Revista Colombiana de Matemáticas
Volumen XXVIII (1993), págs. 213-222

ON DIHEDRAL ALGEBRAIC FUNCTION FIELDS*

WILSON ZÚÑIGA

§1. INTRODUCTION

The purpose of this note is to present some results on the arithmetic of dihedral algebraic function fields. A dihedral algebraic function field will be an extension $N/\mathbb{F}_q$ of $\mathbb{F}_q(X)/\mathbb{F}_q$, whose Galois group $G =$ Gal $(N/\mathbb{F}_q(X)$ is the dihedral group $D_{2\ell}$, $\ell \neq 2, p$, where p is the characteristic of $\mathbb{F}_q(X)$ and ℓ is a prime number. We will especifically present results on ramification of prime divisors of $\mathbb{F}_q(X)/\mathbb{F}_q$ in $N/\mathbb{F}_q$, discriminant, genus, relations among the zeta function of such extension and the zeta functions of some of its subextensions, and similar relations for zero-degree prime divisor class number and ideal class number.

Using the well-known presentation of $D_{2\ell}$

$$D_{2\ell} =< \sigma, \tau \ : \ \sigma^{\ell} = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} > ,$$

it is an easy matter to show that all non-trivial subgroups of $D_{2\ell}$ are $H_j =$ $< \tau\sigma^j >$, $j = 0, 1, \cdots \ell - 1$, $H =< \sigma >$; H is the unique normal subgroup of $D_{2\ell}$ and the subgroups H_j are conjugates by pairs. Let $L = K(H)$ and $L_j = K(H_j)$, $j = 0, 1, \cdots, \ell - 1$, be the corresponding intermediate fields in $N/\mathbb{F}_q(X)$, so that, by Galois theory fundamental theorem, the extensions N/L, $L/\mathbb{F}_q(X)$ and N/L_j, $j = 0, 1, \ldots, \ell - 1$, are Galois extensions, while $L_j/\mathbb{F}_q(X)$ are not. The subfields L_j, $j = 0, 1, \cdots, \ell - 1$, are conjugated by pairs.

§2. MAIN RESULTS

The following three theorems will be proved here:

Theorem 1. *Let $N/\mathbb{F}_q$ be a dihedral algebraic function field of characteristic $p \neq 2, \ell$. Then the prime divisors of $\mathbb{F}_q(X)/\mathbb{F}_q$ can be divided in six disjoint classes according to their decompositions in the extensions $L/\mathbb{F}_q(X)$, $L_0/\mathbb{F}_q(X)$, $N/\mathbb{F}_q(X)$, as shown in Table 1.*

This work is based on the author's Master Thesis, submitted at the Universidad de los Andes, Santafé de Bogotá .

TABLE 1

Class	$L/\mathbb{F}_q(X)$	e	d	r	$L_0/\mathbb{F}_q(X)$	e	d	r	$N/\mathbb{F}_q(X)$	e	d	r
C_1	$\mathfrak{G}^2$	2	1	1	$\mathfrak{G}'_1\cdots\mathfrak{G}'_{\frac{\ell+1}{2}}$	$e_1=1$, $e_i=2$, $i\neq 1$	1	$\frac{\ell+1}{2}$	$\mathfrak{P}_1^2\cdots\mathfrak{P}_\ell^2$	2	1	ℓ
C_2	$\mathfrak{G}$	1	2	1	$\mathfrak{G}'^{\ell}$	ℓ	1	1	$\mathfrak{P}^{\ell}$	ℓ	2	1
C_3	$\mathfrak{G}_1\mathfrak{G}_2$	1	1	2	$\mathfrak{G}'^{\ell}$	ℓ	1	1	$\mathfrak{P}_1^{\ell}\mathfrak{P}_2^{\ell}$	ℓ	1	2
C_4	$\mathfrak{G}$	1	2	1	$\mathfrak{G}'_1\cdots\mathfrak{G}'_{\frac{\ell+1}{2}}$	1	$d_1=1$ $d_i=2$, $i\neq 1$	$\frac{\ell+1}{2}$	$\mathfrak{P}_1\cdots\mathfrak{P}_\ell$	1	2	ℓ
C_5	$\mathfrak{G}_1\mathfrak{G}_2$	1	1	2	$\mathfrak{G}'$	1	ℓ	1	$\mathfrak{P}_1\mathfrak{P}_2$	1	ℓ	2
C_6	$\mathfrak{G}_1\mathfrak{G}_2$	1	1	2	$\mathfrak{G}'_1\cdots\mathfrak{G}'_\ell$	1	1	ℓ	$\mathfrak{P}_1\cdots\mathfrak{P}_\ell\mathfrak{P}'_1\cdots\mathfrak{P}'_\ell$	1	1	2ℓ

Theorem 2. *Let $N/\mathbb{F}_q$ as above. Then*

(2A) *The discriminants of $N/\mathbb{F}_q(X)$, $L/\mathbb{F}_q(X)$, and $L_0/\mathbb{F}_q(X)$ are related by*

$$\mathcal{D}(N/\mathbb{F}_q(X)) = (\mathcal{D}(L/\mathbb{F}_q(X)))^{\ell}\,(\mathcal{D}(L_0/\mathbb{F}_q(X)))^2 .$$

(2B) *The genus of $N/\mathbb{F}_q$ is given by*

$$g_N = 1 - 2\ell + \frac{1}{2}\left\{ \sum_{p(X)\in C_1} \ell d_{\mathbb{F}_q(X)}(p(X)) + \sum_{p(x)\in C_2\cup C_3} 2(\ell-1) d_{\mathbb{F}_q(X)}(p(X)) \right\} .$$

(2C) *The genera of $N/\mathbb{F}_q$, $L/\mathbb{F}_q$, and $L_0/\mathbb{F}_q$ are related by*

$$g_N = g_L + 2g_{L_0} .$$

Theorem 3. *Let $N/\mathbb{F}_q$ as above. Then*

(3A) *The zeta function of $N/\mathbb{F}_q$, $L/\mathbb{F}_q$, and $\mathbb{F}_q(X)/\mathbb{F}_q$ are related by*

$$\zeta(\mathbb{F}_q(X), s)^{-2}\zeta(L, s)^2\zeta(N, s)^{-1} = 1 .$$

(3B) *The zero-degree divisor class number of $N/\mathbb{F}_q$ is given by*

$$h(N) = h(L)h(L_0)^2 .$$

(3C) *The ideal class number $h(\mathcal{O}_N)$ of N is given by*

$$h(\mathcal{O}_N) = \frac{R_L R_{L_0}^2}{R_N \ell^{\alpha}} h(\mathcal{O}_L) h(\mathcal{O}_{L_0})^2$$

where α is equal to 1 if the infinite prime of $\mathbb{F}_q(X)/\mathbb{F}_q$ is decomposed in $N/\mathbb{F}_q$ as the prime divisors in class C_5 in Table 1; otherwise, α is equal to zero. $h(\mathcal{O}_L)$ and $h(\mathcal{O}_{L_0})$ denote the ideal class number of L and L_0, respectively.

As it has been pointed out by the anonymous referee, Theorem 3 is a special case of a more general result due to Frey & Rück, and Kani; their result depends on the explicit knowledge of a relation between norm idempotents in the group algebra [FR], [K]. The result (3C) was proved by Brauer [B] in the case of number fields. In this note we use a direct approach to the problem following closely the classical examples on this matter [A], [Z].

§3. Proof of the theorems

In this section we will use the notations and results for ramification groups as established in [S] (Chap. I-IV).

We shall accomplish the proof of Theorem 1 by means of a series of lemmata.

Lemma 1. *Let $p(X)$ be a prime of $\mathbb{F}_q(X)/\mathbb{F}_q$, finite or infinite, ramifying in $L/\mathbb{F}_q$, i.e., $p(X) = \mathfrak{G}^2$, where $\mathfrak{G}$ is a prime divisor of $L/\mathbb{F}_q$. Then, in $N/\mathbb{F}_q$, $\mathfrak{G}$ is the product of ℓ different prime divisors. In particular, $\mathfrak{G}$ does not ramify.*

Proof. Since N/L is a Galois extension and $\ell = [N : L]$ is a prime, then either $\mathfrak{G}$ is inert ($\mathfrak{G} = \mathfrak{P}$, where $\mathfrak{P}$ is a prime divisor of $N/\mathbb{F}_q$), or is totally ramified ($\mathfrak{G} = \mathfrak{P}^\ell$, where $\mathfrak{P}$ is a prime divisor of $N/\mathbb{F}_q$), or splits completely ($\mathfrak{G} = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_\ell$, where the $\mathfrak{P}_i$ are ℓ distinct prime divisors of $N/\mathbb{F}_q$). In order to prove the lemma, it is sufficiente to show that the first two possibilities cannot occur. Indeed, if $\mathfrak{G} = \mathfrak{P}$ then $G_1(\mathfrak{P}) = D_{N/\mathbb{F}_q(X)}(\mathfrak{P}) = D_{2\ell}$; clearly $\mathfrak{P}$ is ramified in $N/\mathbb{F}_q(X)$ and $e_{N/\mathbb{F}_q(X)}(\mathfrak{P}) = 2$; thus $\#G_0(\mathfrak{P}) = \#T_{N/\mathbb{F}_q(X)}(\mathfrak{P}) = 2$, but this contradicts the fact that $G_0(\mathfrak{P})$ is a normal subgroup of $G_{-1}(\mathfrak{P}) = D_{2\ell}$. Therefore $\mathfrak{G} = \mathfrak{P}$ cannot hold. To see that $\mathfrak{G} = \mathfrak{P}^\ell$ does not hold, let us first remark that since $p \neq 2$, then $G_1(\mathfrak{P})$ is a p-subgroup (see [S], Chap. IV, Paragraph 2, Corollary 3) and since $p \neq \ell$ we must have $G_1(\mathfrak{P}) = 1$, and $G_0/G_1 \approx D_{2\ell}$. But this is impossible since G_0/G_1 is always a cyclic group (see [S], Chap. IV, Paragraph 2, Corollary 1). Therefore $\mathfrak{G} = \mathfrak{P}^\ell$ cannot hold. □

Lemma 2. *Let N, L and L_0 be as above. Then*

(1) *No prime divisor of $\mathbb{F}_q(X)/\mathbb{F}_q$, finite or infinte, is inert in $N/\mathbb{F}_q(X)$. In particular, no prime divisor of $\mathbb{F}_q(X)/\mathbb{F}_q$ is simultaneously inert in $L/\mathbb{F}_q(X)$ and N/L, or simultaneously inert in $L_0/\mathbb{F}_q(X)$ and N/L_0.*

(2) *No prime divisor of $\mathbb{F}_q(X)/\mathbb{F}_q$ ramifies totally in $N/\mathbb{F}_q$.*

Proof. (1) Let $p(X)$ be a prime divisor of $\mathbb{F}_q(X)/\mathbb{F}_q$, inert in $L/\mathbb{F}_q(X)$ and N/L, then $T_{N/\mathbb{F}_q(X)}p(X) = 1$ and $D_{N/\mathbb{F}_q(X)}(p(X)) = D_{2\ell}$, so that $D_{2\ell} \approx D_{N/\mathbb{F}_q(X)}(p(X))/T_{N/\mathbb{F}_q(X)}(p(X)) \approx \text{Gal}\ (N_{p(X)}/\mathbb{F}_q(X)_{p(X)})$, which is not possible since the latter group is cyclic. (2) Let us suppose that $p(X)$ totally ramifies, so that $\#T_{N/\mathbb{F}_q(X)}(\mathfrak{P}) = e_{N/\mathbb{F}_q(X)}(\mathfrak{P}) = 2\ell$ and necessarily $e_{L/\mathbb{F}_q(X)}(\mathfrak{P}) = \ell > 1$, which contradicts lemma 1. □

Lemma 3. *Let N, L, and L_0 as above.*

(1) *Let $p(X)$ be a prime divisor of $\mathbb{F}_q(X)/\mathbb{F}_q$ ramified in N/L. Then $p(X)$ in $L_0/\mathbb{F}_q$ is an ℓ-power of a prime divisor of $L_0/\mathbb{F}_q$.*

(2) *Let $p(X)$ be a prime divisor of $\mathbb{F}_q(X)/\mathbb{F}_q$ ramified in $L/\mathbb{F}_q(X)$. Then $p(X)$ in $L_0/\mathbb{F}_q$ decomposes as follows:*

$$\mathfrak{W}_1\mathfrak{W}_2^2\cdots\mathfrak{W}_{(\ell+1)/2}^2 \cdot$$

Proof. (1) According to Lemma 1, the prime divisor $p(X)$ decomposes in $L/\mathbb{F}_q(X)$ either as $p(X) = \mathfrak{G}$ or $p(x) = \mathfrak{G}_1\mathfrak{G}_2$. Since ℓ is a prime, then in $N/\mathbb{F}_q$ we have $p(X) = \mathfrak{P}^\ell$ or $p(X) = \mathfrak{P}_1^\ell\mathfrak{P}_2^\ell$. Now the prime divisors $\mathfrak{P}$, $\mathfrak{P}_1$ and $\mathfrak{P}_2$ have as decomposition groups $D_{2\ell}$, H and H respectively, while the inertia subgroups for each one of them is H. But

$$T_{N/\mathbb{F}_q(X)}(\mathfrak{P}) \cap \text{Gal}\,(N/L_0) = 1, \quad T_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) \cap \text{Gal}\,(N/L_0) = 1,$$
$$D_{N/\mathbb{F}_q(X)}(\mathfrak{P}) \cap \text{Gal}\,(N/L_0) = H_0,\ D_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) \cap \text{Gal}\,(N/L_0) = 1, i = 1, 2.$$

The equalities in the first row indicate that the prime divisors $\mathfrak{P}$, $\mathfrak{P}_1$ and $\mathfrak{P}_2$ do not ramify in N/L_0, while the first equality in the second row shows that $d_{N/L_0}(\mathfrak{P}) = 2$ and $r_{N/L_0}(\mathfrak{P}) = 1$. Therefore, in the first case ($p(X) = \mathfrak{P}^\ell$), we have $p(X) = \mathfrak{W}^\ell$ in $L_0/\mathbb{F}_q$, where $\mathfrak{W}$ is the prime divisor of $L_0/\mathbb{F}_q$ lying under $\mathfrak{P}$.

Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be the prime divisors of $L_0/\mathbb{F}_q$ lying over $\mathfrak{P}_1$ and $\mathfrak{P}_2$, respectively. If $\mathfrak{W}_1 = \mathfrak{W}_2$, we have the result, since $p(X) = \mathfrak{W}_1^\ell$ in $L_0/\mathbb{F}_q$. If $\mathfrak{W}_1 \neq \mathfrak{W}_2$, we get $p(X) = \mathfrak{W}_1^\ell\mathfrak{W}_2^\ell$ in $L_0/\mathbb{F}_q$; but since $r_{N/L_0}(\mathfrak{P}_i) = 2$, we get the following decomposition of $p(X)$ in $N/\mathbb{F}_q$: $p(X) = \mathfrak{P}_1^\ell\mathfrak{P}_1'^\ell\mathfrak{P}_2^\ell\mathfrak{P}_2'^\ell$, where $\mathfrak{P}_1$, $\mathfrak{P}_1'$, $\mathfrak{P}_2$, $\mathfrak{P}_2'$ are different prime divisors in $N/\mathbb{F}_q$, which contradicts our initial hypothesis on the decomposition of $p(X)$ in $N/\mathbb{F}_q$.

(2) If $p(X) = \mathfrak{G}^2$ in $L/\mathbb{F}_q(X)$, then the prime divisor $\mathfrak{G}$ decomposes in N/L as $\mathfrak{G} = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_\ell$; thus the decomposition subgroups $D_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i)$, $i = 1, 2, \cdots, \ell$, are subgroups of order 2, and $p(X) = \sigma(\mathfrak{P}_1)^2\sigma^2(\mathfrak{P}_1)^2\cdots\sigma^{\ell-1}(\mathfrak{P}_1)^2$, so that the decomposition subgroups $D_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i)$, $i = 1, 2, \cdots, \ell$, are mutually different.

By modifying the indexes, if necessary, we may suppose that $L_0/\mathbb{F}_q$ is the decomposition field of $\mathfrak{P}_i$. Let now $\mathfrak{W}_i$ lying under $\mathfrak{P}_i$. Since $d_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) = 1$, $e_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) = 2$, and $r_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) = \ell$, we get:

$$T_{N/L_0}(\mathfrak{P}_i) = \begin{cases} \text{Gal}\,(N/L_0) \cap T_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) = H_0 \cap T_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) = 1 \text{ if } i \neq 1, \\ H_0 \text{ if } i = 1\ . \end{cases}$$

This implies that

$$e_{N/L_0}(\mathfrak{P}_i) = \begin{cases} 1 \text{ if } i \neq 1\ , \\ 2 \text{ if } i = 1\ , \end{cases} \quad r_{N/L_0}(\mathfrak{P}_i) = \begin{cases} 2 \text{ if } i \neq 1, \\ 1 \text{ if } i = 1, \end{cases} \quad d_{N/L_0}(\mathfrak{P}_i) = 1\ .$$

If $i \neq 1$, not all $\mathfrak{W}_i$ are distinct, since otherwise $p(X)$ would not be a product of ℓ distinct prime divisors in $N/\mathbb{F}_q$, because of the value of $r_{N/L_0}(\mathfrak{P}_i)$. Let t be the number of distinct $\mathfrak{W}_i$ ($i \neq 1$), so that $2t = \ell - 1$. Due to all of the above, we must have the following decomposition in N/L_0:

$$p(X) = \mathfrak{W}_1\mathfrak{W}_2^2\cdots\mathfrak{W}_{(\ell+1)/2}^2\ . \quad \square$$

Lemma 4. *Let $p(X)$ be a prime divisor of $\mathbb{F}_q(X)/\mathbb{F}_q$ not ramified in $N/\mathbb{F}_q(X)$. Then, in $N/\mathbb{F}_q$, $p(X)$ decomposes as follows:*

(1) *If $p(X)$ is inert in $L/\mathbb{F}_q(X)$, then $p(X) = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_\ell$, where the $\mathfrak{P}_i$'s are prime divisors of $N/\mathbb{F}_q$.*

(2) *If $p(X)$ splits in $L/\mathbb{F}_q(X)$, then either $p(X) = \mathfrak{P}_1\mathfrak{P}_2$ or $p(X) = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_\ell\mathfrak{P}'_1\mathfrak{P}'_2\cdots\mathfrak{P}'_\ell$ where the $\mathfrak{P}_i$'s and the $\mathfrak{P}'_i$'s are prime divisors of $N/\mathbb{F}_q$.*

Proof. (1) If $p(X)$ is inert in $L/\mathbb{F}_q(X)$, it cannot be inert in N/L. Since, by hypothesis, $p(X)$ does not ramify in $N/\mathbb{F}_q(X)$, then $p(X) = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_\ell$ in $N/\mathbb{F}_q(X)$.

(2) The proof proceeds along the same lines. □

Lemma 5. *Let $p(X)$ be a prime divisor of $\mathbb{F}_q(X)/\mathbb{F}_q$, not ramified in $N/\mathbb{F}_q(X)$. Then:*

(1) *If $p(X)$ is inert in $L/\mathbb{F}_q(X)$, then in $L_0/\mathbb{F}_q(X)$, $p(X)$ decomposes as $p(X) = \mathfrak{W}_1\mathfrak{W}_2\cdots\mathfrak{W}_{(\ell+1)/2}$.*

(2) *If $p(X)$ splits in $L/\mathbb{F}_q(X)$, then $p(X)$ decomposes in $L_0/\mathbb{F}_q(X)$ either as $p(X) = \mathfrak{W}_1$ or as $p(X) = \mathfrak{W}_1\mathfrak{W}_2\cdots\mathfrak{W}_\ell$, where the $\mathfrak{W}_i$'s are prime divisors of $L_0/\mathbb{F}_q$.*

Proof. (1) Let $p(X)$ be a prime divisor of $\mathbb{F}_q(X)/\mathbb{F}_q$, inert in $L/\mathbb{F}_q$. Since $p(X)$ does not ramify in $N/\mathbb{F}_q(X)$, then accordingly to Lemma 4, $p(X) = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_\ell$ in $N/\mathbb{F}_q$, so that $e_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) = 1$, $d_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) = 2$ and $r_{N\mathbb{F}_q(X)}(\mathfrak{P}_i) = 1$; that is, $\#D_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) = 2$, $\#T_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) = 1$, and $D_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) \neq D_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i)$, if $i \neq j$, as in the second part of Lemma 3. By a convenient change of indexes, we may suppose that $L_0/\mathbb{F}_q$ is the decomposition field of $\mathfrak{P}_1$, so that $D_{N/L_0}(\mathfrak{P}_i) = 1$ if $i \neq 1$, and $D_{N/L_0}(\mathfrak{P}_1) = H_0$, $T_{N/L_0}(\mathfrak{P}_1) = 1$. The proof then goes on along the lines of that of Lemma 3, (2).

(2) According to Lemma 4, if a prime divisor $p(X)$ of $\mathbb{F}_q(X)/\mathbb{F}_q$ does not ramify in $N/\mathbb{F}_q(X)$, and splits in $L/\mathbb{F}_q(X)$, then either $p(X) = \mathfrak{P}_1\mathfrak{P}_2$ or $p(X) = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_\ell\mathfrak{P}'_1\mathfrak{P}'_2\cdots\mathfrak{P}'_\ell$. In the first case, we have $e_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) = 1$, $d_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) = \ell$, and $r_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) = 2$, so that $T_{N/\mathbb{F}_q(X)}(\mathfrak{P}_i) = 1$. Thus, in N/L_0, we have $T_{N/L_0}(\mathfrak{P}_i) = 1$, and consequently $e_{N/L_0}(\mathfrak{p}g_i) = 1$, $d_{N/L_0}(\mathfrak{P}_i) = 1$, and $r_{N/L_0}(\mathfrak{p}g_i) = 2$. Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be prime divisors lying under $\mathfrak{P}_1$ and $\mathfrak{P}_2$, respectively. If $\mathfrak{W}_1 \neq \mathfrak{W}_2$, $r_{N/L_0}(\mathfrak{P}_i) = 2$ implies that the decomposition of $p(X)$ in $N/\mathbb{F}_q$ has the form $p(X) = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}'_1\mathfrak{P}'_2$, where all these prime divisors are mutually distinct. But this contradicts our initial hypothesis on the decomposition of $p(X)$. Therefore, $\mathfrak{W}_1 = \mathfrak{W}_2$ and $p(X) = \mathfrak{W}_1$ in $L_0/\mathbb{F}_q$. The second case is similarly proved. □

Proof of Theorem 1. Given a prime divisor in $\mathbb{F}_q(X)/\mathbb{F}_q$, finite or infinite, its decomposition in $L/\mathbb{F}_q(X)$ can only take one of the following forms:

$$(1)\quad p(X) = \mathfrak{G}^2\,, \qquad (2)\quad p(X) = \mathfrak{G}\,, \qquad (3)\quad p(X) = \mathfrak{G}_1\mathfrak{G}_2\,.$$

In the first case, by lemmata 1 and 3, (2), $p(X)$ ramifies in $N/\mathbb{F}_q(X)$ as the prime divisors of class C_1, in the first row of Table 1. If the given prime divisor ramifies in $N/\mathbb{F}_q(X)$, then in the cases (2) and (3), by virtue of Lemma 3, (1), and the fact that the extension N/L is galoisian, we have the second and third rows in Table 1, i.e., the prime divisors of classes C_2 and C_3. If the given prime divisor does not ramify in $N/\mathbb{F}_q(X)$, then in case (2), by virtue of Lemma 4, (1), and Lemma 5, (1), we have the fourth row of Table 1, i.e., the prime divisors of class C_4. In the case (3), as a consequence of lemmata 4, (2), and 5, (2), we have the fifth and sixth rows of Table 1, i.e., the prime divisors of classes C_5 and C_6. □

Proof of Theorem 2. (2A) We denote by $\mathcal{D}(M/N)$ the different of the extension M/N. By the transitivity of the different we have the following relations:

$$\mathcal{D}(N/\mathbb{F}_q(X)) = \mathcal{D}(N/L)\mathcal{D}(L/\mathbb{F}_q(X)) = \mathcal{D}(N/L_0)\mathcal{D}(L_0/\mathbb{F}_q(X)) \ .$$

Furthermore, we have $\mathcal{D}(N/L) = \mathcal{D}(L_0/\mathbb{F}_q(X))$, where we are considering $\mathcal{D}(L_0/\mathbb{F}_q(X))$ as a divisor in $N/\mathbb{F}_q$. This statement is a consequence of the fact that $\mathfrak{P}_i$ is ramified in $N/\mathbb{F}_q(X)$ if and only if $\mathfrak{P}$ is ramified in $L/\mathbb{F}_q(X)$ or (exclusive) $\mathfrak{P}$ is ramified in $L_0/\mathbb{F}_q$. The last statement is a consequence of Theorem 1. Due to all of the above, we have $\mathcal{D}(N/L) = \mathcal{D}(L_0/\mathbb{F}_q(X))$; now, taking norms with respect to N/L, we find the desired relation.

(2B) The genus of $N/\mathbb{F}_q$ is obtained by means of the Hurwitz-Zeuthen genus formula:

$$\begin{aligned} 2g_N &= [N : \mathbb{F}_q(X)](2g_{\mathbb{F}_q(X)}) - 2) + \sum_{\mathfrak{P}} (e_{N/\mathbb{F}_q(X)}(\mathfrak{P}) - 1)d_{\mathbb{F}_q(X)}(\mathfrak{P}) \\ &= [N : \mathbb{F}_q(X)](2g_{\mathbb{F}_q(X)} - 2) + d_{\mathbb{F}_q(X)}(\mathcal{D}(N/\mathbb{F}_q(X))) \ , \end{aligned} \tag{1}$$

where $\mathfrak{P}$ runs over the ramified prime divisors of $N/\mathbb{F}_q$, and $d_{\mathbb{F}_q(X)}(\mathfrak{P})$ denotes the absolute degree of the prime divisor $\mathfrak{P}$.

By Theorem 1 we know that the ramified prime divisors of $N/\mathbb{F}_q$ are lying on prime divisors of $\mathbb{F}_q(X)/\mathbb{F}_q$ that belong to the classes C_1, C_2, C_3. So the sum that appears in (1) can be broken into three sums, each one of them running over one of these classes. The ramification indexes, absolute and relative degrees, and splitting degrees can be calculated by using Table 1. After some simple calculations we find:

$$\begin{aligned} 2g_N - 2 = -4\ell + \sum_{p(X)\in C_1} \ell d_{\mathbb{F}_q(X)}(p(X)) + \sum_{p(X)\in C_2} 2(\ell - 1)d_{\mathbb{F}_q(X)}(p(X)) \\ + \sum_{p(X)\in C_3} 2(\ell - 1)d_{\mathbb{F}_q(X)}p(X) \end{aligned}$$

(2C) By using the fact that $V_{\mathfrak{P}}(\mathcal{D}(N/L)) = \sum_{i\geq 0}(\#G_i - 1)$ (see [S], Chap. IV, Paragraph 1), and Table 1, we have

$$d_{\mathbf{F}_q(X)}(\mathcal{D}(N/\mathbb{F}_q(X))) = \sum_{\mathfrak{P}} V_{\mathfrak{P}}(\mathcal{D}(N/L) d_{\mathbf{F}_q(X)}(\mathfrak{P})$$
$$= \sum_{p(X)\in C_2\cup C_3} 2(\ell-1) d_{\mathbf{F}_q(X)}(p(X)) .$$

By a similar reasoning we get

$$d_{\mathbf{F}_q(X)}(\mathcal{D}(N/L_0) = \sum_{p(X)\in C_1} \ell d_{\mathbf{F}_q(X)}(p(X)) .$$

Now by replacing in the result (2B) we get the desired result. □

Proof of Theorem 3. (3A) The zeta function of the algebraic function field $N/\mathbb{F}_q$ is given by:

$$\zeta(N,s) = \prod_{\mathfrak{P}} (1 - |\mathfrak{P}|^{-s})^{-1} = \prod_{\mathfrak{P}} \left(1 - q^{-s d_{\mathbf{F}_q(X)}(\mathfrak{P})}\right)^{-1} , \tag{2}$$

where $\mathfrak{P}$ runs over the prime divisors of $N/\mathbb{F}_q$, and $|\mathfrak{P}|$ denotes the norm of the prime divisor $\mathfrak{P}$. Let $p(X)$ be the prime divisor of $\mathbb{F}_q(X)/\mathbb{F}_q$ lying under $\mathfrak{P}$, and $d_{\mathbf{F}_q(X)}(\mathfrak{P})$ and $d_{N/\mathbf{F}_q(X)}(\mathfrak{P})$ denote the absolute degree and the relative degree, respectively. The product (2) is absolutely convergent for Re $(s) > 1$, so we may reorder it as follows:

$$\zeta(N,s) = \prod_{p(X)} \prod_{\mathfrak{P}|p(X)} \left(1 - U^{d_{N/\mathbf{F}_q(X)}(\mathfrak{P}) d_{\mathbf{F}_q(X)} p(X)}\right)^{1} ,$$

where $U = q^{-s}$.

The following combinatorial identity is valid for every prime divisor of $\mathbb{F}_q(X)/\mathbb{F}_q$:

$$\prod_{\mathfrak{P}|p(X)} \left(1 - a^{d_{N/\mathbf{F}_q(X)}(\mathfrak{P})}\right)$$
$$= (1-a)^{-2} \prod_{\mathfrak{P}|p(X)} \left(1 - a^{d_{L/\mathbf{F}_q(X)}(\mathfrak{P})}\right) \left(\prod_{\mathfrak{P}|p(X)} \left(1 - a^{d_{L/\mathbf{F}_q(X)}(\mathfrak{P})}\right)\right)^{2} ,$$

where $a = U^{d_{\mathbf{F}_q(X)}(\mathfrak{P})}$, and the products that appear in the above identity are taken over the prime divisors of $N/\mathbb{F}_q$, $L/\mathbb{F}_q$, and $L_0/\mathbb{F}_q$ lying over $p(X)$.

Indeed, this identity can be verified easily using Theorem 1. For example, if $p(X) \in C_1$, then

$$(1-a)^{\ell} = (1-a)^2(1-a)\left[(1-a)^{(\ell+1)/2}\right]^2 .$$

The other cases can be verified in the same manner. This identity implies the first part of Theorem 3. (The result (2C) of Theorem 2 can be also obtained from the above result.)

(3B) The zeta function of an algebraic function field with finite constant field is a rational function (see [W], Chap. 7) of the following form:

$$\zeta(N,s) = \frac{F(q^{-s},N)}{(1-q^{-s})(1-q^{1-s})} ,$$

where $F(q^{-1},N)$ is a polynomial in the variable $U = q^{-s}$ of degree $2g_N$, g_N being the genus of $N/\mathbb{F}_q$. The value of $F(U,N)$ for $U=1$ is the zero-degree divisor class number of the field. If we take into account that $\zeta F(\mathbb{F}_q(X)/\mathbb{F}_q,s) = (1-q^{-s})^{-1}(1-q^{1-s})^{-1}$ and part one of Theorem 1, we find the desired result.

(3C) By a result due to F. K. Schmidt (see [M]) we have:

$$h(N)\mu(N) = h(\mathcal{O}_N)R(N) , \tag{3}$$

where

$$\begin{aligned}\mu(N) = \text{ g.c.d. }_{\mathfrak{P}|\infty}\{d_{\mathbb{F}_q(X)}(\mathfrak{P})\} &= \text{ g.c.d. }_{\mathfrak{P}|\infty}\{d_{N/\mathbb{F}_q(X)}(\mathfrak{P})d_{\mathbb{F}_q(X)}(\infty)\} \\ &= \text{ g.c.d. }_{\mathfrak{P}|\infty}\{d_{N/\mathbb{F}_q(X)}(\mathfrak{P})\}\end{aligned}$$

and

$$R(N) + \left(D_0^{N/\mathbb{F}_q(X)}(\infty) \ : \ P^{N/\mathbb{F}_q(X)}(\infty)\right) ,$$

where $D_0^{N/\mathbb{F}_q(X)}(\infty)$ is the subgroup of zero-degree divisors generated by infinite prime divisors of $N/\mathbb{F}_q$, and $P^{N/\mathbb{F}_q(X)}(\infty)$ is the subgroup of zero-degree divisors generated by units of $N/\mathbb{F}_q$. By Theorem 1, we have:

$$\begin{aligned}\frac{\mu(N)}{\mu(L)\mu(L_0)} &= \begin{cases} 1 & \text{if} \quad \infty \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_6 \\ \ell & \text{if} \quad \infty \in C_5 \end{cases} \\ &= \frac{1}{\ell^{\alpha}} .\end{aligned} \tag{4}$$

The desired result follows now from part (3B), and (3) and (4).

Aknowledgments. The author thanks to Professor Víctor Albis for suggesting this topic for his Master's Dissertation and for his guidance while completing it.

REFERENCES

[A]. Artin, E., *Quadratische Körper im gebiete der höheren Kongruenzen. I, II.*, **Math. Z. 19** (1924), 153–246.

[B]. Brauer, R., *Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoischen Körpes*, Math. Nach. **4** (1951), 158–174.

[F.-R.]. Frey, G. and Rück, H., *The strong Lefschetz principle in algebraic geometry*, **manuscripta math. 55** (1986), 385–401.

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

[M]. MacRae, R. E., *On unique factorization in certain rings of algebraic functions*, J. of Algebra **17** (1971), 243–261.

[S]. Serre, J.-P., *Corps locaux*, Hermann, Paris, 1962.

[W]. Weil, A., *Basic Number Theory*, Springer-Verlag, Berlin, 1967.

[Z]. Zhang, X., *Algebraic function fields of type* $(2, \cdots, 2)$, Scientia Sinica, Ser. A **31** (1988), 908-915.

(Recibido en agosto de 1992; la versión revisada en julio de 1993)

CURRENT ADDRESS: IMPA, ESTRADA DONA CASTORINA 110, JARDÍM BOTÂNICO, C. E. P. 22460-320, RIO DE JANEIRO, RJ – BRASIL