Galois Scaffolds and Galois Module Structure for Cyclic Extensions of Degree p^2 in Characteristic 0

Paul Schwartz

Under the supervision of Kevin Keating

University of Florida

May 27, 2021

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 $K_0 \subseteq K_1 \subseteq K_2$ is a tower of totally ramified fields we may replace the subscript K_i by the subscript i for $0 \leq i \leq 2$ giving us v_i, e_i, $\mathfrak{O}_i$, $\mathfrak{M}_i$ and π_i.

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 $G = H_0 \supset H_1 \supset \ldots \supset H_{n-1} \supset H_n = \{1\}$ such that $H_i/H_{i+1} \cong C_p$ for $0 \leq i \leq n-1$ and $\{G_i : i \geq -1\} \subseteq \{H_i : 0 \leq i \leq n\}$.

Ramification numbers

For $0 \leq i \leq n-1$, choose $\sigma_{i+1} \in H_i \setminus H_{i+1}$ and set

$b_i = v_L((\sigma_i - 1)\pi_L) - 1$, this integer is independent of the choices made

and we call it the i-th *lower ramification number*.

The *upper ramification number* $u_1, ..., u_n$ are defined recursively by

$u_1 = b_1, u_i = u_{i-1} + \dfrac{b_i - b_{i-1}}{p^{i-1}}$ for $2 \leq i \leq n$.

Introduction I

In 2013 N.P. Byott and G.G. Elder constructed totally ramified C_{p^2}-extensions in characteristic p, K_2/K_0, which possess a Galois scaffold, this was a K_2-basis for $K[Gal(K_2/K_0)]$ whose effect on the valuation of elements of K_2 is easy to determine.

If K_2/K_0 is such an extension, it is the case that the lower ramification numbers for K_2/K_0 are relatively prime to p and fall into one residue class modulo p^2, represented by $0 < b < p^2$.

They conclude that the ring of integers $\mathfrak{O}_2$ is free over its associated order $\mathfrak{A}_{K_2/K_0} = \{\alpha \in K_0[Gal(K_2/K_0)] : \alpha\mathfrak{O}_2 \subseteq \mathfrak{O}_2\}$ if and only if $b \mid p^2 - 1$.

Introduction II

Since 2013, much work has been done to generalize Galois scaffolds, make them easier to construct, and study how they determine Galois module structure.

We combine the new theory with Byott and Elder's 2013 paper and Artin-Schreier Witt vectors in characteristic 0 (thanks to the recommendation of Elder) in order to translate these results to the setting of C_{p^2}-extensions in characteristic 0.

Defining Galois Scaffold I

Let K_0 be a local field with residue characteristic p.

Assume K_2/K_0 is a totally ramified C_{p^2}-extension whose lower ramification numbers are relatively prime to p and fall into one residue class modulo p^2 represented by $0 < b < p^2$.

Let $\mathbb{S}_{p^2} = \{0, 1, ..., p^2 - 1\}$. Define $\mathfrak{a} : \mathbb{Z} \to \mathbb{S}_{p^2}$ by $\mathfrak{a}(j) \equiv jb^{-1} \mod p^2$.

For $0 \leq i \leq 1$ let $\mathfrak{a}(j)_{(i)}$ denote the i-th digit in the p-adic expansion of $\mathfrak{a}(j)$.

Defining Galois Scaffold II

Let $G = Gal(K_2/K_0)$. Given an integer $\mathfrak{c} \geq 1$, two things are required for a *Galois scaffold of precision* $\mathfrak{c}$ [BCE, Definition 2.3]:

1. For each $t \in \mathbb{Z}$ an element $\lambda_t \in K_2$ such that $v_2(\lambda_t) = t$ and $\lambda_s \lambda_t^{-1} \in K_0$ whenever $s \equiv t \mod p^2$.

2. Elements Ψ_1, Ψ_2 in the augmentation ideal $(\sigma - 1 : \sigma \in G)$ of $K_0[G]$ such that for each $1 \leq i \leq 2$ and $t \in \mathbb{Z}$

$$\Psi_i \lambda_t \equiv \begin{cases} u_{i,t} \lambda_{t+p^{2-i}b_i} & \mod \lambda_{t+p^{2-i}b_i} \mathfrak{M}_2^{\mathfrak{c}} \quad \text{if } \mathfrak{a}(t)_{(2-i)} \geq 1 \\ 0 & \mod \lambda_{t+p^{2-i}b_i} \mathfrak{M}_2^{\mathfrak{c}} \quad \text{if } \mathfrak{a}(t)_{(2-i)} = 0 \end{cases}$$

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

Depth of ramification

Let K be a local field and let L/K be a finite extension. We have the following definition from Hyodo (1987). For finite M/L, and $F \in \{M, L, K\}$ define the depth of ramification (with respect to F) by

$$d_F(M/L) := \inf\{v_F\left(Tr_{M/L}(y)/\,y\right) : y \in M \setminus \{0\}\}.$$

It is elementary to see that $d_F(M/L) \geq 0$. Hyodo points out that

$$d_F(M/L) = v_F(\mathfrak{D}_{M/L}) - v_F(\pi_L) + v_F(\pi_M) \tag{1}$$

where $\mathfrak{D}_{M/L}$ is the different for M/L.

Nice formulas

So if M/K is a totally ramified C_{p^2}-extension we see that

$$d_M(M/K) = (p-1)b_2 + p(p-1)b_1.$$

It also follows from (1) that

$$d_F(M/L) = d_F(M/N) + d_F(N/L)$$

for any intermediate field N.

Witt vectors

Let B be a commutative ring with unity. Let

$$S_1(X_1, Y_1) = X_1 + Y_1$$

$$S_2(X_1, X_2, Y_1, Y_2) = X_2 + Y_2 + \frac{X_1^p + Y_1^p - (X_1 + Y_1)^p}{p}.$$

Let the *Witt vectors of length 2 over B* be the set $W_2(B) = B \times B$ with addition defined by

$$(a_1, a_2) \oplus (b_1, b_2) = (S_1(a_1, b_1), S_2(a_1, a_2, b_1, b_2)).$$

Artin-Schreier operator

Define the *Frobenius map* $\mathrm{F} : W(B) \to W(B)$ by $\mathrm{F}(a_1, a_2) = (a_1^p, a_2^p)$. The map $\wp = \mathrm{F} - id$ (Witt vector subtraction) is called the *Artin-Schreier operator*.

The following allows us to construct C_{p^2}-extensions using Artin-Schreier equations.

Artin-Schreier Witt equations

From this point K_0 denotes a finite extension of $\mathbb{Q}_p$ and we fix an algebraic closure K_0^{alg} of K_0.

Theorem (Vostokov, Zukov; 1995)

Let $a_1 \in K_0$ such that $-\frac{p}{p^2-1}e_0 < v_0(a_1) \leq 0$. Also let $a_2 \in K_0$ with $v_0(a_1) + v_0(a_2) > -\frac{p}{p-1}e_0$. Put $K_2 = K_0(x_1, x_2)$ for $\wp(x_1, x_2) = (a_1, a_2)$. If $x_1 \notin K_0$, then K_2/K_0 is a C_{p^2}-extension and

$$d_{K_0}(K_2/K_0) < \frac{p^2+1}{p^2+p}e_0.$$

Choices

Here we use Witt vectors to construct a totally ramified C_{p^2}-extension which possesses a Galois scaffold.

Choice

Choose $a_1 \in K_0 \setminus \wp(K_0)$ *such that* $p \nmid v_0(a_1)$ *and* $-\frac{p}{p^2-1}e_0 < v_0(a_1) < 0$.

Choice

Choose $\mu \in K_0$ *such that* $m := -v_0(\mu) > 0$ *satisfies:*

$$\frac{p}{p-1}e_0 > pm - \left(2 + \frac{1}{p(p-1)}\right) v_0(a_1) \tag{2}$$

$$p^2 m > -(p^2-1)v_0(a_1). \tag{3}$$

Declarations

Set $a_2 = \mu^p a_1$ and let $x_1, x_2 \in K_0^{alg}$ satisfy $\wp(x_1, x_2) = (a_1, a_2)$. That is to say

$$x_1^p - x_1 = a_1 \quad \text{and} \quad x_2^p - x_2 = a_2 + \frac{x_1^p + a_1^p - (x_1 + a_1)^p}{p}.$$

Set

$$K_1 = K_0(x_1) \quad \text{and} \quad K_2 = K_0(x_1, x_2).$$

Observe that a_1 and a_2 were chosen so that K_1/K_0 is a totally ramified C_p-extension and K_2/K_0 is a C_{p^2}-extension.

Ramification

Since $p \mid v_1(a_2)$ we have to prove the following:

Proposition (Keating, S; 2021)

K_2/K_0 is a totally ramified extension with lower ramification numbers $b_1 = -v_0(a_1)$ and $b_2 = p^2 m + b_1$. The upper ramification numbers for K_2/K_0 are $u_1 = b_1$ and $u_2 = -v_0(a_2) = pm + b_1$.

It follows from (3) that

$$b_2 > p^2 b_1. \tag{4}$$

Because we're in characteristic 0

Proposition (Keating, S; 2021)

Let $C_1 = \frac{x_1^p + 1 - (x_1+1)^p}{p} \in K_1$. *There is* $\sigma_1 \in Gal(K_2/K_0)$ *such that*

$$(\sigma_1 - 1)x_1 = 1 + \epsilon$$

$$(\sigma_1 - 1)x_2 = C_1 + \delta'$$

where $v_2(\epsilon) = p^2 e_0 - p(p-1)b_1 > 0$ *and* $v_2(\delta') > 0$.

This means that

$$\sigma_1(x_1, x_2) \equiv (x_1, x_2) \oplus (1, 0) \mod W_2(\mathfrak{M}_2)$$

Things we need for the scaffold

Set $\sigma_2 = \sigma_1^p$, we find that $\sigma_2(x_1, x_2) \equiv (x_1, x_2) \oplus (0, 1) \mod W_2(\mathfrak{M}_2)$.

So $(\sigma_2 - 1)x_2 = 1 + \delta$ for some $\delta \in \mathfrak{M}_2$. Moreover, we can show that

$v_2(\delta) \geq p^2 e_0 + (p-1)v_1(a_2) = p^2 e_0 - p(p-1)u_2 > 0$.

For $x, y \in K_2$ we have *truncated exponentiation* given by

$$x^{[y]} = \sum_{i=0}^{p-1} \binom{y}{i} (x-1)^i$$

where $\binom{y}{i} = \frac{y(y-1)\cdots(y-i+1)}{i!}$.

The scaffold

Following the construction given in "Sufficent conditions for large Galois scaffolds" [Byott, Elder; 2018] we get a scaffold.

Theorem (Keating, S; 2021)

There is a Galois scaffold for K_2/K_0 of precision

$$\mathfrak{c} \geq \min\{b_2 - p^2 b_1, p^2 e_0 - (p-1)b_2 - p(p-1)b_1\}$$

with Ψ_1 and Ψ_2 defined by $\Psi_1 + 1 = \sigma_1 \sigma_2^{[\mu]} = \sigma_1 \sum_{i=0}^{p-1} \binom{\mu}{i} (\sigma_2 - 1)^i$ *and* $\Psi_2 = \sigma_2 - 1$.

Meat and potatoes

Thanks to the work done in "Scaffolds and Generalized Integral Module Structure" [Byott, Childs, Elder; 2018] we get the following:

Corollary (Keating, S; 2021)

For each $0 \leq i, j \leq p-1$

$$v_2\left(\Psi_1^i \Psi_2^j \alpha\right) = v_2(\alpha) + jb_2 + ipb_1$$

whenever $\alpha \in K_2$ *satisfies* $v_2(\alpha) \equiv b_2 \mod p^2$.

Book keeping

For $a \geq 0$ let

$$\Psi^{(a)} = \begin{cases} \Psi_2^{a_{(1)}} \Psi_1^{a_{(0)}}, & a < p^2 \\ 0, & \text{otherwise} \end{cases}$$

where $a = \sum_{i=0}^{\infty} a_{(i)} p^i$ with $0 \leq a_{(i)} \leq p-1$. Also define a function $\mathfrak{b}$ from the non-negative integers to $\mathbb{Z} \cup \{\infty\}$ by

$$\mathfrak{b}(a) = \begin{cases} (1 + a_{(1)}) b_2 + a_{(0)} p b_1, & a < p^2 \\ \infty, & \text{otherwise} \end{cases}$$

If $\rho \in K_2$ with $v_2(\rho) = b_2$, we see that $v_2(\Psi^{(a)}\rho) = \mathfrak{b}(a)$ for $0 \leq a < p^2$.

Basis elements

For $0 \leq a < p^2$, set $d_a = \left\lfloor \frac{\mathfrak{b}(a)}{p^2} \right\rfloor$, so $\mathfrak{b}(a) = d_a p^2 + r(\mathfrak{b}(a))$ where $r(\mathfrak{b}(a))$ is the least non-negative residue modulo p^2 of $\mathfrak{b}(a)$. Also set $d_a = \infty$ when $a \geq p^2$. For $0 \leq j < p^2$ let $w_j = \min\{d_{j+a} - d_a : 0 \leq a < p^2 - j\}$. Fix $\rho_0 \in K_2$ with $v_2(\rho_0) = r(b_2)$ Set $\rho = \pi_0^{d_0} \rho_0$, so $v_2(\rho) = b_2$. Moreover, for $a \geq 1$ set

$$\rho_a = \pi_0^{-d_a} \Psi^{(a)} \rho.$$

Now $\rho_a = 0$ whenever $a \geq p^2$ and $v_2(\rho_a) = r(\mathfrak{b}(a))$ when $0 \leq a < p^2$. Thus $\{\rho_a\}_{a=0}^{p^2-1}$ is a $\mathfrak{O}_0$-basis for $\mathfrak{O}_2$. Additionally, $\{\Psi^{(a)}\}_{a=0}^{p^2-1}$ is a K_0-basis for $K_0[G]$.

Obstacles

In characteristic p it is the case that $\Psi_1^p = \Psi_2$ and $\Psi_2^p = 0$. In characteristic 0 we have to make due with the approximations

$$\Psi_1^p \rho \equiv \Psi_2 \rho \mod \mathfrak{M}_2^{p^2 e_0 - (p-1)b_2 + pb_1}$$
$$\Psi_2^p \rho \equiv 0 \mod \mathfrak{M}_2^{p^2 e_0 + b_2}.$$

Additionally, in characteristic p it is true that $\Psi^{(j)}\rho_r = \pi_0^{d_{j+r} - d_r}\rho_{j+r}$ for all $j, r \geq 0$. This is a very powerful result and it takes a lot of calculations to make up for its absence.

More like characteristic p

Observe that if

$$p^2 e_0 - (p+1)b_2 + (p-1)b_1 > 0 \tag{5}$$

then $p^2 e_0 - (p-1)b_2 + pb_1 > 2b_2$ which implies that $v_2(\Psi_1^p \rho) = 2b_2$.

This leads us to our main result...

Main result

Theorem (Keating, S; 2021)

Let K_2/K_0 be the C_{p^2}-extension constructed using the choices above.

Assume further that the lower ramification numbers b_1 and b_2 satisfy (5).

(a) The associated order $\mathfrak{A}_{K_2/K_0}$ of $\mathfrak{O}_2$ has $\mathfrak{O}_0$-basis $\{\pi_0^{-w_j}\Psi^{(j)}\}_{j=0}^{p^2-1}$.

(b) If $w_j = d_j - d_0$ for all $0 \leq j \leq p^2 - 1$, then $\mathfrak{O}_2$ is free over $\mathfrak{A}_{K_2/K_0}$; moreover, $\mathfrak{O}_2 = \mathfrak{A}_{K_2/K_0} \cdot \rho_0$.

(c) Conversely, if $\mathfrak{O}_2$ is free over $\mathfrak{A}_{K_2/K_0}$ then $w_j = d_j - d_0$ for all $0 \leq j \leq p^2 - 1$.

Final result

Corollary (Keating, S; 2021)

Let K_2/K_0 satisfy the conditions of the previous theorem. Let $r(b_2)$ be the least non-negative residue of b_2 modulo p^2. Then $\mathfrak{O}_2$ is free over its associated order $\mathfrak{A}_{K_2/K_0}$ if and only if $r(b_2) \mid p^2 - 1$. Furthermore, if $\mathfrak{O}_2$ is free over $\mathfrak{A}_{K_2/K_0}$ then $\mathfrak{O}_2 = \mathfrak{A}_{K_2/K_0} \cdot \rho_0$ for any $\rho_0 \in K_2$ such that $v_2(\rho_0) = r(b_2)$.

End

Thank You

References

[BCE] Nigel P. Byott, Lindsay N. Childs, G. Griffith Elder, Scaffolds and Generalized Integral Module Structure, Tome 68, no 3 (2018) 965-1010.

[BE13] Nigel P. Byott, 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.

[BE18] N. P. Byott, G. G. Elder, Sufficient Conditions For Large Galois Scaffolds, Journal of Number Theory 182 (2018) 95-130.

[E] G. Griffith Elder, A valuation criterion for normal basis generators in local fields of characteristic p, Arch. Math. 94 (2010), 43-47.

References 2

[FV] I.B. Fesenko, S. V. Vostokov, Local Fields and Their Extensions (2nd edition) Translations of mathematical monographs. 1993. American Mathematical Society.

[H] O. Hyodo, Wild Ramification in the Imperfect Residue Field Case, Advanced Studies in Mathematics 12, 1987, Galois Representations and Arithmetic Algebraic Geometry pp. 287-314.

[MW] R. E. Mackenzie, G. Whaples, Artin-Schreier Equations in Characteristic Zero, American Journal of Mathematics, Vol 78, No. 3 (July 1956), pp. 473-485. The Johns Hopkins University Press.

References 3

[VZ] S. V. Vostokov, I. B. Zhukov, Some approaches to the construction of abelian extensions for p-adic fields, Amer. Math Soc. Transl. (2) Vol. 166, 1995.