Polishing two old problems

Griff Elder

University of Nebraska at Omaha

May 18, 2014

The week's focus

K is a local field,

complete with respect to a discrete valuation v_K

normalized so that $v_K(K^\times) = \mathbb{Z}$

Let $\mathfrak{O}_K = \{\alpha \in K : v_K(\alpha) \geq 0\}$ be the valuation ring, with

$\mathfrak{P}_K = \{\alpha \in K : v_K(\alpha) > 0\}$, its maximal ideal,

and $\kappa = \mathfrak{O}_K/\mathfrak{P}_K$ its residue field

Assume the residue field κ has characteristic p.

Examples:

- $K = \kappa((t))$, *local function fields*;
- $K/\mathbb{Q}_p$ finite extension of the p-adic numbers, *local number fields*.

We are interested in

- field extensions L/K of degree p^n, *esp.* the totally ramified ones;
- Hopf-algebras over K of dimension p^n, *esp.* those that act on L/K.

Idea: Char. 0 approximates char. p

When a result in characteristic 0 holds under the requirement that $v_K(p)$ is *large enough*, it *ought* to be a characteristic p result.

Conversely, *every* characteristic p result *ought* to hold in characteristic 0, *once* $v_K(p)$ is assumed *large enough*.

Why?

The characteristic is p if and only if $v_K(p)$ is as large as it can be, namely

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

Simple examples:

- Artin-Schreier equations in characteristic zero;
- Ramification in C_{p^2}-extensions;
- Hopf orders in $K[C_p]$.

MacKenzie and Whaples, 1956: "Artin-Schreier equations in characteristic zero"

Recall that given a Galois extension L/K, with $G = \mathrm{Gal}(L/K)$, there is a ramification filtration

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

Integers i such that $G_i \supsetneq G_{i+1}$ are ramification numbers.

It is known that if K is a finite extension of $\mathbb{Q}_p$, the ramification number b for the cyclic extension L/K of degree p satisfies

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

MacKenzie and Whaples proved that if $(p-1)b/p < v_K(p)$, then L is Artin-Schreier: $L = K(x)$ where x satisfies an Artin-Schreier equation, *just like when K has characteristic p*.

In particular, if L/K is ramified (thus totally ramified), then $b > 0$ and WLOG there is a $\beta \in K$ with $v_K(\beta) = -b$ such that $x^p - x = \beta$.

Ramification in C_{p^2}-extensions

There are necessarily two ramification break numbers $b_1 < b_2$. Assuming L/K is totally ramified, the pairs (b_1, b_2) can be plotted:

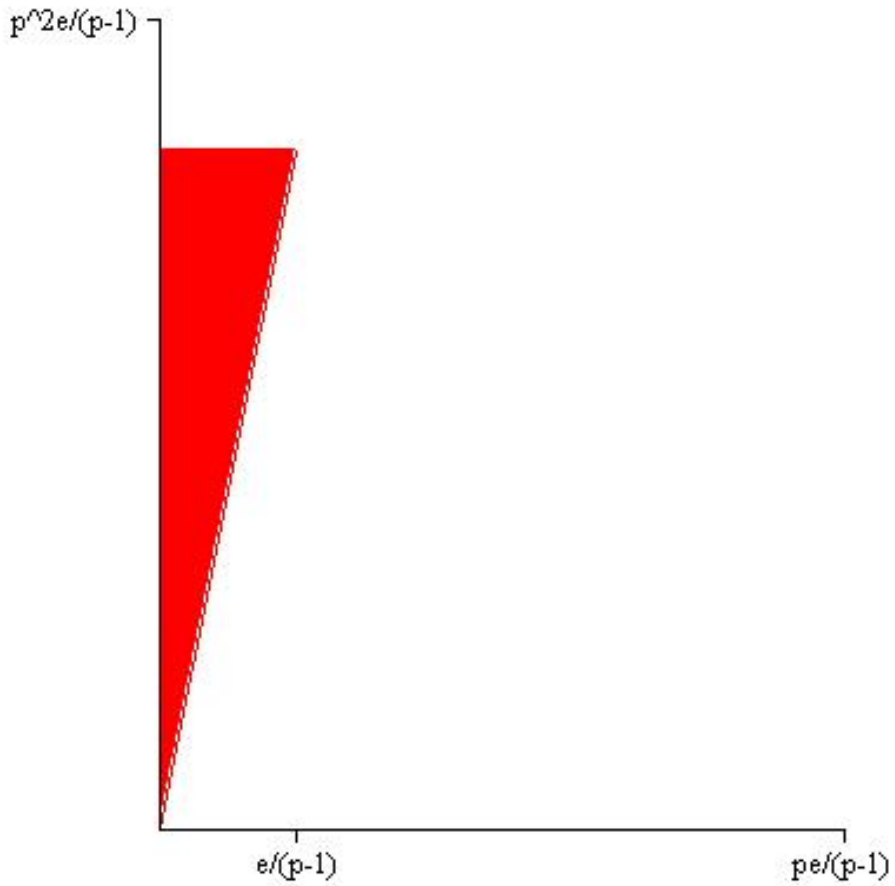


Figure: Char. p means $e = v_K(p) = \infty$

Ramification in C_{p^2}-extensions

There are necessarily two ramification break numbers $b_1 < b_2$. Assuming L/K is totally ramified, the pairs (b_1, b_2) can be plotted:

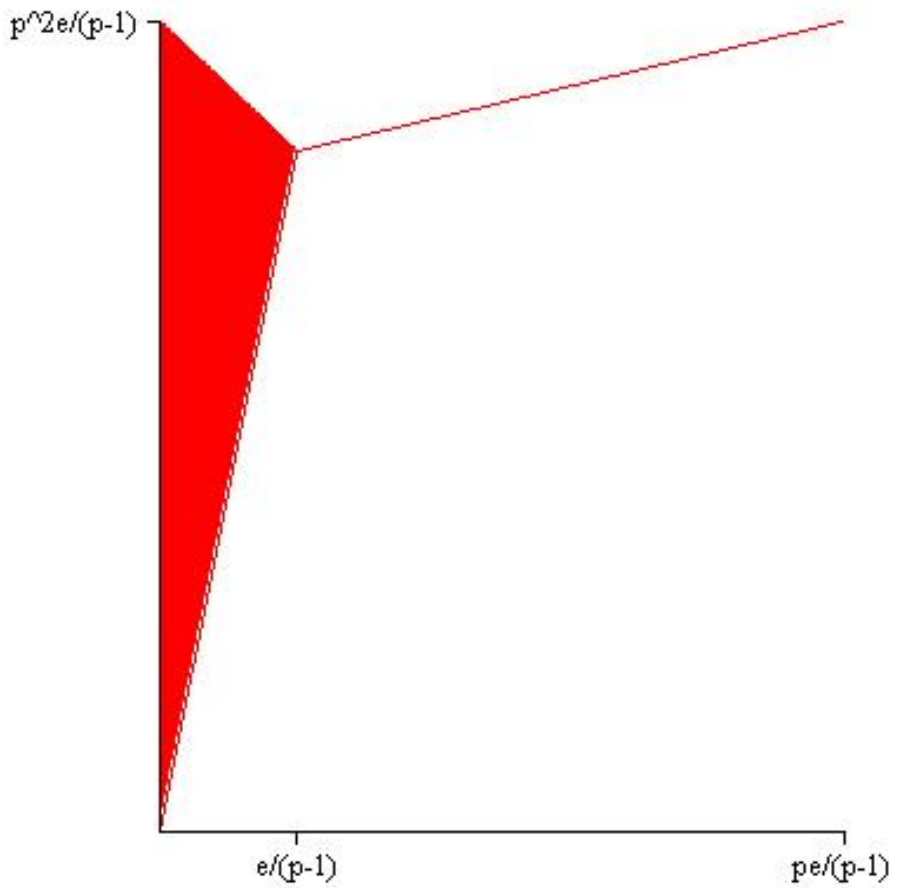


Figure: Char. 0 means $e = v_K(p) < \infty$

In characteristic p, we are talking about all positive integer points (b_1, b_2) relatively prime to p, namely $p \nmid b_1, b_2$, such that

$$b_2 \geq (p^2 - p + 1)b_1.$$

And further: if $b_2 > (p^2 - p + 1)b_1$, then $b_2 \not\equiv (p-1)b_1 \bmod p^2$.

In characteristic 0, we impose restrictions that are vacuous in char. p.

- For $1 \leq b_1 \leq \frac{v_K(p)}{p-1}$,

$$b_2 \leq p^2 \frac{v_K(p)}{p-1} - (p-1)b_1;$$

- For $\frac{v_K(p)}{p-1} \leq b_1 \leq p\frac{v_K(p)}{p-1}$,

$$b_2 = b_1 + pv_K(p).$$

This last situation is what Wyman, 1969 refers to as *stable ramification*, char. 0 phenomona does not occur in char. p for the simple-minded reason that there are no integers b_1 satisfying $\infty \leq b_1 \leq \infty$.

Tate and Oort, 1970: Hopf orders in $K[C_p]$.

The group ring $K[G]$ is a Hopf algebra over K with comultiplication, counit and antipode defined by

$$\Delta(\sigma) = \sigma \otimes \sigma, \quad \epsilon(\sigma) = 1, \quad \lambda(\sigma) = \sigma^{-1}$$

for all $\sigma \in G$.

A *Hopf order* in $K[C_p]$ is a Hopf algebra, defined over $\mathfrak{O}_K$ and contained in $K[C_p]$ (but with full rank p), with Δ, ϵ and λ as in $K[C_p]$.

Tate and Oort classified the Hopf orders in $K[C_p]$ with $\langle\sigma\rangle = C_p$. They are all Larson orders:

$$\mathfrak{O}_K\left[\frac{\sigma - 1}{\pi_K^M}\right] \quad \text{where} \quad 0 \leq M \leq \frac{v_K(p)}{p-1}.$$

The result holds in both characteristics, except that in char. p the upper bound on M holds vacuously.

The first old problem being polished

Beginning with Tate-Oort...

Determine all the Hopf orders in a given Hopf algebra H, defined over K.

More on this topic on Thursday.

I just want to record an observation. Let $H = K[G]$ for G a p-group.

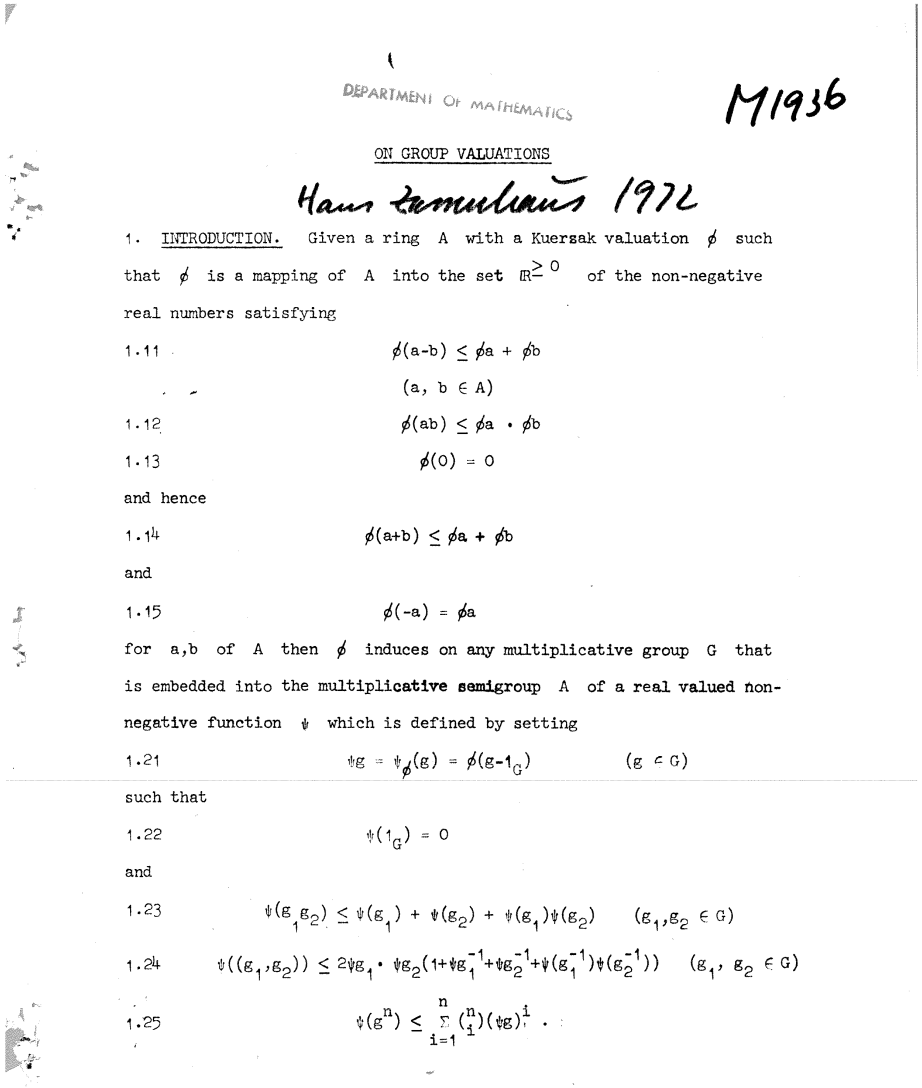
Larson, 1976 defines a *group valuation*, a function $v : G \to \mathbb{Z}_{>0} \cup \{\infty\}$ that satisfying certain properties.

He mentions that "group valuations were first discussed by Zassenhaus", and then points to a unpublished paper.

At the end of April, I became curious and emailed Richard Larson. His reply was that: "Probably there were informal discussions with him..."

Were they never written down??

David Goss contacts Sudarshan Sehgal, who shares 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 $$\psi(g^n) \leq \sum_{i=1}^{n} \binom{n}{i} (\psi g)^i .$$

Along with long hair and bell bottoms...

The 1970's was about group valuations, or what are also called

p-valuations.

Larson, 1976 defines a *group valuation*, a function $v : G \to \mathbb{Z}_{>0} \cup \{\infty\}$ that satisfying certain properties:

1. $v(g) = \infty$ if and only if $g = 1$,
2. $v(gh) \geq \min\{v(g), v(h)\}$
3. $v([g, h]) \geq v(g) + v(h)$
4. $v(g^p) \geq pv(g)$

Include the *order-bounded* property, $v(g) \leq \frac{v_K(p)}{\phi(|g|)}$, then every group valuation determines a Hopf order. Conversely, every Hopf order determines a group valuation that determines a distinguished Hopf sub-order, a Larson order, within the given Hopf order.

But ignore the order-bounded property for the moment.
Assume $v(g) \geq 2$, then define $w(g) = \log_p(v(g))$ is a p-valuation.

p-valuations are functions $w : G \to (0, \infty]$ that satisfying certain properties:

1. $w(g) = \infty$ if and only if $g = 1$,
2. $w(gh) \geq \min\{w(g), w(h)\}$
3. $w([g, h]) \geq w(g) + w(h)$
4. $w(g^p) \geq w(g) + 1$

When G is abelian, this definition appears in Richman and Walker, 1979. They are studying infinite abelian groups. They use additive notation for the group operation. And as Richman states in his 1976 *A guide to valuated groups*, "If you stare at heights long enough you will begin to see valuations". Importantly, in these groups, multiplication by p moves you "up" into the group. Interestingly, in 1976 Richman and Walker prove that if you have any valuated group embeds in a group where the valuation is a height.

For Richman and Walker, valuations with equality $w(g^p) = w(g) + 1$ are associated with *free valuated groups*.

Take-away point: "height" has an intuition, and this intuition may be useful when we think about group valuations.

p-adic Lie groups

If we stick with the *free group valuation* property, $w(g^p) = w(g) + 1$, but return to nonabelian groups, we have a p-valuation in the sense of the book of Schneider, 2011.

Except that we also need the lower bound

$$w(g) > \frac{1}{p-1},$$

which I assume is a specialization of $\frac{v_K(p)}{p-1}$ because apparently Schneider is working over $K = \mathbb{Q}_p$. This inequality comes up when he needs the exponential series to converge.

Interestingly, Schneider proves that any p-valuable pro-p-group G carries a unique structure over $\mathbb{Q}_p$, which makes it into a p-adic Lie group. Conversely, any p-adic Lie group G contains a compact open subgroup $G' \subseteq G$ and an integer valued p-valuation w on G' defining the topology of G' where G' is "special" for G (technical relationship omitted).

Lazard and Ramification Theory

Are there any truly new ideas?

Calling a group valuation is apparently a 1970's thing, which goes back to Zassenhaus, but the *properties* of a p-valuation weren't new. They are satisfied by

$$i_G(\sigma) = v_L((\sigma - 1)\pi_L),$$

recalling now the definition of the ramification filtration

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

for the Galois group of the totally ramified extension L/K of local fields.

Some thoughts...

1. Could Lazard be that "perspective, that vantage point from which it all becomes simple – so simple as to possibly be trivial." *Wishful thinking perhaps...* And unfortunately, it is unlikely that I will ever know. Except that..., Lazard is evocative in a way that seems likely to lead someplace interesting.
2. Thinking of the ramification filtration in terms of heights is something new to my way of thinking, which has me wondering where the perspective might lead. In particular, there is a whole literature of heights for infinite abelian groups... Hmm.
3. What is the connection between Koch and Malagon, 2007 on *bounded order, p-adic group valuations* (*a lá* Larson) and the work of Miki, Maus, Wyman and Marshall on ramification break numbers? In some sense, all this is concerned with values taken by group (p-)valuations.

The other old problem: Galois module theory

Normal Basis Theorem: Given any finite, Galois extension of fields, L/K, there is an element $\alpha \in L$ such that $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}$ is a K-basis for L. *i.e.*

$$L = K[\mathrm{Gal}(L/K)]\alpha.$$

Timeline:

1850 Conjectured, by Eisenstein, for finite fields.

1888 Proven, by Hensel, for finite fields.

- Used by Dedekind in his work on discriminants of number fields.

1932 Proven, by E. Noether, for certain infinite fields.

1932 Uniform proof by Deuring for all fields.

Also in 1932, Noether considers the analogous question for rings of integers in number fields. Is there an $\alpha \in \mathfrak{O}_L$ such that $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}$ is a $\mathfrak{O}_K$-basis for $\mathfrak{O}_L$? *i.e.*

$$\mathfrak{O}_L = \mathfrak{O}_K[\mathrm{Gal}(L/K)]\alpha?$$

local Galois module theory

Noether finds, in 1932, that there isn't an $\alpha \in \mathfrak{O}_L$ such that

$$\mathfrak{O}_L = \mathfrak{O}_K[\mathrm{Gal}(L/K)]\alpha,$$

unless L/K is either unramified, or, if ramified, then only tamely ramified.

But then in 1959, Leopoldt finds, for absolutely abelian extensions $L/\mathbb{Q}$, that if you replace the group ring $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ with the larger "associated order"

$$\mathcal{A} = \{x \in \mathbb{Q}[\mathrm{Gal}(L/\mathbb{Q})] : x\mathfrak{O}_L \subseteq \mathfrak{O}_L\},$$

there is an $\alpha \in \mathfrak{O}_L$ such that

$$\mathfrak{O}_L = \mathcal{A}\alpha,$$

regardless of ramification.

Noether's work directs us toward totally ramified p-extensions (the opposite of tame is wild, and these are as wild as possible). Leopoldt gives us the "correct" question to ask.

Totally ramified p-extensions

There is something about totally ramified p-extensions that overcomes the

separable – inseparable divide.

We will see this when we talk about scaffolds, but I want to point out its utility in ramification theory, where *indices of inseparability* provide a mechanism that addresses a basic problem...

In the ramification filtration of a totally ramified extension L/K, quotients of consecutive ramification groups G_i/G_{i+1} are elementary abelian p-groups. The problem is that $|G_i/G_{i+1}| > p$ is possible, in which case there are two elements of the Galois group σ_1, σ_2 (independent: neither generated by the other) such that the p-valuation yields $i_G(\sigma_1) = i_G(\sigma_2)$. The p-valuation has a *singularity*.

Blundering ahead, the *indices of inseparability* of Fried, 1974 and Heiermann, 1996 is "somehow" concerned with the "resolution of these singularities". And does so by thinking about a totally ramified p-extensions as though they are purely inseparable. (I'm *blowing smoke*)

Keeping things superficial

Compare

ramified, *inseparable*, degree p with ramified, *Galois*, degree p.

In both cases, WLOG there is a $\beta \in K$ with $p \nmid v_K(\beta) < 0$, such that the extension L/K is $K(x)/K$ with either

$$x^p = \beta \text{ or } x^p - x = \beta.$$

In either case, $v_L(x) = v_K(\beta) < 0$.

In particular, $v_L(x^p) < v_L(x)$. So it "makes sense" to think of the Galois extension as being somehow "inseparable modulo $x\mathfrak{O}_L$".

This is as much as I truly understand about indices of inseparability, *except* Keating, 2014 links indices of inseparability with refined ramification, an invariant defined in Byott and Elder, 2005 and 2009 that is tailored to similarly "resolve singularities in the ramification p-valuation" but this time for the purposes of Galois module theory

Idea: Totally ramified p-extensions approx. inseparable

A circle of ideas seems to be emerging. The more I learn, the tighter the circle appears, which makes me think that there has just *got to be a perspective from which it is all "oh, so obvious!"*

One key component seems to be that totally ramified, Galois, p-extensions L/K *with ramification numbers that are congruent modulo* $[L : K]$

are approximately inseparable,

namely that they resemble purely inseparable extensions of the same size attached to similar invariants.

Intuition of a Scaffold

L/K is a totally ramified p-extension. A is a K-algebra A 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

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

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,

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

for a sufficiently large "tolerance" $\mathfrak{T}$. 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.

From this *perspective*, it is "obvious" that scaffolds should appear naturally in the setting of higher derivations acting on purely inseparable extensions. It is obvious *now*. See Byott, Childs and Elder, preprint. See Alan's Thursday talk.

In wasn't at all obvious back in 2005-ish, when motivated by some nice Galois module structure in $C_p \times C_p$-extensions and a conversation with Dave (char. $p \leftrightarrow$ char. 0), I came up with this interesting construction that had these nice properties, which *surely* should be useful for Galois module theory. The construction was simplified through a perspective that I learned from Lara Thomas in 2007 and appeared in 2009. The justification of the "surely" is mainly Nigel's work and will appear in PAMS this year.

Everything is generalized in the above preprint with Lindsay. More importantly, I think that we finally have the *right perspective* on this topic.

... though, certainly there is much more depth to plumb in this "totally ramified p-extensions with a certain rigidity in the ramification filtration are inseparable" idea.

Galois scaffold

To motivate my talk on Thursday, let me close by discussing Galois scaffolds, namely some of the ideas in Byott and Elder, preprint.

Recall the intuition of a scaffold. We start with integers $p \nmid b_i > 0$, then we identify elements $X_i \in L$ with $v_L(X_i) = -p^{n-i} b_i$. Since the extension of degree p^n is totally ramified, the easy way to arrange for the valuation of an element to be divisible by a power of p, is to choose it from a subfield of degree p^{n-i} below L.

So that we can do this in such a way that the b_i are ramification numbers, we choose a composition series $\{H_i\}$ that refines the ramification filtration. Choose $H_0 = G$, $H_n = \{1\}$, $H_{i-1}/H_i \cong C_p$.

Choose $\sigma_i \in H_{i-1} \setminus H_i$. Let $b_i = v_n((\sigma_i - 1)\pi_n) - 1$, then $\{b_i\}$ is the set of lower ramification numbers.

Let $K_i = K_n^{H_i}$. Because $\{H_i\}$ refines the ramification filtration, the ramification number of K_i/K_{i-1} is b_i. Assume $p \nmid b_i$ (Weak assumption). Assume $b_i \equiv b_j \bmod p^n$ (Strong assumption).

WLOG there are $X_j \in K_j$ satisfying the Artin-Schreier equation $X_j^p - X_j \in K_{j-1}$ and $v_j(X_j) = -b_j$. Thus $v_j((\sigma_j - 1)X_j - 1) > 0$.

In char. p, $(\sigma_j - 1)X_j = 1$. Indeed, given any polynomial in X_j, $f(X_j)$ we find that $(\sigma_j - 1)f(X_j) = f(X_j + 1) - f(X_j)$. We have found that $\sigma_j - 1$ behaves like a Δ_1, the foward difference operator.

instead of derivations, we are in the setting of difference equations

But because in general we have congruences $(\sigma_j - 1)X_j \equiv 1 \bmod \mathfrak{P}_j$, we only have "approximate" difference operators.

More generally, the congruence we impose, namely $b_i \equiv b_j \bmod p^n$, means that for $1 \leq i < j \leq n$, we have $v_j((\sigma_i - 1)X_j) = b_i - b_j \equiv 0 \bmod p^n$. Thus

$$(\sigma_i - 1)X_j = \mu_{i,j} + \epsilon_{i,j}$$

for $\mu_{i,j} \in K_0$ and $\epsilon_{i,j} \in K_j$ some error term.

Then

$$(\sigma_i - 1)X_j = \mu_{i,j}(\sigma_j - 1)X_j \bmod \text{"higher terms"}$$

$$(\sigma_i - 1)X_j = \mu_{i,j}(\sigma_j - 1)X_j \text{ mod "higher terms"}$$

is interpreted as stating that the $\mu_{i,j} \in K$ are "partial differences"

$$\mu_{i,j} \leftrightarrow \frac{\partial_i}{\partial_j}$$

Falling factorials $X_j(X_j - 1)\cdots(X_j - i + 1) = i!\binom{X_j}{i}$ behave under the foward difference operator Δ_1, like powers x^i under the derivative $\frac{d}{dx}$

Thus $\sigma_i \sim \sigma_j^{[\mu_{i,j}]} = \sum_{r=0}^{p-1} \binom{\mu_{i,j}}{r}(\sigma_j - 1)^r$ is the right way to use σ_j to approximate the effect of σ_i

(Byott & Elder, prepr. 2) If $v_n(\epsilon_{i,j}) - v_n(\mu_{i,j}) \geq p^{n-1}u_i - p^{n-j}b_i + \mathfrak{T}$, where u_i is the corresponding upper ramification number, there is a Galois scaffold of tolerance $\mathfrak{T}$.

(MacKenzie & Whaples, 1956) Cyclic degree p extensions of a p-adic field are (generally) defined by an Artin-Schreier equation.

We determine sufficient conditions on the Artin-Schreier equations for an elementary abelian extension to have a Galois scaffold

For example, the extension $K_n = K_0(x_1, x_2, \ldots, x_n)$ where

$$x_i^p - x_i = \omega_i^{p^{n-1}}\beta + \epsilon_i$$

will have a Galois scaffold of tolerance $\mathfrak{T}$ if $v_0(p)$ is "big enough", and $v_0(\epsilon_i) - v_0(\omega_i^{p^{n-1}}\beta)$ is "big enough".

Using (Byott & Elder, prepr. 1), necessary and sufficient conditions for an ideal to be free over its associated order are given, additional invariants *a lá* (de Smit & Thomas, 2007) are determined.

Let $r(b)$ denote the common residue $b_i \equiv b_j \bmod p^n$. Result can be expressed simply as:

$n = 1$ $\mathfrak{O}_L$ is free over $\mathcal{A}_{L/K}$ iff $r(b) \mid p - 1$
$n = 2$ $\mathfrak{O}_L$ is free over $\mathcal{A}_{L/K}$ iff $r(b) \mid p^2 - 1$
$n > 3$ $\mathfrak{O}_L$ is free over $\mathcal{A}_{L/K}$ if $r(b) \mid p^m - 1$ for some $1 \leq m \leq n$.

The iff conditions for $n > 3$ conditions are more complicated to state. These conditions are those of (Miyata, 1998) concerning GMS in a certain family of cyclic Kummer extensions of local number fields, as translated in (Byott, 2008). Byott conditions

Unexpected pay-off: Classification of Hopf orders

Given a local number field K of characteristic 0 with residue characteristic p and p-group G, $K[G]$ is a Hopf algebra.

(Tate & Oort, 1970) Classifies Hopf orders in $K[C_p]$

(Underwood, 1994) Classification in $K[C_{p^2}]$

We still don't have a complete classification for $K[C_{p^3}]$ (Childs & Underwood, 2003, 2004, 2006), (Underwood, 2008).

We need new methods.

Hopf orders from Galois scaffolds

Let K_n/K_0 be a totally ramified extension with $\mathrm{Gal}(L/K) \cong G$, and lower ramification numbers $b_i \equiv -1 \bmod p^n$. Then $\mathfrak{D}_{L/K} = \delta\mathfrak{O}_L$ for some $\delta \in K$. Under $\mathfrak{D}_{L/K} = \delta\mathfrak{O}_L$, $\delta \in K$, and K a local number field with G abelian, (Bondarko, 2000) proves that

$$\mathfrak{O}_L \text{ is free over } \mathcal{A}_{L/K} \text{ iff } \mathcal{A}_{L/K} \text{ is a Hopf order.}$$

So *IF* we have a Galois scaffold for $K[G]$'s action on L, then, because the hypothesis $b_i \equiv -1 \bmod p^n$ means that the shifts automatically satisfy Byott conditions, $\mathcal{A}_{L/K}$ will be a Hopf order.

Using this...

Hopf orders for $K[C_p^2]$

Let $\langle \sigma_1, \sigma_2 \rangle = C_p^2$ and K be a local number field with residue characteristic p. Then

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

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

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

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

Hopf orders for $K[C_p^3]$

Let $\langle \sigma_1, \sigma_2, \sigma_3 \rangle = C_p^3$ and K be a local number field with residue characteristic p. Then

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

is a Hopf order in $K[C_p^3]$ where $M_1, M_2, M_3 \in \mathbb{Z}$ and $\mu_{i,j} \in K$ satisfying

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

$$v_K(\mu_{1,2}) = p^{i-j} M_i - M_j$$

additionally,...

because these Hopf orders come from a Galois scaffold, the process requires $p^2 \mid (pM_3 - M_2)$, and there must exist some $\omega_2, \omega_3 \in K$ with $v_K(\omega_3) \leq v_K(\omega_2) \leq 0$ with $\omega_2^p \not\equiv \omega_2 \bmod \mathfrak{P}_K$ such that

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

At this point, I don't know whether the above conditions are necessary, or just a by-product of our method. Regardless, the Hopf orders we exhibit are realizable. Their duals are monogenic (Byott, 2004). And there is no upper bound on the size of the group C_p^n.