Algebraic function fields of class number one

by

MANOHAR L. MADAN* and CLIFFORD S. QUEEN (Columbus, Ohio)

§ 1. Introduction. Let $F$ be a field of algebraic functions of one variable having a finite field $K$ with $g$ elements as its exact field of constants. The group of divisor classes of degree zero of such a congruence function field is a finite abelian group. Its order $h_F$ is called the class number of $F$. In this paper, we discuss the following question: Which congruence function fields have class number one? The special case, when $F$ is a quadratic extension of a rational field and has a prime of degree one, has been studied by Mac Rae [7]. He determines all such fields with class number one. It turns out that the critical case is when $K$ is the prime field of characteristic 2 or 3 and genus $g$ is larger than one. We show that, if $g = 2$ and genus is larger than 4, or $q = 3$ and genus is larger than 2, the class number is not one. This is carried out in § 2. In § 3, we obtain explicit expressions for zeta-function and class number for $g = 2, 3, 4$ and $q$ arbitrary. From these formulae, we deduce that also for $g = 3$ and $g = 2$, the class number is larger than one. For $q = 2$ and $g = 2, 3, 4$, we derive necessary and sufficient conditions for class number to be one. In § 4, we discuss the case of quadratic extensions and show that, up to isomorphism, there is exactly one quadratic field of class number one which has no prime of degree one. In § 5, we give two examples of fields of genus 3 defined over the field of 2 elements to illustrate that the necessary and sufficient condition given in § 3 can be satisfied. At the time of writing this paper, we do not have a similar example for genus 4.

It should be remarked that for prime fields of characteristic different from 2, the arithmetic and analytic theory of quadratic extensions was developed by Artin in his dissertation [2]. An extension $F/K(X)$ is called imaginary if the infinite prime of $K(X)$ does not decompose in $F$ as product

* This research is partially supported by N. S. F. Grant GP-13327.

(*) Following a procedure suggested by Professor John Tate, we have proved that there is, in fact, no such field.
of two different primes. Artin had predicted ([2], p. 237) that there is, essentially, only one imaginary quadratic field for which the integral closure \( R \) of \( K[X] \) in \( F \) is a unique factorization domain. This has been proved by MacRae [7] who also shows that, in addition to the one given by Artin, there are three fields of characteristic 2 (\( K \) not necessarily prime field), for which \( R \) is a unique factorization domain and the infinite prime of \( K(X) \) is ramified in \( F \). In the sense of Artin, the extension \( F/K(X) \) is imaginary also in the case when the infinite prime is tame in \( F \). In this case, however, it follows from a relation between \( h_F \) and the class number of the Dedekind ring \( \mathcal{O} \), that the latter is even ([9], p. 32).

§ 2. If \( F \) has genus zero and \( K \) is arbitrary, it follows from the Riemann–Roch theorem that a class of degree zero has dimension one. It is, therefore, the principal class, because no other class of degree zero has integral divisors. Thus, for a congruence function field, \( h_F = 1 \) one.

We shall now assume \( g_F \geq 1 \). We shall also assume that \( g \leq 4 \), for otherwise \( h_F \) is larger than one ([1], see also [2], p. 337). We recall that the Riemann Hypothesis is equivalent to the inequality

\[
|N_1 - (g+1)| \leq 2g_0\sqrt{g},
\]

where \( N_1 \) denotes the number of primes of degree one. Let \( F/K \) be a constant extension of \( F/K \) of degree \( 2g_F - 1 \). The field \( K \) being perfect, \( g_F = g_F' = g \). We apply (1) to \( F/K \) and obtain

\[
N_1 \geq q^{2g-1} + 1 - 2g \cdot q^{(2g-1)/2}.
\]

A prime of degree \( d \) of \( F \) decomposes (14), p. 164) into \( F \) as product of \((d, 2g - 1)\) primes of degree \( d, 2g - 1 \). Primes of degree one of \( F \), therefore, lie over such primes of \( F \) of which degree divides \( 2g - 1 \). Using (2), it follows that \( F \) has at least

\[
q^{2g-1} + 1 - 2g \cdot q^{(2g-1)/2}
\]

integral divisors of degree \( 2g - 1 \). On the other hand, the Riemann–Roch Theorem implies that a class of degree \( 2g - 1 \) has dimension \( g \). There are, precisely, \((q^g - 1) (q - 1)^{-1}\) integral divisors in such a class ([4], p. 64). Therefore, \( h_F \) is larger than one if

\[
(q - 1) [q^{2g-1} + 1 - 2g \cdot q^{(2g-1)/2}] > (2g - 1) (q^g - 1).
\]

Let

\[
S(g, g) = (q - 1) [q^{2g-1} + 1 - 2g \cdot q^{(2g-1)/2}] - (2g - 1) (q^g - 1).
\]

We observe

\[
\begin{align*}
S(4, 1) &= 3(4 - 4) = 0, \\
S(4, 2) &= 3(50 - 32) > 0, \\
S(3, 2) &= 8(4 - 3\sqrt{3}) < 0, \\
S(3, 3) &= 2(179 - 54\sqrt{3}) > 0, \\
S(2, 4) &= 8(3 - 8\sqrt{2}) < 0, \\
S(2, 5) &= 8(37 - 20\sqrt{2}) > 0.
\end{align*}
\]

We now show that, as a function of \( g \), \( S(g, g) \) is increasing, if

\[
q = 4, \quad g \geq 2; \quad q = 3, \quad g \geq 3; \quad q = 2, \quad g \geq 5.
\]

We obtain from (4),

\[
\frac{dS}{dg} = (q - 1) [q^{2g-1} - 2(q^g - 1)^2 - 2g(q^g - 1)^{3/2} \ln q] - 2(q^g - 1) - 2(q - 1) q^{2g-1} \ln q
\]

where

\[
T(q, g) = (q - 1) q^{2g-1} - 2(q^g - 1)^2 - 2(q^g - 1)^{3/2} \ln q - (2(q - 1) q^{2g-1} \ln q.
\]

Considering it as a function of \( g \), we have

\[
\frac{dT}{dg} = (q - 1) q^{2g-1} \ln q - 2(q - 1) q^{2g-1} \ln q - 2q^{2g-1} \ln q - (2(q - 1) q^{2g-1} \ln q.
\]

\[
\frac{dT}{dg} = 2[q^{2g-1} \ln 2 - 2 - 2(q^g - 1) \ln q - (2q - 1) q^{2g-1} \ln q.
\]

If any of the conditions (6) is satisfied, one sees easily from (8), (9) and (7) that \( T(q, g) \) and \( dT/dg \) are positive and that \( S \) is an increasing function. We see from (5), (4) and the observation preceding (5), that we have proved the following

**Theorem 1.** Let \( F \) be a field of algebraic functions of one variable of genus \( g \) having a finite field with \( q \) elements as its exact field of constants. The class number of \( F \) is larger than one if any of the following conditions is satisfied: \( q = 4, \quad g \geq 2; \quad q = 3, \quad g \geq 3; \quad q = 2, \quad g \geq 5.\)

7. — Acta Arithmetica XXXI.
§ 3. Using the notation of [5], let
\[ L(u) = 1 + a_1 u + a_2 u^2 + \ldots + a_{2g} u^{2g} = \prod_{k=1}^{2g} (1 - \omega_k u) \]
be the numerator of the zeta-function. Then,
\[ u^{-g} L(u) = u^{g-1} + a_1 u^{-1} + a_2 u^{-2} + \ldots + a_{2g} u^{-2g} \]
is invariant if we replace \( u \) by \( q^{-1} u^{-1} \). Using this functional equation, we obtain
\[ a_g = q^g, \quad a_{g-1} = q^{g-1} a_1, \quad a_{g-2} = q^{g-2} a_2, \quad \ldots, \quad a_1 = q^{g-1} \]
and, hence from (10),
\[ L(u) = 1 + a_1 u + a_2 u^2 + \ldots + a_g u^g + a_{g-1} u^{g-1} + \ldots + a_1 u \]
The expression for the class number is
\[ \text{h} = L(1) = (q^g + 1) + a_1 (q^{g-1} + 1) + \ldots + a_{g-1} (q + 1) + a_g. \]
We shall calculate \( a_1, a_2, a_3, a_4 \) which will suffice for the discussion of the cases \( g = 2, 3, 4 \). Let \( S_i = \sum_{d=1}^{2g} d \alpha_i^k \). Then ([8]),
\[ -S_i = \sum_{d=1}^{2g} d(N_d - n_d), \]
where \( N_d, n_d \) denote, respectively, the number of primes of degree \( d \) of \( F \) and \( K(x) \). Using the recursion formula ([10], p. 102) for \( S_i \) in terms of \( S_1, \ldots, S_{i-1} \) and the elementary symmetric functions, we obtain from (10)
\[ a_1 = -S_1, \]
\[ a_2 = -S_2, \]
\[ a_3 = -S_3, \]
\[ a_4 = -S_4. \]

Also, we have Dedekind's formulae ([3]),
\[ n_d = \begin{cases} q + 1 & \text{if } d = 1, \\ \frac{1}{d} \sum_{j|d} q^j \mu \left( \frac{d}{j} \right) & \text{if } d > 1, \end{cases} \]
where \( \mu(m) \) denotes the Möbius function. From (13) and (15), we obtain
\[ -S_1 = N_1 - n_1 = N_1 - (q + 1), \]
\[ -S_2 = N_1 + 2N_2 - (q^2 + 1), \]
\[ -S_3 = N_1 + 3N_2 - (q^3 + 1), \]
\[ -S_4 = N_1 + 2N_2 + 3N_4 - (q^4 + 1). \]
The substitution of these values in (14) gives, after simplification,
\[ a_1 = N_1 - (q + 1), \]
\[ 2a_2 = N_1^2 - (2q + 1) N_1 + 2N_2 - 2q, \]
\[ 6a_3 = N_1^3 - 3q N_1^2 + (3q - 1) N_1 - 6(q + 1) N_2 + 6N_1 N_2 + 6N_3, \]
\[ 24a_4 = (4q - 2) N_1 - N_1^2 + (2q - 4) N_2^2 + (12 + 24q) N_3 - (12 + 24q) N_1 N_2^2 - 24(N_1 N_2 - 1) N_2^2 - 24(q + 1) N_2 N_3 + 24N_1 N_2 N_3 + 24N_4. \]
Substitution in (11) gives the numerator of the zeta-function for \( g = 2, 3, 4 \). We return, now, to the study of algebraic function fields of class number one. We remark that such a field, if its genus is different from zero, cannot have two primes of degree one, for, otherwise if \( P_1, P_2 \) are two such primes, the divisor \( P_1 P_2^{-1} \) is principal (a) and \([F : K(x)] = 1\). Now, we prove

**Theorem 2.** Let \( F \) be a field of algebraic function of one variable of genus \( g \) having a finite field with \( q \) elements as its exact field of constants. Let \( N_i \) denote the number of primes of degree \( i \). Then

(i) \( g = 3, \quad N_1 = 2 \Rightarrow \text{the class number is larger than one; \( \)} \)
(ii) \( g = 2, N_1 = 2 \Rightarrow \text{the class number is one if } N_1 = 3; \)
(iii) \( g = 2, N_1 = 1 \Rightarrow \text{the class number is one if } N_1 = 2; \)
(iv) \( g = 2, N_1 = 3 \Rightarrow \text{the class number is one if } N_1 = 0, N_2 = 1; \)
(v) \( g = 2, N_1 = 4 \Rightarrow \text{the class number is one if } N_1 = 0, N_2 = 1. \)

**Proof.** (i) From (12) and (16), we obtain
\[ h = 10 + 4a_1 + a_2 = -6 + N_1 + N_2 + 2N_3, \]
\[ \ldots \Rightarrow h = 1 \Leftrightarrow N_1 + N_2 + 2N_3 = 8. \]
From (11) and (16), we have
\[ L(u) = 1 + (N_1 - 4) u + \frac{N_1^2 - 7N_1 + 6N_2 + 6}{2} u^2 + \ldots + 3^s u^s. \]
Also, by the Riemann Hypothesis, the reciprocals of roots of \( L(u) \) are \( 3^{1/2} \alpha \pm \sqrt{2}, 3^{1/2} \alpha \mp \sqrt{2} \), and hence
\[ L(u) = (1 - 3^{1/2} \alpha^2 u)(1 - 3^{1/2} \alpha^2 u)(1 - 3^{1/2} \alpha^2 u)(1 - 3^{1/2} \alpha^2 u) \]
\[ = [1 - 2 \cdot 3^{1/2} \cos \theta_2 u + 3 u^2] \cdot [1 - 2 \cdot 3^{1/2} \cos \theta_3 u + 3 u^2]. \]
Comparing coefficients in (18) and (19), we obtain
\[ \cos \theta_1 + \cos \theta_2 = \frac{(4-N_3)3^{1/2}}{6}, \]
\[ \cos \theta_1 \cos \theta_2 = \frac{N_1^2 - 7N_1 + 2N_2 - 6}{24}. \]

Using (17), we see that, if the class number is one, \( \cos \theta_1, \cos \theta_2 \) are roots of the quadratic polynomial
\[ f(x) = x^2 + \frac{(N_1 - 4)3^{1/2}}{6} x + \frac{1 - 4N_1}{12}. \]
But,
\[ f(1) = \frac{[12 + 1 - 8 \cdot 3^{1/2}] + N_1[2 \cdot 3^{1/2} - 4]}{12} \]
which is always negative. Thus, \( f(x) \) has a root larger than one. This is a contradiction.

(ii) As in (i), one obtains the following class number formula
\[ h = \frac{N_1^2 + N_1 + 2N_2 - 4}{2}. \]
The condition for class number to be one is
\[ N_1^2 + N_1 + 2N_2 = 6. \]

(ii), (iii) are obvious from this equation.

(iv) The class number formula obtained from (12) and (16) is
\[ h = \frac{-10N_1 + 3N_2^2 + N_1^2 + 8N_2N_4 + 6N_4}{6}. \]

Thus, the class number is one iff
\[ N_1 = 1 \quad \text{for} \quad N_4 = 0, \]
\[ N_1 + N_2 = 2 \quad \text{for} \quad N_4 = 1. \]

We shall, now, show that the case \( N_1 = 1 \) is not possible. As in (i), comparing coefficients in two expressions for \( L(u) \), we obtain for \( N_1 = 1 \),
\[ \sum \cos \theta_1 = \frac{\sqrt{2}}{2}, \]
\[ \sum \cos \theta_1 \cos \theta_2 = \frac{N_2 - 6}{8}, \]
\[ \cos \theta_1 \cos \theta_2 \cos \theta_4 = \frac{(3N_4 - 10)\sqrt{2}}{32}. \]

Thus, \( \cos \theta_1, \cos \theta_2, \cos \theta_4 \) are roots of the cubic polynomial
\[ f(x) = x^3 - \frac{\sqrt{2}}{2} x^2 + \frac{N_4 - 6}{8} x + \frac{(10 - 3N_4)\sqrt{2}}{32}. \]
But,
\[ f(1) = \frac{(8 - 6\sqrt{2}) + (4 - 3\sqrt{2}) N_4}{32} < 0, \]
which implies that \( f(x) \) has a root larger than one. A contradiction.

(v) For \( q = 2, g = 4 \), the class number formula is
\[ 24h = N_1^2 + 6N_2^2 - 13N_4^2 - 18N_4 - 36N_2 + 12N_1N_4 + 12N_1^2N_4 + 12N_2^2N_4 + 24N_1N_2N_4 + 24N_2N_4. \]

For our discussion, it will be convenient to distinguish the two cases \( N_4 = 0, N_4 = 1 \). The necessary and sufficient condition for the class number to be one is
\[ N_1^2 - 3N_1 + 2N_4 = 2 \quad \text{if} \quad N_4 = 0, \]
\[ N_1^2 - N_1 + 2N_4 = 4 \quad \text{if} \quad N_4 = 1. \]

As in (i), comparing coefficients of \( u, u^2, u^3, u^4 \) in two expressions for \( L(u) \), we obtain the following polynomial
\[ f(x) = x^4 + \frac{N_1 - 3}{2\sqrt{2}} x^3 + \frac{a_2 - 8}{8} x^2 + \frac{a_4 - 6a_2}{16\sqrt{2}} x + \frac{-a_4 - 4a_2 + 8}{64} \]
of which \( \cos \theta_j, j = 1, 2, 3, 4 \) are the roots. (Here \( \sqrt{2} e^{\pi i j}, j = 1, 2, 3, 4 \), are the reciprocals of the roots of \( L(u) \).

Distinguishing the two cases, we obtain using (16) and (20),
\[ f(x) = x^4 - \frac{3\sqrt{2}}{4} x^3 + \frac{N_4 - 6}{8} x^2 + \frac{N_4 - 3N_1 + 18}{16\sqrt{2}} x + \frac{2 - 6N_4}{128} \quad \text{if} \quad N_4 = 0 \]
and
\[ f(x) = x^4 - \frac{\sqrt{2}}{2} x^3 + \frac{N_4 - 8}{8} x^2 + \frac{N_4 - 2N_2 + 12}{16\sqrt{2}} x + \frac{10 - 3N_4 - 3N_2}{64} \quad \text{if} \quad N_4 = 1. \]

If \( N_4 = 1 \),
\[ f(1) = \frac{(10 - 3\sqrt{2}) + N_4(5 - 4\sqrt{2}) + N_2(4\sqrt{2} - 6)}{64} < 0. \]
Therefore, in this case the class number is not one, because the function \( f(x) \) has a root larger than 1.

If \( N_4 = 0 \),

\[
f(1) = \frac{(17 - 12\sqrt{2}) + N_4(8 - 6\sqrt{2}) + N_4(2\sqrt{2} - 3)}{64}.
\]

We see \( f(1) < 0 \), unless \( N_4 = 0 = N_5 \) in which case \( f(1) \) is positive. Thus, \( N_4 = 0 = N_5 \) is a necessary condition for \( h = 1 \). Together with (20), which is a necessary and sufficient condition, we see that \( N_4 = N_5 = 0, N_4 = 1 \) is a necessary and sufficient condition. In this case,

\[
L(u) = 1 - 3u^2 + 2u^3 + u^4 + 8u^5 - 24u^6 + 16u^8.
\]

We do not have an example of a function field for which this is the numerator of the zeta-function.

§ 4. Quadratic extensions. Macrae [7] has determined all quadratic extensions which have a prime divisor of degree one and class number one. What about quadratic extensions with class number one which have no prime divisor of degree one? We remark that a congruence function field of genus one has necessarily a prime of degree one. Therefore, our discussion of the last two sections, it follows that a quadratic function field \( F/K \) having no prime divisor of degree one has class number one if and only if \( g = 2, \gamma = 2, N_2 = 3 \). We shall discuss this case systematically, using, without explicit reference, some results from [6] concerning the arithmetic of cyclic extensions.

Assume \( h_F = 1 \). Let \( P \) be a prime of degree 2. Then, \( P \) is in the canonical class, the only class of degree 2. Using the same notation as in [4], we have by the Riemann–Roch Theorem

\[
\ell(P^n) = \dim L(P^n) = 2(n - 1) + 1 \quad \text{if} \quad n > 1,
\]

\[
\ell(P^{-1}) = \dim L(P^{-1}) = 2.
\]

Let \( x \in L(P^{-1}) \) such that \( \{1, x\} \) is a basis of \( L(P^{-1}) \). Then \( \{1, x, x^2\} \) is a basis of \( L(P^{-1}) \). Considering that \( \ell(P^{-1}) = 5 \), we see that there exists \( t \in L(P^{-1}) \) such that \( \{1, x, x^2, x^3, t\} \) is a basis of \( L(P^{-1}) \). Necessarily, \( t \) is not in \( K(x) \). Since \( \ell(P^{-1}) = 11 \), the following 12 elements of \( L(P^{-1}) \) must be linearly dependent:

\[
1, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8, x^9, x^{10}, x^{11}.
\]

We have \( \ell(K(t)) = 6 \). Therefore, there exist polynomials \( D(x) \), \( C(x) \) in \( K[x] \) such that \( \deg D(x) = 6 \), \( \deg C(x) \leq 3 \) and

\[
t^5 + C(x)t = D(x).
\]

Further, \( C(x) \neq 0 \) for otherwise \( g_F = 0 \).

Now, setting \( t^5 = tC(x)^{-1} \), we obtain from (21),

\[
t^5 + t^3 = D(x)C(x)^{-1},
\]

and \( F = K(x, t) \). Using \( N_1 = 0, N_2 = 3 \), we see that no prime of degree one or two is a zero or a pole of \( D(x)C(x)^{-1} \) in \( K(x) \). Thus, \( \deg D(x) = \deg C(x)^2 \) and \( C(x) \) is irreducible of degree 3. There exists \( d(x) \) in \( K[x] \) such that

\[
D(x)d(x) + D(x) = d(x)C(x).
\]

Setting \( Y = t^5 + D(x)^4C(x)^{-1} \), we obtain, from (22) and (23),

\[
Y^2 + Y = h(x)C(x)^{-1},
\]

where, \( h(x) = d(x) + D(x)^4 \). As before, we conclude that \( h(x) \) is irreducible polynomial of degree 3. There are two possibilities for (24),

\[
Y^2 + Y = \frac{x^3 + x^2 + 1}{x^3 + x + 1}, \quad \text{or} \quad \frac{x^3 + x + 1}{x^3 + x^2 + 1},
\]

giving isomorphic fields. It is easily checked that for \( F = K(x, Y), g_F = 2, N_1 = 0, N_2 = 3 \) and, hence, the class number is one.

§ 5. Examples. We have shown in § 3 that a function field \( F/K \) of genus 3 has class number one if \( g = 2 = \ell(K), N_1 = 0 \) and \( N_2 = 1 \). Using the same notation as in § 3, the cubic polynomial of which \( \cos \theta_1, \cos \theta_2, \cos \theta_3 \) are roots, then reduces to

\[
f(x) = x^3 - \frac{3\sqrt{2}}{4}x^2 + \frac{2N_1 - 8}{16}. \quad \text{This gives}
\]

\[
f(1) = \frac{16 - 11\sqrt{2} + (4 - 3\sqrt{2})N_2}{32}
\]

which is negative if \( N_2 \geq 2 \). Thus, \( h_F = 1 \) implies \( N_2 = 0 \) or 1.

We give, now, two examples to demonstrate that each of these cases does occur.

**Example 1.** Let the defining equation of \( F = K(x, Y) \) be

\[
Y^4 + (x^3 + x + 1)Y + (x^4 + x^2 + 1) = 0.
\]

Then, \( F/K(x) \) is separable extension of degree 4. The pole of \( K(x) \) is tame in \( F \). In particular, it is unramified. Further, \( \{1, Y, Y^2, Y^3\} \) is integral basis and \( (x^3 + x + 1)^4 \) is the discriminant of \( F/K(x) \). All these facts are easily verified. From the Riemann–Hurwitz genus formula, it follows that \( g_F = 3 \). Considering that \( \{1, Y, Y^2, Y^3\} \) is integral basis,
one verifies without difficulty that $N_1 = 0$ and $N_2 = N_3 = 1$. The numerator of the zeta-function is

$$L(s) = 1 - 3s + 3s^2 - 2s^3 + 6s^4 - 12s^5 + 8s^6.$$  

**Example 2.** Let $F = K(x, Y)$ be defined by the equation

$$Y^3 + xY^2 + (x^2 + x) Y + (x^2 + 1) = 0.$$  

Again, the pole of $s$ in $K(s)$ is tame in $F$ and $(1, Y, Y^2, Y^3)$ is integral basis of $F/K(s)$. The discriminant is $(x^2 + x + 1)^2$ and, hence, the genus is 3. Reduction modulo primes of $K(s)$ of degree $\geq 2$ and $\geq 3$ shows that $N_1 = 0 = N_2$ and $N_3 = 1$. The numerator of the zeta-function is

$$L(s) = 1 - 3s + 2s^2 + s^3 + 4s^4 - 12s^5 + 8s^6.$$  

**Remark.** Following the procedure of § 4, one could determine all fields of genus 3 with class number one. However, we do not pursue this question here.

**References**


DEPARTMENT OF MATHEMATICS  
OHIO STATE UNIVERSITY  
Columbus, Ohio

Received on 23 February 1972 (186)