Scaffolds and (Generalised) Galois Module Structure

Nigel Byott

University of Exeter

24 June 2015
Scaffolds give a new approach to Galois module structure in local fields. When they exist, they give a lot of information in purely numerical form, but interpreting this to get explicit module-theoretic statements requires further effort.

This is joint work with Griff Elder and Lindsay Childs.

Main reference:

NB + L. Childs + G. Elder: **Scaffolds and Generalized Integral Galois Module Structure**
arXiv:1308.2088
Outline of Talk:

- Motivation I: Inseparable Extensions
- Motivation II: Galois Module Structure in Prime Degree
- What is a Scaffold?
- When do Galois Scaffolds Exist?
- Consequences of Having a Scaffold
- Example: Weakly Ramified Extensions
Motivation I: Inseparable Extensions

Can we ”do Galois theory” for inseparable extensions?

Take: $K$ a field of characteristic $p > 0$;
$L$ a primitive, purely inseparable extension of $K$ of degree $p^n$:

$$L = K(x) \text{ with } x^{p^n} = \alpha \in K^\times \setminus K^{\times p}.$$ 

The only $K$-automorphism of $L$ is the identity, but another familiar sort of $K$-linear operator is given by (formal) differentiation.

Let $\delta: L \to L$ be the $K$-linear map given by

$$\delta(x^j) = jx^{j-1}.$$ 

This makes sense as $\delta(x^{p^n}) = 0 = \delta(\alpha)$, but depends on the choice of generator $x$. We have

$$\delta(x^j) = 0 \text{ if } p \mid j;$$
$$\delta^p = 0.$$
Motivation I: Inseparable Extensions

We want to introduce operators $\delta^{(s)}$ that “behave like” $\frac{1}{s!} \frac{d^s}{dx^s}$.

For $0 \leq s \leq p^n - 1$, write

$$s = s(0) + ps(1) + \cdots + p^{n-1}s(n-1) \text{ with } 0 \leq s(i) \leq p - 1.$$

Then define a $K$-linear map $\delta^{(s)}: L \rightarrow L$ by

$$\delta^{(s)}(x^j) = \binom{j}{s} x^{j-s} = \prod_{i=0}^{n-1} \binom{j(i)}{s(i)} x^{j-s}.$$

(Think of $\delta^{(p^i)}$ as differentiation with respect to $x^{p^i}$, where we pretend that $x$, $x^p$, $x^{p^2}$, ..., $x^{p^{n-1}}$ are independent variables.)

**Notation:** For $0 \leq s, j \leq p^n - 1$,

$$s \preceq j \text{ means } s(i) \leq j(i) \text{ for } 0 \leq i \leq n - 1.$$

Then $\delta^{(s)}(x^j) = 0$ unless $s \preceq j$. 
Motivation I: Inseparable Extensions

We have
\[ \delta(s) \delta(t) = \binom{s + t}{s} \delta(s + t). \]

(This is 0 if \( s + t \geq p^n \).)

The commutative \( K \)-algebra \( A \) with basis \( (\delta(s))_{0 \leq s \leq p^n - 1} \) acts on \( L \).

This is analogous to action of the group algebra in standard Galois theory. The group algebra is a Hopf algebra, and its action is compatible with the comultiplication. In the same way, if we make \( A \) into a Hopf algebra with comultiplication
\[ \delta(s) \mapsto \sum_{r=0}^{s} \delta(r) \otimes \delta(s-r), \]
then \( L \) is an \( A \)-Hopf-Galois extension of \( K \).

\( A \) is the \textbf{divided power} Hopf algebra of dimension \( p^n \).
Motivation I: Inseparable Extensions

Now bring in ramification.

Say $K$ is the local field $\mathbb{F}_{p^f}((T))$ with valuation $v_K(T) = 1$.

Suppose $v_K(\alpha) = -b$ with $p \nmid b$.

So $L/K$ is totally ramified and $v_L(x) = -b$.

$(x^j)_{0 \leq j \leq p^n - 1}$ is a $K$-basis of $L$ with valuations distinct modulo $p^n$, and

$$v_L(\delta^{(s)} \cdot x^j) = \begin{cases} v_L(x^j) + bs & \text{if } s \leq j, \\ \infty & \text{otherwise.} \end{cases}$$
Motivation I: Inseparable Extensions

The action becomes even more transparent if we adjust our bases by suitable units: set

\[ \Psi(s) = \left[ \prod_{i=0}^{n-1} s(i)! \right] \delta(s), \quad y(j) = \left[ \prod_{i=0}^{n-1} j(i)! \right]^{-1} x^j. \]

Then

\[ v_L(y(j)) = v_L(x^j) = -jb \]

and

\[ \Psi(s) \cdot y(j) = \begin{cases} y^{(j-s)} & \text{if } s \leq j, \\ 0 & \text{otherwise}. \end{cases} \]

The elements \( \Psi(p^j) \) and \( y(j) \) form a prototypical example of a scaffold.
Let $K$ be a finite extension of $\mathbb{Q}_p$ with absolute ramification index $v_K(p) = e$.

Let $L/K$ be a totally ramified Galois extension of degree $p$.

Let $G = \langle \sigma \rangle = \text{Gal}(L/K)$.

We want to study the valuation ring $\mathcal{O}_L$ of $L$ as a Galois module. As $L/K$ is wildly ramified, $\mathcal{O}_L$ cannot be free over $\mathcal{O}_K[G]$, so consider the associated order

$$\mathcal{A} := \{ \alpha \in K[G] : \alpha \cdot \mathcal{O}_L \subseteq \mathcal{O}_L \}.$$ 

This is the largest order in $K[G]$ over which $\mathcal{O}_L$ is a module.

**Basic Question:** When is $\mathcal{O}_L$ a free module over $\mathcal{A}$?
Motivation II: Galois Module Structure in Prime Degree

$L/K$ has **ramification break** $b$ characterised by

$$\forall x \in L\{0\}, \nu_L((\sigma - 1) \cdot x) \geq \nu_L(x) + b,$$

with equality unless $p \mid \nu_L(x)$.

Then

$$1 \leq b \leq \frac{ep}{p-1}, \quad p \nmid b \text{ unless } b = \frac{ep}{p-1}.$$

We assume $b \leq \frac{ep}{p-1} - 1$.

Bertrandias, Bertrandias and Ferton (1972) showed that

$$\mathfrak{O}_L \text{ is free over } \mathfrak{A} \iff (b \mod p) \mid p - 1.$$

Ferton (1972) determined when a given power $\mathfrak{P}^h$ of the maximal ideal $\mathfrak{P}$ of $\mathfrak{O}_L$ is free over its associated order, in terms of the continued fraction expansion of $b/p$.

Analogous results in characteristic $p$ (so $K = \mathbb{F}_{p^f}(T)$ and $e = \infty$) were given by Aiba (2003), de Smit & Thomas (2007) and Huynh (2014).
These results all depend on the following idea:

Let $\Psi = \sigma - 1$ and choose $x \in L$ with $\nu_L(x) = b$.

For $0 \leq j \leq p - 1$ set $y_j = \Psi^j \cdot x$, so $\nu_L(y_j) = (j + 1)b$.

Then, for $0 \leq s \leq p - 1$,

$$\Psi^s \cdot y_j \begin{cases} = y_{s+j} & \text{if } s + j \leq p - 1; \\ \equiv 0 \pmod{x^{s+j} \Psi^\Xi} & \text{otherwise} \end{cases}$$

where

$$\Xi = ep - (p - 1)b.$$

Then $\Psi$ and the $y_j$ form a scaffold.
What is a Scaffold?

Let $K$ be a local field of residue characteristic $p > 0$, let $\pi \in K$ with $v_K(\pi) = 1$, and let $L/K$ be a totally ramified extension of degree $p^n$.

Fix $b \in \mathbb{Z}$ with $p \nmid b$ and for each $t \in \mathbb{Z}$ define

$$a(t) = a(t)_0 + pa(t)_1 + \cdots + p^{n-1}a(t)_{n-1} := (-b^{-1}t) \mod p^n.$$ 

A scaffold of shift $b$ and infinite tolerance on $L$ consists of

- elements $\lambda_t \in L$ with $v_L(\lambda_t) = t$ for each $t \in \mathbb{Z}$;
- $K$-linear maps $\Psi_1, \Psi_2, \ldots, \Psi_n : L \rightarrow L$ such that

$$\psi_i \cdot \lambda_t = \begin{cases} 
\lambda_t + p^{n-i}b & \text{if } a(t)_{n-i} \geq 1, \\
0 & \text{if } a(t)_{n-i} = 0,
\end{cases}$$

and $\psi_i \cdot K = 0$. 
What is a Scaffold?

For \(0 \leq s \leq p^{n-1}\), set

\[
\psi(s) = \psi_n^s \psi_{n-1}^s \cdots \psi_1^s.
\]

Then

\[
\psi(s) \cdot \lambda_t = \begin{cases} 
\lambda_{t+sb} & \text{if } s \leq a(t), \\
0 & \text{otherwise}.
\end{cases}
\]

Moreover \(L\) is a free module over the commutative \(K\)-algebra \(A = K[\psi_1, \ldots, \psi_n]\) on the generator \(\lambda_b\).

**Example:** \(K = \mathbb{F}_{p^n}(T)\) and \(L = K(x)\) purely inseparable of degree \(p^n\), \(b = -\nu_L(x)\), \(\lambda_{cp^n-bj} = T^c y^{(j)}\) and \(\psi_i = \delta(p^{n-i})\).
What is a Scaffold?

Now fix $\mathcal{T} > 0$. A **scaffold of tolerance** $\mathcal{T}$ is similar except that the formula for the action of $A$ on $L$ only holds “up to an error”:

$$
\psi^{(s)} \cdot \lambda_t \equiv \begin{cases} 
\lambda_{t+sb} & \text{if } s \leq a(t), \\
0 & \text{otherwise.}
\end{cases}
$$

where the congruence is modulo terms of valuation $\geq t + sb + \mathcal{T}$. (Then $A$ no longer need be commutative.)

**Example:** $L/K$ totally ramified Galois extension of degree $p$. $\Psi_1 = \sigma - 1$, and $\lambda_{cp^n + b(j+1)} = \pi^c \psi_1^j \cdot x$ where $v_L(x) = b$; here $\mathcal{T} = ep - (p - 1)b$.

**Remark:** In the BCE paper, we allowed a slightly more general definition of scaffold.
When do Galois Scaffolds Exist?

Suppose \( L/K \) is a totally ramified Galois extension of degree \( p^n \).

Take a generating set \( \sigma_1, \ldots, \sigma_n \) of \( G = \text{Gal}(L/K) \) so that the subgroups

\[
H_i = \langle \sigma_{n-i+1}, \ldots, \sigma_n \rangle, \quad 0 \leq i \leq n
\]

satisfy \( |H_i| = p^i \) and refine the ramification filtration.

Then we have (lower) ramification breaks \( b_1 \leq b_2 \leq \cdots \leq b_n \), characterised by

\[
\forall y \in L^\times, v_L((\sigma_i - 1) \cdot y) \geq v_L(y) + b_i,
\]

with equality if and only if \( p \nmid v_L(y) \).
When do Galois Scaffolds Exist?

Now if \( x \) is any element of the intermediate field \( K_i = L^{H_{n-i}} \) of degree \( p^i \) over \( K \), then \( p^{n-i} \mid \nu_L(x) \), and if \( p^{n-i+1} \mid \nu_L(x) \) then

\[
\nu_L((\sigma_i - 1) \cdot x) = \nu_L(x) + p^{n-i}b_i.
\]

We now make 3 assumptions:

**Assumption 1 (very weak):** \( p \nmid b_1 \).

**Assumption 2 (fairly weak):** \( b_i \equiv b_n \pmod{p^i} \) for each \( i \).

If \( G \) is abelian, this holds by the Hasse-Arf Theorem.

Now set \( \Psi_n = \sigma_n - 1 \).

**Assumption 3 (pretty strong):**

For \( 1 \leq i \leq n - 1 \), we can replace \( \sigma_i - 1 \) with \( \Theta_i \in K[H_{n+1-i}] \) so that

\[
\nu_L(\Theta_i \cdot y) = \nu_L(y) + p^{n-i}b_i \quad \forall y \in L^\times \text{ with } \nu_L(y)_{(n-i+1)} \neq 0.
\]

Nigel Byott (University of Exeter)
When do Galois Scaffolds Exist?

Now set

\[ \psi_i = \pi^{(b_n-b_i)/p^i} \Theta_i, \]

\[ \psi(s) = \psi_s^{s(0)} \psi_s^{s(1)} \cdots \psi_s^{s(n-1)}. \]

Pick \( y \in L \) with \( V_L(y) = b \) and set

\[ \lambda_{cp^n+b(s+1)} = \pi^c \psi(s) \cdot y. \]

Then we have a scaffold of tolerance 1.

Having higher tolerance amounts to the \( \psi_i^p \) being "close enough" to 0.
When do Galois Scaffolds Exist?

For $K$ of characteristic $p$, and any $b \not\equiv 0 \pmod{p}$ and $n \geq 1$, Elder constructed a large family of elementary abelian extensions $L/K$ of degree $p^n$ with unique ramification number $b$ which admit a scaffold of tolerance $\infty$. (These are the “nearly one-dimensional extension”.) This can be made to work in characteristic 0 (with finite tolerance).

So, although extensions admitting a scaffold are quite special, there are plenty of examples.

In particular, let $L/K$ be a Galois extension which is totally and weakly ramified (i.e. the only ramification break is 1). If $K$ has characteristic $p$, then $K$ has a scaffold of infinite tolerance. If $K$ has characteristic 0, it has a scaffold of “high enough” tolerance $2p^n - 1$ provided $e \geq 3$. 
Suppose $L/K$ has a scaffold with shift $b$ and tolerance $\mathcal{T} \geq 2p^n - 1$. Consider any fractional ideal $\mathfrak{P}^h$ of $\mathcal{O}_L$ as a module over its associated order

$$A = A_h := \{ \alpha \in K[G] : \alpha \cdot \mathfrak{P}^h \subseteq \mathfrak{P}^h \}.$$ 

We assume without loss of generality that $b \geq h > b - p^n$. For $0 \leq s \leq p^n - 1$ define

$$d(s) = \left\lfloor \frac{sb + b - h}{p^n} \right\rfloor,$$

$$w(s) = \min\{ d(s + j) - d(j) : j \leq p^n - 1 - s \}.$$ 

So $d(0) = 0$ and $w(s) \leq d(s)$. 
Theorem

For $L/K$ admitting a scaffold as above,

- we have an explicit description of the associated order: $\mathfrak{A}_h$ has $\mathcal{O}_K$-basis $\pi^{-w(s)}\psi(s)$ for $0 \leq s \leq p^n - 1$.

- $\mathfrak{P}^h$ is free over $\mathfrak{A}_h$ if and only if $w(s) = d(s)$ for all $s$; in this case, any $y \in L$ with $v_L(y) = b$ is a generator.

This gives a purely numerical (but not very transparent) criterion for freeness. Extracting an explicit list of ideals which are free is not easy!
Moreover, following ideas of de Smit and Thomas (in case degree $p$, characteristic $p$), we also have

**Theorem**

- the minimal number of generators for $\mathfrak{P}^h$ as an $\mathcal{A}_h$-modules is

$$\# \{ u : d(u) > d(u - s) + w(s) \forall s : 0 \prec s \preceq u \}.$$  

(The minimal number of generators is $1 \iff \mathfrak{P}^h$ is free over $\mathcal{A}$.)

- Let $\mathcal{M}$ be the maximal ideal of the local ring $\mathcal{A}_h$ and let $\kappa$ be the residue field of $\mathcal{O}_K$. Then the embedding dimension of $\mathcal{A}_h$ is

$$\dim_{\kappa}(\mathcal{M}/\mathcal{M}^2) = \# \{ u : w(u) > w(u - s) + w(s) \forall s : 0 \prec s \prec u \}.$$
Weakly Ramified Extensions

As an illustration of these results, let $L/K$ be totally and weakly ramified of degree $p^n$ (so $G = \text{Gal}(L/K)$ is elementary abelian). Suppose $p \neq 2$ and either $\text{char}(K) = p$ or $e \geq 3$.

Then $b = 1$, and we consider $\mathfrak{P}^h$ with $1 - p^n < h \leq 1$.

First consider two special cases:

$h = 1$: $\mathfrak{P}$ is free over $\mathcal{O}_K[G]$ which has embedding dimension $n + 1$.

$h = 0$: $\mathcal{O}_L$ is free over $\mathcal{O}_K \left[ G, \pi^{-1} \sum_{g \in G} g \right]$, which has embedding dimension $n + 2$.

This leaves us with $1 - p^n < h < 0$.
Weakly Ramified Extensions

Put

\[ m = h + p^n - 1, \quad \text{so } 0 < m < p^n - 1; \]

\[ k = \max(m, p^n - m). \]

Then

\[
\begin{align*}
d(s) &= \begin{cases} 
1 & \text{if } s \geq m; \\
0 & \text{otherwise};
\end{cases} \\
w(s) &= \begin{cases} 
1 & \text{if } s \geq k; \\
0 & \text{otherwise.}
\end{cases}
\end{align*}
\]

So

\[ \mathfrak{P}^h \text{ is free } \iff w(s) = d(s) \forall s \]

\[ \iff h \geq \frac{1}{2} (3 - p^n). \]

Thus (including cases \( h = 1, 0 \)) just over half the ideals are free.
Weakly Ramified Extensions

- when \( \mathcal{P}^h \) is not free, \( 2 + \alpha(m) - \beta(m) \) generators are required;
- the embedding dimension of \( \mathcal{A}_h \) is \( n + 2 + \alpha(k) \);

where \( \alpha(s) = \# \{ i : s(i) \neq p - 1 \text{ and } i > v_p(s) \} \),

\[
\beta(s) = \max \{ c : 0 \leq c < n - v_p(s), \ s(n-1) = \ldots = s(n-c) = \frac{1}{2}(p - 1) \}.
\]

**Example:** \( p^n = 5^6 = 15625, \ h = -7884 \).

As \( 1 - p^n < h < \frac{1}{2}(3 - p^n) \), \( \mathcal{P}^h \) is **not** free over its associated order.

\[
m = h + p^n - 1 = 7740 = 221430_5,
\]

so \( m(0) = 0, \ m(1) = 3, \ m(2) = 4, \ m(3) = 1, \ m(4) = 2, \ m(5) = 2 \), and

\[
\alpha(m) = 3, \quad \beta(m) = 2.
\]

Also, \( k = p^n - m = 223020_5 \), so \( \alpha(k) = 4 \).

Hence \( \mathcal{P}^h \) requires \( 2 + \alpha(m) - \beta(m) = 3 \) generators over its associated order, and the embedding dimension of the associated order is

\( n + 2 + \alpha(k) = 12 \).