Indices of Inseparability and New Ramification Breaks

Kevin Keating
Department of Mathematics
University of Florida

May 30, 2013

Notation

$[K : \mathbb{Q}_p] = n = ef$ with $p > 2$

$T/\mathbb{Q}_p =$ maximum unramified subextension of $K/\mathbb{Q}_p$

$e = [K : T]$; $f = [T : \mathbb{Q}_p]$

$K^{ab}/K =$ maximal abelian extension of K

$L/K =$ totally ramified subextension of K^{ab}/K

$G = \mathrm{Gal}(L/K) \cong C_p \times C_p$

$\mathcal{O}_K \supset \mathcal{M}_K = \pi_K \mathcal{O}_K$; $\mathcal{O}_K/\mathcal{M}_K \cong \mathbb{F}_q$ with $q = p^f$

$U_K^c = 1 + \mathcal{M}_K^c$ for $c \geq 1$

$v_K(K^\times) = \mathbb{Z}$

Similar definitions apply for T and L

Ramification Breaks

For $\tau \in G$ define $i(\tau) = v_L((\tau - 1)\pi_L) - 1$.

For $a \geq 0$, $G_a = \{\tau \in G : i(\tau) \geq a\}$ is a subgroup of G.

Say $a \in \mathbb{N}$ is a ramification break of L/K if $G_a \neq G_{a+1}$.

Since $G \cong C_p \times C_p$ we see that L/K has either 1 or 2 ramification breaks. When there is only one break we want to replace the "missing" ramification data.

From now on we assume that L/K has a single ramification break $b > 0$. Thus for every $\tau \in G$ with $\tau \neq 1$ we have $i(\tau) = b$.

Indices of Inseparability (Fried, Heiermann)

Let π_K, π_L be uniformizers for K, L.

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 $0 \leq j \leq 2$ set

$$i_j^* = \min\{h \geq 0 : c_h \neq 0,\ v_p(h+p^2) \leq j\}$$

$$i_j = \min\{i_{j'}^* + p^2 e \cdot (j' - j) : j \leq j' \leq 2\}.$$

Then

1. i_j^* may depend on the choice of π_L, but i_j does not.
2. $0 = i_2 \leq i_1 \leq i_0$.

Canonical Definition of i_j

For $d \geq 0$ and $0 \leq j \leq 2$ set

$$B_d = \mathcal{O}_L/\mathcal{M}_L^{p^2+d}$$
$$A_d = (\mathcal{O}_K + \mathcal{M}_L^{p^2+d})/\mathcal{M}_L^{p^2+d}$$
$$B_d[\epsilon_j] = B_d[\epsilon]/(\epsilon^{p^{j+1}})$$

Then $\epsilon_j = \epsilon + (\epsilon^{p^{j+1}})$ satisfies $\epsilon_j^{p^{j+1}} = 0$.

Theorem: i_j is equal to the largest $d \geq 0$ such that there exists an A_d-algebra homomorphism $s : B_d \to B_d[\epsilon_j]$ satisfying:

1. $s \equiv \mathrm{id}_{B_d} \pmod{\pi_L \epsilon_j}$
2. $s \not\equiv \mathrm{id}_{B_d} \pmod{\pi_L \epsilon_j \cdot (\pi_L, \epsilon_j)}$

Relation with Ramification Data

Theorem (Fried, Heiermann): For $x \geq 0$,

$$\phi_{L/K}(x) = \frac{1}{p^2} \cdot \min\{i_j + p^j x : 0 \leq j \leq 2\}.$$

Hence if L/K has 2 distinct ramification breaks then $\phi_{L/K}$ determines i_0, i_1, and i_2.

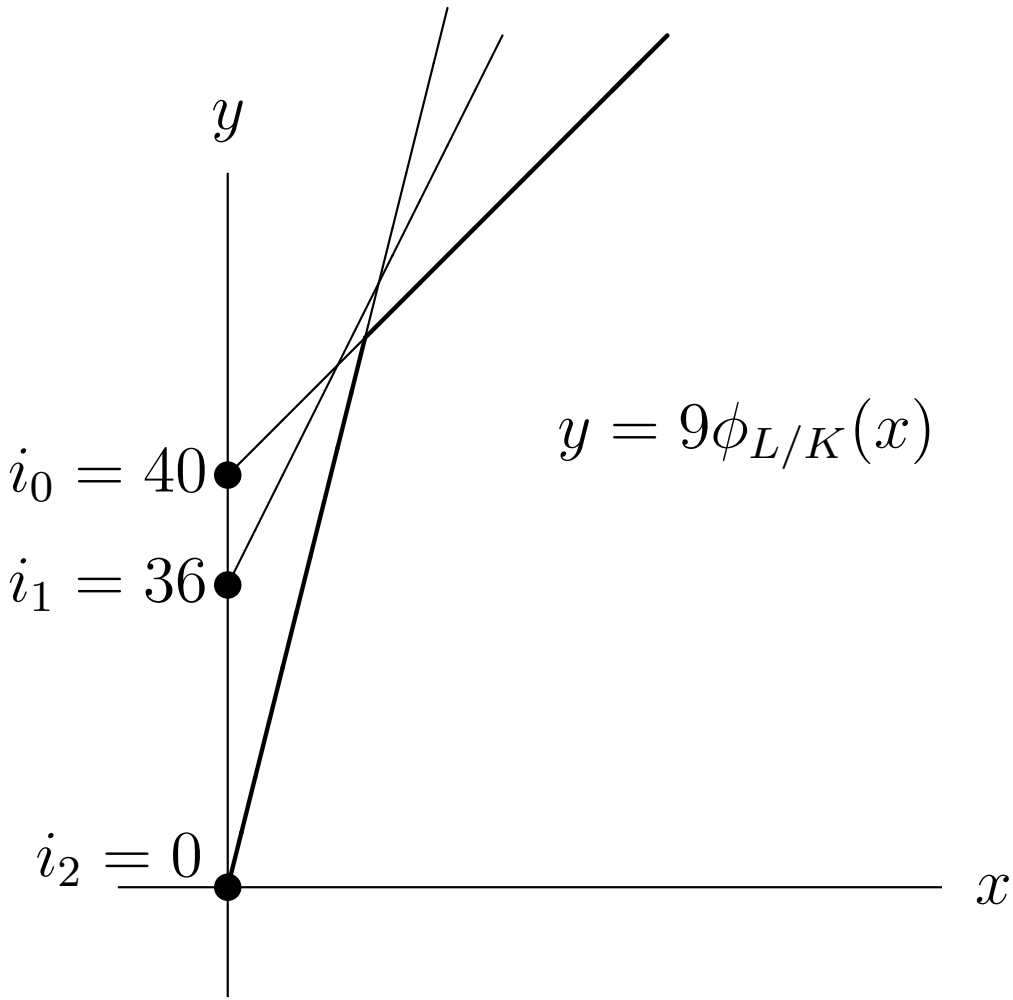
Example: Let K be an extension of $\mathbb{Q}_3$ of degree 8, with $e = 4$ and $f = 2$. Let L/K be a $(C_3 \times C_3)$-extension such that

$$\pi_K = \pi_L^9(1 + \pi_L^{18} + \pi_L^{27} - \pi_L^{39} - \pi_L^{40} + \dots).$$

Then $i_2 = i_2^* = 0$, $i_1^* = 39$, $i_1 = 36$, and $i_0 = i_0^* = 40$.

The Hasse-Herbrand function $\phi_{L/K}$ can be deduced from this data:

Graph of $\phi_{L/K}$



Truncated Exponentiation

For $\psi(X) \in XK[[X]]$, $\alpha \in K$, define

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

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

Byott and Elder defined "truncated exponentiation" by

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

Let $\alpha \in \mathcal{O}_K$. Then $g_\alpha(X) = (1+X)^{[\alpha]}$ lies in $\mathcal{O}_K[X]$.

For $c \in K$ define $c^{[\alpha]} = g_\alpha(c-1)$.
For $\tau \in G$ define $\tau^{[\alpha]} = g_\alpha(\tau - 1)$.

Computing i_j in Terms of Class Field Theory

Let $H = \mathrm{N}_{L/K}(L^\times)$ be the subgroup of $K^\times$ which corresponds to L/K under CFT.

Definition: Say $A \leq U_K^1$ is "$\boldsymbol{\mu}_{p^2-1}$-invariant" if

1. f is even, so that $K^\times$ contains $\boldsymbol{\mu}_{p^2-1} \cong C_{p^2-1}$, and
2. $u^{[\alpha]} \in A$ for every $u \in A$ and $\alpha \in \boldsymbol{\mu}_{p^2-1}$.

Theorem: If f is odd set $k = b$. Otherwise, let k be minimum such that $H \cap U_K^{k+1}$ is $\boldsymbol{\mu}_{p^2-1}$-invariant. Then $i_0 = p^2 b - b$, $i_2 = 0$, and

$$\begin{aligned} i_1 &= \min\{p^2 e,\ p^2 b - pk,\ p^2 b - b\} \\ &= (p^2-1)b - \max\{(p^2-1)b - p^2 e,\ pk - b,\ 0\}. \end{aligned}$$

Idea of the Proof

Let the minimum polynomial for π_L over K be

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

Using the formula

$$-a_{p^2} = \pi_L^{p^2} + a_1 \pi_L^{p^2-1} + \cdots + a_{p^2-1} \pi_L$$

one can compute i_1 in terms of $v_K(a_i)$.

One can also obtain explicit generators for

$$H \cap U_K^{k+1} = \mathrm{N}_{L/K}(U_L^{k+1})$$

in terms of the a_i. By comparing these we get the theorem.

Refined Ramification Breaks (Byott-Elder)

Write $G = \langle \gamma, \sigma \rangle$ and choose $\rho_0 \in L$ such that $v_L(\rho_0) = b$.

Then $b = v_L((\tau - 1)\rho_0) - v_L(\rho_0)$ for every $\tau \in G$ with $\tau \neq 1$.

There is $\omega \in \boldsymbol{\mu}_{q-1} \setminus \boldsymbol{\mu}_{p-1}$ such that

$$(\gamma - 1)\rho_0 \equiv -\omega(\sigma - 1)\rho_0 \pmod{\mathcal{M}_L^{2b+1}}.$$

Define

$$\Theta = \gamma\sigma^{[\omega]} \in \mathcal{O}_T[G]$$
$$b_* = v_L((\Theta - 1)\rho_0) - v_L(\rho_0).$$

Then $b_* > b$ does not depend on the choices of γ, σ, or ρ_0.

The Kummer Pairing

Assume from now on that K contains a primitive pth root of unity ζ_p.

The Kummer Pairing $\langle\ ,\ \rangle_p : K^\times \times K^\times \to \boldsymbol{\mu}_p$ is defined by

$$\langle \alpha, \beta \rangle_p = \frac{\sigma_\beta(\alpha^{1/p})}{\alpha^{1/p}},$$

where $\sigma_\beta \in \mathrm{Gal}(K^{ab}/K)$ corresponds to β under CFT.

$\langle\ ,\ \rangle_p$ is $\mathbb{Z}$-bilinear and skew-symmetric, with kernel $(K^\times)^p$.

For $1 \leq i \leq \frac{pe}{p-1}$ the orthogonal complement of U_K^i with respect to $\langle\ ,\ \rangle_p$ is

$$(U_K^i)^\perp = (K^\times)^p \cdot U_K^{\frac{pe}{p-1}-i+1}.$$

Subgroups of $K^\times$ that Correspond to L/K

Recall that $H = \mathrm{N}_{L/K}(L^\times)$ corresponds to L/K under CFT.

Let $R \leq K^\times$ correspond to L/K under Kummer theory. Then

1. $H \supset (K^\times)^p$; $R \supset (K^\times)^p$
2. $R/(K^\times)^p \cong K^\times/H \cong C_p \times C_p$.
3. $R = H^\perp$; $H = R^\perp$

Set $R_0 = R \cap U_K^{\frac{pe}{p-1}-b}$. Then

1. $R = R_0 \cdot (K^\times)^p$
2. The image $\overline{R}_0$ of R_0 in $U_K/U_K^{\frac{pe}{p-1}-b+1}$ is isomorphic to $C_p \times C_p$.

b_* revisited

Let $1+\delta_1, 1+\delta_2 \in R_0$ generate $\overline{R}_0$. Then

$$v_K(\delta_1) = v_K(\delta_2) = \frac{pe}{p-1} - b.$$

Hence there is $\eta \in \boldsymbol{\mu}_{q-1} \smallsetminus \boldsymbol{\mu}_{p-1}$ such that

$$\delta_2/\delta_1 \equiv \eta \pmod{\mathcal{M}_K}$$
$$(1+\delta_1)^{[\eta]} \equiv 1+\delta_2 \pmod{\mathcal{M}_K^{\frac{pe}{p-1}-b+1}}.$$

Theorem (Byott-Elder): Let $1 \le s \le \frac{pe}{p-1}$ be maximum such that $(1+\delta_1)^{[\eta]} \in R_0 \cdot U_K^s$, and set $t = \frac{pe}{p-1} - s$. Then

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

Compare $i_1 = (p^2-1)b - \max\{(p^2-1)b - p^2e,\ pk - b,\ 0\}$.

Orthogonal Complements and $\boldsymbol{\mu}_{p^2-1}$-invariance

Theorem: 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 $c \in \mathcal{O}_T$. Then

$$\langle \alpha^{[c]}, \beta \rangle_p = \langle \alpha, \beta^{[c]} \rangle_p.$$

Corollary: Let i, j be positive integers such that $i + pj > \frac{pe}{p-1}$ and $pi + j > \frac{pe}{p-1}$. Let A be a $\boldsymbol{\mu}_{p^2-1}$-invariant subgroup of U_K^i which contains U_K^{pi}. Then $A^\perp \cap U_K^j$ is $\boldsymbol{\mu}_{p^2-1}$-invariant.

The proof of the theorem is based on Vostokov's formula for computing $\langle \alpha, \beta \rangle_p$.

Relation Between b_* and i_1

Theorem: Assume that $i_1 > p^2 b - pb$. Then

1. f is even,
2. $\eta \in \boldsymbol{\mu}_{p^2-1}$,
3. s is the largest integer $\leq \frac{pe}{p-1}$ such that $R_0 \cdot U_K^s$ is $\boldsymbol{\mu}_{p^2-1}$-invariant.

Theorem: If $i_1 > p^2 b - pb$ then

$$b_* = i_1 - p^2 b + pb + b.$$

Remark: In general we have $p^2 b - pb \leq i_1 \leq p^2 b - b$. If $f > 2$ then all realizable second refined breaks b_* can be realized with $i_1 = p^2 b - pb$.

Hence i_1 and b_* together give more information about L/K than either number alone.

Sketch of the Proof

Let $b/p < m < b$ and $m > pb - pe$. Then

$$
\begin{aligned}
i_1 \geq p^2 b - pm &\Leftrightarrow H \cap U_K^{m+1} \text{ is } \boldsymbol{\mu}_{p^2-1}\text{-invariant} \\
&\Leftrightarrow (H \cap U_K^{m+1})^{\perp} \cap U_K^{\frac{pe}{p-1}-b} \text{ is } \boldsymbol{\mu}_{p^2-1}\text{-invariant} \\
&\Leftrightarrow R_0 \cdot U_K^{\frac{pe}{p-1}-m} \text{ is } \boldsymbol{\mu}_{p^2-1}\text{-invariant} \\
&\Leftrightarrow s \leq \frac{pe}{p-1} - m \\
&\Leftrightarrow b_* \geq pb + b - pm.
\end{aligned}
$$

Vostokov's Formula: A Power Series Field

Definition: Let $T\{\{X\}\}$ denote the set of power series $\sum_{n=-\infty}^{\infty} a_n X^n$, with $a_n \in T$ satisfying

1. $\lim_{n \to -\infty} v_T(a_n) = \infty$
2. There exists $m \in \mathbb{Z}$ such that $v_T(a_n) \geq m$ for all $n \in \mathbb{Z}$.

$T\{\{X\}\}$ certainly has the operation of addition.

The conditions on the coefficients imply that the natural multiplication on $T\{\{X\}\}$ is also well-defined.

These operations make $T\{\{X\}\}$ a field.

Let $\mathcal{O}_T\{\{X\}\}$ denote the subring of $T\{\{X\}\}$ consisting of power series with coefficients in $\mathcal{O}_T$.

Elements of $\mathcal{O}_K$ as Power Series

For each $\alpha \in \mathcal{O}_K$ choose $\tilde{\alpha}(X) \in \mathcal{O}_T[[X]]$ so that $\tilde{\alpha}(\pi_K) = \alpha$.

Let $\phi : T \to T$ be the p-Frobenius map. For $\alpha \in \mathcal{O}_K$ define

$$\tilde{\alpha}^{\Delta}(X) = \tilde{\alpha}^{\phi}(X^p)$$

$$I(\tilde{\alpha}) = p^{-1} \log(\tilde{\alpha}^p / \tilde{\alpha}^{\Delta}).$$

Also define

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

Then $\Phi_{\alpha,\beta}(X) \in \mathcal{O}_T[[X]]$.

Computing the Kummer Pairing

Let $s(X) = \tilde{\zeta}_p(X)^p - 1$. Then

1. $s(X) \in \mathcal{O}_T\{\{X\}\}^\times$.
2. There are $\kappa(X) \in \mathcal{O}_T[[X]]$ and $\lambda(X) \in \mathcal{O}_T\{\{X\}\}$ with

$$\frac{1}{s(X)} = X^{-\frac{pe}{p-1}}\kappa(X) + p\lambda(X).$$

Let $\mathrm{Res}(\psi)$ denote the coefficient of X^{-1} in $\psi(X) \in T\{\{X\}\}$.

Theorem (Vostokov): Let $p > 2$. Then

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

Hence to prove $\langle \alpha^{[c]}, \beta \rangle_p = \langle \alpha, \beta^{[c]} \rangle_p$ it suffices to show that

$$\mathrm{Res}(\Phi_{\alpha^{[c]},\beta}/s) \equiv \mathrm{Res}(\Phi_{\alpha,\beta^{[c]}}/s) \pmod{p}.$$

The Artin-Hasse Exponential Series

$\mu =$ Möbius function; $\exp(X) =$ exponential series.

$$\begin{aligned} E_p(X) &= \prod_{p \nmid c} (1 - X^c)^{-\mu(c)/c} \\ &= \exp\left(X + \tfrac{1}{p}X^p + \tfrac{1}{p^2}X^{p^2} + \cdots\right) \\ &\in \mathbb{Z}_{(p)}[[X]]. \end{aligned}$$

By the $\mathbb{Z}$-bilinearity and continuity of $\langle\ ,\ \rangle_p$ we can assume

$$\begin{aligned} \alpha &= E_p(u\pi_K^g), \quad \tilde{\alpha}(X) = E_p(uX^g) \\ \beta &= E_p(v\pi_K^h), \quad \tilde{\beta}(X) = E_p(vX^h) \end{aligned}$$

with $u, v \in \boldsymbol{\mu}_{q-1}$, $g \geq i$, and $h \geq j$.

Completing the Proof

It follows that

$$\begin{aligned}
\Phi_{\alpha,\beta}(X) &\equiv guvX^{g+h-1} && (\text{mod } X^{\frac{pe}{p-1}}) \\
\Phi_{\alpha^{[c]},\beta}(X) &\equiv g(cu)vX^{g+h-1} && (\text{mod } X^{\frac{pe}{p-1}}) \\
\Phi_{\alpha,\beta^{[c]}}(X) &\equiv gu(cv)X^{g+h-1} && (\text{mod } X^{\frac{pe}{p-1}}).
\end{aligned}$$

Using the formula for $1/s(X)$ we deduce that

$$\frac{\Phi_{\alpha^{[c]},\beta}(X) - \Phi_{\alpha,\beta^{[c]}}(X)}{s(X)} = \mu(X) + p\nu(X)$$

for some $\mu(X) \in \mathcal{O}_T[[X]]$ and $\nu(X) \in \mathcal{O}_T\{\{X\}\}$. Hence

$$\text{Res}\left(\frac{\Phi_{\alpha^{[c]},\beta}(X)}{s(X)}\right) \equiv \text{Res}\left(\frac{\Phi_{\alpha,\beta^{[c]}}(X)}{s(X)}\right) \quad (\text{mod } \mathcal{M}_T).$$