Quadratic function fields
whose class numbers are not divisible by three

by

HUMIO ICHIMURA (Yokohama)

1. Introduction. For an algebraic number field $K$, let $Cl(K)$ be its ideal class group and $h(K) = |Cl(K)|$. For a prime number $l$ dividing the degree $[K : \mathbb{Q}]$, we have a lot of information on the $l$-part $Cl(K)(l)$ of $Cl(K)$ (see e.g. [2], [3], [11], [14]). On the other hand, when $l \nmid [K : \mathbb{Q}]$, not so many results are known on $Cl(K)(l)$. One of such is that of Hartung [8] and Horie [9], who proved that there exist infinitely many imaginary quadratic fields $K$ with $l \nmid h(K)$ (and satisfying some additional conditions) for any odd prime number $l$. When $l = 3$, there are stronger results concerning the “density” of the set of quadratic fields $K$ with $3 \nmid h(K)$ (and satisfying some additional conditions), which were obtained by Davenport and Heilbronn [5], Datskovsky and Wright [4], and Kimura [12]. They also obtained analogous results for quadratic extensions over the rational function field $\mathbb{F}_q(T)$, where $\mathbb{F}_q$ is a fixed finite field.

Since the methods in the papers referred to above are not constructive, it is desirable to give explicit families of infinitely many quadratic extensions $K$ over $\mathbb{Q}$ or $\mathbb{F}_q(T)$ with $l \nmid h(K)$ for each odd prime number $l$. Here, $h(K)$ is the number of divisor classes of $K$ of degree zero when $K$ is a function field of one variable over a finite constant field. The main purpose of this note is to give such families when $l = 3$ in the function field case.

Let us give the main results. Let $p$ be a fixed prime number, $q$ a fixed power of $p$, and $\mathbb{F}_q$ the finite field with cardinality $q$. Let $T$ be a fixed indeterminate. We take the rational function field $\mathbb{F}_q(T)$ as the base field. For simplicity, we assume $p \geq 5$ in this section. For $n \geq 1$ and $a \in \mathbb{F}_q^\times$, we put

$$L_{n,a} = \mathbb{F}_q(T, (T^{3^n} + a)^{1/2}).$$

1991 Mathematics Subject Classification: Primary 11R58; Secondary 11R11, 11R29.

The author was partially supported by Grant-in-Aid for Scientific Research (C), Grant Number 11640041.
The genus of $L_{n,a}$ is $(3^n - 1)/2$. We show that $3 \nmid h(L_{n,a})$ when $q \equiv 1 \mod 3$ and $a \not\in (\mathbb{F}_q^\times)^2$ (Theorem 1(II)). However, when $q \equiv -1 \mod 3$, we have $3 \mid h(L_{n,a})$ for all $a \in \mathbb{F}_q^\times$ and $n$ (Theorem 1(III)). So, we have to find another family. We define rational functions $X_n = X_n(T)$ in $\mathbb{F}_q(T)$ inductively as follows:

\begin{equation}
X_0 = T, \quad X_n = (X_n^3 - 3X_{n-1} - 1)/(3(X_{n-1}^2 + X_{n-1})) \quad \text{for } n \geq 1.
\end{equation}

We easily see that when $q \equiv -1 \mod 3$, there exists $\gamma \in \mathbb{F}_q^\times$ such that $\gamma^2 - 3\gamma + 9 \not\in (\mathbb{F}_q^\times)^2$. We put $L''_n = \mathbb{F}_q(T, (3X_n + \gamma)^{1/2})$. The genus of $L''_n$ is $3^n - 1$. We show that $3 \nmid h(L''_n)$ for all $n \geq 1$ when $q \equiv -1 \mod 3$ (Theorem 4). We give similar families also when $p = 2, 3$ (Theorem 4, Theorem 3).

**Remark 1.** The second formula in (1) is a variant of the polynomial $f_a = X^3 - aX^2 - (a + 3)X - 1$ ($a \in \mathbb{Z}$). This polynomial was first effectively used by Shanks [16]. A property of $f_a$ is that its discriminant is $(a^2 + 3a + 9)^2$, which is used in the proof of Theorem 4.

**Remark 2.** Let $\infty_T$ be the prime divisor of $\mathbb{F}_q(T)$ corresponding to the pole of $T$. After Artin [1], we say that a quadratic extension $K/\mathbb{F}_q(T)$ of nonzero genus is a “real” quadratic extension when $\infty_T$ splits, and an “imaginary” one otherwise. The quadratic extensions given in Theorems 1–4 in Section 2 are imaginary ones.

**Remark 3.** Nagell [13] (resp. Yamamoto [17]) constructed infinitely many imaginary (resp. real) quadratic extensions (over $\mathbb{Q}$) whose class numbers are divisible by a given integer. For analogous results for the function field case, see Friesen [6] and the author [10].

**Convention.** For the rational function field $\mathbb{F}_q(X)$ with an indeterminate $X$, we denote by $\infty_X$ its prime divisor corresponding to the pole of $X$. Further, for an irreducible monic $P = P(X)$ in the polynomial ring $\mathbb{F}_q[X]$, we denote by $(P)$ the prime divisor of $\mathbb{F}_q(X)$ corresponding to the zeros of $P$. When $l \neq p$, let $\mu_{l^a}$ be the group of $l^a$th roots of unity for all $a \geq 1$ in the algebraic closure $\bar{\mathbb{F}}_q$, and $\zeta_l$ a primitive $l^a$th root of unity. For a module $M$, we abbreviate the quotient $M/lM$ (or $M/M'$) by $M/l$.

**2. Families of quadratic extensions over $\mathbb{F}_q(T)$.** Let $q$ be a fixed power of a prime number $p$, and $l$ a fixed odd prime number. In this section, we give several families of quadratic extensions $L$ over $\mathbb{F}_q(T)$ with $l \mid h(L)$ (resp. $l \nmid h(L)$). The results announced in Section 1 for $l = 3$ are contained in these ones.
For an element $x$ of the algebraic closure $\overline{\mathbb{F}}_q(T)$, we put

$$x^P = x^P - x \quad \text{and} \quad x^{P^n} = (x^{P^{n-1}})^P \quad \text{for} \quad n \geq 1.$$ 

We also denote by $x^{1/P^n}$ an element $z$ satisfying $z^{P^n} = x$.

First, assume that $l \neq p$. For $n \geq 1$ and $a \in \mathbb{F}_q$, we put

$$L_{n,a} = \begin{cases} \mathbb{F}_q(T,(T^n + a)^{1/2}) & \text{for} \quad p \neq 2, \\ \mathbb{F}_q(T,(T^n + a)^{1/2}) & \text{for} \quad p = 2. \end{cases}$$

Here, we assume $a \neq 0$ when $p \neq 2$. Let $\delta_l(q)$ be the order of $q$ mod $l$ in the multiplicative group $(\mathbb{Z}/l\mathbb{Z})^\times$, and let $\mathbb{F}^P_q$ be the subset of $\mathbb{F}_q$ consisting of elements $x^P$ with $x \in \mathbb{F}_q$. For the quadratic extensions $L_{n,a}$, we prove the following assertions.

**THEOREM 1.** Assume that $l \neq p$ and $p \neq 2$.

(I) When $a \in (\mathbb{F}^\times_q)^2$, we have $l \mid h(L_{n,a})$ for all $n$.

(II) When $\delta_l(q)$ is odd, we have $l \mid h(L_{n,a})$ if and only if $a \in (\mathbb{F}^\times_q)^2$.

(III) When $\delta_l(q) = 2$, we have $l \mid h(L_{n,a})$ for all $a$ and $n$.

**THEOREM 2.** Assume that $l \neq p$ and $p = 2$.

(I) When $a \in \mathbb{F}^P_q$, we have $l \mid h(L_{n,a})$ for all $n$.

(II) When $\delta_l(q)$ is odd, we have $l \mid h(L_{n,a})$ if and only if $a \in \mathbb{F}^P_q$.

(III) When $\delta_l(q) = 2$, we have $l \mid h(L_{n,a})$ for all $a$ and $n$.

Next, assume that $l = p$. For $n \geq 1$ and $a \in \mathbb{F}_q$, we put

$$L'_{n,a} = \mathbb{F}_q(T,(T^{P^n} + a)^{1/2}).$$

For these quadratic extensions, we prove the following:

**THEOREM 3.** Assume that $l = p$. We have $l \nmid h(L'_{n,a})$ for all $a$ and $n$.

Finally, let $l = 3$ and $q \equiv -1 \pmod 3$. Let $X_n = X_n(T)$ be the rational function in $\mathbb{F}_q(T)$ defined by (1), and when $p \neq 2$, let $\gamma$ be a fixed element of $\mathbb{F}^\times_q$ such that $\gamma^2 - 3\gamma + 9 \notin (\mathbb{F}^\times_q)^2$. For $n \geq 1$, we put

$$L''_n = \begin{cases} \mathbb{F}_q(T,(3X_n + \gamma)^{1/2}) & \text{for} \quad p \neq 2, \\ \mathbb{F}_q(T,(X_n)^{1/P}) & \text{for} \quad p = 2. \end{cases}$$

For these quadratic extensions, we prove the following:

**THEOREM 4.** Assume that $l = 3$ and $q \equiv -1 \pmod 3$. We have $3 \nmid h(L''_n)$ for all $n$.

**REMARK 4.** When $\delta_l(q)$ is even but not 2, the author could not show whether or not $l \mid h(L_{n,a})$ for $a \notin (\mathbb{F}^\times_q)^2$.

**3. Some lemmas.** Let $k$ be a fixed algebraic function field of one variable with constant field $\mathbb{F}_q$, and let $l$ be a fixed prime number (not necessarily
In this section, we give several lemmas concerning the class number $h(k)$ of $k$ or that of a finite separable extension over $k$. They are well known or, otherwise, known to specialists.

The following lemma follows from class field theory.

**Lemma 1.** Let $p$ be a prime divisor of $k$ with $l \nmid \deg(p)$, where $\deg(\ast)$ denotes the degree of a divisor. Then $l \mid h(k)$ if and only if there exists an unramified cyclic extension over $k$ of degree $l$ in which $p$ splits completely.

For this, the readers may consult Rosen [15, p. 368]. From this lemma, we immediately obtain the following corollaries.

**Corollary 1.** Let $p$ be as in Lemma 1. Let $\mathbb{F}_q$ be a finite extension and $K = k\mathbb{F}_q$. Assume that $p$ remains prime in $K$. Then $l \mid h(K)$ if $l \mid h(k)$.

**Corollary 2.** Let $p$ be as in Lemma 1. Let $K/k$ be a finite separable extension in which $p$ is totally ramified. Then $l \mid h(K)$ if $l \mid h(k)$.

The following lemma is a function field analogue of a theorem of Iwasawa [11] on the class numbers of algebraic number fields.

**Lemma 2.** Let $K/k$ be a finite $l$-Galois extension. Assume that exactly one prime divisor $\mathfrak{P}$ of $K$ is ramified over $k$ and that $l \mid \deg(\mathfrak{P})$. Then $l \mid h(K)$ implies $l \mid h(k)$.

**Proof.** Though this assertion is more or less known, we give a proof for the convenience of the readers. Assume that $l \mid h(K)$. Let $H/K$ be the maximal unramified abelian extension of exponent $l$ in which $\mathfrak{P}$ splits completely. As $l \mid h(K)$, we have $H \neq K$ by Lemma 1. Put $p = \mathfrak{P} \cap k$. Then we see that $\mathfrak{P}$ is the unique prime divisor of $K$ over $p$ from an assumption of the lemma. Therefore, $H$ is Galois over $k$. Let $G = \text{Gal}(H/k)$ and $Z \subseteq G$ the decomposition group of an extension of $\mathfrak{P}$ in $H$. We have $G \neq Z$ as $H \neq K$. Then, since $G$ is an $l$-group, there exists a normal subgroup $\tilde{Z}$ of $G$ such that $[G : \tilde{Z}] = l$ and $\tilde{Z} \supseteq Z$ (cf. Hall [7, Theorem 4.3.2]). Let $E$ be the intermediate field of $H/k$ corresponding to $\tilde{Z}$ by Galois theory. Then $E/k$ is an unramified cyclic extension of degree $l$, and $p$ splits completely in $E$. Therefore, we obtain $l \mid h(k)$ by Lemma 1.

The following is a version of Lemma 2. As in Section 1, we denote by $\infty_T$ the prime divisor of $\mathbb{F}_q(T)$ corresponding to the pole of $T$.

**Lemma 3.** Let $k = \mathbb{F}_q(T)$ and $K/k$ a finite $l$-Galois extension. Assume that $q \equiv 1 \mod l$. Assume further that (i) $\infty_T$ is totally ramified in $K$, (ii) exactly one prime divisor $p$ of $k$ other than $\infty_T$ ramified in $K$, and (iii) $l \mid \deg(p)$. Then $l \mid h(K)$.

**Proof.** Assume that $l \mid h(K)$. Then, in a way similar to the proof of Lemma 2, we see that there exists a cyclic extension $E$ over $k$ of degree $l$
unramified outside \( p \) in which \( \infty_T \) splits completely. Let \( P = P(T) (\in \mathbb{F}_q[T]) \) be the irreducible monic corresponding to \( p \). Since \( q \equiv 1 \mod l \), we can write \( E = \mathbb{F}_q(T, (\zeta P^n)^{1/l}) \) for some \( \zeta \in \mathbb{F}_q^\times \) and \( n \in \mathbb{Z} \). Then, since \( l \not| \deg(P) \) and \( \infty_T \) splits in \( E \), it follows that \( l \mid a \) and \( \zeta \in (\mathbb{F}_q^\times)^l \), and hence \( E = k \). This is a contradiction.

The following lemma is known as Abhyankar’s lemma (cf. Cornell [2]).

**Lemma 4.** Let \( E_i \) be a finite separable extension over a local field \( k \) with ramification index \( e \), \( i = 1, 2 \). If \( E_2 \) is at most tamely ramified and \( e_2 \mid e_1 \), then \( E_1 E_2/E_1 \) is unramified.

Finally, assume that \( l \not= \text{char}(k) = (p) \). Let \( \zeta = \zeta_i \) be a primitive \( l \)th root of unity, \( K = k(\zeta) \) and \( \Delta = \text{Gal}(K/k) \). Let \( \infty \) be a fixed prime divisor of \( k \) such that \( \deg(\infty) \) is relatively prime to \( l|\Delta| \). There exists a unique prime divisor \( \infty \) of \( K \) over \( \infty \) as deg(\( \infty \)) and \( |\Delta| \) are relatively prime. For \( v \in K^\times \), we denote by \([v]\) the class in \( K^\times/l = K^\times/(K^\times)^l \) represented by \( v \). We regard \( K^\times/l \) as a module over the group ring \( \mathbb{F}_l[\Delta] \). For an \( \mathbb{F}_l[\Delta] \)-module \( M \) and an \( (\mathbb{F}_l\text{-valued}) \) character \( \chi \) of \( \Delta \), let \( M(\chi) \) denote the \( \chi \)-component of \( M \). Namely, \( M(\chi) \) is the maximal submodule of \( M \) on which \( \Delta \) acts via \( \chi \). Let \( \omega \) be the \((\mathbb{F}_l\text{-valued}) \) character of \( \Delta \) representing its Galois action on \( \zeta \), and \( \chi_0 \) the trivial character of \( \Delta \).

**Lemma 5.** In the above setting, we have \( l \mid h(k) \) if and only if there exists a nontrivial element \([v]\) of \((K^\times/l)(\omega)\) or \((K^\times/l)(\chi_0)\) such that (i) the cyclic extension \( K(v^{1/l})/K \) of degree \( l \) is unramified and (ii) \( \infty \) splits completely in this extension.

**Proof.** Denote by \( Cl_K \) the divisor class group of \( K \) of degree zero. Let \( \bar{H}/K \) be the maximal unramified abelian extension of exponent \( l \), and \( H \) the maximal intermediate field of \( \bar{H}/K \) in which \( \infty \) splits completely. The fields \( \bar{H} \) and \( H \) are Galois also over \( k \) as \( \infty \) is the unique prime of \( K \) over \( \infty \). We put \( A = \text{Gal}(H/K) \). Further, let \( \tilde{V} \) and \( V \) be the subgroups of \( K^\times/l \) such that
\[
\tilde{H} = K(v^{1/l} \mid [v] \in \tilde{V}) \quad \text{and} \quad H = K(v^{1/l} \mid [v] \in V)
\]
respectively. The groups \( A, \tilde{V}, V \) as well as \( Cl_K/l = Cl_K/Cl_K \) are naturally regarded as modules over \( \mathbb{F}_l[\Delta] \) since \( \bar{H} \) and \( H \) are Galois over \( k \). By class field theory, we have a canonical isomorphism \( Cl_K/l \cong A \) compatible with the action of \( \Delta \). So, we identify these two modules. We see that \( l/h(k) \) if and only if \((Cl_K/l)(\chi_0)\) is nontrivial from class field theory (cf. [15, p. 368]).

Now, let \( \chi \) be any \( \mathbb{F}_l \)-valued character of \( \Delta \). We prove the following:

**Claim 1.** The dimensions of the four vector spaces
\[
(Cl_K/l)(\chi), \quad (Cl_K/l)(\omega \chi^{-1}), \quad V(\chi), \quad V(\omega \chi^{-1})
\]
over \( \mathbb{F}_l \) are equal.
The desired assertion follows from this.

Let $\mu^a = \mu^\infty \cap K$. Then we easily see that $\widetilde{H} = H(\zeta_{a+1})$. From this, it follows that

$$\dim V(\chi) = \begin{cases} \dim V(\chi) & \text{for } \chi \neq \omega, \\ \dim V(\chi) + 1 & \text{for } \chi = \omega. \end{cases}$$

Here, $\dim(\ast)$ denotes the dimension of $\ast$ over $F$. For each element $[v] \in \widetilde{V}$, the principal divisor $(v)$ is written as $(v) = \mathfrak{A}^l$ for some divisor $\mathfrak{A}$ of $K$. By mapping $[v]$ to the divisor class $[\mathfrak{A}]$ of $\mathfrak{A}$, we obtain the following exact sequence:

$$0 \to \mu^a / \mu^{a-1} \to \widetilde{V} \to \imath Cl_K \to 0.$$ 

This sequence is compatible with the $\Delta$-action. Hence, by (2), we obtain

$$\dim(\imath Cl_K / l)(\chi) = \dim V(\chi)$$

for any $\chi$. On the other hand, the Kummer pairing $A \times V \to \mu_l$, $(\sigma, [v]) \to \langle \sigma, [v]\rangle = (v^{1/l})^{\sigma-1}$ is nondegenerate and satisfies

$$\langle \sigma^\varrho, [v]^{\varrho} \rangle = \langle \sigma, [v]\rangle^{\varrho} = \langle \sigma, [v]\rangle^{\omega(\varrho)}$$

for $\varrho \in \Delta$.

From this, we easily obtain

$$\dim(\imath Cl_K / l)(\chi) = \dim V(\omega \chi^{-1})$$

for any $\chi$. The assertion of Claim 1 follows from (3) and (4). ■

4. Proof of Theorems 1 and 2. We give a proof only for the case $p \neq 2$ (Theorem 1). The case $p = 2$ (Theorem 2) can be proved in a similar way.

We assume that $l \neq p$ and $p \neq 2$. We fix $a \in \mathbb{F}^\times_q$, and write $L_n = L_{n,a}$ for brevity. Putting $Y = (T^{l^n} + a)^{1/2}$, we have

$$L_n = \mathbb{F}_q(Y, (Y^2 - a)^{1/l^n}).$$

Proof of (I) and (III). The prime divisor $\infty_Y$ of $\mathbb{F}_q(Y)$ is totally ramified in the extension $L_n/\mathbb{F}_q(Y)$. Therefore, we see that the condition $l \mid h(L_{n-1})$ implies $l \mid h(L_n)$ by the second corollary of Lemma 1. Hence, it suffices to prove the assertions (I) and (III) only when $n = 1$. We write $L = L_1$ for brevity. Let $\zeta = \zeta_l$, and let $Q = [\mathbb{F}_q(\zeta)]$ so that $\mathbb{F}_Q = \mathbb{F}_q(\zeta)$. Put $\tilde{L} = L \mathbb{F}_Q$. We identify the Galois group $\Delta = \text{Gal}(\mathbb{F}_Q/\mathbb{F}_q)$ with $\text{Gal}(\mathbb{F}_Q(Y)/\mathbb{F}_q(Y))$ and $\text{Gal}(\tilde{L}/L)$ in the obvious way. Let $\infty_Y$ be the unique prime divisor of $\tilde{L}$ over $\infty_Y$.

First, assume that $a = b^2$ with $b \in \mathbb{F}_q^\times$. Put $v = (Y - b)/(Y + b)$. Clearly, we have $[v] \in (\tilde{L}^\infty/l)(\chi_0)$. We see that the cyclic extension $\tilde{L}(v^{1/l})/\tilde{L}$ is
unramified by Lemma 4, and that \( \infty_Y \) splits completely in this extension as \( v \equiv 1 \pmod{(1/Y)} \). Therefore, by Lemma 5, we get \( l \mid h(L) \).

Next, assume that \( \delta_l(q) = 2 \) and \( a \not\in (\mathbb{F}_q^\times)^2 \). The condition \( \delta_l(q) = 2 \) implies \(|\Delta| = |F_Q : F_q| = 2\). Hence, \( a = \alpha^2 \) for some \( \alpha \in F_q \). Put \( v = (Y - \alpha)/(Y + \alpha) \). We have \([v] \in (\bar{L}^\times/\ell)(\omega) \) as \( \delta_l(q) = 2 \). We see that the cyclic extension \( \bar{L}(v^{1/\ell})/\bar{L} \) is unramified and that \( \infty_Y \) splits completely in this extension similarly to the above. Therefore, we get \( l \mid h(L) \) by Lemma 5. The assertions (I) and (III) follow from these.

**Proof of (II).** By (I), it suffices to show that \( l \nmid h(L_n) \) when \( a \not\in (\mathbb{F}_q^\times)^2 \).

So, we assume \( a \not\in (\mathbb{F}_q^\times)^2 \). Let \( Q_n = |F_q(\zeta_{q^n})| \) so that \( F_{Q_n} = F_q(\zeta_{q^n}) \). We put \( \bar{L}_n = L_nF_{Q_n} \). To prove \( l \nmid h(L_n) \), it suffices to show \( l \nmid h(\bar{L}_n) \) because of the first corollary of Lemma 1. As \( \delta_l(q) = |F_Q : F_q| \) is odd, \( |F_{Q_n} : F_q| \) is also odd. Hence, \( a \not\in (\mathbb{F}_{Q_n}^\times)^2 \), and \( Y^2 - a \) is irreducible over \( F_{Q_n} \). Therefore, the extension \( \bar{L}_n \) over \( F_{Q_n}(Y) \) satisfies the assumptions of Lemma 3, and hence, we obtain \( l \nmid h(\bar{L}_n) \).

**5. Proof of Theorem 3.** We assume that \( l = p \). We fix \( a \in \mathbb{F}_q \), and write \( L'_n = L'_{n,a} \) \((n \geq 1)\) for brevity. Putting \( Y = (T^{q^n} + a)^{1/2} \), we have

\[
L'_n = F_q(Y, (Y^2 - a)^{1/p^n}) \quad (n \geq 1).
\]

We put \( L'_0 = F_q(Y) \). Let \( Z = (Y^2 - a)^{1/p^{n-1}} \). Then

\[
L'_{n-1} = F_q(Y, Z) \quad \text{and} \quad L'_n = F_q(Y, Z^{1/p}).
\]

The prime divisor \( \infty_Z \) of \( F_q(Z) \) is ramified in the quadratic extension \( L'_{n-1}/F_q(Z) \). The Artin–Schreier extension \( F_q(Z^{1/p})/F_q(Z) \) is unramified outside \( \infty_Z \) and is totally ramified at \( \infty_Z \). Therefore, we see that the cyclic extension \( L'_n/L'_{n-1} \) of degree \( l = p \) is ramified only at the unique prime of \( L'_{n-1} \) over \( \infty_Z \). Then, by Lemma 2, the condition \( l \mid h(L'_n) \) implies \( l \mid h(L'_{n-1}) \). From this, we obtain the assertion as \( l \nmid h(L'_0) \).

**6. Proof of Theorem 4.** We give a proof only for the case \( p \neq 2 \). The case \( p = 2 \) can be proved in a similar way.

We assume that \( l = 3 \), \( q \equiv -1 \pmod{3} \) and \( p \neq 2 \). Fix \( n \geq 1 \). For \( 1 \leq i \leq n \), we put

\[
N_i = F_q(X_{n-i}) \quad \text{and} \quad M_i = F_q(X_{n-i}, (3X_n + \gamma)^{1/2}).
\]

Then we see from (1) that

\[
N_1 \subseteq N_2 \subseteq \ldots \subseteq N_n = F_q(T), \quad M_1 \subseteq M_2 \subseteq \ldots \subseteq M_n = L''_n
\]
and that $M_i/N_i$ is a quadratic extension. The polynomial $P_i = X_{n-i}^2 + X_{n-i} + 1 \in \mathbb{F}_q[X_{n-i}]$ is irreducible as $q \equiv -1 \mod 3$. We denote by $(P_i)$ the prime divisor of $N_i$ corresponding to the zeros of $P_i$.

To prove Theorem 4, we prepare several claims.

**Claim 2.** The extension $N_{i+1}/N_i$ is cyclic cubic and unramified outside $(P_i)$. We have $(P_i) = (P_{i+1})^3$ in this extension.

**Proof.** Put $Y = X_{n-(i+1)}$ and $Z = X_{n-i}$ for brevity. Then $N_{i+1} = \mathbb{F}_q(Y)$ and $N_i = \mathbb{F}_q(Z)$. By (1), $Y$ is a root of the polynomial $Y^3 - 3ZY^2 - 3(1 + Z)Y - 1$ over $\mathbb{F}_q(Z)$. The discriminant of this polynomial is $3^4(Z^2 + Z + 1)^2$. Hence, $N_{i+1}/N_i$ is a cyclic cubic extension, in which $(P_i)$ is ramified. Since $P_i = Z^2 + Z + 1 = (Y^2 + Y + 1)^3/(9(Y^2 + Y)^2)$, we see that $(P_i) = (P_{i+1})^3$ in $N_{i+1} = \mathbb{F}_q(Y)$. Finally, we see that the other primes are unramified in $N_{i+1}/N_i$ because $N_i$ and $N_{i+1}$ are of genus zero and because of the Riemann–Hurwitz formula for genus of algebraic function fields.

Let $\zeta = \zeta_3$, and $\mathbb{F}_Q = \mathbb{F}_q(\zeta)$ with $Q = q^2$.

**Claim 3.** $\gamma + 3\zeta$ is not a square in $\mathbb{F}_Q^\times$.

**Proof.** Assume, on the contrary, that $\gamma + 3\zeta = (\lambda + \mu\zeta)^2$ for some $\lambda, \mu \in \mathbb{F}_q$. Clearly, $\mu \neq 0$. By the above, we get $\gamma = \lambda^2 - \mu^2$ and $3 = 2\lambda\mu - \mu^2$.

From this, we obtain $3(\lambda/\mu)^2 - 2\gamma(\lambda/\mu) + (\gamma - 3) = 0$.

Hence, the discriminant $4(\gamma^2 - 3\gamma + 9)$ of this quadratic polynomial must be a square in $\mathbb{F}_q^\times$. This contradicts the choice of $\gamma$.

**Claim 4.** The prime $(P_1)$ of $N_1$ remains prime in the quadratic extension $M_1/N_1$.

**Proof.** We see from (1) that $3X_n + \gamma \equiv 3X_{n-1} + \gamma \mod P_1 (= X_{n-1}^2 + X_{n-1} + 1)$. Since $\zeta$ is a root of $P_1$, the assertion follows from Claim 3.

**Claim 5.** We have $3 \nmid h(M_1)$.

**Proof.** Put $Y = X_{n-1}$ and $Z = (3X_n + \gamma)^{1/2}$. Then $M_1 = \mathbb{F}_q(Y, Z)$. We see that the genus of $M_1$ is 2 because exactly 6 prime divisors are ramified in the quadratic extension $M_1/\mathbb{F}_q(\zeta)$. In the following, we view $M_1$ as an extension over $\mathbb{F}_q(Z)$. By (1), $Y$ is a root of the polynomial $Y^3 - (Z^2 + \gamma)Y^2 - (Z^2 - \gamma + 3)Y - 1$.
Quadratic function fields

over \( F_q(Z) \). The discriminant of this polynomial is \( P^2 \) with

\[
P = P(Z) = (Z^2 - \gamma)^2 + 3(Z^2 - \gamma) + 9.
\]

A root \( \alpha \) of \( P(Z) \) satisfies \( \alpha^2 = \gamma + 3\zeta \). Then, by Claim 3, we see that \( \alpha \) is of degree 4 over \( F_q \), and hence, \( P \) is irreducible over \( F_q \). From the above, we see that \( M_1/F_q(Z) \) is a cyclic cubic extension, in which the prime of \( F_q(Z) \) corresponding to the irreducible monic \( P(Z) \) is ramified. Since the genus of \( M_1 \) is 2 and \( \deg(P) = 4 \), we see that the other primes of \( F_q(Z) \) are unramified in \( M_1 \) by the Riemann–Hurwitz formula. Hence, we obtain 3 \( \nmid h(M_1) \) by Lemma 2.

**Claim 6.** Assume that 3 \( \nmid h(M_i) \) and the prime \( (P_i) \) of \( N_i \) remains prime in the quadratic extension \( M_i/N_i \). Then we have 3 \( \nmid h(M_{i+1}) \), and \( (P_{i+1}) \) remains prime in \( M_{i+1}/N_{i+1} \).

**Proof.** Since \( M_{i+1} = M_i N_{i+1} \), we obtain the assertion by using Claim 2 and Lemma 2.

Now, we obtain Theorem 4 for the case \( p \neq 2 \) from Claims 4, 5 and 6.

The case \( p = 2 \) can be proved in a similar way by using, in place of Claim 3, the following:

**Claim 7.** Let \( p = 2 \) and \( q \equiv -1 \mod 3 \). Then \( T^4 + T + 1 \) is irreducible over \( F_q \).

References


Department of Mathematics
Yokohama City University
22-2, Seto, Kanazawa-ku
Yokohama, 236-0027 Japan
E-mail: ichimura@yokohama-cu.ac.jp

Received on 12.2.1999