Through a dihedral prism

Griff Elder

University of Nebraska at Omaha

June 2, 2023

(additive) Galois module structure

Let p be prime and let K be a local field of residue characteristic p. *e.g.*

- in characteristic 0: K is a finite extension of $\mathbb{Q}_p$, the p-adic numbers.
- in characteristic p: $K = \mathbb{F}((t))$, field of Laurent series with coefficients in a finite field $\mathbb{F}$ of characteristic p.

Let L/K be a finite, totally ramified Galois extension with $G = \mathrm{Gal}(L/K)$ a p-group

The normal basis theorem says that $L = K[G] \cdot \alpha$ for some $\alpha \in L$.

Towards an integral version: If there is an order $\mathcal{A}$ in $K[G]$ such that the ring of integers $\mathcal{O}_L = \mathcal{A} \cdot \alpha$ for some $\alpha \in \mathcal{O}_L$, this order $\mathcal{A}$ must be the *associated order*:

$$\mathcal{A}_{L/K} = \{x \in K[G] : x \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}.$$

We use "$\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \alpha$" and "$\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$" interchangeably.

This is the goal of (additive) GMS.

Snapshot: C_p-extensions

Theorem (F. Bertrandias, J.P. Bertrandias, M.J. Ferton, 1972)

Let K be a finite extension of $\mathbb{Q}_p$. Let L/K be a totally ramified extension of degree p with ramification break b. (Necessarily, $1 \leq b \leq \frac{pv_K(p)}{p-1}$)

1. If $p \mid b$, then $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$.
2. If $p \nmid b$, let $r(b) \equiv b \bmod p$ with $1 \leq r(b) \leq p-1$, then
   a. if $1 \leq b \leq \frac{pv_K(p)}{p-1} - 1$, then $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $r(b) \mid (p-1)$.
   b. if $b \geq \frac{pv_K(p)}{p-1} - 1$, $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $N \leq 4$, where N is the length of the continued fraction expansion

$$\frac{b}{p} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots \cfrac{1}{\cdots + \cfrac{1}{a_N}}}}$$

   with $a_N \geq 2$.

Theorem (A. Aiba, 2003)

In characteristic p, namely $K = \mathbb{F}((t))$, $v_K(p) = \infty$ and there is only one case: $p \nmid b$. Furthermore, $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $r(b) \mid (p-1)$.

Snapshot: C_p-extensions

Theorem (F. Bertrandias, J.P. Bertrandias, M.J. Ferton, 1972)

Let K be a finite extension of $\mathbb{Q}_p$. Let L/K be a totally ramified extension of degree p with ramification break b. (Necessarily, $1 \leq b \leq \frac{pv_K(p)}{p-1}$)

1. If $p \mid b$, then $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$.
2. If $p \nmid b$, let $r(b) \equiv b \bmod p$ with $1 \leq r(b) \leq p-1$, then
   a. if $1 \leq b \leq \frac{pv_K(p)}{p-1} - 1$, then $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $r(b) \mid (p-1)$.
   b. if $b \geq \frac{pv_K(p)}{p-1} - 1$, $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $N \leq 4$, where N is the length of the continued fraction expansion

$$\frac{b}{p} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots \cfrac{1}{\cdots + \cfrac{1}{a_N}}}}$$

   with $a_N \geq 2$.

Theorem (A. Aiba, 2003)

In characteristic p, namely $K = \mathbb{F}((t))$, $v_K(p) = \infty$ and there is only one case: $p \nmid b$. Furthermore, $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $r(b) \mid (p-1)$.

Snapshot: C_p-extensions

Theorem (F. Bertrandias, J.P. Bertrandias, M.J. Ferton, 1972)

Let K be a finite extension of $\mathbb{Q}_p$. Let L/K be a totally ramified extension of degree p with ramification break b. (Necessarily, $1 \le b \le \frac{pv_K(p)}{p-1}$)

1. If $p \mid b$, then $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$.
2. If $p \nmid b$, let $r(b) \equiv b \bmod p$ with $1 \le r(b) \le p-1$, then
   - (a) if $1 \le b \le \frac{pv_K(p)}{p-1} - 1$, then $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $r(b) \mid (p-1)$.
   - (b) if $b \ge \frac{pv_K(p)}{p-1} - 1$, $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $N \le 4$, where N is the length of the continued fraction expansion

$$\frac{b}{p} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots \cfrac{1}{\cdots + \cfrac{1}{a_N}}}}$$

     with $a_N \ge 2$.

Theorem (A. Aiba, 2003)

In characteristic p, namely $K = \mathbb{F}((t))$, $v_K(p) = \infty$ and there is only one case: $p \nmid b$. Furthermore, $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $r(b) \mid (p-1)$.

(a) char p is part of the char 0 picture. (b) "Galois scaffold"

Intuition of a Scaffold

L/K is a totally ramified p-extension. A is a K-algebra of the same size: $\dim_K(A) = \dim_K(L)$, with a K-action on L.

An *A-scaffold on L* consists of certain special elements in A which act on suitable elements of L in a way which is tightly linked to valuation.

The intuition: Given any positive integers b_i for $1 \leq i \leq n$ such that $p \nmid b_i$, there are elements $X_i \in L$ such that $v_L(X_i) = -p^{n-i}b_i$. Since the valuations, v_L, of the monomials

$$\mathbb{X}^a = X_n^{a_{(0)}} X_{n-1}^{a_{(1)}} \cdots X_1^{a_{(n-1)}} : 0 \leq a_{(i)} < p,$$

provide a complete set of residues modulo p^n and L/K is totally ramified of degree p^n, these monomials provide a convenient K-basis for L.

The action of A on L is clearly determined by its action on the $\mathbb{X}^a$.

So if there were $\Psi_i \in A$ for $1 \leq i \leq n$ such that each Ψ_i acts on the monomial basis element $\mathbb{X}^a$ of L as if it were the differential operator d/dX_i and the X_i were independent variables, namely if

$$\Psi_i \mathbb{X}^a = a_{(n-i)} \mathbb{X}^a / X_i,$$

then the monomials in the Ψ_i (with exponents bound $< p$) would furnish a convenient basis for A whose effect on the $\mathbb{X}^a$ would be easy to determine.

As a consequence, the determination of the associated order of a particular ideal $\mathfrak{P}_L^h$, and of the structure of this ideal as a module over its associated order, would be reduced to a purely numerical calculation involving h and the b_i. This remains true if equality is loosened to the congruence,

$$\Psi_i \mathbb{X}^a \equiv a_{(n-i)} \mathbb{X}^a / X_i \bmod (\mathbb{X}^a / X_i) \mathfrak{P}_L^{\mathfrak{c}}$$

for a sufficiently large "precision" $\mathfrak{c}$. The Ψ_i, together with the $\mathbb{X}^a$, constitute an A-scaffold on L. The formal definition focuses solely on valuation, remaining agnostic on the actual nature of the action.

Galois scaffolds

Ironically, the first scaffolds were **not** constructed in purely inseparable p-extensions where derivations occur naturally.

Those only arose when the "intuition" met Lindsay Childs. See (Byott, Childs, E., 2018) and (Koch, 2015),

...and this intuition took a long time to develop:

The first scaffolds were Galois scaffolds and arose for elementary abelian p-extensions (E., 2009), (Byott, E., 2013) in characteristic p.

Focused study of $C_p \times C_p$-extensions with Byott.

Although, Galois scaffolds for C_{p^2}-extensions were constructed in (Byott, E., 2013), it wasn't clear how to generalize the construction to C_{p^n}-extensions with $n \geq 3$.

That is... until (E., Keating, 2022).

Today I would like to talk about a further generalization (with Kevin) to all p-groups in characteristic p.

through the lense of one small group...

Dihedral extensions in characteristic 2

Let $K = \mathbb{F}((t))$ with $\mathbb{F}$ a finite field of characteristic 2. Let

$$D_8 = \langle \gamma, \sigma : \sigma^8 = \gamma^2 = 1, \gamma\sigma\gamma = \sigma^{-1} \rangle$$

Proposition. L is a totally ramified D_8-extension over K if and only if

1. there is a vector $(\alpha, \beta_1, \beta_2, \beta_3) \in K^4$ satisfying certain conditions: $t = -v_K(\alpha) > 0$, $w_1 = -v_K(\beta_1) > 0$ both odd and furthermore, if $t = w_1$, then $-v_K(\alpha + \beta_1) = t = w_1$, meanwhile, for $i = 2, 3$ and $\beta_i \neq 0$, either $w_i = -v_K(\beta) = 0$ or $w_i = -v_K(\beta) > 0$ is odd, and
2. $L = K(y, x_1, x_2, x_3)$ for some $y, x_1, x_2, x_3 \in K^{\mathrm{sep}}$ such that

$$\begin{aligned} y^2 - y &= \alpha, \\ x_1^2 - x_1 &= \beta_1, \\ x_2^2 - x_2 &= \beta_1 x_1 + \beta_1 y + \beta_2, \\ x_3^2 - x_3 &= \beta_1^3 x_1 + \beta_1 x_1^3 + \beta_1\beta_2 x_1 + \beta_1 x_1 x_2 + \beta_2 x_2 \\ &\quad + \beta_1^2 x_1 y + \beta_1 x_2 y + (\beta_2 + \beta_1\beta_2 + \beta_1^2\alpha + \beta_1) y + \beta_3. \end{aligned}$$

Since L is a C_8-extension over $K(y)$, it is associated with a Witt vector of length 3

$$(\beta_1,\ \beta_1 y + \beta_2,\ (\beta_2 + \beta_1\beta_2 + \beta_1^2\alpha + \beta_1 + \alpha) y + \beta_3) \in W_3(K(y)).$$

Discussion

We arrive at this result, by observing that $Z(D_8) = \langle \sigma^4 \rangle$ and $D_8/Z(D_8) \cong D_4$.

Furthermore, $Z(D_4) = \langle \bar{\sigma}^2 \rangle$ and that $D_4/Z(D_4) \cong C_2 \times C_2$.

Thus starting with the $C_2 \times C_2$-extension $K(y, x_1)$, we build up a D_4-extension $K(y, x_1, x_2)$ by solving one embedding problem.

$$\begin{aligned} y^2 - y &= \alpha, \\ x_1^2 - x_1 &= \beta_1, \\ x_2^2 - x_2 &= \beta_1 x_1 + \beta_1 y + \beta_2. \end{aligned}$$

Then we build up the D_8-extension $K(y, x_1, x_2, x_3)$ by solving another.

$$\begin{aligned} x_3^2 - x_3 = {} & \beta_1^3 x_1 + \beta_1 x_1^3 + \beta_1\beta_2 x_1 + \beta_1 x_1 x_2 + \beta_2 x_2 \\ & + \beta_1^2 x_1 y + \beta_1 x_2 y + (\beta_2 + \beta_1\beta_2 + \beta_1^2\alpha + \beta_1) y + \beta_3. \end{aligned}$$

Theorem (Witt, 1936)
These embedding problems (for p-groups in characteristic p) are all solvable.

Since these Artin-Schreier constants are so complicated, we can simplify them using the formalism of Witt vectors. Recall that Witt addition results produces certain polynomials

$$D_1(X_1; Y_1) = \frac{X_1^p + Y_1^p - (X_1 + Y_1)^p}{p},$$
$$D_1(X_1, X_2; Y_1, Y_2) = \frac{X_1^{p^2} + Y_1^{p^2} - (X_1 + Y_1)^{p^2} + p(X_2^p + Y_2^p - (X_2 + Y_2 + D_1(X_1; Y_1))^p}{p^2}.$$

The Witt vector corresponds to the C_8-extensions $L/K(y)$.

$$(\beta_1,\ \beta_1 y + \beta_2,\ (\beta_2 + \beta_1\beta_2 + \beta_1^2\alpha + \beta_1 + \alpha)y + \beta_3) \in W_3(K(y)).$$

(Save this observation for later.)

Theorem (Saltman, 1978)
For each p-group G, there exist polynomials similar to the Witt polynomials for C_{p^n}-extensions. These polynomials, which depend only upon the group G, can be used to construct all such G-extensions. Let's call them Saltman polynomials S_i.

In our example with a group of order 2^4 there are four Saltman polynomials S_0, S_1, S_2, S_3 and a vector $(\alpha, \beta_1, \beta_2, \beta_3) \in K^4$ such that $y^2 - y = S_0 + \alpha$, $x_1^2 - x_1 = S_1(y) + \beta_1$ with

$$S_0 = 0, \quad S_1(y) = 0 \in \mathbb{F}_p[y],$$

$x_2^2 - x_2 = S_2(y, x_1) + \beta_2$ with

$$S_2(y, x_1) = \beta_1 x_1 + \beta_1 y = (x_1^2 - x_1)x_1 + (x_1^2 - x_1)y \in \mathbb{F}_p[y, x_1],$$

and $x_3^2 - x_3 = S_3(y, x_1, x_2) + \beta_3$ with

$$\begin{aligned} S_3(y, x_1, x_2) &= \beta_1^3 x_1 + \beta_1 x_1^3 + \beta_1\beta_2 x_1 + \beta_1 x_1 x_2 + \beta_2 x_2 \\ &\qquad + \beta_1^2 x_1 y + \beta_1 x_2 y + (\beta_2 + \beta_1\beta_2 + \beta_1^2\alpha + \beta_1)y \\ &= (x_1^2 - x_1)^3 x_1 + (x_1^2 - x_1)x_1^3 + (x_1^2 - x_1)(x_2^2 - x_2)x_1 + (x_1^2 - x_1)x_1 x_2 + (x_2^2 - x_2)x_2 \\ &\qquad + (x_1^2 - x_1)^2 x_1 y + (x_1^2 - x_1)x_2 y \\ &\quad + ((x_2^2 - x_2) + (x_1^2 - x_1)(x_2^2 - x_2) + (x_1^2 - x_1)^2(y^2 - y) + x_1^2 - x_1)y \in \mathbb{F}_p[y, x_1, x_2]. \end{aligned}$$

Record that the total degrees of S_2 and S_3 are $l_2 = 3$ and $l_3 = 7$, respectively.

Generic scaffolds

Theorem. (with Kevin Keating) Let K_0 be a local field of characteristic p and let G be a p-group with a composition series chosen. The result adjusts (Saltman, 1978) slightly and describes all G-extensions K_n/K_0: There exist $x_i \in K_0^{\mathrm{sep}}$ such that for $1 \leq i \leq n$ $K_i = K_0(x_1, \ldots, x_i)$ with $x_i^p - x_i \in K_{i-1}$ and chosen composition series

$$\{\mathrm{Gal}(K_n/K_i) : 0 \leq i \leq n\}.$$

This description uses Saltman polynomials $S_i \in \mathbb{F}_p[X_1, \ldots, X_{i-1}]$ for $1 \leq i \leq n$. Polynomials that depend only on the group G, and a Saltman vector $(\beta_1, \ldots, \beta_n) \in K_0^n$ such that

$$x_i^p - x_i = S_i(x_1, \ldots, x_{i-1}) + \beta_i.$$

Then restricting the Saltman vector $(\beta_1, \ldots, \beta_n) = \beta_1 \cdot (1, \omega_2^{p^{n-1}}, \ldots, \omega_n^{p^{n-1}})$ with $p \nmid v_K(\beta_1)$ and $v_K(\beta_i) = -u_i$ such that $0 > -u_1 > -u_2 > \cdots > -u_n$. If we assume that the integers b_i are defined recursively by $b_1 = u_1$ and $b_i = b_{i-1} + p^{i-1}(u_i - u_{i-1})$ and are spread sufficiently apart:

$$b_i > -p^{n-1} v_K(S_i(x_1, \ldots, x_{i-1})) - p^{n-i} b_{i-1} + p^{n-1} u_{i-1}, \tag{1}$$

$$b_i > p^{n-1} u_{i-1}, \tag{2}$$

for all $2 \leq i \leq n$, then $\{\mathrm{Gal}(K_n/K_i) : 0 \leq i \leq n\}$ is the list of ramification groups, $u_1, \ldots, u_n$ are the upper ramification breaks, $b_1, \ldots, b_n$ are the lower ramification breaks and K_n/K_0 admits a Galois scaffold with precision $\mathfrak{c}$ equal to the minimum gap of (1), (2).

Additionally, $v_K(x_i) = -p^{-1}u_i$. Using the crudist upper bound, we have

$$l_i u_{i-1} \geq -v_K(S_i(x_1, \ldots, x_{i-1}))$$

where l_i is the total degree of S_i. Thus we can replace (1) and (2) with

$$b_i > p^{n-2}u_{i-1} - p^{n-i}b_{i-1} + p^{n-1}u_{i-1}$$

for $2 \leq i \leq n$ with the result that we have a Galois scaffold with precision $\mathfrak{c}$ the minimum of that gaps among these inequalities.

Note that until we know what group G we are working with, and know the Saltman polynomials, we can't do much better than this.

On the other hand, we can do much better if we know the *ramification spectrum* for the particular group.

Namely, in the case of D_8-extensions, if we knew the set

$$\{u_1, u_2, u_3, u_4\}$$

of all realizable upper ramification breaks (equivalently, the set $\{l_1, l_2, l_3, l_4\}$ of lower ramification breaks).

Towards ramification breaks

Given a prime element $\pi_L \in L$ the ramification groups (in lower numbering) are given by

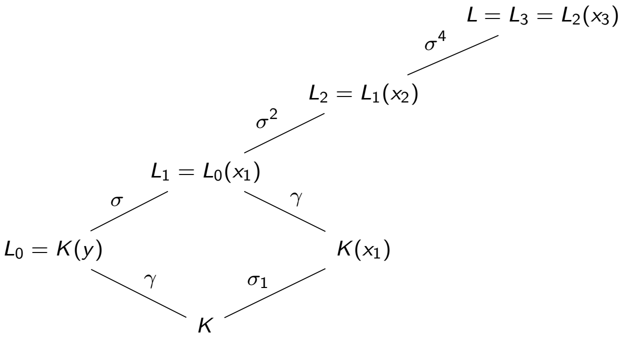
$$G_i = \{\sigma \in \mathrm{Gal}(L/K) : v_L((\sigma - 1)\pi_L) \geq i + 1\}.$$

Ramification breaks b occur when $G_b \supsetneq G_{b+1}$. Since L/K is totally ramified, $b \geq 1$.

Ch. IV in *Local Fields* by Serre: If $\sigma_1 \in G_{i_1}$ and $\sigma_2 \in G_{i_2}$, then $\sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1} \in G_{i_1+i_2+1}$. Thus the center contains smallest nontrivial ramification group (largest break number).

Since $Z(D_8) = \langle\sigma^4\rangle$ and $Z(D_8/\langle\sigma^4\rangle) = \langle\bar{\sigma}^2\rangle$ both have order $p = 2$,

$$\langle\sigma^4\rangle = G^{u_4} = G_{l_4} \text{ and } \langle\sigma^2\rangle = G^{u_3} = G_{l_3} \text{ are ramification groups.}$$



This means that the first two lower ramification breaks of L_3/K, namely $l_1 \leq l_2$, are also the lower ramification breaks of L_1/K.

Meanwhile, recall the Hasse-Herbrand function

$$\phi_{L/K}(x) = \int_0^x \frac{dt}{[G_0 : G_t]},$$

which allows us to define the upper ramification numbering, $G_i = G^{\phi_{L/K}(i)}$. The lower numbering passing nicely to subgroups $H_i = G_i \cap H$. Upper numbering passes nicely to quotients $(G/N)^i = (G^i N)/N$.

The upper ramification breaks for L_2/K are thus the three smallest upper ramification breaks for L_3/K. These were determined by Bradley Weaver (2018) in his solution of the *local-lifting problem* for D_4; namely, his proof that D_4 is a *local Oort group for* $p = 2$.

Our contribution then is the fourth upper ramification break.

Our approach

Determine the ramification breaks of the C_8-extensions L_3/L_0 based upon the Witt vector:

$$(\beta_1,\ \beta_1 y+\beta_2,\ (\beta_2+\beta_1\beta_2+\beta_1^2\alpha+\beta_1+\alpha)y+\beta_3)\in W_3(K(y)).$$

Big "If": If our Witt vector was reduced to $(\rho_1,\ \rho_2,\ \rho_3)\in W_3(K(y))$; that is, if we had

$$(\rho_1,\ \rho_2,\ \rho_3)\equiv(\beta_1,\ \beta_1 y+\beta_2,\ (\beta_2+\beta_1\beta_2+\beta_1^2\alpha+\beta_1+\alpha)y+\beta_3)\pmod{W_3(K(y))^{\wp}}$$

where first $\rho_1\in L_0$ has maximal valuation modulo $W_3(K(y))^{\wp}=\{\phi(\vec{x})\ominus\vec{x}:\vec{x}\in K(y)\}$, then ρ_2 is adjusted so that it has maximal valuation modulo $W_3(K(y))^{\wp}$, etc., where ϕ is the Frobenius and $\ominus$ is Witt vector subtraction.

...if so, then we can use a very useful technical result in L. Thomas, 2005: If u_2 is the second upper ramification break in the C_4-extension associated with the reduced Witt vector $(\rho_1,\ \rho_2)$, then $2u_2$ is the third upper break in the C_8-extension associated with $(\rho_1,\ \rho_2,\ 0)$.

In general: From $(\rho_1,\dots,\rho_n)$ to $(\rho_1,\dots,\rho_n,0)$ largest upper break goes from u to pu.

Thus the largest upper break in the C_8-extension associated with reduced vector $(\rho_1,\ \rho_2,\ \rho_3)$ is

$$u_3=\max\{2u_2,w_3\}$$

where $w_3=-v_K(\rho_3)$. Remember: L. Thomas' result is for cyclic extensions.

Upper breaks $u_1 \leq u_2 < u_3 < u_4$ of L_3/K

A lot of very technical calculations go into reducing

$$(\beta_1,\ \beta_1 y + \beta_2,\ (\beta_2 + \beta_1\beta_2 + \beta_1^2\alpha + \beta_1 + \alpha)y + \beta_3) \in W_3(K(y)).$$

Once completed, the result is familiar: $u_1 \leq u_2 < u_3$ agree with Weaver's result, moreover...

Theorem $u_4 = \max\{2u_3, w_3\}$ where u_3 is the largest upper ramification break of L_2/K and $w_3 = -v_K(\beta_3)$ for the coordinate $\beta_3 \in K$ added to the D_4-Saltman vector $(\alpha, \beta_1, \beta_2)$ to produce the D_8-Saltman vector $(\alpha, \beta_1, \beta_2, \beta_3)$.

Using this we can strengthen the result with Keating when it is applied to D_8-extensions.

But perhaps more interesting:

D_8 has the same ramification spectrum as two other groups of order 16: the semidihedral and generalized quaternion group.

take-away point:

"You can't know a group by its ramification spectrum."

Wild guessing

Perhaps what we saw in D_8-extensions, namely $u_4 \geq 2u_3$, happens more generally:

If $u_1 \leq u_2 < u_3 < \cdots < u_n$ are the upper ramification breaks for a $D_{2^{n-1}}$-extension L/K then $u_1 \leq u_2 < u_3$ are as in Weaver's result. And maybe for $3 < i \leq n$,

$$u_i = \max\{2u_{i-1}, w_{i-1}\}$$

where $w_i = -v_K(\beta_i)$ for the coordinate $\beta_i \in K$ in the $D_{2^{n-1}}$-Saltman vector $(\alpha, \beta_1, \beta_2, \ldots, \beta_{n-1})$.

Wild guess-a-llaries. This would give an arbitrarily large family of totally ramified p-extensions where the upper ramification breaks are all integers.

$p = 2$ is very different from characteristic $p > 2$.

Plug "A converse to the Hasse-Arf theorem" w/ Keating.

Thank you!

...and thank you for participating in

Hopf algebras & Galois module theory 2023