Examples: Refined ramification under a Galois scaffold

Griff Elder

University of Nebraska at Omaha

May 23, 2016

Setting: local fields

p is a fixed prime integer

K is a local field, complete with respect to a discrete valuation v_K, normalized so that $v_K(K^\times) = \mathbb{Z}$

Then K has

- a valuation ring $\mathcal{O}_K = \{x \in K \ : \ v_K(x) \geq 0\}$,
- uniformizers π_K such that $v_K(\pi_K) = 1$,
- a unique maximal ideal $\mathcal{M}_K = \{x \in K \ : \ v_K(x) > 0\}$, and
- a residue field $\kappa = \mathcal{O}_K/\mathcal{M}_K$.

Assume that κ is perfect, and $\mathrm{char}(\kappa) = p$.

So if κ is finite, then either

- K is a finite extension of $\mathbb{Q}_p$ $(\mathrm{char}(K) = 0)$; or
- $K = \kappa((t))$ with $v_K(t) = 1$ $(\mathrm{char}(K) = p)$.

flaw in ramification

Let L/K be a totally ramified, Galois extension of degree p^n with Galois group and ramification filtration of normal subgroups,

$$G_i = \{\sigma \in \mathrm{Gal}(L/K) : (\sigma - 1)\pi_L \in P_L^{i+1}\}.$$

Then for each i, G_i/G_{i+1} is a (possibly trivial) elementary abelian p-group.

Integers b such that $G_b \neq G_{b+1}$ are called ramification breaks/numbers.

Ramification breaks encode valuable information. Clearly we can't have more than n where $|\mathrm{Gal}(L/K)| = p^n$. If we have fewer, information is lacking.

How to repair this deficiency?

Two fixes: Degrees of inseparability & Refined ramification

and refined ramification comes in two flavors.

Two flavors: the main difference

In both cases, we focus on the subextension where "information is lacking" – where the Galois group is $G = G_b/G_{b+1}$ and $|G| > p$. There we find ourselves interested in measuring the increase in valuation that results from application of an element $\gamma \in \kappa[G]$.

Version VC: Measured on elements of **V**aluation **C**riterion for a normal basis generator: Let $\rho \in L$ satisfy $v_L(\rho) = b$, then

$$v_L(\gamma\rho) - v_L(\rho).$$

Version SS: Take the **S**mallest **S**hift:

$$\hat{v}_L(\gamma) = \min\{v_L(\gamma x) - v_L(x) : x \in L^\times\}.$$

VC Benefit: There are n refined breaks for $|G| = p^n$.
VC Deficiency: Unless $n \leq 2$, there is no proof that refined breaks are independent of choice of element ρ.

SS Benefit: Value of refined breaks is independent of choices.
SS Deficiency: Unless $n \leq 2$, there is no proof that all lacking information is retrieved – namely that we get n refined breaks for $|G| = p^n$.

Henceforth we restrict our attention to totally ramified Galois extensions L/K with one break in their ramification filtration at b.

Conjecture 1: (Strong) Let $\rho \in L$ with $v_L(\rho) = b$. Let $\gamma \in \kappa[G]$, then for all $x \in L^\times$,

$$v_L(\gamma\rho) - v_L(\rho) \leq v_L(\gamma x) - v_L(x).$$

Conjecture 2: (Weak) Let $\rho, \rho' \in L$ with $v_L(\rho) = v_L(\rho') = b$. Let $\gamma \in \kappa[G]$. Then

$$v_L(\gamma\rho) = v_L(\gamma\rho').$$

Theorem. If the extension has degree p or p^2, or has a scaffold (of any tolerance/precision $\mathfrak{C} \geq 1$), Conjecture 1 holds.

Under Conjecture 1, the competing flavors of refined ramification agree.

Under Conjecture 2, the VC refined breaks are canonical – independent of choice of element $\rho \in L$ with $v_L(\rho) = b$.

Benefit of VC definition

Upper bounds from subextensions.

Proposition. Let K_n/K_0 be an elementary abelian extension of degree p^n with one ramification break at b with Galois group G_n. Let K_{n-1}/K_0 be a subextension of degree p^{n-1} with Galois group G_{n-1}.
Let $r_1 < r_2 < \cdots < r_n$ be the refined breaks measured on $\rho \in K_n$ satisfying $v_n(\rho) = b$. Let $\rho' = \mathrm{Tr}_{K_n/K_{n-1}}\rho \in K_{n-1}$. Observe that $v_{n-1}(\rho') = b$. Let $s_1 < s_2 < \cdots < s_{n-1}$ be the refined breaks for K_{n-1}/K_0 measured on $\rho' \in K_{n-1}$. Then for $2 \leq i \leq n$, we have

$$r_i \leq ps_{i-1}.$$

Proof. Associated with $r_1, r_2, \ldots, r_n$ are elements γ_i in the augmentation ideal I of $\kappa[G]$ such that $r_i = v_n(\gamma_i\rho) - v_n(\rho)$. In other words,

$$v_n(\gamma_i\rho) = b + r_i.$$

We view $\kappa[G]$ as vector space over κ under the usual scalar multiplication, ignoring κ-action via truncated powers.

Without loss of generality, $\gamma_1 = \sigma_n - 1$ where $\langle \sigma_n \rangle = \mathrm{Gal}(K_n/K_{n-1})$. Recall $G_n = \mathrm{Gal}(K_n/K_0)$, and $G_{n-1} = \mathrm{Gal}(K_{n-1}/K_0) \cong G/\langle \sigma_n \rangle$.

Using [Serre: Local Fields, V §3 Lemma 4]

$$v_{n-1}(\mathrm{Tr}_{K_n/K_{n-1}} \gamma_i \rho) = b + \left\lfloor \frac{p-1+r_i}{p} \right\rfloor .$$

Since G is abelian, $\mathrm{Tr}_{K_n/K_{n-1}} \gamma_i \rho = \overline{\gamma}_i \rho'$ where $\overline{\gamma}_i = \gamma_i \langle \sigma_n \rangle \in \kappa[G_{n-1}]$. Thus

$$v_{n-1}(\overline{\gamma}_i \rho') - v_{n-1}(\rho') = \left\lfloor \frac{p-1+r_i}{p} \right\rfloor . \tag{1}$$

Since the r_i are distinct, the elements $\{\gamma_i : 1 \leq i \leq n\}$ cannot be linearly dependent over κ. Thus they provide a κ-basis for $\kappa[G_n]$, which means that their image $\{\overline{\gamma}_i : 2 \leq i \leq n\}$ provides a κ-basis for $\kappa[G_{n-1}]$.

Associated with $s_1, s_2, \dots, s_{n-1}$ are elements γ_i' in the augmentation ideal of $\kappa[G_{n-1}]$ such that $v_{n-1}(\rho') + s_i = v_{n-1}(\gamma_i' \rho')$. Since the s_i are distinct, $\{\gamma_i' : 1 \leq i \leq n-1\}$ is a κ-basis for $\kappa[G_{n-1}]$. Thus for each $2 \leq j \leq n$,

$$\overline{\gamma}_j = \sum_{i=1}^{n-1} a_{i,j} \gamma_i', \text{ with } a_{i,j} \in \kappa.$$

$$\text{Recall } \overline{\gamma}_j = \sum_{i=1}^{n-1} a_{i,j}\gamma_i'. \text{ Notice at least one } a_{i,j} \neq 0.$$

Since $s_1 < s_2 < \ldots < s_{n-1}$ and using (1),

$$\left\lfloor \frac{p-1+r_j}{p} \right\rfloor = v_{n-1}(\overline{\gamma}_j\rho') - v_{n-1}(\rho') = \min\{s_i : a_{i,j} \neq 0\},$$

which is equivalent to

$$\min\{p(s_i - 1) : a_{i,j} \neq 0\} < r_j \leq \min\{ps_i : a_{i,j} \neq 0\}.$$

If there is a $2 \leq k \leq n$ such that $ps_{k-1} < r_k$, then for all $k \leq j \leq n$,

$$\overline{\gamma}_j = \sum_{i=k}^{n-1} a_{i,j}\gamma_i',$$

which means that $\{\overline{\gamma}_j : k \leq j \leq n\}$ can be expressed in terms of $\{\gamma_i' : k \leq i \leq n-1\}$. Thus $\{\overline{\gamma}_j : k \leq j \leq n\}$ is linearly dependent, contradicting the fact that $\{\overline{\gamma}_i : 2 \leq i \leq n\}$ is a κ-basis for $\kappa[G_{n-1}]$.

Example: Refined breaks p^3 with scaffold

Notation: $\wp(x) = x^p - x$. Truncated yth power $(1+x)^{[y]} = \sum_{i=0}^{p-1} \binom{y}{i} x^i$.

Let $p \nmid b > 0$, and $\beta \in K_0 = \kappa((t))$ with $v_0(\beta) = -b$.

Define $\wp(x_1) = \beta$. Choose $\omega_2, \omega_3 \in \kappa$ such that $\{1, \omega_2, \omega_3\}$ are linearly independent over $\mathbb{F}_p$, and $\alpha_2, \alpha_3 \in \mathcal{M}_0$. Set $\Omega_i = \omega_i + \alpha_i$, and define

$$\wp(x_i) = \Omega_i^{p^2} \beta, \ i = 2, 3.$$

Let $K_1 = K_0(x_1)$, $K_2 = K_0(x_1, x_2)$, $K_3 = K_0(x_1, x_2, x_3)$. Then K_3/K_0 is a C_p^3-extension with only one ramification break at b.

Set

$$\begin{aligned} X_1 &= x_1, \text{ then} & v_1(X_1) &= -b, \\ X_2 &= x_2 - \Omega_2^p x_1, \text{ then} & v_2(X_2) &= -b, \\ X_3 &= (x_3 - \Omega_3^p x_1) - \tfrac{\wp(\Omega_3)}{\wp(\Omega_2)}(x_2 - \Omega_2^p x_1), & v_3(X_3) &= -b. \end{aligned}$$

Define $\sigma_i \in \mathrm{Gal}(K_3/K_0)$ by $(\sigma_i - 1)x_j = \delta_{i,j}$. Collect data:

$$\begin{array}{rclrclrcl}
(\sigma_3-1)X_3 &=& 1 & (\sigma_3-1)X_2 &=& 0 & (\sigma_3-1)X_1 &=& 0,\\
(\sigma_2-1)X_3 &=& -\mu_{23} & (\sigma_2-1)X_2 &=& 1 & (\sigma_2-1)X_1 &=& 0,\\
(\sigma_1-1)X_3 &=& -\mu_{13} & (\sigma_1-1)X_2 &=& -\mu_{12} & (\sigma_1-1)X_1 &=& 1.
\end{array}$$

where

$$\begin{array}{rclrcl}
\mu_{12} &=& \Omega_2^p, & \omega_{12} &=& \omega_2^p,\\
\mu_{23} &=& \wp(\Omega_3)/\wp(\Omega_2), & \omega_{23} &=& \wp(\omega_3)/\wp(\omega_2),\\
\mu_{13} &=& (\Omega_2^p\Omega_3 - \Omega_3^p\Omega_2)/\wp(\Omega_2), & \omega_{13} &=& (\omega_2^p\omega_3 - \omega_3^p\omega_2)/\wp(\omega_2).
\end{array}$$

Define $\eta_{12} = \omega_{12} - \mu_{12}$, $\eta_{23} = \omega_{23} - \mu_{23}$, and $\eta_{13} = \omega_{13} - \mu_{13} \in \mathcal{M}_0$.

Then $\Theta_3 = \sigma_3$, $\Theta_2 = \sigma_2 \Theta_3^{[\mu_{23}]}$, and $\Theta_2 = \sigma_1 \Theta_3^{[\mu_{13}]} \Theta_2^{[\mu_{12}]}$ provide a scaffold: Setting $\Psi_s = \Theta_s - 1$. Then for $0 \leq i, j, k < p$,

$$\Psi_1 \binom{X_3}{i}\binom{X_2}{j}\binom{X_1}{k} = \binom{X_3}{i}\binom{X_2}{j}\binom{X_1}{k-1},$$

and Ψ_2, Ψ_3 act similarly.

Let $\Theta_3' = \sigma_3$, $\Theta_2' = \sigma_2(\Theta_3')^{[\omega_{23}]}$, and $\Theta_2' = \sigma_1(\Theta_3')^{[\omega_{13}]}(\Theta_2')^{[\omega_{12}]}$.

Let

$$\rho = \binom{X_3}{p-1}\binom{X_2}{p-1}\binom{X_1}{p-1} \in K_3.$$

The VC refined breaks for K_3/K_0 are

$$\begin{aligned} r_1 &= v_3((\Theta_3' - 1)\rho) - v_3(\rho) = b, \\ r_2 &= v_3((\Theta_2' - 1)\rho) - v_3(\rho) = \min\{b + v_3(\eta_{23}), pb\}, \\ r_3 &\stackrel{?}{=} v_3((\Theta_1' - 1)\rho) - v_3(\rho) = \quad ? \end{aligned}$$

The VC refined breaks for K_2/K_0 are

$$\begin{aligned} s_1 &= b, \\ s_2 &= \min\{b + v_2(\eta_{12}), pb\}. \end{aligned}$$

So we should expect to see

$$\begin{aligned} r_1 &= v_3((\Theta_3' - 1)\rho) - v_3(\rho) = b, \\ r_2 &= v_3((\Theta_2' - 1)\rho) - v_3(\rho) = \min\{b + v_3(\eta_{23}), pb\}, \\ r_3 &\stackrel{?}{=} v_3((\Theta_1' - 1)\rho) - v_3(\rho) = \min\{\quad ? \quad, pb + v_3(\eta_{12}), p^2 b\} \end{aligned}$$

We see

$$\begin{aligned} & v_3((\Theta_1' - 1)\rho) - v_3(\rho) \\ & \quad = \min\{b + v_3(\omega_{12}\eta_{23} + \eta_{13}), (p+1)b + (p-2)r_2 + v_3(\eta_{23}), \\ & \qquad\qquad pb + v_3(\eta_{12}), p^2 b\} \end{aligned}$$

Caution: I haven't shown that applying an element in J_κ^p, where J_κ is the augmentation ideal of $\kappa[G]$, cannot increase this value. In other words, I haven't actually proven that $r_3 = v_3((\Theta_1' - 1)\rho) - v_3(\rho)$.

Closing question

A choice was made in (Byott-Elder, 2009) to work in

$$(1 + J_\kappa)/(1 + J_\kappa^p),$$

which is a κ-vector space under truncated κ-powers.

For extensions of degree p^2 this choice was good enough: It can be shown that elements of J_κ^p increase valuation by at least pb: It can be shown that the second refined break is always bound from above by pb. And there are only two refined breaks to worry about.

Now that we are trying to develop a theory for larger extensions, we might want to revisit that decision. Modulo $(1 + J_\kappa^p)$ pulls a veil over things – one that I do not know how to remove.