JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

G. Griffith ELDER

Ramified extensions of degree p and their Hopf–Galois module structure

Tome 30, n^{o} 1 (2018), p. 19-40.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_1_19_0>

Journal de Théorie des Nombres de Bordeaux **30** (2018), 19–40

Ramified extensions of degree p and their Hopf–Galois module structure

par G. Griffith ELDER

Résumé. Les extensions cycliques ramifiées L/K de degré p d'un corps local dont la caractéristique résiduelle est p sont plutôt bien comprises. Elles sont définies par une équation d'Artin–Schreier sauf lorsque $\mathrm{char}(K) = 0$ et $L = K(\sqrt[p]{\pi_K})$ pour une certaine uniformisante $\pi_K \in K$. De plus, depuis les travaux de Bertrandias–Ferton ($\mathrm{char}(K) = 0$) puis Aiba ($\mathrm{char}(K) = p$), plusieurs résultats sont connus sur la structure galoisienne des idéaux de telles extensions: on sait par exemple décrire la structure de chaque idéal $\mathfrak{P}_L^n$ comme module sur son ordre associé $\mathfrak{A}_{K[G]}(n) = \{x \in K[G] : x\mathfrak{P}_L^n \subseteq \mathfrak{P}_L^n\}$, où $G = \mathrm{Gal}(L/K)$. Le but de cet article est d'étendre ces résultats aux extensions séparables et ramifiées de degré p qui ne sont pas galoisiennes.

Abstract. Cyclic, ramified extensions L/K of degree p of local fields with residue characteristic p are fairly well understood. They are defined by an Artin–Schreier equation, unless $\mathrm{char}(K) = 0$ and $L = K(\sqrt[p]{\pi_K})$ for some prime element $\pi_K \in K$. Moreover, through the work of Bertrandias–Ferton ($\mathrm{char}(K) = 0$) and Aiba ($\mathrm{char}(K) = p$), much is known about the Galois module structure of the ideals in such extensions: the structure of each ideal $\mathfrak{P}_L^n$ as a module over its associated order $\mathfrak{A}_{K[G]}(n) = \{x \in K[G] : x\mathfrak{P}_L^n \subseteq \mathfrak{P}_L^n\}$ where $G = \mathrm{Gal}(L/K)$. The purpose of this paper is to extend these results to separable, ramified extensions of degree p that are not Galois.

1. Introduction

Let K be a local field with valuation v_K normalized so that $v_K(K^\times) = \mathbb{Z}$, and with finite residue field κ of characteristic $p > 0$. This means that either

Manuscrit reçu le 19 octobre 2015, révisé le 19 avril 2017, accepté le 19 avril 2017.
2010 *Mathematics Subject Classification.* 11S15, 11R33, 16T05.
Mots-clefs. Artin–Schreier equation, Galois module structure.
I thank Alan Koch for discussions that led to this project; thank Martha Rzedowski-Calderón for explaining equation (1.2) in the theory of global function fields; thank Lindsay Childs for advice on the proof of Theorem 3.1; thank Nigel Byott for the conclusions of Corollary 3.6; thank the University of Exeter for its hospitality in 2014-2015 while this paper was being written; and finally, I would like to thank the anonymous referee for their many helpful suggestions.

K is a finite extension of the field of p-adic numbers $\mathbb{Q}_p$, or K is the field of Laurent series $\kappa((X))$ with X indeterminate. We are interested in ramified extensions L of degree p over K. Some of these extensions are generated by a root of a prime element $\pi_K \in K$, namely, $L = K(x)$ with $x^p = \pi_K$. We call them *atypical*: If $\mathrm{char}(K) = p$, these are the inseparable totally ramified extensions. If $\mathrm{char}(K) = 0$ and K contains the pth roots of unity, these are precisely the degree p Galois extensions whose ramification break is divisible by p. In this paper, we are interested in the other extensions, which we call *typical*: the separable and totally ramified degree p extensions that cannot be generated by a root of a prime element. Such extensions include ramified Artin–Schreier extensions, for which a certain uniformity of approach to Galois module structure, based upon the particularly simple defining equation, is available. It is this uniformity of approach, based upon a similar defining equation, that we extend to all typical extensions.

As is well-known, when a typical extension L/K is Galois, it can be defined by an Artin–Schreier polynomial

$$p(x) = x^p - x - \beta \in K[x]. \tag{1.1}$$

The ramification break b satisfies $p \nmid b$ where $v_K(\beta) = -b$. Recall that a ramification break in a Galois extension (variously, also a ramification jump or ramification number) is an integer $i \geq -1$ such that $G_i \neq G_{i+1}$ where $G_i = \{\sigma \in \mathrm{Gal}(L/K) : v_L((\sigma - 1)\pi_L) \geq i + 1\}$ is the ramification filtration of the Galois group [23, Chapter IV]. Our first result, which appears in §2, proves that every typical extension can be defined by a polynomial of the form

$$p(x) = x^p - \alpha x - \beta \in K[x]. \tag{1.2}$$

Here again, the ramification break for L/K (defined appropriately) is linked in a transparent manner to the coefficients. The result is proven by adjusting the argument of [21] for Galois typical extensions, as presented in [12, Chapter III §2]. Of course, these extensions may also be defined in terms of Eisenstein polynomials, as in [2]. The value in using equation (1.2) is that in addition to a transparent description of ramification, other properties that include Galois module structure can be easily described. In the setting of global function fields, equation (1.2) is used to determine the Hasse–Witt invariant [25, 20].

In §3, we turn to Galois module structure, or rather what, for a general typical extension, must be called Hopf–Galois module structure. In its classical setting, when L/K is Galois with $G = \mathrm{Gal}(L/K)$, the search is for an integral version of the Normal Basis Theorem. Based upon results of Noether and Leopoldt, the quest is for those conditions under which the ring of integers $\mathfrak{O}_L = \{x \in L : v_L(x) \geq 0\}$ in L is free over its associated order $\mathfrak{A}_{K[G]} = \{y \in K[G] : y\mathfrak{O}_L \subseteq \mathfrak{O}_L\}$ in $K[G]$, the largest $\mathfrak{O}_K$-order in

$K[G]$ that acts on $\mathfrak{O}_L$. For general extensions, this and variations of this question present very difficult problems, and progress, starting in the 1970s, has been slow.

On the other hand, for one specific class of extensions, cyclic of degree p, progress has been good [1, 4, 11, 15, 22, 24]. One explanation for the progress with cyclic ramified extensions of degree p is that these extensions, unless they are generated by a root of a prime element, naturally possess a *scaffold*. This is discussed in [6, Example 2.8]. Since the definition of a scaffold as presented in [6, §2] is a challenge to quickly digest, we point out (and explain in §3.2) that a very simple sufficiency condition is available for extensions of degree p: If there is an element $x \in L$ with $p \nmid v_L(x)$ and an element $\Psi \in K[G]$ that "acts like" the derivative d/dx on the K-basis $\{x^i\}_{i=0}^{p-1}$ for L over K, there is a scaffold. As we shall see, "acts like" is exact if $\mathrm{char}(K) = p$, namely $\Psi \cdot x^i = ix^{i-1}$ for $0 \le i < p$. If $\mathrm{char}(K) = 0$, it is approximate:

$$\Psi \cdot x^i \equiv ix^{i-1} \bmod x^{i-1}\mathfrak{P}_L^{\mathfrak{c}},$$

where $\mathfrak{P}_L = \{x \in L : v_L(x) > 0\}$ is the prime ideal and the degree of approximation is captured by the integer $\mathfrak{c} \ge 1$, the *precision* of the scaffold. The *shift parameter* for this scaffold is $-v_L(x)$.

As explained in [6, Example 2.8], a cyclic typical extension L/K possesses a scaffold of precision

$$\mathfrak{c} = \begin{cases} \infty & \text{if } \mathrm{char}(K) = p, \\ v_L(p) - (p-1)b & \text{if } \mathrm{char}(K) = 0, \end{cases}$$

where the ramification break b of the extension is the shift parameter for the scaffold. Thus, without further restriction if $\mathrm{char}(K) = p$, but assuming $v_L(p) > (p-1)(b+2)$ if $\mathrm{char}(K) = 0$, we are able to conclude, as explained in [6, Example 3.3], that letting $0 \le \bar{b} < p$ be the least nonnegative residue of b mod p,

$$\mathfrak{O}_L \text{ is free over its associated order if and only if } \bar{b} \mid p-1.$$

This statement follows from [6, Theorem 3.1]. If $\mathrm{char}(K) = 0$, it is due to [4]. If $\mathrm{char}(K) = p$, it follows from [1].

The purpose of this paper is to extend this classical result (and others in [11, 15, 22, 24]) that were proven for cyclic typical extensions to all typical extensions L/K. This is accomplished by first using [7, §2] to identify the unique K-Hopf algebra $\mathcal{H}$ that acts upon L (making L an $\mathcal{H}$-Galois extension). This Hopf algebra has one generator. We then proceed further than [7] by explicitly describing the action of this generator on the K-basis $\{x^i\}_{i=0}^{p-1}$ for L with x satisfying (1.2). This generator "acts like" the derivative $\mathrm{d}/\mathrm{d}x$, which means that we have a $\mathcal{H}$-scaffold on L with a certain precision and shift parameter. Since a scaffold exists, we can apply the main results of [6, Theorems 3.1 and 3.6]. In particular, a similar statement with the associated order of $\mathfrak{O}_L$ in $\mathcal{H}$ defined as $\{y \in \mathcal{H} : y\mathfrak{O}_L \subseteq \mathfrak{O}_L\}$ holds. Other structural results hold as well. These are discussed briefly in §3.2.

1.1. Summary of notation. Let p be a prime. The field K is either a finite extension of the field of p-adic numbers (if $\mathrm{char}(K) = 0$), or a field of Laurent series (if $\mathrm{char}(K) = p$). Following common conventions, we use subscripts to denote field of reference. So v_K is the valuation normalized so that $v_K(K^\times) = \mathbb{Z}$, π_K is a prime element in K (with $v_K(\pi_K) = 1$), $\mathfrak{O}_K = \{x \in K : v_L(x) \geq 0\}$ is the ring of integers in K. It has a unique maximal ideal $\mathfrak{P}_K = \{x \in L : v_K(x) \geq 1\}$, and a finite residue field $\kappa = \mathfrak{O}_K/\mathfrak{P}_K$. An extension L/K is said to be *typical* if L is a ramified extension of K of degree p that *is not* generated by a pth root of a prime element π_K. As is well-known, Galois typical extensions are Artin–Schreier.

2. Typical extensions & their ramification break

The definition of ramification break for a separable, non-Galois extension appears in [23, Chapter IV §3 Remark 2], and is developed more fully in [14]. Ramification breaks occur as the first coordinates of the vertices of the Herbrand function, an increasing, continuous, piecewise linear function that maps the real halfline $[-1, \infty)$ into itself (see graphs [3, p. 116–117]). For a typical extension L/K with Galois closure M, the Herbrand function is defined to be $\varphi_{L/K} = \varphi_{M/K} \circ \psi_{M/L}$, where the Herbrand functions $\varphi_{M/K}, \varphi_{M/L}$ for the two Galois extensions, M/K and M/L, are defined as usual, and $\psi_{M/L}$ is the inverse of $\varphi_{M/L}$. See [23, Chapter IV §3 Remark 2], or [14, §1 Proposition 2].

Remark 2.1 (Caution)**.** When comparing the value of the ramification break in Theorem 2.2 with statements elsewhere in the literature, it is important to recognize that there are two different conventions regarding the graphing of the Herbrand function. One may follow [23, Chapter IV §3], as we have here, and plot the graph over the real interval $[-1, \infty)$. In this case, we shall say that the ramification break has a *Serre* value. Or one may shift the graph of the Herbrand function over by one so that it is plotted over the nonnegative reals, as in [14, p. 2274], [16, §3] and [18, §2]. In this case, we shall say that the ramification break has an *Artin* value. To translate the Serre value of a ramification break into an Artin value, simply add one.

2.1. Statement of the main result.

Theorem 2.2. *If L/K is a typical extension, there are positive integers e, f, d, and not necessarily positive integers t, b satisfying:*

(1) $ef = d$ *and* $d \mid (p-1)$,
(2) $0 \le t < e$ *and* $\gcd(t, e) = 1$ *(observe* $e = 1$ *if and only if* $t = 0$*),*
(3) $0 < b + pt/e < pv_K(p)/(p-1)$ *with* $\gcd(b, p) = 1$,

as well as two elements α and $\beta \in K$ satisfying:

(1) $v_K(\beta) = -b$,
(2) $\alpha = \pi_K^{ft}\gamma^f\mu \in \mathfrak{O}_K$ *for some units* $\gamma, \mu \in \mathfrak{O}_K^\times$ *with* μ *representing a coset of order* f *in the quotient group* $\kappa^\times/(\kappa^\times)^f$,

so that $L = K(x)$ with

$$x^p - \alpha^{(p-1)/d}x = \beta\,.$$

Conversely, every such equation defines a typical extension over K with ramification break

$$\ell = b + \frac{pt}{e}\,,$$

and different

$$\mathfrak{D}_{L/K} = \mathfrak{P}_L^{(\ell+1)(p-1)}.$$

Note $\ell \equiv b \bmod p$ in $\mathbb{Z}_{(p)}$, the integers localized at p.

The Galois closure for L/K is $M = K(x, y)$ where $y^d = \alpha$; it has inertia degree f and ramification index e over L. Moreover, there exists an integer r of order d modulo p such that, setting $\rho = r$ if $\operatorname{char}(K) = p$, or setting ρ to be the Teichmüller character for r (a primitive dth root of unity in the ring of p-adic integers $\mathbb{Z}_p$ such that $\rho \equiv r \bmod p$) if $\operatorname{char}(K) = 0$; the Galois group of M/K is generated by two automorphisms σ and τ:

$$\operatorname{Gal}(M/K) = \langle \sigma, \tau : \sigma^p = \tau^d = 1, \tau\sigma\tau^{-1} = \sigma^r \rangle,$$

with $\tau(y) = \rho y$, $\tau(x) = x$, $\sigma(y) = y$, and $\sigma(x) = x + y + y\eta$ where $\eta = 0$ if $\operatorname{char}(K) = p$, and $\eta \in M$ with $v_M(\eta) = v_M(p) - (p-1)e\ell$ if $\operatorname{char}(K) = 0$. Furthermore, the ramification break of the cyclic extension $M/K(y)$ is $e\ell$.

Remark 2.3. If $p = 2$, then $d = 1$ and the typical extension is Galois.

Remark 2.4. If a typical extension L/K is Galois, then $e = f = d = 1$, so that $t = 0$. This means that α is some unit in $\mathfrak{O}_K$, and the element x/α, which generates L/K, satisfies the Artin–Schreier equation $X^p - X = \beta/\alpha^p$. The ramification break for L/K is b, the different $\mathfrak{D}_{L/K} = \mathfrak{P}_L^{(b+1)(p-1)}$, and $(\sigma - 1)(x/\alpha) = 1 + \eta$ with $\eta = 0$ if $\operatorname{char}(K) = p$ and $\eta \in L$ with $v_L(\eta) = pv_K(p) - (p-1)b$ if $\operatorname{char}(K) = 0$.

The rest of this section is concerned with the proof of Theorem 2.2.

2.2. Proof.

2.2.1. ***Galois closure of a typical extension.*** We begin with an argument from group theory. Since the residue field κ is finite, the group $G = \mathrm{Gal}(M/K)$ for the Galois closure M/K of L/K is solvable [23, Chapter IV §2 Corollary 5]. Any solvable transitive subgroup G of the symmetric group S_p on p letters contains a unique subgroup $\langle\sigma\rangle$ of order p and is contained in the normalizer of $\langle\sigma\rangle$ in S_p (e.g. [9, p. 638 Exercise 20]). The quotient group $\mathrm{Gal}(M/K)/\langle\sigma\rangle$ is thus cyclic of order d for some $d \mid (p-1)$, as it is isomorphic to a subgroup of $\mathrm{Aut}(\langle\sigma\rangle)$. Let M^σ be the fixed field of $\langle\sigma\rangle$, a cyclic extension of K of degree d. Let $\langle\tau\rangle$ be the subgroup that fixes L. From this it follows that there is an integer r of order d modulo p such that G is as in the statement above. At this point, the elements $\sigma, \tau \in G$ along with the integers d, r are fixed.

2.2.2. ***Kummer generators.*** A subfield lattice for M/K is developed over the following paragraphs. We begin with the extension M^σ/K. Since the residue field κ contains $\mathbb{F}_p^\times$, K contains the dth roots of unity. If $\mathrm{char}(K) = p$ this is clear because $\kappa \subset K$. If $\mathrm{char}(K) = 0$, this is a consequence of Hensel's Lemma. Thus M^σ/K is a Kummer extension and $M^\sigma = K(y)$ with $y^d = \alpha$ for some $\alpha \in K$ representing a coset of order d in the quotient group $K^\times/(K^\times)^d$, and $\tau(y) = \rho y$ where $\rho \in \mathfrak{O}_K$ is the primitive dth root of unity defined in Theorem 2.2. See [17, Chapter VI §6 Theorem 6.2]. Within M^σ there is a maximal unramified extension of K, which we call K'. Let $e = [M^\sigma : K']$ and $f = [K' : K]$. Thus $d = ef$. Let π_K, $\pi_{K'}$ denote prime elements in K, K', respectively. We can replace y by $y\pi_K^i$ for some integer i, and still have a Kummer generator for M^σ/K, and so we can assume that $0 < v_{M^\sigma}(y) \le e$. Since M^σ/K' is totally ramified and tame (including the case $e = 1$ where $M^\sigma = K'$), $M^\sigma = K'(z)$ where $z^e = \pi_{K'}$. Since K'/K is unramified, $\pi_{K'} = \pi_K u$ for some $u \in \mathfrak{O}_{K'}^\times$. Since both y and z are Kummer generators of M^σ/K' we have $y = z^t\omega$ for some $1 \le t \le e$ satisfying $\gcd(t, e) = 1$, and $\omega \in \mathfrak{O}_{K'}^\times$. Thus $y^e = \pi_K^t u^t \omega^e$. Let $\omega' = u^t\omega^e \in \mathfrak{O}_{K'}^\times$. Since K'/K is an unramified Kummer extension, $K' = K(v)$ for some $v \in K'$ such that $v^f = \mu \in \mathfrak{O}_K^\times$ where μ represents a coset of order f in the quotient group $\kappa^\times/(\kappa^\times)^f$. But $\omega' = y^e/\pi_K^t$ is also a Kummer generator for K', so $\omega' = v^s\gamma$ for some $1 \le s < f$ satisfying $\gcd(s, f) = 1$, and $\gamma \in \mathfrak{O}_K^\times$. As a result, $y^d = (y^e)^f = \pi_K^{tf}\gamma^f\mu^s$. Then, without any loss of generality, we can replace μ by μ^s and relabel, since the descriptions of these two elements are the same. Now for the converse, observe that for $y^d = \alpha$ with α as above, $y^e/(\pi_K^t\gamma)$ satisfies the equation $v^f = \mu$ and thus generates an unramified extension of degree f. Furthermore, y satisfies $y^e = \pi_K^t\gamma v \in K'$. Since $\gcd(t, e) = 1$, let $t't \equiv 1 \bmod e$. Then the e-th power of $y^{t'}$ belongs to $\pi_{K'}(K')^e$ for some prime element $\pi_{K'} \in K'$. In

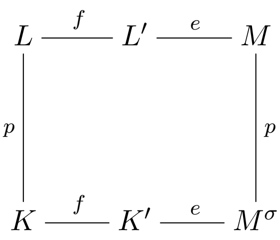

FIGURE 2.1.

summary, we have found that $M^\sigma = K(y)$ where $y^d = \alpha = \pi_K^{tf}\gamma^f\mu^s$ as in the statement of the theorem. Note that $v_{M^\sigma}(y) = t$.

A diagram recording the subfield lattice for M/K is provided in Figure 2.1. As there are various ways that each subfield is described, we note: $L = M^\tau = K(x)$, $M^\sigma = K'(z) = K(y)$, and $K' = K(v)$.

The cyclic extension M/M^σ is ramified because L/K is ramified of degree p, and ramification is multiplicative in towers. Assume for a contradiction that M/M^σ is atypical. So M^σ contains the pth roots of unity, and $M = M^\sigma(X)$ for some element $X \in M$ such that $X^p = \pi_{M^\sigma}$. Then the norm $z = N_{M/L}(X) = \prod_{i=0}^{d-1}\tau^i(X) \in L$ satisfies $z^p = N_{M/L}(X^p) = \prod_{i=0}^{d-1}\tau^i(\pi_{M^\sigma}) \in K$, since z^p is fixed by both σ and τ. Since $v_{M^\sigma}(z^p) = d$, $v_K(z^p) = f$. Since $\gcd(f,p) = 1$, this would imply that we can generate L by a pth root of a prime element, contradicting our assumption that L/K is typical. We therefore conclude that M/M^σ is an typical Galois extension, which means that $M = M^\sigma(X)$ where $X^p - X = \beta'$ for some $\beta' \in M^\sigma$ with $v_{M^\sigma}(\beta') = -b'$, $1 \le b' < v_M(p)/(p-1)$ with $p \nmid b'$ and $(\sigma - 1)X = 1 + \epsilon$ for some $\epsilon \in M$ satisfying $v_M(\epsilon) > 0$ [12, Chapter III §2 Propositions (2.4) and (2.5)]. Since $\sigma(X) = X + 1 + \epsilon$ satisfies $X^p - X = \beta'$, if $\operatorname{char}(K) = p$, $\epsilon = 0$, and if $\operatorname{char}(K) = 0$, then one can determine that $v_M(\epsilon) = v_M(p) - (p-1)b'$.

2.2.3. *From M/M^σ to L/K.* We have shown that M/M^σ is Artin–Schreier. It seems reasonable to suppose that we might use the Artin–Schreier generator X for M/M^σ to produce an element in L of some significance. In this direction, let $\mathbb{X} = yX$. Observe that $v_M(\mathbb{X}) = pt - b'$, and set

$$x_1 = \frac{1}{d}(1 + \tau + \cdots + \tau^{d-1})\mathbb{X} \in L. \tag{2.1}$$

Define

$$b = -\left\lceil \frac{pt - b'}{e} \right\rceil.$$

Towards a proof that $v_L(x_1) = -b$, we first show $v_L(x_1) \ge -b$. Let G_i be the ramification filtration for $\operatorname{Gal}(M/K)$, then $G_i \cap \langle\sigma\rangle$ yields the ramification filtration for $\mathrm{Gal}(M/L)=\langle\tau\rangle$. As a result the maximal unramified extension of L, called L', satisfies $[M:L']=e$ and $[L':L]=f$. The different for M/L, $\mathfrak{D}_{M/L}$, is $\mathfrak{P}_M^{e-1}$. Since the trace for M/L, $\mathrm{Tr}=1+\tau+\cdots+\tau^{d-1}$, is $\mathfrak{O}_L$-linear, the trace of an ideal of $\mathfrak{O}_M$ is an ideal of $\mathfrak{O}_L$. For any integers n,s, [23, Chapter 3 §3 Proposition 7] shows that $\mathrm{Tr}(\mathfrak{P}_M^n)\subseteq\mathfrak{P}_L^s$ if and only if $\mathfrak{P}_M^n\subseteq\pi_L^s\mathfrak{D}_{M/L}^{-1}=\mathfrak{P}_M^{es-e+1}$ (i.e. $s\le(n+e-1)/e$). Given an integer n, $\mathrm{Tr}(\mathfrak{P}_M^n)=\mathfrak{P}_L^s$ where $s=1+\lfloor(n-1)/e\rfloor=\lceil n/e\rceil$. This proves $v_L(x_1)\ge\lceil(pt-b')/e\rceil=-b$.

Since $b'=eb+pt+s'$ for some $0\le s'<e$, we have

$$v_M(x_1/y)\ge -eb-pt=s'-b'\ge -b'=v_M(X)\,.$$

If either inequality were strict, then $v_M(x_1/y)>v_M(X)=-b'$, which would imply $(\sigma-1)(x_1/y)\in\mathfrak{P}_M$, since $v_M((\sigma-1)\mu)\ge v_M(\mu)+b'$ for all $\mu\in M$. Since this would contradict Lemma 2.5, it follows that

$$v_L(x_1)=-b\,,\quad b'=eb+pt\,,\quad\text{and thus}\quad p\nmid b\,.$$

Lemma 2.5. *$(\sigma-1)(x_1/y)=1+\eta_1\in M$ where $\eta_1=0$ if $\mathrm{char}(K)=p$ and $v_M(\eta_1)>b'-(eb+pt)\ge 0$ if $\mathrm{char}(K)=0$.*

Proof. Recall that $M=M^\sigma(X)$ where X satisfies an Artin–Schreier equation. Since the details if $\mathrm{char}(K)=p$ are particularly transparent, we begin with this case. For $1\le i<d$, check that $\sigma\tau^i=\tau^i\sigma^{r^{-i}}$. Since $\rho=r$, using (2.1) we have

$$\begin{aligned}\sigma x_1&=\frac{\sigma}{d}(1+\tau+\cdots\tau^{d-1})\mathbb{X}\\&=\frac{1}{d}(\sigma+\tau\sigma^{r^{-1}}+\tau^2\sigma^{r^{-2}}+\cdots+\tau^{d-1}\sigma^{r^{-(d-1)}})\mathbb{X}\\&=\frac{1}{d}((\mathbb{X}+y)+\tau(\mathbb{X}+r^{-1}y)+\tau^2(\mathbb{X}+r^{-2}y)+\cdots+\tau^{d-1}(\mathbb{X}+r^{-(d-1)}y))\\&=x_1+y\,,\end{aligned}$$

which means that $(\sigma-1)x_1=y$. So $(\sigma-1)(x_1/y)=1$.

When $\mathrm{char}(K)=0$, recall from the end of §2.2.2 that $(\sigma-1)X=1+\epsilon$ where $v_M(\epsilon)=v_M(p)-(p-1)b'>0$. Thus $\sigma^i\mathbb{X}=\mathbb{X}+iy+(1+\sigma+\cdot+\sigma^{i-1})y\epsilon\equiv\mathbb{X}+iy+iy\epsilon\bmod y\epsilon\mathfrak{P}_M^{b'}$ for $0\le i<p$. We do not have $\rho=r$, but we do have $\rho\equiv r\bmod p$. So for $0\le j<d$, given r^{-j}, we may define $\bar r_j\equiv r^{-j}\bmod p$ with $0\le\bar r_j<p$. This means that $\tau^j\sigma^{r^{-j}}\mathbb{X}=\tau^j\sigma^{\bar r_j}\mathbb{X}\equiv\tau^j\mathbb{X}+\rho^j\bar r_jy+\tau^j\bar r_jy\epsilon\bmod y\epsilon\mathfrak{P}_M^{b'}$ where $\rho^j\bar r_j\equiv 1\bmod p$. Since $v_M(p)\ge v_M(\epsilon)+b'$, we find that $\tau^j\sigma^{r^{-j}}\mathbb{X}\equiv\tau^j\mathbb{X}+y+y\tau^j\epsilon\bmod y\epsilon\mathfrak{P}_M^{b'}$.

Therefore

$$\sigma x_1 = \frac{\sigma}{d}(1+\tau+\cdots\tau^{d-1})\mathbb{X} = \frac{1}{d}(\sigma+\tau\sigma^{r^{-1}}+\tau^2\sigma^{r^{-2}}\cdots\tau^{d-1}\sigma^{r^{-(d-1)}})\mathbb{X}$$
$$\equiv x_1 + \frac{1}{d}\sum_{j=0}^{d-1} y + \frac{y}{d}\sum_{j=0}^{d-1}\tau^j\epsilon \equiv x_1 + y + \frac{y}{d}\operatorname{Tr}(\epsilon) \bmod y\epsilon\mathfrak{P}_M^{b'},$$

where Tr is the trace for M/L. Recall that $\operatorname{Tr}(\mathfrak{P}_M^n) = \mathfrak{P}_L^{\lceil n/e\rceil}$. Since $e \mid v_M(p)-(p-1)b' = v_M(\epsilon)$ and $v_M(p) > (p-1)b'$, this means that $v_M(\operatorname{Tr}(\epsilon)) = v_M(\epsilon) = v_M(p)-(p-1)b' \geq e$. We have proven that $(\sigma-1)x_1 = y + y\eta_1$ for some $\eta_1 \in M$ where $v_M(\eta_1) = v_M(p)-(p-1)b' \geq e > s' = b'-(eb+pt)$. $\square$

2.2.4. *Determination of x and the defining equation for L/K.* In this step, we will identify an element $x \in L$ such that $L = K(x)$, $v_L(x) = -b$, $(\sigma-1)(x/y) \in 1+\mathfrak{P}_M$, and $x^p - \alpha^{(p-1)/d}x \in K$. If $\operatorname{char}(K) = p$, it will be $x = x_1$. If $\operatorname{char}(K) = 0$, x_1 provides us with only a first approximation for x. We will set $x_0 = 0$, and construct a sequence $\{x_n\} \subset L$ satisfying certain properties such that $x = \lim x_n$ gives us the desired element. Thus the two arguments diverge. Before they diverge, observe that as soon as we prove there exists a x as above such that $x^p - \alpha^{(p-1)/d}x = \beta$ for some $\beta \in K$, then since $0 < b' = eb + pt$, we have $-b < pt/e$, which means that $v_L(x^p) < v_L(\alpha^{(p-1)/d}x)$. This implies $v_K(\beta) = -b$. Note that $p \nmid b$. The bounds on b' yield

$$0 < b + pt/e < pv_K(p)/(p-1).$$

Assume $\operatorname{char}(K) = p$**.** Based upon Lemma 2.5, $\sigma^i x_1 = x_1 + iy$ for $0 \leq i < d$. So the norm of x_1, namely $N_{M/M^\sigma}(x_1) = \prod_{i=0}^{p-1}\sigma^i x_1$ is

$$\prod_{i=0}^{p-1}(x_1+iy) = y^p\prod_{i=0}^{p-1}\left(\frac{x_1}{y}+i\right) = y^p\left(\frac{x_1^p}{y^p}-\frac{x_1}{y}\right) = x_1^p - \alpha^{(p-1)/d}x_1.$$

Clearly $x_1^p - \alpha^{(p-1)/d}x_1$, because it is a norm, is fixed by σ, but because $\alpha^{(p-1)/d} \in K$, it is also fixed by τ. As a result, $x_1^p - \alpha^{(p-1)/d}x_1 \in K$, and our considerations if $\operatorname{char}(K) = p$ are complete.

Assume $\operatorname{char}(K) = 0$**.** In addition to Lemma 2.5, we require two further preliminary results before we define the sequence $\{x_n\} \subset L$ such that $x = \lim x_n$ gives us the desired element. The first result concerns the polynomial

$$\wp_\alpha(X) = y((X/y)^p - X/y) = \frac{1}{y^{p-1}}X^p - X = \frac{1}{\alpha^{(p-1)/d}}X^p - X \in K[X].$$

Lemma 2.6. *$v_M((\sigma-1)\wp_\alpha(x_1)) > b' - eb$.*

Proof. Using Lemma 2.5, we have

$$\begin{aligned}\frac{1}{y}(\sigma-1)\wp_\alpha(x_1) &= \left(\frac{x_1}{y}+1+\eta_1\right)^p - \left(\frac{x_1}{y}+1+\eta_1\right) - \left(\left(\frac{x_1}{y}\right)^p - \frac{x_1}{y}\right)\\ &= \left(\frac{x_1}{y}+1+\eta_1\right)^p - \left(\frac{x_1}{y}\right)^p - (1+\eta_1)\\ &= \sum_{i=1}^{p-1}\binom{p}{i}\left(\frac{x_1}{y}\right)^i(1+\eta_1)^{p-i} + \sum_{i=1}^{p-1}\binom{p}{i}\eta_1^i + (\eta_1^p - \eta_1)\,.\end{aligned}$$

Multiplying back through by y, it is enough to show that $v_M(py(x_1/y)^{p-1}) \geq b' - eb$ when $v_M(x_1/y) \leq 0$, and $v_M(px_1) \geq b' - eb$ when $v_M(x_1/y) > 0$, while also showing $v_M(y\eta_1) \geq b' - eb$. Under $v_M(x_1/y) \leq 0$, $v_M(py(x_1/y)^{p-1}) \geq b' - eb$ is equivalent to $v_M(p) \geq b' + (p-2)(be+pt)$, which follows from $v_M(p) > (p-1)b'$ and $b' \geq be + pt$. Under $v_M(x_1/y) > 0$, $v_M(px_1) \geq b' - eb$ follows from $v_M(p) > (p-1)b' \geq b'$. This leaves $v_M(y\eta_1) > b' - eb$, which is equivalent to $v_M(\eta_1) > b' - (eb+pt) = s'$ and follows from Lemma 2.5. □

The next result is a generalization of [12, Chapter III §2 Lemma (2.2)].

Lemma 2.7. *Given $Z \in L \setminus K$ there is some element $z \in K$ such that $v_M((\sigma-1)Z) = v_M(Z-z) + b'$.*

Proof. Let $\pi_L \in L$ be a prime element, and express $Z = \sum_{i=0}^{p-1} a_i \pi_L^i$ for some $a_i \in K$. For $1 \leq i < p$, $p \nmid v_M(\pi_L^i)$, and thus $v_M((\sigma-1)\pi_L^i) = v_M(\pi_L^i) + b'$. Let $z = a_0$. Then $v_M((\sigma-1)Z) = v_M((\sigma-1)(Z-z) = v_M((Z-z) + b'$. □

We are now prepared to adapt the argument for [12, Chapter III §2 Proposition (2.4)] and recursively construct a sequence $\{x_n\} \subset L$ that satisfies the following conditions

$$\begin{aligned} v_L(x_n) = -b, \quad v_L(x_{n+1}-x_n) \geq v_L(x_n - x_{n-1}) + 1\,,\\ v_M(\delta_{n+1}) \geq v_M(\delta_n) + 1\,, \end{aligned} \tag{2.2}$$

with $\delta_n = (\sigma-1)\wp_\alpha(x_n)$ and $\wp_\alpha$ as in Lemma 2.6. Recall that we intend $x = \lim x_n$ to be the desired generator for L/K.

Using Lemma 2.6, $v_M(\delta_1) > b' - eb$, which since $b' = eb + pt$, means that $v_M(\delta_1) > pt = v_M(y)$. So at this point, together with Lemma 2.5, we have $v_L(x_1) = -b$, $v_M(\delta_1) > b' - eb = pt = v_M(y)$, and $(\sigma-1)x_1 = y + y\eta_1$ with $v_M(\eta_1) > 0$.

Assume by induction that $v_L(x_n) = -b$, $v_M(\delta_n) > b' - eb = pt = v_M(y)$, and $(\sigma-1)x_n = y + y\eta_n$ where $v_M(\eta_n) > 0$. To define x_{n+1}, use Lemma 2.7 to see that there is a $c_n \in K$ such that $v_M(\delta_n) = v_M(\wp_\alpha(x_n) + c_n) + b'$. Put $\mu_n = \wp_\alpha(x_n) + c_n \in L$ and set

$$x_{n+1} = x_n + \mu_n \in L\,. \tag{2.3}$$

Observe though, that if we ever have $\delta_n = 0$, then $\wp_\alpha(x) \in K$. In this case, we can simply set $x = x_n \in L$, observe that $v_L(x) = -b$, $x^p - \alpha^{(p-1)/d}x \in K$, and because $v_M(\eta_n) > 0$, $(\sigma-1)(x/y) \in 1+\mathfrak{P}_M$, as desired. Thus we assume throughout the remainder of the argument that $\delta_n \neq 0$.

Record that $v_M(\mu_n) = v_M(\delta_n) - b'$ and that $(\sigma - 1)\mu_n = \delta_n$. Since $v_M(\delta_n) > b' - eb$, $v_M(\mu_n) > -eb \geq -b$, (2.3) gives $v_L(x_{n+1}) = -b$. Furthermore, applying $(\sigma - 1)$ to (2.3) produces $(\sigma - 1)x_{n+1} = (\sigma - 1)x_n + \delta_n$. Thus $(\sigma - 1)x_{n+1} = y + y\eta_{n+1}$ where $\eta_{n+1} = \eta_n + \delta_n/y$. Thus $v_M(\eta_{n+1}) > 0$. Since $v_L(x_{n+1} - x_n) = v_L(\mu_n)$ and $v_M(\mu_n) = v_M(\delta_n) - b'$, all that remains of (2.2), is verified in our next lemma.

Lemma 2.8.

$$\delta_{n+1} = (\sigma - 1)\wp_\alpha(x_{n+1}) = (\sigma - 1)\wp_\alpha(x_n + \mu_n) \equiv 0 \bmod \delta_n\mathfrak{P}_M\,.$$

Proof. Using the definition of δ_n, this is the same as proving that

$$\begin{aligned}(\sigma - 1)\big(\wp_\alpha(x_n + \mu_n) - \wp_\alpha(x_n)\big) \\ = (\sigma - 1)y^{1-p}\sum_{i=1}^{p-1}\binom{p}{i}x_n^i\mu_n^{p-i} + (\sigma - 1)\wp_\alpha(\mu_n) \\ \equiv 0 \bmod \delta_n\mathfrak{P}_M\,.\end{aligned}$$

There are two summands to consider. Consider the first. Note that

$$\begin{aligned}v_M\left((\sigma - 1)y^{1-p}\sum_{i=1}^{p-1}\binom{p}{i}x_n^i\mu_n^{p-i}\right) \\ \geq b' - (p-1)pt + v_M(p) - (p-1)eb + v_M(\mu_n)\,.\end{aligned}$$

Since $v_M(p) > (p-1)b' = (p-1)(eb+pt)$ and $v_M(\mu_n) = v_M(\delta_n) - b'$, it follows that the first summand is 0 mod $\delta_n\mathfrak{P}_M$. Consider the second. Note that

$$(\sigma - 1)\wp_\alpha(\mu_n) = \wp_\alpha(\mu_n + \delta_n) - \wp_\alpha(\mu_n) = y^{1-p}\sum_{i=1}^{p-1}\binom{p}{i}\mu_n^i\delta_n^{p-i} + \wp_\alpha(\delta_n)\,.$$

For $1 \leq i \leq p-1$, $v_M(y^{1-p}\binom{p}{i}\mu_n^i\delta_n^{p-i}) = v_M(p) - (p-1)pt + pv_M(\delta_n) - ib' \geq v_M(p) - (p-1)(pt+eb) + (p-1-i)b' + v_M(\delta_n) \geq v_M(p) - (p-1)(pt + eb) + v_M(\delta_n) \geq v_M(p) - (p-1)b' + v_M(\delta_n) > v_M(\delta_n)$. Furthermore, since $v_M(\delta_n/y) > 0$, we also have $\wp_\alpha(\delta_n) \equiv 0 \bmod \delta_n\mathfrak{P}_M$. □

We have proven that the sequence $\{x_n\}$ is Cauchy, and thus converges in L. Additionally, $\lim \wp_\alpha(x_n) = 0$. Thus $x = \lim x_n \in L$ satisfies $\wp_\alpha(x) = 0$. Since $v_L(x_n) = -b$ for all n, $v_L(x) = -b$. Since $\wp_\alpha(x) = 0$, $x^p - \alpha^{(p-1)/d}x \in K$. Since $v_M(\eta_n) > 0$ for all n, $(\sigma - 1)(x/y) - 1 = \eta \in \mathfrak{P}_M$.

2.2.5. ***The converse.*** Assume that $e, f, d, t, b, \alpha, \beta$ are as in Theorem 2.2. Then as proven in §2.2.2, $K(y)/K$ with $y^d = \alpha$ has ramification index e and inertia degree f with $v_{K(y)}(y) = t$. Let x satisfy $x^p - \alpha^{(p-1)/d}x = \beta$. Then x/y satisfies the Artin-Schreier equation $X^p - X = \beta/y^p$ over $K(y)$. Using [12, Chapter III §2 Proposition (2.5)], we see that $M = K(x, y)$ is Galois over K, that the ramification break for $M/K(y)$ is $b' = -v_{K(y)}(\beta/y^p) = ep + pt$, and that there is some generator $\sigma \in \mathrm{Gal}(M/K(y))$ such that $(\sigma - 1)(x/y) = 1 + \eta \in M$ where $\eta = 0$ if $\mathrm{char}(K) = p$, and $v_M(\eta) = v_M(p) - (p-1)b'$ if $\mathrm{char}(K) = 0$. Thus we may conclude that there are generators $\sigma, \tau \in \mathrm{Gal}(M/K)$ as in Theorem 2.2.

2.2.6. ***Ramification.*** We turn now to the ramification break for a typical extension, adopting the notation of Theorem 2.2. Doing so means that we need to compute Herbrand functions for the Galois extensions M/L and M/K. Using [23, Chapter IV §3] or [3, p. 116–117], we see that

$$\varphi_{M/L}(x) = \begin{cases} x & \text{for } -1 \leq x \leq 0, \\ x/e & \text{for } 0 \leq x, \end{cases}$$

and letting b' denote the ramification break for M/M^σ, we have

$$\varphi_{M/K}(x) = \begin{cases} x & \text{for } -1 \leq x \leq 0, \\ x/e & \text{for } 0 \leq x \leq b', \\ x/pe + (p-1)b'/pe & \text{for } b' \leq x. \end{cases}$$

We now compute $\varphi_{L/K} = \varphi_{M/K} \circ \psi_{M/L}$, where $\psi_{M/L}$ is the inverse of $\varphi_{M/L}$, and find that

$$\varphi_{L/K}(x) = \begin{cases} x & \text{for } -1 \leq x \leq b'/e, \\ x/p + (p-1)b'/pe & \text{for } 0 \leq x. \end{cases}$$

From this it follows that the ramification break for L/K is $\ell = b'/e$. Since $b' = eb + pt$, this means that

$$\ell = b + pt/e\,. \tag{2.4}$$

Unless $e = 1$, ℓ is not an integer.

2.2.7. ***Different.*** Using the fact that $\mathfrak{D}_{M/K} = \mathfrak{D}_{M/L}\mathfrak{D}_{L/K}$ [23, Chapter III §4 Proposition 8] along with the formula for the exponent on the different in the Galois case, namely [23, Chapter IV §1 Proposition 4], we see that $\mathfrak{D}_{M/K} = \mathfrak{P}_M^{(ep-1)+(eb+pt)(p-1)}$ and $\mathfrak{D}_{M/L} = \mathfrak{P}_M^{e-1}$. Therefore

$$\mathfrak{D}_{L/K} = \mathfrak{P}_L^{(\ell+1)(p-1)}.$$

2.3. Examples of non-Galois typical extensions. There are online resources that generate lists of extensions of degree p over $\mathbb{Q}_p$ for primes p below certain bounds. For instance, there is the resource described by [16], which has been included in [26]. When using such resources be aware of the difference between Serre and Artin values. For instance, [16] uses Artin values.

Example 2.9 (Dihedral example)**.** Let $p \equiv 3 \bmod 4$ and $2 \nmid [\kappa : \mathbb{F}_p]$ where $\mathbb{F}_p$ is the field with p elements (equivalently, assume $-1 \notin K^2$). Let $e = 1, d = f = 2$, $t = 0$, and $\alpha = -1$. So $\alpha^{(p-1)/d} = -1$. Choose $\beta \in K$ with $v_K(\beta) = -b$ where $1 \leq b < pv_K(p)/(p-1)$ and $\gcd(p, b) = 1$. Then $L = K(x)$ with

$$x^p + x = \beta\,.$$

In either characteristic, the Galois closure for L/K is a dihedral extension of K with inertia $f = 2$ and ramification index p. The ramification break for L/K is

$$\ell = b\,.$$

Example 2.10 (Lubin's example)**.** The Eisenstein equation $x^p - px = p$ appears in [19, §1.4 Example 2] with $K = \mathbb{Q}_p$ and $\pi_K = p$, where the ramification break is reported as $p/(p-1)$. This is an Artin value. Let $p > 2$, so that L/K is not Galois. For an arbitrary local field K in either characteristic, let $f = 1$, $e = d = p-1$, $t = 1$, $b = -1$, and $\alpha = \beta = \pi_K$. So $L = K(x)$ with

$$x^p - \pi_K x = \pi_K\,.$$

The Galois closure is a totally ramified extension with its Galois group, a semi-direct product $C_p \rtimes C_{p-1}$. The Serre value of the ramification break is

$$\ell = \frac{1}{p-1}\,,$$

which agrees with the computation in [19, §1.4 Example 2].

Example 2.11. Let $p > 2$, $f = 1$, $e = d = p-1$, $t = p-2$, $b = 2-p$, and $\alpha = \beta = \pi_K^{p-2}$. So $L = K(x)$ where

$$x^p - \pi_K^{p-2} x = \pi_K^{p-2}\,.$$

Then the Galois closure in either characteristic is a totally ramified extension with its Galois group, a semi-direct product $C_p \rtimes C_{p-1}$. The ramification break of L/K is

$$\ell = \frac{p-2}{p-1}\,.$$

Example 2.12. Let $p > 2$, and let $K/\mathbb{Q}_p$ be a finite extension such that $\gcd(v_K(p), p-1) = 1$. The division algorithm yields $v_K(p) = q(p-1) + s$ for some integers q, s with $0 \leq s < p-1$. For each integer $1 \leq u <$

$p\min\{1, v_K(p)/(p-1)\}$, set $f = 1$, $e = d = p-1$, $t = s$, $b = pq - u$, $\alpha = \pi_K^s$, and $\beta = \pi_K^{u-pq}$. So $L = K(x)$ where

$$x^p - \pi_K^s x = \pi_K^{u-pq}.$$

Then the Galois closure is a totally ramified extension with its Galois group, a semi-direct product $C_p \rtimes C_{p-1}$. The ramification break of L/K is

$$\ell = \frac{pv_K(p)}{p-1} - u.$$

3. Hopf–Galois module structure

The purpose of this section is to extend Galois module structure results that are known for cyclic typical extensions to non-Galois typical extensions. Since by Remark 2.3 typical extensions are Galois for $p = 2$, we assume throughout the section that $p > 2$.

Greither and Pareigis classified the finitely many Hopf–Galois structures that are possible on a given separable extension [13]. Childs then showed that there is only one such structure on a separable extension L/K of degree p, and explicitly described the unique K-Hopf algebra $\mathcal{H}$ by descent [7, §2]. While the assumption $\mathrm{char}(K) = 0$ is stated in [7, §2], it is never used. So, to make it clear that Childs' argument is valid in both characteristics, we reproduce it in §3.1, relying on [8] to clarify some of the details.

In §3.2, we go further than [7], by using Theorem 2.2 and Childs' Theorem 3.1 to explicitly describe the $\mathcal{H}$-action on L/K. This is Theorem 3.5. With the action explicitly described, we observe that Theorem 3.5 provides a $\mathcal{H}$-scaffold on L/K, as defined in [6, Definition 2.3]. Thus we are able to use the results of [6] to show that Galois module structure results from [4, 11, 1, 24, 22, 15], concerning cyclic typical extensions, hold more generally.

3.1. Hopf–Galois structure.

Theorem 3.1 (Childs). *Let $p > 2$, and adopt the notation of Theorem 2.2 for a given typical extension L/K. Recall that $d \mid p-1$. Let $ds = p-1$, and let r_0 denote a primitive root modulo p with Teichmüller representative ρ_0 such that $r_0^s \equiv r \bmod p$ and $\rho_0^s = \rho$. Set*

$$\Psi = -\frac{1}{y}\sum_{k=0}^{p-2} \rho_0^{-k}\sigma^{r_0^k}.$$

Then the unique K-Hopf algebra $\mathcal{H}$ such that L/K is a $\mathcal{H}$-Galois extension is explicitly $\mathcal{H} = K[\Psi]$. It is contained in the group ring $K[y][\langle\sigma\rangle]$ and inherits its counit $\varepsilon(\Psi) = 0$, antipode $S(\Psi) = -\Psi$ and comultiplication Δ

from $K[y][\langle\sigma\rangle]$*. For example, if* $\mathrm{char}(K) = p$*, explicitly*

$$\Delta(\Psi) = \Psi \otimes 1 + 1 \otimes \Psi - \alpha^s \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} \Psi^i \otimes \Psi^{p-i}.$$

Remark 3.2. If L/K is Galois, the K-Hopf algebra $K[\Psi]$ is $K[\sigma]$.

Remark 3.3. If $p = 2$, we necessarily have $\alpha = y = 1$. Since $\Delta(\sigma) = \sigma \otimes \sigma$, thus $\Delta(\Psi) = -\Psi \otimes \Psi$. So for $p = 2$, the explicit expression for comultiplication Δ in Theorem 3.1 is not correct.

Proof. As Childs explains in [7, §2], the unique Hopf algebra $\mathcal{H}$ is described by descent. Using our notation, the group algebra $M^\sigma[\langle\sigma\rangle]$ where $M^\sigma = K(y)$ has K-basis $\{y^i\sigma^j : 0 \le i < d, 0 \le j < p\}$. The action of $\langle\tau\rangle$ on these basis elements is given by $\tau^k(y^i\sigma^j) = (\rho^k y)^i\sigma^{jr^k} = (\rho_0^{sk} y)^i\sigma^{jr_0^{sk}}$ with the Hopf algebra $\mathcal{H} = M^\sigma[\langle\sigma\rangle]^{\langle\tau\rangle}$ determined to be the sub-algebra of $M^\sigma[\langle\sigma\rangle]$ fixed by τ. The counit ε, antipode S and comultiplication Δ for $\mathcal{H}$ are determined in $M^\sigma[\langle\sigma\rangle]$.

Given a basis element for $M^\sigma[\langle\sigma\rangle]$, the sum over its orbit under $\langle\tau\rangle$ certainly lies in $M^\sigma[\langle\sigma\rangle]^{\langle\tau\rangle}$. There is only one element in the orbit of $y^0\sigma^0$, namely 1. The orbit of $y^i\sigma^0$ for $i \neq 0$ is a sum of dth roots of unity and thus is zero. Consider now the orbit generated by $y^i\sigma^j$, where $j \neq 0$ represents some coset of $\mathbb{F}_p^\times/\langle r\rangle$. A complete set of coset representatives for $\mathbb{F}_p^\times/\langle r\rangle$ is given by $\{r_0^t : 0 \le t < s\}$. Thus, adopting the notation $y^i\theta(i,t)$ for the sum over the orbit of $y^i\sigma^{r_0^t}$, we find

$$y^i\theta(i,t) = y^i \sum_{k=0}^{d-1} \rho_0^{isk}\sigma^{r_0^{t+sk}}.$$

These orbits biject with $\{(i,t) : 0 \le i < d, 0 \le t < s\}$, a set with $ds = p-1$ elements. Together with 1, we have a K-basis of dimension p for $\mathcal{H}$.

We would like now, as in [7, §2], to perform a change in basis. First, we introduce, mechanically, the basis change from [7, §2]. Second, we motivate everything based upon [8, Chapter 4 §16]. Observe that $\theta(i,t) = \theta(i+bd,t)$ for all $b \in \mathbb{Z}$, and for $0 \le i < p$, let

$$\Theta(i) = \sum_{t=0}^{s-1} \rho_0^{it}\theta(i,t) = \sum_{k=0}^{p-2} \rho_0^{ik}\sigma^{r_0^k}.$$

The idea is to replace, for a fixed i in $0 \le i < d$, the s elements $\{y^i\theta(i,t) : 0 \le t < s\}$ in our basis with the alternate s elements $\{y^i\Theta(i+bd) : 0 \le b < s\}$. Since $y^{i+bd} = \alpha^b y^i \in K^\times y^i$, this is the same as replacing them with $\{y^{i+bd}\Theta(i+bd) : 0 \le b < s\}$. Clearly, $\{y^i\Theta(i+bd) : 0 \le b < s\}$ is contained in the K-span of $\{y^i\theta(i,t) : 0 \le t < s\}$. Furthermore since $\sum_{b=0}^{s-1} \rho_0^{(t-a)(i+bd)} = s\delta_{t,a}$ where $\delta_{t,a}$ is the Kronecker delta function, we have

$sy^i\theta(i,a) = \sum_{b=0}^{s-1} \rho_0^{-a(i+bd)} y^i\Theta(i+bd)$ and thus find that the K-spans are equal. This means that $\{1\} \cup \{y^i\Theta(i) : 0 \leq i \leq p-2\}$ is a K-basis for $\mathcal{H}$. Since $\sum_{k=0}^{p-2} \rho_0^{ik} = 0$ unless $(p-1) \mid i$, we see that $\{y^i\Theta(i) : 1 \leq i \leq p-2\}$ lies within the augmentation ideal $\mathcal{H}^+ = \{h \in \mathcal{H} : \varepsilon(h) = 0\}$. Furthermore, $\varepsilon(\Theta(0)) = (p-1)$, thus $\Theta(0) - (p-1) \in \mathcal{H}^+$ as well. We now adjust Childs' basis very slightly to one more amenable to our purposes. Set $j = p-i-1$ and for $1 \leq i < p-1$, set

$$\Psi_j = -\frac{y^i\Theta(i)}{\alpha^s} = \frac{-1}{y^j} \sum_{k \in \mathbb{Z}/(p-1)\mathbb{Z}} \rho_0^{-jk} \sigma^{r_0^k},$$

and additionally, $\Psi_{p-1} = -(\Theta(0) - (p-1))/y^{p-1}$. Thus $\{\Psi_j : 1 \leq j \leq p-1\}$ is a K-basis for $\mathcal{H}^+$.

We now refer to [8, Chapter 4 §16] to explain this choice of basis and determine that $\mathcal{H} = K[\Psi_1]$. There, in [8, Chapter 4 Proposition (16.1)], a ring homomorphism $[\ ]$ is defined from $\mathbb{Z}$ to the R-Hopf endomorphisms of $\mathcal{H}$, a ring under convolution and composition. For the sake of brevity, we omit its definition and the development of its properties. We simply note that since $\mathcal{H}$ has rank p, this induces a homomorphism, also called $[\ ]$, from $\mathbb{F}_p^\times$ to the group of Hopf algebra automorphisms of $\mathcal{H}$. Given $m \in \mathbb{F}_p^\times$, the automorphism is denoted by $[m]$. The kernel of the counit $\mathcal{H}^+$ is shown to be a $\mathbb{Z}_p[\mathbb{F}_p^\times]$-submodule of $\mathcal{H}$ if $\mathrm{char}(K) = 0$ or an $\mathbb{F}_p[\mathbb{F}_p^\times]$-submodule if $\mathrm{char}(K) = p$ [8, Chapter 4 Lemma (16.2)]. Let χ be the identity map if $\mathrm{char}(K) = p$. Let χ be the Teichmüller character such that the primitive root $r_0 \in \mathbb{F}_p^\times$ maps to $\rho_0 \in \mathbb{Z}_p$ if $\mathrm{char}(K) = 0$. In either case, the idempotent elements of the group ring decompose $\mathcal{H}^+ \cong \oplus_{j=1}^{p-1} \mathcal{H}_j$ into one-dimensional K-spaces $\mathcal{H}_j = \{h \in \mathcal{H}^+ : [m](h) = \chi^j(m)h\}$, an eigenspace decomposition. Since $[m](\sigma) = \sigma^m$, one can check that $\mathcal{H}_j = K\Psi_j$, which explains the significance of the basis that we have chosen. Let $x_i = y^i\Psi_i$ so that x_i agrees with notation in [8, Chapter 4 §16]. The argument leading to [8, Chapter 4 Proposition (16.5)] proves that $K[x_1]$ equals the K-span on $\{1, x_1, \ldots, x_{p-1}\}$. This implies $K[\Psi_1] = \mathcal{H}$ as well. Now for the statement in the theorem, set $\Psi = \Psi_1$.

If $\mathrm{char}(K) = p$, it is easy to show that $x_1^i = i!x_i$ for $1 \leq i < p$. Thus, using the formula for comultiplication in [8, Chapter 4 (16.7)], the formula for comultiplication $\Delta(\Psi)$ in the statement in the theorem follows from Lemma 3.4. If $\mathrm{char}(K) = 0$, there are units $w_i \in \mathbb{Z}_p$ such that $x_1^i = w_i x_i$. These units do not have a simple description. So we leave the formula for $\Delta(\Psi)$ implicit in this case. □

Lemma 3.4. *Let $\mathbb{Z}_{(p)}$ be the integers localized at p. Then for $1 \le i \le p-1$,*

$$\left(-\sum_{k=1}^{p-1} \frac{1}{k} x^k\right)^i \equiv -i! \sum_{k=1}^{p-1} \frac{1}{k^i} x^k \mod (p, x^p - 1)$$

in the polynomial ring $\mathbb{Z}_{(p)}[x]$.

Proof. Since r_0 is a primitive root modulo p, $\sum_{k=1}^{p-1} r_0^{ek} \equiv 0 \bmod p$, for any exponent $1 \le e \le p-2$. This means that $\sum_{t=2}^{p-1} \frac{1}{t^e} = \sum_{k=1}^{p-2} r_0^{-ek} \equiv -1 \bmod p$. It is easy to see that $\frac{1}{t^i(1-t)} = \frac{1}{1-t} + \sum_{e=1}^{i} \frac{1}{t^e}$. Thus $\sum_{t=2}^{p-1} \frac{1}{t^i(1-t)} = \sum_{t=2}^{p-1}(\frac{1}{1-t} + \sum_{e=1}^{i} \frac{1}{t^e}) = \sum_{t=2}^{p-1}(\frac{1}{1-t} + \frac{1}{t}) + \sum_{e=2}^{i}\sum_{t=2}^{p-1} \frac{1}{t^e} = (\frac{1}{p-1} - 1) + \sum_{e=2}^{i} -1 \equiv -(i+1) \bmod p$. Let $t \equiv k/m \bmod p$. This identity becomes $\sum \frac{m^i}{k^i}\frac{m}{m-k} \equiv -(i+1) \bmod p$, where the left-hand-sum is over all $1 \le k \le p-1$ except $k = m$. This means that $\sum \frac{1}{k^i}\frac{1}{m-k} \equiv \frac{-(i+1)}{m^{i+1}} \bmod p$, which allows us to prove by induction that for $1 \le i \le p-2$,

$$\left(\sum_{k=1}^{p-1} \frac{1}{k^i} x^k\right)\left(\sum_{k=1}^{p-1} \frac{1}{k} x^k\right) \equiv -(i+1) \sum_{k=1}^{p-1} \frac{1}{k^{i+1}} x^k \mod (p, x^p - 1).$$

From this the result follows. □

3.2. Hopf–Galois module structure. Let $p > 2$, and let L/K be a typical extension. Following Theorem 3.1, let $\mathcal{H} = K[\Psi]$ be the unique Hopf algebra that makes L/K Hopf–Galois. The following result explicitly describes the action of $\mathcal{H}$ on L. Thanks to this simple description, we are able to generalize classical Galois module structure results for ramified degree p extensions to all typical extensions.

Theorem 3.5. *Let $L = K(x)$ be a typical extension of K, with x as in Theorem 2.2 and ramification break ℓ. Then $\Psi \cdot 1 = 0$ and for $1 \le i \le p-1$, $\Psi \cdot x^i \in L$. In particular,*

$$\Psi \cdot x^i \begin{cases} = ix^{i-1} & \textit{if } \operatorname{char}(K) = p, \\ \equiv ix^{i-1} \bmod x^{i-1}\mathfrak{P}_L^{v_L(p)-(p-1)\ell} & \textit{if } \operatorname{char}(K) = 0. \end{cases}$$

Proof. Recall that σ is an automorphism of M/K. Since $\sum_{k=0}^{p-2} \rho_0^{-k} = 0$, $\Psi \cdot 1 = 0$. Because the argument is much simpler for $\operatorname{char}(K) = p$, we treat it first. Note $\sigma^i x = x + iy$ and $\rho_0 = r_0$. Thus

$$\Psi \cdot x^i = \frac{-1}{y} \sum_{k=0}^{p-2} r_0^{-k}(x + r_0^k y)^i = \frac{-1}{y} \sum_{k=0}^{p-2}\sum_{t=0}^{i} \binom{i}{t} x^{i-t} r_0^{(t-1)k} y^t$$

$$= -\sum_{t=0}^{i} \binom{i}{t} x^{i-t} y^{t-1} \sum_{k=0}^{p-2} r_0^{(t-1)k} = \sum_{t=0}^{i} \binom{i}{t} x^{i-t} y^{t-1} \delta_{t,1} = ix^{i-1},$$

where $\delta_{i,j}$ is the Kronecker delta function. If $\mathrm{char}(K)=0$, $\sigma x = x+y+y\eta$ where $\eta\in M$ with $v_M(\eta)=v_M(p)-(p-1)(be+pt)$, we need to introduce further notation. Let $1\le r_k<p$ satisfy $r_k\equiv r_0^k \bmod p$ and set $\eta_k=(1+\sigma+\cdots+\sigma^{r_k-1})\eta$, we have $\sigma^{r_0^k}=\sigma^{r_k}=x+y(r_k+\eta_k)$ for $1\le k\le p-2$. [Note: This η_k is not the same element as η_n defined before (2.3) in §2.2.4.] As a result,

$$\begin{aligned}\Psi\cdot x^i &= \frac{-1}{y}\sum_{k=0}^{p-2}\rho_0^{-k}(x+y(r_k+\eta_k))^i\\ &= \frac{-1}{y}\sum_{k=0}^{p-2}\rho_0^{-k}\sum_{s=0}^{i}\binom{i}{s}x^{i-s}y^s(r_k+\eta_k)^s\\ &= \frac{-1}{y}\sum_{s=0}^{i}\binom{i}{s}x^{i-s}y^s\sum_{k=0}^{p-2}\rho_0^{-k}(r_k+\eta_k)^s\,.\end{aligned}$$

Since ρ_0 is a primitive $(p-1)$th root of unity, $\sum_{k=0}^{p-2}\rho_0^{-k}(r_0^k+\eta_{r_0^k})^s=0$ for $s=0$. Since $\rho_0^{-k}r_k\equiv 1 \bmod p$ and $p\equiv 0 \bmod \eta$, we have $\sum_{k=0}^{p-2}\rho_0^{-k}(r_0^k+\eta_{r_0^k})^s\equiv -\delta_{s,1} \bmod \eta$ for $1\le s\le i$. Since $v_M(y/x)=pt+eb>0$, we have $x^{i-s}y^s\equiv 0 \bmod x^{i-1}y$ for $1\le s\le i$. Therefore $\Psi\cdot x^i\equiv ix^{i-1} \bmod x^{i-1}\eta$. Since $\Psi\in\mathcal{H}$, $\Psi\cdot L\subset L$. The result follows by considering the value of $v_L(\eta)$. □

To explain why, based upon Theorem 3.5, L/K has a $\mathcal{H}$-scaffold as defined in [6, Definition 2.3], we set up the following notation: We set $b_1=b$ to be the lone shift parameter. Let $\mathfrak{b}:\{0,1,\dots,p-1\}\to\mathbb{Z}$ be defined by $\mathfrak{b}(s)=sb$, and let $\mathfrak{a}:\mathbb{Z}\to\{0,1,\dots,p-1\}$ be defined by $\mathfrak{a}(t)\equiv -tb^{-1} \bmod p$. The definition of $\mathfrak{a}$ means that for each $t\in\mathbb{Z}$, there is an $f_t\in\mathbb{Z}$ such that $t=-\mathfrak{a}(t)b+f_tp$. Using this, set $\lambda_t=x^{\mathfrak{a}(t)}\pi_K^{f_t}\in L$. Observe that $v_L(\lambda_t)=t$, and $\lambda_{t_1}\lambda_{t_2}^{-1}\in K$ when $t_1\equiv t_2 \bmod p$. Now set $\Psi_1=\Psi\in\mathcal{H}$, and observe that Theorem 3.5 yields the following congruence modulo $\lambda_{t+b}\mathfrak{P}_L^{\mathfrak{c}}$

$$\Psi_1\cdot\lambda_t\equiv\begin{cases}\mathfrak{a}(t)\lambda_{t+b} & \text{if } \mathfrak{a}(t)\ge 1,\\ 0 & \text{if } \mathfrak{a}(t)\ge 0,\end{cases}$$

where

$$\mathfrak{c}=\begin{cases}\infty & \text{if } \mathrm{char}(K)=p,\\ v_L(p)-(p-1)\ell & \text{if } \mathrm{char}(K)=0.\end{cases}$$

Comparing this with [6, Definition 2.3], we see that L/K has a $\mathcal{H}$-scaffold of precision $\mathfrak{c}$ with shift parameter b. Furthermore since $\ell=b$ for cyclic typical extensions, there is agreement between this statement and [6, Example 2.8].

Thus we are able to extend classical Galois module structure results to non-Galois typical extensions. To do so, we will have to assume that

$v_L(p)$ is large enough for the precision $\mathfrak{c}$ of the scaffold to satisfy lower bounds required by [6, Theorems 3.1 and 3.6]. This is a restriction only when $\mathrm{char}(K) = 0$. But then given an ideal $\mathfrak{P}_L^n$, and assuming $v_L(p)$ is large enough for the desired result, these theorems

(i) determine a basis for its associated order

$$\mathfrak{A}_{\mathcal{H}}(n) = \{h \in \mathcal{H} : h\mathfrak{P}_L^n \subseteq \mathfrak{P}_L^n\};$$

(ii) determine that $\mathfrak{A}_{\mathcal{H}}(n)$ is a local ring, with maximal ideal $\mathfrak{M}$ and residue field $\mathfrak{A}_{\mathcal{H}}(n)/\mathfrak{M} \cong \kappa = \mathfrak{O}_L/\mathfrak{P}_L$;

(iii) determine whether $\mathfrak{P}_L^n$ is free over $\mathfrak{A}_{\mathcal{H}}(n)$, namely whether $\mathfrak{P}_L^n$ is generated by one element over $\mathfrak{A}_{\mathcal{H}}(n)$;

(iv) determine the minimal number of generators for $\mathfrak{P}_L^n$ over $\mathfrak{A}_{\mathcal{H}}(n)$, if it is not free;

(v) and determine the embedding dimension $\dim_\kappa(\mathfrak{M}/\mathfrak{M}^2)$.

For example, as a result of Theorem 3.5 and [6, Theorem 3.1], we have:

Corollary 3.6. *Let L/K be a typical extension with b and ℓ as in Theorem 2.2. Set $\bar{b} \equiv b \equiv \ell \bmod p$ with $0 \leq \bar{b} < p$. Then*

(1) *For $n \equiv \bar{b} \bmod p$, $\mathfrak{P}_L^n$ is free over $\mathfrak{A}_{\mathcal{H}}(n)$.*

For the next two statements, assume the lower bound on $v_K(p)$, or alternatively, the upper bound on ℓ,

$$\ell < \frac{pv_K(p)}{p-1} - 2\,.$$

(2) *For $n \equiv 0 \bmod p$, $\mathfrak{P}_L^n$ is free over $\mathfrak{A}_{\mathcal{H}}(n)$ if and only if $\bar{b} \mid (p-1)$. This includes the ring of integers $\mathfrak{O}_L$.*

(3) *For $n \equiv \bar{b}+1 \bmod p$, $\mathfrak{P}_L^n$ is free over $\mathfrak{A}_{\mathcal{H}}(n)$ if and only if $\bar{b} = p-1$. This includes the inverse different $\mathfrak{D}_{L/K}^{-1}$.*

Proof. The point of [6] is that once there is a scaffold of high enough precision with respect to the ideal being considered, all that matters is whether a condition $w(s) = d(s)$ holds for all s. The $w(s)$ and $d(s)$ are as in [6, Theorem 3.1]. Note that the difference $w(s) - d(s)$ is completely determined by the residue classes of the exponent n of the ideal and the shift parameter b. This means that any statement that holds for a Galois extension with a scaffold of sufficiently high precision and shift parameter b will also hold for a non-Galois typical extension with sufficiently high precision and the same shift parameter b.

Therefore we first address the conditions on $\mathfrak{c}$ required for the conclusions of [6, Theorem 3.1] to hold, then we reference the relevant statements for cyclic extensions. Recall that [6, Example 2.8] provides a scaffold for cyclic typical extensions of precision $\mathfrak{c} = v_L(p) - (p-1)b$ and shift parameter b. Since $\ell = b$ for cyclic typical extensions, this agrees with the scaffold exhibited in this paper for non-Galois typical extensions of precision $\mathfrak{c} = v_L(p) - (p-1)\ell$ and shift parameter b.

For $n \equiv \bar{b} \bmod p$, we use [6, Theorem 3.1 (i)]. The restriction on the precision for this statement can be seen to be $\mathfrak{c} = v_L(p) - (p-1)\ell \geq 1$, which holds as a result of the upper bound on ℓ in Theorem 2.2. In the other two cases, we use [6, Theorem 3.1 (ii)]. Based upon [6, Remark 3.2], we require $\mathfrak{c} \geq 2p - 1$, which is equivalent to $\mathfrak{c} > 2p - 2$. Therefore $\mathfrak{c} = v_L(p) - (p-1)\ell > 2p - 2$, which yields the stated condition on ℓ.

Thus the first statement, for $n \equiv \bar{b} \bmod p$, follows from [11]. Ferton's condition in terms of continued fractions is easily checked. The second statement, for $n \equiv 0 \bmod p$, follows from [4]. It is easiest to verify the third statement, for $n \equiv \bar{b} + 1 \bmod p$, by using [5, Theorem 3.10] for the necessity of $\bar{b} = p - 1$. Use [11], as discussed in [5, p. 210 Remark (i)], for its sufficiency. □

For the sake of completeness, we briefly turn to the topic of Hopf–Galois module structure outside of the bounds on ℓ imposed by Corollary 3.6, a topic that is only relevant if $\mathrm{char}(K) = 0$. Such extensions can be constructed using Example 2.12. If we restrict our discussion to Galois extensions of degree p when $\mathrm{char}(K) = 0$, we may reference the complete result for $\mathfrak{O}_L$ that is available in [4]. Under the bound on ℓ imposed by Corollary 3.6, which can be expressed as $b < v_L(p)/(p-1) - 2$, scaffold methods can be used to see that $\mathfrak{O}_L$ is free over its associated order if and only if $\bar{b} \mid (p-1)$. Previous to the development of scaffolds, the authors of [4] proved the stronger result that if $b < v_L(p)/(p-1) - 1$, $\mathfrak{O}_L$ is free over its associated order if and only if $\bar{b} \mid (p-1)$. They furthermore proved that if $b \geq v_L(p)/(p-1) - 1$, and the continue fraction expansion for b/p is

$$\frac{b}{p} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_n}}},$$

then $\mathfrak{O}_L$ is free over its associated order if and only if $n \leq 4$. Since our focus in this paper is on scaffold methods, we do not pursue the analogous extensions of Corollary 3.6 here.

4. Concluding remarks

The definition of a scaffold, as presented in [6], was still evolving when the term, Galois scaffold, was coined in [10]. At that time, the underlying intuition, articulated in [10, §1], was that extensions with Galois scaffolds should "somehow" be no more complicated than ramified cyclic extensions of degree p. A more mature intuition is now available and appears in [6, §1]. Still, the first intuition is useful, and now that the definition of a scaffold has been generalized beyond Galois extensions and classical Galois module theory, the question arose whether all ramified extensions of degree p are, in this way, no more complicated than ramified cyclic extensions of degree p. This paper addresses separable extensions with an affirmative answer. Elsewhere, evidence is provided regarding inseparable extensions [6, §5].

References

[1] A. Aiba, "Artin-Schreier extensions and Galois module structure", *J. Number Theory* **102** (2003), no. 1, p. 118-124.

[2] S. Amano, "Eisenstein equations of degree p in a $\mathfrak{p}$-adic field", *J. Fac. Sci. Univ. Tokyo, Sect. I A* **18** (1971), p. 1-21.

[3] E. Artin & J. Tate, *Class field theory*, 2nd ed., Advanced Book Classics, Addison-Wesley Publishing Company, 1990, xxxviii+259 pages.

[4] F. Bertrandias, J.-P. Bertrandias & M.-J. Ferton, "Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local", *C. R. Acad. Sci., Paris, Sér. A* **274** (1972), p. 1388-1391.

[5] N. P. Byott, "Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications", *J. Théor. Nombres Bordx.* **9** (1997), no. 1, p. 201-219.

[6] N. P. Byott, L. N. Childs & G. G. Elder, "Scaffolds and generalized integral Galois modules structure", to appear in *Ann. Inst. Fourier*, `https://arxiv.org/abs/1308.2088v3`, 2017.

[7] L. N. Childs, "On the Hopf Galois theory for separable field extensions", *Commun. Algebra* **17** (1989), no. 4, p. 809-825.

[8] ———, *Taming wild extensions: Hopf algebras and local Galois module theory*, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, 2000, viii+215 pages.

[9] D. S. Dummit & R. M. Foote, *Abstract algebra*, 3rd ed., Wiley International Edition, 2004, xii+932 pages.

[10] G. G. Elder, "Galois scaffolding in one-dimensional elementary abelian extensions", *Proc. Am. Math. Soc.* **137** (2009), no. 4, p. 1193-1203.

[11] M.-J. Ferton, "Sur les idéaux d'une extension cyclique de degré premier d'un corps local", *C. R. Acad. Sci., Paris, Sér. A* **276** (1973), p. 1483-1486.

[12] I. B. Fesenko & S. V. Vostokov, *Local fields and their extensions*, 2nd ed., Translations of Mathematical Monograph, vol. 121, Translations of Mathematical Monograph, 2002, xi+345 pages.

[13] C. Greither & B. Pareigis, "Hopf Galois theory for separable field extensions", *J. Algebra* **106** (1987), no. 1, p. 239-258.

[14] C. Helou, "On the ramification breaks", *Commun. Algebra* **19** (1991), no. 8, p. 2267-2279.

[15] D. V. Huynh, "Artin-Schreier extensions and generalized associated orders", *J. Number Theory* **136** (2014), p. 28-45.

[16] J. W. Jones & D. P. Roberts, "A database of local fields", *J. Symb. Comput.* **41** (2006), no. 1, p. 80-97.

[17] S. Lang, *Algebra*, Graduate Texts in Mathematics, vol. 211, Springer, 2002, xv+914 pages.

[18] J. Lubin, "The local Kronecker-Weber theorem", *Trans. Am. Math. Soc.* **267** (1981), p. 133-138.

[19] ———, "Elementary analytic methods in higher ramification theory", *J. Number Theory* **133** (2013), no. 3, p. 983-999.

[20] F. Luca, M. Rzedowski-Calderón & M. R. Maldonado-Ramírez, "A generalization of a lemma of Sullivan", *Commun. Algebra* **40** (2012), no. 7, p. 2301-2308.

[21] R. E. MacKenzie & G. Whaples, "Artin-Scheier equations in characteristic zero", *Am. J. Math.* **78** (1956), p. 473-485.

[22] M. Marklove, "Local Galois module structure in characteristic p", PhD Thesis, University of Exeter (UK), 2013.

[23] J.-P. Serre, *Local fields.*, Graduate Texts in Mathematics, vol. 67, Springer, 1979, viii+241 pages.

[24] B. de Smit & L. Thomas, “Local Galois module structure in positive characteristic and continued fractions”, *Arch. Math.* **88** (2007), no. 3, p. 207-219.

[25] F. J. Sullivan, “p-torsion in the class group of curves with too many automorphisms”, *Arch. Math.* **26** (1975), p. 253-261.

[26] The LMFDB Collaboration, “The L-functions and Modular Forms Database”, 2016, `http://www.lmfdb.org`.

G. Griffith Elder
Department of Mathematics
University of Nebraska at Omaha
Omaha, NE 68182-0243, USA
E-mail: `elder@unomaha.edu`