Truncated exponential: Refined ramification, Galois scaffolds and beyond

Griff Elder

May 27 – 31, 2013

The story begins...

Let K be a finite extension of $\mathbb{Q}_p$ and let L be a totally ramified Galois extension of K.

Then $\mathfrak{O}_L$ is a free $\mathbb{Z}_p$-module upon which $G = \mathrm{Gal}(L/K)$ acts.

i.e. $\mathfrak{O}_L$ is a $\mathbb{Z}_p[G]$-module.

$\mathbb{Z}_p[G]$-modules decompose uniquely into indecomposable modules (Krull-Schmidt Theorem holds)

But there are only a few situations where a classification of indecomposable $\mathbb{Z}_p[G]$-modules is possible. G a p-group:

- $G \cong C_p$ (Diederichsen, 1938), (Reiner, 1957)
- $G \cong C_{p^2}$ (Heller, Reiner, 1962)
- $G \cong C_2 \times C_2$ (Nazarova, 1961)
- $G \cong C_8$ (Jakovlev, 1972)

After determining $\mathbb{Z}_p[C_{p^2}]$-structure of $\mathfrak{O}_L$ when L/K is cyclic of degree p^2 (Elder, 1995), I began working on biquadratic extensions.

(Elder, 1998) when L/K has two distinct breaks in its ramification filtration

(Byott, Elder, 2002) when L/K has one break, at b. If $G = \langle \sigma, \gamma \rangle$, then $v_L((\sigma - 1)\pi_L) = b + 1$ and $v_L((\gamma - 1)\pi_L) = b + 1$. Since L/K is a totally ramified extension, there is a unit $\omega \in \mathfrak{O}_K^\times$ such that

$$(\gamma - 1)\pi_L \equiv \omega(\gamma - 1)\pi_L \bmod \mathfrak{P}_L^{b+2}.$$

In fact, $\gamma - 1 - \omega(\sigma - 1)$ **always** resulted in an interesting increase in valuation when applied to $\rho \in L$ with $v_L(\rho) \equiv b \bmod 4$.

Truncated exponentiation and valuation criterion for a NBG appear

(In fact, scaffolds appear. None are recognized.)

Valuation criterion for a normal basis generator (NBG)

Given an Galois extension of local fields L/K, is there an integer b such for any $\rho \in L$ with $v_L(\rho) = b$

$$\{\sigma\rho : \sigma \in G\}$$

is a K-basis for L? (Byott, Elder, 2007)

Necessary conditions: L/K a totally ramified p-extension.

If yes, then b is any integer that satisfies

$$b \equiv b_{\max} - [L : K]u_{\max} \bmod [L : K]$$

Yes, it K is a field of characteristic p (Elder, 2010)

More interesting and technical in char. 0, (de Smit, Florence, Thomas, 2012)

Point: Study Galois action on these "special" elements.

Truncated exponentiation

$$(1+X)^{[Y]} = \sum_{i=0}^{p-1} \binom{Y}{i} X^i$$
$$= 1 + YX + \frac{Y(Y-1)}{2!}X^2 + \frac{Y(Y-1)(Y-2)}{3!}X^3 + \cdots$$
$$\cdots + \frac{Y(Y-1)\cdots(Y-(p-2))}{(p-1)!}X^{p-1} \in \mathbb{Z}_{(p)}[X,Y].$$

Notice that

$$\gamma - 1 - \omega(\sigma - 1) = \gamma - \sigma^{[\omega]}$$

when $p = 2$.

Bicyclic extensions with one break

Attempting to generalize (Byott, Elder, 2002) from $p = 2$ to $p > 2$, we again have an $C_p \times C_p$-extension with $G = \langle \sigma, \gamma \rangle$ and

$$v_L((\sigma - 1)\pi_L) = 1 + b = v_L((\gamma - 1)\pi_L)$$

where b is the one ramification break number.

Again, the extension is totally ramified so that there is a unit $\omega \in \mathfrak{O}_K^\times$ such that

$$(\gamma - 1)\pi_L \equiv \omega(\sigma - 1)\pi_L \bmod \mathfrak{P}_L^{2+b}.$$

Amazingly...

Amazingly...

When $\rho \in L$ satisfies the normal basis generator criterion, *generally*

$$v_L\left(\left(\gamma - \sum_{i=0}^{t} \binom{\omega}{i} (\sigma - 1)^i\right)\rho\right) = v_L(\rho) + (t+1)b.$$

Namely,

$$\begin{aligned}
&\gamma - 1 && \leftrightarrow && b \\
&\gamma - 1 - \omega(\sigma - 1) && \leftrightarrow && 2b \\
&\gamma - 1 - \omega(\sigma - 1) - \tfrac{\omega(\omega-1)}{2}(\sigma - 1)^2 && \leftrightarrow && 3b \\
&\gamma - 1 - \omega(\sigma - 1) - \tfrac{\omega(\omega-1)}{2}(\sigma - 1)^2 - \tfrac{\omega(\omega-1)(\omega-2)}{6}(\sigma - 1)^3 && \leftrightarrow && 4b \\
& && && \vdots
\end{aligned}$$

Until $t = p - 1$ and the "shift" in valuation is pb, except when "an obstruction" gets in the way of this maximal shift.

Bifurcation

- No obstruction leads to Galois scaffold,
- Obstruction involves Refined ramification.

Return to obstruction and refined ramification later.

Details are simplest in char. p & No obstruction

Let $K = \kappa((t))$ with κ perfect with characteristic p

Ramified C_p-extensions are Artin-Schreier with

$$L = K(x), \quad x^p - x = \beta, \quad v_K(\beta) = -b < 0$$

where b is the ramification number for L/K, and $p \nmid b$.

One break $C_p \times C_p$-extension means that $L = K(x, y)$ with

$$y^p - y = \beta^*, \quad v_K(\beta^*) = -b < 0$$

as well. Thus $\beta^* \equiv u\beta \bmod \beta\mathfrak{P}_K$ for some $u \in \kappa$.

Since κ is perfect, there is $\omega \in \kappa$ such that $u = \omega^p$. Thus

$$\beta^* = \omega^p \beta + \overbrace{\epsilon}^{\text{error}}.$$

Since $x^p - x = \beta$ and $v_K(\beta) < 0$, $v_K(x) < 0$ and $v_K(x^p) = v_K(\beta)$

Thus $v_{K(x)}(x) = v_K(\beta) = -b$

Consider the case where $v_K(\epsilon) > -b/p$ (we will see that this leads to "no obstruction"), then letting $Y = y - \omega x$,

$$\begin{aligned} Y^p - Y &= y^p - \omega^p x^p - y + \omega x \\ &= (y^p - y) - \omega^p x^p + \omega x) \\ &= \omega^p \beta + \epsilon - \omega^p (x + \beta) - \omega x \\ &= -(\omega^p - \omega)x + \epsilon. \end{aligned}$$

If $\omega^p - \omega = 0$ the $C_p \times C_p$-extension degenerates into a C_p-extension. So we find, because

$$v_{K(x)}((\omega^p - \omega)x) = -b < v_{K(x)}(\epsilon),$$

that

$$v_L(Y) = -b.$$

Therefore

$$\rho_a = \frac{1}{Y}$$

satisfies $v_L(\rho_a) = b \equiv b \bmod p^2$, the valuation criterion. So we study Galois action on ρ_a.

Let $G = \langle \sigma, \gamma \rangle$ with

$$\begin{array}{rclrcl} \sigma(y) & = & y+1 & \sigma(x) & = & x \\ \gamma(y) & = & y & \gamma(x) & = & x+1 \end{array}$$

Since $Y = y - \omega x$

$$\sigma(Y) = Y + 1 \quad \text{and} \quad \gamma(Y) = Y - \omega,$$

we have

$$(\gamma - 1)\frac{1}{Y} = \frac{1}{Y - \omega} - \frac{1}{Y} \equiv \frac{\omega}{Y^2} \bmod \frac{1}{Y^2}\mathfrak{P}_L.$$

$$(\sigma - 1)\frac{1}{Y} = \frac{1}{Y + 1} - \frac{1}{Y} \equiv \frac{-1}{Y^2} \bmod \frac{1}{Y^2}\mathfrak{P}_L.$$

$$(\gamma - 1)\rho_a \equiv -\omega(\sigma - 1)\rho_a \text{ mod 'higher terms'}$$

Should we think of $-\omega$ as somehow the partial derivative

$$\frac{\partial_\gamma}{\partial_\sigma}?$$

To show that $\sigma^{[-\omega]}$ is the "right way" to approximate γ we work with another element satisfying the valuation criterion:

$$\begin{aligned}\rho_b &= \binom{Y}{p-1}\binom{x}{p-1} \\ &= \frac{Y(Y-1)\cdots(Y-(p-2))}{(p-1)!} \cdot \frac{x(x-1)\cdots(x-(p-2))}{(p-1)!}\end{aligned}$$

satisfies $v_L(\rho_b) = -(p-1)b - (p-1)pb \equiv b \text{ mod } p^2$.

Observe that

$$\sigma^{[-\omega]}\rho_b = \sum_{i=0}^{p-1} \binom{-\omega}{i} (\sigma-1)^i \binom{Y}{p-1} \binom{x}{p-1}$$

$$= \binom{x}{p-1} \sum_{i=0}^{p-1} \binom{-\omega}{i} (\sigma-1)^i \binom{Y}{p-1}$$

The Pascal identity $\binom{Y}{j-1} + \binom{Y}{j} = \binom{Y+1}{j}$ means that

$$(\sigma-1)\binom{Y}{j} = \binom{Y}{j-1} \text{ and thus } (\sigma-1)^i \binom{Y}{p-1} = \binom{Y}{p-1-i}$$

Therefore

$$\sigma^{[-\omega]}\rho_b = \binom{x}{p-1} \sum_{i=0}^{p-1} \binom{-\omega}{i} \binom{Y}{p-1-i}$$

The Vandermonde Convolution Identity $\binom{A+B}{k} = \sum_{i=0}^{k} \binom{A}{i}\binom{B}{k-i}$ means that

$$\sigma^{[-\omega]}\rho_b = \binom{x}{p-1}\sum_{i=0}^{p-1}\binom{-\omega}{i}\binom{Y}{p-1-i} = \binom{x}{p-1}\binom{Y-\omega}{p-1}$$

On the other hand,

$$\gamma\rho_b = \binom{x+1}{p-1}\binom{Y-\omega}{p-1}$$

As a result,

$$\gamma\sigma^{[\omega]}\rho_b = \binom{x+1}{p-1}\binom{Y}{p-1}$$

and

$$\left(\gamma\sigma^{[\omega]} - 1\right)\rho_b = \binom{Y}{p-1}\binom{x}{p-2}.$$

Thus

$$v_L\left(\left(\gamma\sigma^{[\omega]} - 1\right)\rho_b\right) = v_L(\rho_b) + pb.$$

Recall $v_K(\epsilon)$, in $\beta^* = \omega^p\beta + \epsilon$, is big. "No obstruction" Shift$= pb$.

no obstr. = "max refined ramification" = Galois scaffold

We may generalize $\beta^* = \omega^p \beta + \epsilon$ by allowing $\omega \in K$ with $v_K(\omega) \leq 0$. If $v_K(\omega) \neq 0$, the extension has two ramification numbers

that are congruent modulo p^2.

If $v_K(\epsilon)$ is big enough to be ignored, we have a scaffold (infinite tolerance) using

$$(\sigma-1)^i \left(\gamma\sigma^{[\omega]} - 1\right)^j \binom{Y}{p-1} \binom{x}{p-1} = \binom{Y}{p-1-i} \binom{x}{p-1-j}.$$

This leads to the Galois scaffolds in arbitrarily large elementary abelian p-extensions over a field of characteristic p (Elder, 2009)

Strategy for constructing Galois scaffolds

In a preprint with Byott, we have shown that when a Galois scaffold exists (in C_9 or $C_3 \times C_3$-extensions), there is one that adheres to this strategy.

But first: Why does our approach to creating Galois scaffolds require the ramification numbers to be congruent modulo the degree of the extension?

Let L/K be totally ramified extension of degree p^n. Given an element $\rho \in L$ that satisfies the valuation criterion for a normal basis generator and $\sigma, \gamma \in G$, there will be an element $\omega \in L$ such that

$$(\gamma - 1)\rho \equiv \omega(\sigma - 1)\rho \bmod \text{ 'higher terms'}.$$

We are going to want to use $\sigma^{[\omega]}$ to approximate γ. At the same time, we are going to want expressions such as $\sigma^{[\omega]}$ to lie in $K[G]$.

$$\text{We need } \omega \in K.$$

Thus $v_L((\sigma - 1)\rho) \equiv v_L((\gamma - 1)\rho) \bmod p^n$.

But for any $\sigma \in G$,

$$v_L((\sigma - 1)\rho) - v_L(\rho)$$

will be a ramification number. So the ramification numbers have to be congruent modulo p^n.

Now for purposes of illustration, assume L/K is cyclic of degree p^n with $G = \langle \sigma \rangle$, and ramification numbers

$$b_1 < b_2 < \cdots < b_n$$

Let $\sigma_i = \sigma^{p^{n-i-1}}$ and $K_i = L^{\sigma_{i+1}}$. In K_j there is an element of valuation $v_j(X_j) = -b_j$, and

$$v_j((\sigma_i - 1)X_j) = b_i - b_j,$$

for $1 \leq i \leq j \leq n$.

Since the ramification numbers are congruent modulo p^n.

$$(\sigma_i - 1)X_j = \mu_{i,j} + \overbrace{\epsilon_{i,j}}^{\text{“error”}}$$

for some $\mu_{i,j} \in K$ with $v_j(\mu_{i,j}) = v_j((\sigma_i - 1)X_j) = b_i - b_j$.

Referring to the $C_p \times C_p$ example from earlier, letting $\sigma_2 = \sigma$ and $\sigma_1 = \gamma$, $X_2 = Y$ and $X_1 = x$, note that we had “no error”

$$\begin{aligned}(\sigma_2 - 1)X_2 &= 1\\ (\sigma_1 - 1)X_2 &= -\omega\\ (\sigma_1 - 1)X_1 &= 1\end{aligned}$$

But in other cases, we can get the error “out of the way” if we assume

$$v_n(\epsilon_{i,j}) - v_n(\mu_{i,j}) \geq (p-1)\sum_{k=1}^{i-1} p^{n-k-1}b_k + (p^{n-i} - p^{n-j})b_i + \mathfrak{t},$$

for all $1 \leq i \leq j \leq n$, for some tolerance $\mathfrak{t} \geq 1$.

All this, including the resulting Galois scaffold, appears in another preprint with Byott where we work out conditions on the Artin-Schreier equations defining the C_p^n-extension local number fields that are sufficient for the resulting "errors" to be "out of the way". The involvement of a tolerance $\mathfrak{t}$ became necessary in characteristic 0.

We may then plug the result into the Theorem that Byott discussed on Tuesday to determine whether or not the ring of integers is free over its associated order for these extensions.

If the ramification numbers are all congruent to -1 mod p^n, the degree of the extension, three very nice things happen:

1. Byott's conditions are satisfied: $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$.
2. There is a $\delta \in K$ such that $\mathfrak{D}_{L/K}^{-1} = \delta \mathfrak{O}_L$ so (Bondarko, 2000) applies. Therefore $\mathfrak{A}_{L/K}$ is a Hopf order.
3. The Hopf order $\mathfrak{A}_{L/K}$ has a nice description.

Realizable Hopf orders in $K[C_p^2]$

$$\mathfrak{O}_K\left[\frac{\sigma_2-1}{\pi_K^{M_2}},\frac{\sigma_1\sigma_2^{[-\mu_{1,2}]}-1}{\pi_K^{M_1}}\right]$$

is a realizable Hopf order in $K[C_p^2]$ where $C_p^2=\langle\sigma_1,\sigma_2\rangle$ for all $M_1,M_2\in\mathbb{Z}$ and $\mu_{1,2}\in K$ satisfying

$$(*)\quad \frac{v_K(p)}{p-1}>M_1+M_2,\qquad pM_2\geq M_1>0,\ \text{and}$$

$$(**)\quad v_K(-\mu_{1,2})=M_2-\frac{M_1}{p}.$$

Because $v_K(-\mu_{1,2})\in\mathbb{Z}$, this means $p\mid M_1$, as well. It seems reazonable that this "implies" that these are also Hopf orders under $(*)$ with $(**)$ loosened to

$$v_K(-\mu_{1,2})\geq M_2-\frac{M_1}{p}.$$

Where unless we have equality, we don't require $p\mid M_1$.

Realizable Hopf orders in $K[C_p^3]$

$$\mathfrak{O}_K\left[\frac{\sigma_3-1}{\pi_K^{M_3}},\frac{\sigma_2\sigma_3^{[-\mu_{2,3}]}-1}{\pi_K^{M_2}},\frac{\sigma_1\sigma_3^{[-\mu_{1,3}]}\left(\sigma_2\sigma_3^{[-\mu_{2,3}]}\right)^{[-\mu_{1,2}]}-1}{\pi_K^{M_1}}\right],$$

is a realizable Hopf order in $K[C_p^3]$ for all $M_1, M_2, M_3 \in \mathbb{Z}$ and $\mu_{1,2}, \mu_{1,3}, \mu_{2,3} \in K$ satisfying

$$\frac{v_K(p)}{p-1} > M_1+M_2+M_3, \qquad p^2M_3 \geq pM_2 \geq M_1 > 0, \text{ and}$$

$$v_K(\mu_{i,j}) = M_j - \frac{M_i}{p^{j-i}}.$$

Note that this means $p^2 \mid M_1$, $p \mid M_2$, as well. Furthermore, our process imposes some additional restrictions: $p^2 \mid (pM_3 - M_2)$, there exist $\omega_2, \omega_3 \in K$ with $v_K(\omega_3) \leq v_K(\omega_2) \leq 0$ and $\omega_2 \notin \mathbb{F}_p$ with

$$\mu_{1,2} = -\omega_2, \quad \mu_{2,3} = -\frac{\omega_3^p-\omega_3}{\omega_2^p-\omega_2}, \quad \mu_{1,3} = \frac{\omega_2\omega_3^p-\omega_3\omega_2^p}{\omega_2^p-\omega_2}.$$

Refined Ramification Numbers: Simplest in char. p

Let $K = \kappa((t))$ with κ perfect with characteristic p

One break $C_p \times C_p$-extension L/K means that there are $\beta \in K$ with $v_K(\beta) = -b < 0$ and $\omega \in \kappa$ such that $L = K(x, y)$ with

$$\begin{aligned} x^p - x &= \beta \\ y^p - y &= \omega^p \beta + \overbrace{\epsilon}^{\text{error}}. \end{aligned}$$

Again $v_{K(x)}(x) = v_K(\beta) = -b$.
A technical argument yields an $E \in K(x)$ such that

$$v_{K(x)}(\epsilon + E^p - E) = v_K(\epsilon) = -e,$$

where without loss of generality, if $e > 0$ then $e \not\equiv 0, b \bmod p$.
Letting $Y = y - \omega x + E$ yields

$$\begin{aligned} Y^p - Y &= y^p - \omega^p x^p - y + \omega x + E^p - E \\ &= (y^p - y) - \omega^p x^p + \omega x + E^p - E) \\ &= -(\omega^p - \omega)x + (\epsilon + E^p - E). \end{aligned}$$

Since $v_{K(x)}((\omega^p - \omega)x) = -b < v_{K(x)}(\epsilon + E^p - E)$

$$v_L(Y) = -b.$$

Recall that this was an important step earlier. We are off to the races, except that

$$(\gamma - 1)Y = -\omega + (\gamma - 1)E$$

Let $\mathcal{E} = (\gamma - 1)E \in K(x)$. Note that

$$v_{K(x)}(\mathcal{E}) = b - e \not\equiv 0, b \bmod p.$$

Furthermore,

$$\gamma\sigma^{[\omega]}\binom{Y}{p-1}\binom{x}{p-1} = \binom{x+1}{p-1}\binom{Y+\mathcal{E}}{p-1}$$

Using the Vandermonde Convolution Identity

$$\gamma\sigma^{[\omega]}\binom{Y}{p-1}\binom{x}{p-1} = \binom{x+1}{p-1}\binom{Y+\mathcal{E}}{p-1}$$
$$= \binom{x+1}{p-1}\sum_{i=0}^{p-1}\binom{Y}{i}\binom{\mathcal{E}}{p-1-i}$$

So

$$\left(\gamma\sigma^{[\omega]}-1\right)\binom{Y}{p-1}\binom{x}{p-1} = \binom{Y}{p-1}\binom{x}{p-2}$$
$$+\binom{x+1}{p-1}\binom{Y}{p-2}\binom{\mathcal{E}}{1} \text{ mod } \text{“higher terms”}$$

$$v_L\left(\left(\gamma\sigma^{[\omega]}-1\right)\rho\right) - v_L(\rho) = \min\{b + v_L(\mathcal{E}), pb\}.$$

This is the second refined break.

In characteristic 0...

(Byott, Elder, 2009) The second refined break b_* is canonical and satisfies $b < b_* \leq \min\{pb, b + p(pv_K(p) - (p-1)b)\}$, and if $b_* < \min\{pb, b + p(pv_K(p) - (p-1)b)\}$ then

$$b_* \equiv b + pi \bmod p^2$$

with $i \neq 0, b$.

Furthermore, under $b_* < (p - 1 + \frac{1}{p})b$, we can say that the

$$\mathbb{F}_p[G] - \text{structure of } \mathfrak{O}_L/p\mathfrak{O}_L \text{ depends upon } b_*.$$

Do larger ramification number depend upon refined breaks?

(Elder, Hooper, 2007) Yes in quaternion extensions.

(Elder, preprint 2006) Not in a simple way when $p > 2$.

What do refined breaks mean?

When the refined breaks are maximal, you have a Galois scaffold. So, for example in $C_p \times C_p$-extensions with

$$\begin{aligned} x^p - x &= \beta \\ y^p - y &= \omega^p \beta + \overbrace{\epsilon}^{\text{error}}. \end{aligned}$$

allowing $v_K(\omega) < 0$, when $v_K(\epsilon)$ is too small to be "out of the way" for a Galois scaffold to exist, there should still be an invariant similar to the second refined ramification number. It seems reasonable to expect that this invariant will also be necessary for Galois module structure somehow in analogy with (Byott, Elder, 2009). But then, since these extensions already have two ramification breaks, this would suggest that this invariant be thought of as something other than a "ramification number". Doesn't it?