Sharp bounds on ramification breaks in nonabelian extensions of degree p^3

Griff Elder

University of Nebraska at Omaha

May 31, 2019

Setting

Let p be a prime. Let $\mathbb{F}_q$ be a finite field with $q = p^f$ elements, and let

$$K = \mathbb{F}_q((t))$$

be the field of formal Laurent series. In concrete terms, elements $\alpha \in K$ look like

$$\alpha = \frac{1}{t^n}(a_0 + a_1 t + a_2 t^2 + \cdots)$$

where $a_i \in \mathbb{F}_q$, $a_0 + a_1 t + a_2 t^2 + \cdots$ is a formal power series.

There is a valuation, $v_K : K \to \mathbb{Z} \cup \{\infty\}$. Namely, assuming that $a_0 \neq 0$, then $v_K(\alpha) = -n$. Thus K has

- a ring of integers $\mathcal{O}_K = \{x \in K \ : \ v_K(x) \geq 0\}$,
- prime elements 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 $\mathbb{F}_q = \mathcal{O}_K/\mathcal{M}_K$.

Totally ramified, Galois p-extensions

Let N/K be a finite extension of fields. Necessarily, there is a valuation, $v_N : N \to \mathbb{Z} \cup \{\infty\}$, and

- a ring of integers $\mathcal{O}_N = \{x \in N \ : \ v_N(x) \geq 0\}$,
- prime elements π_N such that $v_N(\pi_N) = 1$,
- a unique maximal ideal $\mathcal{M}_N = \{x \in N \ : \ v_N(x) > 0\}$, and
- a residue field $\mathcal{O}_N/\mathcal{M}_N$.

Impose three restrictions: Restrict...

1. to totally ramified extensions: Defined by Eisenstein polynomial $f(x)$

   $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$, $v_K(a_i) \geq 1$ and $v_K(a_0) = 1$.

   $\iff [\mathcal{O}_N/\mathcal{M}_N : \mathcal{O}_K/\mathcal{M}_K] = 1$.
2. to p-extensions: $[N : K] = m = p^n$ for some $n \geq 1$.
3. to Galois extensions: splitting field for $f(x)$ and $\gcd(f(x), f'(x)) = 1$.

The original Group Valuation

Let $G = \mathrm{Gal}(N/K)$, and following Serre's "Local Fields", define

$$i_G(\sigma) = v_N(\sigma(\pi_N) - \pi_N).$$

Shift. Define $j_G : G \to \mathbb{Z}^{>0} \cup \{\infty\}$ by $j_G(\sigma) = i_G(\sigma) - 1$ then we have a group valuation

1. $j_G(\sigma\tau) \geq \min\{j_G(\sigma), j_G(\tau)\}$
2. $j_G(\sigma^{-1}\tau^{-1}\sigma\tau) \geq j_G(\sigma) + j_G(\tau)$

We also have (because we are in characteristic p)

3. $j_G(\sigma^p) \geq (p^2 - p + 1)j_G(\sigma)$

...if you are coming from Childs 2000

Namely, coming with a primary interest in Hopf orders/Larson orders and restrict to p-groups in characteristic p. Then the definition of a *p-adic order-bounded group valuation on G*. $\nu : G \to \mathbb{Z}^{>0} \cup \{\infty\}$ (with numbering as in Childs 2000) is

(i)	$j_G(\sigma\tau) \geq \min\{j_G(\sigma), j_G(\tau)\}$	$\nu(\sigma\tau) \geq \min\{\nu(\sigma), \nu(\tau)\}$
(ii)	$j_G([\sigma,\tau]) \geq j_G(\sigma) + j_G(\tau)$	$\nu([\sigma,\tau]) \geq \nu(\sigma) + \nu(\tau)$
(v)	$j_G(\sigma^p) \geq (p^2 - p + 1) j_G(\sigma)$	$\nu(\sigma^p) \geq p\nu(\sigma)$.

Since G is finite, the image $j_G(G)$ (excluding ∞) is a finite set of integers.

This finite set of integers is our focus today, as this is the set of *ramification breaks* (in the *lower numbering*).

Before we switch...

In Richard Larson's 1976 paper, which gives, what is to this day, the only general construction of Hopf orders in group rings,..

Larson writes that "group valuations were first discussed by Zassenhaus [20]", which points to a unpublished paper entitled *On group valuations*.

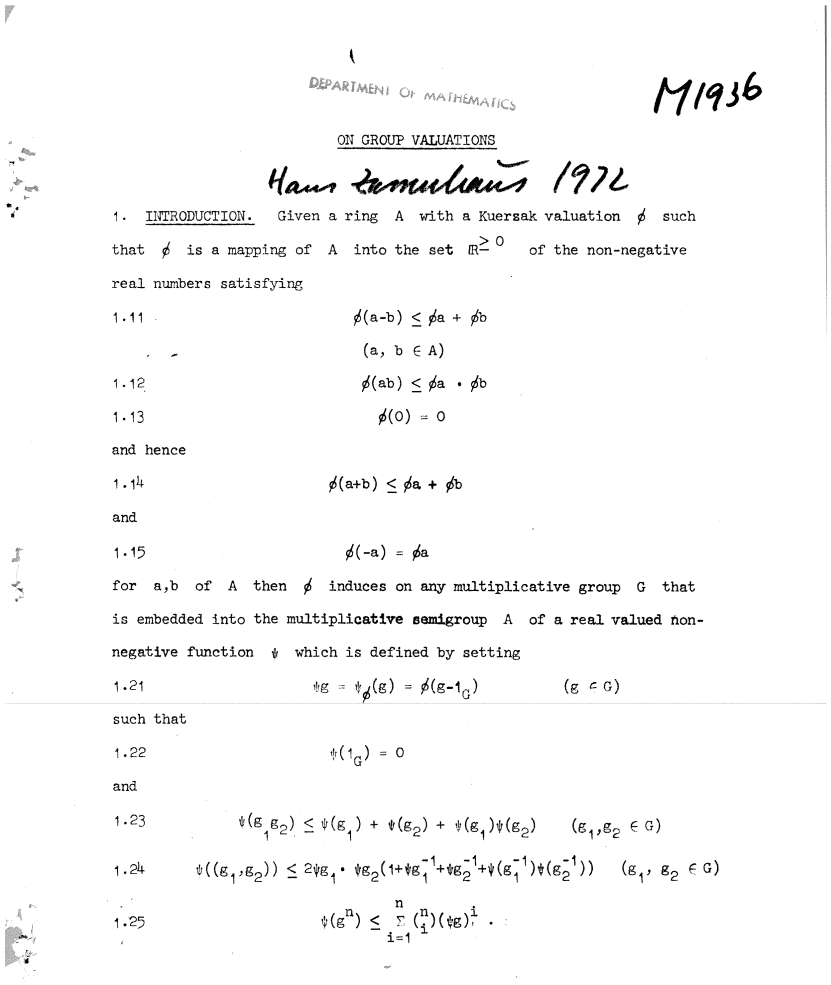
As I prepared for our 2013 conference, I got curious about this unpublished paper and contacted Richard Larson about it.

His reply was that he didn't have a copy and referring to Zassenhaus wrote: "Probably there were informal discussions with him..." as Larson thought Zassenhaus was visiting University of Illinois – Champaign-Urbana at the time.

Did the document actually exist?

Zassenhaus ended his career at Ohio State. So I contacted David Goss...

who contacts Sudarshan Sehgal at Univ of Alberta, who shared a copy with me!!



DEPARTMENT OF MATHEMATICS

M1936

ON GROUP VALUATIONS

Hans Zassenhaus 1972

1. INTRODUCTION. Given a ring A with a Kuersak valuation ϕ such that ϕ is a mapping of A into the set $\mathbb{R}^{\geq 0}$ of the non-negative real numbers satisfying

1.11 $$\phi(a-b) \leq \phi a + \phi b \qquad (a, b \in A)$$

1.12 $$\phi(ab) \leq \phi a \cdot \phi b$$

1.13 $$\phi(0) = 0$$

and hence

1.14 $$\phi(a+b) \leq \phi a + \phi b$$

and

1.15 $$\phi(-a) = \phi a$$

for a,b of A then ϕ induces on any multiplicative group G that is embedded into the multiplicative semigroup A of a real valued non-negative function ψ which is defined by setting

1.21 $$\psi g = \psi_\phi(g) = \phi(g-1_G) \qquad (g \in G)$$

such that

1.22 $$\psi(1_G) = 0$$

and

1.23 $$\psi(g_1 g_2) \leq \psi(g_1) + \psi(g_2) + \psi(g_1)\psi(g_2) \qquad (g_1, g_2 \in G)$$

1.24 $$\psi((g_1, g_2)) \leq 2\psi g_1 \cdot \psi g_2 (1+\psi g_1^{-1}+\psi g_2^{-1}+\psi(g_1^{-1})\psi(g_2^{-1})) \qquad (g_1, g_2 \in G)$$

1.25 $$\psi(g^n) \leq \sum_{i=1}^{n} \binom{n}{i} (\psi g)^i .$$

If you have ever been curious about this reference, I can share a copy.

Contrast

- Larson 1976 proved that *every* p-adic order-bounded group valuation ν on G, satisfying
  1. $\nu(\sigma\tau) \geq \min\{\nu(\sigma), \nu(\tau)\}$
  2. $\nu([\sigma, \tau]) \geq \nu(\sigma) + \nu(\tau)$
  3. $\nu(\sigma^p) \geq p\nu(\sigma)$

  produces a Hopf order in $K[G]$, namely

$$\mathcal{O}_K \left[\frac{\sigma - 1}{\pi_K^{\nu(\sigma)}} : \sigma \in G \right].$$

- On the other hand, *not every* group valuation j_G that satisfies
  1. $j_G(\sigma\tau) \geq \min\{j_G(\sigma), j_G(\tau)\}$
  2. $j_G([\sigma, \tau]) \geq j_G(\sigma) + j_G(\tau)$
  3. $j_G(\sigma^p) \geq (p^2 - p + 1)j_G(\sigma)$

  belongs to a Galois extension. As we shall see...

Ramification filtration

Define the ramification subgroups

$$G_i = \{\sigma \in G : v_N(\sigma(\pi_N) - \pi_N) \geq i + 1\}.$$

Namely, $\sigma \in G_i$ if and only if $j_G(\sigma) \geq i$.

Since $j_G(\tau\sigma\tau^{-1}) = j_G(\sigma)$, these ramification subgroups are normal.

$$G = G_1 \supseteq G_2 \supseteq G_3 \supseteq \cdots.$$

Integers i in the range of j_G (also $G_i \supsetneq G_{i+1}$) are *lower ramification breaks*. They are related to upper ramification breaks by a "mechanical" process:

The Herbrand function $\varphi(x)$ is a piecewise linear function with slope $1 = 1/[G : G_{b_1}]$ from the origin to $x = b_1$, the first lower break. Slope $1/[G : G_{b_2}]$ from $x = b_1$ to $x = b_2$, the second lower break, and so forth.

Upper ramification breaks are simply the y-coordinates of the actual breaks/bends in this piecewise linear function.

Lower ramification breaks are used to give the lower ramification breaks of a *subgroup*

$$G_i \cap H = H_i.$$

Upper ramification breaks are used to give the upper ramification breaks of a *quotient group*

$$G^i N/N = (G/N)^i.$$

If $H = N$ is a ramification subgroup, we don't need to be so careful.

The Groups

There are two nonabelian groups of order p^3.

For $p > 2$:

- The Heisenberg group modulo p:

$$H(p^3) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{F}_p \right\}$$

- A subgroup of the affine group modulo p^2

$$A(p^3) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z}/(p^2), a \equiv 1 \bmod p \right\}$$

For $p = 2$

- The quaternion group, Q_8.
- The dihedral group, D_8.

In all cases...

- ... the group G is generated by two elements γ, σ,
- $\tau = \gamma^{-1}\sigma^{-1}\gamma\sigma$ generates the center, which is the unique normal subgroup, and
- $G/\langle\tau\rangle \cong C_p \times C_p$.

For example, when $p > 2$:

- $H(p^3)$

$$\gamma = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

- $A(p^3)$

$$\gamma = \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}.$$

...thus our strategy:

Let N/K be a totally ramified Galois extension with one of these groups.

Observe: Regardless of which nonabelian Galois group, N/K may be viewed as a cyclic degree p extension N/M with Galois group $\langle\tau\rangle$ on top of a $C_p \times C_p$-extension M/K with Galois group $\langle\bar{\gamma}, \bar{\sigma}\rangle$.

Strategy: Assume that the extension M/K is given with $M = K(x, y)$

$$x^p - x = \beta, \quad y^p - y = \alpha.$$

Let $u_1 \leq u_2$ denote the upper ramification numbers for M/K. WLOG assume that $\{u_1, u_2\} = \{a, b\}$ where $v_K(\alpha) = -a$, $v_K(\beta) = -b$. Necessarily, $p \nmid a, b > 0$. Note: Constant terms are *not* integral.

Note: Valuation of the constant in the Artin-Schreier equation linked to ramification numbers. Link is "secure" only when $p \nmid$ valuation.

Note: $H(p^3)$ and Q_8 are symmetric in γ, σ. So in these cases, we will be able to assume WLOG that $b \leq a$. However, this is not the case for $A(p^3)$ and D_8. So for now, we leave the relationship between a and b vague.

Strategy cont.

Assume that M/K and its ramification information are given. Since N/M is a cyclic extension of degree p, $N = M(z)$ where

$$z^p - z = B \in M, \text{ and WLOG } \tau(z) = z + 1.$$

The element $B \in M$ completely determines N. Thus it completely determines the extension N/K.

So... all the information that we are interested in:

- structure of the Galois group.
- ramification number of N/M.

must be somehow be encoded in the element B.

Galois group

Theorem. Let $M = K(x, y)$ where $x^p - x = \beta$ and $y^p - y = \alpha$ determine a $C_p \times C_p$-extension with

$$\begin{aligned} (\gamma - 1)x = 0, \quad (\gamma - 1)y = 1, \\ (\sigma - 1)x = 1, \quad (\sigma - 1)y = 0. \end{aligned}$$

Then $N = M(z)$ with $z^p - z = B$ and $(\tau - 1)z = 1$ determines a nonabelian Galois extension of K (for $G = D_8$ or $A(p^3)$ with $|\sigma| = p^2$) if and only if

$$B \in \begin{cases} \beta x + \alpha x + \alpha y + M^{\wp} + K & \text{for } G = Q_8, \\ \alpha x + M^{\wp} + K & \text{for } G = H(p^3), \\ \alpha x - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i}\beta^i x^{p-i} + M^{\wp} + K & \text{for } G = D_8 \text{ or } A(p^3), \end{cases}$$

with $M^{\wp} = \{\wp(m) : m \in M\}$ where $\wp(v) = v^p - v$ is the $\mathbb{F}_p$-linear map.

Note: $\wp(xy) = (xy)^p - xy = (x + \beta)(y + \alpha) - xy = \alpha x + \beta y + \alpha\beta$. Thus

$$\alpha x + \beta y \in M^{\wp} + K, \text{ restoring symmetry.}$$

Towards ramification breaks

Consider the situation where $G = H(p^3)$. Thus $N = M(z)$ and

$$z^p - z = B \in \alpha x + M^{\wp} + K.$$

Since we are interested in bounds on the ramification break and $\alpha x \in L = K(x)$, we seek the element of $\alpha x + L^{\wp} + K$ of largest valuation.

Step 1. Observe that since we are in characteristic p, the set $K^p = \{k^p : k \in K\}$ is a subfield of K.

Indeed, K/K^p is a totally ramified, purely inseparable extension, and

$$K = K^p(\beta).$$

So $\alpha = \sum_{i=0}^{p-1} \mu_i^p \beta^i$ for some coefficients $\mu_i^p \in K^p$, and

$$\alpha x = \sum_{i=0}^{p-1} \mu_i^p \beta^i x.$$

Step 2. We break αx into three pieces:

$$\alpha x = \mu_0^p x + \left(\sum_{i=1}^{p-2} \mu_i^p \beta^i x \right) + \mu_{p-1}^p \beta^{p-1} x.$$

The middle piece doesn't exist for $p = 2$.

- WLOG we change α in $\alpha + K^\wp$, so that $\mu_0 \in \mathbb{F}_q$. We can ignore.
- $v_L(\mu_{p-1}^p \beta^{p-1} x)$ the largest valuation in $\mu_{p-1}^p \beta^{p-1} x + L^\wp + K$, while
- $v_L\left(\sum_{i=1}^{p-2} \mu_i^p \beta^{i-1} x^2\right)$ is the largest valuation in

$$\sum_{i=0}^{p-2} \mu_i^p \beta^i x + L^\wp + K.$$

Reason. Expand/set $t = i + 1$: $\wp(\mu x^t) = \mu^p x^{pt} - \mu x^t = \mu^p (x + \beta)^t - \mu x^t$

$$(i+1)\mu_i^p \beta^i x + \mu_i^p \sum_{j=2}^{i+1} \binom{i+1}{j} \beta^{i-j+1} x^j - \mu_i x^{i+1}$$

$$= \wp(\mu_i x^{i+1}) - \mu_i \beta^{i+1} \in L^\wp + K.$$

Ramification breaks, $p > 2$

Let M/K be a totally ramified $C_p \times C_p$-extension with upper ramification breaks $u_1 \leq u_2$. Thus $M = K(x, y)$ where $x^p - x = \beta$, $y^p - y = \alpha$ with $v_K(\beta) = -b$, $v_K(\alpha) = -a$ and $\{a, b\} = \{u_1, u_2\}$. Embed M/K in a totally ramified nonabelian extension N/K of degree p^3 with $G = \mathrm{Gal}(N/K)$ (for $A(p^3)$ with $\sigma^{p^2} = \gamma^p = 1$). Let

$$\alpha = \sum_{i=0}^{p-1} \mu_i^p \beta^i.$$

Set $a_* = -v_K(\mu_{p-1}^p \beta^{p-1})$, and set

$$d = \begin{cases} \max\{u_1 + a_*, u_2 + u_1/p\} & \text{for } G = H(p^3), \\ \max\{pu_1, u_1 + a_*, u_2 + u_1/p\} & \text{for } u_1 = b, u_2 = a, G = A(p^3), \\ pu_2 & \text{for } u_1 = a, u_2 = b, G = A(p^3). \end{cases}$$

Important: $u_1 + a_* \in p\mathbb{Z}$ and $u_2 + u_1/p \notin \mathbb{Z}$.

Upper breaks for N/K are: $u_1 \leq u_2 < u_3$ where either $u_3 = d$, or $u_3 \in \mathbb{Z}$ and $p \nmid u_3 > d$.

Focus on Heisenberg extensions

- Example: Conclusion of Hasse-Arf can fail.
  Let $K = \mathbb{F}_9((t))$ and choose $\omega \in \mathbb{F}_9 \setminus \mathbb{F}_3$. Let $M = K(x, y)$ and $N = M(z)$ where

$$\begin{aligned} x^3 - x &= 1/t, \\ y^3 - y &= \omega/t, \\ z^3 - z &= \omega x/t. \end{aligned}$$

  Then N/K is Galois, $\mathrm{Gal}(N/K) \cong H(p^3)$ and $u_1 = u_2 = 1$, $u_3 = 4/3$.
- Recall the group valuation condition $j_G([\sigma, \tau]) \geq j_G(\sigma) + j_G(\tau)$, which can be restated as

$$b_3 \geq b_2 + b_1.$$

  Since $u_3 \geq d \geq u_2 + u_1/p$, we have

$$b_3 \geq b_2 + pb_1.$$

  Not all group valuations can be attached to a field extension.

Ramification breaks, $p = 2$ so $a = a^*$

Let M/K be a totally ramified biquadratic extension with upper ramification breaks $u_1 \leq u_2$. Thus $M = K(x, y)$ where $x^2 - x = \beta$, $y^2 - y = \alpha$ with $v_K(\beta) = -b$, $v_K(\alpha) = -a$ and $\{a, b\} = \{u_1, u_2\}$. Embed M/K in a totally nonabelian ramified extension N/K of degree 8 with $G = \mathrm{Gal}(N/K)$ (recall $G = D_8$ has $\sigma^4 = \gamma^2 = 1$). So

$$\alpha = \mu_1^2 \beta + \mu_0.$$

And if $u_1 = u_2$, then $\mu_1 \equiv \omega \bmod \mathcal{M}_K$ for some $\omega \in \mathbb{F}_q$.

$$d = \begin{cases} (5u_1 - r)/2 & \text{for } G = Q_8, u_1 = u_2 \text{ and } \omega \in \mathbb{F}_4 \\ 2u_2 & \text{for } G = Q_8, \text{ and } \begin{cases} u_1 = u_2 \text{ and } \omega \notin \mathbb{F}_4 \\ u_1 < u_2 \end{cases} \\ \max\{2b, a + b\} & \text{for } G = D_8. \end{cases}$$

Upper breaks for N/K are: $u_1 \leq u_2 < u_3$ where either $u_3 = d$ or $u_3 > d$ is an odd integer. Refined break $0 < r \leq 2u_1$ is odd, unless $r = 2u_1$.

Focus on Quaternion extensions

- Example: Conclusion of Hasse-Arf can fail.
  Let $K = \mathbb{F}_4((t))$ and choose $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Let $M = K(x, y)$ and $N = M(z)$ where

$$\begin{aligned} x^2 - x &= 1/t, \\ y^2 - y &= \omega/t, \\ z^2 - z &= (1+\omega)x/t + \omega y/t. \end{aligned}$$

  Then N/K is Galois, $\mathrm{Gal}(N/K) \cong Q_8$ and $u_1 = u_2 = 1$, $u_3 = 3/2$.
- $r = 2u_1$ is "maximal refined ramification" – motivated Galois scaffold.
- $\omega \notin \mathbb{F}_4 \implies u_3 \geq 2u_1$. Only when $\omega \in \mathbb{F}_4$ can u_3 fall below $2u_1$ and Hasse-Arf fail.

Curious. This kind of obstruction/trapdoor/keyhole has been seen before.

The great RB/II controversy of 2014/2015!

For p-adic $C_p \times C_p$-extensions M/K with one break b, [Keating, 2014] relates refined ramification and indices of inseparability

$$i_0 - i_1 = pb - r, \tag{1}$$

assuming that $i_1 \neq p(p-1)b$. Note: $i_0 = (p^2-1)b$ always.

In characteristic p, details are easier: Namely, let $M = K(x, y)$ where $x^p - x = \beta$ and $y^p - y = \omega^p \beta + \epsilon$, $\omega \in \mathbb{F}_q \setminus \mathbb{F}_p$, $v_K(\epsilon) > v_K(\beta) = -b$.

And the assumption $i_1 \neq p(p-1)b$ has a simpler description:

$$\omega \in \mathbb{F}_{p^2}.$$

This is the obstruction/trapdoor/keyhole!!

The Great Controversy: It seems that $\omega \notin \mathbb{F}_{p^2}$ should be the general condition, while $\omega \in \mathbb{F}_{p^2}$ should be considered very special. So...

...if "in general" $i_1 = p(p-1)b$ and $i_0 = (p^2-1)b$ are both fixed, can we really say that $\{i_0, i_1\}$ successfully replaces the missing 2nd break?

But now (5/30/2019),... I begrudgingly say "uncle"

...if we use indices of inseparability, rather than refined breaks in the result on ramification breaks in nonabelian extensions of degree 8,

$$d = \begin{cases} (5u_1 - r)/2 & \text{for } G = Q_8, u_1 = u_2 \text{ and } \omega \in \mathbb{F}_4 \\ 2u_2 & \text{for } G = Q_8, \text{ and } \begin{cases} u_1 = u_2 \text{ and } \omega \notin \mathbb{F}_4 \\ u_1 < u_2 \end{cases} \\ \max\{2b, a+b\} & \text{for } G = D_8. \end{cases}$$

gets replaced by

$$d = \begin{cases} (6u_1 - i_1)/2 & \text{for } G = Q_8, \\ \max\{2b, a+b\} & \text{for } G = D_8. \end{cases}$$

Closing questions: What do "things" mean?

1. In $C_p \times C_p$ extensions with one break b, $x^p - x = \beta$, $y^p - y = \alpha = \omega^p \beta + \epsilon$. What is the meaning of $v_K(\epsilon)$?

   Answer: Its meaning resides in the refined ramification break r, which is necessary for Galois module structure, and for understanding the failing of the conclusion of Hasse-Arf in Quaternion extensions.

2. What is the meaning of the condition $\omega \in \mathbb{F}_{p^2}$ vs. $\omega \notin \mathbb{F}_{p^2}$?

   Discussion: It couples/uncouples refined ramification from indices of inseparability. It seems that indices are the "correct invariant" for determining sharp bounds on larger ramification breaks. Refined breaks are the "correct invariant" for Galois module structure. They are coupled while they can be used interchangeably, but precisely when the invariants diverge, they uncouple.

3. What is the meaning of the decomposition

$$\alpha = \mu_0^p + \left(\sum_{i=1}^{p-2} \mu_i^p \beta^i \right) + \mu_{p-1}^p \beta^{p-1}?$$

Discussion: Let $-c^*$ be the valuation of the middle term, and let $-a^* = v_K(\mu_{p-1}^p \beta^{p-1})$.

Since $v_K(\alpha) = -\max\{c^*, a^*\}$ the maximum of c^* and a^* is an upper ramification break. So the max has meaning. But what are the meanings of the individual parts c^* and a^*? Is there a reason why I should have been able to predict that the part involving β^{p-1} will be treated differently?