Arithmetic vs. Geometric results in char. 0

Griff Elder

May 27 – 31, 2013

Setting

Let p be prime and $\mathbb{Q}_p$ be the *p-adic numbers*.

Elements of $\mathbb{Q}_p$ look like Laurent series in p:

$$a_{-t}\frac{1}{p^t} + \cdots + a_{-1}\frac{1}{p} + a_0 + a_1 p + a_2 p^2 + \cdots$$

with $0 \leq a_i \leq p-1$. (Note: The a_i *can be identified with* elements in the finite field $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$.)

Think of them as "base p" numbers with a topology such that

$$n \to \infty \text{ implies } p^n \to 0.$$

Let K be an algebraic extension of $\mathbb{Q}_p$, then there is a "prime element" $\pi_K \in K$ such that every element $\alpha \in K$ can be written as

$$\alpha = a_{-t}\frac{1}{\pi_K^t} + \cdots + a_{-1}\frac{1}{\pi_K} + a_0 + a_1\pi_K + a_2\pi_K^2 + \cdots$$

This time, the a_i *can be identified with* elements in finite field $\mathbb{F}_{p^f}$

Each α has a "largest power of π_K that can be "factored out", its *valuation*. We say,

$$v_K(\alpha) = -t.$$

The *integers* are those elements "without denominator"

$$\mathfrak{O}_K = \{x \in K : v_K(x) \geq 0\}.$$

There is a unique *maximal ideal*

$$\mathfrak{P}_K = \{x \in K : v_K(x) > 0\}.$$

The quotient $\mathfrak{O}_K/\mathfrak{P}_K \cong \mathbb{F}_{p^f}$ is called the *residue field*.

Today's topic

$p \in \mathbb{Q} \subset \mathbb{Q}_p \subset K$. So $v_K(p) \in \mathbb{Z}$

For certain questions, the size of $v_K(p)$ matters. We say

absolute ramification matters.

For example, say $1 + \alpha \in 1 + \mathfrak{P}_K$, then

$$v_K((1+\alpha)^p - 1) = \begin{cases} v_K(\alpha^p) & \text{if } v_K(\alpha) < v_K(p)/(p-1), \\ ??? & \text{if } v_K(\alpha) = v_K(p)/(p-1), \\ v_K(p\alpha) & \text{if } v_K(\alpha) > v_K(p)/(p-1). \end{cases}$$

Similar setting

There are similar fields $K = \mathbb{F}_{p^f}((T))$, where every element $\alpha \in K$ can be written as

$$\alpha = a_{-t}\frac{1}{T^t} + \cdots + a_{-1}\frac{1}{T} + a_0 + a_1 T + a_2 T^2 + \cdots$$

Here the a_i *are* elements in $\mathbb{F}_{p^f}$. The field has characteristic p.

Again elements have valuation. So we say

$$v_K(\alpha) = -t.$$

There are *integers*, a unique *maximal ideal*, etc. all defined similarly.
Except, here p *is* zero, and zero is infinitely divisible. So

$$v_K(p) = \infty.$$

For $1+\alpha \in 1+\mathfrak{P}_K$, instead of

$$v_K((1+\alpha)^p - 1) = \begin{cases} v_K(\alpha^p) & \text{if } v_K(\alpha) < v_K(p)/(p-1), \\ ??? & \text{if } v_K(\alpha) = v_K(p)/(p-1), \\ v_K(p\alpha) & \text{if } v_K(\alpha) > v_K(p)/(p-1). \end{cases}$$

we have

$$v_K((1+\alpha)^p - 1) = v_K(\alpha^p)$$

But this last statement is obvious, which leads to our main point.

Easy observations in characteristic p can give us part of the characteristic 0 answer. Not the lower bound on $v_K(p)$, but at least the equality that holds under that bound. And *that* might be just the foot–in–the–door that we need.

Main Point

Integral Galois module structure, the classification of Hopf orders over K a finite extension of $\mathbb{Q}_p$ – these are old and difficult topics.

Complicated. We get bogged down. Progress is slow.

Where there is a question with an answer that we just can't see, perhaps we should restrict our ambitions to a partial answer – the answer that holds in char. p.

This is our "characteristic independent" answer.

If we interpret the title "*Les corps locaux de caractéristique p, limites de corps locaux de caractéristique* 0" of (Deligne, 1984) to say that for "the questions that we ask", the characteristic p answer will hold in characteristic 0,

"if $v_K(p)$ is large enough"

Then...

Then...

All we need to do is follow these steps:

1. work the answer out in characteristic p,
2. determine lower bounds on $v_K(p)$ for our characteristic independent answer to hold in characteristic zero,

   "geometric result"

   and then
3. turn to the complement.

   "arithmetic result"

And if we are "lucky", we will get the complement for free.

Re-frame old results: Hopf orders in $K[C_p]$

When K has characteristic p, it is easy to see that

$$\mathfrak{O}_K \left[\frac{\sigma - 1}{\pi_K^i} \right]$$

with $i \geq 0$ is a Hopf order in $K[C_p]$ where $C_p = \langle \sigma \rangle$.

Closure under multiplication and co-multiplication are easy. (The converse is a little more involved.)

Step 1 is done.

When K has characteristic 0, these are the Tate-Oort orders under

$$0 \leq i \leq \frac{v_K(p)}{p-1}.$$

Note: Lower bound on $v_K(p)$. Step 2 is done.

All Hopf orders are Tate-Oort. *No* complement. Step 3 for free.

Re-frame old results: Hopf orders in $K[C_{p^2}]$

Using *truncated exponentiation*

$$(1+X)^{[Y]} = \sum_{i=0}^{p-1} \binom{Y}{i} X^i \in \mathbb{Z}_{(p)}[X,Y],$$

it isn't hard to show that for K a local field of characteristic p,

$$H_1 = \mathfrak{O}_K \left[\frac{\sigma^p - 1}{\pi_K^i}, \frac{\sigma(\sigma^p)^{[\mu]} - 1}{\pi_K^j} \right]$$

is a Hopf order under

$$i \geq pj, \quad \text{and} \quad v_K(\mu) \geq \frac{j}{p} - i.$$

Using Childs' book, there are two things to check

1. $(\sigma u)^p \in 1 + \pi_K^{pj} \mathfrak{O}_K \left[\frac{\sigma^p - 1}{\pi_K^i}\right]$, and
2. $\Delta(u) \equiv u \otimes u \mod \mathfrak{O}_K \left[\frac{\sigma^p - 1}{\pi_K^i}\right] \otimes \mathfrak{O}_K \left[\frac{\sigma^p - 1}{\pi_K^i}\right]$

where

$$u = (\sigma^p)^{[\mu]}.$$

The first is trivial, since $u^p = 1$ in characteristic p. This leads to the "p-adic condition" $i \geq pj$.

The second, requires more work, and leads to $v_K(\mu) \geq j/p - i$.

(Step 1 still requires the converse – Rob's topic on Friday.)

Still, things are much easier than in characteristic 0, which is where the Greither orders were originally defined.

Greither orders...

Let $K/\mathbb{Q}_p$ be finite, $\zeta_p \in K$, and set $e' = v_K(p)/(p-1)$. Set $i' = e' - i$, $j' = e' - j$. Assume $e' > i \geq pj > 0$. Then

$$H_2 = \mathfrak{O}_K \left[\frac{\sigma^p - 1}{\pi^i}, \frac{\sigma a_v - 1}{\pi^j} \right]$$

is a Greither order in $K[C_{p^2}]$ for $v \in 1 + \mathfrak{P}_K^{\max\{i'+j/p, i'/p+j\}}$, $a_v = \sum_{m=0}^{p-1} v^m e_m$ where $e_m = (1/p) \sum_{n=0}^{p-1} \zeta_p^{-mn} \sigma^{pn}$.

(with Underwood) Set $\mu = \frac{1}{\zeta_p - 1} \sum_{r=1}^{p-1} \frac{(1-v)^r}{r}$. If $e' > i + j$, then $v_K(\mu) \geq j/p - i$ and

$$H_2 = H_1.$$

Greither orders have a characteristic independent description.

Step 2 is done.

(Underwood 1994) shows that a Hopf order in $K[C_{p^2}]$ with $\zeta_p \in K$ is a Greither order, or its dual is a Greither order.

Step 3 is much less for free, but still the complement can be described in terms of the characteristic independent objects.

But here we are retreading old material.

Towards new results... Hopf orders in $K[C_{p^3}]$

Families have been given (Underwood, 1994) Realizable ones are missing (Underwood, Childs, 2006)

(Underwood, 2008) provides a realizable family.

More work is needed.

Towards new results: Hopf orders in $K[C_{p^3}]$

Let σ generate C_{p^3} and let $K = \mathbb{F}_q((t))$.

Let $i, j, k \geq 0$ satisfy $i \geq pj \geq p^2 k$. Assume $v_K(\mu) \geq j/p - i$, $v_K(\eta) \geq k/p - i$ and $v_K(\nu) \geq k/p - j$. Then

$$H = \mathfrak{O}_K \left[\frac{\sigma^{p^2} - 1}{t^i}, \frac{(\sigma^{p^2})^{[\mu]}\sigma^p - 1}{t^j}, \frac{\left((\sigma^{p^2})^{[\mu]}\sigma^p\right)^{[\nu]}(\sigma^{p^2})^{[\eta]}\sigma - 1}{t^k} \right]$$

is a Hopf order in $K[C_{p^3}]$.

The converse is needed before Step 1 is done.

Need step 2. See Thursday's talk for a strategy and its implementation with $K[C_p^3]$.

Step 3 will be very interesting!

Irritant in the "oyster"

Vernon Armitage gave an expository lecture on the history of Taylor's Theorem at the 1994 Durham meeting on Arithmetic Galois Modules

- Late 60's: Armitage – irritant in the oyster
- 1971: J.-P. Serre's "crazy idea"
- 1972: Fröhlich's Conjecture
- 1981: Martin Taylor's Theorem – the pearl of GMT

My aspirations are at the level of laying down irritants. We need some crazy ideas, a conjectural framework, and then some

PEARLS!!

Childs' Tricotomy from last year

Starting with the state of Galois Module Theory at time of Childs' book, several directions of research:

- Field level: counting and classifying Hopf Galois structures on field extensions with a given Galois group: Byott and Childs' talks on Thursday.
- Hopf orders level: given a Hopf algebra H over a local field K with valuation ring R, find (classify) Hopf orders over R in H. Koch today, and Underwood on Friday.
- Arithmetic of local field extensions: given a H-Hopf Galois extension L/K of local fields with valuation rings S/R, find conditions (ramification conditions + ?) so that
  (a) S is free over the associated order A of S in H, or
  (b) the associated order of S in H is a Hopf order in H.

Griff works exclusively in III. Rob has worked predominantly in II. Alan works in II predominantly, but by entirely different methods. Recently, Lindsay has worked in I.

After the dust settles from this week, I will go back to working things out in local field extensions.

Projects

Left on my own, I will work on

- Galois scaffolds in C_{p^n}-extensions of local function fields – describing the extensions with Galois scaffolds in terms of Witt vectors.
- Artin-Schreier-Witt extensions in characteristic zero. (Describing cyclic extensions of local number fields by Witt vectors.)

Where I see a dividend (because just because you figure something out, doesn't mean that anyone else will care), is in developing families of Hopf orders.

Interesting Project

Let G be a p-group with presentation:

$$G = G_1 = \{\sigma_1^{a_1}\sigma_2^{a_2}\cdots\sigma_n^{a_n} : 0 \leq a_i \leq p-1\}$$

along with normal subgroups

$$G_1 \trianglerighteq G_2 \trianglerighteq G_3 \cdots \trianglerighteq G_n \trianglerighteq \{1\}$$

defined by $G_i = \{\sigma_i^{a_i}\cdots\sigma_n^{a_n} : 0 \leq a_i \leq p-1\}$. Is there interest in determining generic (independent of G, incl. non-abelian) conditions on

$M_i \in \mathbb{Z}$ and $v_K(\mu_{i,j})$ where $\mu_{i,j} \in K$ so that

$$\mathfrak{O}_K\left[\frac{\Theta_n - 1}{\pi_K^{M_n}}, \frac{\Theta_{n-1} - 1}{\pi_K^{M_{n-1}}}, \frac{\Theta_{n-2} - 1}{\pi_K^{M_{n-2}}}, \ldots\right]$$

where

$$\begin{aligned}
\Theta_n &= \sigma_n \\
\Theta_{n-1} &= \sigma_{n-1}\Theta_n^{[\mu_{n-1,n}]} \\
\Theta_{n-2} &= \sigma_{n-2}\Theta_n^{[\mu_{n-2,n}]}\Theta_{n-1}^{[\mu_{n-2,n-1}]} \\
\Theta_{n-3} &= \sigma_{n-3}\Theta_n^{[\mu_{n-3,n}]}\Theta_{n-1}^{[\mu_{n-3,n-1}]}\Theta_{n-2}^{[\mu_{n-3,n-2}]} \\
&\vdots
\end{aligned}$$

is a Hopf order in $K[G]$? Sharp conditions (the boundary) will depend upon the group. Indeed, determine the group?

Now to other "questions that we ask"

If K has characteristic p and L/K is a cyclic extension of degree p with ramification number b, then

- L/K is Artin-Schreier: $L = K(x)$ for some x such that $x^p - x = \beta \in K$.
- The ramification number $b = -v_K(\beta)$ can be any integer relatively prime to p.

If K is a finite extension of $\mathbb{Q}_p$ then

$$1 \leq b \leq \frac{pv_K(p)}{p-1},$$

and if $b < pv_K(p)/(p-1)$ then

- L/K is Artin-Schreier: $L = K(x)$ for some x such that $x^p - x = \beta \in K$ (MacKenzie, Whaples, 1956)
- The ramification number $b = -v_K(\beta)$ satisfies $p \nmid b$.

C_{p^2}-extensions

If K has characteristic p

- L/K is Artin-Schreier: $L = K(x_1, x_2)$ where

$$\begin{aligned} x_1^p - x_1 &= \beta_1 \\ x_1^p - x_1 &= \frac{x_1^p + \beta_1^p - (x_1 + \beta_1)^p}{p} + \beta_2 \end{aligned}$$

- The ramification numbers $b_1 = -v_K(\beta)$ and $b_2 \geq (p^2 - p + 1)b_1$ can be any integers relatively prime to p, except $b_2 > (p^2 - p + 1)b_1$ implies $b_2 \not\equiv -(p-1)b_1 \bmod p^2$.

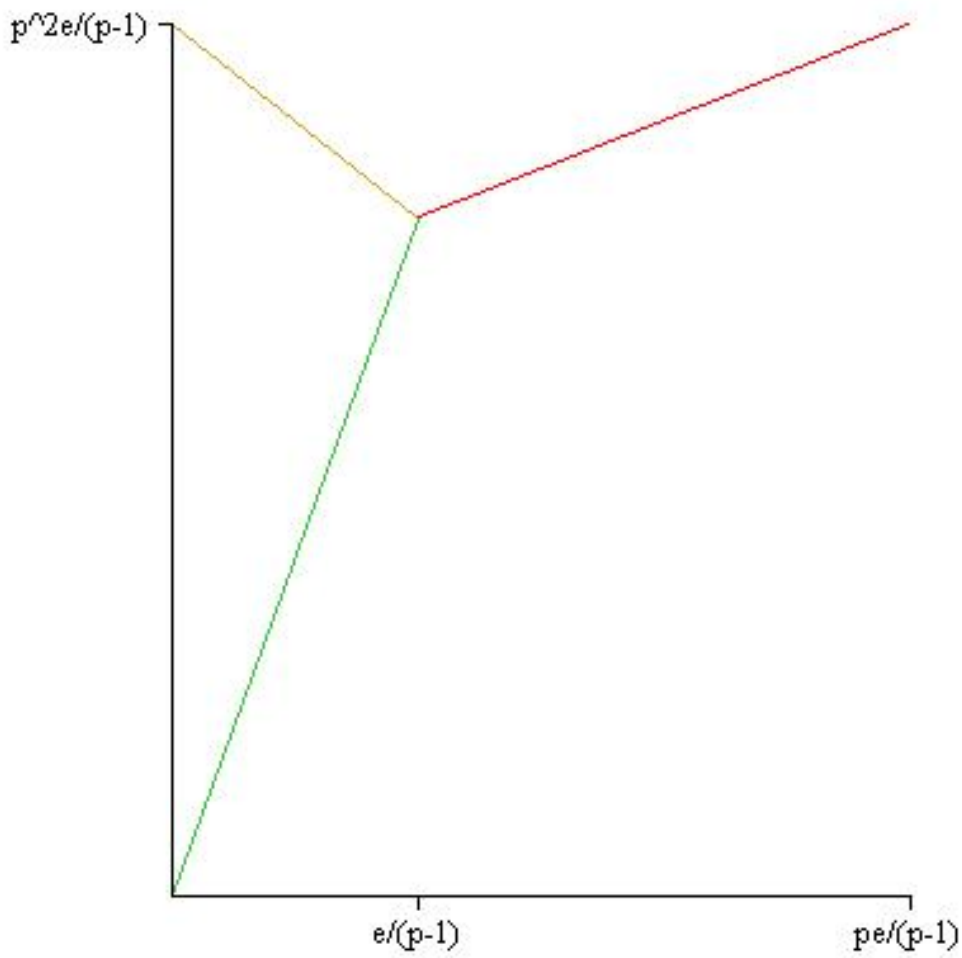
If K is a finite extension of $\mathbb{Q}_p$ then

$$1 \leq b_1 \leq \frac{pv_K(p)}{p-1}, \quad 1 \leq b_1 \leq \frac{p^2 v_K(p)}{p-1}$$

and if $b_1 \geq v_K(p)/(p-1)$ then $b_2 = b_1 + pv_K(p)$, otherwise "unstable ramification" (Wyman, 1969)

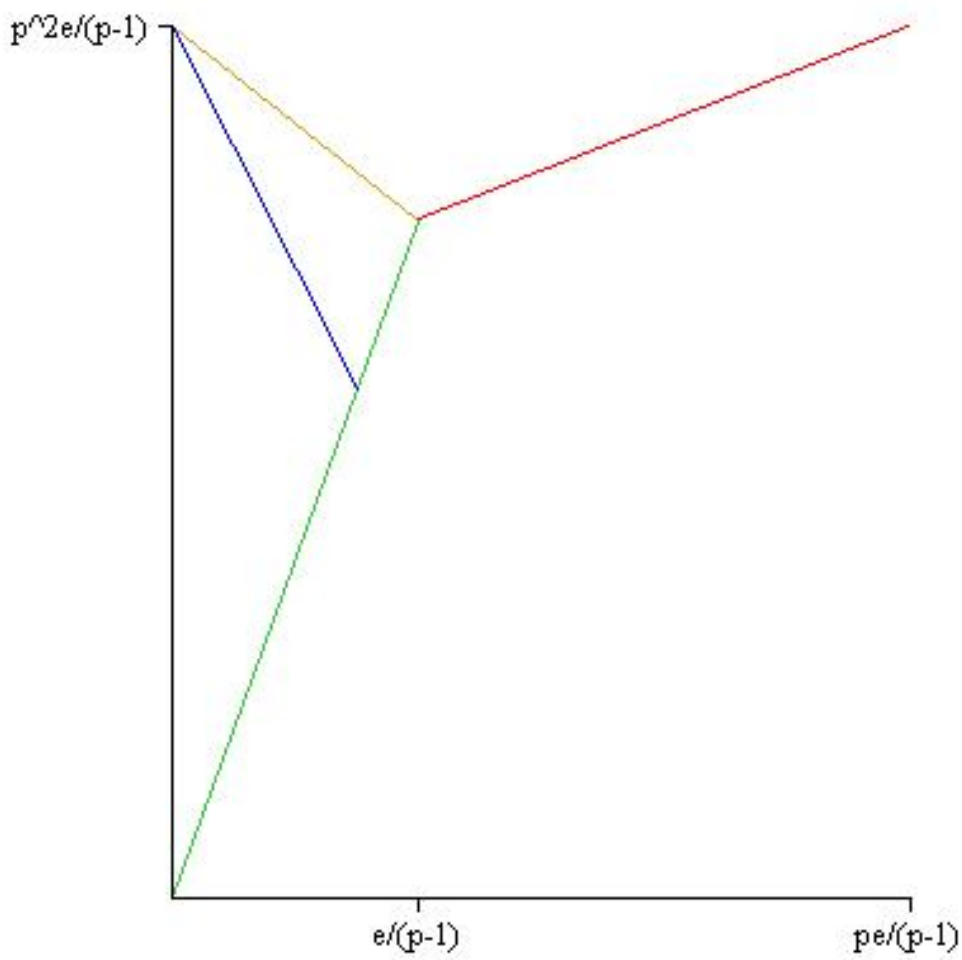
Picture in char 0: Possible ramification pairs (b_1, b_2)

$p = 3$



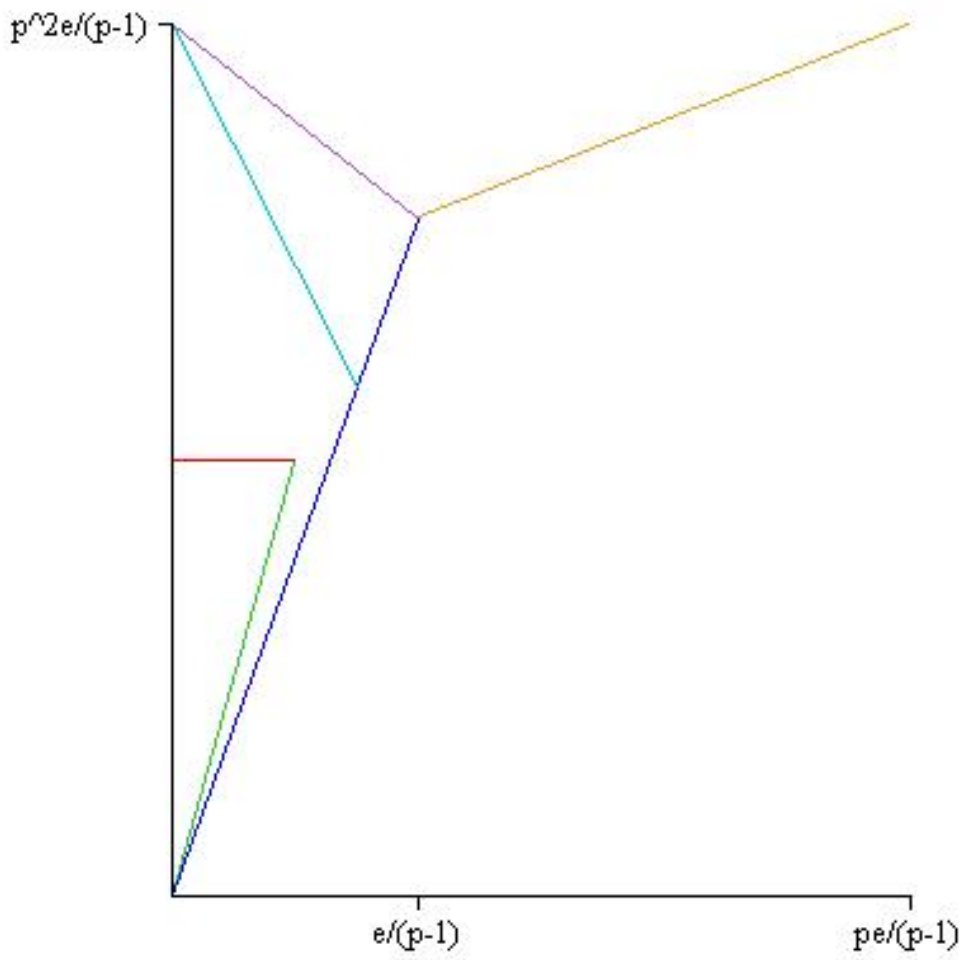
Picture in char 0: Possible ramification pairs (b_1, b_2)

$p = 3$ Artin-Schreier-Witt (Alex James)



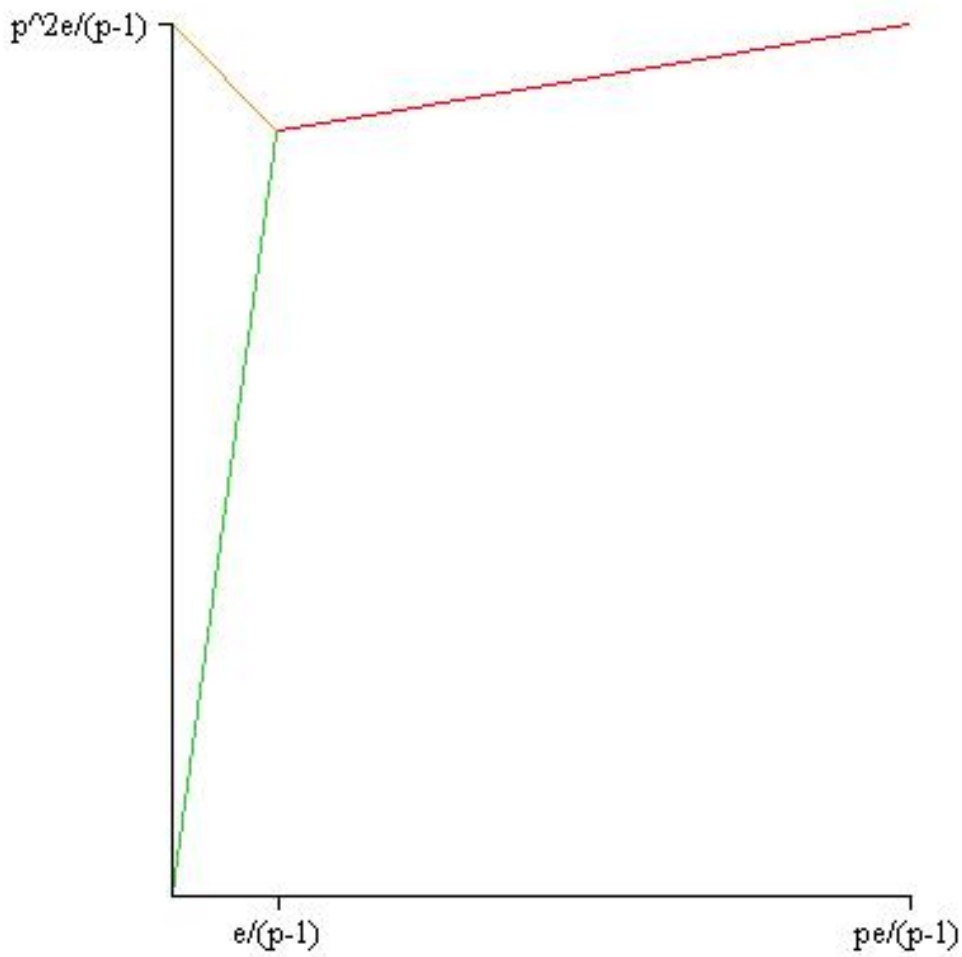
Picture in char 0: Possible ramification pairs (b_1, b_2)

$p = 3$ Galois scaffold



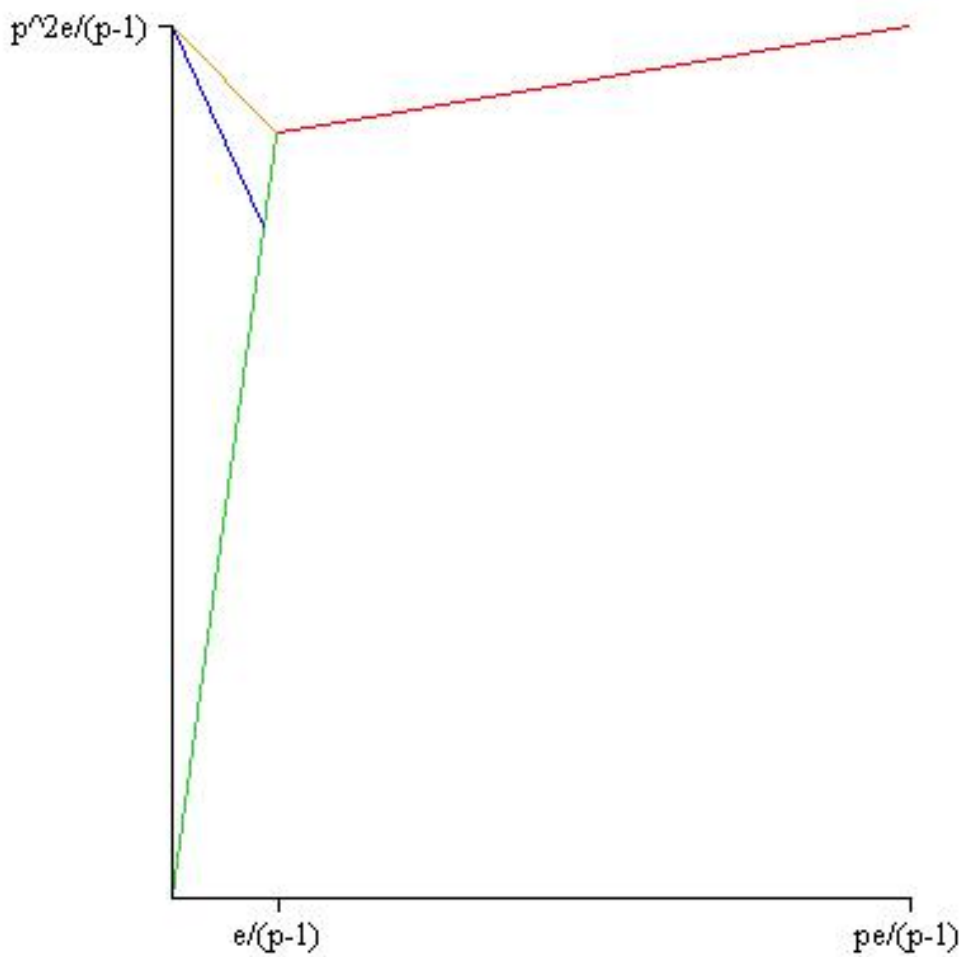
Picture in char 0: Possible ramification pairs (b_1, b_2)

$p = 7$



Picture in char 0: Possible ramification pairs (b_1, b_2)

$p = 7$ Artin-Schreier-Witt (Alex James)



Picture in char 0: Possible ramification pairs (b_1, b_2)

$p = 7$ Galois scaffold