BULLETIN OF THE BRAZILIAN MATHEMATICAL SOCIETY

Bull Braz Math Soc, New Series 40(4), 539-552

On ramification in the compositum of function fields

Nurdagül Anbar, Henning Stichtenoth and Seher Tutdere

Abstract. The aim of this paper is twofold: Firstly, we generalize well-known formulas for ramification and different exponents in cyclic extensions of function fields over a field K (due to H. Hasse) to extensions $E = F(y)$, where y satisfies an equation of the form $f(y) = u \cdot g(y)$ with polynomials $f(y), g(y) \in K[y]$ and $u \in F$. This result depends essentially on Abhyankar's Lemma which gives information about ramification in a compositum $E = E_1E_2$ of finite extensions E_1, E_2 over a function field F. Abhyankar's Lemma does not hold if both extensions E_1/F and E_2/F are wildly ramified. Our second objective is a generalization of Abhyankar's Lemma if E_1/F and E_2/F are cyclic extensions of degree $p = \mathrm{char}(K)$. This result may be useful for the study of wild towers of function fields over finite fields.

Keywords: function fields, ramification, Abhyankar's Lemma.

Mathematical subject classification: 14H05, 14G15, 11R58.

1 Introduction

In general it is a difficult task to compute the genus $g = g(E)$ of an algebraic function field E/K with constant field K. Perhaps the most powerful tool to do this is the Hurwitz genus formula, which relates $g(E)$ with the genus $g(F)$ of a subfield $K \subseteq F \subseteq E$ of finite degree $[E\colon F] < \infty$. The main ingredient of this formula is the different $\mathrm{Diff}(E/F)$, which is a divisor of E and contains all places of E which are ramified over F. It is therefore of fundamental importance to determine the different exponents $d(P'|P)$ for all places P of F and all places P' of E lying above P.

The field E is often obtained as the compositum of two subfields $E = E_1E_2$, where E_1 and E_2 are finite separable extensions of some field $F \subseteq E_1 \cap E_2$.

Received 11 March 2009.

In this situation, Abhyankar's Lemma (see Proposition 1.1 below) gives information about ramification in E/E_1 (resp. in E/E_2) if one knows the behaviour of ramified places in E_1/F and E_2/F.

The aim of our paper is twofold. In Section 2 we use Abhyankar's Lemma to give a simple proof for ramification and different exponents in cyclic extensions of function fields (due to H. Hasse [4]). Our approach yields a far-reaching generalization of Hasse's formulas, see Theorem 2.1. In Section 3 we consider the case where E_1 and E_2 are both cyclic extensions of F of degree $[E_1 : F] = [E_2 : F] = p = \mathrm{char}(K)$ and hence $E = E_1E_2$ is an elementary-abelian extension of F of degree $[E : F] = p^2$. This case (where Abhyankar's Lemma does not work because of wild ramification) has been of great interest in the study of towers of function fields over finite fields, cf. [2, 3]. We give a version of Abhyankar's Lemma in this situation, which might be useful for further investigations of towers.

Throughout this paper we use standard notations from the theory of algebraic function fields, cf. [5, 6, 7]. Let F/K be a function field with K being the full constant field of F, and assume always that K is a perfect field. The discrete valuation corresponding to a place P of F/K is denoted by v_P, and the corresponding valuation ring is $\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\}$. Let E/F be a finite separable extension. For a place P of F and a place P' of E lying over P, denote by $e(P'|P)$ (resp. $d(P'|P)$) the ramification index (resp. the different exponent) of $P'|P$. The extension $P'|P$ is said to be tame if $e(P'|P)$ is not divisible by the characteristic of K, otherwise $P'|P$ is called wild. In the case of tame ramification, the different exponent is given by $d(P'|P) = e(P'|P) - 1$, and in case of wild ramification one has $d(P'|P) \geq e(P'|P)$.

Now we state Abhyankar's Lemma [6, p. 137]:

Proposition 1.1 (Abhyankar's Lemma)**.** *Let E/F be a finite separable extension of function fields over K. Suppose that $E = E_1E_2$ is the compositum of two intermediate fields $F \subseteq E_1, E_2 \subseteq E$. Let P' be a place of E and set $P := P' \cap F$, $P_1 := P' \cap E_1$ and $P_2 := P' \cap E_2$. Assume that at least one of the extensions $P_1|P$ or $P_2|P$ is tame. Then*

$$e(P'|P) = \mathrm{lcm}\{e(P_1|P), e(P_2|P)\}\ ,$$

where lcm *stands for the least common multiple.*

2 A generalization of Hasse's Formulas

In his paper "Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper" [4], H. Hasse gave explicit for-

mulas for the different exponents if E can be written as $E = F(y)$ and y satisfies one of the following equations:

$$y^n = u \in F, \quad \text{with} \quad \gcd(n, \mathrm{char}(K)) = 1\ , \ \text{or} \tag{2.1}$$

$$y^p - y = u \in F, \quad \text{where} \quad \mathrm{char}(K) = p > 0\ . \tag{2.2}$$

In case (2.1), the extension E/F is a Kummer extension (if K contains all n^{th} roots of unity), in case (2.2) it is an Artin-Schreier extension; so in both cases, E/F is a cyclic Galois extension. Hasse's formulas are extremely useful for genus computations in Galois extensions of function fields; we will recall them in Corollary 2.2 and 2.3 below. Here we just remark that Hasse's proofs in the cases (2.1) and (2.2) are quite different; in case (2.2) one uses the explicit description of the automorphisms of E/F.

Observe that both equations (2.1), (2.2) are of the form $f(y) = u \in F$ with some polynomial $f(y) \in K[y]$. We consider now a more general situation. Suppose that $E = F(y)$ and y satisfies an equation

$$f(y) = u \cdot g(y) \quad \text{with} \quad f(y), g(y) \in K[y] \quad \text{and} \quad u \in F \setminus K\ . \tag{2.3}$$

Without loss of generality we can assume that the polynomials $f(y)$, $g(y)$ are relatively prime in $K[y]$. If the characteristic of K is $\mathrm{char}(K) = p > 0$, we also assume that the extension $F/K(u)$ is separable, and not both $f(y)$, $g(y)$ are in $K[y^p]$ (which implies that E/F is separable as well). It follows from Equation (2.3) that $K(u) \subseteq F \subseteq E$ and $K(u) \subseteq K(y) \subseteq E$, and E is the compositum $E = F \cdot K(y)$. Setting $n := \max\{\deg f, \deg g\}$, it is clear that $[K(y)\colon K(u)] = n$. We do not assume however that the polynomial $f(Y) - ug(Y) \in F[Y]$ is irreducible over F; it may happen that it is reducible and hence $[E\colon F] < n$. The main result of this section is as follows:

Theorem 2.1. *With notations and assumptions as above, let P' be a place of E. Set $P := P' \cap F$, $Q := P' \cap K(u)$ and $Q' := P' \cap K(y)$. Assume that not both extensions $P|Q$ and $Q'|Q$ are wild. We set $e_0 := e(P|Q)$, $e := e(Q'|Q)$, $r := \gcd(e_0, e)$ and $d := d(Q'|Q)$. Then the following hold:*

(a) *$e(P'|P) = e/r$. In particular, if $Q'|Q$ is tame then $P'|P$ is also tame and hence its different exponent is $d(P'|P) = e(P'|P) - 1 = e/r - 1$.*

(b) *If $P|Q$ is tame, then*

$$d(P'|P) = \frac{e_0(d + 1 - e) + e}{r} - 1\ .$$

Proof.

(a) This is just Abhyankar's Lemma.

(b) Using transitivity of different exponents [6, p. 98] in the extensions $K(u) \subseteq F \subseteq E$ and $K(u) \subseteq K(y) \subseteq E$ and observing that the extensions $P|Q$ and $P'|Q'$ are tame, we obtain

$$d(P'|P) + (e_0 - 1) \cdot e(P'|P) = (e(P'|Q') - 1) + e(P'|Q') \cdot d \ .$$

As $e(P'|P) = e/r$ and $e(P'|Q') = e_0/r$ by (a), the result follows easily. □

Hasse's formulas for ramification and different exponents in Kummer and Artin-Schreier extensions are simple special cases of Theorem 2.1:

Corollary 2.2 (Kummer extensions)**.** *Suppose that $E = F(y)$ and y satisfies the equation*

$$y^n = u \in F, \quad \textit{with} \ \ \gcd(n, \mathrm{char}(K)) = 1 \ .$$

Let P be a place of F and let P' be a place of E lying above P. Then $P'|P$ is tame, and the ramification index of $P'|P$ is given by

$$e(P'|P) = n/r \ , \ \ \textit{with} \ \ r := \gcd(n, v_P(u)) \ .$$

In particular, all places P with $v_P(u) \equiv 0 \mod n$ are unramified in E/F.

Proof. With notations as in Theorem 2.1, the only ramified places in the extension of rational function fields $K(y)/K(y^n)$ are the zero Q_0 and the pole Q_∞ of $u = y^n$, and their ramification index in $K(y)/K(y^n)$ is $e = n$. The ramification index of a place P of F lying above Q_0 (resp. Q_∞) is $e_0 = v_P(u)$ (resp. $e_0 = -v_P(u)$). Hence the result follows from Theorem 2.1. □

Corollary 2.3 (Artin-Schreier extensions)**.** *Suppose that $E = F(y)$ and y satisfies the equation*

$$y^p - y = u \in F, \quad \textit{with} \quad \mathrm{char}(K) = p > 0 \ .$$

Let P be a place of F and let P' be a place of E lying above P. If $v_P(u) \geq 0$ then $P'|P$ is unramified in E/F. If $v_P(u) = -m < 0$ with $m \not\equiv 0 \mod p$, then $e(P'|P) = p$, and the different exponent is given by

$$d(P'|P) = (m + 1)(p - 1) \ .$$

Proof. The only ramified place in the extension $K(y)/K(u)$ is the pole Q_∞ of $u = y^p - y$. Let Q'_∞ be the place of $K(y)$ above Q_∞ (so Q'_∞ is the pole of y in $K(y)$). It is easy to check that

$$e(Q'_\infty|Q_\infty) = p \quad \text{and} \quad d(Q'_\infty|Q_\infty) = 2p - 2$$

(see also Example 2.5 below). Now we apply Theorem 2.1(b) and obtain

$$d(P'|P) = m((2p-2) + 1 - p) + p - 1 = (m+1)(p-1)\,. \qquad \square$$

In order to apply Theorem 2.1 in other cases, one has to know the ramified places and their different exponents in the extension of rational function fields $K(y)/K(u)$, where $u = f(y)/g(y) \in K(y)$. The polynomials $f(y), g(y)$ are relatively prime, and in case of positive characteristic $\mathrm{char}(K) = p > 0$ not both of them are in $K[y^p]$. After an appropriate rational transformation $u \mapsto (au+b)/(cu+d)$ with $a, b, c, d \in K$ and $ad - bc \neq 0$ we can assume that moreover

$$u = \frac{f(y)}{g(y)}\,, \quad f(y) \text{ and } g(y) \text{ are monic polynomials, and}$$

$$\deg f(y) =: n > m := \deg g(y). \tag{2.4}$$

In what follows we will assume all these normalizations implicitly. Note that $K(y)/K(u)$ is a separable extension of degree $[K(y)\colon K(u)] = n$. The places of the rational function field $K(y)$ are in 1-1 correspondence with monic irreducible polynomials $p(y) \in K[y]$, and the pole of y; we will denote them as $P_{p(y)}$ and P_∞, respectively. Similarly the places of $K(u)$ will be denoted as $Q_{q(u)}$, resp. Q_∞. From (2.4) it follows that the places of $K(y)$ lying above Q_∞ are exactly the places corresponding to irreducible factors $p(y)|g(y)$, and also P_∞ (since $\deg f(y) > \deg g(y)$).

Proposition 2.4. *With the above notations, suppose that $P = P_{p(y)}$ is a place of $K(y)$ which is neither the pole of y nor a zero of $g(y)$ (i.e., $p(y) \nmid g(y)$). Let $Q := P \cap K(u)$. Then we have:*

(a) *$P|Q$ is ramified if and only if $p(y)$ divides $(f'(y)\cdot g(y) - f(y)\cdot g'(y))$.*

(b) *$d(P|Q) = v_P(f'(y)g(y) - f(y)g'(y))$ (i.e., $d(P|Q)$ is the exponent of $p(y)$ in the factorization of $f'(y)\cdot g(y) - f(y)\cdot g'(y)$ into irreducible factors).*

Proof. Let $\mathcal{O}_Q \subseteq K(u)$ be the valuation ring of the place Q, and let $\tilde{\mathcal{O}}_Q \subseteq K(y)$ be its integral closure in $K(y)$. The minimal polynomial for y over $K(u)$ is the polynomial $\varphi(Y) = f(Y) - ug(Y) \in \mathcal{O}_Q[Y]$, so y is integral over $\mathcal{O}_Q$ and

$$\mathcal{O}_Q[y] = \sum_{i=0}^{n-1} \mathcal{O}_Q \cdot y^i \subseteq \tilde{\mathcal{O}}_Q.$$

As every ring R with $K[y] \subseteq R \subseteq K(y)$ is integrally closed, it follows that $\mathcal{O}_Q[y] = \tilde{\mathcal{O}}_Q$ and hence $\{1, y, y^2, \ldots, y^{n-1}\}$ is an integral basis at Q. Then the different exponent $d(P|Q)$ is given by $d(P|Q) = v_P(\varphi'(y))$ (see [6, p. 107]). Since

$$\varphi'(y) = f'(y) - u \cdot g'(y) = f'(y) - \frac{f(y)}{g(y)} \cdot g'(y) = \frac{(f'g - fg')(y)}{g(y)}$$

and $v_P(g(y)) = 0$, we obtain

$$d(P|Q) = v_P(f'(y)g(y) - f(y)g'(y)) \,.$$

Hence we have proved (b). From this we also conclude (a), because exactly the ramified places have different exponents $d(P|Q) > 0$. □

Those places of $K(y)$ whose ramification behaviour in $K(y)/K(u)$ is not described by Proposition 2.4, are the pole P_∞ of y and the zeros of $g(y)$; they are just the poles of u in $K(y)$, and one can read their ramification indices immediately from the equation $u = f(y)/g(y)$. The different exponents of such places can be determined as follows: choose an element $\alpha \in K$ such that $f(\alpha) = 0$. (If necessary, one has to extend the constant field for finding α. This does not matter since in a constant field extension the different exponents do not change.) Then the element $t := (y - \alpha)^{-1}$ satisfies the equation

$$\frac{1}{u} = \frac{g(\alpha + t^{-1}) \cdot t^{\deg f}}{f(\alpha + t^{-1}) \cdot t^{\deg f}} =: \frac{f_1(t)}{g_1(t)}$$

with polynomials $f_1(t)$, $g_1(t) \in K[t]$ and $\deg f_1 > \deg g_1$. This gives an integral equation for t at the pole of u, and we obtain the different exponents as in Proposition 2.4.

We illustrate our results with 2 examples.

Example 2.5. Assume that $u = f(y)$ is a polynomial of degree $n > 1$ (and f is not a polynomial in y^p if $\mathrm{char}(K) = p > 0$). Then the pole Q_∞ of u is totally ramified in $K(y)/K(u)$, the place above is just the pole P_∞ of y.

The other ramified places are exactly the zeros of $f'(y)$, by Proposition 2.4. Their different exponents are

$$d(P|Q) = v_P(f'(y)) .$$

From Hurwitz genus formula follows that the degree of the different of $K(y)/K(u)$ is $2n-2$ and hence

$$d(P_\infty|Q_\infty) = 2n - 2 - \deg f'(y) .$$

A special case of this example is when $f(y)$ has the form

$$f(y) = ay + \sum_{j=0}^{k} a_j y^{jp} \text{ with } a, a_j \in K \text{ and } a \neq 0 .$$

In this case $f'(y) = a$ has no zeros, hence only the pole P_∞ of y is ramified in $K(y)/K(u)$, with ramification index $e(P_\infty|Q_\infty) = n$ and different exponent $d(P_\infty|Q_\infty) = 2(n-1)$.

As an application we obtain a generalization of Corollary 2.3.

Corollary 2.6. *Let F/K be a function field with $char(K) = p > 0$, and consider an extension $E = F(y)$, where y satisfies the equation*

$$ay + \sum_{j=1}^{k} a_j y^{jp} = u \in F \text{ with } a, a_j \in K \text{ and } a, a_k \neq 0 .$$

Then we have:

(a) *All places of F with $v_P(u) \geq 0$ are unramified in E/F.*

(b) *Suppose that P is a place of F with $v_P(u) = -m < 0$ and $p \nmid m$. Set $r := \gcd(m,k)$. Let P' be a place of E lying above P. Then the ramification index and different exponent of $P'|P$ are*

$$e(P'|P) = kp/r \text{ and } d(P'|P) = \frac{m(kp-1)+kp}{r} - 1 .$$

In particular, if $\gcd(m, kp) = 1$, then $[E\colon F] = kp$, P is totally ramified in E/F and

$$d(P'|P) = (m+1)(kp-1) .$$

Example 2.7. Suppose that $\mathrm{char}(K) = p > 0$. We consider the extension of rational function fields $K(y)/K(u)$ given by

$$u = \frac{f(y)}{g(y)} \quad \text{with} \quad f(y) = y^{2p} - y^p - 1\,, g(y) = y^p - y\,.$$

We assume that

$$p \equiv 2 \text{ or } 3 \mod 5, \quad \text{and} \quad \mathbb{F}_{p^2} \subseteq K\,.$$

From these assumptions follows easily (using quadratic reciprocity) that the two roots α, β of $f(y) = 0$ are in $K \setminus \mathbb{F}_p$, hence $f(y)$ and $g(y)$ are relatively prime. It is clear that above the zero Q_0 of u there are exactly 2 places P_α, P_β of $K(y)$, namely the zeros of $y - \alpha$ and of $y - \beta$. Their ramification indices are $e(P_\alpha|Q_0) = e(P_\beta|Q_0) = p$, so they are wild. It is also obvious that the pole P_∞ of y lies above the pole Q_∞ of u with ramification index $e(P_\infty|Q_\infty) = p$, and the other places above Q_∞ are unramified in $K(y)/K(u)$. We want to determine the different exponents of P_α, P_β and P_∞.

It follows from Proposition 2.4 that for each place P, which is not the pole of y or a zero of $y^p - y$, the different exponent of P over $Q := P \cap K(u)$ is

$$\begin{aligned} d(P|Q) &= v_P\big(f'(y)g(y) - f(y)g'(y)\big) \\ &= v_P\big(y^{2p} - y^p - 1\big) = p \cdot v_P\big(y^2 - y - 1\big). \end{aligned}$$

Hence $d(P_\alpha|Q_0) = d(P_\beta|Q_0) = p$. For the place $P = P_\infty$ we consider the element $t := (y - \alpha)^{-1}$ which satisfies the equation

$$u^{-1} = \frac{\big((\alpha + t^{-1})^p - (\alpha + t^{-1})\big) \cdot t^{2p}}{\big((\alpha + t^{-1})^{2p} - (\alpha + t^{-1})^p - 1\big) \cdot t^{2p}} =: \frac{f_1(t)}{g_1(t)}\,.$$

Now Proposition 2.4 gives

$$\begin{aligned} d(P_\infty|Q_\infty) &= v_{P_\infty}\big(f_1'(t)g_1(t) - f_1(t)g_1'(t)\big) \\ &= v_{P_\infty}\big(f_1'(t) \cdot g_1(t)\big) = 2p - 2\,. \end{aligned}$$

All places except P_α, P_β and P_∞ are unramified in $K(y)/K(u)$.

Another question which is raised by Abhyankar's Lemma, is the following. Given a compositum $E = E_1E_2$ of function fields $E_i \supseteq F$ $(i = 1, 2)$ and places P_1 of E_1 and P_2 of E_2 such that $P_1 \cap F = P_2 \cap F$, does there always exist a place P' of E which lies over P_1 and P_2? Since we did not find an easily accessible reference, we include here the following result (see [8]).

Proposition 2.8. *Let E/F be a finite separable extension of function fields such that $E = E_1E_2$ is the compositum of two intermediate fields $F \subseteq E_1$, $E_2 \subseteq E$. Let P be a place of F and let P_1 (resp. P_2) be a place of E_1 (resp. E_2) lying above P. Assume moreover that $[E\colon E_1] = [E_2\colon F]$ (i.e., the fields E_1 and E_2 are linearly disjoint over F). Then there exists a place P' of E which lies over P_1 and P_2.*

Proof. We fix a finite extension field $M \supseteq E$ such that M/F is Galois, and denote by $\mathrm{Gal}(M/F)$ the Galois group of M/F. Choose places R and S of M with $R|P_1$ and $S|P_2$. Since $\mathrm{Gal}(M/F)$ acts transitively on the extensions of P in M, there is an automorphism $\sigma \in \mathrm{Gal}(M/F)$ with $\sigma(R) = S$.

Next we choose an element $z \in E_1$ with the following properties: $v_{P_1}(z) > 0$, and $v_Q(z) \leq 0$ for all places $Q \neq P_1$ of E_1. It holds in particular that

$$v_S\big(\sigma(z)\big) = v_{\sigma(R)}\big(\sigma(z)\big) = v_R(z) > 0.$$

Let $h(T) \in F[T]$ be the minimal polynomial of z over F. Then $h(T)$ is also irreducible over the field E_2. The Galois group of M/E_2 acts transitively on the roots of $h(T)$, so there exists an automorphism $\tau \in \mathrm{Gal}(M/E_2)$ with $\tau(\sigma(z)) = z$. We claim that the place $\tau(S)$ of M lies over P_1 and P_2. In fact, since $S \cap E_2 = P_2$ and $\tau \in \mathrm{Gal}(M/E_2)$, it is clear that $\tau(S)|P_2$. On the other hand,

$$v_{\tau(S)}(z) = v_{\tau(S)}\big(\tau(\sigma(z))\big) = v_S\big(\sigma(z)\big) > 0.$$

As P_1 is the only place of E_1, which lies above P and is a zero of z, we conclude that $\tau(S)|P_1$. This proves our claim.

The restriction $P' := \tau(S) \cap E$ of $\tau(S)$ to E is a common extension of P_1 and P_2 in E, as desired. □

Proposition 2.8 does not hold in general without the assumption that the fields E_1, E_2 are linearly disjoint over F, as the following example shows. Let $E = E_1E_2$ with $[E_1\colon F] = n$, $[E_2\colon F] = m$ and $[E\colon F] = k < mn$. Suppose that P is a place of F which splits completely in E_1/F and in E_2/F; i.e., there are n distinct places $Q_1, \ldots, Q_n$ of E_1 and m distinct places $R_1, \ldots, R_m$ of E_2 above P. Since P has at most $k = [E\colon F]$ extensions P' in E, not all of the nm pairs (Q_i, R_j) can be obtained as $(P' \cap E_1, P' \cap E_2)$.

3 Elementary abelian extensions of degree p^2

As before, we consider a finite separable extension E/F of function fields over K, where E can be obtained as the compositum $E = E_1E_2$ of two intermediate

fields $F \subseteq E_1, E_2 \subseteq E$. We assume in this section that the characteristic of K is positive, $\mathrm{char}(K) = p > 0$. Let P' be a place of E and $P := P' \cap F$, $P_i := P' \cap E_i$ for $i = 1, 2$. If both extensions $P_1|P$ and $P_2|P$ are wild, then Abhyankar's Lemma does not apply to give information about ramification of $P'|P_1$ (resp. $P'|P_2$).

In the papers [2, 3] the following lemma plays a key role for determining the asymptotic behaviour of the genus in some towers of function fields over finite fields of characteristic p.

Lemma 3.1. *With notations as above, assume that the extensions E_1/F and E_2/F are cyclic extensions of degree p with $E_1 \neq E_2$, so their compositum $E = E_1E_2$ is Galois over F of degree $[E : F] = p^2$. Assume that the places $P_1|P$ and $P_2|P$ are ramified with ramification index $e(P_1|P) = e(P_2|P) = p$ and different exponent $d(P_1|P) = d(P_2|P) = 2(p-1)$. Then one of the following assertions holds:*

(1) $e(P'|P_1) = e(P'|P_2) = 1$, *or*

(2) $e(P'|P_1) = e(P'|P_2) = p$ *and* $d(P'|P_1) = d(P'|P_2) = 2(p-1)$.

In Theorem 3.4 below we will generalize Lemma 3.1. As a preparation we recall briefly Hilbert's theory of ramification groups, cf. [6, Sec. 3.8]. Let E/F be a Galois extension of function fields, $G := \mathrm{Gal}(E/F)$ its Galois group. Let P be a place of F and P' a place of E lying over P. One defines for every $i \geq -1$ the i-th ramification group of $P'|P$,

$$G_i(P'|P) = \left\{\sigma \in G \mid v_{P'}(\sigma z - z) \geq i + 1 \text{ for all } z \in \mathcal{O}_{P'}\right\}.$$

Hilbert's different formula states that the different exponent $d(P'|P)$ is then given as

$$d(P'|P) = \sum_{i \geq 0} \left(\mathrm{ord}\ G_i(P'|P) - 1\right).$$

For a subgroup $U \subseteq G$ we denote by E^U the fixed field of U, so E/E^U is Galois with Galois group U. The restriction of P' to E^U is denoted by $P^U := P' \cap E^U$.

An extension E/F is called elementary abelian of degree p^2, if E/F is Galois and $\mathrm{Gal}(E/F)$ is an elementary abelian group of order p^2 (i.e., it is a non-cyclic group of order p^2). We need two lemmas.

Lemma 3.2. *Let E/F be an elementary abelian extension of degree p^2, let P be a place of F and P' a place of E lying over P. Assume that $P'|P$ is totally ramified, i.e. $e(P'|P) = p^2$. Set $G := Gal(E/F)$ and $G_i := G_i(P'|P)$. Suppose that*

$$G = G_0 = G_1 = \cdots = G_a \supsetneq G_{a+1} = 1 \, .$$

Let $U \subseteq G$ be a subgroup of order p. Then it follows that

$$\begin{aligned} d\big(P'|P\big) &= (a+1)\big(p^2-1\big) \qquad \text{and} \\ d\big(P'|P^U\big) &= d\big(P^U|P\big) = (a+1)(p-1) \, . \end{aligned}$$

Moreover, $a \not\equiv 0 \mod p$.

Proof. The equation $d(P'|P) = (a+1)(p^2-1)$ follows immediately from Hilbert's different formula. The i-th ramification group U_i of $P'|P^U$ is by definition equal to the intersection $U \cap G_i(P'|P)$, hence

$$U = U_0 = U_1 = \cdots = U_a \supsetneq U_{a+1} = 1.$$

Again by Hilbert's different formula, we obtain $d(P'|P^U) = (a+1)(p-1)$. By transitivity of the different in $F \subseteq E^U \subseteq E$ we have that $d(P'|P) = d(P'|P^U) + p \cdot d(P^U|P)$, and therefore we get $d(P^U|P) = (a+1)(p-1)$. The assertion that $a \not\equiv 0 \mod p$ follows from the following fact, see [6, Lemma 3.7.7]: If H/F is a cyclic extension of degree p and P is a place of F which is ramified in H, then its different exponent is $d = (k+1)(p-1)$ with $k \not\equiv 0 \mod p$. □

Lemma 3.3. *With notations as in Lemma 3.2, suppose now that*

$$G = G_0 = G_1 = \cdots = G_a \supsetneq G_{a+1} = \cdots = G_b \supsetneq G_{b+1} = 1 \, .$$

Then the following hold:

(1) $d(P'|P) = (a+1)(p^2-1) + (b-a)(p-1)$.

(2) *If $U = G_b$ then $d(P'|P^U) = (b+1)(p-1)$ and $d(P^U|P) = (a+1)(p-1)$.*

(3) *If V is a subgroup of G of order p and $V \neq G_b$, then $d(P'|P^V) = (a+1)(p-1)$ and $d(P^V|P) = (a+1)(p-1) + p^{-1}(b-a)(p-1)$.*

Moreover, $a \not\equiv 0 \mod p$ and $b \equiv a \mod p$.

Proof. The proof can be omitted since it is very similar to the proof of Lemma 3.2. □

Now we can prove the main result of Section 3 (see also [1]).

Theorem 3.4. *Let E_1/F and E_2/F be cyclic extensions of degree $[E_1 : F] = [E_2 : F] = p$ with $E_1 \neq E_2$, and consider their compositum $E := E_1E_2$. Let P be a place of F and P_1 (resp. P_2) a place of E_1 (resp. E_2) over P. Let P' be a place of E lying above P_1 and P_2. Assume that both places $P_1|P$ and $P_2|P$ are totally ramified with different exponents $d(P_1|P) = s_1(p-1)$ and $d(P_2|P) = s_2(p-1)$. Then $s_1 \not\equiv 1 \mod p$, $s_2 \not\equiv 1 \mod p$, and the following hold:*

(1) *If $s_1 < s_2$, then $P'|P_1$ and $P'|P_2$ are totally ramified and their different exponents are $d(P'|P_1) = (p(s_2 - s_1) + s_1)(p-1)$ and $d(P'|P_2) = s_1(p-1)$.*

(2) *If $s_1 = s_2 =: s$, then $e(P'|P_1) = e(P'|P_2) = 1$ or p. The different exponents of $P'|P_1$ and $P'|P_2$ satisfy $d(P'|P_1) = d(P'|P_2) = t(p-1)$ with $0 \leq t \leq s$ and $t \not\equiv 1 \mod p$.*

Proof. The assertions $s_1 \not\equiv 1 \mod p$, $s_2 \not\equiv 1 \mod p$ and $t \not\equiv 1 \mod p$ follow again from [6, Lemma 3.7.7]. The case where $P'|P_1$ (and hence $P'|P_2$) is unramified, is trivial. So we can assume that $e(P'|P_1) = e(P'|P_2) = p$. We are then in the situation of Lemma 3.2 or Lemma 3.3. Denote by $G_i := G_i(P'|P)$ the higher ramification groups of $P'|P$, for all $i \geq 0$. If $G_0 = G_1 = \cdots = G_a$ and $G_{a+1} = 1$, then it follows from Lemma 3.2 that $d(P_i|P) = d(P'|P_i) = (a+1)(p-1)$ for $i = 1, 2$, so Theorem 3.4 holds in this case.

It remains to consider the case

$$G = G_0 = G_1 = \cdots = G_a \supsetneq G_{a+1} = \cdots = G_b \supsetneq G_{b+1} = 1.$$

There are exactly p subgroups $V \subseteq \mathrm{Gal}(E/F)$ of order p which are distinct from G_b. For these subgroups it follows from Lemma 3.3 that $d(P^V|P) = (a+1)(p-1) + p^{-1}(b-a)(p-1)$, and for the subgroup $U := G_b$ we have $d(P^U|P) = (a+1)(p-1)$. If both extensions E_1 and E_2 correspond to subgroups $V \neq G_b$, then we conclude that $s = s_1 = s_2 = a + 1 + p^{-1}(b-a)$ and $d(P'|P_i) = (a+1)(p-1) < s(p-1)$. If however E_1 corresponds to the subgroup $U = G_b$ and E_2 corresponds to a subgroup $V \neq G_b$, then it follows from Lemma 3.3 that $s_1 = a + 1$ and $s_2 = a + 1 + p^{-1}(b-a)$. Now Lemma 3.3 yields $d(P'|P_2) = (a+1)(p-1) = s_1(p-1)$ and $d(P'|P_1) = d(P'|P^U) = (b+1)(p-1) = (s_1 + p(s_2 - s_1))(p-1)$. □

Remark 3.5. Note that Lemma 3.1 is a special case of Theorem 3.4 (namely $s_1 = s_2 = 2$).

Remark 3.6. Suppose that the constant field of F is the finite field $\mathbb{F}_p$ of prime order and P is a place of F of degree one. Then, in the situation of Theorem 3.4 (2), the case $t = s$ cannot occur; i.e., one has $d(P'|P_i) = t(p-1)$ with $0 \leq t < s$. This follows from the fact that the factor groups G_i/G_{i+1} are isomorphic to subgroups of the additive group of the residue class field of P' (which is under our assumptions the additive group of $\mathbb{F}_p$), see [6, Prop. 3.8.5].

Remark 3.7. One can easily construct examples which show that all situations as in Theorem 3.4 can actually occur.

Remark 3.8. After completing this work, we learnt that the result of Theorem 3.4 has also been obtained by Qingquan Wu and Renate Scheidler (private communication).

Acknowledgements. We would like to thank Alp Bassa, Peter Beelen, Arnaldo Garcia and Jörg Wulftange for discussions about parts of this paper.

References

[1] A. Bassa. *Towers of function fields over cubic fields.* PhD Thesis, University of Duisburg-Essen (2007).

[2] A. Bassa, A. Garcia and H. Stichtenoth. *A new tower over cubic finite fields.* Moscow Math. J., **8** (2008), 401–418.

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

[4] H. Hasse. *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper.* J. Reine Angew. Math., **172** (1934), 37–54.

[5] H. Niederreiter and C.P. Xing. *Rational points on curves over finite fields.* London Math. Soc. Lecture Notes Ser., **285** (2001), Cambridge Univ. Press, Cambridge.

[6] H. Stichtenoth. *Algebraic function fields and codes.* 2nd Edition, Graduate Texts in Mathematics, **254** (2009), Springer Verlag.

[7] G.D. Villa Salvador. *Topics in the theory of algebraic function fields.* Birkhäuser Verlag, Boston, Basel, Berlin (2006).

[8] J. Wulftange. *Zahme Türme algebraischer Funktionenkörper.* PhD Thesis, University of Essen (2002).

Nurdagül Anbar,
Henning Stichtenoth
and
Seher Tutdere
Sabancı University, MDBF, Orhanlı
34956 Tuzla, İstanbul
TURKEY

E-mails: nurdagul@su.sabanciuniv.edu /
henning@sabanciuniv.edu /
sehertutdere@su.sabanciuniv.edu