World Scientific
www.worldscientific.com

THE RAMIFICATION GROUPS AND DIFFERENT OF A COMPOSITUM OF ARTIN–SCHREIER EXTENSIONS

QINGQUAN WU[*,‡] and RENATE SCHEIDLER[†,§]

Department of Engineering, Mathematics and Physics
Texas A&M International University
5201 University Boulevard, Laredo, TX 78041, USA

†*Department of Mathematics and Statistics*
University of Calgary, 2500 University Drive NW
Calgary, Alberta, T2N 1N4, Canada
‡*qingquan.wu@tamiu.edu*
§*rscheidl@ucalgary.ca*

Let K be a function field over a perfect constant field of positive characteristic p, and L the compositum of n (degree p) Artin–Schreier extensions of K. Then much of the behavior of the degree p^n extension L/K is determined by the behavior of the degree p intermediate extensions M/K. For example, we prove that a place of K totally ramifies/is inert/splits completely in L if and only if it totally ramifies/is inert/splits completely in every M. Examples are provided to show that all possible decompositions are in fact possible; in particular, a place can be inert in a non-cyclic Galois function field extension, which is impossible in the case of a number field. Moreover, we give an explicit closed form description of all the different exponents in L/K in terms of those in all the M/K. Results of a similar nature are given for the genus, the regulator, the ideal class number and the divisor class number. In addition, for the case $n = 2$, we provide an explicit description of the ramification group filtration of L/K.

Keywords: Artin–Schreier extension; compositum; decomposition law; different; ramification group.

Mathematics Subject Classification 2010: 11R58, 14H05, 11R20, 14H45

1. Introduction

When investigating algebraic number fields and function fields, Hilbert ramification theory is a convenient tool, especially in the study of wild ramification. Fix a function field K over a perfect constant field of positive characteristic p, and let L be the compositum of two or more (degree p) Artin–Schreier extensions of K. We investigate the splitting and the different exponent at a place $\mathcal{P}$ of K in the field extension L/K. In the case where L is the compositum of just two Artin–Schreier extensions, i.e. $[L : K] = p^2$, we also completely characterize the collection

of ramification groups of L/K at $\mathcal{P}$. Our main results are obtained by extensive use of valuation theory and the explicit construction of a suitable uniformizer for any place of L lying above $\mathcal{P}$.

The decomposition of $\mathcal{P}$ in L is in essence completely determined by its decomposition in all the intermediate degree p Artin–Schreier extensions M/K. For example, if $\mathcal{P}$ (totally) ramifies in every such extension M/K, then $\mathcal{P}$ totally ramifies in L/K. Note that this is exactly the opposite of Abhyankar's Lemma, due to the fact that $\mathcal{P}$ is wildly ramified in all the intermediate degree p extensions M/K. In fact, much more can be said; namely that $\mathcal{P}$ totally ramifies/is inert/splits completely in L/K if and only if it (totally) ramifies/is inert/splits (completely) in all Artin–Schreier subfields M/K with $[M:K] = p$. Thus, for these extreme splitting types, the decomposition in the compositum of Artin–Schreier extensions faithfully reflects the decompositions in the intermediate degree p Artin–Schreier extensions.

Literature on the topic of (generalized) Artin–Schreier extensions is extensive. The terminology arises from a paper by Artin and Schreier [3]. Hasse [16] investigated Artin–Schreier extensions at length and introduced a standard form description whose explicit nature facilitates the investigation of these objects considerably. In [20], the standard form description is extended to cyclic generalized Artin–Schreier extensions (or Artin–Schreier–Witt extensions), while the ramification groups of Artin–Schreier–Witt extensions are studied in [24]. For generalized Artin–Schreier extensions whose Galois groups are elementary abelian p-groups, we refer to a series of papers by Beelen, Garcia, and Stichtenoth [12, 13, 4, 14, 6]. In the context of applications to coding theory, the main focus of these papers is frequently the asymptotic "good" or "bad" behavior of field extension towers; specifically, how the number of rational points varies with respect to the genus in the extension towers. A good survey can be found in [15].

Throughout this paper, we use the following notation:

- k is a perfect field of characteristic $p > 0$;
- K is a function field with constant field k;
- $\mathcal{P}$ is a place of K whose degree is denoted by $\deg(\mathcal{P})$;
- $v_{\mathcal{P}} : K \mapsto \mathbb{Z} \cup \{\infty\}$ is the (surjective) discrete valuation corresponding to $\mathcal{P}$;
- $\mathcal{O}_{\mathcal{P}} = \{\alpha \in K \mid v_{\mathcal{P}}(\alpha) \geq 0\}$ is the valuation ring corresponding to $\mathcal{P}$.

Then $\mathcal{O}_{\mathcal{P}}/\mathcal{P}$ is an extension field of k of extension degree $\deg(\mathcal{P})$.

For any extension L of K and any place $\mathfrak{P}$ of L lying above $\mathcal{P}$, we write $\mathfrak{P} \mid \mathcal{P}$. Let $e(\mathfrak{P} \mid \mathcal{P})$, $f(\mathfrak{P} \mid \mathcal{P})$, $r(\mathfrak{P} \mid \mathcal{P})$, and $d(\mathfrak{P} \mid \mathcal{P})$ be the ramification index, relative degree, number of places of L lying above $\mathcal{P}$, and different exponent of $\mathfrak{P} \mid \mathcal{P}$, respectively; we note that $r(\mathfrak{P} \mid \mathcal{P})$ is in fact independent of $\mathfrak{P}$, but we use this notation to specify the field L containing $\mathcal{P}$ if necessary. If L/K is a Galois extension, we denote the first three of these quantities by $e(\mathcal{P})$, $f(\mathcal{P})$, and $r(\mathcal{P})$, respectively, if there is no need to specify L. In this case, $e(\mathcal{P})f(\mathcal{P})r(\mathcal{P}) = [L:K]$, the degree of the extension L/K, and the ramification groups of $\mathfrak{P} \mid \mathcal{P}$ are given by

$$G_i = G_i(\mathfrak{P} \mid \mathcal{P}) = \{\sigma \in \mathrm{Gal}(L/K) \mid v_{\mathfrak{P}}(t^{\sigma} - t) \geq i+1 \text{ for all } t \in \mathcal{O}_{\mathfrak{P}}\} \quad (1.1)$$

for $i \geq 0$. The connection between these groups and the different exponent is reflected in Hilbert's different formula (see, for example, [23, Theorem 3.8.7, p. 136]):

$$d(\mathfrak{P} \mid \mathcal{P}) = \sum_{i=0}^{\infty} (\#G_i(\mathfrak{P} \mid \mathcal{P}) - 1). \tag{1.2}$$

We also recall the transitivity of the decomposition data and the different exponent. If $K \subseteq F \subseteq L$ are function fields, $\mathfrak{P}$ a place of L, $\mathfrak{p} = \mathfrak{P} \cap F$, and $\mathcal{P} = \mathfrak{P} \cap K$, then

$$e(\mathfrak{P} \mid \mathcal{P}) = e(\mathfrak{P} \mid \mathfrak{p})e(\mathfrak{p} \mid \mathcal{P}), \quad f(\mathfrak{P} \mid \mathcal{P}) = f(\mathfrak{P} \mid \mathfrak{p})f(\mathfrak{p} \mid \mathcal{P}),$$
$$r(\mathfrak{P} \mid \mathcal{P}) = r(\mathfrak{P} \mid \mathfrak{p})r(\mathfrak{p} \mid \mathcal{P}), \tag{1.3}$$

and

$$d(\mathfrak{P} \mid \mathcal{P}) = e(\mathfrak{P} \mid \mathfrak{p})d(\mathfrak{p} \mid \mathcal{P}) + d(\mathfrak{P} \mid \mathfrak{p}). \tag{1.4}$$

Henceforth, we restrict to the Artin–Schreier set-up. For $1 \leq i \leq n$, let y_i have a defining equation of the form

$$y_i^p - y_i = a_i \in K. \tag{1.5}$$

Let L be the compositum of the fields $K(y_i)$, $1 \leq i \leq n$. Then L/K is an elementary abelian p-extension of type $(p, p, \ldots, p)$ (at most n copies). Henceforth, we assume there are exactly n copies, so $[L : K] = p^n$.

2. The Case $n = 1$

When $n = 1$, then L/K is simply an Artin–Schreier function field extension. This scenario is very well understood. For any Artin–Schreier generator y of L/K, say $y^p - y = c \in K$, we may assume that

$$\text{either } v_{\mathcal{P}}(c) \geq 0, \quad \text{or } p \nmid v_{\mathcal{P}}(c) < 0. \tag{2.1}$$

This result was given by Hasse [16] and is also formulated as [23, Lemma 3.7.7, p. 125]. In fact, when K is the rational function field, Hasse proved that (2.1) holds simultaneously for all places $\mathcal{P}$ of K. When K is an arbitrary function field, we can assume that (2.1) holds for any fixed place $\mathcal{P}$ of K, but the choice of c may depend on $\mathcal{P}$. The proof of how to choose c corresponding to $\mathcal{P}$ is, in essence, revisited in the proof of Lemma 3.9 below.

Throughout this section, let $L = K(y)$ with $y^p - y = c \in K$, such that (2.1) holds.

It is easy to see when exactly k is the (full) constant field of L:

Proposition 2.1. *k is the (full) constant field of L if and only if $c \notin k$.*

Proof. If k is the full constant field of L, then obviously $c \notin k$. Conversely, suppose $c \notin k$. Then by (2.1), there exists a place $\mathcal{Q}$ of K so that $p \nmid v_{\mathcal{Q}}(c) < 0$. Let $\bar{k}$ be a fixed algebraic closure of k. Consider the constant field extension $K\bar{k}/K$, and let $\bar{\mathcal{Q}}$ be the unique place of $K\bar{k}$ lying above $\mathcal{Q}$. Then $v_{\bar{\mathcal{Q}}}(c) = v_{\mathcal{Q}}(c)$ since $K\bar{k}/K$ is

unramified. It follows from Eisenstein's Criterion ([23, Proposition 3.1.15, p. 76]) that $T^p - T - c$ is irreducible over $K\bar{k}$. Hence L has full constant field k. $\qquad\square$

Recall the decomposition of a place in an Artin–Schreier extension L/K:

Theorem 2.2. *The decomposition of any place $\mathcal{P}$ of K in L is*

$$(e(\mathcal{P}), f(\mathcal{P}), r(\mathcal{P})) = \begin{cases} (1, 1, p) & \text{if } v_{\mathcal{P}}(c) \geq 0 \\ & \text{and } T^p - T - c \text{ splits modulo } \mathcal{P}, \\ (1, p, 1) & \text{if } v_{\mathcal{P}}(c) = 0 \\ & \text{and } T^p - T - c \text{ is irreducible modulo } \mathcal{P}, \\ (p, 1, 1) & \text{if } p \nmid v_{\mathcal{P}}(c) < 0. \end{cases}$$

Proof. This is an easy consequence of Kummer's Theorem ([23, Theorem 3.3.7, p. 86]) and Eisenstein's Criterion ([23, Proposition 3.1.15, p. 76]). $\qquad\square$

Note that $T^p - T - c$ always splits modulo $\mathcal{P}$ if $v_{\mathcal{P}}(c) > 0$.

Let $\mathfrak{P}$ be any place of L lying above $\mathcal{P}$. By Proposition 3.7.8(c), p. 127 of [23], the different exponent of $\mathfrak{P} \mid \mathcal{P}$ is

$$d(\mathfrak{P} \mid \mathcal{P}) = (m + 1)(p - 1) \quad \text{with } m = \begin{cases} -1 & \text{if } e(\mathcal{P}) = 0, \\ -v_{\mathcal{P}}(c) & \text{if } e(\mathcal{P}) > 0. \end{cases} \tag{2.2}$$

Hence by Hilbert's Different Formula (1.2), the ramification groups $G_i = G_i(\mathfrak{P} \mid \mathcal{P})$ are

$$G_0 = G_1 = \cdots = G_m \supsetneq G_{m+1} = \{\text{Id}\}.$$

Finally, we establish a one-to-one correspondence between the places $\mathfrak{P}$ of L with $v_{\mathfrak{P}}(y) \neq 0$ and the places $\mathcal{P}$ of K with $v_{\mathcal{P}}(c) \neq 0$.

Theorem 2.3. *For any place $\mathfrak{P} \mid \mathcal{P}$ of L/K, the following hold*:

(1) *If $v_{\mathcal{P}}(c) < 0$, then $\mathfrak{P}$ is the unique place of L lying above $\mathcal{P}$, and $v_{\mathfrak{P}}(y) = v_{\mathcal{P}}(c) < 0$.*

(2) *If $v_{\mathcal{P}}(c) = 0$, then $v_{\mathfrak{P}}(y) = v_{\mathcal{P}}(c) = 0$.*

(3) *If $v_{\mathcal{P}}(c) > 0$, then $\mathcal{P}$ splits completely in L/K. If $\mathfrak{P}_1 = \mathfrak{P}, \mathfrak{P}_2, \ldots, \mathfrak{P}_p$ are the places of L lying above $\mathcal{P}$, then $v_{\mathfrak{P}_i}(y) = v_{\mathcal{P}}(c) > 0$ for one index i, and $v_{\mathfrak{P}_j}(y) = 0$ for all $j \neq i$.*

Proof. The uniqueness of $\mathfrak{P}$ in part (1) follows from Theorem 2.2, since $\mathcal{P}$ (totally) ramifies in L/K. The other results in parts (1) and (2) are immediate by applying the strict triangle inequality at $\mathfrak{P}$ to the equation $y^p - y - c = 0$. For part (3), when $v_{\mathcal{P}}(c) > 0$, then $\mathcal{P}$ splits completely in L/K by Theorem 2.2. We claim that

$$v_{\mathfrak{P}_i}(y) > 0 \quad \text{for some } i \Rightarrow v_{\mathfrak{P}_j}(y) = 0 \quad \text{for all } j \neq i. \tag{2.3}$$

Indeed, since the Galois group $\mathrm{Gal}(L/K)$ of L/K acts transitively on the places $\mathfrak{P}_i$, there exists for any distinct pair of indices i, j an automorphism $\sigma \in \mathrm{Gal}(L/K)\backslash\{\mathrm{Id}\}$ such that $\mathfrak{P}_i^\sigma = \mathfrak{P}_j$. Then $y^\sigma = y + l$ for some $1 \leq l \leq p - 1$, since $\{y + l \mid l \in \mathbb{F}_p\}$ is the set of roots of the equation $T^p - T = c$. Now $v_{\mathfrak{P}_j}(y + l) = v_{\mathfrak{P}_j^\sigma}(y^\sigma) = v_{\mathfrak{P}_i}(y) > 0$. Hence, by the strict triangle inequality, $v_{\mathfrak{P}_j}(y) = \min\{v_{\mathfrak{P}_j}(y + l), v_{\mathfrak{P}_j}(l)\} = v_{\mathfrak{P}_j}(l) = 0$.

Without loss of generality, we can assume that $v_{\mathfrak{P}_i}(y) = 0$ for $2 \leq i \leq p$. It remains to show that $v_{\mathfrak{P}}(y) = v_{\mathcal{P}}(c) > 0$. Note that $v_{\mathfrak{P}}(y) \in \{0, v_{\mathcal{P}}(c)\}$ by applying the strict triangle inequality at $\mathfrak{P}$ to the equation $T^p - T - c = 0$. In particular, we have

$$\sum_{\mathfrak{Q} \mid \mathcal{P}} v_{\mathfrak{Q}}(y) \leq v_{\mathcal{P}}(c), \tag{2.4}$$

where $\mathfrak{Q}$ runs through all the places in L lying above $\mathcal{P}$. Here, equality holds if and only if $v_{\mathfrak{P}}(y) = v_{\mathcal{P}}(c)$. Note that (2.4) is true for an arbitrary place $\mathcal{P}$ of K, as long as $v_{\mathcal{P}}(c) > 0$. Let D_K and D_L denote the divisor groups of K and L, respectively, and consider the principal divisors $(c) \in D_K$ and $(y) \in D_L$. By part (1), the degree of the pole divisor of (c) in D_K equals the degree of the pole divisor of (y) in D_L. Hence the same is true for the zero divisors of (c) and (y), i.e.

$$\sum_{v_{\mathfrak{Q}}(y)>0} v_{\mathfrak{Q}}(y) \deg(\mathfrak{Q}) = \sum_{v_{\mathcal{Q}}(c)>0} v_{\mathcal{Q}}(c) \deg(\mathcal{Q}). \tag{2.5}$$

By parts (1) and (2) and (2.3), we see that for all places $\mathcal{Q}$ of K, $v_{\mathfrak{Q}}(y) \neq 0$ for at most one place $\mathfrak{Q} \mid \mathcal{Q}$. Thus, (2.5) implies

$$\sum_{v_{\mathcal{Q}}(c)>0} \sum_{\mathfrak{Q} \mid \mathcal{Q}} v_{\mathfrak{Q}}(y) \deg(\mathfrak{Q}) = \sum_{v_{\mathcal{Q}}(c)>0} v_{\mathcal{Q}}(c) \deg(\mathcal{Q}). \tag{2.6}$$

Note that when $v_{\mathcal{Q}}(c) > 0$, $\deg(\mathcal{Q}) = \deg(\mathfrak{Q})$ for any $\mathfrak{Q} \mid \mathcal{Q}$. Our result now follows by multiplying (2.4) by $\deg(\mathcal{P})$, summing both sides of the resulting identity over all places $\mathcal{Q}$ of K such that $v_{\mathcal{Q}}(c) > 0$, and comparing with (2.6). $\qquad\square$

It should be noted that some of the results of Theorem 2.3 can be generalized to complete discrete valuation fields of characteristic 0; see [11, Proposition 2.5, p. 77f].

Corollary 2.4. *For every place $\mathcal{P}$ of K with $v_{\mathcal{P}}(c) \neq 0$, there exists a unique place $\mathfrak{P}$ of L lying above $\mathcal{P}$ such that $v_{\mathfrak{P}}(y) \neq 0$. Conversely, for every place $\mathfrak{P}$ of L such that $v_{\mathfrak{P}}(y) \neq 0$, its restriction $\mathcal{P} = \mathfrak{P} \cap K$ to K has the property that $v_{\mathcal{P}}(c) \neq 0$.*

3. The Case $n = 2$

This setting turns out to be crucial in our analysis of the case of general n that will be investigated in the next section. Throughout this section, let L be the compositum of two Artin–Schreier extensions $K(y)$ and $K(z)$, so $L = K(y, z)$ with

$$y^p - y = a \in K, \quad z^p - z = b \in K. \tag{3.1}$$

For an arbitrary fixed place $\mathcal{P}$ of K, we assume throughout this section that (2.1) holds for both $c = a$ and $c = b$ without loss of generality; that is,

$$\text{either } v_{\mathcal{P}}(c) \geq 0, \quad \text{or } p \nmid v_{\mathcal{P}}(c) < 0 \quad \text{for } c \in \{a, b\}. \tag{3.2}$$

We also require that $K(y)$ and $K(z)$ be disjoint. To guarantee this, it suffices to assume that $a \neq ib + d^p - d$ for any $i \in \mathbb{F}_p^*$ and $d \in K$, by [25, Proposition 5.8.6, p. 171]. Then L/K is an elementary abelian p-extension of degree p^2. Note that L/K has $p + 1$ intermediate fields of degree p, given by $K(y)$ and $K(iy + z)$ for $i \in \mathbb{F}_p$.

We begin again with a characterization of the constant field of L.

Proposition 3.1. *k is the (full) constant field of L if and only if $a \notin k$ and $ia + b \notin k$ for any $i \in \mathbb{F}_p$.*

Proof. We only show that the constant field of L is k if $a \notin k$, $ia + b \notin k$ for any $i \in \mathbb{F}_p$. The other direction is trivial.

By Proposition 2.1, $K(y)$ and $K(iy + z)$ have full constant field k for all $i \in \mathbb{F}_p$. Let l be the constant field of L. Since $K(y)$ has constant field k, $[l : k] \in \{1, p\}$. If $[l : k] = p$, then the compositum Kl of K and l is a degree p intermediate field over K in the extension L/K. Hence Kl is either $K(y)$ or $K(iy + z)$ for some $i \in \mathbb{F}_p$. This is a contradiction since all these $p + 1$ fields have constant field k. $\square$

As in the previous section, we provide an easy description of the decomposition in L/K of any place of $\mathcal{P}$ of K. For this, and for comparison to our later results, we will need Abhyankar's Lemma ([23, Proposition 3.9.1, p. 137]):

Proposition 3.2 (Abhyankar's Lemma). *Let F be a function field, $E = F_1 F_2$ the compositum of two intermediate fields $F \subseteq F_1$, $F_2 \subseteq E$, $\mathfrak{P}$ a place of E, $\mathfrak{p}_i = \mathfrak{P} \cap F_i$ for $i = 1, 2$, and $\mathcal{P} = \mathfrak{P} \cap F$. Assume that $\mathcal{P}$ is tamely ramified in F_i/F for at least one i. Then $e(\mathfrak{P} \,|\, \mathcal{P}) = \mathrm{lcm}\{e(\mathfrak{p}_1 \,|\, \mathcal{P}), e(\mathfrak{p}_2 \,|\, \mathcal{P})\}$.*

We will also make use of the following lemma:

Lemma 3.3. *Let F be any field with a place $\mathcal{P}$, E the compositum of extension fields of F so that E/F is Galois, and assume that E/F admits at least one intermediate field $F \subsetneq M \subsetneq E$. Then $\mathcal{P}$ is inert/totally ramified in E/F if and only if $\mathcal{P}$ is inert/totally ramified in all the intermediate fields N with $F \subsetneq N \subsetneq E$.*

Proof. If $\mathcal{P}$ is inert/totally ramified in E/F, then by (1.3), $\mathcal{P}$ is inert/totally ramified in all the intermediate field extensions N/F. Now let $\mathfrak{P}$ be any place of E lying above $\mathcal{P}$. First, suppose that $\mathcal{P}$ is inert in all the intermediate fields N with $F \subsetneq N \subsetneq E$. Then $e(\mathcal{P}) = 1$ by Proposition 3.2, so it suffices to show that $r(\mathcal{P}) = 1$.

By way of contradiction, assume that $r(\mathcal{P}) > 1$. Then $1 < r(\mathcal{P}) < [E:F]$. Let E^D be the decomposition field of $\mathfrak{P} \,|\, \mathcal{P}$. Then E^D is an intermediate field with $F \subsetneq E^D \subsetneq E$ so that $1 < r(\mathcal{P}) = [E^D : F] < [E : K]$, and $\mathcal{P}$ splits completely in

E^D/F. This contradicts our assumption that $\mathcal{P}$ should be inert in the intermediate extension E^D/F.

Now suppose that $\mathcal{P}$ totally ramifies in all the intermediate fields N with $F \subsetneq N \subsetneq E$, so it suffices to show that $f(\mathcal{P})r(\mathcal{P}) = 1$. Assume again that $f(\mathcal{P})r(\mathcal{P}) > 1$, so $1 < f(\mathcal{P})r(\mathcal{P}) < [E:F]$. Then the inertia field E^I of $\mathfrak{P} \mid \mathcal{P}$ is an intermediate field with $F \subsetneq E^I \subsetneq E$, so $1 < f(\mathcal{P})r(\mathcal{P}) = [E^I:F] < [E:F]$ and $\mathcal{P}$ is unramified in E^I/F. This is again a contradiction. $\qquad\square$

We require additional notation. For any place $\mathfrak{P}$ of L, write

$$\mathcal{P} = \mathfrak{P} \cap K, \quad \mathfrak{p}_0 = \mathfrak{P} \cap K(y), \quad \mathfrak{p}_i = \mathfrak{P} \cap K(iy+z) \quad \text{for } 1 \leq i \leq p. \qquad (3.3)$$

Then $\mathcal{P}$ splits in L as follows:

Theorem 3.4. *If $\mathcal{P}, \mathfrak{P}, \mathfrak{p}_i$ $(0 \leq i \leq p)$ are given by (3.3), then the decomposition of $\mathcal{P}$ in L is*

$$(e(\mathfrak{P} \mid \mathcal{P}), f(\mathfrak{P} \mid \mathcal{P}), r(\mathfrak{P} \mid \mathcal{P})) = \begin{cases} (1,1,p^2) & \text{if } r(\mathfrak{p}_i \mid \mathcal{P}) = p \text{ for all } 0 \leq i \leq p; \\ (1,p,p) & \text{if } r(\mathfrak{p}_i \mid \mathcal{P}) = p \text{ for one } i \\ & \quad \text{and } f(\mathfrak{p}_j \mid \mathcal{P}) = p \text{ for all } j \neq i; \\ (1,p^2,1) & \text{if } f(\mathfrak{p}_i \mid \mathcal{P}) = p \text{ for all } i; \\ (p,1,p) & \text{if } r(\mathfrak{p}_i \mid \mathcal{P}) = p \text{ for one } i \\ & \quad \text{and } e(\mathfrak{p}_j \mid \mathcal{P}) = p \text{ for all } j \neq i; \\ (p,p,1) & \text{if } f(\mathfrak{p}_i \mid \mathcal{P}) = p \text{ for one } i \\ & \quad \text{and } e(\mathfrak{p}_j \mid \mathcal{P}) = p \text{ for all } j \neq i; \\ (p^2,1,1) & \text{if } e(\mathfrak{p}_i \mid \mathcal{P}) = p \text{ for all } i. \end{cases}$$

Furthermore, if k is a finite field, then the case $(1,p^2,1)$ does not occur.

Proof. If $r(\mathfrak{p}_i \mid \mathcal{P}) = p$ for at least two indices i, then $r(\mathfrak{p}_i \mid \mathcal{P}) = p$ for all i, so $r(\mathfrak{P} \mid \mathcal{P}) = p^2$ by [23, Proposition 3.9.6(b), p. 141].

Suppose now that $r(\mathfrak{p}_i \mid \mathcal{P}) = p$ for exactly one i. Then $f(\mathfrak{p}_j \mid \mathcal{P})e(\mathfrak{p}_j \mid \mathcal{P}) = p$ for some $j \neq i$. Without loss of generality, assume that $i = 0$ and $j = p$.

If $f(\mathfrak{p}_p \mid \mathcal{P}) = p$, then obviously $(e(\mathfrak{P} \mid \mathcal{P}), f(\mathfrak{P} \mid \mathcal{P}), r(\mathfrak{P} \mid \mathcal{P})) = (1,p,p)$. Furthermore, by Theorem 2.2, $T^p - T - a$ splits modulo $\mathcal{P}$ and $T^p - T - b$ is irreducible modulo $\mathcal{P}$, which implies the irreducibility of $T^p - T - (ia + b)$ modulo $\mathcal{P}$, for all $1 \leq i \leq p$. Hence, $f(\mathfrak{p}_i \mid \mathcal{P}) = p$ for $1 \leq i \leq p$.

If $e(\mathfrak{p}_p \mid \mathcal{P}) = p$, then obviously $(e(\mathfrak{P} \mid \mathcal{P}), f(\mathfrak{P} \mid \mathcal{P}), r(\mathfrak{P} \mid \mathcal{P})) = (p,1,p)$. Then $v_{\mathcal{P}}(a) \geq 0$ and $p \nmid v_{\mathcal{P}}(b) < 0$ by Theorem 2.2. Hence $p \nmid v_{\mathcal{P}}(ia + b) = v_{\mathcal{P}}(b) < 0$ by the strict triangle inequality, which implies $e(P_i \mid \mathcal{P}) = p$ for $1 \leq i \leq p$, again by Theorem 2.2.

Lastly, suppose that $r(\mathfrak{p}_i \mid \mathcal{P}) = 1$ for $1 \leq i \leq p$. If $f(\mathfrak{p}_i \mid \mathcal{P}) = p$ for some i and $e(\mathfrak{p}_j \mid \mathcal{P}) = p$ for some $j \neq i$, then arguments similar to the case $r(\mathfrak{p}_0 \mid \mathcal{P}) = 1$ apply. In this case, $e(\mathfrak{p}_j \mid \mathcal{P}) = p$ for all $j \neq i$, and $(e(\mathfrak{P} \mid \mathcal{P}), f(\mathfrak{P} \mid \mathcal{P}), r(\mathfrak{P} \mid \mathcal{P})) = (p,p,1)$.

If $f(\mathfrak{p}_i \,|\, \mathcal{P}) = p$ for all $0 \leq i \leq p$ or $e(\mathfrak{p}_i \,|\, \mathcal{P}) = p$ for all $0 \leq i \leq p$, then our claim follows immediately from Lemma 3.3.

Finally, we prove that the case $(1, p^2, 1)$ does not occur when k is finite. Let $\mathcal{O}_\mathcal{P}/\mathcal{P} = \mathbb{F}_q$ and $\wp : u \mapsto u^p - u$ the Artin–Schreier operator. Then $\wp$ is an endomorphism on the additive group of $\mathbb{F}_q$. It is easy to see that $\wp$ is a p-to-1 map, hence the image $\text{Im}(\wp)$ of $\wp$ in $\mathcal{O}_\mathcal{P}/\mathcal{P} = \mathbb{F}_q$ has cardinality q/p and $\mathbb{F}_q/\text{Im}(\wp)$ has cardinality p.

Consider the $p + 1$ polynomials $T^p - T - a \pmod{\mathcal{P}}$, $T^p - T - (ia + b) \pmod{\mathcal{P}}$, $1 \leq i \leq p$, over $\mathbb{F}_q$. By the Pigeon Hole Principle, at least two of them are in the same residue class modulo $\text{Im}(\wp)$. Without loss of generality, assume that $T^p - T - a \equiv T^p - T - b \pmod{\text{Im}(\wp)}$, so $a - b = u^p - u$ for some $u \in \mathbb{F}_q$. Then $(p-1)a + b = (-u)^p - (-u)$, which implies that $T^p - T - ((p-1)a + b) \pmod{\mathcal{P}}$ has a root in $\mathbb{F}_q$. By Theorem 2.2, $r(\mathfrak{p}_{p-1} \,|\, \mathcal{P}) > 1$, and hence $r(\mathfrak{P} \,|\, \mathcal{P}) > 1$. It follows that $f(\mathfrak{P} \,|\, \mathcal{P}) = p^2$ cannot occur. $\qquad\square$

Theorem 3.4 implies that in a compositum of two Artin–Schreier extensions, the converse of Abhyankar's Lemma (Proposition 3.2) also holds; that is, if $e(\mathfrak{P} \,|\, \mathcal{P}) = \text{lcm}\{e(\mathfrak{p}_i \,|\, \mathcal{P}), e(\mathfrak{p}_j \,|\, \mathcal{P})\}$ for some $0 \leq i, j \leq p$, then $\mathcal{P}$ is tamely ramified (and hence unramified) in at least one of the degree p Artin–Schreier extensions of K. In fact, unless $\mathcal{P}$ is inert or totally ramified or splits completely, we have $e(\mathfrak{P} \,|\, \mathcal{P}) = \text{lcm}\{e(\mathfrak{p}_i \,|\, \mathcal{P}) \mid 0 \leq i \leq p\}$, $f(\mathfrak{P} \,|\, \mathcal{P}) = \text{lcm}\{f(\mathfrak{p}_i \,|\, \mathcal{P}) \mid 0 \leq i \leq p\}$, and $r(\mathfrak{P} \,|\, \mathcal{P}) = \text{lcm}\{r(\mathfrak{p}_i \,|\, \mathcal{P}) \mid 0 \leq i \leq p\}$.

We saw that the totally inert case described in Lemma 3.3 cannot happen over finite constant fields. It should be noted that this case happens rather rarely in number fields as well. For example, let L/K be a Galois extension of number fields with a non-cyclic Galois group. Then by [8, Corollary 10.1.7, p. 479], no prime ideal of K is inert in L/K.

However, the totally inert case does occur in the compositum of Artin–Schreier extensions L/K:

Example 3.5. For any rational prime $p > 0$, there exists an (infinite) perfect field k of characteristic p, so that for any function field K with constant field k and any place $\mathcal{P}$ of K, there exists a field L that is the compositum of two Artin–Schreier extensions of K so that $[L : K] = p^2$, k is the full constant field of L, and $\mathcal{P}$ is inert in L.

Proof. For any rational prime $p > 0$, let $\mathbb{F}_q$ be a finite field of characteristic p, $U_0 = \mathbb{F}_q(x)$ the rational function field, and $\bar{U}_0$ a fixed algebraic closure of U_0. For $i \geq 1$, let $U_i = \{\alpha \in \bar{U}_0 \mid \alpha^p \in U_{i-1}\}$, and set $k = \bigcup_{i \geq 0} U_i$. It is easy to see that U_i is a field for all $i \geq 0$, and that k is a perfect field.

For any function field K with constant field k, and any place $\mathcal{P}$ of K, we choose $a_j, b_j \in K \backslash k$ so that $a_j - x^{1+jp} \in \mathcal{P}$ and $b_j - x^{1+p+jp} \in \mathcal{P}$ for all $j \geq 0$. This is possible since $k \subseteq \mathcal{O}_\mathcal{P}/\mathcal{P}$. For example, choose $a_j = x^{1+jp} + \pi$ where π is a uniformizer

of $\mathcal{P}$; similarly for b_j. Then $a_j, b_j \in K\backslash k$ as $x \in k$ and $\pi \in K\backslash k$. Set $L_j = K(y_j, z_j)$, where $y_j^p - y_j = a_j$, $z_j^p - z_j = b_j$, for all $j \geq 0$.

Note that $[L_j : K] \leq p^2$. By Proposition 2.1, $K(y_j)/K$ and $K(z_j)/K$ define Artin–Schreier extensions of K with full constant field k for all $j \geq 0$. Thus, k is the full constant field of L_j by Proposition 3.1. For $1 \leq i \leq p$ and $j \geq 0$, consider the polynomials

$$f_{0,j}(T) = T^p - T - x^{1+jp}, \quad f_{i,j}(T) = T^p - T - (ix^{1+jp} + x^{1+p+jp}).$$

It remains to show by Theorems 2.2 and 3.4 that for some j, the polynomials $f_{i,j}(T)$ remain irreducible over $\mathcal{O}_\mathcal{P}/\mathcal{P}$ for all $i \in \mathbb{F}_p$.

Note that $f_{i,j}(T)$ is defined over k. We claim that

$$f_{i,j}(T) \text{ is irreducible over } k \text{ for all } 0 \leq i \leq p \text{ and } j \geq 0. \tag{3.4}$$

In fact, we prove a more general result:

$$g(T) = T^p - T - h(x) \quad \text{is irreducible over } k$$

$$\text{if } h(x) \in \mathbb{F}_q[x] \quad \text{with } p \nmid \deg_x(h). \tag{3.5}$$

By Artin–Schreier theory (see, for example, [19, Theorem 6.4, p. 290]), it suffices to show that $g(T)$ has no roots in k. Assume to the contrary that $\alpha \in U_l$ is a root of $g(T)$. Then $\alpha^{p^l} \in \mathbb{F}_q(x)$ is a root of $T^p - T - h(x)^{p^l}$. Since $\mathbb{F}_q[x]$ is integrally closed, it follows that $\alpha^{p^l} \in \mathbb{F}_q[x]$. If $l = 0$, then $\alpha \in \mathbb{F}_q[x]$ is a root of $T^p - T - h(x)$, which cannot be the case since $p \nmid \deg_x(h)$. So $l > 0$.

Set $\alpha^{p^l} = h(x)^{p^{l-1}} + \beta$ with $\beta \in \mathbb{F}_q[x]$. Then β is a root of $T^p - T - h(x)^{p^{l-1}}$. After a finite number of such steps, with l decreasing in each step, we eventually obtain a root $\gamma \in \mathbb{F}_q[x]$ of $T^p - T - h(x)$, a contradiction. This finishes the proof of (3.5) and hence (3.4).

Next, we claim that the splitting fields of $f_{i,j}(T)$ are pairwise distinct for fixed i and distinct j. In other words, the fields defined by $f_{i,j_1}(T)$ and $f_{i,j_2}(T)$ are distinct for all i, if $j_1 \neq j_2$. Since both polynomials are of Artin–Schreier type, it suffices to show that

$$x^{1+j_1p} \neq lx^{1+j_2p} + d^p - d \qquad \text{for any } l \in \mathbb{F}_p^* \text{ and } d \in k,$$
$$ix^{1+j_1p} + x^{1+p+j_1p} \neq l(ix^{1+j_2p} + x^{1+p+j_2p}) + d^p - d \quad \text{for all } l \in \mathbb{F}_p^*, d \in k,$$

by [25, Proposition 5.8.6, p. 171]. Equivalently, this states that both $T^p - T - (x^{1+j_1p} - lx^{1+j_2p})$ and $T^p - T - (ix^{1+j_1p} + x^{1+p+j_1p} - l(ix^{1+j_2p} + x^{1+p+j_2p}))$ are irreducible over k, which is true by (3.5).

For any fixed place $\mathcal{P}$ of K, $\mathcal{O}_\mathcal{P}/\mathcal{P}$ is a fixed extension field of k. Since the splitting fields of $f_{0,j}(T)$ over k are pairwise distinct for distinct j, there are infinitely many $f_{0,j}(T)$ that are irreducible over $\mathcal{O}_\mathcal{P}/\mathcal{P}$. Similarly, among these infinitely many indices j, there are infinitely many $f_{1,j}(T)$ that are irreducible over $\mathcal{O}_\mathcal{P}/\mathcal{P}$. In this way, we eventually obtain infinitely many indices j so that $f_{i,j}(T)$ is irreducible over $\mathcal{O}_\mathcal{P}/\mathcal{P}$ for all $0 \leq i \leq p$.

Set $L = L_j$ such that $f_{i,j}(T)$ is irreducible over $\mathcal{O}_{\mathcal{P}}/\mathcal{P}$ for all $0 \le i \le p$. It remains to show $[L : K] = p^2$ to finish the proof. Clearly $T^p - T - a_j$ and $T^p - T - b_j$ are irreducible over K, since they are irreducible modulo $\mathcal{P}$. Also it is obvious that $K(y_j)$ and $K(z_j)$ are disjoint, by a similar modulo $\mathcal{P}$ analysis. $\qquad\square$

Next, we give two examples for the totally ramified case in Theorem 3.4. These examples will be revisited and their distinctions explained later on in this section.

Example 3.6. For an arbitrary rational prime $p > 0$, let K be any function field of characteristic p, $\mathcal{P}$ any place of K, a any element of K so that $p \nmid v_{\mathcal{P}}(a) < 0$, $b = a^{p+1}$, and $L = K(y, z)$ with y, z defined by (3.1). Then $\mathcal{P}$ is totally ramified in L.

Proof. Note that a can for example be chosen to be the inverse of a uniformizer of $\mathcal{P}$. Then $p \nmid v_{\mathcal{P}}(a) < 0$ and $p \nmid v_{\mathcal{P}}(b) = (p+1)v_{\mathcal{P}}(a) < 0$, so $p \nmid v_{\mathcal{P}}(ia + b) = (p+1)\, v_{\mathcal{P}}(a) < 0$ for all $1 \le i \le p - 1$. Hence $\mathcal{P}$ ramifies in $K(y)/K$ and $K(iy + z)/K$ for all $1 \le i \le p$ by Theorem 2.2. By Theorem 3.4, $\mathcal{P}$ totally ramifies in L/K.

We can provide an alternative proof using the Hurwitz Genus Formula instead of Theorems 2.2 and 3.4 if we construct the element a more carefully. Let g_K denote the genus of K, and $l(D)$ the k-dimension of the Riemann–Roch space $\mathcal{L}(D)$ of any divisor D of K. Then by [23, Theorem 1.5.17, p. 31], we have $l(d\mathcal{P}) = d \deg(\mathcal{P}) - g_K + 1$ for any integer $d \ge 2g_K - 1$. Take d sufficiently large so that $p \nmid d$ and $d \ge 2g_K$, and let $a \in \mathcal{L}(d\mathcal{P}) \backslash \mathcal{L}((d-1)\mathcal{P})$.

Note that $\mathcal{P}$ is the only ramified place in $K(y)/K$ and $K(iy + z)/K$ for all $1 \le i \le p$. By way of contradiction, suppose that $\mathcal{P}$ is not totally ramified in L/K. Then $L/K(y)$ and $L/K(iy + z)$ are unramified for $1 \le i \le p$. Denote by g_L, g_0, and g_p the genera of L, $K(y)$, and $K(z)$, respectively. Then $2g_L - 2 = p\,(2g_0 - 2) = p(2g_p - 2)$ by the Hurwitz Genus Formula, which implies $g_0 = g_p$.

On the other hand, again by the Hurwitz Genus Formula,

$$2g_0 - 2 = p(2g_K - 2) + (p-1)\deg(\mathcal{P})(1 - v_{\mathcal{P}}(a))$$
$$\ne p(2g_K - 2) + (p-1)\deg(\mathcal{P})(1 - p\,v_{\mathcal{P}}(a) - v_{\mathcal{P}}(a)) = 2g_p - 2,$$

contradicting $g_0 = g_p$. $\qquad\square$

Example 3.7. For an arbitrary rational prime $p > 0$, let K be any function field with a perfect constant field $k \supsetneq \mathbb{F}_p$, $\alpha \in k \backslash \mathbb{F}_p$, $\mathcal{P}$ any place of K, a any element of K so that $p \nmid v_{\mathcal{P}}(a) < 0$, and $v_{\mathcal{Q}}(a) \ge 0$ for all places $\mathcal{Q} \ne \mathcal{P}$ of K, $b = \alpha a$, and $L = K(y, z)$ with y, z defined by (3.1). Then $\mathcal{P}$ is totally ramified in L, and $v_{\mathcal{P}}(a) = v_{\mathcal{P}}(ia + b)$ for all $0 \le i \le p$.

Proof. In light of Example 3.6, it suffices to show that $v_{\mathcal{P}}(ia + b) = v_{\mathcal{P}}(a)$ for all $0 \le i \le p$. But this is obvious since $v_{\mathcal{P}}(i + \alpha) = 0$ for $i \in \mathbb{F}_p$, since $\alpha \in k \backslash \mathbb{F}_p$. $\qquad\square$

We now provide a simple description of the entire ramification group sequence $G_i = G_i(\mathfrak{P} \mid \mathcal{P})$, and hence the different exponent, of any place $\mathfrak{P} \mid \mathcal{P}$ of L/K. Obviously $\#G_i \in \{1, p, p^2\}$ for all $i \geq 0$. In light of (2.2), it will be useful to define the quantities

$$
\begin{aligned}
m &= \min\{d(\mathfrak{p}_i \mid \mathcal{P})/(p-1) - 1 \mid 0 \leq i \leq p\}, \\
M &= \max\{d(\mathfrak{p}_i \mid \mathcal{P})/(p-1) - 1 \mid 0 \leq i \leq p\},
\end{aligned}
\tag{3.6}
$$

with $\mathfrak{p}_i$, $0 \leq i \leq p$, as in (3.3). Clearly, m and M are integers that depend on the field extension L/K only. For example, if $\mathfrak{P}$ totally ramifies in L/K (and hence in $K(y)/K$ and $K(z)/K$ by Lemma 3.3), and if $v_{\mathcal{P}}(b) < v_{\mathcal{P}}(a)$, then $m = -v_{\mathcal{P}}(a)$ and $M = -v_{\mathcal{P}}(b)$ by (2.2). We point out that both $m < M$ and $m = M$ can occur when $\mathcal{P}$ totally ramifies in L/K: Examples 3.6 and 3.7 represent scenarios for the former and latter case, respectively.

It is straightforward to compute the ramification group sequence when $\mathcal{P}$ does not totally ramify in L/K. In this case, $e(\mathfrak{p}_j \mid \mathcal{P}) = 1$ for some $0 \leq j \leq p$ by Lemma 3.3, so obviously $\#G_i \in \{1, p\}$, and $m = -1$ by (2.2).

Proposition 3.8. *Let $\mathcal{P}$ be a place of K that does not totally ramify in L, $\mathfrak{P} \mid \mathcal{P}$ a place of L, and M defined by (3.6). Then the ramification group filtration of $\mathfrak{P} \mid \mathcal{P}$ as defined in (1.1) is given by*

$$
G_0 = G_1 = \cdots = G_M \supsetneq G_{M+1} = \{\mathrm{Id}\},
$$

where $\#G_0 = e(\mathfrak{P} \mid \mathcal{P}) \in \{1, p\}$, and $M = -1$ if and only if $\mathcal{P}$ is unramified in L/K. Furthermore, $d(\mathfrak{P} \mid \mathcal{P}) = (M+1)(p-1)$.

Proof. If $\mathcal{P}$ is unramified in L, then there is nothing to prove, so suppose that $e(\mathfrak{P} \mid \mathcal{P}) = p$. Let $\mathfrak{p}_i$ $(0 \leq i \leq p)$ be given by (3.3). By Theorem 3.4, $e(\mathfrak{p}_j \mid \mathcal{P}) = p$ for some $0 \leq j \leq p$, so $d(\mathfrak{p}_j \mid \mathcal{P}) = (M+1)(p-1)$ by (2.2). Then $e(\mathfrak{P} \mid \mathfrak{p}_j) = 1$ by (1.3), and hence $d(\mathfrak{P} \mid \mathfrak{p}_j) = 0$. It follows that $d(\mathfrak{P} \mid \mathcal{P}) = (M+1)(p-1)$ by (1.4). The characterization of the G_i now follows from (1.2). □

The totally ramified case is much more interesting, so we assume henceforth, until the end of this section, that $\mathcal{P}$ totally ramifies in L/K. Our analysis of the groups G_i proceeds in several stages. First, we produce a recursive sequence of Artin–Schreier generators $z_h \in K[y, z]$ $(h \geq 0)$ of $L/K(y)$ whose $v_{\mathfrak{P}}$-values increase as h increases until a certain threshold is reached. Since this threshold is not divisible by p, this guarantees the existence of an Artin–Schreier generator $w \in K[y, z]$ of $L/K(y)$ with $p \nmid v_{\mathfrak{P}}(w)$; note that we cannot choose $w = z$ as $v_{\mathfrak{P}}(z) = p v_{\mathcal{P}}(b)$ is divisible by p. Now by [23, Proposition 3.8.5, p. 134], it suffices to check the membership property of any G_i for a uniformizer t of $\mathfrak{P}$ only. The existence of w will yield such a uniformizer for which it will be possible to explicitly determine all the groups G_i.

By relabeling the intermediate degree p extensions of K in L if necessary, we may henceforth assume that

$$m = -v_\mathcal{P}(a) \quad \text{and} \quad M = -v_\mathcal{P}(b) \quad \text{if } \mathcal{P} \text{ totally ramifies in } L. \tag{3.7}$$

Lemma 3.9. *Let $\mathcal{P}$ be a place of K that totally ramifies in L, $\mathfrak{P}$ and $\mathfrak{p}_0$ given by (3.3), and m, M defined by (3.6). Then there exist sequences $b_h \in K$ and $z_h \in K[y, z]$ such that for all $h \geq 0$ the following properties hold:*

(1) $v_\mathcal{P}(b_{h+1}) > v_\mathcal{P}(b_h)$;
(2) $z_h^p - z_h \in K[y]$ *and* $v_{\mathfrak{p}_0}(z_h^p - z_h) = \min\{v_{\mathfrak{p}_0}(b_h), p(m - M) - m\}$;
(3) z_h *is an Artin–Schreier generator of $L/K(y)$.*

Proof. By Theorems 3.4 and 2.2, we have $p \nmid v_\mathcal{P}(a) < 0$ and $p \nmid v_\mathcal{P}(b) < 0$. We begin by constructing a sequence $b_h \in K$ ($h \geq 0$) such that part (1) of the lemma holds. Initialize $b_0 = b$. Suppose we are given b_h with $h \geq 0$. Since $p \nmid v_\mathcal{P}(a)$, there exist $i_h, j_h \in \mathbb{Z}$ with $i_h > 0$ and $i_h v_\mathcal{P}(a) + j_h p = v_\mathcal{P}(b_h)$. Let π be any uniformizer of $\mathcal{P}$. Then $v_\mathcal{P}(\pi^{j_h p} a^{i_h}) = v_\mathcal{P}(b_h)$. Hence, $b_h \pi^{-j_h p} a^{-i_h} \in \mathcal{O}_\mathcal{P}^* = \{\alpha \in \mathcal{O}_\mathcal{P} \mid v_\mathcal{P}(\alpha) = 0\} \subseteq K$.

Since $\mathcal{O}_\mathcal{P}/\mathcal{P}$ is perfect, there exists $u_h \in \mathcal{O}_\mathcal{P}^*$ such that $b_h \pi^{-j_h p} a^{-i_h} - u_h^p \in \mathcal{P}$, so $v_\mathcal{P}(b_h \pi^{-j_h p} a^{-i_h} - u_h^p) > 0$. Set $b_{h+1} = b_h - u_h^p \pi^{j_h p} a^{i_h}$. Then $v_\mathcal{P}(b_{h+1}) > v_\mathcal{P}(b_h)$ as required.

Next, we define auxiliary sequences $\beta_h, \alpha_h \in K[y]$ as follows.

$$\beta_h = u_h \pi^{j_h} y^{i_h} \quad (h \geq 0),$$

$$\alpha_0 = b_0 - b_1 - \beta_0^p + \epsilon\beta_0, \quad \alpha_h = b_h - b_{h+1} - \beta_h^p \quad (h \geq 1),$$

where $\epsilon = 1$ if $m = M$ and $\epsilon = 0$ if $m < M$. We compute the $v_{\mathfrak{p}_0}$-values for both these sequences. Since $v_{\mathfrak{p}_0}(y) = v_\mathcal{P}(a)$ by Theorem 2.3, we have $v_{\mathfrak{p}_0}(\beta_h) = j_h p + i_h v_\mathcal{P}(a) = v_\mathcal{P}(b_h)$. Now fix $h \geq 1$ if $m = M$ and $h \geq 0$ if $m < M$. Then by construction of b_h and β_h as well as (3.1),

$$\alpha_h = u_h^p \pi^{j_h p} a^{i_h} - u_h^p \pi^{j_h p} y^{i_h p} = u_h^p \pi^{j_h p} a^{i_h} - u_h^p \pi^{j_h p}(y + a)^{i_h}$$

$$= -u_h^p \pi^{j_h p} \sum_{l=1}^{i_h} \binom{i_h}{l} y^l a^{i_h - l}. \tag{3.8}$$

Now $v_{\mathfrak{p}_0}(y) = v_\mathcal{P}(a)$, and obviously $v_{\mathfrak{p}_0}(a) = pv_\mathcal{P}(a)$, so

$$v_{\mathfrak{p}_0}(y^l a^{i_h - l}) = (l + (i_h - l)p)v_\mathcal{P}(a) = (pi_h - l(p-1))v_\mathcal{P}(a) \quad (0 \leq l \leq i_h). \tag{3.9}$$

Since $v_\mathcal{P}(a) < 0$, the expression on the right-hand side of (3.9) strictly increases as l increases. It follows that the sum in (3.8) takes on its $v_{\mathfrak{p}_0}$-value at the term with $l = 1$. Since $v_{\mathfrak{p}_0}(\pi^{j_h p} a^{i_h}) = v_{\mathfrak{p}_0}(b_h)$ and $v_{\mathfrak{p}_0}(y) = v_\mathcal{P}(a)$, we obtain by (3.9),

$$v_{\mathfrak{p}_0}(\alpha_h) \geq v_{\mathfrak{p}_0}(\pi^{j_h p} y a^{i_h - 1}) = v_{\mathfrak{p}_0}(\pi^{j_h p} a^{i_h}) + v_{\mathfrak{p}_0}(y) - v_{\mathfrak{p}_0}(a)$$

$$= v_{\mathfrak{p}_0}(b_h) + (1 - p)v_\mathcal{P}(a)$$

$$= p(v_\mathcal{P}(b_h) - v_\mathcal{P}(a)) + v_\mathcal{P}(a), \tag{3.10}$$

where equality holds if and only if $p \nmid i_h$. In particular, equality holds for α_0 if $m < M$. We still need to determine $v_{\mathfrak{p}_0}(\alpha_0)$ in the case when $m = M$. In this case, $v_{\mathcal{P}}(a) = v_{\mathcal{P}}(la + b)$ for all $l \in \mathbb{F}_p$. Recall that $i_0 v_{\mathcal{P}}(a) + j_0 p = v_{\mathcal{P}}(b_0) = v_{\mathcal{P}}(b) = v_{\mathcal{P}}(a)$, so we can assume that $i_0 = 1$ and $j_0 = 0$. Hence $b_1 = b - u_0^p a$.

We claim that $v_{\mathcal{P}}(u_0 - u_0^p) = 0$. To that end, assume to the contrary that $v_{\mathcal{P}}(u_0 - u_0^p) > 0$. Then $u_0 \equiv u_0^p \pmod{\mathcal{P}}$, where $\overline{\theta} \pmod{\mathcal{P}}$ denotes the projection of $\theta \in \mathcal{O}_{\mathcal{P}}$ in $\mathcal{O}_{\mathcal{P}}/\mathcal{P}$. Hence $u_0 \equiv -l \pmod{\mathcal{P}}$ for some $l \in \mathbb{F}_p^*$. It follows that $ba^{-1} \equiv -l \pmod{\mathcal{P}}$, so $al + b \in \mathcal{P}$. But $al + b \equiv b - u_0 a \equiv b - u_0^p a \equiv b_1 \pmod{\mathcal{P}}$, so $v_{\mathcal{P}}(al + b) = v_{\mathcal{P}}(b_1) > v_{\mathcal{P}}(a)$, contradicting our assumption $m = M$. So $v_{\mathcal{P}}(u_0 - u_0^p) = 0$.

Since $\beta_0 = u_0 y$, we have

$$\alpha_0 = u_0^p a - u_0^p y^p + u_0 y = u_0^p a - u_0^p(y + a) + u_0 y = (u_0 - u_0^p)y.$$

Thus, $v_{\mathfrak{p}_0}(\alpha_0) = v_{\mathfrak{p}_0}(y) = v_{\mathcal{P}}(a)$, so (3.10) holds in this case as well. In both cases, by (3.7), we have

$$v_{\mathfrak{p}_0}(\alpha_0) = p(m - M) - m. \tag{3.11}$$

Finally, we construct the sequence z_h $(h \geq 0)$ satisfying parts (2) and (3) of the lemma. Set $z_0 = z$ and $z_{h+1} = z_h - \beta_h$ for $h \geq 1$. Then $z_h \in K[y, z]$ for $h \geq 0$, and since each z_h is a translation of z by an element in $K[y]$, the elements z_h form a sequence of Artin–Schreier generators of $L/K(y)$. By Theorem 2.3 and (3.7),

$$v_{\mathfrak{p}_0}(z_0^p - z_0) = v_{\mathfrak{p}_0}(b) = -pM < -pM + (p - 1)m = p(m - M) - m,$$

so part (2) holds for $h = 0$. Now let $h \geq 1$. Then $z_h^p - z_h = \gamma_h$ where

$$\gamma_h = (z^p - z) - \sum_{l=0}^{h-1}(\beta_l^p - \beta_l)$$

$$= b - \sum_{l=1}^{h-1}(b_l - b_{l+1} - \alpha_l - \beta_l) - (b_0 - b_1 + (\epsilon - 1)\beta_0 - \alpha_0)$$

$$= b_h + A_h + B_h \in K[y],$$

where $A_h = \sum_{l=0}^{h-1} \alpha_l$ and $B_h = \sum_{l=0}^{h-1} \beta_l - \epsilon\beta_0$. It suffices to prove $v_{\mathfrak{p}_0}(\gamma_h) = \min\{v_{\mathfrak{p}_0}(b_h), p(m - M) - m\}$ for all $h \geq 0$ to finish the proof of the lemma.

We claim that $v_{\mathfrak{p}_0}(B_h) > v_{\mathfrak{p}_0}(A_h) = p(m - M) - m \neq v_{\mathfrak{p}_0}(b_h)$. By (3.10) and part (1) of the lemma, $v_{\mathfrak{p}_0}(A_h) = v_{\mathfrak{p}_0}(\alpha_0) = p(m-M)-m$ by (3.11). Since $v_{\mathfrak{p}_0}(\beta_l) = v_{\mathcal{P}}(b_l)$, we see from part (1) that $v_{\mathfrak{p}_0}(\beta_l)$ also strictly increases as l increases. If $\epsilon = 0$, then $m < M$, so by (3.7),

$$v_{\mathfrak{p}_0}(B_h) = v_{\mathfrak{p}_0}(\beta_0) = v_{\mathcal{P}}(b) = -M$$

$$= p(m - M) - m + (p - 1)(M - m) > p(m - M) - m.$$

If $\epsilon = 1$, then $m = M$ and $B_h = \sum_{i=1}^{h-1} \beta_l$, so

$$v_{\mathfrak{p}_0}(B_h) = v_{\mathfrak{p}_0}(\beta_1) = v_{\mathcal{P}}(b_1) > v_{\mathcal{P}}(b) = -M = -m = p(m - M) - m.$$

So in both cases, $v_{\mathfrak{p}_0}(B_h) > p(m - M) - m = v_{\mathfrak{p}_0}(A_h)$. Now $p \nmid p(m - M) - m$, and $p \mid v_{\mathfrak{p}_0}(b_h) = pv_{\mathcal{P}}(b_h)$, so $p(m - M) - m \neq v_{\mathfrak{p}_0}(b_h)$. By the strict triangle inequality, we obtain $v_{\mathfrak{p}_0}(\gamma_h) = \min\{v_{\mathfrak{p}_0}(b_h), p(m - M) - m\}$ as claimed.   □

Corollary 3.10. *There exist an Artin–Schreier generator $w \in K[y, z]$ of $L/K(y)$ with $v_{\mathfrak{P}}(w) = p(m - M) - m$.*

Proof. Let $\mathfrak{p}_0$ be given by (3.3). By part (1) of Lemma 3.9, there exists an index $h \geq 0$ such that $v_{\mathfrak{p}_0}(b_h) > p(m - M) - m$. Then by parts (2) and (3) of the same lemma, $w = z_h \in K[y, z]$ is an Artin–Schreier generator of $L/K(y)$ with $v_{\mathfrak{P}}(w^p - w) = p(m - M) - m$. Since $p \nmid p(m - M) - m < 0$, by Theorem 2.3, $v_{\mathfrak{P}}(w) = v_{\mathfrak{p}_0}(w^p - w) = p(m - M) - m$.   □

Theorem 3.11. *Let $\mathcal{P}$ be a place of K that totally ramifies in L, $\mathfrak{P}$ the place of L lying above $\mathcal{P}$, and m, M defined by (3.6). Then the ramification group filtration of $\mathfrak{P} \mid \mathcal{P}$ is given by*

$$G_0 = G_1 = \cdots = G_r \supsetneq G_{r+1} = \cdots = G_s \supsetneq G_{s+1} = \{\mathrm{Id}\},$$

where $r = m$ and $s = m + p(M - m)$.

Proof. As mentioned earlier, the membership property of any G_i only needs to be verified for a uniformizer t of $\mathfrak{P}$; see, for example, [23, Proposition 3.8.5, p. 134]. We construct a suitable such uniformizer as follows. Let i, j be integers with $i > 0$ and $i(p(m - M) - m) + jp^2 = 1$. By Corollary 3.10, there exists an Artin–Schreier generator $w \in K[y, z]$ with $v_{\mathfrak{P}}(w) = p(m - M) - m$. Let π be a uniformizer of $\mathcal{P}$, and set $t = w^i \pi^j$. Then $t \in \mathcal{P}K[y, z] \subseteq \mathfrak{P}$ and $v_{\mathfrak{P}}(t) = 1$, so t is a uniformizer of $\mathfrak{P}$.

Let σ and τ generate the fixed groups of $K(y)$ and $K(z)$, respectively, under Galois correspondence. Then σ and τ generate the Galois group of L/K, so it suffices to compute $v_{\mathfrak{P}}(t^\sigma - t)$ and $v_{\mathfrak{P}}(t^\tau - t)$. Obviously $y^\sigma = y$ and $z^\tau = z$. By replacing σ by a suitable power of σ if necessary, we may assume that $z^\sigma = z + 1$ without loss of generality; similarly, $y^\tau = y + 1$.

By construction of w, $w = z_h = z - B_h$ for some $h \in \mathbb{N}$, where $B_h = \sum_{l=0}^{h-1} \beta_l \in K[y]$. It follows that $(w - z)^\sigma = w - z$, and so $w^\sigma = z^\sigma + w - z = w + 1$. Thus,

$$t^\sigma - t = \pi^j((w + 1)^i - w^i) = \pi^j \sum_{l=0}^{i-1} \binom{i}{l} w^l.$$

Since $v_{\mathfrak{P}}(w) < 0$ by Corollary 3.10, $v_{\mathfrak{P}}(w^l)$ strictly decreases as l increases, so the sum above takes its $v_{\mathfrak{P}}$-value at the term with $l = i - 1$. Hence, $v_{\mathfrak{P}}(t^\sigma - t) = v_{\mathfrak{P}}(\pi^j w^{i-1}) = v_{\mathfrak{P}}(t) - v_{\mathfrak{P}}(w) = 1 + m + p(M - m)$, where the last equality follows again from Corollary 3.10.

Finally, we compute $t^\tau - t$. We have $w^\tau = z - B_h^\tau = w + (B_h - B_h^\tau)$. Recall that $B_h = \sum_{l=0}^{h-1} \beta_l$ where $\beta_l = u_l \pi^{j_l} y^{i_l}$ with $u_l \in \mathcal{O}_{\mathcal{P}}^*$, $i_l \in \mathbb{N}$, $j_l \in \mathbb{Z}$, and

$i_l v_{\mathcal{P}}(a) + j_l p = v_{\mathcal{P}}(b_l)$. Thus,

$$\beta_l - \beta_l^\tau = u_l \pi^{j_l}(y^{i_l} - (y+1)^{i_l}) = -u_l \pi^{j_l} \sum_{n=0}^{i_l-1} \binom{i_l}{n} y^n.$$

Since $v_{\mathfrak{p}_0}(y) = v_{\mathcal{P}}(a) < 0$, $v_{\mathfrak{p}_0}(y^n)$ strictly decreases as n increases. So

$$v_{\mathfrak{p}_0}(\beta_l - \beta_l^\tau) \geq v_{\mathfrak{p}_0}(\pi^{j_l} y^{i_l-1}) = v_{\mathfrak{p}_0}(\beta_l) - v_{\mathfrak{p}_0}(y) = v_{\mathcal{P}}(b_l) - v_{\mathcal{P}}(a),$$

where equality holds if and only if $p \nmid j_l$. In particular, we have $v_{\mathfrak{p}_0}(\beta_0 - \beta_0^\tau) = v_{\mathcal{P}}(b) - v_{\mathcal{P}}(a)$.

By part (1) of Lemma 3.9, $v_{\mathcal{P}}(b_l) - v_{\mathcal{P}}(a)$ strictly increases as l increases, so

$$v_{\mathfrak{p}_0}(B_h - B_h^\tau) = v_{\mathfrak{p}_0}(\beta_0 - \beta_0^\tau) = v_{\mathcal{P}}(b) - v_{\mathcal{P}}(a) = m - M. \tag{3.12}$$

Thus,

$$t^\tau - t = \pi^j((w^\tau)^i - w^i) = \pi^j((w + (B_h - B_h^\tau))^i - w^i)$$

$$= \pi^j \sum_{l=0}^{i-1} \binom{i}{l} (B_h - B_h^\tau)^{i-l} w^l.$$

Since $v_{\mathfrak{P}}(w) = p(m-M) - m < p(m-M) = v_{\mathfrak{P}}(B_h - B_h^\tau)$ by (3.12), this expression takes on its $v_{\mathfrak{P}}$-value for $l = i - 1$, so again by Corollary 3.10 and (3.12),

$$v_{\mathfrak{P}}(t^\tau - t) = v_{\mathfrak{P}}(\pi^j(B_h - B_h^\tau)w^{i-1})$$

$$= v_{\mathfrak{P}}(\pi^j w^i) - v_{\mathfrak{P}}(w) + v_{\mathfrak{P}}(B_h - B_h^\tau)$$

$$= 1 - (p(m-M) - m) + p(m-M) = 1 + m.$$

It follows that

$$G_i = \begin{cases} \mathrm{Gal}(L/K) & \text{for } 0 \leq i \leq m, \\ \langle \sigma \rangle & \text{for } m+1 \leq i \leq m + p(M-m), \\ \{\mathrm{Id}\} & \text{for } i \geq m + p(M-m) + 1. \end{cases} \qquad \square$$

Note that if $M = m$, then $r = s = m$, so no ramification group has order p. In general, the number of ramification groups of order p is $s - r = p(M - m)$. The fact that this number is divisible by p is a consequence of the Hasse–Arf Theorem [2]. More specifically, an order p group occurs in the ramification group filtration of L/K if and only if there exist two degree p Artin–Schreier extensions of K with distinct different exponents. If this is the case, then the number of such order p groups is exactly $p/(p-1)$ times the gap between the two distinct different exponents.

An immediate consequence of Theorem 3.11 is the following simple formula for the different exponent of $\mathfrak{P} \,|\, \mathcal{P}$:

Corollary 3.12. *With the notation of Theorem 3.11, the different exponent of $\mathfrak{P} \,|\, \mathcal{P}$ is $d(\mathfrak{P} \,|\, \mathcal{P}) = (p-1)(pM + p + m + 1)$.*

Proof. By (1.2), $d(\mathfrak{P} \mid \mathcal{P}) = (r+1)(p^2-1)+(s-r)(p-1)$. The result now follows from Theorem 3.11. $\qquad\square$

It is straightforward to determine the relative different exponents $d(\mathfrak{P} \mid \mathfrak{p}_i)$ from Corollary 3.12 via (1.4), namely

$$d(\mathfrak{P} \mid \mathfrak{p}_0) = (m+1)(p-1), \qquad (3.13)$$

$$d(\mathfrak{P} \mid \mathfrak{p}_i) = (m+p(M-m)+1)(p-1) \quad \text{for } 1 \le i \le p. \qquad (3.14)$$

Note that (3.13) is true even if $\mathcal{P}$ does not totally ramify in L/K, by Proposition 3.8.

We remark that [1, Theorem 3.4] provides a partial result on the relative different exponents in a compositum of two Artin–Schreier extensions. When $\mathcal{P}$ has distinct different exponents in the two extensions — this corresponds to our case $m < M$ — then $\mathcal{P}$ totally ramifies in L, and the result of [1] agrees with (3.13) and (3.14). However, when $\mathcal{P}$ has the same different exponent in both extensions, then the result of [1] only specifies a range of possible values for the relative different exponents, whereas (3.13) and (3.14) provide the actual values.

4. The Case of Arbitrary n

We now derive the decomposition law and the different exponents for the case of arbitrary n; the ramification group filtration is the subject of a forthcoming paper. Throughout this section, let L be the compositum of $n \ge 2$ degree p Artin–Schreier extensions of K so that $[L:K]=p^n$. We assume that each of these extensions satisfies (2.1). Repeated application of Theorem 3.4 immediately yields the following:

Corollary 4.1. *Let E be any intermediate field of L/K, and $\mathcal{P}$ a place of K. Then $\mathcal{P}$ totally ramifies/is inert/splits completely in E/K if and only if $\mathcal{P}$ (totally) ramifies/is inert/splits (completely) in every intermediate degree p Artin–Schreier extension of E/K.*

Clearly, the intermediate degree p extensions of L/K are crucial in understanding the decomposition of any place of K in L. This suggests the following definitions:

$$\mathcal{M} = \{M \mid K \subseteq M \subseteq L \text{ and } [M:K]=p\}, \qquad (4.1)$$

and

$$\mathcal{S} = \{M \in \mathcal{M} \mid \mathcal{P} \text{ splits in } M/K\},$$

$$\mathcal{I} = \{M \in \mathcal{M} \mid \mathcal{P} \text{ is inert in } M/K\}, \qquad (4.2)$$

$$\mathcal{R} = \{M \in \mathcal{M} \mid \mathcal{P} \text{ ramifies in } M/K\}.$$

It is easy to deduce that $\#\mathcal{M} = (p^n-1)/(p-1)$. The cardinalities of the sets in (4.2) are given as follows.

Lemma 4.2. *Let $\mathcal{P}$ be any place of K, L^D the decomposition field of $\mathcal{P}$ in L, and H any maximal intermediate field of L/K so that $\mathcal{P}$ is inert in every degree p extension*

of K contained in H. Set $p^s = [L^D : K]$ and $p^t = [H : K]$. Then the sets $\mathcal{S}, \mathcal{I}$, and $\mathcal{R}$ as defined in (4.2) have the following cardinalities:

$$\#\mathcal{S} = \frac{p^s - 1}{p - 1}, \quad \#\mathcal{I} = \frac{p^{s+t} - p^s}{p - 1}, \quad \#\mathcal{R} = \frac{p^n - p^{s+t}}{p - 1}.$$

Proof. We first observe that L^D is the compositum of certain Artin–Schreier extensions over K, so it contains exactly $(p^s - 1)/(p - 1)$ intermediate degree p extensions of K. By Corollary 4.1, these are exactly the fields $M \in \mathcal{M}$ in which $\mathcal{P}$ splits, i.e. the fields in $\mathcal{S}$. This proves $\#\mathcal{S} = (p^s - 1)/(p - 1)$.

Next, we note that $\mathcal{P}$ is inert in H, again by Corollary 4.1. Furthermore, $H \cap L^D = K$, since otherwise $H \cap L^D$ would contain a degree p extension of K that would impossibly have to belong to both $\mathcal{S}$ and $\mathcal{I}$. Hence, the compositum HL^D is a degree p^{s+t} extension of K that is the compositum of certain Artin–Schreier extensions of K. It thus contains $(p^{s+t} - 1)/(p - 1)$ intermediate degree p extensions of K. None of these can belong to $\mathcal{R}$ by Corollary 4.1, and all $(p^s - 1)/(p - 1)$ fields belonging to $\mathcal{S}$ are among them. The remaining $(p^{s+t} - p^s)/(p - 1)$ such fields must therefore represent all of $\mathcal{I}$.

Finally, $\#\mathcal{R} = \#\mathcal{M} - \#\mathcal{I} - \#\mathcal{S} = (p^n - p^{s+t})/(p - 1)$. $\qquad\square$

Corollary 4.3. *With the notation of Lemma 4.2, $HL^D = L^I$, the inertia field of $\mathcal{P}$.*

Proof. $\mathcal{P}$ is unramified in all $M \in \mathcal{M}$ with $M \subseteq HL^D$, and ramified in all other $M \in \mathcal{M}$. By definition of H and L^D as well as Corollary 4.1, HL^D is the maximal intermediate field of L/K in which $\mathcal{P}$ is unramified. $\qquad\square$

An immediate consequence of Corollary 4.1 is the decomposition law for the case of arbitrary n:

Theorem 4.4. *Let $\mathcal{M}$ be as given in (4.1), $\mathcal{P}$ a place of K, and s, t as in Lemma 4.2. Then the decomposition of $\mathcal{P}$ in L is $(e(\mathcal{P}), f(\mathcal{P}), r(\mathcal{P})) = (p^{n-s-t}, p^t, p^s)$. Furthermore, if k is finite, then $t \in \{0, 1\}$.*

Proof. $r(\mathcal{P}) = [L^D : K] = p^s$, $f(\mathcal{P}) = [L^I : L^D] = [HL^D : L^D] = p^t$ by Corollary 4.1, and $e(\mathcal{P}) = [L : L^I] = p^{n-s-t}$.

Now consider the compositum of Artin–Schreier extensions L^I/L^D. Every place of L^D is inert in L^I of relative degree p^t. If k is finite, then Theorem 3.4 forces $t \leq 1$. $\qquad\square$

The following example shows that all possible values for s and t can occur.

Example 4.5. Let $n \in \mathbb{N}$ and $s, t \in \mathbb{Z}$ so that $s, t \geq 0$ and $s + t \leq n$. Then for any rational prime $p > 0$, there exists a perfect field k of characteristic $p > 0$, such that for any function field K with constant field k and any place $\mathcal{P}$ of K, there exists an extension L of K that is the compositum of n degree p Artin–Schreier

extensions of K, so that the decomposition law of $\mathcal{P}$ in L/K is $(e(\mathcal{P}), f(\mathcal{P}), r(\mathcal{P})) = (p^{n-s-t}, p^t, p^s)$.

Proof. Repeatedly apply Examples 3.6 and 3.5 to construct L_1 and L_2 as composita of degree p Artin–Schreier extensions of K so that $[L_1 : K] = p^{n-s-t}$, $[L_2 : K] = p^t$, $\mathcal{P}$ totally ramifies in L_1/K, and $\mathcal{P}$ is inert in L_2/K. Note that if $t \geq 2$, then the base field k must be infinite by Theorem 4.4, whereas if $t \in \{0, 1\}$, any perfect base field k can be chosen.

Now construct L_3 as the compositum of degree p Artin–Schreier extensions of K so that $[L_3 : K] = p^s$ and $\mathcal{P}$ splits completely in L_3/K. The simplest way to do this is to set $L_3 = M_1 M_2 \cdots M_s$ where $M_i = K(y_i)$ with y_i as in (1.5) and $v_{\mathcal{P}}(a_i) > 0$ for $1 \leq i \leq s$. Finally, set $L = L_1 L_2 L_3$. $\qquad\square$

In principle, any different exponent $d(\mathfrak{P} \mid \mathcal{P})$ could be found by repeatedly applying Theorem 3.11. However, a closed form formula can be obtained via Theorem 4.4 by applying the following restructuring technique. For any field $M \in \mathcal{M}$ with $\mathcal{M}$ as in (4.1), denote by $\mathfrak{p}_M$ a place of M lying above $\mathcal{P}$. Write

$$\{d(\mathfrak{p}_M \mid \mathcal{P}) \mid M \in \mathcal{M}\} = \{d_1, d_2, \ldots, d_l\},$$

where the d_i are ordered so that $d_1 > d_2 > \cdots > d_l$. Clearly $l \leq n$. Now there exist positive integers $m_1, m_2, \ldots, m_l$ with $m_1 + m_2 + \cdots + m_l = n$ so that $d(\mathfrak{p}_M \mid \mathcal{P}) = d_i$ for exactly c_i fields $M \in \mathcal{M}$, where

$$c_i = \frac{p^{m_i + \cdots + m_l} - p^{m_{i+1} + \cdots + m_l}}{p - 1} = p^{m_{i+1} + \cdots + m_l} \frac{p^{m_i} - 1}{p - 1} \quad (1 \leq i \leq l).$$

Recall that $L = K(y_1, y_2, \ldots, y_n)$ with y_i given by (1.5) for $1 \leq i \leq n$. Set

$$\begin{aligned} K_0 &= L_n = K, \\ K_i &= K(y_1, y_2, \ldots, y_i), \quad L_{i-1} = K(y_i, \ldots, y_n) \quad \text{for } 1 \leq i \leq n, \end{aligned} \tag{4.3}$$

so $L = K_i L_i$ for $0 \leq i \leq n$. Now choose Artin–Schreier generators, again denoted by $y_1, y_2, \ldots, y_n$, so that

- $d(\mathfrak{p}_M \mid \mathcal{P}) = d_l$ for all $M \in \mathcal{M}$ with $M \subseteq L_{m_1 + \cdots + m_{l-1}}$;
- $d(\mathfrak{p}_M \mid \mathcal{P}) = d_{l-1}$ for all $M \in \mathcal{M}$ with $M \subseteq L_{m_1 + \cdots + m_{l-2}} \backslash L_{m_1 + \cdots + m_{l-1}}$;

$\qquad \vdots$

- $d(\mathfrak{p}_M \mid \mathcal{P}) = d_i$ for all $M \in \mathcal{M}$ with $M \subseteq L_{m_1 + \cdots + m_{i-1}} \backslash L_{m_1 + \cdots + m_i}$;

$\qquad \vdots$

- $d(\mathfrak{p}_M \mid \mathcal{P}) = d_1$ for all $M \in \mathcal{M}$ with $M \subseteq L_0 \backslash L_{m_1}$.

We are now ready to compute $d(\mathfrak{P} \mid \mathcal{P})$. The idea is to compute this quantity via the reordered field extension tower $L = K_n / K_{n-1} / \cdots / K_1 / K_0 = K$. Note that we restructured this tower by adjoining at the ith level the Artin–Schreier generator y_i with the largest remaining different exponent. That way, if $\mathfrak{q}_i$ denotes a place of

$K(y_i)$ lying above $\mathcal{P}$, then the field extension tower is reordered in such a way that the different exponents $d(\mathfrak{q}_i \,|\, \mathcal{P})$ range from largest to smallest, from bottom to top. This "pyramid-like" structure with respect to the size of different exponents turns out to be convenient for our computation.

Theorem 4.6. *Let $\mathcal{P}$ be a place of K and $\mathfrak{P} \,|\, \mathcal{P}$ a place of L. Let $y_1, y_2, \ldots, y_n$ be chosen as above, and K_i, L_i $(0 \leq i \leq n)$ given by (4.3). Set $\mathfrak{q}_i = \mathfrak{P} \cap K(y_i)$ for $1 \leq i \leq n$, and $\mathfrak{r}_i = \mathfrak{P} \cap K_i$ for $0 \leq i \leq n$. Then the different exponent at $\mathcal{P}$ is given by $d(\mathfrak{P} \,|\, \mathcal{P}) = d(\mathfrak{r}_n \,|\, \mathcal{P})$, where the intermediate different exponents can be computed recursively via $d(\mathfrak{r}_1 \,|\, \mathcal{P}) = d(\mathfrak{q}_1 \,|\, \mathcal{P})$ and $d(\mathfrak{r}_{i+1} \,|\, \mathcal{P}) = e(\mathfrak{q}_{i+1} \,|\, \mathcal{P})d(\mathfrak{r}_i \,|\, \mathcal{P}) + d(\mathfrak{q}_{i+1} \,|\, \mathcal{P})$ for $1 \leq i \leq n-1$, and we have*

$$d(\mathfrak{P} \,|\, \mathcal{P}) = \frac{e(\mathcal{P})}{p^n} \sum_{M \in \mathcal{M}} d(\mathfrak{p}_M \,|\, \mathcal{P}), \tag{4.4}$$

where $\mathfrak{p}_M$ is any place of M lying above $\mathcal{P}$ and $e(\mathcal{P})$ is the ramification index of $\mathcal{P}$ in L/K.

Proof. Since $\mathfrak{r}_1 = \mathfrak{q}_1$, the initialization $d(\mathfrak{r}_1 \,|\, \mathcal{P}) = d(\mathfrak{q}_1 \,|\, \mathcal{P})$ is obvious. By (1.4), it suffices to show $d(\mathfrak{r}_{i+1} \,|\, \mathfrak{r}_i) = d(\mathfrak{q}_{i+1} \,|\, \mathcal{P})$ and $e(\mathfrak{r}_{i+1} \,|\, \mathfrak{r}_i) = e(\mathfrak{q}_{i+1} \,|\, \mathcal{P})$ for $1 \leq i \leq n-1$. However, the second equality immediately follows from the first, since both ramification indices are equal to 1 or p, and

$$e(\mathfrak{q}_{i+1} \,|\, \mathcal{P}) = 1 \Leftrightarrow d(\mathfrak{q}_{i+1} \,|\, \mathcal{P}) = 0 \Leftrightarrow d(\mathfrak{r}_{i+1} \,|\, \mathfrak{r}_i) = 0 \Leftrightarrow e(\mathfrak{r}_{i+1} \,|\, \mathfrak{r}_i) = 1.$$
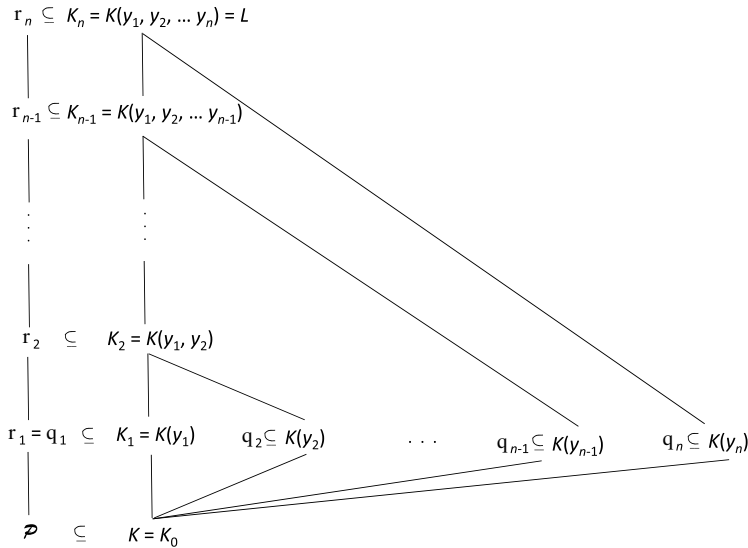
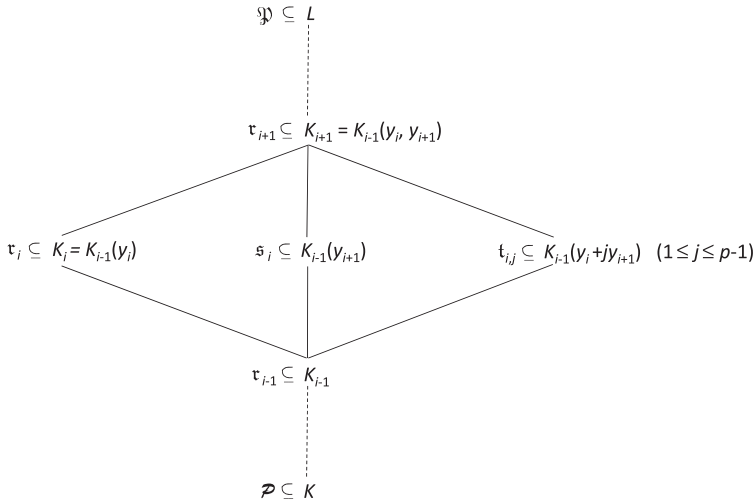

Fig. 1. Notation for the statement of Theorem 4.6.

Fig. 2. Notation for the proof of Theorem 4.6.

We induct on i to prove that $d(\mathfrak{r}_{i+1} \,|\, \mathfrak{r}_i) = d(\mathfrak{q}_{i+1} \,|\, \mathcal{P})$ for $0 \leq i \leq n-1$. Since $\mathfrak{r}_0 = \mathcal{P}$ and $\mathfrak{r}_1 = \mathfrak{q}_1$, this holds for $i = 0$. Let $1 \leq i \leq n-1$ and consider the elementary abelian p-extension K_{i+1}/K_{i-1} of degree p^2. Set $\mathfrak{s}_i = \mathfrak{P} \cap K_{i-1}(y_{i+1})$ and $\mathfrak{t}_{i,j} = \mathfrak{P} \cap K_{i-1}(y_i + jy_{i+1})$ for all $1 \leq j \leq p-1$. Then $d(\mathfrak{r}_i \,|\, \mathfrak{r}_{i-1}) = d(\mathfrak{q}_i \,|\, \mathcal{P})$, $d(\mathfrak{s}_i \,|\, \mathfrak{r}_{i-1}) = d(\mathfrak{q}_{i+1} \,|\, \mathcal{P})$, and $d(\mathfrak{t}_{i,j} \,|\, \mathfrak{r}_{i-1}) = d(\mathfrak{p}_M \,|\, \mathcal{P})$ for $M = K(y_i + jy_{i+1})$ by induction hypothesis. By the definition of the y_j, we have

$$d(\mathfrak{q}_i \,|\, \mathcal{P}) \geq d(\mathfrak{q}_{i+1} \,|\, \mathcal{P}). \tag{4.5}$$

If equality holds in (4.5), we have $d(\mathfrak{p}_M \,|\, \mathcal{P}) = d(\mathfrak{q}_i \,|\, \mathcal{P})$ for all $M \in \mathcal{M}$ with $M \subseteq L_{i-1}\backslash L_i$ by the definition of y_{i+1}. In particular, this implies

$$d(\mathfrak{p}_M \,|\, \mathcal{P}) = d(\mathfrak{q}_i \,|\, \mathcal{P}) \quad \text{if } M = K(y_i + jy_{i+1}) \quad \text{for any } 1 \leq j \leq p-1. \tag{4.6}$$

Note that (4.6) is true automatically by the strict triangle inequality if inequality holds in (4.5). Hence $d(\mathfrak{t}_{i,j} \,|\, \mathfrak{r}_{i-1}) = d(\mathfrak{p}_M \,|\, \mathcal{P}) = d(\mathfrak{q}_i \,|\, \mathcal{P})$ for $M = K(y_i + jy_{i+1})$ by (4.6). Thus $d(\mathfrak{r}_i \,|\, \mathfrak{r}_{i-1}) = (M+1)(p-1)$ and $d(\mathfrak{s}_i \,|\, \mathfrak{r}_{i-1}) = (m+1)(p-1)$; here, m and M are defined as in (3.6) with K, $K(y)$, $K(z)$ and L replaced by K_{i-1}, $K_{i-1}(y_{i+1})$, K_i and K_{i+1}, respectively. Now $d(\mathfrak{r}_{i+1} \,|\, \mathfrak{r}_i) = (m+1)(p-1) = d(\mathfrak{q}_{i+1} \,|\, \mathcal{P})$ follows from (3.13).

Finally, (4.4) follows easily by applying the recursive formula. $\square$

In particular, if $\mathcal{P}$ totally ramifies in L/K, then by Theorem 4.6,

$$d(\mathfrak{P} \,|\, \mathcal{P}) = \sum_{M \in \mathcal{M}} d(\mathfrak{p}_M \,|\, \mathcal{P}). \tag{4.7}$$

The above identity (4.7) can also be found in the (unpublished) Ph.D. dissertation [26]. Note that once again the closed form formulae (4.7) and (4.4) show that

the different exponent of L/K can be read directly from the intermediate degree p extensions M/K.

We conclude this section with another application of Theorem 4.4 that leads to an easy and direct proof of a multiplicative formula connecting the zeta functions of L, K, and the intermediate degree p Artin–Schreier extensions of K. This result was first given in [9], based on techniques from [17, 10]; see [21]. For any function field E over a finite field, denote by ζ_E the zeta function of E.

Theorem 4.7. *Suppose k is finite of characteristic p, and $\mathcal{M}$ given by (4.1). Then*

$$\frac{\zeta_L}{\zeta_K} = \prod_{M \in \mathcal{M}} \frac{\zeta_M}{\zeta_K}.$$

Proof. Fix an arbitrary place $\mathcal{P}$ of K and set $\mathfrak{s}$ to be a complex variable. Let $\mathcal{R}$, $\mathcal{I}$ and $\mathcal{S}$ be defined by (4.2), and s, t as given in Lemma 4.2. Since the Euler products of the zeta functions exist for $\mathrm{Re}(\mathfrak{s}) > 1$, it suffices to show

$$(1 - N^{p^t})^{p^s} = (1 - N)^{1 - \#\mathcal{M}} \prod_{M \in \mathcal{R}} (1 - N) \prod_{M \in \mathcal{I}} (1 - N^p) \prod_{M \in \mathcal{S}} (1 - N)^p, \qquad (4.8)$$

where $N = q^{-\mathfrak{s} \deg(\mathcal{P})}$. By Theorem 4.4, $t \in \{0, 1\}$. Obviously, (4.8) reduces to

$$(1 - N^{p^t})^{p^s} = (1 - N)^{1 - \#\mathcal{M}} (1 - N)^{\#\mathcal{R}} (1 - N^p)^{\#\mathcal{I}} (1 - N)^{p \, \#\mathcal{S}},$$

and this identity is straightforward to verify for $t = 0, 1$ using Lemma 4.2. □

Theorem 4.8 easily yields similar multiplicative relationships linking various invariants of L, K and the intermediate fields in $\mathcal{M}$. For any function field extension $E/\mathbb{F}_q(x)$, let h_E, H_E, and R_E denote the divisor class number, the ideal class number, and the regulator of E, respectively, of $E/\mathbb{F}_q(x)$ for some fixed $x \in E$ that is transcendental over $\mathbb{F}_q$. Also, let f_E be the least common multiple of $f(\mathfrak{p} \,|\, P_\infty)$ for all infinite places $\mathfrak{p}$ of E, where P_∞ is the infinite place of the rational function field $\mathbb{F}_q(x)$. By [22], we have

$$h_E f_E = H_E R_E. \qquad (4.9)$$

This implies the following:

Corollary 4.8. *Suppose k is finite of characteristic p, and $\mathcal{M}$ given by (4.1). Then*

$$\frac{h_L}{h_K} = \prod_{M \in \mathcal{M}} \frac{h_M}{h_K}, \quad \frac{H_L}{H_K} = \prod_{M \in \mathcal{M}} \frac{H_M}{H_K}.$$

If $\mathcal{P}$ is any place of K lying above the infinite place of $\mathbb{F}_q(x)$, and s, t as given in Lemma 4.2, then

$$\frac{R_L}{R_K} = \prod_{M \in \mathcal{M}} \frac{R_M}{R_K} \quad \text{if } t = 0 \quad \text{and} \quad p^{s-1} \frac{R_L}{R_K} = \prod_{M \in \mathcal{M}} \frac{R_M}{R_K} \quad \text{if } t = 1.$$

Proof. The divisor class number formula follows immediately from Theorem 4.7. The ideal class number formula follows by applying (4.8) at all finite places of K and taking products.

If $t = 0$, then $f_L = f_K = f_M$ for all $M \in \mathcal{M}$. Then the regulator formula follows from (4.9) and the formulae for the divisor and ideal class numbers. If $t = 1$, then $f_L = pf_K$. By Lemma 4.2, there are exactly $\#\mathcal{I} = (p^{s+1} - p^s)/(p - 1) = p^s$ fields $M \in \mathcal{M}$ satisfying $f_M = pf_K$. The remaining $\#\mathcal{M} - \#\mathcal{I}$ fields $M \in \mathcal{M}$ satisfy $f_M = f_K$. Again our result follows from (4.9), the formulae for the divisor and ideal class numbers. □

We remark on an interesting link between the multiplicative divisor class number formula of Theorem 4.7 and an additive genus formula. By a result of Kani [17], certain relations among the idempotents of $\mathrm{Gal}(L/K)$ in the group algebra over $\mathbb{Q}$ imply corresponding relations among the genera of the intermediate fields of L/K. Using this result, Garcia and Stichtenoth [12] found an additive genus formula which was also obtained in [18]. In our notation, if g_E denotes the genus of a function field E, this reads

$$g_L = \sum_{M \in \mathcal{M}} g_M - \frac{p^n - p}{p - 1} g_K.$$

5. Conclusion

The different exponents and decomposition properties for a compositum of Artin–Schreier extensions are essentially determined by the splitting in all the intermediate degree p Artin–Schreier extensions. In particular, a place is inert/totally ramifies/ splits completely in any intermediate field if and only if it exhibits the same corresponding decompositions in all the intermediate degree p Artin–Schreier extensions.

The decomposition law for Artin–Schreier composita can be used to derive closed form formulae for any different exponent. This is accomplished by choosing suitable Artin–Schreier generators. The extension tower is then built up in a pyramid-like fashion, with the different exponents in the degree p extensions decreasing as the corresponding level increases. Another direct consequence of the decomposition law is a multiplicative formula for the zeta function, yielding in turn corresponding relations for the divisor class number, ideal class number, and regulator.

In a compositum of just two Artin–Schreier extensions, we noted that the converse of Abhyankar's Lemma (Proposition 3.2) holds. Moreover, the ramification group filtration is also completely dictated by the decomposition data in the intermediate degree p extensions. A characterization of the ramification group sequence in a compositum of an arbitrary (finite) number of Artin–Schreier extensions is the subject of a forthcoming paper.

Also of interest is the question to what extent analogous phenomena occur in other types of composita; for example, for which types of field extension towers the behavior of a place in the top level field (or any intermediate field) is characterized

solely by the corresponding behavior at the second level, or more generally, in lower levels.

Acknowledgments

References

[1] N. Anbar, H. Stichtenoth and S. Tutdere, On ramification in the compositum of function fields, *Bull. Braz. Math. Soc.* (*N.S.*) **40** (2009) 539–552.

[2] C. Arf, Untersuchungen über reinverzweigte Erweiterungen diskret bewerteter perfekter Körper, *J. Reine Angew. Math.* **181** (1940) 1–44.

[3] E. Artin and O. Schreier, Eine Kennzeichnung der reell abgeschlossenen Körper, *Hamb. Abh.* **5** (1927) 225–231.

[4] P. Beelen, A. Garcia and H. Stichtenoth, On towers of function fields of Artin–Schreier type, *Bull. Braz. Math. Soc.* (*N.S.*) **35** (2004) 151–164.

[5] P. Beelen, A. Garcia and H. Stichtenoth, On towers of function fields over finite fields, in *Arithmetic, Geometry and Coding Theory* (*AGCT 2003*), Sémin. Congr., Vol. 11 (Soc. Math. France, Paris, 2005), pp. 1–20.

[6] P. Beelen, A. Garcia and H. Stichtenoth, Towards a classification of recursive towers of function fields over finite fields, *Finite Fields Appl.* **12** (2006) 56–77.

[7] E. Çakçak and F. Özbudak, Some Artin–Schreier type function fields over finite fields with prescribed genus and number of rational places, *J. Pure Appl. Algebra* **210** (2007) 113–135.

[8] H. Cohen, *Advanced Topics in Computational Number Theory*, GTM, Vol. 193 (Springer-Verlag, New York, 2000).

[9] I. Duursma, H. Stichtenoth and C. Voss, Generalized Hamming weights for duals of BCH codes, and maximal algebraic function fields, in *Arithmetic, Geometry and Coding Theory* (*AGCT 1993*) (de Gruyter, Berlin, 1996), pp. 53–65.

[10] G. Frey and H.-G. Rück, The strong Lefschetz principle in algebraic geometry, *Manuscripta Math.* **55** (1986) 385–401.

[11] I. B. Fesenko and S. V. Vostokov, *Local Fields and Their Extensions*, Translation of Mathematical Monographs, Vol. 121, 2nd edn. (American Mathematical Society, Providence, RI, 2002).

[12] A. Garcia and H. Stichtenoth, Elementary abelian p-extensions of algebraic function fields, *Manuscripta Math.* **72** (1991) 67–79.

[13] A. Garcia and H. Stichtenoth, A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound, *Invent. Math.* **121** (1995) 211–222.

[14] A. Garcia and H. Stichtenoth, Some Artin–Schreier towers are easy, *Mosc. Math. J.* **5** (2005) 767–774.

[15] C. Güneri and F. Özbudak, Artin–Schreier extensions and their applications, in *Topics in Geometry, Coding Theory and Cryptography*, Algebr. Appl., Vol. 6 (Springer, Dordrecht, 2007), pp. 105–133.

[16] H. Hasse, Theorie der relativ zyklischen algebraischen Funktionenkörper, *J. Reine Angew. Math.* **172** (1934) 37–54.

[17] E. Kani, Relations between the genera and between the Hasse–Witt invariants of Galois coverings of curves, *Canad. Math. Bull.* **28** (1985) 321–327.

[18] G. Lachaud, Artin–Schreier curves, exponential sums, and the Carlitz–Uchiyama bound for geometric codes, *J. Number Theory* **39** (1991) 18–40.

[19] S. Lang, *Algebra*, GTM, Vol. 211, 2nd edn. (Addison-Wesley, Reading, MA, 1984).

[20] D. J. Madden, Arithmetic in generalized Artin–Schreier extensions of $k(x)$, *J. Number Theory* **10** (1978) 303–323.

[21] A. Pacheco, A note on relations between the zeta-functions of Galois coverings of curves over finite fields, *Canad. Math. Bull.* **33** (1990) 282–285.

[22] F. K. Schmidt, Analytische Zahlentheorie in Körpern der Charakteristik p, *Math. Z.* **33** (1931) 668–678.

[23] H. Stichtenoth, *Algebraic Function Fields and Codes*, GTM, Vol. 254, 2nd edn. (Springer-Verlag, Berlin–Heidelberg, 2009).

[24] L. Thomas, Ramification groups in Artin–Schreier–Witt extensions, *J. Théor. Nombres Bordeaux* **17** (2005) 689–720.

[25] G. D. Villa Salvador, *Topics in the Theory of Algebraic Function Fields* (Birkhäuser Boston Inc., 2006); Translated from Spanish.

[26] C. Voss, Abschätzungen der Parameter von Spurcodes mit Hilfe algebraischer Funktionenkörper, Ph.D. Dissertation, Universität Duisburg-Essen, Germany (1993).