TOKYO J. MATH.
VOL. 14, NO. 1, 1991

Cyclotomic Function Fields with Divisor Class Number One

Masanari KIDA and Naoki MURABAYASHI

Waseda University

(Communicated by Y. Shimizu)

Introduction.

Let k be a rational function field over the finite field $\boldsymbol{F}_q$ with q elements. In 1974 D. R. Hayes [Ha1] constructed the maximal abelian extension of k developing an idea of Carlitz. In his construction he uses "cyclotomic" function fields which are closely analogous to classical cyclotomic extensions of the rational number field.

In this paper we give genus formulae for the maximal "real" subfields of cyclotomic function fields, and apply the formulae to the determination of cyclotomic function fields and their maximal real subfields with divisor class number one respectively.

1. Preliminaries.

In this section we provide a quick review of Carlitz-Hayes' theory.

Let k be as in Introduction. We fix a generator T of k such that $k=\boldsymbol{F}_q(T)$ and put $R=\boldsymbol{F}_q[T]$. We denote by ∞ the prime divisor corresponding to the pole of T i.e. $\mathrm{ord}_\infty(f)=-\deg(f)$ for $f\in R$. We define an action of R to the additive group of $\tilde{k}$ an algebraic closure of k as follows. For any $u\in\tilde{k}$,

$$u^T=u^q+Tu\,,$$

$$u^\alpha=\alpha u \qquad (\alpha\in\boldsymbol{F}_q)\,.$$

It is easily checked that this action endows $\tilde{k}$ with an R-module structure. For an $M\in R$ we put

$$\Lambda_M=\{\lambda\in\tilde{k}\,;\,\lambda^M=0\}$$

and $K_M=k(\Lambda_M)$. In the following we assume $M\in R\setminus\boldsymbol{F}_q$. Then we can prove the following facts, which are quite analogous to the case of the classical cyclotomic theory.

1. As a polynomial in u over k, u^M is separable of degree q^d, where d is the degree

Received April 20, 1990

of M.

2. Suppose $M=\alpha\prod P^n$ is the factorization of M into powers of monic irreducibles ($\alpha\in F_q$). Then

$$\Lambda_M=\bigoplus\Lambda_{P^n}\qquad\text{(direct sum)}$$

and each Λ_{P^n} is a cyclic R-module and naturally isomorphic to $R/(P^n)$.

3. The extension K_M/k is an abelian extension and its Galois group G_M is canonically isomorphic to $(R/(M))^\times$.

$$\begin{array}{rcl}(R/(M))^\times & \to & G_M\\ A \bmod M & \mapsto & \sigma_A\end{array}$$

where $\sigma_A:\lambda\mapsto\lambda^A$, $\lambda\in\Lambda_M$. Hence the degree of the extension is equal to

$$\Phi(M)=\#(R/(M))^\times=\prod_{i=1}^r\#(R/(P_i^{n_i}))^\times=\prod_{i=1}^r q^{d_i(n_i-1)}(q^{d_i}-1)$$

when we decompose M as $M=\prod_{i=1}^r P_i^{n_i}$ and let $d_i=\deg P_i$ (when we decompose M into powers of irreducibles in the later sections, we use this notation). And if Q is a finite prime which does not divide M, then σ_Q is given by the Artin symbol.

4. Let $M=P^n$. Then only P and ∞ ramify and P is totally ramified in the extension. And the generator λ of Λ_{P^n} is a generator of the principal ideal of K_{P^n} lying above P. We call these fields K_M *cyclotomic function fields* after Galovich-Rosen [G-R1].

5. Put $G_0=\{\sigma_A\in G_M\,;\,A\in F_q^\times\}$. Then G_0 is the inertia group of P_∞, where P_∞ is any prime divisor of K_M lying above ∞. We denote by K_M^+ the fixed field of G_0. The infinite prime ∞ splits completely in K_M^+, the ramification index $e_\infty=e(P_\infty, K_M/K_M^+)=q-1$, and the inertia degree $f_\infty=f(P_\infty, K_M/K_M^+)=1$. We call K_M^+ *the maximal real subfield* of K_M. Note that if $q=2$, then $K_M=K_M^+$.

For more information and proofs, refer to the papers of Hayes [Ha1] and Galovich and Rosen [G-R1] [G-R2].

2. Differents and genus formulae.

We continue to use the notations in the previous section.

First we calculate the differents of cyclotomic function fields and their maximal real subfields.

THEOREM 1. *Let $M=\prod_{i=1}^r P_i^{n_i}$ be the factorization of $M\in R$ into powers of irreducibles and $d_i=\deg P_i$. The differents $D(K_M/k)$ and $D(K_M/K_M^+)$ are given in the following formulae:*

$$D(K_M/k)=\prod_{i=1}^r\mathfrak{p}_i^{s_i}\prod_{P_\infty\mid\infty}P_\infty^{q-2},\tag{1}$$

$$D(K_M/K_M^+)=\mathfrak{p}_1^{q-2}\prod_{P_\infty\mid\infty}P_\infty^{q-2}\qquad \textit{if}\quad r=1\,, \tag{2}$$

$$D(K_M/K_M^+)=\prod_{P_\infty\mid\infty}P_\infty^{q-2}\qquad \textit{if}\quad r\geqslant 2\,, \tag{3}$$

where $\mathfrak{p}_i$ is the unique prime divisor of $K_{P_i^{n_i}}$ lying above P_i, P_∞ runs over $\Phi(M)/(q-1)$ prime divisors of K_M lying above ∞, and $s_i=n_i\Phi(P_i^{n_i})-q^{d_i(n_i-1)}$. Note that $\mathfrak{p}_i$'s in the above equalities should be regarded as divisors of K_M.

Proof. First we prove (1). If $r=1$, then the formula is proved by Hayes [Ha1]. By 5 in section 1 we find that ∞ is tamely ramified in the extension K_M/k, therefore the exponent of P_∞ in the different is $e_\infty-1=q-2$.

The remaining part is the non-∞-part. For simplicity we restrict our attention to the case $r=2$. The other cases can be shown by the same argument. By 4 in section 1, the fields $K_{P_i^{n_i}}$ $(i=1,2)$ are linearly disjoint, and the non-∞-part of the differents $D(K_{P_i^{n_i}}/k)_\infty$ $(i=1,2)$ are relatively prime. So by the formula

$$D(K_M/K_{P_1^{n_1}})_\infty D(K_{P_1^{n_1}}/k)_\infty=D(K_M/K_{P_2^{n_2}})_\infty D(K_{P_2^{n_1}}/k)_\infty\,,$$

we have

$$D(K_M/K_{P_i^{n_i}})_\infty=D(K_{P_j^{n_j}}/k)_\infty\qquad \text{for}\quad i\neq j\,,\quad \text{and}\quad i,j=1,2$$

as divisors in K_M. Hence the formula (1) follows from Hayes' formula for $r=1$.

If $r=1$, then both P and P_∞ are tamely and totally ramified in the extension K_M/K_M^+. Therefore we get the formula (2) immediately. Suppose $r\geq 2$ and let λ be a generator of Λ_M. Then obviously $K_M=K_M^+(\lambda)$. Let O_M and O_M^+ denote the integral closures of R in K_M and K_M^+ respectively. Then we see that the discriminant of O_M/O_M^+ divides the discriminant of λ:

$$d(\lambda)=(\mathrm{Norm}_{K_M/K_M^+}f'(\lambda))=\Big(\prod_{a\in F_q^\times}a(q-1)\lambda^{q-2}\Big)=(\lambda^{(q-1)(q-2)})\,,$$

where

$$f(u)=\mathrm{Irr}(\lambda,K_M^+\,;\,u)=\prod_{a\in F_q^\times}(u-a\lambda)=u^{q-1}-\lambda^{q-1}\,.$$

Corollary 1.9 of Galovich and Rosen [G-R2] shows that λ is a unit of O_M if $r\geq 2$. Hence we find the discriminant of O_M/O_M^+ is trivial, so the extension is unramified outside ∞. Since the ∞-part is the same as (2), the formula (3) follows. □

Corollary 1 (Genus Formulae). *Let g_M and g_M^+ be the genera of the fields K_M and K_M^+ respectively. They are given by the formulae below*:

$$2g_M-2=-2\Phi(M)+\sum_{i=1}^{r} s_i\frac{\Phi(M)}{\Phi(P_i^{n_i})}d_i+(q-2)\frac{\Phi(M)}{q-1}\,, \tag{4}$$

$$2g_M^+-2=(dn-2)\frac{\Phi(M)}{q-1}-d\frac{q^{d(n-1)}-1}{q-1}-d \quad \textit{if} \quad r=1\,, \tag{5}$$

$$2g_M^+-2=\frac{1}{q-1}\left\{(2g_M-2)-\frac{\Phi(M)}{q-1}(q-2)\right\} \quad \textit{if} \quad r\geq 2\,. \tag{6}$$

In equation (5) $d=d_1$ *and* $n=n_1$.

Proof. If (4) is once proved, then the formulae (5) and (6) are straightforward from the Riemann-Hurwitz formula:

$$2g_M-2=[K_M : K_M^+](2g_M^+-2)+\deg(D(K_M/K_M^+))\,. \tag{7}$$

So we show (4). Let $\mathfrak{p}_i$ be as in (1) in Theorem 1. If the prime divisor $\mathfrak{p}_i$ of $K_{p_i^{n_i}}$ is decomposed as $(\tilde{\mathfrak{p}}_1\tilde{\mathfrak{p}}_2\cdots\tilde{\mathfrak{p}}_{g_i})^{e_i}$ in K_M, then the degree of $\mathfrak{p}_i$ as a divisor of K_M is

$$\deg_M \mathfrak{p}_i=\deg_M((\tilde{\mathfrak{p}}_1\tilde{\mathfrak{p}}_2\cdots\tilde{\mathfrak{p}}_{g_i})^{e_i})=e_if_ig_i\times d_i=[K_M : K_{P_i^{n_i}}]\times d_i=\frac{\Phi(M)}{\Phi(P_i^{n_i})}\times d_i\,,$$

where f_i is the inertia degree. Therefore the degree of the different is

$$\sum_{i=1}^{r} s_i\frac{\Phi(M)}{\Phi(P_i^{n_i})}d_i+(q-2)\frac{\Phi(M)}{q-1}\,,$$

where the second term is determined by 5 in section 1. Now the proof is complete by the Riemann-Hurwitz formula. □

3. Algebraic function fields with divisor class number one.

Let L be an algebraic function field of one variable with the finite field $\boldsymbol{F}_q$ with q elements as a field of constants. We denote by $\mathrm{Div}^0(L)$ and $P(L)$ the group of divisors of degree zero and the group of principal divisors of L respectively. Then the divisor class number h_L is defined by

$$h_L=\#(\mathrm{Div}^0(L)/P(L))\,.$$

It is well-known that h_L is finite.

First we note that if a function field L has genus zero, then the Riemann-Roch theorem implies that L is a rational function field and so $h_L=1$.

In this section we give some criteria for general function fields over finite fields to have divisor class number one.

Proposition 1 ([Ar] or [Mac]). *Suppose L is as above and assume that* $q>4$ *and* *its genus* $\neq 0$. *Then* h_L *is larger than one.* □

PROPOSITION 2 ([M-Q]). *Let* L *be a function field over the finite field with* q *elements* ($q \leq 4$) *and* g ($\neq 0$) *its genus. If the divisor class number of* L *is one, then one of the following properties holds*:

(a) $q=2$ *and* $g \leq 4$,

(b) $q=3$ *and* $g=1$,

(c) $q=4$ *and* $g=1$.

Moreover suppose $q=2$ *and let* N *be the number of* $\boldsymbol{F}_2$*-rational points of the curve associated with* L. *Then* N *is not greater than one.* □

REMARK. If L has genus one, then the argument in [M-Q] shows that $h_L = N$.

4. Divisor class number of cyclotomic function fields.

In this section let h_M and h_M^+ denote the divisor class numbers of the cyclotomic function field K_M and its maximal real subfield K_M^+ respectively.

LEMMA 1. *Let* K_M *be a cyclotomic function field and* N *the number of* $\boldsymbol{F}_q$*-rational points of the associated curve. Then we have*

$$N \geq \frac{\Phi(M)}{q-1}.$$

The same holds for the maximal real subfield K_M^+ *of* K_M.

PROOF. By 5 in section 1 we find the absolute degree of the points lying above the infinite point ∞ is one. Hence they are $\boldsymbol{F}_q$-rational. Thus the number of $\boldsymbol{F}_q$-rational points is not smaller than the number of the points lying above ∞, which is equal to $\Phi(M)/(q-1)$. □

THEOREM 2. *For the cyclotomic function field* K_M, $h_M = 1$ *if and only if its genus* $g_M = 0$. *The same holds for* K_M^+.

PROOF. If $\Phi(M)/(q-1) > 1$, then Theorem 2 follows from Lemma 1, Proposition 2 and the remark after Proposition 2. Hence we consider the case $\Phi(M)/(q-1) = 1$. By the definition of $\Phi(M)$ it is easy to see that $\Phi(M)/(q-1) = 1$ if and only if

$$\begin{cases} r=1, \quad d_1 = n_1 = 1, & \text{if} \quad q=2, \\ r=2, \quad d_i = n_i = 1 \ (i=1,2), & \text{if} \quad q=2, \\ r=1, \quad d_1 = n_1 = 1, & \text{if} \quad q \geq 3. \end{cases}$$

For the above cases the genera are zero. The converse part is trivial by the remark in the beginning of section 3. This completes the proof of Theorem 2. □

By Theorem 2 we have only to find the fields with genus zero for our purpose. The next lemma is easy, but useful.

LEMMA 2. *Suppose L/K is a finite extension of algebraic function fields over a finite field. And let g_L and g_K be genera of L and K respectively. Then we have $g_L \geq g_K$.*

PROOF. If g_K is zero, then the lemma is obvious. So we may assume $g_K \neq 0$. By the Riemann-Hurwitz formula we have

$$2g_L-2=(2g_K-2)[L:K]+(\text{degree of different}) \geq (2g_K-2)[L:K] \geq (2g_K-2)\,.$$

Hence we have $g_L \geq g_K$. □

LEMMA 3. *Let $q \geq 3$. Suppose $M=P^n$ and $\deg P=d$. If $g_M^+=0$, then $(n, d)=(1, 1)$, $(1, 2)$ and $(2, 1)$.*

PROOF. Suppose $d(n-1)\geq 2$. Then $dn>2$ and $d/(dn-2)\leq 1$. By the trivial inequality

$$q^{d(n-1)}(q^d-2)>q-2\,,$$

we have

$$\frac{q^{dn}-q^{d(n-1)}}{q-1}>\frac{q^{d(n-1)}-1}{q-1}+1\,.$$

Thus

$$\frac{q^{dn}-q^{d(n-1)}}{q-1}>\left(\frac{q^{d(n-1)}-1}{q-1}+1\right)\times\frac{d}{dn-2}\,.$$

Therefore we have

$$(dn-2)\frac{q^{dn}-q^{d(n-1)}}{q-1}-d\left(\frac{q^{d(n-1)}-1}{q-1}+1\right)>0$$

because $dn-2>0$. By the genus formula (5) we get $2g_M^+-2>0$. This is impossible by the assumption $g_M^+=0$. Hence we have $d(n-1)<2$ i.e. $n=1$ or $(n, d)=(2, 1)$. If $n=1$, by (5)

$$-2=(d-2)\frac{q^d-1}{q-1}-d\,,$$

so

$$(d-2)\left(\frac{q^d-1}{q-1}-1\right)=0\,.$$

Thus we have $d=1$ or 2. □

We are now in a position to determine the fields with divisor class number one. We start with treating the maximal real subfields. We can neglect the case $q=2$ by 5 in section 1. Let $r=1$. It is easily verified by the genus formula (5) that the converse of Lemma 3 is also true. Thus we have three cases for $g_{P^n}^+=0$:

(a) $P^n=P_1$, $\deg P_1=1$,

(b) $P^n=P_2$, $\deg P_2=2$,

(c) $P^n=P_1^2$, $\deg P_1=1$

for $q\geq 3$.

We next consider the case that M contains at least two distinct prime factors.

1. $q=3$:

(a) $r=2$: By Lemma 2 only P_1, P_2 and P_1^2 (for notations as in the argument after Lemma 3) can be a factor of M. So we have the following table of genera for this case.

TABLE 1. Genus of the Field K_M^+ ($q=3, r=2$)

M	$P_1P'_1$	P_1P_2	$P_1P'^2_1$	$P_2P'_2$	$P_1^2P_2$	$P_1^2P'^2_1$
g	0	2	1	25	16	10

By Table 1 we have the only one case i.e., $M=P_1P'_1$ ($P_1\neq P'_1$, deg $P_1=$deg P'_1).

(b) $r=3$: $P_1P'_1$ can be a factor of M. Then other factor of M cannot be a polynomial of degree 2, because if P_2 or P_1^2 is a factor of M, then the genus of the field is larger than zero by Table 1 and Lemma 2. Hence we need to compute genus for the only one case i.e. $M=P_1P'_1P''_1$ in the obvious notation. For this M we have $g_M=0$ by the genus formula (6).

(c) $r\geq 4$: There are exactly three monic polynomials of degree one over $\boldsymbol{F}_3$. Hence the case $r\geq 4$ is impossible.

2. $q\geq 4$: In this case we need another lemma.

LEMMA 4. *Let $q\geq 4$, $r\geq 2$ and suppose M is one of the following types*:

(1) $M=\prod_{i=1}^{r_1}P_{1,i}$, $\deg P_{1,i}=1$,

(2) $M=\prod_{i=1}^{r_2}P_{2,i}$, $\deg P_{2,i}=2$,

(3) $M=\prod_{i=1}^{r_3}P_{1,i}^2$, $\deg P_{1,i}=1$.

The genus is greater than one if and only if one of the following inequalities holds:

$$r_1\geq 3\,,\quad r_2\geq 2\quad \textit{and}\quad r_3\geq 2\,.$$

PROOF. First we prove the case (1). Put $n_i=d_i=1$ in the genus formula (4) and let $r=r_1$. Then we have

$$2g_M-2=(q-1)^{r-1}(q(r-1)-2r)\,.$$

By the genus formula (6) we have

$$2g_M^+-2=(q-1)^{r-2}((r-2)q-2r+2)\,.$$

Hence, *if* $g_M^+=0$, then we must have

$$r^2-4r+2\leq(r-2)q-2r+2<0\,,$$

since obviously $r\leq q$. Hence r must be equal to 2 or 3. Coversely if $r=2$, then $2g_M^+-2=-2$. Thus in this case $g_M^+=0$. Let $r=3$. Then we must have $2g_M^+-2=(q-1)(q-4)<0$. This is impossible because $q\geq 4$.

Let $r=r_2$ and M be as (2). The same formulae give the following equalities:

$$2g_M-2=(q^2-1)^{r-1}((2r-1)q^2-q-4r)\,,$$
$$2g_M^+-2=(q+1)(q^2-1)^{r-2}(2(r-1)q^2-4r+2)\,.$$

Therefore, if $g_M^+=0$, then we have

$$2(r^2-3r+1)\leq 2(r-1)q^2-4r+2<0\,,$$

since $r\leq q^2$. Hence we have $r=2$. But conversely if $r=2$, then $2g_M^+-2=(q+1)(2q^2-6)>0$. Thus the genus cannot be zero in this case. This completes the proof of (2).

The case (3) follows from a similar method like (2). We compute the genus and the remaining part is omitted, as its proof is easy.

$$2g_M-2=q^r(q-1)^{r-1}((2r-1)q-3r)\,,$$
$$2g_M^+-2=q^r(q-1)^{r-2}(2(r-1)q-3r+2)\,.$$

□

(a) $r=2$: By Lemma 4 we have to determine the genera of the following four cases.

(A) $M=P_1P'_1$, (B) $M=P_1P_2$, (C) $M=P_1P_1'^2$, (D) $M=P_1^2P_2$,

where $\deg P_1=\deg P'_1=1$ and $\deg P_2=2$.

(A): By the argument in the proof of Lemma 4 we have $g_M^+=0$ in this case.

(B): The genus formulae (4) and (6) show that

$$2g_M-2=2(q-1)(q^2-q-4)\,,$$

and

$$2g_M^+-2=q^2-q-6\,.$$

Hence $g_M^+=0$ if and only if $q^2-q-4=0$. This is impossible, because q is an integer.

(C): In this case we have

$$2g_M-2=q(q-1)(2q-5)\,,$$

and

$$2g_M^+ - 2 = q^2 - 3q\,.$$

Hence $g_M^+ = 0$, if and only if $q^2 - 3q + 2 = 0$. This is also impossible, because $q \geq 4$.
(D): In this case we have

$$2g_M - 2 = q(q-1)(3q^2 - 2q - 7)\,,$$

and

$$2g_M^+ - 2 = q(2q^2 - q - 5)\,.$$

But the right hand of the equation is greater than zero when $q \geq 4$.
(b) $r \geq 3$: By Lemma 4 and Lemma 2 we need not consider these cases.

Summarizing the above results, we obtain the following theorem.

THEOREM 3. *The divisor class number h_M^+ of the maximal real subfield K_M^+ of the cyclotomic function field K_M is one, if and only if M is one of the following types*:

(a) *If $q = 3$, then* (1) $M = P_1$, (2) $M = P_2$, (3) $M = P_1^2$, (4) $M = P_1P'_1$, (5) $M = P_1P'_1P''_1$, *where* $\deg P_1 = \deg P'_1 = \deg P''_1 = 1$, $\deg P_2 = 2$ *and* P_1, P'_1 *and* P''_1 *are relatively prime.*

(b) *If* $q \geq 4$, *then* (1) $M = P_1$, (2) $M = P_2$, (3) $M = P_1^2$, (4) $M = P_1P'_1$, *where* $\deg P_1 = \deg P'_1 = 1$, $\deg P_2 = 2$ *and* $P_1 \neq P'_1$. □

Now we turn our attention to the cyclotomic function fields. We shall prove the next theorem.

THEOREM 4. *The divisor class number h_M of the cyclotomic function field K_M is one if and only if M is one of the following types*:

(a) *If $q = 2$, then* (1) $M = P_1$, (2) $M = P_2$, (3) $M = P_1^2$, (4) $M = P_1P'_1$, (5) $M = P_1P'^2_1$, (6) $M = P_1P_2$, (7) $M = P_1P'_1P_2$, *where* $\deg P_1 = \deg P'_1 = \deg P''_1 = 1$, $\deg P_2 = 2$ *and* P_1, P'_1 *and* P''_1 *are relatively prime.*

(b) *If* $q = 3$, *then* (1) $M = P_1$, (2) $M = P_1P'_1$, *where* $\deg P_1 = \deg P'_1 = 1$ *and* $P_1 \neq P'_1$.

(c) *If* $q \geq 4$, *then* (1) $M = P_1$, *where* $\deg P_1 = 1$.

PROOF. Let $M = \prod_{i=1}^r P_i^{n_i}$ be the factorization of M. We start with the case $r = 1$ and $q = 2$. Put $r = 1$ and $g_M = 0$ in the genus formula (4). Then we can easily find the solutions of the equation. They are as follows:

$$M = P_1,\ P_2 \text{ and } P_1^2\,,$$

where $\deg P_1 = 1$ and $\deg P_2 = 2$.

Next we consider the case $r \geq 2$. Suppose $q = 2$ and $r = 2$. Note that there is only two monic irreducible polynomials of degree one and only one of degree two. Hence we have the only five possible cases for the genus zero. Their genera are in Table 2.

TABLE 2. Genus of the Field K_M ($q=2$, $r=2$)

M	$P_1P'_1$	P_1P_2	$P_1P'^2_1$	$P^2_1P_2$	$P^2_1P'^2_1$
g_M	0	0	0	2	1

Let $r=3$. In this case the only possible case is $M=P_1P'_1P_2$, where $\deg P_1=\deg P'_1=1$, $\deg P_2=2$ and $P_1\neq P'_1$. For this M the genus is zero. By the remark in the case $r=2$ it is impossible that r is larger than 3.

Suppose $q\geq 3$. By Lemma 2 we have only to compute the genera for the cases in Theorem 3. By the genus formula (4) we have the following two tables (the notations are as in Theorem 3).

TABLE 3. Genus of the Field K_M ($q=3$)

M	P_1	P_2	P^2_1	$P_1P'_1$	$P_1P'_1P''_1$
g_M	0	2	1	0	1

TABLE 4. Genus of the Field K_M ($q\geq 4$)

M	P_1	P_2	P^2_1	$P_1P'_1$
g_M	0	$(q+1)(q-2)/2$	$(q-1)(q-2)/2$	$(q-1)(q-2)$

The terms in Table 4 are greater than zero.

This completes the proof of Theorem 4. □

Remark on the unique factorization.

Let O_M be the integral closure of R in K_M. It is known that O_M is a Dedekind domain. Hence the order of its ideal class group is finite. We call it *the ideal class number* of K_M and denote it by h^*_M. There is a relation between h_M and h^*_M known as the F. K. Schmidt formula:

$$h^*_M r_M = h_M\,,$$

where r_M is called the *regulator* of K_M. (For its definition see [Ar] or [Mac]. The latter also includes more general facts concerning this remark.) If the divisor class number h_M is one, then the ideal class number h^*_M must be one. Hence then O_M has the unique factorization property. It is equally ture for O^+_M. We can find these M's by Theorems 3, 4 and the proof of Theorem 2. On the other hand, for the case $h_M\neq 1$, it is still unknown for which polynomial M the rings O_M and O^+_M have the unique factorization property, because of the regulator.

For further results on ideal class numbers of cyclotomic function fields, see the papers of Galovich and Rosen [G-R1] [G-R2] and Okada [Ok].

Appendix. Elliptic curves associated with cyclotomic function fields.

By the similar method which we use in this paper we can also determine the cyclotomic function fields with genus one. They are as follows:

THEOREM 3′. *The maximal real subfield K_M^+ of the cyclotomic function field K_M is elliptic if and only if M is one of the following types*:

(a) *If* $q=3$, *then* $M=P_1P_1'^2$, *where* $\deg P_1=\deg P_1'$ *and* $P_1\neq P_1'$.

(b) *If* $q=4$, *then* $M=P_1P_1'P_1''$, *where* $\deg P_1=\deg P_1'=\deg P_1''$, *and* P_1, P_1' *and* P_1'' *are relatively prime.*

There is no cases for genus one when $q\geq 5$. □

THEOREM 4′. *The cyclotomic function field K_M is elliptic if and only if M is one of the following types*:

(a) *If* $q=2$, *then* (1) $M=P_1^2P_1'^2$, (2) $M=P_1^3$, (3) $M=P_1^3P_1'$, *where* $\deg P_1=\deg P_1'$ *and* $P_1\neq P_1'$.

(b) *If* $q=3$, *then* (1) $M=P_1^2$, (2) $M=P_1P_1'P_1''$, *where* $\deg P_1=\deg P_1'=\deg P_1''$, *and* P_1, P_1' *and* P_1'' *are relatively prime.*

There is no cases for genus one when $q\geq 4$. □

ACKNOWLEDGEMENT. The authors would like to thank Nobuhiro Terai for his help.

References

[Ar] J. V. ARMITAGE, Corrigendum and addendum: Euclid's algorithm in algebraic function fields, J. London Math. Soc., **43** (1968), 171–172.

[G-R1] S. GALOVICH and M. ROSEN, The class number of cyclotomic function fields, J. Number Theory, **13** (1981), 363–375.

[G-R2] S. GALOVICH and M. ROSEN, Units and class groups in cyclotomic function fields, J. Number Theory, **14** (1982), 156–184.

[Ha1] D. R. HAYES, Explicit class field theory for rational function fields, Trans. Amer. Math. Soc., **189** (1974), 77–91.

[Ha2] D. R. HAYES, Explicit class field theory for global function fields, *Studies in Algebra and Number Theory*, ed. by Rota, Academic Press (1979).

[I-S] K. F. IRELAND and SMALL, Class number of cyclotomic function fields, Math. Comp., **46** (1986), 337–340.

[Iw] K. IWASAWA, *The Theory of Algebraic Functions* (in Japanese), Iwanami Shoten (1952).

[Mac] R. E. MACRAE, On unique factorization in certain rings of algebraic functions, J. Algebra, **17** (1971), 243–246.

[M-Q] M. L. MADAN and C. S. QUEEN, Algebraic function fields of class number one, Acta Arith., **20** (1972), 423–432.

[Ok] S. OKADA, An analogue of Kummer theory in function fields (in Japanese), RIMS Kôkyuroku, **658** (1988), 63–72.

Present Address:
DEPARTMENT OF MATHEMATICS, SCHOOL OF SCIENCE AND ENGINEERING, WASEDA UNIVERSITY
OKUBO, SHINJUKU-KU, TOKYO 169, JAPAN