JOURNAL de Théorie des Nombres de BORDEAUX

*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Qingquan WU

**Explicit construction of integral bases of radical function fields**

Tome 22, n° 1 (2010), p. 259-270.

<http://jtnb.cedram.org/item?id=JTNB_2010__22_1_259_0>

*Journal de Théorie des Nombres*
*de Bordeaux* **22** (2010), 259-270

# Explicit construction of integral bases of radical function fields

par Qingquan WU

Résumé. Nous donnons une construction explicite d'une base entière pour le corps de fonction $K = k(t, \rho)$, où $\rho^n = D \in k[t]$, sous l'hypothèse $[K : k(t)] = n$ et $\mathrm{char}(k) \nmid n$. Le discriminant du corps $K$ est également calculé. Nous expliquons pourquoi ces questions sont considérablement plus faciles que dans le cas des corps de nombres. Quelques formules pour les $P$-signatures des corps de fonction radiciels sont également présentées dans ce papier.

Abstract. We give an explicit construction of an integral basis for a radical function field $K = k(t, \rho)$, where $\rho^n = D \in k[t]$, under the assumptions $[K : k(t)] = n$ and $\mathrm{char}(k) \nmid n$. The field discriminant of $K$ is also computed. We explain why these questions are substantially easier than the corresponding ones in number fields. Some formulae for the $P$-signatures of a radical function field are also discussed in this paper.

## 1. Introduction

An important problem in computational number theory is the question of computing an integral basis of a number field or a function field. It is needed for almost every problem involving ideals, for example, computing the ideal class group, the ideal class number, a system of fundamental units, the regulator, etc. Methods for computing an integral basis of an arbitrary field extension, such as the Round 2 algorithm and its variants, are given in [2] and [18], and have been implemented in Magma [1] and KANT [9]. However, it is essential to find a "good" method. Here "good" refers to both efficiency of the method and simplicity of the form of the basis. The general methods in [2] [18] are not efficient even if the extension degree is of modest size.

Nevertheless, efforts in finding integral bases in certain types of number fields have been quite fruitful. For example, there are explicit classifications of integral bases for quadratic, purely cubic, biquadratic and cyclotomic number fields [14]. Integral bases for certain types of quartic number fields were given in [6] and [5]. But when the extension degree is larger than 4,

Manuscrit reçu le 22 octobre 2008.

there are only a few results, and usually they come with strong assumptions, for example, see pp. 270–276, of [19].

In this paper, we construct the integral basis explicitly for any (tame) radical function field; that is, we construct the integral basis for $k(t, \rho)$, where $\rho$ is a fixed root of $Y^n - D$, $D \in k[t]$, and we assume that $Y^n - D$ is irreducible in over $k(t)$ and $\mathrm{char}(k) \nmid n$. It must be emphasized that our result gives explicit formula, hence it should not be compared with other algorithmic approaches of this problem, such as [23] or [25]. Also, our result is on absolute extensions. On the existence (and the computation) of integral bases on relative extensions, see, for example, [12] [15] [10] [11].

Unlike many other results in function field theory, our method is totally original in the sense that it does not come from an adaptation of a technique used in number fields. To our knowledge, Okutsu [17] was the first to establish an algorithm to compute integral bases for radical number fields. His technique, using Newton's diagram, is entirely different from ours. Although it is possible to adapt his method to the function field case, our approach is better in several ways. One is that our method gives a formula instead of an algorithm. By using the formula, we can compute integral bases of radical function fields even if they are given by abstract parameters, hence our method is more basic and more convenient. Another is that our computational complexity is bounded by the squarefree factorization of a polynomial, which is computationally easy to find. Also, the basis we construct is a "diagonal basis with denominators", which is of the simplest form that one can expect. The "diagonal basis with denominators" here means if the integral basis is written in terms of the generators $\{1, \rho, \rho^2, \cdots, \rho^{n-1}\}$, then the transformation matrix is diagonal with non-zero entries in $k(t)$. This result is important both theoretically and computationally in the sense that it is independent of the size of the field extension degree and the size of the constant field. Some formulae for the $P$-signatures of a radical function field are also discussed in this paper.

We give a short introduction for radical function fields and present the main result of this paper in Section 2. Section 3 contains a proof of the main result. In Section 4, for all places $P$ in the rational function field $k(t)$ and all places $P' \mid P$ in the radical function field $K$, a formula is given in Theorem 4.2 on the least common multiple of $f(P'|P)\deg(P)$ and an integer $m$ that is independent of $K$. The formula characterizes the $P$-signature completely when $K/k(t)$ is cyclic Galois, which is true if and only if $m = 1$. An example is also presented there to show that the relative degrees $f(P'|P)$ are not independent of the places $P'$ lying above $P$. As a result, a unified formula for the relative degrees $f(P'|P)$ does not exist.

## 2. Radical function fields

A general introduction to function fields can be found in [22] or [20]. In particular, results about radical function fields can be found in pp. 109-118, of [22].

Let $k$ be a perfect field, $k^*{=}k\backslash\{0\}$, and the characteristic of $k$ is denoted by $\mathrm{char}(k)$. For some fixed element $t$ that is transcendental over $k$, denote by $k[t]$ and $k(t)$ the ring of polynomials and the field of rational functions, respectively, over $k$ in the variable $t$. A *function field* (of one variable) $K$ is an extension of degree $n$ over $k(t)$; here, we require $\mathrm{char}(k)$ to be either 0 or not a divisor of $n$, hence $K/k(t)$ is separable. The *constant field* of $K$ is the set $\{a \in K \mid a \text{ is algebraic over } k\}$. The set of places of $K$ is denoted by $\mathbb{P}_K$. For $P \in \mathbb{P}_K$, denote the corresponding (surjective) discrete valuation for $P$ by $v_P : K \to \mathbb{Z} \cup \{\infty\}$ and the valuation ring by $\mathcal{O}_P$. The *degree* of $P$, denoted by $\deg(P)$, is the field extension degree $[\mathcal{O}_P/P : k_1]$, where $k_1$ is the constant field of $K$. In $k(t)$, every place except for one can be uniquely identified with an irreducible polynomial in $k[t]$; we call these the *finite places* (of $k(t)$), and call the exceptional place the *infinite place* (of $k(t)$) and denote it by $P_\infty$.

The integral closure $\mathcal{O}_K$ of $k[t]$ in $K$ is a ring and a free $k[t]$-module of rank $n$ whose discriminant is referred to as the *discriminant* of $K/k(t)$ and is denoted by $\mathrm{disc}(K)$. Note that $\mathrm{disc}(K)$ is only defined up to squares in $k^*$, hence any results below concerning $\mathrm{disc}(K)$ only hold up to squares in $k^*$. A $k[t]$-basis of $\mathcal{O}_K$ is called an *integral basis* of $K$. For a fixed algebraic closure $\overline{K}$ of $K$, there exist exactly $n$ $k(t)$-embeddings from $K$ into $\overline{K}$; call them $\sigma_i$, $1 \le i \le n$. For $\alpha_1, \ldots \alpha_n \in K$, we define the *discriminant* of $\{\alpha_1, \ldots \alpha_n\}$, denoted by $\mathrm{disc}(\alpha_1, \ldots \alpha_n)$, to be the square of the determinant of the $n \times n$ matrix $(\sigma_i(\alpha_j))_{i,j}$. When $\alpha_i = \alpha^{i-1}$ for some $\alpha \in K$, we simply call $\mathrm{disc}(\alpha_1, \ldots \alpha_n)$ to be $\mathrm{disc}(\alpha)$. Note that $\mathrm{disc}(K) = \mathrm{disc}(\alpha_1, \ldots \alpha_n)$ when $\{\alpha_1, \ldots \alpha_n\}$ is an integral basis of $K$, up to squares in $k^*$. If $K = k(t, \alpha)$, then $\mathrm{disc}(\alpha) = Ind(\alpha)^2 \mathrm{disc}(K)$, where $Ind(\alpha) \in k(t)$ is the *index* of $\alpha$, up to squares in $k^*$.

Let $L$ be a function field containing $K$ with constant field $l$ and $\mathrm{char}(K) \nmid [L : K]$, $P \in \mathbb{P}_K$, $P' \in \mathbb{P}_L$ and $P' \mid P$. From the identity $[\mathcal{O}_{P'}/P' : l][l : k] = [\mathcal{O}_{P'}/P' : \mathcal{O}_P/P][\mathcal{O}_P/P : k]$, we have

$$\deg(P')[l : k] = f(P'|P) \deg(P). \tag{2.1}$$

The tuple of pairs $(e(P'|P), f(P'|P))$ with $P'$ lying over $P$, usually sorted in lexicographical order, is the *$P$-signature* of $L/K$; here, $e(P'|P), f(P'|P)$ denote the *ramification index* and *relative degree* of $P' \mid P$, respectively. $K/k(t)$ is called a *tame* extension if $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) \nmid e(P'|P)$ for any $P \in \mathbb{P}_{k(t)}$ and any $P' \mid P$.

A *radical function field* (of degree $n$) is a function field $K = k(t, \rho)$ where $\rho$ is a fixed root of $Y^n = D$, $D \in k[t]$ and $Y^n - D$ is irreducible over $k(t)$. Without loss of generality, we can assume that $D$ is $n$-th power free; that is, no $Q \in k[t]\backslash k$ exists such that $Q^n | D$. This can be done via the squarefree factorization of polynomials over $k$, which is computationally easy when $\mathrm{char}(k) = 0$ or $k$ is finite. See Algorithm 3.4.2, p. 125, of [3]. Write

$$D = \mathrm{sgn}(D) \prod_{i=1}^{n-1} G_i^i, \tag{2.2}$$

where $\mathrm{sgn}(D) \in k^*$, $G_i \in k[t]$ are monic, squarefree and pairwise coprime, for $1 \le i \le n-1$. The crucial fact we shall need on radical extensions is the following

$$e(P'|P) = \frac{n}{\gcd(n, v_P(D))} \tag{2.3}$$

Note that (2.3) is independent of $P'$, henceforth $e(P'|P)$ will be denoted by $e(P)$. It is clear by (2.3) that $K/k(t)$ is tame, under the assumption that $\mathrm{char}(k) \nmid n$.

The curve $Y^n - D = 0$ defining $K/k(t)$ is nonsingular if and only if $D$ is squarefree. In this case, an integral basis of $K$ is just $\{1, \rho, \rho^2, \ldots, \rho^{n-1}\}$ and $\mathrm{disc}(K) = (-1)^{(n-1)(n+2)/2} n^n D^{n-1}$. So we need to work out the case of non-squarefree $D$.

Although Theorem 2.1 below seems complicated at first glance, it is exceptionally suitable for computation. In fact, if the squarefree factorization of $D$ is known, the remaining job to complete the integral basis computation can be done by hand. Also note that our result is independent of $n = [K : k(t)]$ and the size of the constant field of $K$. Recall that $\lfloor r \rfloor$ and $\lceil r \rceil$ denote the floor and ceiling, respectively, of $r \in \mathbb{R}$, i.e. $\lfloor r \rfloor$ is the maximal integer not exceeding $r$, and $\lceil r \rceil$ is the minimal integer no less than $r$.

Now we give our main result:

**Theorem 2.1.** *Let $k$ be a perfect field, $K = k(t, \rho)$ a radical function field, where $\rho^n = D \in k[t]$, $\mathrm{char}(k) \nmid n$, and $G_i$ given by (2.2). Then an integral basis of $K$ is given by $\{1, \dfrac{\rho}{D_1}, \dfrac{\rho^2}{D_2}, \dfrac{\rho^3}{D_3}, \ldots, \dfrac{\rho^{n-1}}{D_{n-1}}\}$, where*

$$\begin{aligned} D_m = {} & G_{\lceil \frac{n}{m} \rceil} G_{\lceil \frac{n}{m} \rceil + 1} \cdots G_{\lceil \frac{2n}{m} \rceil - 1} G^2_{\lceil \frac{2n}{m} \rceil} \cdots \\ & \cdots G^2_{\lceil \frac{3n}{m} \rceil - 1} G^3_{\lceil \frac{3n}{m} \rceil} \cdots G^{m-1}_{\lceil \frac{(m-1)n}{m} \rceil} \cdots G^{m-1}_{n-1}, \end{aligned} \tag{2.4}$$

*for $1 \le m \le n-1$. In particular, we have $D_1 = 1$, $D_1 \mid D_2 \mid \ldots \mid D_{n-1}$, and $\prod_{i=1}^{n-1} D_i = Ind(\rho)$, the index of $\rho$.*

We give an example to illustrate how to compute $D_m$ from $n, m$.

**Example.** Assume that $n = 12, m = 5$, then $\lceil \frac{n}{m} \rceil = 3, \lceil \frac{2n}{m} \rceil = 5, \lceil \frac{3n}{m} \rceil = 8, \lceil \frac{4n}{m} \rceil = 10$. These numbers determine the subscript $i$ where the exponent of $G_i$ increases by one. The first increment in the exponent (from 0 to 1) occurs at $\lceil \frac{n}{m} \rceil = 3$, the second increment (from 1 to 2) occurs at $\lceil \frac{2n}{m} \rceil = 5$, the third one at $\lceil \frac{3n}{m} \rceil = 8$, and the fourth and last one at $\lceil \frac{4n}{m} \rceil = 10$. Hence $D_5 = G_3 G_4 G_5^2 G_6^2 G_7^2 G_8^3 G_9^3 G_{10}^4 G_{11}^4$.

## 3. A proof of Theorem 2.1

We follow the notation of Theorem 2.1. For non-zero $F \in k[t]$ and $G \in k[t] \setminus k$, $v_G(F)$ is the exact power of $G$ that divides $F$. This coincides with the discrete valuation $v_P(D)$ when $G = P$ is irreducible and corresponds to a place in $k(t)$.

We claim that Theorem 2.1 follows from the following two lemmas:

**Lemma 3.1.** *Let $k$ be a perfect field, $K = k(t, \rho)$ a radical function field, where $\rho^n = D \in k[t]$, $char(k) \nmid n$, and $G_i, D_i$ given by (2.2) and (2.4). Then $\dfrac{\rho^j}{D_j} \in \mathcal{O}_K$ for any $j \in [1, n-1]$,*

*Proof.* For any fixed $j \in [1, n-1]$, let us simply verify $(\rho^j/D_j)^n \in k[t]$. We have $(\rho^j/D_j)^n = D^j/D_j^n = \operatorname{sgn}(D)^j \prod_{i=1}^{n-1} G_i^{ij}/D_j^n$, and we know that $D_j$ is a product of certain $G_i$, hence it suffices to show

$$v_{G_i}(D_j^n) = n\, v_{G_i}(D_j) \le ij, \text{ for all } i \in [1, n-1] \text{ such that } G_i \ne 1. \tag{3.1}$$

For fixed $i$ such that $G_i \ne 1$, there exists a unique integer $l \in [0, j-1]$, such that $\lceil ln/j \rceil \le i < \lceil (l+1)n/j \rceil$. Then $v_{G_i}(D_j) = l$ by (2.4). Hence $v_{G_i}(D_j^n) = ln$ and $ln/j \le \lceil ln/j \rceil \le i$, so (3.1) is proved. □

**Lemma 3.2.** *Let $k$ be a perfect field, $K = k(t, \rho)$ a radical function field, where $\rho^n = D \in k[t]$, $char(k) \nmid n$, and $G_i, D_i$ given by (2.2) and (2.4). Then $disc(K) = disc(1, \dfrac{\rho}{D_1}, \dfrac{\rho^2}{D_2}, \ldots, \dfrac{\rho^{n-1}}{D_{n-1}})$, up to squares in $k^*$.*

Note that Lemma 3.1 implies $\rho^j/D_j$ is integral over $k[t]$ for $j \in [1, n-1]$ and Lemma 3.2 implies that $\operatorname{disc}(1, \rho/D_1, \rho^2/D_2, \ldots, \rho^{n-1}/D_{n-1})$ is exactly $\operatorname{disc}(K)$, up to a constant square. By a simple linear algebra argument, we know $\{1, \rho/D_1, \rho^2/D_2, \ldots, \rho^{n-1}/D_{n-1}\}$ is an integral basis of $K$. Hence it suffices to prove Lemma 3.2.

Recall that for all tamely ramified finite places $P$, we have $v_P(\operatorname{disc}(K)) = \sum_{P'|P} (e(P)-1) f(P'|P)$, where the sum is over all $P' \mid P$. First, we compute $\operatorname{disc}(K)$:

**Theorem 3.1.** *Let $k$ be a perfect field, $K = k(t, \rho)$ a radical function field, where $\rho^n = D \in k[t]$, $char(k) \nmid n$, and $G_i, D_i$ given by (2.2) and (2.4). Then*

$disc(K) = (-1)^{(n-1)(n+2)/2} n^n (\mathrm{sgn}(D))^{n-1} \prod_{i=1}^{n-1} G_i^{n-\gcd(n,i)}$, *up to squares in* $k^*$.

*Proof.* Let $P \in \mathbb{P}_{k(t)}$ be any finite place and $P' \in \mathbb{P}_K$ lying above $P$. Since $\mathrm{char}(k) \nmid n$, $K/k(t)$ is tame so $v_P(\mathrm{disc}(K)) = \sum_{P'|P}(e(P)-1)f(P'|P)$, where the sum is over all $P' \mid P$. Hence by (2.3), we have

$$\begin{aligned} v_P(\mathrm{disc}(K)) &= \sum (e(P)-1)f(P'|P) \\ &= \sum e(P)f(P'|P) - (\sum e(P)f(P'|P))/e(P) \\ &= n - n/e(P) = n - \gcd(n, v_P(D)), \end{aligned}$$

where all summations are taken over all places $P' \in \mathbb{P}_K$ lying above $P$.

By (2.2), if $P \mid G_i$ for some $i$, then $v_P(D) = i$. So

$$v_P(\mathrm{disc}(K)) = n - \gcd(n,i), \text{ for } P \mid G_i. \tag{3.2}$$

If $P_1$, $P_2$ are two irreducible divisors of $G_i$, we have $v_{P_1}(\mathrm{disc}(K)) = v_{P_2}(\mathrm{disc}(K))$ by (3.2). Hence for any $G_i \neq 1$, we have $v_{G_i}(\mathrm{disc}(K)) = n - \gcd(n,i)$. Theorem 3.1 follows, since $\mathrm{disc}(\rho) = (-1)^{(n-1)(n+2)/2} n^n D^{n-1}$ and $\mathrm{sgn}(\mathrm{disc}(\rho)) = \mathrm{sgn}(\mathrm{disc}(K))$, up to squares in $k^*$. □

To prove Lemma 3.2, it suffices to show that for any $i \in [1, n-1]$ such that $G_i \neq 1$, we have

$$v_{G_i}(\mathrm{disc}(1, \frac{\rho}{D_1}, \frac{\rho^2}{D_2}, \ldots, \frac{\rho^{n-1}}{D_{n-1}})) = n - \gcd(n,i). \tag{3.3}$$

Indeed, up to squares in $k^*$, we have

$$Ind(\rho)^2 \mathrm{disc}(K) = \mathrm{disc}(\rho) = \mathrm{disc}(1, \frac{\rho}{D_1}, \frac{\rho^2}{D_2}, \ldots, \frac{\rho^{n-1}}{D_{n-1}}) \prod_{i=1}^{n-1} D_i^2.$$

If (3.3) is true, then $\mathrm{disc}(1, \rho/D_1, \rho^2/D_2, \ldots, \rho^{n-1}/D_{n-1})$ and $\mathrm{disc}(K)$ differ by a square in $k^*$. This also proves $Ind(\rho) = \prod_{i=1}^{n-1} D_i$, up to squares in $k^*$. Hence it suffices to show (3.3) to prove Lemma 3.2 and hence Theorem 2.1. We have

**Lemma 3.3.** *Let $k$ be a perfect field, $K = k(t, \rho)$ a radical function field, where $\rho^n = D \in k[t]$, $char(k) \nmid n$, and $G_i, D_i$ given by (2.2) and (2.4). Then for any $1 \leq i \leq n-1$ such that $G_i \neq 1$, we have*

$$v_{G_i}(disc(1, \frac{\rho}{D_1}, \frac{\rho^2}{D_2}, \ldots, \frac{\rho^{n-1}}{D_{n-1}})) = i(n-1) - 2\sum_{j=1}^{n-1} \lfloor \frac{ij}{n} \rfloor .$$

*Proof.* Fix any $1 \le i \le n-1$ such that $G_i \neq 1$. By direct computation, we have

$$v_{G_i}(\mathrm{disc}(1, \frac{\rho}{D_1}, \frac{\rho^2}{D_2}, \ldots, \frac{\rho^{n-1}}{D_{n-1}})) = v_{G_i}(\mathrm{disc}(\rho)) - 2\, v_{G_i}(\prod_{j=1}^{n-1} D_j)$$
$$= i(n-1) - 2\sum_{j=1}^{n-1} v_{G_i}(D_j)\ .$$

Now let us compute $\sum_{j=1}^{n-1} v_{G_i}(D_j)$. For any fixed $j \in [1, n-1]$, there exists a unique integer $l \in [0, i-1]$ such that $\lceil ln/i \rceil \le j < \lceil (l+1)n/i \rceil$. Then $ln/i \le j < (l+1)n/i$ since $j$ is an integer. So $ln/j \le i < (l+1)n/j$, hence $\lceil ln/j \rceil \le i < \lceil (l+1)n/j \rceil$ since $i$ is an integer. Thus $v_{G_i}(D_j) = l$ by (2.4). But $ij/n - 1 < l \le ij/n$ implies $\lfloor ij/n \rfloor = l = v_{G_i}(D_j)$. □

We give the following mathematical identity to conclude (3.3), Lemma 3.2 and hence Theorem 2.1:

**Proposition 3.1.** *For any positive integers $i$ and $n$,*

$$2\sum_{j=1}^{n-1} \lfloor \frac{ij}{n} \rfloor = in - i - n + \gcd(n, i).$$

*Proof.* For any $r \in \mathbb{R}$, we have

$$\lfloor -r \rfloor = \begin{cases} -\lfloor r \rfloor & \text{if } r \text{ is an integer,} \\ -\lfloor r \rfloor - 1 & \text{if } r \text{ is not an integer.} \end{cases}$$

It follows that

$$\sum_{j=1}^{n-1} \left\lfloor \frac{-ij}{n} \right\rfloor = -\sum_{j=1}^{n-1} \left\lfloor \frac{ij}{n} \right\rfloor - n + \gcd(i, n), \tag{3.4}$$

where the equality is obtained by checking how many times $\dfrac{ij}{n}$ is an integer for $1 \le j \le n-1$.

By (3.4), it is easy to see

$$2\sum_{j=1}^{n-1} \left\lfloor \frac{ij}{n} \right\rfloor = \sum_{j=1}^{n-1} \left\lfloor \frac{ij}{n} \right\rfloor + \sum_{j=1}^{n-1} \left\lfloor \frac{i(n-j)}{n} \right\rfloor$$
$$= \sum_{j=1}^{n-1} \left\lfloor \frac{ij}{n} \right\rfloor + i(n-1) + \sum_{j=1}^{n-1} \left\lfloor \frac{-ij}{n} \right\rfloor$$
$$= in - i - n + \gcd(i, n),$$

where we use the fact that $\lfloor c + r \rfloor = c + \lfloor r \rfloor$ if $c \in \mathbb{Z}$ in the second equality. □

**Remark.** The proof is essentially due to the same idea−used by Gauss as a little boy−to sum up the numbers from 1 through 100. Also, there exists a geometric proof of Proposition 3.1. Let $T$ be the triangle with vertices $(0,0),(n,0)$ and $(n,i)$. Then it is not hard to see that the summation of the number of integer points in and on $T$ is given by $\sum_{j=0}^{n}(\lfloor ij/n \rfloor + 1)$. Then one can apply Pick's Theorem and our result follows.

Finally, we want to reemphasize that our method does not come from an adaptation of a technique used in number fields, neither can it be directly adapted to number fields. Note that there is no analogue of the formal derivative in $\mathbb{Z}$, hence Algorithm 3.4.2, p. 125, of [3], is not applicable to compute the squarefree factorizations of integers. In fact, the squarefree factorization of (large) integers is computationally hard to find. Even if we had a squarefree integer $a \in \mathbb{Z}$, the method we present in Theorem 2.1 is still not adaptable to the number field $\mathbb{Q}(\sqrt[n]{a})$. The easiest example to see that the analogous result to Theorem 2.1 does not hold in the number field case is $\mathbb{Q}(\sqrt{a})$ with a squarefree integer $a \equiv 1 \pmod 4$. This is because we can ignore the $n^n$ part in the expression of $\mathrm{disc}(\rho)$ in function fields since it is a unit; whereas in the number field case, this large factor cannot be disregarded for the discriminant computation.

## 4. Signature of a radical function field

Throughout this section, we assume that $k = \mathbb{F}_q$ is a finite field, and $K = \mathbb{F}_q(t,\rho)$ is a radical function field of (full) constant field $\mathbb{F}_q$, where $\rho$ is a fixed root of $f(Y) = Y^n - D = 0$ and $\gcd(n,q) = 1$. Note that if $D = \mathrm{sgn}(D)\prod_{i=1}^{n-1} G_i^i$ is the squarefree factorization of $D$, then $\mathbb{F}_q$ is the (full) constant field of $K$ if $G_i \neq 1$ for any $i$ such that $\gcd(i,n) = 1$, by Eisenstein's Criterion.

We will study how the infinite place $P_\infty$ splits in $K/\mathbb{F}_q(t)$, i.e. we want to find the ramification index $e(P'|P_\infty)$ and relative degree $f(P'|P_\infty)$ for every $P' \in \mathbb{P}_K$ lying above $P_\infty$. The work goes back to Hecke [4]. Other literature on this topic include [13], [24], and [16] .

The ramification index is easy by (2.3), hence it remains to find $f(P'|P_\infty)$. To that end, we apply Kummer theory. Note that Kummer theory requires an assumption on primitive $l$-th root of unity, which we shall discuss briefly next.

Recall that a *primitive $l$-th root of unity* in a field $F$ is an element $\zeta_l \in F$ such that $\zeta_l^l = 1$ and $\zeta_l^i \neq 1$ for any $i < l$. For a finite field $\mathbb{F}_q$, we know $\zeta_l \in \overline{\mathbb{F}_q}$ if and only if $\gcd(l,q) = 1$ and $\zeta_l \in \mathbb{F}_q$ if and only if $l \mid (q-1)$. It follows that the minimal extension field of $\mathbb{F}_q$ containing $\zeta_l$ is $\mathbb{F}_{q^m}$, where $\gcd(l,q) = 1$ and $m = \mathrm{ord}_l(q)$ is the order of $q$ modulo $l$, i.e. $m = \min\{j \geq 1 \mid q^j \equiv 1 \pmod l\}$. Next, we present a useful result:

**Lemma 4.1.** *Let $F$ be a field containing a primitive $l$-th root of unity for some $l \in \mathbb{N}$, and $u \in F$ an element satisfying*

$$u \neq w^d \text{ for all } w \in F \text{ and } d \mid l,\ d > 1.$$

*Then the polynomial $Y^l - u$ is irreducible over $F$.*

*Proof.* When $F$ is a function field, Lemma 4.1 is presented as Proposition III.7.3, part(a), pp. 110f, of [22]. A complete proof of Lemma 4.1 can be found in the proof of Theorem 7.11, pp. 295f, of [7]. □

Now we proceed to compute $f(P'|P_\infty)$.

**Theorem 4.1.** *Let $\mathbb{F}_q$ be a finite field, $K = \mathbb{F}_q(t, \rho)$ a radical function field of full constant field $\mathbb{F}_q$, where $\rho$ is a fixed root of $Y^n - D = 0$ such that $\gcd(n, q) = 1$. If $P' \in \mathbb{P}_K$ lies over $P_\infty \in \mathbb{P}_{k(t)}$, then $e(P'|P_\infty) = \frac{n}{d}$, $lcm(f(P'|P_\infty), m) = m\frac{d}{r}$, where $d = \gcd(n, \deg(D))$, $m = ord_n(q)$, $r = \max\{j \in \mathbb{N} \mid j|d, \operatorname{sgn}(D) = a^j \text{ for some } a \in \mathbb{F}_q^*\}$. In particular, when $K/\mathbb{F}_q(t)$ is (cyclic) Galois, we have $f(P'|P_\infty) = d/r$.*

*Proof.* The result for $e(P'|P_\infty)$ is simply a restatement of (2.3). We first establish that $r$ is well-defined. In fact, let $\mathcal{S} = \{j \in \mathbb{N} \mid j|d, \operatorname{sgn}(D) = a^j \text{ for some } a \in \mathbb{F}_q^*\}$. Then $1 \in \mathcal{S}$ and every element of $\mathcal{S}$ is a divisor of $d$. Hence the maximum of $\mathcal{S}$ exists.

For our radical function field $K$, we have that $\zeta_n \in \mathbb{F}_q$ if and only if $K/\mathbb{F}_q(t)$ is (cyclic) Galois. This is easy to see since all roots of $f(Y)$ are of the form $\rho\zeta_n^i$ for $0 \leq i \leq n-1$. We know $m = \operatorname{ord}_n(q) = [\mathbb{F}_q(\zeta_n) : \mathbb{F}_q]$, hence $\mathbb{F}_q(\zeta_n) = \mathbb{F}_{q^m}$. Consider the four field extensions $K(\zeta_n)/K$, $\mathbb{F}_q(\zeta_n, t)/\mathbb{F}_q(t)$, $K(\zeta_n)/\mathbb{F}_q(\zeta_n, t)$ and $K/\mathbb{F}_q(t)$. The first two are constant field extensions, $K(\zeta_n)/\mathbb{F}_q(\zeta_n, t)$ is cyclic of degree $n$, and the extension $K/\mathbb{F}_q(t)$ is the one we are interested in. Let $\hat{P} \in \mathbb{P}_{\mathbb{F}_q(\zeta_n,t)}$ lie over $P_\infty$ and $P'' \in \mathbb{P}_{K(\zeta_n)}$ lie over $P'$. For the places $P_\infty, P', \hat{P}, P''$, let their valuation rings be $\mathcal{O}_{P_\infty}, \mathcal{O}_{P'}, \mathcal{O}_{\hat{P}}$, $\mathcal{O}_{P''}$, respectively. Our goal is to find $f(P'|P_\infty)$. Note that $f(P'|P_\infty)$ $f(P''|P') = f(P''|P_\infty) = f(P''|\hat{P})f(\hat{P}|P_\infty)$. So we compute the relative degrees $f(\hat{P}|P_\infty)$, $f(P''|P')$, and $f(P''|\hat{P})$, thus obtaining our desired degree $f(P'|P_\infty)$.

We first determine $f(\hat{P}|P_\infty)$ by studying the extension $\mathbb{F}_q(\zeta_n, t)/\mathbb{F}_q(t)$, which is a constant field extension of extension degree $m$. Thus the constant field of $\mathbb{F}_q(\zeta_n, t)$ is $\mathbb{F}_{q^m}$. By Theorem III.6.3, p. 103, of [22], applying to $\hat{P} \mid P_\infty$, we know $\mathcal{O}_{\hat{P}}/\hat{P} = (\mathcal{O}_{P_\infty}/P_\infty)\,\mathbb{F}_q(\zeta_n) = \mathbb{F}_q\mathbb{F}_{q^m} = \mathbb{F}_{q^m}$, hence

$$\deg(\hat{P}) = [\mathcal{O}_{\hat{P}}/\hat{P} : \mathbb{F}_{q^m}] = 1. \tag{4.1}$$

Applying (2.1) to $\hat{P} \mid P_\infty$, we have

$$\deg(\hat{P})\,[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = f(\hat{P}|P_\infty)\deg(P_\infty),$$

hence (4.1) yields

$$f(\hat{P}|P_\infty) = [\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = m. \tag{4.2}$$

Similarly, by applying (2.1) to $P' \mid P_\infty$, we have

$$\deg(P') = f(P'|P_\infty)\deg(P_\infty) = f(P'|P_\infty). \tag{4.3}$$

Next, consider the constant field extension $K(\zeta_n)/K$ of extension degree $m$. Similarly, by Theorem III.6.3, p. 103, of [22], applying to $P''/P'$, we have $\mathcal{O}_{P''}/P'' = (\mathcal{O}_{P'}/P')\,\mathbb{F}_q(\zeta_n) = \mathbb{F}_{q^{\deg(P')}}\mathbb{F}_{q^m}$, hence

$$\deg(P'') = [\mathcal{O}_{P''}/P'' : \mathbb{F}_{q^m}] = \frac{\operatorname{lcm}(\deg(P'),\, m)}{m}. \tag{4.4}$$

Consider the function field extension $K(\zeta_n)/\mathbb{F}_q(t)$ now. Applying (2.1) to $P'' \mid P_\infty$ yields that $\deg(P'')\, m = f(P''|P_\infty)\deg(P_\infty)$, hence

$$f(P''|P_\infty) = \deg(P'')\, m. \tag{4.5}$$

Now (4.3), (4.4) and (4.5) imply

$$f(P''|P_\infty) = \operatorname{lcm}(f(P'|P_\infty),\, m). \tag{4.6}$$

Note that $f(P''|P_\infty) = f(P''|\hat{P})f(\hat{P}|P_\infty)$, hence (4.2) and (4.6) imply

$$\operatorname{lcm}(f(P'|P_\infty),\, m) = f(P''|\hat{P})\, m. \tag{4.7}$$

It remains to show $f(P''|\hat{P}) = d/r$. Consider the cyclic Galois extension $K(\zeta_n)/\mathbb{F}_q(\zeta_n, t)$. We know $e(P''|\hat{P}) = n/d$ by (2.3). Let $\theta = \rho^{n/d}$ and $F = \mathbb{F}_q(\zeta_n, t)(\theta)$, then $F$ is an intermediate field extension of $K(\zeta_n)/\mathbb{F}_q(\zeta_n, t)$. Let $P_F \in \mathbb{P}_F$ lie over $\hat{P}$, then $P_F$ is totally ramified in $K(\zeta_n)/F$ by applying Proposition III.7.3, p. 110, of [22], to the minimal polynomial $Y^{n/d} - \theta$ of $\rho$ over $F$. Note that $Z^d - D$, the minimal polynomial of $\theta$ over $\mathbb{F}_q(\zeta_n, t)$, is not integral over $\hat{P}$. Let $E = D\, t^{-\deg(D)}$ and $\eta = \theta\, t^{-\deg(D)/d}$, then the minimal polynomial of $\eta$ over $\mathbb{F}_q(\zeta_n, t)$ is $g(Z) = Z^d - E$, which is integral over $\hat{P}$.

Now we apply Kummer theory to the field extension $F/\mathbb{F}_q(\zeta_n, t)$ and the place $P_F \mid \hat{P}$. Let $a \in \mathbb{F}_q^*$ be an $r$-th root of $\operatorname{sgn}(D)$, i.e. $a^r = \operatorname{sgn}(D)$, and $\zeta_r = \zeta_n^{n/r}$ a primitive $r$-th root of unity. It is easy to see that $g(Z) \equiv \prod_{i=1}^{r}(Z^{d/r} - \zeta_r^i a) \pmod{\hat{P}}$. Since $\mathbb{F}_q(\zeta_n, t)/\mathbb{F}_q(t)$ is unramified, a prime element of $P_\infty$ is also a prime element of $\hat{P}$. It follows that $g(Z) \pmod{\hat{P}}$ is the same as $g(Z) \pmod{P_\infty}$. By the definition of $r$, we know that $Z^{d/r} - \zeta_r^i a$ is irreducible modulo $P_\infty$ for all $i$, by Lemma 4.1. By Kummer's Theorem (Theorem III.3.7, p. 76, of [22]), we know $f(P''|\hat{P}) = d/r$. Our result follows from (4.7). □

When $D$ is monic, then $r = d$ is maximal and Theorem 4.1 implies that $\operatorname{lcm}(f(P'|P_\infty), m) = m$, hence $f(P'|P_\infty) \mid m$ in particular. When $K/\mathbb{F}_q(t)$ is (cyclic) Galois, which is equivalent to $m = 1$, we have complete results on the signature. This decides the *decomposition field* (group, resp.) and *inertia field* (group, resp.) of $P_\infty$ over $K/k(t)$ uniquely, since $K/\mathbb{F}_q(t)$ is cyclic.

We point out that there exists no unified formula for $f(P'|P_\infty)$ in general. In fact, $f(P'|P_\infty)$ is not independent of $P'$. The easiest example to see this fact is a purely cubic function field. Set $n = 3$, $\operatorname{sgn}(D) = 1$, $q \equiv -1 \pmod 3$, then $f(P_1'|P_\infty) = 1$, $f(P_2'|P_\infty) = 2$, where $P_1', P_2' \in \mathbb{P}_K$ are the two infinite places lying above $P_\infty$. For more detail, see Theorem 2.1, of [21].

Theorem 4.1 can be easily generalized to all finite places $P$. We have the following

**Theorem 4.2.** *Let $\mathbb{F}_q$ be a finite field, $K = \mathbb{F}_q(t, \rho)$ a radical function field of full constant field $\mathbb{F}_q$, where $\rho$ is a fixed root of $Y^n - D = 0$ such that $\gcd(n, q) = 1$. If $P' \in \mathbb{P}_K$ lies over $P \in \mathbb{P}_{k(t)} \setminus P_\infty$, then $e(P'|P) = \frac{n}{d}$, $lcm(f(P'|P)\deg(P), l) = lcm(\deg(P), l)\frac{d}{r}$, where $d = \gcd(n, v_P(D))$, $l = ord_n(q)$, $r = \max\{m \in \mathbb{N} \mid m|d, \frac{D}{P^{v_P(D)}} = a^m$ for some $a \in \mathbb{F}_{q^{\deg(P)}}^*\}$. In particular, when $K/\mathbb{F}_q(t)$ is cyclic Galois, we have $f(P'|P) = d/r$.*

Finally, to find $r$, it suffices to analyze whether an element $a \in \mathbb{F}_q^*$ is an $m$-th power. This is well-known, see Proposition 4.2.1, p. 45, of [8].

## Acknowledgements

I thank Renate Scheidler for bringing this topic into my attention, reading the first a few versions of the paper and many constructive discussions, Kevin Ford for his simplification of the proof of Proposition 3.1, Han Duong and Bruce Rezmick for pointing out a geometric proof of Proposition 3.1, as well as Mark Bauer and the anonymous referee for their useful comments. A special word of thanks is due to CiSaC at University of Calgary for facilitating my research.

## References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language.* J. Symb. Comp. **24** (1997), 235–265.

[2] J. A. Buchmann and H. W. Lenstra Jr., *Approximating rings of integers in number fields.* J. Theor. Nombres Bordeaux **6** (1994), 221–260.

[3] H. Cohen, *A course in computational algebraic number theory.* Springer-Verlag, 1993.

[4] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen.* Akademische Verlagsgesellschaft, 1954.

[5] J. G. Huard, B. K. Spearman, and K. S. Williams, *Integral bases for quartic fields with quadratic subfields.* J. Number Theory **51** (1995), 103–117.

[6] R. H. Hudson and K. S. Williams, *The integers of a cyclic quartic field*. Rocky Mountain J. Math. **20** (1990), 145–150.
[7] T. W. Hungerford, *Algebra*. Springer-Verlag, 1974.
[8] K. F. Ireland and M. Rosen, *A classical introduction to modern number theory*. Springer-Verlag, 1990.
[9] KANT/KASH, *Computational Algebraic Number Theory/KAnt SHell*. http://www.math.tu-berlin.de/∼kant/kash.
[10] E. Lamprecht, *Verzweigungsordnungen, Differenten und Ganzheitsbasen bei Radikalerweiterungen. I.* Arch. Math. **56** (1991), 569–585.
[11] E. Lamprecht, *Existence of and computation of integral bases*. Acta Math. Inform. Univ. Ostrav. **6** (1998), 121–128.
[12] H. B. Mann, *On integral basis*. Proc. Amer. Math. Soc. **9** (1958), 167–172.
[13] H. B. Mann and W. Y. Vélez, *Prime ideal decomposition in* $F(\sqrt[m]{\mu})$. Monatsh. Math. **81** (1976), 131–139.
[14] D. Marcus, *Number Fields*. Springer-Verlag, 1977.
[15] L. R. McCulloh, *Integral bases in Kummer extensions of Dedekind fields*. Canad. J. Math. **15** (1963), 755–765.
[16] M. J. Norris and W. Y. Vélez, *Structure theorems for radical extensions of fields*. Acta Arith. **38** (1980/81), 111–115.
[17] K. Okutsu, *Integral basis of the field* $\mathbb{Q}(\sqrt[n]{a})$. Proc. of Japan Acad. Ser. A Math. Sci. **58** (1982), 219–222.
[18] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*. Cambridge University Press, 1997.
[19] P. Ribenboim, *Algebraic numbers*. John-Wiley & Sons. Inc., 1972.
[20] M. Rosen, *Number theory in function fields*. Springer-Verlag, 2002.
[21] R. Scheidler and A. Stein, *Voronoi's algorithm in purely cubic congruence function fields of unit rank 1*. Math. Comp. **69** (2000), 1245–1266.
[22] H. Stichtenoth, *Algebraic function fields and codes*. Springer-Verlag, 1993.
[23] M. van Hoeij, *An algorithm for computing an integral basis in an algebraic function field*. J. Symb. Comp. **18** (1994), 353–363.
[24] W. Y. Vélez, *Prime ideal decomposition in* $F(\mu^{1/p})$. Pacific J. Math. **75** (1978), 589–600.
[25] P. G. Walsh, *A polynomial-time complexity bound for the computation of the singular part of a Puiseux expansion of an algebraic function*. Math. Comp. **69** (2000), 1167–1182.

Qingquan Wu
Department of Mathematics and Statistics
University of Calgary
2500 University Drive NW
Calgary, Alberta T2N 1N4
*E-mail*: quwu@ucalgary.ca