}\), where \(a_{ij}\) is the coefficient of \(\pi^i \pi^j\) in (3).

It is easily seen that \(r(i, j)\) does not depend on the choice of an expansion of the form (3).

Proposition 1.5.3. Suppose the point \((u, v)\) is a generator of \(D_f + D_g\), \(a = \phi^{-1}(f) = \sum a_{ij} \pi^i \pi^j\) and \(b = \phi^{-1}(g) = \sum b_{ij} \pi^i \pi^j\) are expansions of the from (3), and \(\sum a_{ij} b_{u-iv-j} \in \omega^*\). Then in any expansion of \(ab\) of the form (3), the coefficient of \(\pi^u \pi^v\) is congruent to \(\sum a_{ij} b_{u-iv-j} \mod \mathcal{M}_{\omega}\), whence \((u, v) \in G(f * g)\).

1.6. Diagonals of diagrams.

Definition 1.6.1. The set \(\{(i, j) \in X, i + j = w\}\) will be called the \(w\)th diagonal of \(X\). The set of points \((i, j) \in G(\beta)\) such that the value of \(i + j\) is minimal is the lower diagonal of \(\beta\); we denote \(i + j\) by \(d(\beta)\). The lower diagonal of \(D(\beta)\) is denoted by \(N(\beta)\).

Also, with \(\beta\) we associate an element of the algebra \(\mathfrak{J} = \mathcal{K}[X]/(X^n - 1)\):
\[
p(\phi(\beta)) = p(\beta) = \sum_{i+j=d(\beta)} r(a_{ij})X^i.
\]

Note that \(X^i = X^j\) if \(i\) and only if \(i \equiv j \mod n\). From now on we shall identify such powers of \(X\).

Certainly, \(p(\beta)\) does not depend on the choice of an expansion of \(\beta\) of the form (3).

Proposition 1.6.2. For the lower diagonal of \(\beta\) we have \(d(\beta) = \min_{x \in K^*}(v(\phi(\beta)(x)) - v(x)) - d\).

The following statement describes the structure of the graded ring \(\bigoplus X_i/X_{i+1}\).

Proposition 1.6.3. 1) \(d(f * g) \geq d(f) + d(g)\).
   2) \(d(f * g) = d(f) + d(g)\) if and only if \(p(f)p(g) \neq 0\). In this case we have \(p(f * g) = p(f)p(g)\).

It is easy to describe how the quantities defined above change when we lift an extension by an (at most) tamely ramified one.

Proposition 1.6.4. Let \(E/k\) be a tamely ramified extension, let \(a\) be the residue of the ramification index of \([E : k]\) modulo \(n\), and let \(F = EK\). If \(p(\beta) = m(X) \in \mathfrak{J}\), then for \(\beta_* \in F \otimes_E F\) we have \(p(\beta_*) = m(X^a)\) and \(d(\xi_*) = ed(\beta)\).
1.7. Semistable extensions and their properties. Now we define a principal subclass of Leopoldt extensions.

**Definition 1.7.1.** An extension $K/k$ is said to be semistable if for some $c$ prime to $p$ there exists an element $\xi \in k[G]$ such that $d(\xi) = c$ and $p(\xi) = aX^c - a$ for some $a \in \overline{k}$.

We may assume that the number $c = c(K/k)$ is equal to the residue $-h \mod n$ (i.e., $0 < c < n$). The following statement implies that $c$ is an invariant of a semistable extension $K/k$.

**Proposition 1.7.2.** 1) If $\xi \in k[G]$ and $N(\xi) = \{(0, c); (c, 0)\}$,

then $\xi$ satisfies the conditions of Definition 1.7.1.

2) If $K/k$ is semistable, then all ramification numbers of $K/k$ are congruent to $-c$ modulo $n$.

3) $p(\xi^i) = (X^c - 1)^j$ and $d(\xi^j) = je$ for $0 \leq j < n$, where the power is taken with respect to the multiplication $\ast$.

4) For any $y \in k$ with $v(y) = -d$ we have $v(\xi^i(y)) = i - d$.

The conditions imposed on $\xi$ in Definition 3.1.1 of [B2] were even weaker than those in item 1) of Proposition 1.7.2. The equivalence of the two definitions was proved in Subsection 3.2 of [B2]. The equivalence of Definition 1.7.1 to several other assertions was proved in [B2], Theorem 4.4.

In Subsection 4.3 of [B2], the third and the fourth part of Proposition 1.7.2 allowed us to construct a “power” (with respect to $\xi$ and $\ast$) base for all $A_i$ and prove that $A_i(y) = M_i^{-d}$. Moreover, it was proved that all semistable extensions are Leopoldt.

In [B2] it was proved that an Abelian extension is semistable if and only if it is Kummer for some formal group and certain conditions on the valuation of the root of the corresponding equation are fulfilled. Thus, we may say that the Abelian semistable extensions were described completely in [B2]. The non-Abelian semistable extensions will be classified in one of the subsequent papers. We do not formulate the corresponding statements here because now we shall not need them.

1.8. Indecomposable and free ideals. An essential tool in the study of Leopoldt ideals is the following statement, which was formulated in [B2]. The idea of the proof was proposed by N. Byott.

**Lemma 1.8.1.** Suppose that, in a totally ramified extension $K/k$, an ideal $I = M^i$ is Leopoldt and $A_{K/k}(I, I)$ is indecomposable (i.e., contains no nontrivial idempotents). Then for any $y \in K$ such that $v(y) = i + (-c - i) \mod n$ we have $A_{K/k}(I, I)y = I$.

**Remark 1.8.2.** If char $k > 0$, then $k[G]$ is indecomposable, so that all $A_{K/k}(I, I)$ are also indecomposable. For char $k = 0$ and Abelian $K/k$, in [BVZ] it was proved that all ideals of $K$ are indecomposable (and so are $A_{K/k}(I, I)$) if and only if $K/k$ is not almost maximally ramified, i.e., $n \not| D_{K/k}$.

§2. Categorical properties of Leopoldt extensions

2.1. General properties.

**Proposition 2.1.** 1) Suppose that an ideal $I$ is free over $A_{K/k}(I, I)$ and that $F$ is a normal intermediate extension in $K/k$, Gal($F/k) = G$/Gal($K/F) = G/H$, $m = [K : F]$. 

The ideal $I_F = \text{tr}_{K/F} I$ of the field $F$ is free over its associated order and $\mathfrak{A}_{F/k}(I_F, I_F) = S_{K/F}(\mathfrak{A}_{K/k}(I, I))$, where $S_{K/F}$ is the map from $k[G]$ into $k[G/H]$ defined by the formula

$$S_{K/F} \left( \sum_{\sigma \in G} a_\sigma \sigma \right) = \sum_{\tau \in G/H} \sum_{\sigma \in \tau} a_\sigma \tau.$$ 

2) Let $E/k$ be an extension with ramification index $e'$, $(e', p) = 1$. Suppose that the ideal $I = \mathfrak{M}_L$ in the extension $L = EK$ is free over $\mathfrak{A}_{L/E}(I, I)$ and its associated order is indecomposable. Then the ideal $I' = \mathfrak{M}^{-d - \left(\frac{\deg e'}{2} - 2\right) \mod n}$ in the extension $K/k$ is free over $\mathfrak{A}_{K/k}(I', I')$ and $\mathfrak{A}_{K/k}(I', I') = \mathfrak{A}_{L/E}(I, I) \cap k[G]$.

Proof. 1) Let $I$ be equal to $\mathfrak{A}_{K/k}(I, I)(y), y \in I$. Then we have $\text{tr}_{K/F} \mathfrak{A}_{K/k}(I, I)(y) = S_{K/F}(\mathfrak{A}_{K/k}(I, I)(\text{tr}_{K/F} y)) = I_F$. Moreover, if $f, g \in S_{K/F}(\mathfrak{A}_{K/k}(I, I)), f = S_{K/F}(f'), g = S_{K/F}(g')$, then $f \circ g = S_{K/F}(f' \circ g')$, whence $S_{K/F}(\mathfrak{A}_{K/k}(I, I))$ is an $\sigma$-algebra. We see that $S_{K/F}(I_F, I_F) = S_{K/F}(\mathfrak{A}_{K/k}(I, I))$ and $I_F = S_{K/F}(I_F, I_F)(\text{tr}_{K/F} y)$.

2) There is no loss of generality in assuming that $i \leq -d < i + n$. Then we choose $y \in K$ such that $\nu_L(y) = e' \nu(y) = -de'$. Let $I$ be free over $\mathfrak{A}_{K/k}(I, I)$ by Proposition 1.8.1, we obtain $I = \mathfrak{A}_{K/k}(I, I)(y)$. Thus, for $f \in E[G]$, we have $f \in \mathfrak{A}_{K/k}(I, I) \iff f(y) \in I$. Then for $f \in k[G]$ we obtain the equivalence $f \in \mathfrak{A}_{K/k}(I, I) \cap k[G] \iff f(y) \in I \cap K$. On the other hand, $\mathfrak{A}_{L/E}(I, I) \cap k[G]$ is an intersection of rings and so is a ring. We conclude that $\mathfrak{A}_{K/k}(I', I') = \mathfrak{A}_{L/E}(I, I) \cap k[G]$ and $I' = \mathfrak{A}_{K/k}(I', I')(y)$. 2
\[ v_F(x) = -d_{F/k} - c, \]  
\[ \text{then } v_F(\xi_{G/H}(x)) = 0 \] and  
\[ \min_{x \in E} (v_F(\xi_{G/H}(x)) - v_F(x)) = d_{F/k} + c. \]  
Thus,  
\[ N_{F/k}(\xi_{G/H}) = \{(c, 0), (0, c)\}. \]

3. The fact that  
\[ N(\xi_s) = \{(ce', 0), (0, ce')\} \]  
follows immediately from Proposition 1.6.4. Now Proposition 1.7.2 implies that \( L/E \) is semistable. \( \square \)

**Proposition 2.2.2.** Suppose that the extension \( KE/E \) is semistable,  
\[ N(\xi_E) = \{(ce', 0), (0, ce')\}, \]  
\( E/k \) is finite, and \( \overline{E}/\overline{k} \) is separable. Then \( K/k \) is also separable and there exists an element  
\[ x \in \mathfrak{o}_E^{*} \]  
such that  
\[ x = \sum_{\sigma \in G} \text{tr}_{E/k}(xa_{\sigma}) \sigma \]  
we have  
\[ N_{K/k}(\xi') = \{(c, 0), (0, c)\}. \]  
If \( E/k \) is totally ramified, then any \( x \in \mathfrak{o}_E^{*} \) fits.

**Proof.** Take  
\[ y \in L \]  
and put  
\[ v_L(y) = -e'd. \]  
We have  
\[ v_L(\xi_E(y)) = ce' \]  
(see Proposition 1.4.2). Since \( \overline{E}/\overline{k} \) is separable, there exists  
\[ x \in \mathfrak{o}_E^{*} \]  
such that  
\[ v_L(\xi'(y)) = v_L(\text{tr}_{L/k}(x\xi_E(y))) = ce'. \]  
If \( E/k \) is totally ramified, then we can take any \( x \) with such a valuation. Moreover, for any \( x \in L \) we have  
\[ v_L(\xi'(x)) \geq v_L(\xi(x)). \]  
Then  
\[ d_{L/E}(\xi') = ce', \]  
whence  
\[ d_{K/k}(\xi') = c. \]  
Also, we see that the lower diagonal of \( \xi' \) cannot contain more than two points. Since  
\[ n \mid d_{K/k}(\xi'), \]  
the set  
\[ N_{K/k}(\xi') \]  
cannot consist of one point. Thus,  
\[ N_{K/k}(\xi') = \frac{1}{\sigma} N_{L/E}(\xi) = \{(c, 0), (0, c)\}. \]  
The proposition is proved. \( \square \)

Remark 2.2.3. A similar result can be proved in the case where \( E/k \) is not necessarily separable and finite if we replace the function \( \text{tr} xa \) in the formula for \( \xi' \) by any projector of \( K \) onto \( k \) that does not reduce the valuations.

Remark 2.2.4. With the help of the elements described in this subsection, we can express the Galois structure of ideals and construct bases of associated modules by using the formulas in [B2], Corollary 4.2.2 and Theorem 4.3.2. We can also do that for any extension \( K/f \) such that \( K/k \) is Abelian and \( k/f \) is tamely ramified.

2.3. We prove a theorem about congruence modulo \( n \) of the ramification jumps of \( G = \text{Gal}(K/k) \) in a Leopoldt extension.

**Theorem 2.3.1.** Let \( h_{\min} \) be the smallest ramification jump for the extension \( K/k \). Suppose that the inequality  
\[ h(\text{min}(p - 1) \geq 2n \]  
is fulfilled. In the case where  \( \text{char} k = 0 \), we also assume that  
\[ h \leq \frac{2n}{p-1}, \]  
where \( h \) is the greatest ramification jump for the group \( G \). If there is an ideal \( I \) free over its associated order in the extension \( K/k \), then all ramification jumps of \( K/k \) are congruent modulo \( n \).

**Proof.** Suppose  
\[ I = \mathfrak{M}^p \]  
is free over  \( \mathfrak{A}_{K/k}(I, I) \). We choose an element  
\[ g \in G \]  
such that the corresponding ramification jump is equal to \( h \). Obviously, the subgroup generated by \( g \) in the group \( G \) is normal. We introduce the following notation:  
\[ K_1 = K^H, \ H = \langle g \rangle. \]  
We have  \( g^p = 1 \), so that  \( [K : K_1] = p \). If  \( \sigma \in G \setminus H \) and the ramification jump corresponding to \( \sigma \) is equal to \( h_{\sigma} \), then, by ramification theory, the ramification jump corresponding to the element \( \sigma/H \) in the extension \( K_1/k \) is also equal to \( h_{\sigma} \).

Let \( y \) be a Galois generator of the ideal \( I \), i.e.,  
\[ y \in I \]  
and  
\[ I = \mathfrak{A}_{K/k}(I, I)y. \]  
We choose an element  \( t \in K \) such that  \( v(t) = (1 - p)h \) and  \( \text{tr}_{K_1/K}, t = 1 \). Now, let  
\[ x = (g - 1)^p - 2t. \]  
We may assume that  
\[ x \in I \setminus \mathfrak{M}_e I. \]  
Thus, there exists an element \( \xi \in \mathfrak{A}_{K/k}(I, I) \setminus \mathfrak{M}_e \mathfrak{A}_{K/k}(I, I) \) satisfying \( \xi(y) = x \). By Theorem 1.2.1, the element  \( \alpha = \phi^{-1}(\xi) \) belongs to  
\[ I \otimes \mathfrak{D}^{-1} I^{-1}. \]

We show that \( \alpha \) can be written as

\[ (6) \quad \alpha = x \otimes q + v + w, \quad q \in \mathfrak{D}^{-1} I^{-1}, \quad v \in (K_1 \cap I) \otimes \mathfrak{D}^{-1} I^{-1}, \quad w \in \mathfrak{M}_e^2 I \otimes \mathfrak{D}^{-1} I^{-1}. \]

First, we prove that any element \( r \in K \otimes_k K \) can be expanded in a sum of the form

\[ (7) \quad \sum x_s \otimes y_s, \quad x_s \in I, \quad y_s \in \mathfrak{D}^{-1} I^{-1}, \]
where all \(v(x_s)\) are distinct modulo \(n\) and all \(v(y_s)\) are distinct modulo \(n\). We start with presenting \(r\) in the form

\[
\sum_{i \leq s, -d - n - i < j \leq -d - i} a_{sj} \pi^s \otimes \pi^j, \quad a_{sj} \in \mathfrak{o}^*.
\]

We order the set of pairs \(\{(s, j) : i \leq s, -d - i \leq j < n - d - i\}\) in the following way: \((s_1, j_1) < (s_2, j_2)\) if \(ns_1 + j_1 < ns_2 + j_2\). Now, from two summands \(x \otimes y\) and \(z \otimes t\) with \(v(x) = v(y)\) mod \(n\), \(v(x) \leq v(z)\) we extract a term of the form \(x \otimes (y + ct)\), where \(c \in \mathfrak{o}\) and \(cx\) is congruent to \(z\) modulo \(\mathfrak{M}^v(z+1)\). In case \(v(y) = v(t)\), \(v(x) < v(z)\), we extract \((x + cz) \otimes y\) with \(c \in \mathfrak{o}^*, c \equiv \frac{1}{y} \mod \mathfrak{M}\). It is easily seen that the element remaining after such an extraction can be expanded in a sum of \(a_{s_j} \pi^s \pi^j\), where \((s, j)\) is greater than \((v(z), v(t))\) in the sense of \(<\). Using this procedure, we can increase successively the minimum (with respect to \(<\)') of the pairs \((s, j)\) such that our expansion contains \(x \otimes y\) and \(z \otimes t\) for which \(v(x) = s\), \(v(y) = j\), \(v(t) = j\) or \(v(z) = s\) mod \(n\) and \((s, j) > (v(z), v(t))\). This process leads (possibly, in the limit) to the desired representation (7). Similarly, from the representation of \(\alpha\) in the form (7), we can extract an element \(v \in K_1 \cap I \otimes \mathfrak{D}^{-1} I^{-1}\) such that what remains is a sum \(\sum x_s \otimes y_s\), where all \(v(x_s)\) are distinct modulo \(n\) and do not contain \(p\), and all \(v(y_s)\) are distinct modulo \(n\). Now we show that in the resulting representation there is only one summand that does not belong to \(\mathfrak{M}_o^2 I \otimes \mathfrak{D}^{-1} I^{-1}\) and this summand is of the form \(x \otimes q, q \in \mathfrak{D}^{-1} I^{-1}\). Indeed, it is easy to check that \(\xi(I) \mod \mathfrak{M}_o^2 I \subset ax \oplus K_1 \cap I \mod \mathfrak{M}_o^2 I\); an argument of this type can be found before Lemma 3.4.1 (here we use the fact that the element \(g\) lies in the center of \(G\) because its ramification jump is maximal). Suppose we have summands \(x_s \otimes y_s \notin \mathfrak{M}_o^2 I \otimes \mathfrak{D}^{-1} I^{-1}, y_s \in \mathfrak{D}^{-1} I^{-1} \setminus \mathfrak{M}_o \mathfrak{D}^{-1} I^{-1}\). We assume that \(v(x_0) \neq -h \mod n\). The nondegeneracy of the \(o\)-pairing \(\langle u, v \rangle = \text{tr}(uv)\) on \(I \otimes \mathfrak{D}^{-1} I^{-1}\) implies the existence of \(u \in I\) such that \(\text{tr}(uy_s) = 0\) for \(s > 0\) and \(\text{tr}(uy_0) = 1\). We obtain

\[
\xi(u) \equiv \sum_s x_s \text{tr}(uy_s) = x_0 \mod (\mathfrak{M}_o^2 I, I \cap K_1).
\]

But this is impossible, because if \(u = f(y)\), then

\[
(g - 1)\xi(u) \equiv \text{tr} u \mod \mathfrak{M}_o = \text{tr} f(u) = f(\text{tr} u)
\]

and \(n \mid v((g - 1)\xi(u))\).

For each \(\sigma \in G\), consider the element

\[
\beta = \phi^{-1}((\sigma - 1)\xi) = (\sigma \otimes 1 - 1)(\alpha)
\]

(cf. [B1], formula (16)). We have the congruence

\[
(8) \quad \beta \equiv (\sigma - 1)a \otimes q \mod (\mathfrak{M}^{i+h_s+2n} + (\sigma - 1)(I \cap K_1)) \otimes \mathfrak{D}^{-1} I^{-1},
\]

where \(h_s\) is the ramification jump corresponding to the element \(\sigma\) in the field \(K\). Since \(h_s \geq h_{\text{min}}\), we have \((\sigma - 1)(I \cap K_1) \subset \mathfrak{M}^{i+h_s+2n}\). Thus, we see that the valuation of \(\psi_1(\beta)\) in \(K\) is equal to \(v(\sigma - 1)(a) + v(q) = v(a) + v(q) + h_s\). Since \(\phi(\beta) \in k[G]\), it follows that \(h_s \equiv -(v(a) + v(q)) \mod n\). Since this congruence is fulfilled for all ramification jumps of the group \(G\), the jumps are congruent modulo \(n\).

We denote the primitive root of unity of degree \(p\) by \(\zeta = \zeta_p\).

**Remark 2.3.2.** If \(\text{char } k = 0, \zeta_p \in k\), then the restriction imposed on \(h\) can be lifted; cf. an argument in Subsection 5.1.
§3. Formulation of the main theorem.
Properties of minimally unstable extensions

From now on, we assume that $K/k$ is Abelian.

We denote the ramification jumps of the extension $K/k$ by $h_s$, $1 \leq s \leq l$, $h_1 \leq h_2 \leq \cdots \leq h_l$, and the absolute ramification index of the field $k$ in the case where char $k = 0$ by $e$.

### 3.1. The main theorem in the general case.

Here and below, all statements and their proofs refer to both cases where char $k = 0$ and char $k = p$; in the latter case all restrictions where the absolute ramification index $e$ is involved should be removed from the statements.

Let $l \geq 2$.

**Theorem 3.1.** Suppose that $e > 2p$ and that for each $0 < s \leq l$ the conditions

\[
\begin{align*}
    h_s &\geq \frac{(2p+1)p^s}{p-1}, \\
    h_s &\leq \frac{ep^s - p^s(p+1)}{p-1}
\end{align*}
\]

are fulfilled. Suppose also that for each $l \geq s > 1$ there exist $i_s, \eta_s \equiv h \mod p$ such that

\[
-i_s \leq i_s, \eta_s, \eta + \eta < 2i_s + (i_s - h) \mod p^s + (h \mod p^s)(p-1),
\]

\[
\begin{align*}
    (1-1)^{\frac{(2+2(p+1)h}{ph}}{p^s-1/p^{s-2}}} &\equiv \left[\frac{(-\frac{i_s+(p-1)h}{ph}}{p^s - 1} \mod p^s-1/p^{s-2}\right] \\
\text{and} \\
    p^s &\nmid \left[\frac{(-\frac{i_s+(p-1)h}{ph}}{p^s - 1} \mod p^s-1/p^{s-2}\right] \mod p, \text{ for } s > 2.
\end{align*}
\]

Here $i_s = \left\lfloor \frac{i_s+d(K/k_s)}{p} \right\rfloor$, $k_s$ is an intermediate extension in $K/k$ such that $[K : k_s] = p^{l-s}$ and the ramification jumps equal to $h_{s+1}, h_{s+2}, \ldots, h_l$ correspond to the Galois group $K/k_s$. Suppose that the ideal $I = M^t$ is free over the associated order $A_{K/k}(I, I)$. Then the extension $K/k$ is semistable.

Since $K/k$ is Abelian, condition (10) implies that all ideals of $K$ are indecomposable. See Remark 1.8.2.

### 3.2. Extensions of degree $p$.

We establish the properties of cyclic extensions of degree $p$ that we need in the proof of Theorem 3.1.

**Lemma 3.2.** Suppose the degree of the extension $[K : k]$ is equal to $p$ and $h$ is the ramification jump for the group $G = \langle \sigma \rangle$. For char $k = 0$ we also assume that $K/k$ is not maximally ramified, i.e., $(h, p) = 1$, which is equivalent to the condition $h < \frac{p^2}{p-1}$. Then:

1. $K/k$ is semistable;
2. $(M^s)^p \mod M^{p^r + h(n-1)} \subset M^r \mod M^{p^r + h(n-1)}$;
3. for each $x \in K^*$ we have $v(x - \sigma^{p-1}(x)) \geq v(x) + pe$.

**Proof.** 1. For $x \in K^*$ we have $v((\sigma - 1)x) \geq v(x) + h$, and $v((\sigma - 1)(x)) = v(x) + h \iff (v(x), p) = 1$. Consider the element $\eta = (\sigma - 1)^{p-2}$. We have $(h, p) = 1$. It follows that $v(\eta(x)) \geq v(x) + h(p-2)$ for $x \in K^*$, and equality is attained if either $v(x) \equiv h \mod p,$
or \( v(x) \equiv 2h \mod p \). Thus, \( N(\xi) = \{(0, -h), (-h, 0)\} \), whence the extension \( K/k \) is semistable.

2. Let \( x \in \mathfrak{M}^n \), and let \( X^p + \sum_{1 \leq s \leq p} a_s X^{p-s} \) be the minimal polynomial for \( x \) in the extension \( K/k \). We have

\[
a_s = (-1)^s \sum_{0 \leq r_1 < r_2 < \cdots < r_s < p} \prod_j \sigma^{r_j} x.
\]

It is easily seen that, for \( s < p \), we can partition the set \( G_s = \{ (\sigma^{r_1}, \sigma^{r_2}, \ldots, \sigma^{r_s}) \mid 0 \leq r_1 < r_2 < \cdots < r_s < p \} \) into subsets \( G_s^r \) such that \( \sigma^{s_1}(G_s^r) = G_s^{r_1 + r_2} \); here the action of \( G \) on \( (\sigma^{r_1}, \sigma^{r_2}, \ldots, \sigma^{r_s}) \) is assumed to be coordinatewise. We obtain

\[
a_s = \text{tr} \left( \sum_{(\tau_1, \ldots, \tau_s) \in G_s^r} \tau_1(x) \cdots \tau_s(x) \right),
\]

whence \( v(a_s) \geq sr + h(n - 1) \). Thus, \( x^p \equiv a_p \mod \mathfrak{M}^{h(n-1)+pr} \).

3. An easy computation shows that \( \left( \frac{p-1}{j} \right) \equiv 1 \), \( 0 \leq j < p \), and we see that \( (\text{tr} - (\sigma - 1)^{p-1})(x) \in p\mathfrak{M}^{v(x)} \).

Since \( (a+b)p = ap + bp + p \sum_{0 < j < p} \left( \frac{r}{p} \right) a^j b^{p-j} \), we see also that for \( \text{char } k = 0 \) the set \( \mathfrak{D}_{K^p} \mod \mathfrak{M}^{pe} \) is a ring with a unit. If \( \text{char } k = p \), then \( K^p \) is a field.

### 3.3. Formulation of the main lemma

We prove Theorem 3.1 by induction on \( l \). The case where \( l = 1 \) was studied in Lemma 3.2. Hence, obviously, it suffices to prove the following lemma for \( l \geq 2 \).

**Lemma 3.3.** We fix a tower of subextensions \( k_s \) in \( K/k \), \( 0 \leq s \leq l \), \( k_0 = k, k_1 = K, [k_r : k_{r-1}] = p \), and denote by \( h_r \) the ramification jump for the group \( \text{Gal}(k_r/k_{r-1}) \). We write \( h \) for \( h_l \) and \( K_1 \) for \( k_{l-1} \).

Suppose that the extension \( K_1/k \) is semistable,

\[
e > 2p, \quad 2p + 1 \leq h_1, \quad \frac{(2p+1)n}{p-1} \leq h,
\]

and

\[
h \leq \frac{en - n(p+1)}{p-1}.
\]

Suppose there exist \( r, \eta \equiv h \mod p \) such that

\[
i \leq r_s, \eta_s, r_s + \eta_s < 2i + (i - h) \mod n + (-h \mod n)(p-1),
\]

\[
(15) \quad (-1)\frac{r+(p-1)h}{ph} \mod p^{l-1}/p^{l-2} = \left( \frac{r+(p-1)h}{ph} \mod p^{l-1}/p^{l-2} \right) \mod p.
\]

If \( l > 2 \), we also demand that

\[
p \upharpoonright \left( (-1)\frac{r+(p-1)h}{ph} \mod p^{l-2} \right),
\]

Then the extension \( K/k \) is also semistable.

If an extension \( K/k \) satisfies the bounds on the jumps in the lemma and is not semistable, while \( K_1/k \) is semistable, then we call \( K/k \) a minimally unstable extension. The above lemma implies Theorem 3.1. Indeed, if \( I \) is free over \( \mathfrak{A}_{K/k}(I, I) \) and the conditions of Theorem 3.1 are fulfilled, then the ideal \( I_F = \text{tr}_{K/F} I \) of the field \( F \).
is also free over its associated order and satisfies the assumptions of Theorem 3.1 (the congruencies for the jumps that we need to check follow from the Hasse–Arf theorem). Choosing various sequences of \( \{k_s\} \), we can relax slightly the bounds (13), (14) on the jumps for noncyclic extensions.

An informal comment on Lemma 3.3. The conditions of Lemma 3.3 are not very easy to check. Here we try to answer the question as to how often these conditions are fulfilled from the “probabilistic” point of view. Yet we do not claim that this answer is quite correct, since the conditions of the lemma are not independent.

Suppose that the restrictions (13) and (14) on the ramification jumps are fulfilled. For fixed numbers \( \varpi, \eta \) that satisfy the necessary inequalities, the probability that the second and the third conditions in (15) are fulfilled is some constant \( c(p) \) independent of \( l \). The known relationship between the digits in the \( p \)-adic expansion of \( \varpi, \eta \) and the power in which \( p \) is contained in the corresponding binomial coefficient implies that the probability for the last condition in (15) to be fulfilled is \( \left( \frac{p+1}{2p} \right)^{l-2} \). We have approximately \( \frac{(i-h) \mod n + (p-1)(-h) \mod n}{p^2} \) pairs \( \varpi, \eta \) that satisfy \( i \leq \varpi, \eta, \varpi + \eta < 2i + (i-h) \mod n + (-h \mod n)(p-1) \). Thus, for any \( i \), if the quantity

\[
((h) \mod n)^2 \left( \frac{p+1}{2p} \right)^l
\]

is sufficiently large, it seems “probable” that the desired pair \( \varpi, \eta \) exists.

It follows that if the number \( (h) \mod n \) does not contain “too many” successive zeros in its \( p \)-adic expansion and the restrictions (9) and (10) on the jumps for the extension \( K/k \) are fulfilled, then this extension satisfies the assumptions of Theorem 3.1.

The restrictions (9) and (10) on the ramification jumps can be relaxed somewhat. However, there seems to be no way to get rid of them completely. The author does not know whether there exists an extension that fulfils (11) and does not satisfy the claim of Theorem 3.1.

3.4. The element \( \xi \in k[G] \): construction and properties. Multiplication of \( I \) by an element of \( k \) does not affect the property to be free over \( \mathfrak{A}_{K/k}(I, I) \). Therefore, in what follows we assume that \( -d - n < i \leq -d \).

As in Subsection 2.3, we suppose that \( K_1 = K^{(\varpi)} \). Again, \( g^p = 1 \). We consider \( y \in K \) such that \( v(y) = -d \). Then \( y \in I \setminus I M_0 \). Proposition 1.8.1 implies that \( I = \mathfrak{A}_{K/k}(I, I) y \). We put \( m = i + (-h - i) \mod n \). Let \( t \in K \) be such that \( v(t) = (1-p)h \) and \( \text{tr}_{K/K_1} = 1 \), and let \( x = (g-1)^{p-2} l \pi_0^{\frac{h}{\alpha}} \). We see that there exists an element \( \xi \in \mathfrak{A}_{K/k}(I, I) \) for which \( \xi(y) = x \). Lemma 3.2 implies the congruence

\[
(g-1)(x) \equiv \frac{m+h}{n} \mod M^{h+m+(p+1)n}.
\]

The module \( \mathfrak{A}_{K/k}(I, I) \cap \text{Ker}(S_{K/k}) \) will be denoted by \( \mathfrak{J} \). If \( z \in \mathfrak{J}(y) \), \( z = f(y) \), then \( (g-1)\xi(z) = (g-1)\xi(f(y)) = \omega(f(1)^{p-1}(1)) \equiv \omega(f(1)) \equiv 0 \mod M^p M^{p+1} \), whence \( \xi(z) \mod I M_0^p \in K_1 \mod I M_0^p \). Thus, \( \xi(I) \mod I M_0^p \subset \sigma x \oplus I \cap K_1 \mod I M_0^p \). We denote \( \phi^{-1}(\xi) \) by \( \alpha \).

Lemma 3.4.1. The extension \( K/k_1 \) is semistable.

Proof. We denote the ring of integers in \( k_1 \) by \( \mathfrak{o}_1 \), its maximal ideal by \( M_1 \), and the Galois group of \( K_1/k \) by \( J \).

We expand \( \alpha \) in a sum of the form (7):

\[
\sum x_s \otimes y_s, \quad x_s \in I, \quad y_s \in D^{-1}I^{-1}.
\]
Since \( x_s \in \xi(I) \), for some \( r \in \mathcal{O}^{-1}I^{-1} \) we have the congruence

\[
\alpha \equiv x \otimes r \mod (\mathcal{IM}_k, I \cap K_1) \otimes \mathcal{O}^{-1}I^{-1}.
\]

Also, we can choose \( r \) so that \( v(r) = 0 \). Indeed, for any \( w \in \mathbb{Z} \) with \( v(y) \neq w \) mod \( n \) we can choose \( z \in K, v(z) = w \), such that \( \text{trz} = 0 \) and so \( z \in \mathfrak{J}(y) \). Let \( \varepsilon \) denote the prime element of \( K_1 \). We represent \( \alpha \) in the form

\[
\sum_{s=0}^{+\infty} a_{sj} e^s \otimes \pi^j + x \otimes r + w, \quad w \in \mathcal{IM}_k \otimes \mathcal{O}^{-1}I^{-1},
\]

\( a_{sj} \in \alpha \), and we consider the element \( \xi^p = \phi(\alpha^p) \in \mathfrak{A}_{pm-2pmd} \). We have

\[
\alpha^p \equiv \sum a_{sj} e^{ps} \otimes \pi^{pj} + x^p \otimes r^p \mod (p^p \otimes (\mathcal{O}^{-1}I^{-1})^p \subset X_{pm+n}).
\]

Formula (2) implies that \( \xi^p(y) \in (\mathcal{M}^m)^p\mathcal{M}_k^p \) (the \( p \)th power is taken elementwise). By Lemma 3.2, \( \xi^p(y) \mod \mathcal{M}^{mp+n} \in K_1 \mod \mathcal{M}^{mp+n} \). Similarly, \( \xi^p(y) \) can be written as \( \varkappa + \lambda \), \( v(\lambda) = pm \), \( \varkappa \in (\mathcal{M}^{m-2n} \cap K_1)^p \). Since \( K_1/k \) is semistable and \( v(tr y) \equiv pm \) mod \( n \), we can choose \( \eta \in k[J] \) such that \( \eta(\text{tr} \mathcal{K}/K_1) \equiv \xi^p(y) \mod \mathcal{M}^{mp+n} \). Since \( I = \mathfrak{A}_{K/k}(I, I)y \), the conditions \( f \in k[G] \) and \( v(f(y)) = s \) imply \( f \in \mathfrak{A}_{s+d-n+1} \). Thus, \( \eta(\text{tr} \mathcal{K}/K_1) - \xi^p \in \mathfrak{A}_{pm+d+1} \). Let \( \alpha_1 \) be an element of \( K_1 \otimes K_1 \) such that \( \xi_1 = \phi(\alpha_1) \) in \( k[G] \) satisfies the assumptions of Definition 1.7.1 for the extension \( K_1/k \). For any \( v \in K \) and \( \rho \in K_1 \otimes K_1 \), we have \( \phi(\rho)(v) = \phi(\alpha)(\text{tr} \mathcal{K}/K)(v) \). Thus, \( \xi_1 \text{tr} \mathcal{K}/K_1 = \phi(\alpha_1) \).

For \( 0 \leq s < p^{j-2} \), Proposition 1.7.2 implies \( v(\xi^p(\text{tr} y)) \equiv -phs \mod p^{l-1} \). Obviously, the dimension of \( \alpha_1^p \mod (p) \) over \( \alpha_1^p \mod (p) \) is equal to \( p^{l-2} \). Hence, there exist \( a_s \in k_1, 0 \leq s < p^{j-2} \), such that

\[
\varkappa \equiv \left( \sum a_s \xi_1^s \right)^p \text{tr} \mathcal{K}/K_1(y) \mod \mathcal{M}^{mp+n}, \quad (a_s \xi_1^s)^p \text{tr} \mathcal{K}/K_1(y) \in \mathcal{M}^{mp-2pn}.
\]

We obtain

\[
d \left( \left( \xi - \sum a_s \xi_1^s \text{tr} \mathcal{K}/K_1 \right)^p \right) = d \left( \left( \eta - \sum a_s \xi_1^p \right) \text{tr} \mathcal{K}/K_1 \right) = pm.
\]

By Lemma 2.2, we have \( \left( \sum a_s \alpha_1^s \right)^p \equiv \sum b_s \alpha_1^p \mod \mathfrak{A}_{mp+d+1} \), where the \( b_s \in k \) satisfy \( b_s \equiv a_s^p \mod \mathfrak{A}_{1}^{(p-1)h_1+pmk} \). Moreover, the semistability of the extension \( K_1/k \), applied to \( \sum b_s \alpha_1^p \), shows that

\[
N(\left( \xi - \sum a_s \xi_1^s \right)^p) = \{(pm - \frac{sn}{p}, \frac{sn}{p}); (\frac{sn}{p}, pm - \frac{sn}{p}) \mid 0 \leq s < p\}.
\]

Now we compute the lower diagonal of the diagram for the element \( \xi' = \theta \ast \text{tr} \mathcal{K}/k_1 \) in the extension \( K_1/k_1 \), where

\[
\theta = \xi - \sum (a_s \otimes 1) \alpha_1^s.
\]

We prove that \( \mu \) can be written as \( (\pi_1 \otimes \pi_1^{-1} - 1) \chi + \nu, \chi \in X_m, \chi \in X_{m-2n+1}, \nu \equiv x \otimes r - r \otimes x \mod X_{m+1} \). Indeed, if \( \chi \in X_{m-2n+1} \), then \( (\pi_1 \otimes \pi_1^{-1} - 1)^p \chi^p \in X_{p(m-2n+1)+(p-1)h_1} \) because \( (\pi_1 \otimes \pi_1^{-1} - 1)^p \in X_{p^2(p-1)} \). We construct the reduction of \( \mu \) modulo \( \pi_1 \otimes \pi_1^{-1} \). Let \( \mu \) be congruent to \( \sum_{0 \leq s < \frac{p}{n}} a_s \pi^s \otimes \pi^j \mod X_{mp+1} \). Since \( n < p|s_1 - s_2| \), no cancelation may occur, so that we can take \( \nu \) equal to \( \sum_{0 \leq s < \frac{p}{n}} a_s \pi^s \otimes \pi^j \). Thus, \( p(\nu^p) = c(X^{-hp} - 1) \), \( c \in \mathbb{K}^+ \).

We have

\[
p(\pi_1 \otimes \pi_1^{-1} - 1)p(\text{tr} \mathcal{K}/k_1) = 0.
\]
Then
\[ N(\xi') = N(\phi(\nu) * \text{tr}_{K/k_1}) \]
\[ = \left\{ \left( m + \frac{n}{p}(-j - d(k_1/k)), n - \frac{n + nj}{p} \right) \mid 0 \leq j < p \right\} \]
\[ \cup \left\{ \left( n - \frac{n + nj}{p}, m + \frac{n}{p}(-j - d(k_1/k)) \right) \mid 0 \leq j < p \right\}. \]

Now as in Proposition 2.2.1, Proposition 1.4.2 implies that
\[ N_{K/k_1}(\xi') = \{(m, 0), (0, m)\}. \]

Since \((m, p) = 1\), Proposition 1.7.2 shows that \(K/k_1\) is semistable. \(\square\)

Let \(M\) denote the module \(\text{Ker tr}_{K/k} : I \to k\).

**Lemma 3.4.2.** For any \(u \in \text{Ker tr}_{K/k_1} : I \to k_1\) we have
\[ v(\xi)(u) \geq v(u) + m + d. \]

**Proof.** We denote by \(H\) the Galois group \(\text{Gal}(K/k_1) \subset G\) of the extension \(K/k_1\).

Since the extension \(K_1/k\) is semistable, for \(f \in k_1[H]\) and \(\varepsilon \in K^*\) we have
\[ v(f(\varepsilon)) - v(\varepsilon) \geq v(f(y)) - v(y). \]

For \(u = w(y), w \in (k[H] \cap \mathfrak{A}_{K/k}(I, I))\), we have \(\xi(u) = \xi(w(y)) = w(\xi(y))\), whence
\[ v(\xi(u)) \geq v(w(y)) - v(y) + v(\xi(y)) = v(y) + m + d. \]

Now, consider the map \(\xi_M : M \to K\) mod \(IM^p_o\) induced by \(\xi\). The image of \(\xi_M\) lies in \(K_1\) mod \(IM^p_0\). Moreover, it has already been proved that for \(\text{tr}_{K/K_1}(w) = 0\) we have \(\xi(w)\) mod \(IM^p_0 \in k\) mod \(IM^p_0\).

The desired statement will be deduced from the properties that were proved for the two types of \(\mu\) considered above. \(\xi_M\) induces a map \(\nu : \Lambda \to K_1/k\) mod \(IM^p_0\), where
\[ \Lambda = \text{tr}_{K/K_1}(I) \text{ mod } \text{tr}_{K/K_1}(I)IM^p_0 \approx I / \text{Ker tr}_{K/K_1}(I \to K_1) \text{ mod } IM^p_0. \]

Let \(v'\) be the valuation induced by \(v_{K_1}\) on \(K_1\) factorized by \(k\). Obviously, it suffices to show that
\[ v_{K_1}(\nu(u)) \geq v'(u) + \frac{m + d + (1 - p)h}{p} \]
for any \(u \in \text{Ker tr}_{K/k_1}(\Lambda)\). For \(u \in \text{tr}_{K/K_1}(k[H] \cap \mathfrak{A}_{K/k}(I, I))\) this is true. Part 4 of Proposition 1.7.2 shows that we can choose
\[ w_s \in \text{tr}_{K/K_1}(k[H] \cap \mathfrak{A}_{K/k}(I, I)) \]
such that \(v'(w_s) \equiv sh \text{ mod } p^{l-1}, 0 \leq s < p^{l-2}\). We know that the ideal \(I_1 = \text{tr}_{K/K_1} I\) is free over its associated order. For each \(0 < j < p\), we consider an element \(\lambda_j \xi_{1}^{p^{l-2}j-1}\), choosing \(\lambda_j \in k\) so that
\[ \lambda_j \xi_{1}^{p^{l-2}j-1} \in \mathfrak{A}_{K_1/k}(I_1, I_1) \setminus \mathfrak{M}_o \mathfrak{A}_{K_1/k}(I_1, I_1). \]

Since \(I\) is free over \(\mathfrak{A}_{K/k}(I, I)\), there exists \(\eta_j \in \mathfrak{A}_{K/k}(I, I)\) such that the restriction of \(\eta_j\) to \(K_1\) is equal to \(\lambda_j \xi_{1}^{p^{l-2}j-1}\). The lower diagonal of \(\xi_{1}^{p^{l-2}j-1}\) in the field \(K_1\) is congruent to \(\{-hr, -hjp^{l-2} + hr + h\}, 0 \leq r < p^{l-2}j\} \text{ modulo } p^{l-1}X_{K_1/k}\). Using the fact that \(\eta_j\) commutes with \(\xi\), we obtain
\[ v_{K_1}(\nu(\lambda_j \xi_{1}^{p^{l-2}j-1}(w_s))) = v_{K_1}(\lambda_j \xi_{1}^{p^{l-2}j-1}(w_s))) \]
\[ \geq v_{K_1}(\lambda_j \xi_{1}^{p^{l-2}j-1}(w_s)) + \frac{m + d + (1 - p)h}{p}. \]
Consequently, inequality (24) is fulfilled also for $\xi_{i_1}^{p^{j-2}j-1}(w_a)$. Since

$$\dim_k \text{Ker tr}_{K_1/k_1}(\Lambda) = \frac{n}{p} - 1$$

and inequality (24) is true for $\frac{n}{p} - 1$ elements of $\text{Ker tr}_{K_1/k_1}(\Lambda)$ with valuations pairwise distinct modulo $\frac{n}{p}$, it is true for all $u \in \text{Ker tr}_{K_1/k_1}(\Lambda)$. Thus, inequality (22) is proved.

\[\square\]

Lemma 3.4.3. If the extension $K/k$ is unstable, then $\alpha$ can be represented in the form

$$x \otimes r + c \sum_{0 < u < p} u(\pi_1 \otimes \pi_1^{-1})^u \pi_0 \frac{[m]}{n} + v + w,$$

where $c \in \mathfrak{o}^*$, $v(r) = 0$, $v \in X_n[\frac{m}{n}] + 1 \cap K_1 \otimes K$, and $w \in X_{m+n^2}$.

Proof. We have (17). It remains to prove that $d(\xi) = n[\frac{m}{n}]$ and $p(\xi) = c \sum_{0 < u < p} \frac{1}{u} x^u$.

Suppose that $d(\xi) = m$. Using an easy computation in the algebra $\mathfrak{J}$ and formula (17), we see that $p(\xi) \notin (X - 1)^2$. Proposition 1.6.3 shows that the $d(\xi_j)$, $0 \leq j < n$, are all different modulo $n$. Then for any element $f \in k[G]$, $p(f)$ is determined by $d(f)$ up to multiplication by a constant. We consider $i(\xi) \in k[G]$ (see Proposition 1.1.3). Obviously, $d(i(\xi)) = d(\xi)$. It follows that the only point in $N(i(\xi))$ whose second coordinate does not contain $p$ is $(0, m)$. Thus, $K/k$ is semistable.

Now suppose that $d(\xi) < m$. For any $s \in \mathbb{Z}$ with $s \neq -d \mod \frac{n}{p}$, we can find $z \in K$ such that $\text{tr} K/k_1 z = 0$ and $v(z) = s$. Thus, the preceding lemma implies that the lower diagonal of $\xi$ contains points whose second coordinates contain $p^{j-1}$ and do not contain $n$.

Since $K_1/k$ is semistable, it is easily seen that for each $s \neq h \mod p^{j-2}$ there exists $\eta \in k[G/\langle g \rangle]$ such that $d_{K_1/k}(\eta) = s$ and $\text{tr}_{K_1/k_1}(\eta) = 0$. Suppose that the lower diagonal of $\xi$ contains the point $(a, r)$. For any $b \in \mathbb{Z}$ with $b \neq -1 \mod p^{j-2}$ we choose an element $\lambda \in k[G]$ that lifts an element $\lambda' \in k[G/\langle g \rangle]$ so that $d_{K_1/k}(\lambda') = -bh - h - \frac{a}{p} - d(K_1/k)$. Since $\lambda$ commutes with $\iota$ (see the proof of Lemma 3.4.2), Proposition 1.7.2 implies that either

$$p \mid \left( p^{j-1} - 1 - (\frac{a}{ph} \mod p^{j-1}) \right),$$

or the lower diagonal of $\xi$ contains $(-phb + r + a - ph, phb + ph)$. Combining these statements for all $b$, we obtain $p^{j-1} \mid a$.

Suppose that $d(\xi) = -jhp^{j-1}$, $0 \leq j < p$, and consider the element $\eta_1$ that lifts $\lambda_1 \xi_1^{p^{j-2}j-1}$, where $\xi_1$ is the element defined in the proof of Lemma 3.4.1. Arguing as above, we obtain

$$p(\xi) = c' \sum_{0 \leq r < p-j} (r + 1) \cdots (r + j - 1) X^{-hp^{j-1}r}, \quad c' \in \overline{\mathbb{F}}^*.$$

Now we show that $n \mid d(\xi)$. Indeed, otherwise we have

$$\psi_1(\xi) \equiv -(p-1)(p-2) \cdots (p-j+1)c' \pi^{d(\xi)} \mod \mathfrak{M}^{d(\xi)+1},$$

which is impossible because $\psi_1(\xi) \in k$.

The fact that $\xi \in \mathfrak{M}_{K/k}(I, I)$ implies immediately that $d(\xi) > m - n$; thus, indeed,

$$d(\xi) = n \left[ \frac{m}{n} \right], \quad p(\xi) = c' \sum_{0 < r < p} \frac{1}{r} X^{p^{j-1}r}, \quad c' \in \overline{\mathbb{F}}^*. \quad \square$$

Proof of the main theorem

4.1. Technical computations. For the proof of Lemma 3.3, we want to estimate the lower diagonals of certain elements. We shall need several technical statements.

We introduce the algebra $\mathcal{Z} = F_p[Z]/(Z^p - 1) = F_p[Z - 1]/(Z - 1)^p$, where $F_p$ is the field of $p$ elements; we also introduce the polynomial ring $\mathcal{Z}[Y]$. Consider the element

$$\mathfrak{F}(Z) = \sum_{0 < w < p} \frac{Z^w}{w}.$$ 

Lemma 4.1.1. For $0 < s < p$ we have

$$(26) \quad \mathfrak{F}(Z)^s = s! \sum_{0 < w < p} w^{p-s-1} Z^w$$

if $0^0$ is assumed to be equal to 1.

Proof. We have $\mathfrak{F}(Z) = \sum_{0 < w < p} w^{p-2} Z^w$. Hence (26) is true for $s = 1$. We prove (26) by induction. Assume that (26) is fulfilled for $s = u < p - 1$. It suffices to prove the formula

$$\sum_{q+r=w} q^{p-u-1} r^{p-2} = (u + 1) w^{p-u-2}.$$ 

We make the following calculations (in the field $F_p$):

$$\sum_{q+r=w} q^{p-u-1} r^{p-2} = w^{2p-u-3} \sum_{q+r=1} q^{p-u-1} r^{p-2} = w^{p-2-u} \sum_{q \in F_p} q^{p-u-1}(1 - q)^{p-2}$$

$$= w^{p-2-u} \sum_{r=p-u-1} (-1)^{r-p+u+1} \sum_{q \in F_p} \left( \frac{p - 2}{r - p + u + 1} \right) q^r.$$ 

Since $\sum_{w \in F_p} w^j = 0$ if $p - 1 \nmid j$ and $\sum_{w \in F_p} w^j = \sum_{w \in F_p^*} 1 = -1$, we have

$$\sum_{r=p-u-1} (-1)^{r-p+u+1} \sum_{q \in F_p} \left( \frac{p - 2}{r - p + u + 1} \right) q^r = (-1)^u \left( \frac{p - 2}{u} \right) = u + 1,$$

which proves (26). \qed

Lemma 4.1.2. 1) For any $0 \leq w < p$ and $0 < j < p - 1$, denote

$$F(Y, Z) = -(1 - Z)^w \sum_{\max(0, j-w) \leq s \leq j} (p-1)(p-2)\cdots(s+1)a_{j-s}(\mathfrak{F}(Z) + Y)^s,$$

where the $a_s$ are the coefficients in the expansion

$$\prod_{0 < u \leq w} (X + u) = \sum_{0 \leq s \leq w} a_s X^s,$$

$a_s = 0$ for $s > w$. Then in the expansion $F(Y, Z) = \sum_{0 \leq u < n} Z^u f_u(Y)$ we have $f_0(Y) = w! Y^j$.

For $w < j$, in the expansion $F(Y, Z) = \sum_{0 \leq u} g_u(Z) Y^u$ we have $g_0(Z) \neq 0$.

2) For $j = p - 1$, we have $f_0(Y) = -w! Y^{p-1} + w!$ and $g_0(Z) = w! \sum_{0 \leq u < p} Z^u$.

3) For $j = p - 2$, $w < p - 1$, we have $g_0(Z) = (w + 1)! \sum_{0 \leq u < p} uZ^u$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proof. Lemma 4.1.1 implies that

\[(Y + \mathfrak{F}(Z))^s = \sum_{0 \leq u \leq s} \left( \binom{s}{u} w^{s-u} \sum_{0 \leq v < p} v^{p-u-1} Z^v \right)\]

Thus,

\[- (p-1)(p-2) \cdots (s+1)(\mathfrak{F}(Z) + Y)^s\]

\[= -(p-1)! \sum_{0 \leq u \leq s} \frac{Y^{s-u}}{(s-u)!} \sum_{0 \leq v < p} v^{p-u-1} Z^v = \sum_{0 \leq u \leq s} \frac{Y^{s-u}}{(s-u)!} \sum_{0 \leq v < p} v^{p-u-1} Z^v.\]

The constant term in \((1 - Z)^w \mathfrak{F}(Z)^s\) is equal to \(s! \sum_{0 \leq u \leq w} (-1)^u \binom{w}{u} (-u)^{p-s-1}\).

It is easy to check that

\[\sum_{0 \leq u \leq w} (-1)^u \binom{w}{u} \frac{1}{-x - u} = \frac{w!}{Y(1 - Y) \cdots (Y + w)}.\]

Then in the formal power series ring \(F_p[[Y]]\) we have the identity

\[w! = (Y + 1) \cdots (Y + w) \left(1 + \sum_{v > 0} Y^v \sum_{0 < u \leq w} (-1)^u \binom{w}{u} (-u)^{-v}\right).\]

This yields the desired formula for \(f_0(Y)\).

Since, obviously, \((Z - 1)^{j+1} \mid g_0(Z)\), for \(j < n - 1\) we have \(g_0(Z) \neq 0\).

2) If \(j = n - 1\), then

\[g_0(Z) = (1 - Z)^w \left(\sum_{0 \leq u < p} Z^u (u+1) \cdots (u+w)\right),\]

whence \(g_0(Z) = w! \sum_{0 \leq u < p} Z^u\), because the \(w\)th difference of a unitary polynomial of degree \(w\) is equal to \(w!\).

3) As above, we have

\[g_0(Z) = (1 - Z)^w \sum_{0 \leq u < p} Z^u u (u+1) \cdots (u+w).\]

Computing the differences, we arrive at the desired results. \(\square\)

4.2. Diagram computations. Now we estimate the lower diagonals for some elements of \(\mathfrak{A}_{K/k}(I, I)\).

We expand the elements of \(I\) in the \(K_1\)-basis formed by the \(x^i\) with \(0 \leq i < p\).

Lemma 4.2. For any \(j\) with \(i \leq j < i + n\), there exist \(\lambda_j \in k[G]\) such that \(v(\lambda_j(y)) = j\) and

\[(27) \quad v(\lambda_j(y)) \mod \mathfrak{M}_a I \in I \cap (K_1 \oplus xK_1 \oplus \cdots \oplus x^{-\frac{i}{p}} \mod pK_1) \mod \mathfrak{M}_a I.\]

The element \(\lambda_j\) can be chosen so as to satisfy the following conditions:

1) \(d(\lambda_j) \geq j - (-\frac{i}{p} \mod p)(-h \mod n)\).
2) If \( \left[ \frac{j}{p} \mod \frac{n}{p^{\nu}} \right] < p - 1 \) and \( j \equiv h \mod p \), then

\[
N(\lambda_j) = \left\{ (j + (1 - p)(-h \mod n) + pah, -pah) : 0 \leq a < p^{l-2}, p \nmid \left( \frac{(-j + (p-1)h)}{ah} \mod p^{l-2} \right) \right\}
\]

(28)

\[
+ \left\{ (bhp^{l-1}, -bhp^{l-1}) : \left( \frac{(-j + h)}{b^{p^{l-1}}} \mod n \right) \neq (-1)^l \cdot \frac{(-j + h)}{b^{p^{l-1}}} \mod p \right\}.
\]

Proof. 1) Suppose that \( \left[ \frac{j}{p} \mod \frac{n}{p^{\nu}} \right] < p - 1 \). We prove our statement by induction on \( -\frac{j}{h} \mod p \). We denote \( \xi_1 \circ \text{tr}_{K/K_1} \) by \( \rho \). Since the element \( \xi_1 \) satisfies the conditions of Definition 1.7.1 for \( K_1/k \), we have

\[ N(\rho) = \{(d(\rho, c); (c, d(\rho)))\}. \]

For \( p \mid j \), consider the element \( \rho^{-\frac{j}{p}} \mod p^{l-1} \). We have

\[ \rho^{(-\frac{j}{p}) \mod p^{l-1}}(y) \in K_1, \quad v(\rho^{-\frac{j}{p}} \mod p^{l-1}(y)) \equiv j \mod n. \]

Hence, if we take

\[ \varkappa_j = \pi_0^{-\frac{j-d(\rho, \frac{j}{p}) \mod p^{l-1}}{n}}, \]

then \( \lambda_j = \varkappa_j \rho^{(-\frac{j}{p}) \mod p^{l-1}} \) satisfies the desired conditions.

Suppose that the claim is true for \(-\frac{j}{h} \mod p < s < p - 1\). We prove it for \(-\frac{j}{h} \mod p = s\) by (inverse) induction on \( j \). Let the claim be true for \( j > j_0 \). Put \( r_0 = \left[ \frac{s}{p^{\nu}} \right] \). For simplicity of computations, we assume that \( p(\rho^{p^{\nu-2}}) = 1 - X^{p^{l-1}} \) (this can always be achieved by considering another prime element or by lifting \( K/k \) by a fiercely ramified extension). Let

\[
n'_{j_0} = \varkappa_{j_0} \rho^{\left[ -\frac{j_0}{h} \mod p^{l-1} \right] \rho^{p^{l-2}}} \sum_{\max(0, s-r_0) \leq u \leq s} (p-1)(p-2) \cdots (u+1)a_{s-u}(-c'^{-1}n \xi \pi_0^{-\left[ \frac{s}{p^{l-1}} \right]})^u,
\]

(29)

where the \( a_s \) are as in Lemma 4.1.2, \( c' \) is taken from Lemma 3.4.3, and

\[ \varkappa_{j_0} = \pi_0^{-\frac{j_0-s(-h \mod n) - d(\rho, \frac{j_0}{p}) \mod p^{l-1}}{n}} \]

(again we may need to modify the valuation by a number containing \( n \)). Since

\[
\xi^s \mod \mathfrak{M}_o(I \otimes \mathcal{D}^{-1}I^{-1})^s \in I^s \cap (K_1 \otimes K_1 \otimes \cdots \otimes x^sK_1) \otimes (\mathcal{D}^{-1}I^{-1})^s \mod \mathfrak{M}_o(I \otimes \mathcal{D}^{-1}I^{-1})^s,
\]

(30)
\[\nu_{j_0}(y) \text{ belongs to } K_1 \otimes xK_1 \otimes \cdots \otimes x^s K \text{ mod } M_0 I. \] By Lemma 4.1.2 (with \(Z = (\pi_1 \otimes \pi_1^{-1})^{-h}\) and \(Y = -\frac{b}{c} x \otimes r \pi_0^{-[\pi]}\)), we have
\[\nu_{j_0}(y) \equiv x^s w \mod (M_0 I, M_{K_1}((j_0 - (p-1)sv(x))/p) + 1 x^s, \]
\[\mathcal{M}_{K_1}((j_0 - (p-1)sv(x) - (h \mod n))/p) + 1 x^{s-1}, \ldots, \]
\[\mathcal{M}_{K_1}((j_0 - (p-1)sv(x) - (h \mod n)/s)/p) + 1 x^{s-1}, \ldots, \]
\[w \in K_1, v_{K_1}(w) = \frac{j_0 - sv(x)}{p}, \]
and
\[d(\nu_{j_0}) \geq j_0 - \left(-\frac{j_0}{h} \mod p\right) (-h \mod n).\]

By the inductive hypothesis, \(v_{j_0}(y) \mod \mathcal{M}_{j_0}^o\) can be represented as a linear combination of \(\lambda_j(y) \mod \mathcal{M}_{j_0}, d(\lambda_j) > j_0 - \left(-\frac{j_0}{h} \mod p\right) (-h \mod n)\). Hence, the desired \(\lambda_j\) exists.

For \(s = p-1\) and \(r_0 = p-1\), we can replace the sum in (29) by \((\xi \pi_0^{-[\pi]})_p^{-1}\), obtaining the same result.

2. For \(s = p-1\) and \(r_0 = p-1\), we modify the definition of \(v_{j_0} \) in (29) by adding the element \(r_0! \lambda_{j_0}(\frac{-j_0 + (p-1)h}{p}) \mod p^{-1} \), where \(\lambda_{j_0}\) is calculated in the same way as above. We obtain
\[N(\lambda_{j_0}) = N(\lambda_{j_0}(\frac{-j_0 + (p-1)h}{p}) \mod p^{-1}) + \sum_{0 \leq u < p} (\pi_1 \otimes \pi_1^{-1})^h - (1 - (\pi_1 \otimes \pi_1^{-1})^h)^r + \{(d(\rho p^{-2}), 0)\} \]
(cf. Proposition 1.5.3). This proves formula (28).

4.3. Proof of the main theorem. We prove Lemma 3.3. Consider \(x \) and \(y\) that satisfy conditions (15). The above lemma implies the existence of \(\lambda_x \in k[G]\) such that \(d(\lambda_x) = x\) and
\[d(\lambda_x)(\pi^n) = x + y + (1 - p)(-h \mod n) < i.\]
But this is impossible because \(I = \mathfrak{A}_{K/k}(I, I) y\), and hence, \(f \in k[G], f(y) \in I \implies f \in \mathfrak{A}_{K/k}(I, I)\).

Lemma 3.3, and, with it, Theorem 3.1, is proved.

§5. Some remarks

5.1. The main theorem for the case where \(\zeta_p \in k\). If char \(k = 0\), \(\zeta_p \in k\), then condition (10) turns out to be unnecessary.

Theorem 5.1. Suppose \(\zeta_p \) belongs to \(k\) and conditions (9) and (11) are fulfilled. If the ideal \(I = \mathcal{M}^i\) is free over \(\mathfrak{A}_{K/k}(I, I)\), then the extension \(K/k\) is semistable.

Proof. The proof is almost the same as that of Theorem 3.1. We only point out the difference.

It suffices to prove a lemma similar to Lemma 3.3. We will take \(x\) equal to
\[\pi_0 \sum_{1 \leq u < p} (g - \zeta^u)(t) (in \ place \ of \ \pi_0 \sum_{1 \leq u < p} (\sigma - 1) p^{-2}(t)). \]
We obtain
\[\pi_0 \sum_{1 \leq u < p} (g - \zeta)(x) = \pi_0 \sum_{1 \leq u < p} (g - \zeta)(x).\]

Then, instead of the congruence in formula (17), we obtain a similar congruence modulo \(I \cap K_1 \otimes \mathcal{O}^{-1} I^{-1}\). After that, we argue as in the proof of Lemma 3.3. The analogs of the congruences in Subsection 4.2 that we obtain in this case are even a little stronger. \(\Box\)
5.2. Other versions of the main theorem. Using part 3 of Lemma 4.1.2, we can prove a lemma similar to Lemma 3.3. An application of that lemma leads to a theorem that differs slightly from Theorem 3.1. Also, we can make some induction steps with the use of Lemma 3.3 and some with the help of the alternative lemma.

**Proposition 5.2.1.** Under conditions (13) and (14) of Lemma 3.3, suppose that $K_1/k$ is semistable and there exist elements $z, h, -h < i$ such that

$$i < r, q, x < 2i + (i - h) \mod n, \quad (h \mod n)(p - 2),$$

$$\left[\frac{(z + (p - 2)h) + ph}{ph}\right] \mod p^{l-1}/p^{l-2} < p - 1,$$

(33)

and

$$p \nmid \left(\frac{(q + (p - 1)h) + ph}{ph}\mod p^{l-2} \right) \left(1 + \frac{(q + (p - 1)h) + ph}{ph}\mod p^{l-2}\right).$$

If in $K/k$ the ideal $I = M_i$ is free over its associated order, then $K/k$ is semistable.

**Proof.** Using part 3 of Lemma 4.1.2, we can prove a suitable analog of part 2 of Lemma 4.2, and the proof follows easily. \(\square\)

Now we formulate a statement about free ideals in lifts of widely ramified extensions by tamely ramified ones.

**Proposition 5.2.2.** Let $E/k$ be an extension with ramification index $e'$, $(e', p) = 1$. Let $K_1/k$ be semistable and assume that the extension $K/k$ satisfies conditions (13) and (14) of Lemma 3.3. If the extension $L = EK/E$ contains ideals that are free over their associated orders, and for the greatest ramification jump $h$ of the extension $K/k$ we have $e'(-h \mod n) > n$, then $K/k$ is semistable.

**Proof.** Suppose that $K/k$ is unstable and that in $L/E$ the ideal $I' = M^{e'}_L$, $-d - n < i \leq -d$, is free over $A_{L/E}(I', I')$. By Proposition 1.1, $I = M_i$ is free over $A_{K/k}(I, I)$. For the extension $K/k$, we consider the element $\xi$ that was constructed in §3. Let $x \in K$ be such that $v(y) = -d$. We have $d_K(\xi) = n[M/K]$ and $\xi(y) \in I$. Then for the element $\xi$, we have $\xi \in I$ and $\xi \notin A_L(I', I')$. Since $v_L(y) \equiv -d_{L/E} \mod n$, $I'$ is not free over $A_{L/E}(I', I')$. \(\square\)

Another statement of this sort can be found in [B2], part 6 of Theorem 4.4.

5.3. Example of an unstable extension containing an ideal that is free over its associated order. As in Subsection 4.7 of [B2], we consider the Lubin–Tate formal group of the unramified extension $F$ of the field $\mathbb{Q}_p$ of degree $r > 1$ such that $[p]_F = x^q + px$, $q = p^r$. We have the congruence

$$F(X, Y) \equiv X + Y + \frac{(X + Y)^q - X^q - Y^q}{p} \equiv X + Y + \frac{1}{p} \sum_{i=1}^{q-1} \binom{q}{i} X^i Y^{q-i} \mod q + 1.$$

For $i = jq^{r-1}$, $0 < j < p$, we have

$$\binom{q}{i} \equiv 1, \quad \frac{(jq^{r-1})}{p} \equiv (-1)^{j-1}j^{-1} \mod p.$$
Our example is Kummer for the formal group $F$. We take a field $k$ that contains $\text{Ker}[p^2]_F$ and satisfies the condition $c \geq 2(q^2 - q)$. Choosing $a \in K$ with $v(a) = 1 + q^2$, we consider the field $N = k(y)$, where $y$ is the root of the equation $[p]_F(Y) = a$. As in §3 of [B2], we see that $[N : k] = q$ and $N/k$ is an Abelian extension. We denote $J = \text{Gal}(N/k) \approx \text{Ker}[p]_F$. The ramification jumps of $N/k$ are equal to $\frac{ea}{q-1} - q^2 - 1$.

Obviously, $(-1)^p a \pi_0^{-q}$ is equal to the norm of $y \pi_0^{-1}$, and $v_0(a \pi_0^{-q}) = 1$. We consider $K = k(x)$, where $x$ is the root of the equation

$$[p^2]_F(X) = c, \quad c = a + [p]_F(a \pi_0^{-q}).$$

Since $[p]_F(x - a \pi_0^{-q}) = a$, it follows that $K$ contains $N$. The conjugates of $x$ in $K$ are of the form $x + t$ with $t \in T$, where $T$ is a subgroup of $\text{Ker}[p^2]_F$. Consequently, $K/k$ is an Abelian extension. Lemma 3.2 yields the congruence

$$[p]_F(y \pi_0^{-1}) \equiv a \pi_0^{-q} \mod \Omega^{(p-1)} \frac{ea}{q-1} - q^2 - 1.$$

We see that $K = N(z)$, where $[p]_F(z) = y + \pi_0^{-q} a - [p]_F(y \pi_0^{-1})$ and $v_N([p]_F(z)) = v_N(y) = q^2 + 1$. Thus, $[K : N] = q$, and it follows that $[K : k] = q^2$ and $T = \text{Ker}[p^2]_F$.

The ramification jumps of $K/k$ that correspond to $\text{Ker}[p]_F \setminus \{0\}$ are equal to $\frac{eq^2}{q-1} - q^2 - 1$, and the ramification jumps that correspond to $\text{Ker}[p^2]_F \setminus \text{Ker}[p]_F$ are equal to $\frac{eq^2}{q-1} - q^2 - 1$.

Thus, we see that $n \mid d - 1$.

Consider the element

$$\alpha = x \otimes 1 - 1 \otimes x - \pi_0^{-q}([p]_F(x) \otimes 1 - 1 \otimes [p]_F(x)).$$

We show that $\xi = \pi_0^{-1} \phi(\alpha) \in k[G]$. Indeed,

$$\psi_\sigma(\alpha) = x - \sigma(x) - \pi_0^{-q} [p]_F(x - \sigma(x)) \in k.$$

Now we estimate $\alpha$. For $p > 2$ we have

$$x \otimes 1 - 1 \otimes x$$

$$= z \otimes 1 - 1 \otimes z + y \pi_0^{-1} \otimes 1 - 1 \otimes y \pi_0^{-1}$$

$$\equiv z \otimes 1 - 1 \otimes z + y \pi_0^{-1} \otimes 1 - 1 \otimes y \pi_0^{-1}$$

$$+ \sum_{i=1}^{p-1} (y \pi_0^{-1})^{\frac{p}{q}} \otimes (y \pi_0^{-1})^{\frac{p}{q}(p-i)} \mod X_{q^2+2},$$

and for $p = 2$ we should put the sign $-$ before the sum, but this does not change anything.

Next, we have

$$[p]_F(x) \otimes 1 - 1 \otimes [p]_F(x) = (y + \pi_0^{-q} a) \otimes 1 - 1 \otimes (y + \pi_0^{-q} a)$$

$$= y \otimes 1 - 1 \otimes y \equiv y \otimes 1 - 1 \otimes y \mod X_{q^2+q}.$$

Thus, we obtain

$$\alpha \equiv z \otimes 1 - 1 \otimes z - \sum_{i=1}^{p-1} \frac{1}{i} (y \pi_0^{-1})^{\frac{p}{q}} \otimes (y \pi_0^{-1})^{\frac{p}{q}(p-i)} \mod X_{q^2+2}.$$
Now we prove that $I = (1, \pi_1 - d_n \xi_s^* \rho_j)$ is free over $A_{K/K_1}$. We take $y$ such that $v(y) = -1$. As in the proof of Proposition 5.2, we check that $K_1/K$ is semistable and the element

$$\eta = \xi_G / \text{Gal}(K/K_1) = \sum_{\tau \in G / \text{Gal}(K/K_1)} \prod_{[\sigma] = \tau, \sigma \in G} a_{\sigma\tau}$$

generates the “power” basis of associated modules in $K_1/K$ (because all summands on the lower diagonals of the corresponding $*$-product cancel). As in Subsection 5.2, it is easy to show that $\langle 1, \pi_1 - d_n \xi_s^* \rho_j \rangle y = I$, $0 \leq s < p$, $0 \leq j < \frac{2p^2}{p}$, $\rho = \eta \text{tr}_{K_1/K}$. Moreover, we have $d(\xi_s^* \rho_j) = 0$, whence $\pi_0 \xi_s^* \rho_j \in A_{K/K_1}(I, I)$. We conclude that $A_{K/K_1}(I, I) = \langle 1, \pi_1 - d_n \xi_s^* \rho_j \rangle$ and the ideal $I = 2M^{-1}$ is free over $A_{K/K_1}(I, I)$.

Since $n \mid d(\xi)$ and $p(\xi) \not\in \mathbb{F}$, the extension $K/k$ is not semistable.

It is easily seen that the restrictions (9) and (10) on the ramification jumps are fulfilled for the extension constructed.

If $e$ is sufficiently large, then, by lifting this $K/k$ by tamely ramified extensions, examples of minimally unstable extensions that contain ideals free over their associated modules can be constructed for almost all values of $h \mod n$ for which the conditions of Lemma 3.3 fail.

References


Department of Mathematics and Mechanics, St. Petersburg State University, Universitetskii Prospect 28, Staryy Peterhof, St. Petersburg 198504, Russia

E-mail address: mbondarko@hotmail.com

Received 1/DEC/2005

Translated by THE AUTHOR