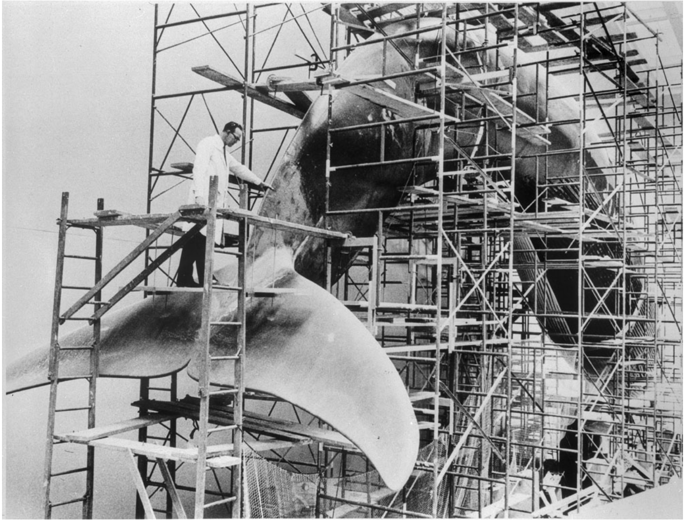
Galois scaffolds and semistable extensions



Kevin Keating University of Florida May 27, 2019

References

[Bon1] Mikhail V. Bondarko, Local Leopoldt's problem for rings of integers in abelian p-extensions of complete discrete valuation fields, Doc. Math. **5** (2000), 657–693.

[Bon2] Mikhail V. Bondarko, Local Leopoldt's problem for ideals in totally ramified p-extensions of complete discrete valuation fields, Algebraic number theory and algebraic geometry, 27–57, Contemp. Math. 300, Amer. Math. Soc., Providence, RI, 2002.

[BCE] Nigel P. Byott, Lindsay N. Childs, and G. Griffith Elder, Scaffolds and generalized integral Galois module structure, Ann. Inst. Fourier (Grenoble) **68** (2018), 965–1010.

Local fields

Let K be a field which is complete with respect to a discrete valuation $v_K : K^\times \to \mathbb{Z}$, whose residue field $\overline{K}$ is a perfect field of characteristic p. Also let

$$\begin{aligned}
\mathcal{O}_K &= \{\alpha \in K : v_K(\alpha) \geq 0\} \\
&= \text{ring of integers of } K \\
\pi_K &= \text{uniformizer for } \mathcal{O}_K \text{ (i.e., } v_K(\pi_K) = 1) \\
\mathcal{M}_K &= \pi_K \mathcal{O}_K \\
&= \text{unique maximal ideal of } \mathcal{O}_K
\end{aligned}$$

Let L/K be a totally ramified Galois extension of degree p^n, and set $G = \text{Gal}(L/K)$.

Galois scaffolds (setup)

Let $b_1 \leq b_2 \leq \cdots \leq b_n$ be the lower ramification breaks of L/K, counted with multiplicity. Assume that $p \nmid b_i$ for $1 \leq i \leq n$.

Set $\mathbb{S}_{p^n} = \{0, 1, \ldots, p^n - 1\}$ and write $s \in \mathbb{S}_{p^n}$ in base p as

$$s = s_{(0)}p^0 + s_{(1)}p^1 + \cdots + s_{(n-1)}p^{n-1}$$

with $0 \leq s_{(i)} < p$. Define a partial order on $\mathbb{S}_{p^n}$ by $s \preceq t$ if $s_{(i)} \leq t_{(i)}$ for $0 \leq i \leq n-1$.

Define $\mathfrak{b} : \mathbb{S}_{p^n} \to \mathbb{Z}$ by

$$\mathfrak{b}(s) = s_{(0)}p^0 b_n + s_{(1)}p^1 b_{n-1} + \cdots + s_{(n-1)}p^{n-1} b_1.$$

Let $r : \mathbb{Z} \to \mathbb{S}_{p^n}$ be the function which maps $a \in \mathbb{Z}$ onto its least nonnegative residue modulo p^n. The function $r \circ (-\mathfrak{b}) : \mathbb{S}_{p^n} \to \mathbb{S}_{p^n}$ is a bijection since $p \nmid b_i$. Therefore we may define $\mathfrak{a} : \mathbb{S}_{p^n} \to \mathbb{S}_{p^n}$ to be the inverse of $r \circ (-\mathfrak{b})$. Extend $\mathfrak{a}$ to a function from $\mathbb{Z}$ to $\mathbb{S}_{p^n}$ by setting $\mathfrak{a}(t) = \mathfrak{a}(r(t))$ for $t \in \mathbb{Z}$.

Galois scaffolds

Definition ([BCE], Definition 2.6)

A Galois scaffold $(\{\Psi_i\}, \{\lambda_t\})$ for L/K with precision $\mathfrak{c} \geq 1$ consists of elements $\Psi_i \in K[G]$ for $1 \leq i \leq n$ and $\lambda_t \in L$ for all $t \in \mathbb{Z}$ such that the following hold:

1. $v_L(\lambda_t) = t$ for all $t \in \mathbb{Z}$.
2. $\lambda_{t_1}\lambda_{t_2}^{-1} \in K$ whenever $t_1 \equiv t_2 \pmod{p^n}$.
3. $\Psi_i(1) = 0$ for $1 \leq i \leq n$.
4. For $1 \leq i \leq n$ and $t \in \mathbb{Z}$ there exists $u_{it} \in \mathcal{O}_K^\times$ such that the following congruence modulo $\lambda_{t+p^{n-i}b_i}\mathcal{M}_L^{\mathfrak{c}}$ holds:

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

A basis for $K[G]$

Let $(\{\Psi_i\}, \{\lambda_t\})$ be a Galois scaffold for L/K with precision $\mathfrak{c}$. For $s \in \mathbb{S}_{p^n}$ set

$$\Psi^{(s)} = \Psi_n^{s_{(0)}} \Psi_{n-1}^{s_{(1)}} \dots \Psi_2^{s_{(n-2)}} \Psi_1^{s_{(n-1)}}.$$

Then for every $t \in \mathbb{Z}$ there are $U_{st} \in \mathcal{O}_K^\times$ such that the following holds modulo $\lambda_{t+\mathfrak{b}(s)} \mathcal{M}_L^{\mathfrak{c}}$:

$$\Psi^{(s)}(\lambda_t) \equiv \begin{cases} U_{st} \lambda_{t+\mathfrak{b}(s)} & \text{if } s \preceq \mathfrak{a}(t), \\ 0 & \text{if } s \not\preceq \mathfrak{a}(t). \end{cases}$$

Then $\{\Psi^{(s)} : s \in \mathbb{S}_{p^n}\}$ is a K-basis for $K[G]$.

For $\xi \in K[G]$ with $\xi \neq 0$ define

$$\hat{v}_L(\xi) = \min\{v_L(\xi(\lambda)) - v_L(\lambda) : \lambda \in L^\times\}.$$

Let $\lambda \in L^\times$ and set $v_L(\lambda) = t$. Then $v_L(\Psi^{(s)}(\lambda)) \geq t + \mathfrak{b}(s)$, with equality if and only if $s \preceq \mathfrak{a}(t)$. Hence $\hat{v}_L(\Psi^{(s)}) = \mathfrak{b}(s)$.

The map $\phi : L \otimes_K L \to L[G]$

There is a K-linear map $\phi : L \otimes_K L \to L[G]$ defined by

$$\phi(a \otimes b) = \sum_{\sigma \in G} a\sigma(b)\sigma.$$

For $x \in L$ we get

$$\phi(a \otimes b)(x) = \sum_{\sigma \in G} a\sigma(bx) = a\mathrm{Tr}_{L/K}(bx).$$

Proposition ([Bon1], Proposition 1.1.2)

ϕ is an isomorphism of K-vector spaces.

A partial order

Recall that $[L : K] = p^n$.

Let H be the subgroup of $\mathbb{Z} \times \mathbb{Z}$ generated by the element $(p^n, -p^n)$.

For $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ write $[a, b]$ for the coset $(a, b) + H$.

Define a partial order on the quotient group $(\mathbb{Z} \times \mathbb{Z})/H$ by $[a, b] \leq [c, d]$ if and only if there is $(c', d') \in [c, d]$ such that $a \leq c'$ and $b \leq d'$.

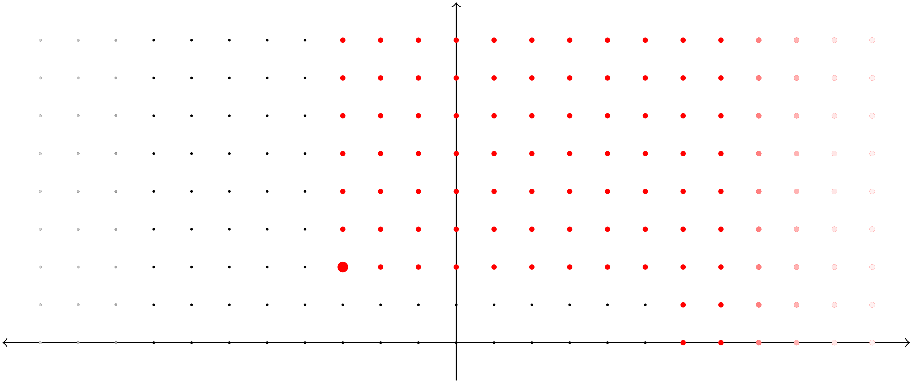
We often use the following set of coset representatives for $(\mathbb{Z} \times \mathbb{Z})/H$:

$$\begin{aligned} \mathcal{F} &= \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : 0 \leq b < p^n\} \\ &= \mathbb{Z} \times \mathbb{S}_{p^n} \end{aligned}$$

An example

Let $p^n = 9$. Here is the set

$$\{(c, d) \in \mathcal{F} : [-3, 2] \leq [c, d]\} :$$



Expansions of tensors

Choose a uniformizer π_L for L and let $\mathcal{T}$ be the set of Teichmüller representatives of K.

Let $\beta \in L \otimes_K L$. Then there are unique $a_{ij} \in \mathcal{T}$ such that

$$\beta = \sum_{(i,j) \in \mathcal{F}} a_{ij} \pi_L^i \otimes \pi_L^j.$$

Set

$$R(\beta) = \{[i,j] : (i,j) \in \mathcal{F},\ a_{ij} \neq 0\}.$$

Then $R(\beta)$ depends on the choice of π_L.

Diagrams and diagonals

Definition

Define the diagram of $\beta \in L \otimes_K L$ to be

$$D(\beta) = \{[x, y] \in (\mathbb{Z} \times \mathbb{Z})/H : [i, j] \leq [x, y] \text{ for some } [i, j] \in R(\beta)\}.$$

Proposition ([Bon2], Remark 2.4.3)

$D(\beta)$ does not depend on the choice of uniformizer π_L for L.

For $\beta \in L \otimes_K L$ with $\beta \neq 0$ define

$$d(\beta) = \min\{i + j : [i, j] \in D(\beta)\}.$$

Define the diagonal of β to be

$$N(\beta) = \{[i, j] \in D(\beta) : i + j = d(\beta)\}.$$

The generating set of a diagram

Let $G(\beta)$ denote the set of minimal elements of $D(\beta)$ with respect to the partial order $\leq$. Then $N(\beta) \subset G(\beta)$.

Set $i_0 = \mathfrak{b}(p^n - 1)$. Then $i_0 + p^n - 1 = v_L(\delta_{L/K})$ is the valuation of the different of L/K.

Theorem ([Bon2], Proposition 2.4.2)

Let $\beta \in L \otimes_K L$ be such that $\xi := \phi(\beta) \in K[G]$. Then the following statements are equivalent:

1. $[a, b] \in G(\beta)$.
2. *For all $\lambda \in L$ with $v_L(\lambda) = -b - i_0$ we have $v_L(\xi(\lambda)) = a$.*

It follows from the theorem that if $\xi = \phi(\beta)$ then $\hat{v}_L(\xi) = d(\beta) + i_0$.

More precisely, for $\lambda \in L^\times$ we have $v_L(\xi(\lambda)) \geq v_L(\lambda) + d(\beta) + i_0$, with equality if and only if $v_L(\lambda) = -b - i_0$ for some $[a, b] \in N(\beta)$.

An example

Let $p^n = 9$ and set

$$\beta = a_{50}\pi_L^5 \otimes \pi_L^0 + a_{44}\pi_L^4 \otimes \pi_L^4 + a_{34}\pi_L^3 \otimes \pi_L^4 + a_{05}\pi_L^0 \otimes \pi_L^5.$$

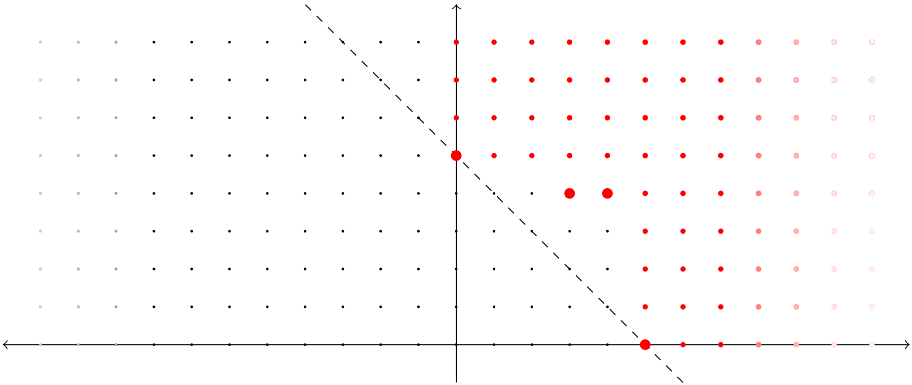
with $a_{ij} \in \mathcal{T} \smallsetminus \{0\}$. We get

$$\begin{aligned} R(\beta) &= \{[5,0],[4,4],[3,4],[0,5]\} \\ G(\beta) &= \{[5,0],[3,4],[0,5]\} \\ N(\beta) &= \{[5,0],[0,5]\} \\ d(\beta) &= 5. \end{aligned}$$

The subset of $\mathcal{F}$ corresponding to $D(\beta)$ is ...

Example diagram

$$p^n = 9, \quad \beta = a_{50}\pi_L^5 \otimes \pi_L^0 + a_{44}\pi_L^4 \otimes \pi_L^4 + a_{34}\pi_L^3 \otimes \pi_L^4 + a_{05}\pi_L^0 \otimes \pi_L^5$$



Semistable extensions

Definition ([Bon2], Definition 3.1.1)

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

1. Say that L/K is semistable if there is $\beta \in L \otimes_K L$ such that $\phi(\beta) \in K[G]$, $p \nmid d(\beta)$, and $|N(\beta)| = 2$.
2. Say that L/K is semistable with precision $\mathfrak{c} \geq 1$ if we may choose β so that $a + b \geq d(\beta) + \mathfrak{c}$ for all $[a, b] \in G(\beta) \smallsetminus N(\beta)$.

Theorem ([Bon2], Proposition 3.2.1)

Let L/K be semistable with precision $\mathfrak{c}$, and let $\beta \in L \otimes_K L$ be the corresponding tensor. Then there is $h \in \mathbb{Z}$ with $h \equiv i_0 \pmod{p^n}$ such that $D(\beta) = \{[0, h], [h, 0]\}$.

Hence by replacing β with a K-multiple we may assume that $D(\beta) = \{[0, i_0], [i_0, 0]\}$.

Galois scaffold $\Rightarrow$ semistable

Theorem

Let L/K be a totally ramified Galois extension of degree p^n which has a Galois scaffold with precision $\mathfrak{c}$. Then L/K is semistable with precision $\mathfrak{c}$.

Proof for $\mathfrak{c} = 1$: Let $(\{\Psi_i\}, \{\lambda_t\})$ be a Galois scaffold for L/K. Set $\xi = \Psi^{(p^n-2)}$. For $\lambda \in L^\times$ we get $v_L(\xi(\lambda)) \geq v_L(\lambda) + \mathfrak{b}(p^n - 2)$, with equality if and only if either $v_L(\lambda) \equiv -\mathfrak{b}(p^n - 1) \pmod{p^n}$ or $v_L(\lambda) \equiv -\mathfrak{b}(p^n - 2) \pmod{p^n}$.

Let $\beta \in L \otimes_K L$ be such that $\phi(\beta) = \xi$. It follows that $N(\beta) = \{[-b_n, 0], [0, -b_n]\}$. Therefore L/K is semistable.

Corollary

Let L/K be a totally ramified Galois extension of degree p^n which has a Galois scaffold. Then the lower ramification breaks of L/K satisfy $b_i \equiv -i_0 \pmod{p^n}$ for $1 \leq i \leq n$.

Coefficientwise multiplication in $K[G]$

Definition

Let $\xi = \sum_{\sigma \in G} a_\sigma \sigma$ and $\eta = \sum_{\sigma \in G} b_\sigma \sigma$ be elements of $K[G]$. Define $\xi * \eta = \sum_{\sigma \in G} a_\sigma b_\sigma \sigma$.

Proposition ([Bon1], Proposition 1.6.1)

Let $\alpha, \beta \in L \otimes_K L$ be such that $\phi(\alpha) \in K[G]$ and $\phi(\beta) \in K[G]$. Then $\phi(\alpha\beta) = \phi(\alpha) * \phi(\beta)$. In particular, $\phi(\alpha\beta) \in K[G]$.

Corollary

Let $\beta \in L \otimes_K L$ satisfy $\phi(\beta) \in K[G]$. Then for all $s \geq 0$ we have $\phi(\beta^s) \in K[G]$.

Another basis for $K[G]$

Let L/K be a semistable extension. Then there is $\beta \in L \otimes_K L$ such that $\phi(\beta) \in K[G]$ and $N(\beta) = \{[0, i_0], [i_0, 0]\}$. Hence there are $t, u \in \mathcal{T} \smallsetminus \{0\}$ and $R \in L \otimes_K L$ with $d(R) > i_0$ and

$$\beta = t\pi_L^0 \otimes \pi_L^{i_0} + u\pi_L^{i_0} \otimes \pi_L^0 + R.$$

It follows that for $s \in \mathbb{S}_{p^n}$ there is $R_s \in L \otimes_K L$ with $d(R_s) > si_0$ and

$$\beta^s = \sum_{j=0}^{s} \binom{s}{j} t^j u^{s-j} \pi_L^{(s-j)i_0} \otimes \pi_L^{si_0} + R_s.$$

It follows that $d(\beta^s) = si_0$ and $D(\beta^s) = \{[(s-j)i_0, ji_0] : j \preceq s\}$.

Set $\xi^{*s} = \phi(\beta^s)$. Then $\xi^{*s} \in K[G]$. For $\lambda \in L^\times$ we get $v_L(\xi^{*s}(\lambda)) \geq v_L(\lambda) + (s+1)i_0$, with equality if and only if $v_L(\lambda) \equiv -(j+1)i_0 \pmod{p^n}$ for some $j \in \mathbb{S}_{p^n}$ such that $j \preceq s$.

The set $\{\xi^{*s} : s \in \mathbb{S}_{p^n}\}$ is a K-basis for $K[G]$.

Semistable $\Rightarrow$ Galois scaffold

Theorem

Let L/K be a semistable extension of degree p^n. Then there is a Galois scaffold for L/K with precision 1.

Proof: There are $\xi \in K[G]$ and $\beta \in L \otimes_K L$ such that $\phi(\beta) = \xi$ and $N(\beta) = \{[i_0, 0], [0, i_0]\}$.

For $1 \leq i \leq n$ define

$$\Theta_i = \phi(\beta^{p^n - p^{n-i} - 1}) = \xi^{*p^n - p^{n-i} - 1}.$$

Then $\Theta_i \in K[G]$. Set $c_i = \hat{v}_L(\Theta_i) = (p^n - p^{n-i})i_0$. Then

$$c_i \equiv -p^{n-i} i_0 \equiv p^{n-i} b_i \pmod{p^n}.$$

Let $\lambda \in L^\times$ and set $t = v_L(\lambda)$. Then $v_L(\Theta_i(\lambda)) \geq t + c_i$, with equality if and only if $\mathfrak{a}(t)_{(n-i)} \geq 1$.

Semistable $\Rightarrow$ Galois scaffold (continued)

Set $v_i = (c_i - p^{n-i} b_i)/p^n$. Then $\Phi_i = \pi_K^{-v_i} \Theta_i$ satisfies $v_L(\Phi_i(\lambda)) \geq t + p^{n-i} b_i$, with equality if and only if $\mathfrak{a}(t)_{(n-i)} \geq 1$.

For $1 \leq i \leq n$ set $\Psi_i = \Phi_i - \Phi_i(1)$. Then $\Psi_i(1) = 0$. Let $\lambda \in L^\times$ and set $t = v_L(\lambda)$. Since $v_L(\Phi_i(1)) > p^{n-i} b_i$ we get

$$\Psi_i(\lambda) \equiv \Phi_i(\lambda) \pmod{\mathcal{M}_L^{t+p^{n-i}b_i+1}}.$$

Let $\{\lambda_t : t \in \mathbb{Z}\}$ be elements of L such that $v_L(\lambda_t) = t$ for all $t \in \mathbb{Z}$ and $\lambda_{t_1} \lambda_{t_2}^{-1} \in K$ for all t_1, t_2 such that $t_1 \equiv t_2 \pmod{p^n}$.

Suppose $\mathfrak{a}(t)_{(n-i)} \geq 1$. Then $v_L(\Psi_i(\lambda_t)) = t + p^{n-i} b_i$, so there is $u_{it} \in \mathcal{O}_K^\times$ such that

$$\Psi_i(\lambda_t) \equiv u_{it} \lambda_{t+p^{n-i}b_i} \pmod{\lambda_{t+p^{n-i}b_i} \mathcal{M}_L}.$$

It follows that $(\{\Psi_1, \ldots, \Psi_n\}, \{\lambda_t\})$ is a Galois scaffold for L/K with precision 1.

Some questions

Let L/K be a semistable extension with precision $\mathfrak{c} > 1$. The Galois scaffold for L/K produced by our methods need not have precision $\mathfrak{c}$. In fact, the best we can say is that it has precision 1.

It would be interesting to know whether a semistable extension with sufficiently high precision must have a Galois scaffold with precision $\mathfrak{c}$ for some $\mathfrak{c} > 1$.

Note however that a semistable extension with sufficiently high precision (e.g., $\mathfrak{c} \geq p^n$) is stable, and hence semistable with infinite precision. Hence we can't expect a semistable extension with precision $\mathfrak{c}$ to have a Galois scaffold with precision $\mathfrak{c}$ in every case.

It would be useful to have some examples of semistable extensions with high precision which don't admit Galois scaffolds with high precision.