Journal of Number Theory 142 (2014) 1–17

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Indices of inseparability and refined ramification breaks

Kevin Keating

Department of Mathematics, University of Florida, Gainesville, FL 32611, USA

ARTICLE INFO

Article history:
Received 23 June 2013
Received in revised form 6 February 2014
Accepted 7 February 2014
Available online 2 April 2014
Communicated by David Goss

Keywords:
Local fields
Ramification
Index of inseparability
Kummer theory
Refined ramification breaks
Truncated exponentiation
Class field theory
Galois modules

ABSTRACT

Let K be a finite extension of $\mathbb{Q}_p$ which contains a primitive pth root of unity ζ_p. Let L/K be a totally ramified $(\mathbb{Z}/p\mathbb{Z})^2$-extension which has a single ramification break b. In [2] Byott and Elder defined a "refined ramification break" b_* for L/K. In this paper we prove that if $p > 2$ and the index of inseparability i_1 of L/K is not equal to $p^2b - pb$ then $b_* = i_1 - p^2b + pb + b$.

1. Introduction

Let K be a finite extension of $\mathbb{Q}_p$, let L/K be a finite Galois extension, and let π_L be a uniformizer for L. For simplicity we assume that L/K is a totally ramified extension of degree p^n for some $n \geqslant 1$. The (lower) ramification breaks of L/K are the integers $v_L(\sigma(\pi_L) - \pi_L) - 1$ for $\sigma \in \mathrm{Gal}(L/K)$, $\sigma \neq \mathrm{id}_L$. The extension L/K has at most n

E-mail address: keating@ufl.edu.

http://dx.doi.org/10.1016/j.jnt.2014.02.007
0022-314X/

distinct ramification breaks; if there are fewer than n breaks then L/K may be viewed as having degenerate ramification data.

There have been several attempts to supply the "missing" ramification data in the cases where L/K has fewer than n breaks. The indices of inseparability $i_0, i_1, \dots, i_n$ of L/K were defined by Fried [6] in characteristic p and by Heiermann [7] in characteristic 0. The indices of inseparability determine the ramification breaks of L/K in all cases. As for the opposite direction, if L/K has n distinct ramification breaks then the breaks determine the indices of inseparability, but if L/K has fewer than n breaks then the indices of inseparability are not completely determined by the breaks. Thus the indices of inseparability give extra information about the extension L/K which can be viewed as the missing ramification data.

In [1,2], Byott and Elder described an alternative method for supplying missing ramification data by defining refined lower ramification breaks for extensions with fewer than n ordinary breaks. Suppose L/K is a totally ramified $(\mathbb{Z}/p\mathbb{Z})^2$-extension with a single (ordinary) ramification break b. Then L/K has one refined break b_*, which is computed in [2] under the assumption that K contains a primitive pth root of unity. Byott and Elder also showed that the Galois module structure of $\mathcal{O}_L$ determines b_* in certain cases.

In this paper we study the relationship between the index of inseparability i_1 of L/K and the refined ramification break b_*. In particular, when $p > 2$ and $i_1 \neq p^2b - pb$ we give a formula which expresses b_* in terms of i_1. Our approach is based on the methods given in [8] for computing i_1 in terms of the norm group $\mathrm{N}_{L/K}(L^\times)$. We relate these methods to the Byott–Elder formula for b_* using Vostokov's formula [9] for computing the Kummer pairing $\langle\, , \rangle_p : K^\times \times K^\times \to \boldsymbol{\mu}_p$. The calculations are simplified somewhat through the use of the Artin–Hasse exponential series $E_p(X)$.

The author would like to thank the referee for writing a very careful and thorough review of this paper.

Notation.

K = finite extension of $\mathbb{Q}_p$.
$K_0/\mathbb{Q}_p$ = maximum unramified subextension of $K/\mathbb{Q}_p$.
v_K = valuation on K normalized so that $v_K(K^\times) = \mathbb{Z}$.
$e = v_K(p)$ = absolute ramification index of K.
$\mathcal{O}_K = \{\alpha \in K\colon\ v_K(\alpha) \geqslant 0\}$ = ring of integers of K.
$\mathcal{M}_K = \{\alpha \in K\colon\ v_K(\alpha) \geqslant 1\}$ = maximal ideal of $\mathcal{O}_K$.
$\mathbb{F}_q \cong \mathcal{O}_K/\mathcal{M}_K$ = residue field of K.
$U_K^c = 1 + \mathcal{M}_K^c$ for $c \geqslant 1$.
K^{ab} = maximal abelian extension of K.
L/K = totally ramified $(\mathbb{Z}/p\mathbb{Z})^2$-subextension of K^{ab}/K with one ramification break b.
π_L = uniformizer for L.
$\pi_K = \mathrm{N}_{L/K}(\pi_L)$ = uniformizer for K.

ζ_n = primitive nth root of unity in K^{ab}.
$\boldsymbol{\mu}_n = \langle \zeta_n \rangle$.
$\mathbb{Z}_{p^2} = \mathbb{Z}_p[\boldsymbol{\mu}_{p^2-1}]$.

2. The Artin–Hasse exponential series and truncated exponentiation

In this section we study the relation between the Artin–Hasse exponential series and the "truncated exponentiation" polynomials of Byott–Elder. We also use the Artin–Hasse exponential series to obtain a new version of a formula from [8] for the index of inseparability i_1 of a $(\mathbb{Z}/p\mathbb{Z})^2$-extension with a single ramification break.

The Artin–Hasse exponential series is defined by

$$E_p(X) = \exp\left(X + \frac{1}{p}X^p + \frac{1}{p^2}X^{p^2} + \cdots\right), \tag{2.1}$$

where $\exp(X) \in \mathbb{Q}[\![X]\!]$ is the usual exponential series. Let μ denote the Möbius function. Then, by Lemma 9.1 in [5, I] we have

$$E_p(X) = \prod_{p \nmid c} \left(1 - X^c\right)^{-\mu(c)/c}.$$

Thus the coefficients of $E_p(X)$ lie in $\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p$. For each $i \geqslant 1$ the power series $E_p(X) = 1 + X + \cdots$ induces a bijection from $\mathcal{M}_K^i$ onto U_K^i. For $\kappa, \lambda \in \mathcal{M}_K$ we have $E_p(\kappa) \equiv E_p(\lambda) \pmod{\mathcal{M}_K^i}$ if and only if $\kappa \equiv \lambda \pmod{\mathcal{M}_K^i}$. Let $\Lambda_p : U_K^1 \to \mathcal{M}_K$ denote the inverse of the bijection from $\mathcal{M}_K$ to U_K^1 induced by $E_p(X)$. Then for $u, v \in U_K^1$ we have $\Lambda_p(u) \equiv \Lambda_p(v) \pmod{\mathcal{M}_K^i}$ if and only if $u \equiv v \pmod{\mathcal{M}_K^i}$.

Let $\psi(X) \in XK[\![X]\!]$ and $\alpha \in K$. The α power of $1 + \psi(X)$ is a series in $K[\![X]\!]$ defined by

$$\left(1 + \psi(X)\right)^{\alpha} = \sum_{n=0}^{\infty} \binom{\alpha}{n} \psi(X)^n,$$

where

$$\binom{\alpha}{n} = \frac{\alpha(\alpha-1)(\alpha-2)\ldots(\alpha-(n-1))}{n!}.$$

Motivated by this formula, Byott and Elder [1, 1.1] defined truncated exponentiation by

$$\left(1 + \psi(X)\right)^{[\alpha]} = \sum_{n=0}^{p-1} \binom{\alpha}{n} \psi(X)^n.$$

Thus $(1 + X)^{[\alpha]}$ is a polynomial with coefficients in K; if $\alpha \in \mathcal{O}_K$ then the coefficients of $(1 + X)^{[\alpha]}$ lie in $\mathcal{O}_K$. For $u \in U_K^1$ define $u^{[\alpha]}$ to be the value of $(1 + X)^{[\alpha]}$ at $X = u - 1$.

Lemma 2.1. *Let $\alpha \in K$. Then $E_p(X)^{[\alpha]} \equiv E_p(\alpha X) \pmod{X^p}$.*

Proof. We have $E_p(X)^{[\alpha]} \equiv \exp(X)^\alpha \equiv \exp(\alpha X) \equiv E_p(\alpha X) \pmod{X^p}$. □

Proposition 2.2. *Let $i \geqslant 1$, let $u, v \in U_K^i$, and let $\alpha \in \mathcal{O}_K$. Then*

$$\Lambda_p(uv) \equiv \Lambda_p(u) + \Lambda_p(v) \pmod{\mathcal{M}_K^{pi}}$$
$$\Lambda_p\bigl(u^{[\alpha]}\bigr) \equiv \alpha\Lambda_p(u) \pmod{\mathcal{M}_K^{pi}}.$$

Proof. Set $\kappa = \Lambda_p(u)$ and $\lambda = \Lambda_p(v)$. Then $\kappa, \lambda \in \mathcal{M}_K^i$, so by Eq. (6) in [4, p. 52] we have

$$E_p(\kappa)E_p(\lambda) \equiv E_p(\kappa + \lambda) \pmod{\mathcal{M}_K^{pi}}.$$

In addition, by Lemma 2.1 we get

$$E_p(\kappa)^{[\alpha]} \equiv E_p(\alpha\kappa) \pmod{\mathcal{M}_K^{pi}}.$$

Applying Λ_p to these congruences gives the desired results. □

Corollary 2.3. *Let $i \geqslant 1$. The scalar multiplication $\alpha \cdot u = u^{[\alpha]}$ induces an $\mathcal{O}_K$-module structure on the group U_K^i/U_K^{pi}. Furthermore, Λ_p induces an isomorphism of $\mathcal{O}_K$-modules from U_K^i/U_K^{pi} onto $\mathcal{M}_K^i/\mathcal{M}_K^{pi}$.*

Corollary 2.4. *Let $u \in U_K^i$ and $\alpha \in \mathbb{Z}_p$. Then $u^\alpha \equiv u^{[\alpha]} \pmod{\mathcal{M}_K^{pi}}$.*

Proof. For $n \geqslant 1$ we have $\Lambda_p(u^n) \equiv n\Lambda_p(u) \equiv \Lambda_p(u^{[n]}) \pmod{\mathcal{M}_K^{pi}}$. □

Corollary 2.5. *Let $i \geqslant 1$ and let A be a subgroup of U_K^i which contains U_K^{pi}. Then $\Lambda_p(A)$ is a $\mathbb{Z}_p$-module.*

Corollary 2.6. *Let $i \geqslant 1$ and let A, B be subgroups of U_K^i such that $U_K^{pi} \subset B$. Then $\Lambda_p(AB) = \Lambda_p(A) + \Lambda_p(B)$.*

Proof. We clearly have $\Lambda_p(AB) \supset \Lambda_p(A)$ and $\Lambda_p(AB) \supset \Lambda_p(B)$. Hence, by Corollary 2.5 we get $\Lambda_p(AB) \supset \Lambda_p(A)+\Lambda_p(B)$. Let $a \in A$, $b \in B$. Then $\Lambda_p(ab) = \Lambda_p(a)+\Lambda_p(b)+m$ for some $m \in \mathcal{M}_K^{pi}$. Let $b' \in U_K^i$ be such that $\Lambda_p(b') = \Lambda_p(b) + m$. Then $b \equiv b' \pmod{\mathcal{M}_K^{pi}}$, so $b' \in B$. Hence $\Lambda_p(AB) \subset \Lambda_p(A) + \Lambda_p(B)$. We conclude that $\Lambda_p(AB) = \Lambda_p(A) + \Lambda_p(B)$. □

Let $\mathbb{Q}_{p^2} = \mathbb{Q}_p(\zeta_{p^2-1})$ denote the unramified extension of $\mathbb{Q}_p$ of degree 2, and let $\mathbb{Z}_{p^2}$ denote the ring of integers of $\mathbb{Q}_{p^2}$.

Corollary 2.7. *Assume $\boldsymbol{\mu}_{p^2-1} \subset K$ and let A be a subgroup of U_K^i which contains U_K^{pi}. Then $\Lambda_p(A)$ is a $\mathbb{Z}_{p^2}$-module if and only if A is stable under the map $a \mapsto a^{[\eta]}$ for every $\eta \in \boldsymbol{\mu}_{p^2-1}$.*

Proof. This follows from Proposition 2.2 and the fact that $\mathbb{Z}_{p^2} = \mathbb{Z}_p[\boldsymbol{\mu}_{p^2-1}]$. □

Proposition 2.8. *Let i, j be positive integers such that $pj \geqslant i$ and $e + \lceil \frac{j}{p} \rceil \geqslant i$, and let $K_0/\mathbb{Q}_p$ be the maximum unramified subextension of $K/\mathbb{Q}_p$. Then $\Lambda_p((K^\times)^p \cap U_K^j) + \mathcal{M}_K^i$ is an $\mathcal{O}_{K_0}$-module.*

Proof. If $i \leqslant j$ then the claim is obvious, so we assume $i \geqslant j+1$. Then

$$i \leqslant e + \left\lceil \frac{i-1}{p} \right\rceil \leqslant e + \frac{i+p-2}{p}.$$

It follows that $i \leqslant \frac{pe}{p-1} + \frac{p-2}{p-1}$, and hence that $i \leqslant \lceil \frac{pe}{p-1} \rceil$. By applying Corollary 2.6 with i replaced by j, $A = (K^\times)^p \cap U_K^j$, and $B = U_K^i$ we get

$$\Lambda_p\big(\big((K^\times)^p \cap U_K^j\big) \cdot U_K^i\big) = \Lambda_p\big((K^\times)^p \cap U_K^j\big) + \mathcal{M}_K^i.$$

Hence, by Corollary 2.5 we see that $\Lambda_p((K^\times)^p \cap U_K^j) + \mathcal{M}_K^i$ is a $\mathbb{Z}_p$-module. Let $u \in (K^\times)^p \cap U_K^j$ with $c = v_K(u-1) < i$. Then there is $\gamma \in \mathcal{M}_K$ such that $u = E_p(\gamma)^p$. Using (2.1) we get

$$\begin{aligned} u &= \exp\left(p\gamma + \gamma^p + \frac{1}{p}\gamma^{p^2} + \cdots\right) \\ &= \exp(p\gamma) \cdot E_p\big(\gamma^p\big). \end{aligned}$$

Since $c < \lceil \frac{pe}{p-1} \rceil$ and c is an integer we have $c < \frac{pe}{p-1}$, so $p \mid c$ and $v_K(\gamma) = \frac{c}{p}$. Therefore $v_K(p\gamma) = e + \frac{c}{p} \geqslant e + \lceil \frac{j}{p} \rceil \geqslant i$, and hence $u \equiv E_p(\gamma^p) \pmod{\mathcal{M}_K^i}$. On the other hand, for each $\gamma \in \mathcal{M}_K$ such that $v_K(\gamma^p) \geqslant j$, the computations above show that $E_p(\gamma^p) = E_p(\gamma)^p \cdot \exp(-p\gamma)$ lies in $((K^\times)^p \cap U_K^j) \cdot U_K^i$. It follows that

$$\Lambda_p\big(\big(K^\times\big)^p \cap U_K^j\big) + \mathcal{M}_K^i = \big\{\gamma^p\colon \gamma \in \mathcal{M}_K,\ v_K\big(\gamma^p\big) \geqslant j\big\} + \mathcal{M}_K^i. \tag{2.2}$$

Let q be the cardinality of the residue field of K. Then $\boldsymbol{\mu}_{q-1} \subset \mathcal{O}_K$, so the right side of (2.2) is stable under multiplication by elements of $\boldsymbol{\mu}_{q-1}$. Since $\mathcal{O}_{K_0} = \mathbb{Z}_p[\boldsymbol{\mu}_{q-1}]$, the proposition follows. □

3. Two invariants of L/K

Let L/K be a totally ramified $(\mathbb{Z}/p\mathbb{Z})^2$-extension with a single ramification break b. Then $1 \leqslant b < \frac{pe}{p-1}$ and $p \nmid b$ (see for instance [3, p. 398]). In this section we define two further invariants of L/K: the refined ramification break b_* and the index of inseparability i_1. We also show how i_1 can be computed in terms of the valuations of the coefficients of the minimum polynomial over K of a uniformizer for L.

To motivate the definition of b_* we first reformulate the definition of $i(\sigma)$ for $\sigma \in \mathrm{Gal}(L/K)$. It is easily seen that

$$i(\sigma) = \min\bigl\{v_L\bigl(\sigma(\alpha) - \alpha\bigr) - v_L(\alpha)\colon\ \alpha \in \mathcal{O}_L,\ \alpha \neq 0\bigr\}.$$

Thus $i(\sigma)$ may be viewed as the valuation of the operator $\sigma - 1$ on $\mathcal{O}_L$. Now let σ_1, σ_2 be generators for $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/p\mathbb{Z})^2$. Since b is the unique ramification break of L/K, for $i = 1, 2$ we have $\sigma_i(\pi_L) - \pi_L = \beta_i$ with $v_L(\beta_i) = b + 1$. Let $\delta \in \boldsymbol{\mu}_{q-1}$ be such that $\beta_1/\beta_2 \equiv \delta \pmod{\mathcal{M}_L}$. Then

$$\sigma_2^{[-\delta]} = \sum_{n=0}^{p-1} \binom{-\delta}{n} (\sigma_2 - 1)^n$$

is an element of the group ring $\mathcal{O}_{K_0}[\mathrm{Gal}(L/K)]$. We define

$$b_* = \min\bigl\{v_L\bigl(\sigma_1 \circ \sigma_2^{[-\delta]}(\alpha) - \alpha\bigr) - v_L(\alpha)\colon\ \alpha \in \mathcal{O}_L,\ \alpha \neq 0\bigr\}.$$

Thus $b_* = i(\sigma_1 \circ \sigma_2^{[-\delta]})$ is the valuation of the operator $\sigma_1 \circ \sigma_2^{[-\delta]} - 1$ on $\mathcal{O}_L$. It is proved in [2] that b_* does not depend on the choice of generators σ_1, σ_2 for $\mathrm{Gal}(L/K)$.

We now define the indices of inseparability of L/K, following Heiermann [7]. Let π_L be a uniformizer for L. Then $\pi_K = \mathrm{N}_{L/K}(\pi_L)$ is a uniformizer for K, and there are unique $c_h \in \boldsymbol{\mu}_{q-1} \cup \{0\}$ such that

$$\pi_K = \sum_{h=0}^{\infty} c_h \pi_L^{h+p^2}.$$

For $0 \leqslant j \leqslant 2$ set

$$\begin{aligned} i_j^* &= \min\bigl\{h \geqslant 0\colon\ c_h \neq 0,\ v_p\bigl(h + p^2\bigr) \leqslant j\bigr\} \\ i_j &= \min\bigl\{i_{j'}^* + p^2 e \cdot \bigl(j' - j\bigr)\colon\ j \leqslant j' \leqslant 2\bigr\}. \end{aligned}$$

Then i_j^* may depend on the choice of π_L, but i_j does not (see [7, Th. 7.1]). Furthermore, we have $0 = i_2 < i_1 \leqslant i_0$. The relation between the indices of inseparability and the ordinary ramification data of L/K is given by [7, Cor. 6.11]. In particular, we have $i_0 = p^2 b - b$.

As in [8] we let

$$g(X) = X^{p^2} + a_1 X^{p^2-1} + \cdots + a_{p^2-1} X + a_{p^2}$$

be the minimum polynomial for π_L over K. Then, by [8, (3.5)] we get

$$\begin{aligned} i_1 &= \min\left(\left\{p^2 v_K(a_i) - i\colon\ 1 \leqslant i \leqslant p^2 - 1\right\} \cup \left\{i_2 + p^2 e\right\}\right) \\ &= \min\left(\left\{p^2 v_K(a_{pi}) - pi\colon\ 1 \leqslant i \leqslant p - 1\right\} \cup \left\{i_2 + p^2 e, i_0\right\}\right) \\ &= \min\left(\left\{p^2 v_K(a_{pi}) - pi\colon\ 1 \leqslant i \leqslant p - 1\right\} \cup \left\{p^2 e, p^2 b - b\right\}\right). \end{aligned}$$

For $j > p^2$ write $j = p^2 u + i$ with $1 \leqslant i \leqslant p^2$ and set $a_j = \pi_K^u a_i$. Then $v_K(a_{pi+p^2c}) = v_K(a_{pi}) + c$, so for every $l \geqslant 0$ we have

$$i_1 = \min\left(\left\{p^2 v_K(a_{pi}) - pi\colon\ l < i \leqslant l + p,\ p \nmid i\right\} \cup \left\{p^2 e, p^2 b - b\right\}\right). \tag{3.1}$$

Let $H = \mathrm{N}_{L/K}(L^\times)$ be the subgroup of $K^\times$ which is associated to the abelian extension L/K by class field theory. Since b is the only ramification break of L/K we have $U_K^{b+1} \leqslant H$ and

$$U_K^b / \left(H \cap U_K^b\right) \cong K^\times / H \cong \mathrm{Gal}(L/K). \tag{3.2}$$

Theorem 3.1. *Let $p > 2$, let L/K be a totally ramified $(\mathbb{Z}/p\mathbb{Z})^2$-extension with a single ramification break $b \geqslant 1$, and set $H = \mathrm{N}_{L/K}(L^\times)$. If $\boldsymbol{\mu}_{p^2-1} \not\subset K$ let $k = b$; otherwise let k be the smallest nonnegative integer such that $\Lambda_p(H \cap U_K^{k+1})$ is a $\mathbb{Z}_{p^2}$-module. Then*

$$i_1 = \min\left\{p^2 b - pk, p^2 e, p^2 b - b\right\}.$$

Proof. Let $i \geqslant 1$ satisfy $p \nmid i$. Then, by [8, (3.25)] we have

$$\mathrm{N}_{L/K}\left(E_p\left(r\pi_L^i\right)\right) \equiv E_p\left(\pi_K^i r^{p^2}\right) \cdot E_p\left(-i a_{pi} r^p - i a_i r\right) \pmod{\mathcal{M}_K^{b+1}}.$$

By [8, Lemma 3.2] we have

$$\begin{aligned} v_K(a_i) &\geqslant b - \frac{b-i}{p^2} = \left(1 - \frac{1}{p^2}\right) b + \frac{1}{p^2} \cdot i \\ v_K(a_{pi}) &\geqslant b - \frac{pb - pi}{p^2} = \left(1 - \frac{1}{p}\right) b + \frac{1}{p} \cdot i. \end{aligned} \tag{3.3}$$

Hence, if $i \leqslant b$ then $v_K(a_i) \geqslant i$ and $v_K(a_{pi}) \geqslant i$, with strict inequalities if $i < b$. It follows that

$$\mathrm{N}_{L/K}\left(E_p\left(r\pi_L^i\right)\right) \equiv E_p\left(\beta_i(r)\right) \pmod{\mathcal{M}_K^{b+1}}, \tag{3.4}$$

with $\beta_i(r) = \pi_K^i r^{p^2} - i a_{pi} r^p - i a_i r$. In addition, we have $v_K(\beta_i(r)) \geqslant i$, with equality if $i < b$ and $r \neq 0$.

Since $\Lambda_p(H \cap U_K^{b+1}) = \mathcal{M}_K^{b+1}$ we have $k \leqslant b$. We claim that $v_K(a_{pi}) \geqslant b + 1$ for all $i \geqslant k + 1$ such that $p \nmid i$. If $k = b$ this follows from (3.3). Let $k < b$ and suppose the claim is false. Let $h \geqslant k + 1$ be maximum with the property that $p \nmid h$ and $v_K(a_{ph}) \leqslant b$. Since $a_{p(h+p)} = \pi_K a_{ph}$ we see that a maximum h exists, and that $v_K(a_{ph}) = b$. Since

$H \cap U_K^{k+1} \supset U_K^{b+1}$, it follows from (3.4) and Corollary 2.6 that $E_p(\beta_h(r)) \in H \cap U_K^{k+1}$ for all $r \in \boldsymbol{\mu}_{q-1} \cup \{0\}$. By the definition of k, $\Lambda_p(H \cap U_K^{k+1})$ is a $\mathbb{Z}_{p^2}$-module. Hence, for every $r \in \boldsymbol{\mu}_{q-1}$ and $\eta \in \boldsymbol{\mu}_{p^2-1}$,

$$\eta\beta_h(r) - \beta_h(\eta r) = ha_{ph}r^p\left(\eta^p - \eta\right)$$

lies in $\Lambda_p(H \cap U_K^{k+1})$. Since every coset of $\mathcal{M}_K^{b+1}$ in $\mathcal{M}_K^b$ is represented by an element of this form, and

$$\Lambda_p\left(H \cap U_K^{k+1}\right) \supset \Lambda_p\left(U_K^{b+1}\right) = \mathcal{M}_K^{b+1},$$

it follows that $\Lambda_p(H \cap U_K^{k+1}) \supset \mathcal{M}_K^b$. Hence $H \supset E_p(\mathcal{M}_K^b) = U_K^b$, which contradicts (3.2). This proves our claim, so we have

$$p^2b - pk \leqslant p^2v_K(a_{pi}) - pi \tag{3.5}$$

for all i such that $k < i \leqslant k + p$ and $p \nmid i$.

Set $m = \min\{p^2b - pk, p^2e, p^2b - b\}$. Suppose $m = p^2b - b$. Then $k \leqslant \frac{b}{p}$, so by the preceding paragraph we have $v_K(a_{pi}) \geqslant b + 1$ for all $i > \frac{b}{p}$ such that $p \nmid i$. Hence, by (3.1) we get

$$\begin{aligned} i_1 &= \min\left(\left\{p^2v_K(a_{pi}) - pi\colon\ \frac{b}{p} < i \leqslant \frac{b}{p} + p,\ p \nmid i\right\} \cup \left\{p^2e, p^2b - b\right\}\right) \\ &= p^2b - b. \end{aligned}$$

Suppose $m = p^2e$. Then $k \leqslant p(b - e)$, so $v_K(a_{pi}) \geqslant b + 1$ for all $i > p(b - e)$ such that $p \nmid i$. Hence, by (3.1) we have

$$\begin{aligned} i_1 &= \min\left(\left\{p^2v_K(a_{pi}) - pi\colon\ p(b - e) < i < p(b - e) + p\right\} \cup \left\{p^2e, p^2b - b\right\}\right) \\ &= p^2e. \end{aligned}$$

Suppose $m = p^2b - pk$ with $p^2b - pk < \min\{p^2e, p^2b - b\}$. We claim that $p \nmid k$. In fact if $p \mid k$ then $k < b < \frac{pe}{p-1}$, so we have

$$H \cap U_K^k = \left(\left(K^\times\right)^p \cap U_K^k\right) \cdot \left(H \cap U_K^{k+1}\right).$$

Since $pk \geqslant b + 1$ and $H \cap U_K^{k+1} \supset U_K^{b+1}$ it follows from Corollary 2.6 that

$$\Lambda_p\left(H \cap U_K^k\right) = \Lambda_p\left(\left(K^\times\right)^p \cap U_K^k\right) + \Lambda_p\left(H \cap U_K^{k+1}\right). \tag{3.6}$$

Since $p^2b - pk < p^2e$ we have $e + \frac{k}{p} \geqslant b + 1$. Therefore, by Proposition 2.8 we see that $\Lambda_p((K^\times)^p \cap U_K^k) + \mathcal{M}_K^{b+1}$ is an $\mathcal{O}_{K_0}$-module. Furthermore, $\Lambda_p(H \cap U_K^{k+1})$ is a $\mathbb{Z}_{p^2}$-module by the definition of k. Since $\mathbb{Z}_{p^2} \subset \mathcal{O}_{K_0}$ and $\Lambda_p(H \cap U_K^{k+1}) \supset \mathcal{M}_K^{b+1}$, it follows from (3.6) that $\Lambda_p(H \cap U_K^k)$ is a $\mathbb{Z}_{p^2}$-module. This contradicts the definition of k, so $p \nmid k$.

Suppose $a_{pk} \in \mathcal{M}_K^{b+1}$. Then for every $\eta \in \boldsymbol{\mu}_{p^2-1}$ and $r \in \boldsymbol{\mu}_{q-1}$ we have

$$\eta\beta_k(r) \equiv \beta_k(\eta r) \pmod{\pi_K^{b+1}}. \tag{3.7}$$

If $\boldsymbol{\mu}_{p^2-1} \subset K$ this implies $\eta\beta_k(r) \in \Lambda_p(H \cap U_K^k)$. Since $\Lambda_p(H \cap U_K^{k+1})$ is a $\mathbb{Z}_{p^2}$-module it follows that $\Lambda_p(H \cap U_K^k)$ is a $\mathbb{Z}_{p^2}$-module, contrary to assumption. Therefore $a_{pk} \notin \mathcal{M}_K^{b+1}$ in this case. If $\boldsymbol{\mu}_{p^2-1} \not\subset K$ then $k = b$ and it follows from (3.7) that the set

$$S = \left\{r \in \boldsymbol{\mu}_{q-1} \cup \{0\}:\ \beta_b(r) \equiv 0 \pmod{\mathcal{M}_K^{b+1}}\right\}$$

is stable under multiplication by elements of $\boldsymbol{\mu}_{p^2-1}$. Hence $S = \{0\}$. Since

$$\beta_b(r + r') \equiv \beta_b(r) + \beta_b(r') \pmod{\mathcal{M}_K^{b+1}}$$

for $r, r' \in \boldsymbol{\mu}_{q-1} \cup \{0\}$ this implies that every coset of $\mathcal{M}_K^{b+1}$ in $\mathcal{M}_K^b$ is represented by $\beta_b(r)$ for some $r \in \boldsymbol{\mu}_{q-1} \cup \{0\}$. It follows that $\Lambda_p(H \cap U_K^b) = \mathcal{M}_K^b$, a contradiction. Hence $a_{pk} \notin \mathcal{M}_K^{b+1}$ in this case as well.

Since $p \nmid k + p$, by (3.5) we have $\pi_K a_{pk} = a_{p(k+p)} \in \mathcal{M}_K^{b+1}$. Thus $v_K(a_{pk}) = b$. Using (3.1) and (3.5) we get

$$\begin{aligned} i_1 &= \min\left(\left\{p^2 v_K(a_{pi}) - pi:\ k \leqslant i < k + p,\ p \nmid i\right\} \cup \left\{p^2 e, p^2 b - b\right\}\right) \\ &= p^2 b - pk. \end{aligned}$$

We conclude that $i_1 = m$ in every case. $\square$

Remark 3.2. Suppose $\boldsymbol{\mu}_{p^2-1} \subset K$. Then it follows from Corollary 2.3 and class field theory that all values of k such that $b/p < k \leqslant b$ and $p \nmid k$ can be realized by extensions L/K satisfying the conditions of Theorem 3.1.

Remark 3.3. Using Theorem 3.1 we obtain the bounds $p^2 b - pb \leqslant i_1 \leqslant p^2 b - b$. These inequalities can also be derived from Corollary 6.11 in [7]. It follows from these bounds that the condition $i_1 > p^2 b - pb$ is equivalent to $i_1 \neq p^2 b - pb$.

4. Kummer theory

Let $p > 2$ and let K be a finite extension of $\mathbb{Q}_p$ which contains a primitive pth root of unity ζ_p. Let K^{ab} be a maximal abelian extension of K and let L/K be a totally ramified $(\mathbb{Z}/p\mathbb{Z})^2$-subextension of K^{ab}/K with a single ramification break b. In [2], Byott and Elder gave a method for computing the refined ramification break b_* of L/K in terms of Kummer theory. In this section we use Vostokov's formula for the Kummer pairing to express b_* in terms of the index of inseparability i_1, under the assumption that i_1 is not equal to $p^2b - pb$. The proof is based on a symmetry relation involving the Kummer pairing and truncated exponentiation.

The Kummer pairing $\langle\,,\rangle_p : K^\times \times K^\times \to \boldsymbol{\mu}_p$ is defined by $\langle\alpha,\beta\rangle_p = \sigma_\beta(\alpha^{1/p})/\alpha^{1/p}$, where $\alpha^{1/p} \in K^{ab}$ is any pth root of α and σ_β is the element of $\mathrm{Gal}(K^{ab}/K)$ that corresponds to β under class field theory. The Kummer pairing is $\mathbb{Z}$-bilinear and skew-symmetric, with kernel $(K^\times)^p$ on the left and right (see for instance Proposition 5.1 in [5, IV]). For $1 \leqslant i \leqslant \frac{pe}{p-1}$ the orthogonal complement of U_K^i with respect to $\langle\,,\rangle_p$ is $(U_K^i)^\perp = (K^\times)^p \cdot U_K^{\frac{pe}{p-1}-i+1}$ (see [3, §1]).

Recall that $K_0/\mathbb{Q}_p$ is the maximum unramified subextension of $K/\mathbb{Q}_p$. In [9] Vostokov gave a formula for computing $\langle\,,\rangle_p$ in terms of residues of elements of

$$K_0\{\{X\}\} = \left\{ \sum_{n=-\infty}^{\infty} a_n X^n\colon\ a_n \in K_0,\ \lim_{n\to-\infty} v_{K_0}(a_n) = \infty,\ \exists m\ \forall n\ v_{K_0}(a_n) \geqslant m \right\}.$$

The set $K_0\{\{X\}\}$ has an obvious operation of addition, and the conditions on the coefficients imply that the natural multiplication on $K_0\{\{X\}\}$ is also well-defined. These operations make $K_0\{\{X\}\}$ a field. Let $\mathcal{O}_{K_0}\{\{X\}\}$ denote the subring of $K_0\{\{X\}\}$ consisting of series whose coefficients lie in $\mathcal{O}_{K_0}$. Also let $\mathrm{Res}(\psi(X))$ denote the coefficient of X^{-1} in $\psi(X) \in K_0\{\{X\}\}$.

For each $\alpha \in U_K^1$ choose $\tilde{\alpha}(X) \in \mathcal{O}_{K_0}[[X]]$ so that $\tilde{\alpha}(0) = 1$ and $\tilde{\alpha}(\pi_K) = \alpha$. Of course there are many series $\tilde{\alpha}(X)$ with this property, but for our purposes it will not matter which we choose. Let $\phi : K_0 \to K_0$ be the p-Frobenius map and define $\tilde{\alpha}^\Delta(X) = \tilde{\alpha}^\phi(X^p)$ and $l(\tilde{\alpha}) = \log(\tilde{\alpha}) - p^{-1}\log(\tilde{\alpha}^\Delta)$, where

$$\log\bigl(1+\psi(X)\bigr) = \psi(X) - \frac{1}{2}\psi(X)^2 + \frac{1}{3}\psi(X)^3 - \cdots$$

for $\psi(X) \in XK_0[[X]]$. By Proposition 2.2 in [5, VI] we have $l(\tilde{\alpha}) \in X\mathcal{O}_{K_0}[[X]]$.

Let $\alpha,\beta \in U_K^1$. Following [5, p. 241] we define

$$\Phi_{\alpha,\beta}(X) = \frac{\tilde{\alpha}'}{\tilde{\alpha}} \cdot l(\tilde{\beta}) - \frac{(\tilde{\beta}^\Delta)'}{p\tilde{\beta}^\Delta} \cdot l(\tilde{\alpha}).$$

Then $\Phi_{\alpha,\beta}(X) \in \mathcal{O}_{K_0}[[X]]$. Let $s(X) = \tilde{\zeta}_p(X)^p - 1$. Then, by Proposition 3.1 in [5, VI], $s(X)$ is a unit in $\mathcal{O}_{K_0}\{\{X\}\}$. Since $p > 2$ and $\alpha,\beta \in U_K^1$, by Theorem 4 in [5, VII] we have

$$\langle\alpha,\beta\rangle_p = \zeta_p^{\mathrm{Tr}_{K_0/\mathbb{Q}_p}(\mathrm{Res}(\Phi_{\alpha,\beta}/s))}. \tag{4.1}$$

Theorem 4.1. *Let $p > 2$ and let K be a finite extension of $\mathbb{Q}_p$ which contains a primitive pth root of unity. Let i, j be positive integers such that $i + pj > \frac{pe}{p-1}$ and $pi + j > \frac{pe}{p-1}$. Let $\alpha \in U_K^i$, $\beta \in U_K^j$, and $\eta \in \mathcal{O}_{K_0}$. Then $\langle\alpha^{[\eta]},\beta\rangle_p = \langle\alpha,\beta^{[\eta]}\rangle_p$.*

Proof. By the linearity and continuity of the Kummer pairing we may assume that $\alpha = E_p(u\pi_K^c)$, $\beta = E_p(v\pi_K^d)$, $\tilde{\alpha}(X) = E_p(uX^c)$, and $\tilde{\beta}(X) = E_p(vX^d)$ with $u, v \in \boldsymbol{\mu}_{q-1}$, $c \geqslant i$, and $d \geqslant j$. It follows from (2.1) that $l(\tilde{\alpha}(X)) = uX^c$ and $l(\tilde{\beta}(X)) = vX^d$. Using (2.1) and Lemma 2.1 we get

$$\begin{aligned}
\frac{\tilde{\alpha}'(X)}{\tilde{\alpha}(X)} &\equiv cuX^{c-1} \pmod{X^{pc-1}} \\
\frac{(\tilde{\beta}^{\Delta})'(X)}{p\tilde{\beta}^{\Delta}(X)} &\equiv 0 \pmod{X^{pd-1}} \\
\frac{(\tilde{\alpha}(X)^{[\eta]})'}{\tilde{\alpha}(X)^{[\eta]}} &\equiv c(\eta u)X^{c-1} \pmod{X^{pc-1}} \\
l\bigl(\tilde{\beta}(X)^{[\eta]}\bigr) &\equiv \eta vX^d \pmod{X^{pd}}.
\end{aligned}$$

Note that $\tilde{\alpha}(X)^{[\eta]}$, $\tilde{\beta}(X)^{[\eta]}$ are elements of $1 + X\mathcal{O}_{K_0}[\![X]\!]$ such that $\tilde{\alpha}(\pi_K)^{[\eta]} = \alpha^{[\eta]}$, $\tilde{\beta}(\pi_K)^{[\eta]} = \beta^{[\eta]}$. Hence we may take $\widetilde{\alpha^{[\eta]}}(X) = \tilde{\alpha}(X)^{[\eta]}$ and $\widetilde{\beta^{[\eta]}}(X) = \tilde{\beta}(X)^{[\eta]}$. Using the computations from the preceding paragraph and the lower bounds for $i + pj$ and $pi + j$ we get

$$\Phi_{\alpha,\beta}(X) \equiv \frac{\tilde{\alpha}'}{\tilde{\alpha}} \cdot l(\tilde{\beta}) \pmod{X^{\frac{pe}{p-1}}}$$

$$\Phi_{\alpha^{[\eta]},\beta}(X) \equiv c(\eta u)vX^{c+d-1} \pmod{X^{\frac{pe}{p-1}}} \tag{4.2}$$

$$\Phi_{\alpha,\beta^{[\eta]}}(X) \equiv cu(\eta v)X^{c+d-1} \pmod{X^{\frac{pe}{p-1}}}. \tag{4.3}$$

It follows from Proposition 3.1 in [5, VI] that the image of $s(X) \in \mathcal{O}_{K_0}\{\!\{X\}\!\}^\times$ in

$$(\mathcal{O}_{K_0}/\mathcal{M}_{K_0})((X)) \cong \mathbb{F}_q((X))$$

has X-valuation $\frac{pe}{p-1}$. Therefore, by (4.2) and (4.3) we have

$$\frac{\Phi_{\alpha^{[\eta]},\beta}(X) - \Phi_{\alpha,\beta^{[\eta]}}(X)}{s(X)} = \gamma(X) + p\delta(X)$$

for some $\gamma(X) \in \mathcal{O}_{K_0}[\![X]\!]$ and $\delta(X) \in \mathcal{O}_{K_0}\{\!\{X\}\!\}$. It follows that

$$\operatorname{Res}\left(\frac{\Phi_{\alpha^{[\eta]},\beta}(X)}{s(X)}\right) \equiv \operatorname{Res}\left(\frac{\Phi_{\alpha,\beta^{[\eta]}}(X)}{s(X)}\right) \pmod{\mathcal{M}_{K_0}}.$$

Therefore, by (4.1) we get $\langle \alpha^{[\eta]}, \beta\rangle_p = \langle \alpha, \beta^{[\eta]}\rangle_p$. □

Corollary 4.2. *Let K, i, j satisfy the hypotheses of Theorem 4.1. Let A be a subgroup of U_K^i such that A contains U_K^{pi} and $\Lambda_p(A)$ is a $\mathbb{Z}_{p^2}$-module. Then $\Lambda_p(A^\perp \cap U_K^j)$ is a $\mathbb{Z}_{p^2}$-module.*

Proof. Let $\alpha \in A$. By Corollary 2.7 we have $\alpha^{[\eta]} \in A$ for every $\eta \in \boldsymbol{\mu}_{p^2-1}$. Hence, for $\beta \in A^\perp \cap U_K^j$ we see that $\langle \alpha, \beta^{[\eta]} \rangle_p = \langle \alpha^{[\eta]}, \beta \rangle_p = 1$. Since this holds for every $\alpha \in A$ we get $\beta^{[\eta]} \in A^\perp \cap U_K^j$. Since $pj \geqslant \frac{pe}{p-1} - i + 1$ we have $A^\perp \cap U_K^j \supset U_K^{pj}$. Therefore, it follows from Corollary 2.7 that $\Lambda_p(A^\perp \cap U_K^j)$ is a $\mathbb{Z}_{p^2}$-module. □

Recall that $H = \mathrm{N}_{L/K}(L^\times)$ is the subgroup of $K^\times$ that corresponds to L/K under class field theory, and let $R = (L^\times)^p \cap K^\times$ denote the subgroup of $K^\times$ that corresponds to L/K under Kummer theory. Then R contains $(K^\times)^p$, and it follows from the basic properties of the Kummer pairing that $R = H^\perp$ and $H = R^\perp$. Furthermore, $R/(K^\times)^p$ and $K^\times/H$ are both elementary abelian p-groups of rank 2. Let $R_0 = R \cap U_K^{\frac{pe}{p-1}-b}$. Since the only ramification break of L/K is b we see that $R = R_0 \cdot (K^\times)^p$ and

$$R_0/\big(\big(K^\times\big)^p \cap U_K^{\frac{pe}{p-1}-b}\big) \cong R/\big(K^\times\big)^p$$

(cf. [3]).

For $a \in \mathcal{O}_K$ we let $\bar{a} = a + \mathcal{M}_K^{\frac{pe}{p-1}-b+1}$ denote the image of a in $\mathcal{O}_K/\mathcal{M}_K^{\frac{pe}{p-1}-b+1}$. Then $\overline{R}_0 \cong R/(K^\times)^p$ is an elementary abelian p-group of rank 2. Let $1+\rho_1$, $1+\rho_2$ be elements of R_0 such that $\overline{1+\rho_1}$, $\overline{1+\rho_2}$ generate $\overline{R}_0$. Then $v_K(\rho_1) = v_K(\rho_2) = \frac{pe}{p-1} - b$. Let $\theta \in \boldsymbol{\mu}_{q-1}$ be such that $\theta \equiv \rho_2/\rho_1 \pmod{\mathcal{M}_K}$. Then $\theta \notin \boldsymbol{\mu}_{p-1}$ and

$$(1+\rho_1)^{[\theta]} \equiv 1 + \rho_2 \quad \big(\mathrm{mod}\ \mathcal{M}_K^{\frac{pe}{p-1}-b+1}\big).$$

Let $s \leqslant \frac{pe}{p-1}$ be maximum such that $(1+\rho_1)^{[\theta]} \in R_0 \cdot U_K^s$, and set $t = \frac{pe}{p-1} - s$. Then, by [2, Prop. 10] we have

$$b_* = pb - \max\big\{pt - b, \big(p^2-1\big)b - p^2 e, 0\big\}. \tag{4.4}$$

Lemma 4.3. *Let $p > 2$ and assume that K contains a primitive pth root of unity. Let L/K be a totally ramified $(\mathbb{Z}/p\mathbb{Z})^2$-subextension of K^{ab}/K with a single ramification break b. Then the following are equivalent:*

1. $\theta \in \boldsymbol{\mu}_{p^2-1}$.
2. $\Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-b+1}$ *is a* $\mathbb{Z}_{p^2}$*-module.*
3. $\Lambda_p(H \cap U_K^b)$ *is a* $\mathbb{Z}_{p^2}$*-module.*
4. $i_1 > p^2 b - pb$.

Proof. To prove the equivalence of the first two statements we note that $\overline{\Lambda_p(1+\rho_1)}$ and $\overline{\Lambda_p(1+\rho_2)} = \theta \cdot \overline{\Lambda_p(1+\rho_1)}$ generate the rank-2 elementary abelian p-group $\overline{\Lambda_p(R_0)}$. Hence, θ lies in $\boldsymbol{\mu}_{p^2-1}$ if and only if $\overline{\Lambda_p(R_0)}$ is a vector space over $\mathbb{F}_{p^2}$, which holds if and only if $\Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-b+1}$ is a $\mathbb{Z}_{p^2}$-module. The equivalence of statements 3 and

4 follows from Theorem 3.1. To prove the equivalence of statements 2 and 3 we observe that if $\Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-b+1}$ is a $\mathbb{Z}_{p^2}$-module then it follows from Corollary 4.2 that

$$\Lambda_p\big(\big(R_0 \cdot U_K^{\frac{pe}{p-1}-b+1}\big)^{\perp} \cap U_K^b\big) = \Lambda_p\big(H \cap U_K^b\big)$$

is a $\mathbb{Z}_{p^2}$-module. Conversely, if $\Lambda_p(H \cap U_K^b)$ is a $\mathbb{Z}_{p^2}$-module then it follows from Corollary 4.2 that

$$\begin{aligned}\Lambda_p\big(\big(H \cap U_K^b\big)^{\perp} \cap U_K^{\frac{pe}{p-1}-b}\big) &= \Lambda_p\big(R_0 \cdot U_K^{\frac{pe}{p-1}-b+1}\big) \\ &= \Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-b+1}\end{aligned}$$

is a $\mathbb{Z}_{p^2}$-module. □

For the rest of this paper we restrict our attention to extensions L/K which satisfy the conditions of Lemma 4.3. Our goal is to compute b_* in terms of i_1 for this class of extensions. The following proposition will allow us to make a connection between $\Lambda_p(R_0)$ and the definition of s.

Proposition 4.4. *Let L/K be an extension which satisfies the conditions of Lemma 4.3, and let i satisfy $1 \leqslant i \leqslant p(\frac{pe}{p-1} - b)$ and $i \leqslant \frac{pe}{p-1} - \lfloor \frac{b}{p} \rfloor$. Then $(1+\rho_1)^{[\theta]} \in R_0 \cdot U_K^i$ if and only if $\Lambda_p(R_0) + \mathcal{M}_K^i$ is a $\mathbb{Z}_{p^2}$-module.*

Proof. If $i \leqslant \frac{pe}{p-1} - b$ then both statements are certainly true, so we assume $i > \frac{pe}{p-1} - b$. If $\Lambda_p(R_0) + \mathcal{M}_K^i$ is a $\mathbb{Z}_{p^2}$-module then it follows from Proposition 2.2 that $(1+\rho_1)^{[\theta]} \in R_0 \cdot U_K^i$. Conversely, suppose that $(1+\rho_1)^{[\theta]} \in R_0 \cdot U_K^i$. Thanks to the upper bounds on i, the hypotheses of Proposition 2.8 are satisfied with $j = \frac{pe}{p-1} - b$. It follows that $\Lambda_p((K^\times)^p \cap U_K^{\frac{pe}{p-1}-b}) + \mathcal{M}_K^i$ is an $\mathcal{O}_{K_0}$-module, and hence a $\mathbb{Z}_{p^2}$-module. By Proposition 2.2 we have $\theta \cdot \Lambda_p(1+\rho_1) \in \Lambda_p(R_0) + \mathcal{M}_K^i$. Therefore the rank-2 elementary abelian p-group

$$\big(\Lambda_p(R_0) + \mathcal{M}_K^i\big)/\big(\Lambda_p\big(\big(K^\times\big)^p \cap U_K^{\frac{pe}{p-1}-b}\big) + \mathcal{M}_K^i\big) \tag{4.5}$$

is generated by the cosets represented by $\Lambda_p(1+\rho_1)$ and $\theta \cdot \Lambda_p(1+\rho_1)$. Since $\theta \in \boldsymbol{\mu}_{p^2-1} \smallsetminus \boldsymbol{\mu}_{p-1}$, it follows that (4.5) is a vector space over $\mathbb{F}_{p^2}$. We conclude that $\Lambda_p(R_0) + \mathcal{M}_K^i$ is a $\mathbb{Z}_{p^2}$-module. □

We now reformulate the Byott–Elder formula for b_* in terms of $\Lambda_p(R_0)$.

Theorem 4.5. *Let L/K be an extension which satisfies the conditions of Lemma 4.3, let R be the subgroup of $K^\times$ that corresponds to L/K under Kummer theory, and set*

$R_0 = R \cap U_K^{\frac{pe}{p-1}-b}$. *Let* $s' \leqslant \frac{pe}{p-1}$ *be maximum such that* $\Lambda_p(R_0) + \mathcal{M}_K^{s'}$ *is a* $\mathbb{Z}_{p^2}$*-module and set* $t' = \frac{pe}{p-1} - s'$. *Then*

$$b_* = pb - \max\{pt' - b, (p^2-1)b - p^2e, 0\}. \tag{4.6}$$

Proof. Recall that $t = \frac{pe}{p-1} - s$, where s is the smallest nonnegative integer such that $(1+\rho_1)^{[\theta]} \in R_0 \cdot U_K^s$. Set

$$M = \max\{pt - b, (p^2-1)b - p^2e, 0\}$$
$$M' = \max\{pt' - b, (p^2-1)b - p^2e, 0\}.$$

By (4.4) we have $b_* = pb - M$. Therefore, to prove the theorem it suffices to show that $M' = M$. We divide the proof into three cases, depending on the value of M.

If $M = (p^2-1)b - p^2e$ then $t \leqslant p(b-e)$, and hence $(1+\rho_1)^{[\theta]} \in R_0 \cdot U_K^{\frac{pe}{p-1}-p(b-e)}$. Since $(p^2-1)b - p^2e \geqslant 0$ we have

$$p\left(\frac{pe}{p-1} - b\right) = \frac{pe}{p-1} - p(b-e) \leqslant \frac{pe}{p-1} - \left\lfloor \frac{b}{p} \right\rfloor.$$

Therefore, by Proposition 4.4 we see that $\Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-p(b-e)}$ is a $\mathbb{Z}_{p^2}$-module. Hence $t' \leqslant p(b-e)$, so $M' = M$ in this case.

If $M = 0$ then $t \leqslant \lfloor \frac{b}{p} \rfloor$ and hence $(1+\rho_1)^{[\theta]} \in R_0 \cdot U_K^{\frac{pe}{p-1}-\lfloor \frac{b}{p} \rfloor}$. Since $(p^2-1)b - p^2e \leqslant 0$ we have $p(\frac{pe}{p-1} - b) \geqslant \frac{pe}{p-1} - \lfloor \frac{b}{p} \rfloor$. Therefore, by Proposition 4.4 we see that $\Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-\lfloor \frac{b}{p} \rfloor}$ is a $\mathbb{Z}_{p^2}$-module. Hence $t' \leqslant \lfloor \frac{b}{p} \rfloor$, so $pt' \leqslant b$. It follows that $M' = M$ in this case.

If $M = pt - b > \max\{(p^2-1)b - p^2e, 0\}$ then $t > p(b-e)$ and $t > \frac{b}{p}$. Hence $s < p(\frac{pe}{p-1} - b)$ and $s < \frac{pe}{p-1} - \lfloor \frac{b}{p} \rfloor$. Since $(1+\rho_1)^{[\theta]} \in R_0 \cdot U_K^s$ and $(1+\rho_1)^{[\theta]} \notin R_0 \cdot U_K^{s+1}$, it follows from Proposition 4.4 that $\Lambda_p(R_0) + \mathcal{M}_K^s$ is a $\mathbb{Z}_{p^2}$-module, but $\Lambda_p(R_0) + \mathcal{M}_K^{s+1}$ is not. Therefore $s' = s$, so $M' = M$ in this case as well. $\square$

Now that we have formulas for computing b_* and i_1 in terms of $\Lambda_p(R_0)$, we can determine the relationship between these two invariants.

Theorem 4.6. *Let* $p > 2$ *and let* K *be a finite extension of* $\mathbb{Q}_p$ *which contains a primitive pth root of unity. Let* L/K *be a totally ramified* $(\mathbb{Z}/p\mathbb{Z})^2$*-extension with a single ramification break* b*. Assume that the index of inseparability* i_1 *of* L/K *is not equal to* $p^2b - pb$*. Then the refined ramification break* b_* *of* L/K *is given by* $b_* = i_1 - p^2b + pb + b$.

Proof. As above we let H denote the subgroup of $K^\times$ that corresponds to the extension L/K under class field theory. By Theorem 3.1 we have

$$i_1 = \min\{p^2b - pk, p^2e, p^2b - b\}, \tag{4.7}$$

where k is the smallest nonnegative integer such that $\Lambda_p(H \cap U_K^{k+1})$ is a $\mathbb{Z}_{p^2}$-module. Let R be the subgroup of $K^\times$ that corresponds to L/K under Kummer theory and set $R_0 = R \cap U_K^{\frac{pe}{p-1}-b}$. Recall that R is equal to the orthogonal complement $H^\perp$ of H with respect to the Kummer pairing $\langle\, , \rangle_p$. In addition, since $R = R_0 \cdot (K^\times)^p$ we have $R_0^\perp = R^\perp = H$. As in Theorem 4.5 we let t' be the smallest nonnegative integer such that $\Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-t'}$ is a $\mathbb{Z}_{p^2}$-module.

Suppose $i_1 = p^2 b - b$. Then

$$\begin{aligned}\Lambda_p\big(\big(H \cap U_K^{\lfloor \frac{b}{p} \rfloor+1}\big)^\perp \cap U_K^{\frac{pe}{p-1}-b}\big) &= \Lambda_p\big(\big(R \cdot U_K^{\frac{pe}{p-1}-\lfloor \frac{b}{p} \rfloor}\big) \cap U_K^{\frac{pe}{p-1}-b}\big)\\ &= \Lambda_p\big(R_0 \cdot U_K^{\frac{pe}{p-1}-\lfloor \frac{b}{p} \rfloor}\big).\end{aligned}$$

Since $p(\frac{pe}{p-1} - b) \geqslant \frac{pe}{p-1} - \lfloor \frac{b}{p} \rfloor$, it follows from Corollary 2.6 that

$$\Lambda_p\big(\big(H \cap U_K^{\lfloor \frac{b}{p} \rfloor+1}\big)^\perp \cap U_K^{\frac{pe}{p-1}-b}\big) = \Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-\lfloor \frac{b}{p} \rfloor}. \tag{4.8}$$

Since $\lfloor \frac{b}{p} \rfloor + 1 > \frac{b}{p} \geqslant p(b-e)$, we have

$$\begin{aligned}\left(\left\lfloor \frac{b}{p} \right\rfloor + 1\right) + p\left(\frac{pe}{p-1} - b\right) &> \frac{pe}{p-1}\\ p\left(\left\lfloor \frac{b}{p} \right\rfloor + 1\right) + \left(\frac{pe}{p-1} - b\right) &> \frac{pe}{p-1}.\end{aligned}$$

Therefore, by (4.8) and Corollary 4.2 with $A = H \cap U_K^{\lfloor \frac{b}{p} \rfloor+1}$, $i = \lfloor \frac{b}{p} \rfloor + 1$, and $j = \frac{pe}{p-1} - b$ we see that $\Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-\lfloor \frac{b}{p} \rfloor}$ is a $\mathbb{Z}_{p^2}$-module. Hence $t' \leqslant \lfloor \frac{b}{p} \rfloor$. Since $(p^2-1)b - p^2 e \leqslant 0$, it follows from Theorem 4.5 that $b_* = pb$ in this case.

Suppose $i_1 = p^2 e$. Then

$$\begin{aligned}\Lambda_p\big(\big(H \cap U_K^{p(b-e)+1}\big)^\perp \cap U_K^{\frac{pe}{p-1}-b}\big) &= \Lambda_p\big(\big(R \cdot U_K^{\frac{pe}{p-1}-p(b-e)}\big) \cap U_K^{\frac{pe}{p-1}-b}\big)\\ &= \Lambda_p\big(R_0 \cdot U_K^{\frac{pe}{p-1}-p(b-e)}\big).\end{aligned}$$

Since $b > p(b-e)$ and $p(\frac{pe}{p-1} - b) = \frac{pe}{p-1} - p(b-e)$ it follows from Corollary 2.6 that

$$\Lambda_p\big(\big(H \cap U_K^{p(b-e)+1}\big)^\perp \cap U_K^{\frac{pe}{p-1}-b}\big) = \Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-p(b-e)}. \tag{4.9}$$

Since $p^2 b - b \geqslant p^2 e$ we have

$$\begin{aligned}\big(p(b-e) + 1\big) + p\left(\frac{pe}{p-1} - b\right) &> \frac{pe}{p-1}\\ p\big(p(b-e) + 1\big) + \left(\frac{pe}{p-1} - b\right) &> \frac{pe}{p-1}.\end{aligned}$$

Therefore, it follows from (4.9) and Corollary 4.2 with $A = H \cap U_K^{p(b-e)+1}$, $i = p(b-e)+1$, and $j = \frac{pe}{p-1} - b$ that $\Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-p(b-e)}$ is a $\mathbb{Z}_{p^2}$-module. Hence $t' \leqslant p(b-e)$. Since $(p^2-1)b - p^2e \geqslant 0$, it follows from Theorem 4.5 that $b_* = p^2(e-b) + pb + b$ in this case.

Suppose $i_1 = p^2b - pk < \min\{p^2b - b, p^2e\}$. Since $H \supset U_K^{b+1}$ we have $k \leqslant b$, so $R_0 \cdot U_K^{\frac{pe}{p-1}-k}$ is contained in $U_K^{\frac{pe}{p-1}-b}$. Hence

$$\begin{aligned}\Lambda_p\big(\big(H \cap U_K^{k+1}\big)^\perp \cap U_K^{\frac{pe}{p-1}-b}\big) &= \Lambda_p\big(\big(R \cdot U_K^{\frac{pe}{p-1}-k}\big) \cap U_K^{\frac{pe}{p-1}-b}\big) \\ &= \Lambda_p\big(R_0 \cdot U_K^{\frac{pe}{p-1}-k}\big).\end{aligned}$$

Since $k > p(b-e)$ we have $p(\frac{pe}{p-1} - b) > \frac{pe}{p-1} - k$. Therefore, by Corollary 2.6 we get

$$\Lambda_p\big(\big(H \cap U_K^{k+1}\big)^\perp \cap U_K^{\frac{pe}{p-1}-b}\big) = \Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-k}. \tag{4.10}$$

It follows from the inequalities $k > p(b-e)$ and $pk > b$ that

$$\begin{aligned} k + p\left(\frac{pe}{p-1} - b\right) &> \frac{pe}{p-1} \\ pk + \left(\frac{pe}{p-1} - b\right) &> \frac{pe}{p-1}. \end{aligned}$$

Therefore, by (4.10) and Corollary 4.2 with $A = H \cap U_K^{k+1}$, $i = k+1$, and $j = \frac{pe}{p-1} - b$ we see that $\Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-k}$ is a $\mathbb{Z}_{p^2}$-module.

Suppose that $\Lambda_p(R_0) + \mathcal{M}_K^{\frac{pe}{p-1}-k+1}$ is also a $\mathbb{Z}_{p^2}$-module. Then, by Corollary 4.2 with $A = R_0 \cdot U_K^{\frac{pe}{p-1}-k+1}$, $i = \frac{pe}{p-1} - b$, and $j = k$ we see that

$$\begin{aligned}\Lambda_p\big(\big(R_0 \cdot U_K^{\frac{pe}{p-1}-k+1}\big)^\perp \cap U_K^k\big) &= \Lambda_p\big(H \cap \big(K^\times\big)^p U_K^k \cap U_K^k\big) \\ &= \Lambda_p\big(H \cap U_K^k\big)\end{aligned}$$

is a $\mathbb{Z}_{p^2}$-module. Since $k \geqslant 1$ this contradicts the definition of k. Hence $\Lambda_p(R_0 \cdot U_K^{\frac{pe}{p-1}-k+1})$ is not a $\mathbb{Z}_{p^2}$-module, so $t' = k$. Since $pk - b > \max\{(p^2-1)b - p^2e, 0\}$ we get $b_* = pb - pk + b$ by Theorem 4.5. By comparing our formulas for b_* with (4.7) we find that $b_* = i_1 - p^2b + pb + b$ in all three cases. □

Remark 4.7. If $i_1 = p^2b - pb$ then b_* can take any of the values allowed by Theorem 5 in [2]. On the other hand, for a given b_* we have either $i_1 = p^2b - pb$ or $i_1 = b_* + p^2b - pb - b$.

References

[1] N.P. Byott, G.G. Elder, New ramification breaks and additive Galois structure, J. Théor. Nombres Bordeaux 17 (2005) 87–107.
[2] N.P. Byott, G.G. Elder, On the necessity of new ramification breaks, J. Number Theory 129 (2009) 84–101.
[3] C.S. Dalawat, Further remarks on local discriminants, J. Ramanujan Math. Soc. 25 (2010) 393–417.
[4] M. Demazure, Lectures on p-Divisible Groups, Lecture Notes in Math., vol. 302, 1972.
[5] I.B. Fesenko, S.V. Vostokov, Local Fields and Their Extensions, Amer. Math. Soc., Providence, RI, 2002.
[6] M. Fried, Arithmetical properties of function fields II. The generalized Schur problem, Acta Arith. 25 (1973/1974) 225–258.
[7] V. Heiermann, De nouveaux invariants numériques pour les extensions totalement ramifiées de corps locaux, J. Number Theory 59 (1996) 159–202.
[8] K. Keating, Indices of inseparability for elementary abelian p-extensions, J. Number Theory 136 (2014) 233–251.
[9] S.V. Vostokov, On the explicit form of the reciprocity law, Dokl. Akad. Nauk SSSR 238 (6) (1978) 1276–1278 (in Russian); translated in Soviet Math. Dokl. 19 (1) (1978) 198–201.