ACTA ARITHMETICA
121.2 (2006)

Class number divisibility of relative quadratic function fields

by

Yoonjin Lee (Burnaby)

Introduction. Determining the class number of a number field or a function field is one of the central problems in number theory since Gauss. It is known that given an integer n, infinitely many number fields and function fields have class number divisible by n (see for example, Nagell [8] for imaginary quadratic number fields, Yamamoto [12] for real quadratic number fields, and Friesen [1] for real quadratic function fields).

Recently, Kishi and Miyake [3] presented complete descriptions for quadratic number fields to have their ideal class numbers divisible by 3. In fact, they provided necessary and sufficient conditions for the ideal class numbers of quadratic number fields to be divisible by 3. For the case of quadratic function fields, however, there has been no result concerning necessary and sufficient conditions for the ideal class number divisibility by 3, except for the only necessary conditions for the ideal class number divisibility of real quadratic function fields, for instance, in Friesen's work [1].

In this paper, we find complete descriptions for quadratic function fields whose ideal class number is divisible by 3. More importantly, we obtain the results for quadratic extensions of any *global function field* K, and such quadratic extensions are called *relative quadratic* extension fields of K. We want to point out that this work is very general in the sense that the base field K is not necessarily a rational function field any more, but it can be any global function field.

Furthermore, we obtain necessary and sufficient conditions for the divisor class number of a quadratic function field to be divisible by 3. And we also find necessary conditions for relative quadratic extension fields of K to have their divisor class numbers divisible by 3.

1. Preliminaries. We begin with some definitions and notations which will be used throughout the paper.

2000 *Mathematics Subject Classification*: Primary 11R29; Secondary 11R58.
Key words and phrases: class group, class number, quadratic function field.

Let $\mathbb{F}_q$ denote a finite field of order q with q a power of a prime $p > 3$, and let $k = \mathbb{F}_q(T)$ be the rational function field over $\mathbb{F}_q$ with a transcendental element T. Let P_∞ be the *prime at infinity* (or the *infinite place*) of k defined by the negative degree valuation, i.e. $v_{P_\infty}(f) = -\deg(f)$ for $f \in k^*$. For any extension F of k in k_{sep} (= the separable closure of k), let $S(F)$ denote the set of all the primes at infinity of F lying above P_∞. We also let $\mathcal{O}_k = \mathbb{F}_q[T]$ be the ring of polynomials (or *maximal order*) of k, and $\mathcal{O}_F$ the integral closure of $\mathcal{O}_k$ in F.

We assume that K is a finite extension of k. A function field in one variable T over a finite field is called a *global function field*. So, in fact, K is a global function field with constant field $\mathbb{F}_{q^f}$, where f is the *relative degree* of P_∞ in K/k.

Throughout this paper, we fix the following notations:

$\wp_\infty$	a fixed *place* (or *prime divisor*) of K lying above P_∞,
$v_{\wp_\infty}$	a usual discrete valuation corresponding to a place $\wp_\infty$ of F,
$\pi_{\wp_\infty}$	an element of K with $v_{\wp_\infty}(\pi_{\wp_\infty}) = 1$
	(called *prime element* or *uniformizing variable* of $\wp_\infty$),
Cl_F	the ideal class group of $\mathcal{O}_F$,
J_F	the group of divisor classes of degree zero of F,
	which we simply call the *divisor class group* of F,
$h_{\text{id}}(F)$	$\lvert\mathrm{Cl}_F\rvert$, the *ideal class number* of F,
$h_{\text{div}}(F)$	$\lvert J_F\rvert$, the *divisor class number* of F,
ζ_3	a primitive cube root of unity.

We note that the triple F, $\mathcal{O}_F$ and $S(F)$ is analogous to an algebraic number field, its ring of integers and its primes at infinity. In fact, $\mathcal{O}_F$ is the ring of elements in F whose only poles are in $S(F)$. Most importantly, $\mathcal{O}_F$ is a Dedekind domain, and its ideal class group Cl_F is finite.

Any quadratic extension of a global function field K is called a *relative quadratic function field* since quadratic extensions of k are often referred to as quadratic function fields. We note that in this paper the base field K is not necessarily a rational function field k, but it can be an arbitrary global function field. For any finite algebraic extension F of K with the constant field $\mathbb{F}$ of F, if the algebraic closure of $\mathbb{F}$ in F is $\mathbb{F}$, then F is called a *geometric extension* of K.

For any finite extension F of K, the *S-unit group* $E(S)$ of F is defined by

$$E(S) = \{a \in F^* \mid v_\wp(a) = 0, \forall \wp \notin S\}$$

with $S = S(F)$. In fact, $E(S)$ is the unit group of $\mathcal{O}_F$. Furthermore, $E(S)$ is finitely generated of rank $|S|-1$, where $|S|$ is the number of elements in S (refer to [9] for details).

For a finite algebraic extension F of K with constant field $\mathbb{F}$, the S-*regulator* of F, denoted by $R_S^{(q)}$, is defined by the determinant of the $(s-1) \times (s-1)$ minors of M, where M is the $(s-1) \times s$ matrix whose ijth entry is $\log_q |e_i|_{\wp_j}$, where $S := S(F) = \{\wp_1, \dots, \wp_s\}$, $s = |S|$, $\{e_1, \dots, e_{s-1}\}$ is a set of S-units whose projection to $E(S)/\mathbb{F}^*$ is a basis.

A separable extension of a function field K/k is said to be *real* if the prime at infinity P_∞ splits completely in K; the rank of the unit group in this case is maximal as it is for totally real number fields. On the other hand, we call a separable extension K/k *imaginary* if there is only one prime lying above P_∞ in K; then the rank of the unit group is minimal as it is for purely imaginary number fields.

The *group of S-divisors* of F, denoted by $\mathcal{D}_S$, is defined to be the subgroup of $\mathcal{D}_F$ generated by the primes *not in* S. A divisor of the form

$$(a)_S = \prod_{P \notin S} P^{v_P(a)}$$

for some $a \in F^*$ is called a *principal S-divisor*. Let $\mathcal{P}_S$ be the set of all the principal S-divisors. Then $\mathcal{D}_S/\mathcal{P}_S$ is isomorphic to Cl_F (we can refer to [11, Theorem 14.5]).

Consider a map $\tau : \mathcal{D}_F \to \mathcal{D}_S$ defined by

$$\tau(D) = \prod_{P \notin S(F)} P^{v_P(D)},$$

where $\mathcal{D}_F$ is the group of divisors of F.

The relation between the divisor class group and the ideal class group is given in the following theorem. We can refer to [11, Lemma 14.3 and Proposition 14.1] for details.

THEOREM 1.1. *Let F be any finite extension of K, $d = \gcd\{\deg(\wp) \mid \wp \in S(F)\}$, and $R_S^{(q)}$ be the S-regulator of F with $S = S(F)$. From the map τ defined as above the following exact sequence is induced*:

$$0 \to \mathrm{Ker}(\tau) \to J_F \xrightarrow{\tau} \mathrm{Cl}_F \to \mathbb{Z}/d\mathbb{Z} \to 0. \tag{1}$$

Then $\mathrm{Ker}(\tau)$ has the order $dR_S^{(q)}/\prod_{\wp \in S} \deg(\wp)$, and the cokernel of τ is cyclic of order d.

The *Hilbert class field* of F with respect to $\mathcal{O}_F$, denoted by H_F, is the maximal unramified abelian extension of F in F_{sep} in which every prime in $S(F)$ splits completely, where F_{sep} is the separable closure of F.

We quote from [10, Theorem 1.3] the following important result of class field theory.

THEOREM 1.2. *$[H_F : F]$ is finite. The Artin symbol $(\,\cdot\,, H_F/F)$ induces an isomorphism*

$$\mathrm{Cl}_F \simeq \mathrm{Gal}(H_F/F).$$

The constant field of H_F is $\mathbb{F}_{q^\delta}$, where $S(F) = \{\wp_1, \dots, \wp_s\}$ and δ is the greatest common divisor of $\{\deg(\wp_i) \mid 1 \le i \le s\}$.

The following class-field-theoretic interpretation results immediately from the theory of the Hilbert class field [10].

THEOREM 1.3. *Let A be a finite abelian group. Then Cl_F contains a subgroup isomorphic to A if and only if there exists an unramified abelian extension H of F with $\mathrm{Gal}(H/F) \cong A$ in which every place from $S(F)$ splits completely.*

When L_1/L_2 is a finite algebraic extension of fields, $\mathfrak{p}$ is a prime of L_2, and $\mathfrak{P}$ is a prime of L_1 lying above $\mathfrak{p}$, we denote by $e(\mathfrak{P}/\mathfrak{p})$ the *ramification index* of $\mathfrak{P}$ over $\mathfrak{p}$ and by $f(\mathfrak{P}/\mathfrak{p})$ the *relative degree* of $\mathfrak{P}$ over $\mathfrak{p}$. We note that the ramification index and the relative degree behave transitively in towers. In detail, let $L_3 \subseteq L_2 \subseteq L_1$ be a tower of function fields with L_1/L_2 and L_2/L_3 finite algebraic extensions. If $\mathfrak{P}$ is a prime of L_1, and $\mathfrak{p}$ and P are the primes lying below $\mathfrak{P}$ in L_2 and L_3 respectively, then

$$e(\mathfrak{P}/P) = e(\mathfrak{P}/\mathfrak{p}) \cdot e(\mathfrak{p}/P), \qquad f(\mathfrak{P}/P) = f(\mathfrak{P}/\mathfrak{p}) \cdot f(\mathfrak{p}/P).$$

If L_1/L_2 is a Galois extension and g primes of L_1 lie above $\mathfrak{p}$, then

$$e(\mathfrak{P}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{p}) \cdot g = [L_1 : L_2].$$

In addition, for any primes $\mathfrak{P}, \mathfrak{P}'$ lying over $\mathfrak{p}$,

$$e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}'/\mathfrak{p}) \quad \text{and} \quad f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}'/\mathfrak{p}).$$

Hence, when L_1/L_2 is a Galois extension, $e_{L_1/L_2}(\mathfrak{p})$ (resp. $f_{L_1/L_2}(\mathfrak{p})$) denotes the *ramification index* (resp. *relative degree*) of $\mathfrak{p}$ in L_1/L_2, and $g_{L_1/L_2}(\mathfrak{p})$ is the total number of primes of L_1 lying above $\mathfrak{p}$.

We note the following well known facts. Suppose that F'/F is a finite separable extension of function fields, F_1, F_2 are intermediate fields of F'/F such that $F' = F_1F_2$ (the compositum of F_1 and F_2), and P is a prime of F. If P splits completely in F_1/F and F_2/F, then P also splits completely in F'/F. In addition, if P is unramified in F_1/F and F_2/F, then it is also unramified in F'/F.

2. A criterion for ideal class number divisibility by 3. In this section we find the complete description for the relative quadratic function fields whose ideal class numbers are divisible by 3. Kishi and Miyake [3] worked on the ideal class number divisibility by 3 for the case of quadratic number fields. We use the notations introduced in Section 1.

Let $g(X) = X^3 - tX - t$ with $t \in K^*$ (not necessarily $t \in \mathcal{O}$). In fact, the $v_{\wp_\infty}$ values of coefficients of $g(X)$ are not necessarily nonnegative at $\wp_\infty$; but, we can make them nonnegative at $\wp_\infty$ by repeating the parametrization $X \to \pi X$, where π denotes $\pi_{\wp_\infty}$ for $\wp_\infty$. If $v_{\wp_\infty}(t)$ is negative even, i.e. $v_{\wp_\infty}(t) = 2n < 0$, then we obtain

$$\widetilde{g}(X) = X^3 - (t\pi^{2n})X - (t\pi^{3n}) = X^3 - t'X - t'', \tag{2}$$

with $t' = t\pi^{2n}$ and $t'' = t\pi^{3n}$. Thus, $v_{\wp_\infty}(t') = 0$ and $v_{\wp_\infty}(t'') > 0$. On the other hand, if $v_{\wp_\infty}(t)$ is negative odd, that is, $v_{\wp_\infty}(t) = 2n+1 < 0$, then we get

$$\widetilde{g}(X) = X^3 - (t\pi^{2(n+1)})X - (t\pi^{3(n+1)}) = X^3 - t'X - t'', \tag{3}$$

where $t' = t\pi^{2(n+1)}$ and $t'' = t\pi^{3(n+1)}$; so, $v_{\wp_\infty}(t') = 1, v_{\wp_\infty}(t'') > 1$. Therefore, we have the following two possible cases:

$$v_{\wp_\infty}(t') = 0,\ v_{\wp_\infty}(t'') > 0 \quad \text{or} \quad v_{\wp_\infty}(t') = 1,\ v_{\wp_\infty}(t'') > 1.$$

Furthermore, when $v_{\wp_\infty}(t)$ is a positive integer, by the repetition of the parametrization $X \to X/\pi$, we may assume that $\widetilde{g}(X)$ has $v_{\wp_\infty}(t'') < 3$, where

$$\widetilde{g}(X) = X^3 - \left(\frac{t}{\pi^{2n}}\right)X - \left(\frac{t}{\pi^{3n}}\right) = X^3 - t'X - t'', \tag{4}$$

with $t' = t/\pi^{2n}$ and $t'' = t/\pi^{3n}$. We note that $v_{\wp_\infty}(t') > v_{\wp_\infty}(t'')$.

We therefore have seen the following:

(i) If $v_{\wp_\infty}(t) = 2n$ is negative even, then with $t' = t\pi^{2n}$ and $t'' = t\pi^{3n}$ as in (2), we have $v_{\wp_\infty}(t') = 0,\ v_{\wp_\infty}(t'') > 0$.

(ii) If $v_{\wp_\infty}(t) = 2n+1$ is negative odd, then with $t' = t\pi^{2(n+1)}$ and $t'' = t\pi^{3(n+1)}$ as in (3), we have $v_{\wp_\infty}(t') = 1,\ v_{\wp_\infty}(t'') > 1$.

(iii) If $v_{\wp_\infty}(t)$ is a positive integer, then with $t' = t/\pi^{2n}$ and $t'' = t/\pi^{3n}$ as in (4), we have $v_{\wp_\infty}(t'') < 3$, $v_{\wp_\infty}(t') > v_{\wp_\infty}(t'')$.

In any of these three cases, $\widetilde{g}(X)$ generates the same cubic field as $g(X)$.

The following theorem is the main result of this section.

Theorem 2.1. *If the ideal class number of K is divisible by* 3, *then the ideal class number of any quadratic extension F of K is also divisible by* 3.

If the ideal class number of K is not divisible by 3, *then for any quadratic extension F of K, the ideal class number of F is divisible by* 3 *if and only if F can be represented as $K(\sqrt{d})$ with d defined as follows.*

Let $g(X) = X^3 - tX - t$ with $t \in K^*$, $d = 4t - 27$ be nonsquare, and u_t be the unit part of t with respect to $\wp_\infty$, that is,

$$u_t = t \cdot (\pi_{\wp_\infty})^{-v_{\wp_\infty}(t)}.$$

Assume $g(X)$ is irreducible over K, and all the zeroes of t have order divisible by 3, *equivalently*, $3 \mid v_P(t)$ *for any prime P in K such that $v_P(t) > 0$. In addition, we assume that $g(X)$ satisfies one of the following conditions*:

(i) *$v_{\wp_\infty}(t)$ is odd.*

(ii) *$v_{\wp_\infty}(t) = 2n$ is negative even, u_t is nonsquare in $\mathbb{F}_{q^f}$, and $\left(\frac{t'}{\wp_\infty}\right) = -1$ with $t' = t\pi^{2n}$ as in* (2).

(iii) *$v_{\wp_\infty}(t) = 2n$ is negative even, u_t is square in $\mathbb{F}_{q^f}$, and $\left(\frac{t'}{\wp_\infty}\right) = 1$ with $t' = t\pi^{2n}$ as in* (2).

The polynomial discriminant of $g(X)$ is $t^2 d$, and is not a square; thus the minimal splitting field L of $g(X)$ contains a quadratic function field $K(\sqrt{d})$, and $\mathrm{Gal}(L/K) \simeq S_3$, the symmetric group. If K_1, K_2 and K_3 are the fixed fields of the three elements of order 2 in $\mathrm{Gal}(L/K)$, then $K(\theta)$ is certainly one of K_i's. We also observe that all K_i's are isomorphic and their composite field is L.

The first part of Theorem 2.1 is proved in the following proposition.

Proposition 2.2. *If the ideal class number of K is divisible by* 3, *then the ideal class number of any quadratic extension F of K is also divisible by* 3.

Proof. Let $\mathfrak{P}_\infty$ be a prime of F lying above $\wp_\infty$. If the ideal class number of K is divisible by 3, then from Theorem 1.2 or Theorem 1.3, it follows that there exists an unramified cyclic cubic extension field $\widetilde{K}$ of K where $\wp_\infty$ splits completely. Therefore, $\widetilde{K} \subseteq H_K$, where H_K is the Hilbert class field of K. Let M be the composite field of $\widetilde{K}$ and F. Since $\wp_\infty$ splits completely in $\widetilde{K}$, $\wp_\infty$ should split completely in M. This implies that $\mathfrak{P}_\infty$ in F splits completely in M. Therefore, M is an unramified cyclic cubic extension of F in which $\mathfrak{P}_\infty$ splits completely, so M is contained in the Hilbert class field H_F of F. The assertion therefore follows immediately by Theorem 1.3. ∎

In the rest of this section we will prove the second part of Theorem 2.1.

We note that $3 \mid h_{\mathrm{id}}(K)$ if and only if there exists an unramified cyclic cubic extension field L of K which splits completely at $\wp_\infty$ by Theorem 1.3. It is therefore sufficient to find necessary and sufficient conditions under which K has an unramified cyclic cubic extension field L where $\wp_\infty$ splits completely.

Every cyclic cubic extension of a quadratic extension field of K is the splitting field L of a cubic equation of the form

$$X^3 - tX - t = 0 \tag{5}$$

with t in K^* as in [3, Section 2]. In detail, let a cubic extension $K(\theta)$ of K be generated by an irreducible polynomial of θ over K, $\mathrm{Irr}(\theta) = X^3 - aX - b$ with $b \neq 0$. Then without loss of generality we may assume that $a \neq 0$ since

$\mathrm{Irr}\big(\theta + 1/\theta\big) = X^3 - 3X - \big(b + 1/b\big)$ also generates the same field $K(\theta)$. As both a and b are nonzero, we can use

$$\mathrm{Irr}\left(\frac{a}{b}\,\theta\right) = X^3 - \frac{a^3}{b^2}\,X - \frac{a^3}{b^2}$$

as the generating polynomial of $K(\theta)$. We note that $\mathrm{Gal}(K(\theta)/K) \simeq S_3$ (= symmetric group on three elements).

$$\begin{tikzcd}[column sep=small, row sep=small]
 & L \arrow[dd, dash] \\
K(\theta) \arrow[ur, dash] \arrow[dd, dash] & \\
 & K(\sqrt{d}) \\
K \arrow[ur, dash] &
\end{tikzcd}$$

We need to determine the conditions under which $L/K(\sqrt{d})$ is unramified at every finite prime; for that the following lemma is necessary. (We can also refer to [6, Lemma 2.2].)

LEMMA 2.3. *Let P be a prime of K (or finite place of K), and $\mathfrak{P}$ be a prime of $K(\sqrt{d})$ lying above P. Then P is totally ramified in $K(\theta)$ if and only if $\mathfrak{P}$ is ramified in $L/K(\sqrt{d})$, where θ is a root of equation* (5).

Proof. Let P' be the prime in L lying above P. First, we observe that P cannot be totally ramified in L/K. Otherwise, the *inertia group* $I(P'/P)$ of P in L/K is of order 6, and it cannot be cyclic; but $I(P'/P)$ has to be cyclic since L/K is *tamely ramified*. Thus, we also note that the inertia group of P in L/K is of order at most 3.

If $\mathfrak{P}$ is ramified in $L/K(\sqrt{d})$, then the inertia group of P in L/K has order 3; hence $K(\sqrt{d})/K$ is unramified at P. We then have two possible cases: P splits or is inert in $K(\sqrt{d})$. If P is inert in $K(\sqrt{d})$, then $e_{L/K}(P) = 3$, $f_{L/K}(P) = 2$ and $g_{L/K}(P) = 1$. Thus, there is only one prime in $K(\theta)$ above P. If P is inert in $K(\theta)$, then this contradicts $f_{L/K}(P) = 2$, so P must be totally ramified in $K(\theta)$. In the case that P splits in $K(\sqrt{d})$, there are two primes in L above P, each with ramification index 3 and relative degree 1. It is also easy to see that P must be totally ramified in $K(\theta)$.

For the other direction, assume that P is totally ramified in $K(\theta)$. Then there are at most two primes in L lying above P. For a contradiction, we assume that $\mathfrak{P}$ is unramified in L. As $L/K(\sqrt{d})$ is a Galois extension, we have only two possibilities: $\mathfrak{P}$ splits completely in L, or $\mathfrak{P}$ is inert in L. It is easy to find contradictions in both cases. ∎

In the following lemma, we find the conditions for $L/K(\sqrt{d})$ to be an unramified extension at finite places.

Lemma 2.4. *Let P be a prime of K (or finite place of K). Then P is totally ramified in $K(\theta)$ if and only if* $v_P(t) \not\equiv 0 \pmod 3$ *for any prime P with $v_P(t) > 0$.*

Proof. Let $\widetilde{P}$ be a prime of $K(\theta)$ above P. We then observe that

$$v_{\widetilde{P}}(\theta) = \frac{1}{3}\, v_P(N(\theta)) = \frac{1}{3}\, v_P(t),$$

where $N(\theta)$ denotes the norm of θ from $K(\theta)$ to K. Thus, the result follows immediately. ∎

It thus follows from Lemmas 2.3 and 2.4 that a necessary and sufficient condition for $L/K(\sqrt{d})$ to be an unramified extension is that $v_P(t) \equiv 0 \pmod 3$ for any prime P with $v_P(t) > 0$.

As before, $\wp_\infty$ denotes a prime of K (or infinite place of K) lying above P_∞ in k. Throughout what follows, let $\mathfrak{P}_\infty$ be a prime of $K(\sqrt{d})$ lying above $\wp_\infty$, $\widetilde{\mathfrak{P}}_\infty$ a prime of L lying above $\wp_\infty$, and $\mathcal{P}_\infty$ a prime of $K(\theta)$ lying above $\wp_\infty$.

It remains to determine the conditions under which $\mathfrak{P}_\infty$ splits completely in $L/K(\sqrt{d})$. In the following lemma, we observe how $\wp_\infty$ splits in $K(\theta)/K$ depending on the coefficients of $\widetilde{g}(X)$.

Lemma 2.5. *The following is the splitting behavior of $\wp_\infty$ in $K(\theta)/K$ depending on the coefficients of $g(X)$.*

If $v_{\wp_\infty}(t)$ is a positive integer, then $\wp_\infty$ is totally ramified in $K(\theta)$.

If $v_{\wp_\infty}(t)$ is a negative integer, then with $\widetilde{g}(X) = X^3 - t'X - t''$ such that $v_{\wp_\infty}(t')$ and $v_{\wp_\infty}(t'')$ are positive integers as given in (2) *and* (3), *we have the following two cases*:

- (i) *If $v_{\wp_\infty}(t) = 2n$ is negative even, we have $t' = t\pi^{2n}$ as in* (2). *Then $\left(\frac{t'}{\wp_\infty}\right) = 1$ if and only if $\wp_\infty$ splits completely in $K(\theta)$, and $\left(\frac{t'}{\wp_\infty}\right) = -1$ if and only if $\wp_\infty$ splits into two primes in $K(\theta)$ with $\wp_\infty = \mathcal{P}_1\mathcal{P}_2$.*
- (ii) *If $v_{\wp_\infty}(t) = 2n + 1$ is negative odd, then with $t' = t\pi^{2(n+1)}$ as in* (3), *$\wp_\infty$ splits into two primes with ramification in $K(\theta)$, i.e. $\wp_\infty = \mathcal{P}_1\mathcal{P}_2^2$.*

Proof. We use the method of *Newton polygon* and *Kummer's Criterion* [2, Theorem 23].

If $v_{\wp_\infty}(t)$ is a positive integer, as seen in (4) we may assume that $v_{\wp_\infty}(t'') < 3$. As $v_{\wp_\infty}(t') > v_{\wp_\infty}(t'')$, the Newton polygon of $\widetilde{g}(X)$ with respect to $\wp_\infty$ has only one side of slope $1/3$ or $-1/3$, therefore $\wp_\infty$ is totally ramified in $K(\theta)$.

If $v_{\wp_\infty}(t)$ is negative even, then from (2) we have $v_{\wp_\infty}(t') = 0$, $v_{\wp_\infty}(t'') > 0$. Thus, Newton polygon has only one side of positive slope, so $\wp_\infty$ splits into two primes or three primes in $K(\theta)$. And we have $\widetilde{g}(X) \equiv X(X^2 - t')$ (mod $\wp_\infty$). Our assertion therefore follows immediately depending on the conditions $\left(\frac{t'}{\wp_\infty}\right) = 1$ or $\left(\frac{t'}{\wp_\infty}\right) = -1$.

If $v_{\wp_\infty}(t)$ is negative odd, we have $v_{\wp_\infty}(t') = 1$, $v_{\wp_\infty}(t'') > 1$ by (3). Hence, there are two sides in the Newton polygon, and one of them is of slope $1/2$. We therefore have $\wp_\infty = \mathcal{P}_1\mathcal{P}_2^2$. ∎

The following lemma shows explicit necessary and sufficient conditions on t for ramification behavior of $\wp_\infty$ in $K(\sqrt{d})/K$ with $d = 4t-27$. It can be proved in a similar way to [11, Proposition 14.6], thus the proof is omitted.

LEMMA 2.6. *In each of the three possible cases for the ramification of $\wp_\infty$ in $K(\sqrt{d})/K$ with $d = 4t - 27$, we have the following explicit criteria*:

(i) *$K(\sqrt{d})$ is totally ramified at $\wp_\infty$ if and only if $v_{\wp_\infty}(t)$ is odd.*
(ii) *$K(\sqrt{d})$ is inert at $\wp_\infty$ if and only if $v_{\wp_\infty}(t)$ is even and u_t is a nonsquare in $\mathbb{F}_{q^f}$.*
(iii) *$K(\sqrt{d})$ splits completely at $\wp_\infty$ if and only if $v_{\wp_\infty}(t)$ is even and u_t is a square in $\mathbb{F}_{q^f}$.*

Now we determine the conditions under which $\mathfrak{P}_\infty$ splits completely in $L/K(\sqrt{d})$. We have three possible cases for the ramification of $\wp_\infty$ in $K(\sqrt{d})/K$. In the following proposition, for each case we find the necessary and sufficient conditions for $\mathfrak{P}_\infty$ to split completely in $L/K(\sqrt{d})$.

PROPOSITION 2.7. *Depending on the ramification of $\wp_\infty$ in $K(\sqrt{d})$, we find the following conditions for $\mathfrak{P}_\infty$ to split completely in $L/K(\sqrt{d})$*:

(i) *Assume that $K(\sqrt{d})$ is totally ramified at $\wp_\infty$. Then $\mathfrak{P}_\infty$ splits completely in $L/K(\sqrt{d})$.*
(ii) *Assume that $K(\sqrt{d})$ is inert at $\wp_\infty$. Then $\mathfrak{P}_\infty$ splits completely in $L/K(\sqrt{d})$ if and only if $v_{\wp_\infty}(t) = 2n$ is negative even and $\left(\frac{t'}{\wp_\infty}\right) = -1$ with $t' = t\pi^{2n}$.*
(iii) *Assume that $K(\sqrt{d})$ splits completely at $\wp_\infty$. Then $\mathfrak{P}_\infty$ splits completely in $L/K(\sqrt{d})$ if and only if $v_{\wp_\infty}(t) = 2n$ is negative even and $\left(\frac{t'}{\wp_\infty}\right) = 1$ with $t' = t\pi^{2n}$.*

Proof. Let $\mathfrak{P}_\infty$ be a prime of $K(\sqrt{d})$ lying above $\wp_\infty$, and let $\widetilde{\mathfrak{P}}_\infty$ be a prime of L lying above $\mathfrak{P}_\infty$.

(i) We assume that $K(\sqrt{d})$ is totally ramified at $\wp_\infty$. Since $L/K(\sqrt{d})$ cannot be totally ramified at $\mathfrak{P}_\infty$, $L/K(\sqrt{d})$ is either inert at $\mathfrak{P}_\infty$, or splits completely at $\mathfrak{P}_\infty$.

We claim that $\mathfrak{P}_\infty$ splits completely in $L/K(\sqrt{d})$. If $L/K(\sqrt{d})$ is inert at $\mathfrak{P}_\infty$, then $\wp_\infty$ is neither totally ramified nor totally inert in L/K, but rather a mix of being ramified and being inert. The *relative degree*

$f(\widetilde{\mathfrak{P}}_\infty/\wp_\infty)$ must be 3; so $\wp_\infty$ is totally inert in each of the cubic subfields of L, hence the inertia field would be L. This contradicts the fact that L/K is ramified.

(ii) Suppose that $\wp_\infty$ is inert in $K(\sqrt{d})$. It is then easy to verify that $L/K(\sqrt{d})$ should split completely at $\wp_\infty$ if and only if $K(\theta)$ splits into two primes such that each of their relative degree is 1 and 2 with $\wp_\infty = \mathcal{P}_1\mathcal{P}_2$ in L, and this will only happen in the case that $v_{\wp_\infty}(t)$ is negative even and $(\frac{t'}{\wp_\infty}) = -1$ from Lemma 2.5.

(iii) Assume that $\wp_\infty$ splits completely in $K(\sqrt{d})$. Then it is easy to see that $\mathfrak{P}_\infty$ in $K(\sqrt{d})$ splits completely in L if and only if $\wp_\infty$ splits completely in $K(\theta)$, equivalently $v_{\wp_\infty}(t)$ is negative even and $\left(\frac{t'}{\wp_\infty}\right) = 1$ by Lemma 2.5. ∎

Combining Lemma 2.3 through Proposition 2.7, we have completed proving Theorem 2.1.

In particular, when K is just a rational function field $k = \mathbb{F}_q(T)$, the following corollary is obtained immediately. We recall that $v_{P_\infty}(g) = -\deg(g)$ for $g \in k^*$, and we note that $P_\infty = \left(\frac{1}{T}\right)$.

Corollary 2.8. *For any quadratic extension F of $k = \mathbb{F}_q(T)$, the ideal class number of F is divisible by 3 if and only if F can be represented as $k(\sqrt{d})$ with d defined as follows.*

Let $g(X) = X^3 - tX - t$ with $t \in k^*$, $d = 4t - 27$ be nonsquare, and $u_t \in \mathbb{F}_q$ be the leading coefficient of t. Assume $g(X)$ is irreducible over k, and all the zeroes of t have order divisible by 3, equivalently, $3 \mid v_P(t)$ for any prime P in k such that $v_P(t) > 0$. In addition, we assume that $g(X)$ satisfies one of the following conditions:

(i) $\deg(t)$ *is odd.*

(ii) $\deg(t) = 2n$ *is positive even, u_t is nonsquare in $\mathbb{F}_q$, and* $\left(\frac{t'}{\wp_\infty}\right) = -1$ *with $t' = t/T^{2n}$ as in* (2).

(iii) $\deg(t) = 2n$ *is positive even, u_t is square in $\mathbb{F}_q$, and* $\left(\frac{t'}{\wp_\infty}\right) = 1$ *with $t' = t/T^{2n}$ as in* (2).

Remark 2.9. We want to point out that the following result by Friesen [1] can be derived immediately from Theorem 2.1 for the ideal class number divisibility by 3.

Let $f \in \mathbb{F}_q[T] \setminus \mathbb{F}_q$, $a \in \mathbb{F}_q^*$, and $M = f^6 + a^2$. If M is monic and squarefree, then the ideal class number of the real quadratic function field $k(\sqrt{M})$ is divisible by 3.

In Corollary 2.8, we let $4t = f^6 + a^2 + 27$ such that f is a monic polynomial in $\mathbb{F}_q[T] \setminus \mathbb{F}_q$ and $a \in \mathbb{F}_q^*$; so $d = 4t - 27 = f^6 + a^2$. Then certainly such

t satisfies all the conditions (with condition (iii)) in Corollary 2.8. It thus follows that the ideal class number of $k(\sqrt{d}) = k(\sqrt{f^6 + a^2})$ is divisible by 3.

3. Divisor class number divisibility by 3. Let $K(\sqrt{d})$ with $d = 4t - 27$ be defined as in Section 2, and let q be an odd prime such that $q \equiv -1 \pmod 3$, so that $\zeta_3 \notin \mathbb{F}_q$. In this section we work on the divisor class numbers of relative quadratic function fields F in terms of divisibility by 3. Basically, we use the relation between the divisor class group and the ideal class group, some results on the divisor class group rank in [7], and the results obtained in Section 2.

If A is an abelian group and m is a positive integer, the *m-rank* of A is defined to be the maximal number r such that A contains a subgroup isomorphic to the direct sum of r copies of $\mathbb{Z}/m\mathbb{Z}$. We define $A(m)$ as the maximal subgroup of A of exponent m. In fact $A(m) \simeq A/A^m$.

The composite field of $K(\zeta_3)$ and F has another geometric quadratic extension F' of K. In fact, F and F' are related by *reflection characters* (refer to [4] for details), and their 3-ranks of the ideal class groups can be compared as in Theorem 3.1 below. This is a special case of [7, Theorem 3.3] (or refer to [4]), so the proof is omitted. It compares the 3-ranks of two ideal class groups Cl_F and $\mathrm{Cl}_{F'}$.

THEOREM 3.1. *Let r be the 3-rank of Cl_F, r' be the 3-rank of $\mathrm{Cl}_{F'}$, and let the degree of $\wp_\infty$ be odd. Then $r' = r$ or $r' = r + 1$.*

We also have a clear relationship between two divisor class groups J_F and $J_{F'}$ (a special case of [7, Theorem 2.1]):

THEOREM 3.2. *Let q be an odd prime such that $q \equiv -1 \pmod 3$. Then $J_F(3)$ is isomorphic to $J_{F'}(3)$.*

We can deduce the following lemma from Theorem 1.1 (or refer to [7, Lemma 2.5]).

LEMMA 3.3. *Let F be a quadratic extension of K such that $\wp_\infty$ in K is ramified or inert in F and $\deg(\wp_\infty)$ is not divisible by 3. Then $J_F(3) \simeq \mathrm{Cl}_F(3)$.*

What follows is the main result of this section. For any quadratic extension of K such that there is only one prime in F lying above $\wp_\infty$, we obtain sufficient and necessary conditions for the divisor class number of F to be divisible by 3. On the other hand, for any quadratic extension of K such that $\wp_\infty$ splits completely in F, we also find necessary conditions for its divisor class number divisibility by 3.

THEOREM 3.4. *Let F be a quadratic extension of K such that $\deg(\wp_\infty)$ is odd and is not divisible by 3. Then we have the following two cases:*

Assume that there is only one prime in F lying above $\wp_\infty$ (that is, $\wp_\infty$ is inert or ramified in F). Then the divisor class number $h_{\mathrm{div}}(F)$ of F is divisible by 3 *if and only if F can be represented as $K(\sqrt{d})$ such that d is defined as in Theorem* 2.1 (*with condition* (i) *or* (ii)).

Let $\wp_\infty$ split completely in F. If F can be represented as $K(\sqrt{d})$ such that d is defined as in Theorem 2.1 *with condition* (iii), *then the divisor class number $h_{\mathrm{div}}(F)$ of F is divisible by* 3.

Proof. We first assume that $\wp_\infty$ is inert or totally ramified in F/K. Then F is imaginary, so the regulator of F is trivial. From Lemma 3.3, it follows immediately that $\mathrm{Cl}_F(3) \simeq J_F(3)$. If F can be written as $K(\sqrt{d})$ such that d is defined as in Theorem 2.1 with condition (i) or (ii), then $3 \mid h_{\mathrm{id}}(F)$ by Theorem 2.1. It thus follows immediately that $3 \mid h_{\mathrm{div}}(F)$ since $\mathrm{Cl}_F(3) \simeq J_F(3)$. For the converse, assuming that $3 \mid h_{\mathrm{div}}(F)$, we have $3 \mid h_{\mathrm{id}}(F)$ since $\mathrm{Cl}_F(3) \simeq J_F(3)$. Thus, from Theorem 2.1, F must be represented as $K(\sqrt{d})$ such that d is defined as in Theorem 2.1 with condition (i) or (ii).

Now we assume that $\wp_\infty$ splits completely in F/K. Then it is easy to see that $\wp_\infty$ is inert or totally ramified in F'/K (refer to [7, Lemma 2.5]). Then if F can be written as $K(\sqrt{d})$ such that d is defined as in Theorem 2.1 with condition (iii), then $3 \mid h_{\mathrm{id}}(F)$ by Theorem 2.1. This implies that $r \geq 1$, thus $r' \geq 1$ by Theorem 3.1, i.e. $\mathrm{Cl}_{F'}$ contains $\mathbb{Z}/3\mathbb{Z}$ as a subgroup. We have $\mathrm{Cl}_{F'}(3) \simeq J_{F'}(3)$ by Lemma 3.3. From Theorem 3.2 we also have $J_{F'}(3) \simeq J_F(3)$, therefore $J_F(3)$ contains $\mathbb{Z}/3\mathbb{Z}$ as a subgroup; so $3 \mid h_{\mathrm{div}}(F)$. ∎

In particular, when the base field K is just a rational function field $k = \mathbb{F}_q(T)$, we can obtain necessary and sufficient conditions for the divisor class number of F to be divisible by 3 with an additional condition for the real quadratic case. Therefore, if the base field K is a rational function field $\mathbb{F}_q(T)$, then the result of the following corollary is stronger than Theorem 3.4.

COROLLARY 3.5. *Let k be a rational function field $\mathbb{F}_q(T)$, and F be a quadratic function field. Then the divisor class number $h_{\mathrm{div}}(F)$ of F is divisible by* 3 *if and only if F can be represented as $k(\sqrt{d})$ with d defined as in Corollary* 2.8.

For the proof of Corollary 3.5 we need the following result in [5] on the condition distinguishing the 3-rank difference between two ideal class groups Cl_F and $\mathrm{Cl}_{F'}$. This is a special case of the result in [5, Theorem 3.1].

THEOREM 3.6. *Let F and F' be quadratic function fields defined as before, F be real, and F' be imaginary. If* 3 *does not divide the regulator R of F, then $r' = r$. Equivalently, if $r' = r + 1$, then* 3 *divides R.*

Proof of Corollary 3.5. We have two possible cases: either F is imaginary, or F is real. It is sufficient to show the sufficient condition for the divisor class number of F to be divisible by 3 when F is real; the other case follows immediately from Theorem 3.4.

If $3 \mid h_{\mathrm{div}}(F)$, then $J_F(3)$ contains $\mathbb{Z}/3\mathbb{Z}$ as a subgroup. In fact, $J_F(3) \simeq J_{F'}(3)$ by Theorem 3.2. Furthermore, $J_{F'}(3) \simeq \mathrm{Cl}_{F'}(3)$ by Lemma 3.3; this implies that $r' \geq 1$. From Theorem 3.6, we have $r' = r$ since the regulator of F is not divisible by 3. Thus, $r \geq 1$, that is, $3 \mid h_{\mathrm{id}}(F)$. Therefore, from Theorem 2.1, F can be represented by $K(\sqrt{d})$ as described in Corollary 2.8. ■

Acknowledgements. Part of this work was done while the author was visiting KIAS (Korea Institute for Advanced Study) during the summer of 2004. The author expresses her gratitude to the Institute.

References

[1] C. Friesen, *Class number divisibility in real quadratic function fields*, Canad. Math. Bull. 35 (1992), 361–370.

[2] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Univ. Press, Cambridge, 1993.

[3] Y. Kishi and K. Miyake, *Parametrization of the quadratic fields whose class numbers are divisible by three*, J. Number Theory 80 (2000), 209–217.

[4] Y. Lee, *Cohen–Lenstra heuristics and the Spiegelungssatz: function fields*, ibid. 106 (2004), 187–199.

[5] —, *The Scholz theorem in function fields*, preprint.

[6] —, *The unit rank classification of a cubic function field by its discriminant*, Manuscripta Math. 116 (2005), 173–181.

[7] Y. Lee and A. Schweizer, *A reflection theorem for relative-quadratic function fields*, preprint.

[8] T. Nagel, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Hamburg. Univ. 1 (1922), 140–150.

[9] M. Rosen, *S-units and S-class group in algebraic function fields*, J. Algebra 26 (1973), 98–108.

[10] —, *The Hilbert class field in function fields*, Expo. Math. 5 (1987), 365–378.

[11] —, *Number Theory in Function Fields*, Springer, New York, 2002.

[12] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. 7 (1970), 57–76.

Department of Mathematics
Simon Fraser University
Burnaby, British Columbia
Canada V5A 1S6
E-mail: yoonjinl@sfu.ca

Received on 23.4.2005
and in revised form on 5.10.2005 (4982)