Scaffolds and Generalised Galois Module Structure)

Nigel Byott

University of Exeter, UK

Omaha - 28 May 2013

(Joint work with Griff Elder)

Let K a local field, whose valuation ring O_K has maximal ideal $\mathfrak{P}_K = \pi O_K$.

We assume the residue field $k = O_K/\pi O_K$ has characteristic p; but $\mathrm{char}(K)$ could be 0 or p.

Let L/K be a totally ramified extension of degree p^n.

Fix $h \in \mathbb{Z}$.

Aim: to study "Galois module structure" of $\mathfrak{P}_L^h$ in the following two situations:

Standard Set-up:

L/K is Galois.

Let $A = K[\Gamma]$ where $\Gamma = \mathrm{Gal}(L/K)$.

Assume k is perfect, and let $b_1 \leq \ldots \leq b_n$ be the ramification breaks of L/K (counted with multiplicity).

We assume

- $b_{i+1} \equiv b_i \pmod{p^i}$ for $1 \leq i < n$ (automatic if Γ is abelian);
- $p \nmid b_i$ for $1 \leq i \leq n$ (automatic if $\mathrm{char}(K) = p$).

Generalized Set-up:

Let A be *some* K-algebra acting on L, so that L is a free A-module of rank 1.

Let $b_1, \ldots, b_m \in \mathbb{Z}$ be *some* parameters, such that $p \nmid b_i$ for $1 \leq i \leq n$.

[This includes the "standard set-up" as a special case, but A could for instance be the group algebra for a non-abelian extension L/K, or a Hopf algebra giving a Hopf-Galois structure on the extension L/K, which need not be normal and/or separable.]

In either set-up, our aim is to study $\mathfrak{P}_L^h$ as a module over its associated order $\mathcal{A}$ in the algebra A.

Motivating Example

Consider the Standard Set-up, with $n = 2$ and $b_1 < b_2$.

We can find σ_1, $\sigma_2 \in \Gamma$ so that

$$v_L\left((\sigma_i - 1) \cdot x\right) \geq v_L(x) + b_i,$$

with equality if and only if $p \nmid v_L(x)$. Then

$$v_L\left((\sigma_1 - 1)^{j_1}(\sigma_2 - 1)^{j_2} \cdot x\right) = v_L(x) + j_1 b_1 + j_2 b_2,$$

provided that

$$v_L(x) \not\equiv 0, -b_1, \ldots, -(j_1 + j_2 - 1)b_1 \pmod{p}$$

(so $j_1 + j_2 \leq p - 1$.)

In contrast to the case $n = 1$, this does not give us enough information to work out the Galois module structure. Scaffolds, when they exist, will provide a way to remedy this deficit. Before defining them, we need some more notation:

Notation

From now on, s, u will always be variables in $\{0, 1, \ldots, p^n - 1\}$. We write them in base p:

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

and similarly for u.

We define a partial order $\preceq$ by

$$s \preceq u \Leftrightarrow s_{(i)} \leq u_{(i)} \text{ for } 0 \leq i \leq n - 1,$$

and write $s \prec u$ for $s \preceq u$ but $s \neq u$.

Define

$$\mathfrak{b}(s) = s_{(n-1}p^{n-1}b_1 + s_{(n-2)}p^{n-2}b_2 + \ldots + s_{(0)}b_{(0)}$$

and, for $t \in \mathbb{Z}$, let $\mathfrak{a}(t)$ be the unique integer satisfying

$$0 \leq \mathfrak{a}(t) \leq p^n - 1, \qquad \mathfrak{b}(\mathfrak{a}(t) \equiv -t \pmod{p^n}.$$

Thus, in the Standard Set-up,

$$\mathfrak{b}(s) \equiv sb_n \pmod{p^n}, \qquad \mathfrak{a}(t) \equiv -b_n^{-1}t \pmod{p^n}.$$

Definition of A-scaffold

An A scaffold on L/K consists of

- Elements $\Psi_1, \ldots, \Psi_n \in A$ with $\Psi_i \cdot 1 = 0$ (for $n = 2$, think of Ψ_1 as $\sigma_2 - 1$ and Ψ_2 as a "modified version" of $\sigma_1 - 1$), and
- elements $\lambda_t \in L$ for $t \in \mathbb{Z}$ with $v_L(\lambda_t) = t$ and $\lambda_{t+p^n} = \pi\lambda_t$, such that

$$\Psi_i \cdot \lambda_t \equiv \begin{cases} \lambda_{t+p^{n-i}b_i} & \text{if } \mathfrak{a}(t)_{(n-i)} \geq 1; \\ 0 & \text{otherwise,} \end{cases}$$

where the congruence is mod $\pi^2\lambda_{t+p^{n-i}b_i}$.

(For ease of exposition, this is a slightly simplified version of the definition in our manuscript.)

For $0 \leq s \leq p^{n-1}$, define

$$\Psi^{(s)} = \Psi_n^{s_{(0)}} \Psi_{n-1}^{s_{(1)}} \cdots \Psi_1^{s_{(n-1)}} \in A.$$

If we have a scaffold, it follows inductively that

$$\Psi^{(s)} \cdot \lambda_t \equiv \begin{cases} \lambda_{t+\mathfrak{b}(s)} & \text{if } s \preceq \mathfrak{a}(t); \\ 0 & \text{otherwise,} \end{cases}$$

where the congruence is mod $\pi^2 \lambda_{t+\mathfrak{b}(s)}$.

Then, in particular, we have

$$v_L\left(\Psi^{(s)} \cdot \lambda_t\right) = t + \mathfrak{b}(s) \text{if } s \preceq \mathfrak{a}(t).$$

The congruence is unaffected if we change the order of the factors in $\Psi^{(s)}$ (even if the algebra A is not commutative).

Perhaps surprisingly, it is possible to construct extensions L/K where scaffolds do exist. These include the class of "almost one-dimensional" elementary abelian extensions in characteristic p (amongst which are all totally and weakly ramified characteristic p extensions), some cyclic extensions of degree p^2 in characteristic p, some characteristic 0 examples, and some *ad hoc* examples where L/K is purely inseparable and A is a Hopf algebra giving L/K a Hopf-Galois structure.

For more about the actual construction of scaffolds, see Griff's (2nd) talk.

The point of all this is that, once we have a scaffold, we can in principle say a lot about the "Galois module structure" of $\mathfrak{P}_L^h$ with respect to A. Before giving a precise statement, we need yet more notation:

Further Notation

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

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

- $$w(s) = \min\{d(s+j) - d(j) : 0 \preceq j \preceq p^n - 1 - s\};$$

- $$\Phi^{(s)} = \pi^{-w(s)} \Psi^{(s)}.$$

Theorem

If L/K admits an A-scaffold then

- $\mathcal{A}$ has O_K-basis $\Phi^{(s)}$ for $0 \leq s \leq p^n - 1$;
- $\mathfrak{P}_L^h$ is free over $\mathcal{A}$ if and only if $w(s) = d(s)$ for all s; moreover, when this occurs, $\mathfrak{P}_L^h = \mathcal{A} \cdot \rho$ for any ρ with $v_L(\rho) = b$;
- the minimal number of generators for $\mathfrak{P}_L^h$ as an $\mathcal{A}$-module is the cardinality of the set

  $$\{u : d(u) > d(u-s) + w(s) \text{ for all } s \text{ with } 0 \prec s \preceq u\}$$

  (this is 1 precisely when $\mathfrak{P}_L^h$ is free over $\mathcal{A}$);
- $\mathcal{A}$ has a unique maximal ideal $\mathcal{M}$ (i.e $\mathcal{A}$ is a local ring, but not necessarily commutative) and its embedding dimension $\dim_k(\mathcal{M}/\mathcal{M}^2)$ is the cardinality of the set

  $$\{u : w(u) > w(u-s) + w(s) \text{ for all } s \text{ with } 0 \prec s \prec u\}.$$

Example

Let L/K be a weakly (and totally) ramified extension (i.e. $b_1 = \cdots = b_n = 1$) in characteristic p.

Suppose without loss of generality that $2 \leq h \leq p^n + 1$. Then

$$\mathfrak{P}_L^h \text{ is free } \Leftrightarrow h \geq 1 + \frac{1}{2}p^n.$$

The same conclusion holds for any extension L/K (in characteristic p or characteristic 0) in which $b_1 \equiv b_2 \equiv \cdots b_n \equiv 1 \pmod{p^n}$ and for which a scaffold exists.