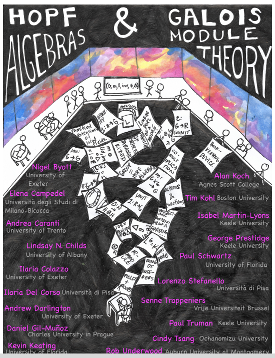
Galois Scaffolds And Galois Module Structure For Totally Ramified Extra-Special p-Extensions

Hopf Algebras & Galois Module Theory 2022

Paul Schwartz & Kevin Keating

Stevens Institute of Technology & University of Florida

June 1, 2022



Notation

Given a local field K, we let $v_K : K \to \mathbb{Z} \cup \{\infty\}$ be the normalized valuation on K ($v_K(0) = \infty$). Notationally we have the following:
$e_K = v_K(p)$ is the absolute ramification index;
$\mathfrak{O}_K = \{x \in K : v_K(x) \geq 0\}$ is the ring of integers;
$\mathfrak{M}_K = \{x \in K : v_K(x) \geq 1\}$ is the maximal ideal of $\mathfrak{O}_K$;
π_K is a uniformizer for K.
If $K_0 \subseteq \cdots \subseteq K_n$ is a tower of totally ramified fields we may replace the subscript K_i by the subscript i for $0 \leq i \leq n$ giving us v_i, e_i, $\mathfrak{O}_i$, $\mathfrak{M}_i$ and π_i.
If K is a local field with residue characteristic p, and $\vec{v} = (a_1, \ldots, a_n)$, we let $\mathbf{F}(\vec{v}) = (a_1^p, \ldots, a_n^p)$.

Ramification groups

Let L/K be a Galois extension of degree p^n of local fields with Galois group G. For $i \geq -1$ we define the i-th *ramification subgroup* by $G_i = \{\sigma \in G : v_L((\sigma - 1)\pi_L) \geq i + 1\}$. It is well known that G_i is a normal subgroup of G and the quotient G_i/G_{i+1} is an elementary abelian p-gorup. This allows us to choose a composition series $G = H_0 \supset H_1 \supset ... \supset H_{n-1} \supset H_n = \{1\}$ such that $H_i/H_{i+1} \cong C_p$ for $0 \leq i \leq n-1$ and $\{G_i : i \geq -1\} \subseteq \{H_i : 0 \leq i \leq n\}$ [BE13].

Ramification numbers

For $0 \leq i \leq n-1$, choose $\sigma_{i+1} \in H_i \setminus H_{i+1}$. Then set $b_i = v_L((\sigma_i - 1)\pi_L) - 1$ for $1 \leq i \leq n$, this integer is independent of the choices made and we call it the i-th *lower ramification number*.

The *upper ramification number* $u_1, \ldots, u_n$ are defined recursively by $u_1 = b_1, u_i = u_{i-1} + \dfrac{b_i - b_{i-1}}{p^{i-1}}$ for $2 \leq i \leq n$ [BE18].

Defining Galois scaffold

Let K_0 be a local field with residue characteristic p.
Assume K_n/K_0 is a totally ramified extension of local fields of degree p^n whose lower ramification numbers are relatively prime to p and fall into one residue class modulo p^n represented by $0 < b < p^n$.
Let $\mathbb{S}_{p^n} = \{0, 1, \ldots, p^n - 1\}$. Define $\mathfrak{a} : \mathbb{Z} \to \mathbb{S}_{p^n}$ by $\mathfrak{a}(j) \equiv -jb^{-1} \mod p^n$ [BCE18]. For $0 \leq i \leq n-1$, let $\mathfrak{a}(j)_{(i)}$ denote the i-th digit in the p-adic expansion of $\mathfrak{a}(j)$.
Put a partial order $\preceq$ on $\mathbb{S}_{p^n}$ defined by $s \preceq t$ if and only if $s_{(i)} \leq t_{(i)}$ for each $0 \leq i \leq n-1$, where $s = \sum_{i=1}^{n} s_{(n-i)} p^{n-i}$ and $t = \sum_{i=1}^{n} t_{(n-i)} p^{n-i}$ are the p-adic expansions of s and t [BCE18].

Defining Galois scaffold II

Let $G = Gal(K_n/K_0)$. Given an integer $\mathfrak{c} \geq 1$, two things are required for a *Galois scaffold of precision* $\mathfrak{c}$ [BCE18]:

1. For each $t \in \mathbb{Z}$ an element $\lambda_t \in K_n$ such that $v_n(\lambda_t) = t$ and $\lambda_s \lambda_t^{-1} \in K_0$ whenever $s \equiv t \mod p^n$.

2. Elements $\Psi_1, \Psi_2, \ldots, \Psi_n$ in the augmentation ideal $(\sigma - 1 : \sigma \in G)$ of $K_0[G]$ such that for each $1 \leq i \leq n$ and $t \in \mathbb{Z}$

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

where $u_{i,t} \in K$ and $v_K(u_{i,t}) = 0$.

Galois Module Structure i

Let $((\lambda_t)_{t\in\mathbb{Z}}, (\Psi_i)_{i=1}^n)$ be a Galois scaffold for L/K of precision $\mathfrak{c}$. Let $0 < b < p^n$ satisfy $b \equiv b_n \mod p^n$. For each $s \in \mathbb{S}_{p^n}$, let

$$\Psi^{(s)} = \Psi_n^{s_{(0)}} \Psi_{n-1}^{s_{(1)}} \cdots \Psi_1^{s_{(n-1)}} \in K[G]$$

$$\mathfrak{b}(s) = \sum_{i=1}^{n} s_{(n-i)} p^{n-i} b_i$$

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

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

where $s = \sum_{i=1}^n a_{(n-i)} p^{n-i}$ is the p-adic expansion of s [BCE18].

Galois Module Structure ii

Theorem (Byott, Childs, Elder, 2018)

1. *Suppose* $\mathfrak{c} \geq 1$. *Then* $\{\pi^{-w(s)}\Psi^{(s)} : s \in \mathbb{S}_{p^n}\}$ *is an* $\mathfrak{O}_K$*-basis for* $\mathfrak{A}_{L/K}$. *If* $w(s) = d(s)$ *for all* $s \in \mathbb{S}_{p^n}$, *then* $\mathfrak{O}_L$ *is free over* $\mathfrak{A}_{L/K}$. *Moreover,* $\mathfrak{O}_L = \mathfrak{A}_{L/K} \cdot \rho$ *for any* $\rho \in L$ *with* $v_L(\rho) = b$.
2. *Assume* $\mathfrak{c} \geq p^n + b$. *Then* $\mathfrak{O}_L$ *is free over* $\mathfrak{A}_{L/K}$ *if and only if* $w(s) = d(s)$ *for all* $s \in \mathbb{S}_{p^n}$. *Moreover, if* $\mathfrak{O}_L$ *is free over* $\mathfrak{A}_{L/K}$, *then* $\mathfrak{O}_L = \mathfrak{A}_{L/K} \cdot \rho$ *for any* $\rho \in L$ *with* $v_L(\rho) = b$ *[BCE18, Theorem 3.1].*

Theorem (Byott, Childs, Elder; 2018)

Let L/K *be a totally ramified Galois extension of degree* p^n *where* $n \geq 2$. *Assume the lower ramification numbers of* L/K *are relatively prime to* p *and fall into one residue class represented by* $0 < b < p^n$. *Assume that* L/K *possesses a Galois scaffold of precision* $\mathfrak{c} \geq p^n + b$. *Then* $\mathfrak{O}_L$ *is free over* $\mathfrak{A}_{L/K}$ *if and only if* $b \mid p^n - 1$ *[BCE18, Theorem 4.8].*

Extra-Special p-Groups

An *extra-special p-group* is a p-group G of order p^{2n+1} for some $n \geq 1$ such that $Z(G) \cong C_p$ and $G \diagup Z(G) \cong C_p^{2n}$. When p is odd there are two classes of extra-special p-groups:

(1) Exponent p, denoted $\mathbb{H}_{2n+1}(\mathbb{F}_p)$

(2) Exponent p^2, denoted $\mathbb{M}_{2n+1}(\mathbb{F}_p)$.

We use the theory of MacKenzie and Whaples [MW56] to construct totally ramified extra-special p-extensions for odd primes. Then we use the work of Byott, Elder, and Keating in [BE18] and [EK22], to construct Galois scaffolds for our extensions.

The two extra-special groups of order 8 are the quaternions Q_8 and the dihedral group D_8 which both have exponent 4. In the case $p = 2$ and $n = 1$, both of our constructions produce D_8-extensions [Bla99].

Exponent p

If B is a commutative ring with 1, we define an algebraic group

$$\mathbb{H}_{2n+1}(B) = \begin{pmatrix} 1 & \vec{a} & c \\ \vec{0} & 1 & \vec{b} \\ 0 & \vec{0} & 1 \end{pmatrix} \leq GL_{n+2}(B)$$

where $\vec{a}$ is a $1 \times n$ row vector with entries in B, $\vec{b}$ is a $n \times 1$ column vector with entries in B, and $c \in B$.
The group

$$\mathbb{H}_3(\mathbb{F}_p) = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$$

is commonly referred to as the *Heisenberg group* [EK20].

Heisenberg extensions in characteristic p

Suppose $\vec{A} := (a_1, \ldots, a_{2n+1}) \in \mathbb{H}_{2n+1}(K_0)$ such that $a_i \notin \wp(K_0)$. Choose $\vec{X} := (x_1, \ldots, x_{2n+1}) \in \mathbb{H}_{2n+1}(K_0^{sep})$ such that $\mathbf{F}(\vec{X}) = \vec{X} * \vec{A}$ that is to say $x_i^p - x_i = a_i$ for $1 \leq i \leq 2n$, and

$$x_{2n+1}^p - x_{2n+1} = a_{2n+1} + \sum_{i=1}^{n} a_{n+i}a_i.$$

For any $\vec{B} \in \mathbb{H}_{2n+1}(\mathbb{F}_p) \subseteq \mathbb{H}_{2n+1}(K_0)$ we have

$$\mathbf{F}(\vec{B} * \vec{X}) = \mathbf{F}(\vec{B}) * \mathbf{F}(\vec{X}) = B * (\vec{X} * \vec{A}) = (\vec{B} * \vec{X}) * \vec{A}.$$

So $\vec{B} * \vec{X}$ is a solution to $\mathbf{F}(\vec{T}) = \vec{T} * \vec{A}$ for all $\vec{B} \in \mathbb{H}_{2n+1}(\mathbb{F}_p)$.
Let $a \in K_0$ such that $p \nmid v_0(a) < 0$. Choose $\omega_1, \ldots, \omega_{2n+1} \in K_0$ such that $0 = v_0(\omega_1) \geq \ldots \geq v_0(\omega_{2n+1})$. For $1 \leq i \leq 2n+1$ set $a_i = a\omega_i^{p^{2n}}$ and set $\vec{A} = (a_1, \ldots, a_{2n+1})$. Assume that $v_0(a_{2n+1}) < v_0(a_{2n}^2 a_n)$.

Heisenberg extensions in characteristic p II

Choose $\vec{X} := (x_1, \ldots, x_{2n+1}) \in \mathbb{H}_{2n+1}(K_0^{sep})$ such that $\mathbf{F}(\vec{X}) = \vec{X} * \vec{A}$. That is $x_i^p - x_i = a_i$ when $1 \leq i \leq 2n$ and

$$x_{2n+1}^p - x_{2n+1} = a_{2n+1} + \sum_{j=1}^{n} a_{n+j} x_j.$$

For $1 \leq i \leq 2n+1$, set $K_i = K_{i-1}(x_i)$.

Theorem (Keating, S; 2022)

K_{2n+1}/K_0 is a totally ramified $\mathbb{H}_{2n+1}(\mathbb{F}_p)$-extension with upper ramification numbers $u_i = -v_0(a_i)$ for $1 \leq i \leq 2n+1$. Moreover, K_{2n+1}/K_0 possesses a Galois scaffold of precision $\mathfrak{c} = b_{2n+1} - p^{2n}(u_{2n} + u_n) \geq p^{2n} + b_{2n}$.

Heisenberg extensions in characteristic 0 I

Let $a \in K_0$ such that $p \nmid v_0(a)$ and $-\frac{pe_0}{p-1} < v_0(a) < 0$. Choose $\omega_1, \ldots, \omega_{2n+1} \in K_0$ such that $0 = v_0(\omega_1) \geq v_0(\omega_2) \geq \ldots \geq v_0(\omega_{2n+1})$. For $1 \leq i \leq 2n+1$ set $a_i = a\omega_i^{p^{2n}}$ and set $\vec{A} = (a_1, \ldots, a_{2n+1})$. Assume that $v_0(a_{2n+1}) < v_0(a_{2n}^2 a_n)$, and

$$v_0(p^{p^2} a_{2n+1}^{p(p-1)} a_{2n}^p a_n) > 0.$$

Heisenberg extensions in characteristic 0 II

Choose $\vec{X} := (x_1, \ldots, x_{2n+1}) \in \mathbb{H}_{2n+1}(K_0^{sep})$ such that $\mathbf{F}(\vec{X}) = \vec{X} * \vec{A}$. That is

$$x_i^p - x_i = a_i \text{ when } 1 \leq i \leq 2n,$$

$$x_{2n+1}^p - x_{2n+1} = a_{2n+1} + \sum_{j=1}^{n} a_{n+j} x_j \text{ when } i = 2n+1.$$

For $1 \leq i \leq 2n+1$, let $K_i = K_{i-1}(x_i)$.

Theorem (Keating, S; 2022)

K_{2n+1}/K_0 is a totally ramified $\mathbb{H}_{2n+1}(\mathbb{F}_p)$-extension with upper ramification numbers $u_i = -v_0(a_i)$ for $1 \leq i \leq 2n+1$. Moreover, K_{2n+1}/K_0 possesses a Galois scaffold of precision

$$\mathfrak{c} = \min\{b_{2n+1} - p^{2n}(u_{2n} + u_n), p^{2n+1}e_0 + b_{2n+1} - p^{2n+1}u_{2n+1}\} \geq p^{2n} + b_{2n}.$$

Exponent p^2

Let B be a commutative ring with 1. Let

$$D(X,Y) = \frac{X^p + Y^p - (X+Y)^p}{p} = \sum_{i=1}^{p-1} p^{-1}\binom{p}{i} X^{p-i}Y^i \in \mathbb{Z}[X,Y].$$

Define an operation $*$ on B^{2n+1} by

$$(X_1, \ldots, X_{2n}, X_{2n+1}) * (Y_1, \ldots, Y_{2n}, Y_{2n+1}) = (Z_1, \ldots, Z_{2n}, Z_{2n+1})$$

where

$$Z_i = \begin{cases} X_i + Y_i, & \text{for} \quad 1 \le i \le 2n \\ X_{2n+1} + Y_{2n+1} + X_n^p Y_{2n} + D(X_n, Y_n) + \sum_{j=1}^{n-1} X_j Y_{n+j} & \text{for} \quad i = 2n+1. \end{cases}$$

Let $\mathbb{M}_{2n+1}(B)$ denote the group $(B^{2n+1}, *)$.

The group $\mathbb{M}_3(\mathbb{F}_p)$

Note that $\mathbb{M}_3(\mathbb{F}_p) \cong \langle x, y | x^{p^2} = 1 = y^p, yxy^{-1} = x^{1+p} \rangle \cong C_{p^2} \rtimes C_p$. So $\mathbb{M}_3(\mathbb{F}_p)$ is a *metacyclic* group. Now we will call $\mathbb{M}_{2n+1}$ the *generalized metacyclic group*.

Generalized metacyclic extension in characteristic p

As was the case with $\mathbb{H}_{2n+1}$, it is easy to construct $\mathbb{M}_{2n+1}(\mathbb{F}_p)$-extensions in characteristic p. Now we construct $\mathbb{M}_{2n+1}(\mathbb{F}_p)$-extensions that possess a scaffold. Choose $a \in K_0$ such that $p \nmid v_0(a) < 0$. Choose $\omega_1, \dots, \omega_{2n+1} \in K_0$ such that $0 = v_0(\omega_1) \geq \dots \geq v_0(\omega_{2n+1})$. For $1 \leq i \leq 2n+1$, set $a_i = a\omega_i^{p^{2n}}$ and set $\vec{A} = (a_1, \dots, a_{2n+1})$. Assume that $v_0(a_{2n+1}) < \min\{v_0(a_{2n}^2 a_n), v_0(a_{2n} a_n^p)\}$.

Generalized metacyclic ext in characteristic p II

Choose $\vec{X} := (x_1, \ldots, x_{2n+1}) \in \mathbb{M}_{2n+1}(\mathbb{F}_p)$ such that $\mathbf{F}(\vec{X}) = \vec{X} * \vec{A}$. That is $x_i^p - x_i = a_i$ for $1 \leq i \leq 2n$, and

$$x_{2n+1}^p - x_{2n+1} = a_{2n+1} - a_{2n}x_n^p - \sum_{j=1}^{n-1} a_{n+j}x_j - D(x_n, a_n).$$

For $1 \leq i \leq 2n+1$, let $K_i = K_{i-1}(x_i)$.

Theorem (Keating, S; 2022)

K_{2n+1}/K_0 is a totally ramified $\mathbb{M}_{2n+1}(\mathbb{F}_p)$-extension with upper ramification numbers $u_i = -v_0(a_i)$ for $1 \leq i \leq 2n+1$. Moreover, K_{2n+1}/K_0 possesses a Galois scaffold of precision
$\mathfrak{c} = \min\{b_{2n+1} - p^{2n}(u_{2n} + u_n), b_{2n+1} - (p-1)p^{2n}u_n\} \geq p^{2n} + b_{2n}$.

Generalized metacyclic extensions in characteristic 0

Let $a \in K_0$ such that $p \nmid v_0(a)$ and $-\frac{pe_0}{p-1} < v_0(a) < 0$. Choose $\omega_1, ..., \omega_{2n+1} \in K_0$ such that $0 = v_0(\omega_1) \geq v_0(\omega_2) \geq \ldots \geq v_0(\omega_{2n+1})$. For $1 \leq i \leq 2n+1$ set $a_i = a\omega_i^{p^{2n}}$ and set $\vec{A} = (a_1, \ldots, a_{2n+1})$. Assume that $v_0(a_{2n+1}) < \min\{v_0(a_{2n}^2 a_n), v_0(a_{2n} a_n^p)\}$ and

$$v_0(p^p a_{2n+1}^{p-1} a_{2n}^p a_n) > 0.$$

Generalized metacyclic ext in characteristic 0 II

Choose $\vec{X} := (x_1, \ldots, x_{2n+1}) \in \mathbb{M}_{2n+1}(K_0^{sep})$ such that $\mathbf{F}(\vec{X}) = \vec{X} * \vec{A}$. That is $x_i^p - x_i = a_i$ for $1 \leq i \leq 2n$ and

$$x_{2n+1}^p - x_{2n+1} = a_{2n+1} - a_{2n}x_n^p - \sum_{j=1}^{n-1} a_{n+j}x_j - D(x_n, a_n).$$

For $1 \leq i \leq 2n+1$, set $K_i = K_{i-1}(x_i)$.

Theorem (Keating, S; 2022)

K_{2n+1}/K_0 is a totally ramified $\mathbb{M}_{2n+1}$-extension with upper ramification numbers $u_i = -v_0(a_i)$ for $1 \leq i \leq 2n+1$. Moreover, K_{2n+1}/K_0 possesses a Galois scaffold of precision
$\mathfrak{c} = \min\{p^{2n+1}e_0 + b_{2n+1} - p^{2n+1}u_{2n+1}, b_{2n+1} - p^{2n+1}u_n, b_{2n+1} - p^{2n}(u_n + u_{2n})\} \geq p^{2n} + b_{2n}$.

Bondarko-Dievsky

Now we restrict to the case $\mathrm{Char}(K) = 0$.

Lemma (Bondarko, Dievsky; 2009)

Let L/K be a totally ramified Galois (non-cyclic) p-extension of degree $q = p^n$ such that $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$. If the ramification numbers for L/K are congruent to -1 modulo q, then $\mathfrak{A}_{L/K}$ does not contain any non-trival idempotents [BD09, Lemma 2.18].

Theorem (Bondarko, Dievsky; 2009)

Let G be a non-cyclic p-group, and $\mathfrak{A} \subseteq K[G]$ an $\mathfrak{O}_K$-order. The following are equivalent:

1. *there exits a totally ramified Galois extension L/K such that $\mathfrak{A}_{L/K} = \mathfrak{A}$, $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$, $\mathfrak{A}_{L/K}$ does not contain any non-trivial idempotents, and the different $\mathfrak{D}_{L/K}$ is generated by an element of K;*
2. *$\mathfrak{A}$ is a colocal comonogenic Hopf algebra*

[BD09, Theorem 3.11].

An Example

Let $K_0 = \mathbb{Q}_3\left(i, \sqrt[113]{3}\right)$, so $p = 3$ and $e_0 = 113$. Let $b = p^3 - 1 = 26$, $a_1 = \pi_0^{-b}$, $a_2 = i^9 a_1 = ia_1$, and $a_3 = (\pi_0^{-10})^9 a_1$. Let x_1, x_2, x_3 satisfy

$$\begin{aligned} x_1^3 - x_1 &= a_1 \\ x_2^3 - x_2 &= a_2 \\ x_3^3 - x_3 &= a_3 + a_1 a_2 + a_2 x_1 + D(a_1, x_1), \end{aligned}$$

and let $K_3 = K_0(x_1, x_2, x_3)$. It is the case that K_3/K_0 is a totally ramified $\mathbb{M}_3[\mathbb{F}_3]$-extension which possesses a Galois scaffold of precision $\mathfrak{c} = 134$. The lower ramification numbers for K_3/K_0 are $b_1 = b_2 = 26$ and $b_3 = 836$ with residue -1 modulo 9 represented by b. Since the precision is greater than $p^3 + b = 53$, it follows from the theory of Byott, Childs and Elder that $\mathfrak{O}_3$ is free over $\mathfrak{A}_{K_3/K_0}$. Now it follows from the Bondarko-Dievsky theorem that $\mathfrak{A}$ is a Hopf algebra. One can try to use the $\mathfrak{O}_0$-basis for $\mathfrak{A}_{K_3/K_0}$ constructed in [BCE18, Theorem 3.1(1)], but it seems to be very complicated.

THANK YOU

References I

- Nigel P. Byott, Lindsay N. Childs, and G. Griffith Elder, *Scaffolds and generalized integral module structure*, Annales De L'Institut Fourier **68** (2018), no. 3, 965–1010.
- M.V. Bondarko and A.V. Dievsky, *Non-abelian associated orders of wildly ramified extensions*, Journal Of Mathematical Sciences **156** (2009), no. 6.
- Nigel P. Byott and G. Griffith Elder, *Galois scaffolds and Galois module structure in extensions of characteristic p local fields of degree p^2*, Journal of Number Theory **133** (2013), 3598–3610.
- ———, *Sufficient conditions for large Galois scaffolds*, Journal of Number Theory **182** (2018), 95–130.
- Simon R Blackburn, *Groups of prime power order with derived subgroup of prime order*, Journal of Algebra **219** (1999), no. 2, 625–657.
- Griffith Elder and Kevin Keating, *Generic ramification in generalized Heisenberg extensions*, pre-print (2020).

References II

G.G. Elder and K. Keating, *Generic p-extensions in characteristic p. (preprint)*.

R. E. Mackenzie and G. Whaples, *Artin-Schreier equations in characteristic zero*, American Journal of Mathematics **73** (1956), no. 3, 473–485.