CLASS NUMBER IN CONSTANT EXTENSIONS OF FUNCTION FIELDS

JAMES R. C. LEITZEL

Abstract. Let $F/K$ be a function field in one variable of genus $g$ having the finite field $K$ as exact field of constants. Suppose $p$ is a rational prime not dividing the class number of $F$. In this paper an upper bound is derived for the degree of a constant extension $E$ necessary to have $p$ occur as a divisor of the class number of the field $E$.

Throughout this paper the term “function field” will mean a function field in one variable whose exact field of constants is a finite field with $q$ elements.

Let $F/K$ be a function field. The order of the finite group of divisor classes of degree zero is the class number $h_F$. For $F/K$ of genus $g$, we use the notation of [2] and denote by $L(u)$ the polynomial numerator of the zeta function of $F$. It follows from the functional equation of the zeta function that

$$L(u) = 1 + a_1 u + a_2 u^2 + \cdots$$
$$+ a_g u^g + q a_{g-1} u^{g+1} + \cdots + q^{g-1} a_1 u^{2g} + q^g u^{2g}$$

and $L(u) \in \mathbb{Z}[u]$, $\mathbb{Z}$ the rational integers. Furthermore the class number $h_F = L(1)$. If $E/F$ is a constant field extension of degree $n$, then the polynomial numerator $L_n(u)$ of the zeta function for $E$ is given by

$$L_n(u) = 1 + b_1 u + \cdots + b_g u^g + q^n b_{g-1} u^{g+1} + \cdots + q^{ng} u^{2g}$$

where the coefficients $b_j$ ($j=1, \cdots, g$) are, with appropriate sign, the elementary symmetric functions of the $n$th powers of the reciprocals of the roots of (1). The genus of $E$ is the same as that of $F$ because $F$ is conservative.

In this paper we give an upper bound for the degree of a constant extension $E$ of $F$ necessary to have a predetermined prime $p$ occur as a
THEOREM 1. Let $F$ be a function field of genus $g$ and $p$ a rational prime. If $p \nmid h_E$ then $p \mid h_E$ for $E$ a constant extension of $F$ of degree $m$ where

(a) $m = p^{r(g)} - 1$ if $p \neq \text{char } K$ and $f = \text{ord } q (p)$.

(b) $m = p^{r(g)} - 1$ if $p = \text{char } K$ and $L(u) \neq 1$ in $\mathbb{Z}_p[u]$.

Here $r(g)$ denotes the least common multiple of the integers $1, 2, \cdots, g$.

1. We collect here some results from the theory of equations. For $K$ a field, we say $f(x) \in K[x]$ is a reciprocal polynomial if and only if $f(x) = x \deg f(1/x)$ [1, Vol. 1, §32]. Observe that if $f(x) = a_0 + a_1x + \cdots + x^n$ and $f(x)$ is a reciprocal polynomial then $a_{n-i} = a_i$, $i = 1, \cdots, [n/2]$, since necessarily $a_0 = 1$.

LEMMA 1. Let $K$ be a finite field, $f(x) \in K[x]$ a monic reciprocal polynomial of even degree $2m$. Let $E$ be a splitting field for $f(x)$ over $K$, then $[E:K] \leq 2r(m)$, where $r(m)$ is the least common multiple of the integers $1, 2, \cdots, m$.

PROOF. Suppose

$$f(x) = x^{2m} + a_1 x^{2m-1} + \cdots + a_m x^m + \cdots + a_1 x + 1.$$ 

Dividing by $x^m$ and combining terms we get

$$f(x)/x^m = (x^m + 1/x^m) + a_1(x^{m-1} + 1/x^{m-1})$$
\[+ \cdots + a_{m-1}(x + 1/x) + a_m.\]

Set $z = x + 1/x$ and for nonnegative integers $s$, $W_s = x^s + 1/x^s$. It is easy to verify that $W_{s+1} = z W_s - W_{s-1}$. Substituting into (3) we get a polynomial $g(z)$ of degree $m$. Since $z = x + 1/x$ the roots of $f(x)$ can be obtained from the roots of $g(z)$ by solving quadratic polynomials. Since finite fields have cyclic galois groups we have from elementary field theory that $g(z)$ splits in an extension of degree at most $r(m)$. For a finite field there is a unique quadratic extension, so a splitting field $E$ for $f(x)$ has degree dividing $2r(m)$.

Now let $K$ be arbitrary and $f(x) \in K[x]$ with degree $f = n$. Then if $x_1, \cdots, x_n$ are the roots of $f(x)$ in a splitting field the sums of the $k$th powers of these roots are elements in $K$. In fact if we let $S_k = \sum_{i=1}^n x_i^k$, then the following relations hold [4, p. 81]:

$$S_k = S_{k-1} x_1 - S_{k-2} x_2 + \cdots + (-1)^{k+1} k x_k \quad \text{for } k \leq n,$$
\[S_k = S_{k-1} x_1 - S_{k-2} x_2 + \cdots + (-1)^{n+1} S_{k-n} x_n \quad \text{for } k > n\]

where $x_i (i = 1, \cdots, n)$ are the elementary symmetric functions of the roots.
Lemma 2. Let \( Z \) denote the rational integers, \( f(x) \in Z[x] \) a monic polynomial. Let \( p \) be a rational prime and \( f^*(x) \in Z_p[x] \) the image of \( f(x) \) under the canonical homomorphism of \( Z[x] \to Z_p[x] \). Let \( S_k (S^*_k) \) denote the sum of the \( k \)th powers of the roots of \( f(x) (f^*(x)) \). Then for all \( k \) we have \( S_k \equiv S^*_k \pmod{p} \).

Proof. Let \( \sigma_i (\sigma^*_i), i=1, \ldots, \deg f \), denote the elementary symmetric functions of the roots of \( f(x) (f^*(x)) \). Since the coefficients of \( f(x) (f^*(x)) \) are, with appropriate sign, these elementary symmetric functions we have \( \sigma_i \equiv \sigma^*_i \pmod{p} \) for all \( i \) by definition. The conclusion then follows from the relations given in (4).

Corollary 2.1. If \( f(x) \in Z[x] \) is a monic polynomial of degree \( 2m \) and \( p \) a prime in \( Z \) such that \( f^*(x) \in Z_p[x] \) is a reciprocal polynomial we have

\[
S_{p^{2r(m)-1}} \equiv 2^m (p).
\]

Proof. By Lemma 1 if \( [E:Z_p]=2r(m) \) then \( E \) contains a splitting field for \( f^*(x) \). In \( E \), every \( \beta \neq 0 \) satisfies \( \beta^{p^{2r(m)-1}}=1 \). Therefore by Lemma 2,

\[
S_{p^{2r(m)-1}} \equiv S^*_{p^{2r(m)-1}} \equiv 2^m (p).
\]

It is clear from (4) that the elementary symmetric functions of the roots of a polynomial can be expressed in terms of the \( S_k \). In fact [1, Vol. 2, p. 39] if \( f(x)=x^n+\sum_{r=1}^{n} a_r x^{n-r} \) then for \( r=1, \ldots, n \) we have

\[
(5)
\]

\[
r! a_r = (-1)^r \det A_r
\]

where \( A_r \) is the \( r \times r \) matrix given by

\[
(6)
\]

In the work that follows we will need to compute the determinant of matrices of the form (6) where the entries \( S_i \) have particular values. All of these are of the general type described in the next result.
Lemma 3. Let \( x, a, k \) be nonnegative integers with \( k \mid x \), say \( x = ky \). Let \( A \) be the \( r \times r \) matrix
\[
A = \begin{pmatrix}
x \\ xa \\ xa^2 \\ \vdots \\ xa^{r-1} \\ xa^r
\end{pmatrix}
\begin{pmatrix}
k & 0 & \cdots & 0 \\ xa & 2k & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ xa^{r-1} & \cdots & (r-1)k & xa
\end{pmatrix}
\]
then \( \det A = k^r a^r \prod_{j=0}^{r-1} (y-j) \).

Proof. Simply use elementary column operations and cofactor expansions; i.e., begin by subtracting \( a \) times column 2 from column 1 and then expand by cofactors of the resulting column 1.

2. Proof of Theorem 1(a). Let \( p \) be a prime and \( F/K \) a function field of genus \( g \). Since constant extensions are essentially unique, we first make the constant extension of degree \( f = \text{ord } q (p) \). Thus without loss of generality we assume that \( F/K \) is a function field with \( |K| = q = 1 \ (p) \) and \( p \neq \text{char } K \). Let \( L(u) \) be the polynomial numerator of the zeta function of \( F \). Because of our assumptions on \( p \) and \( q \) and the form (1) of \( L(u) \) we see that \( L^*(u) \in Z_p[u] \) is a reciprocal polynomial of degree \( 2g \). Hence from Corollary 2.1 we have, for \( S_n \) denoting the sums of the \( n \)th powers of the reciprocals of the roots of \( L(u) \),
\[
S_{k(\varphi(p)-1)} = 2g \ (p), \quad k \in \mathbb{Z}^+.
\]
Let \( m = p^{\varphi(p)-1} - 1 \). The coefficients of \( L_m(u) \) can be computed from (5); namely, \( r! b_r = (-1)^r \det A_r^{(m)} \), where
\[
A_r^{(m)} = \begin{pmatrix}
S_m & 1 & \cdots & 0 \\
S_{2m} & S_m & 2 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
S_{rm} & S_{(r-1)m} & \cdots & S_m
\end{pmatrix}
\]
Using \( S_{km} = 2g \ (p) \) and Lemma 3 with \( x = 2g \), \( a = k = 1 \), we deduce
\[
b_r = (-1)^r \binom{2g}{r} (p).
\]
Moreover
\[ h_E = L_m(1) = 1 + q^m + \sum_{i=1}^{q-1} (1 + q^{m(p-i)})b_i + b_v. \]

Substituting from (8) we get
\[ h_E \equiv 2 + 2 \sum_{i=1}^{q-1} (-1)^i \binom{2g}{i} + (-1)^g \binom{2g}{g} (p). \]

Observing that \((-1)^i \binom{2g}{i} = (-1)^{2g-i} \binom{2g-i}{g-i}\) we conclude
\[ h_E \equiv \sum_{i=0}^{2g} (-1)^i \binom{2g}{i} \equiv 0 (p). \]

3. Proof of Theorem 1(b). Suppose now \(F/K\) is a function field of genus \(g\), and \(p\) a prime with \(p = \text{char } K\). Let \(L(u)\) as given by (1) denote the polynomial numerator of the zeta function of \(F\). Assume that \(L^*(u) \not\equiv 1\) in \(Z_p[u]\) and set \(t = \max \{j\mid \text{such that } a_j \not\equiv 0 (p)\}\). Clearly \(1 \leq t \leq g\). Consequently \(L^*(u)\) is a polynomial of degree \(t\) and therefore splits in the extension of \(Z_p\) of degree \(r(t)\). As before denoting by \(S^*_n\) the sum of the \(n\)th powers of the reciprocals of the roots of \(L^*(u)\), we have, as in Corollary 2.1,
\[ S_{k(t^r(t),-1)} = t (p), \quad k \in Z^+. \]

If \(E\) is the constant extension of degree \(m = p^r(t) - 1\), then to compute \(h_E\) we need the coefficients \(b_i (i=1, \ldots, g)\) of \(L_m(u)\) as given by (2).

From Lemma 3 with \(x=t\), \(a=k=1\) we see
\[ b_j \equiv (-1)^j \binom{t}{j} (p), \quad j = 1, \ldots, t, \]
\[ b_j \equiv 0 (p), \quad j = t + 1, \ldots, g. \]

Then
\[ h_E = L_m(1) = 1 + q^m + \sum_{i=1}^{q-1} b_i (1 + q^{m(p-i)}) + b_v \]
gives, after substitution from (12) and \(q \equiv 0 (p)\),
\[ h_E \equiv 1 + \sum_{i=1}^{t} (-1)^i \binom{t}{i} (p), \]
i.e., \(h_E \equiv \sum_{i=0}^{t} (-1)^i \binom{t}{i} \equiv 0 (p)\). Since \(p^r(t) - 1 \mid p^r(p) - 1\) we have Theorem 1(b).

Note. If \(L(u) \not\equiv 1 (p)\) we can extend the argument to produce a value \(m'\) such that the constant extension \(E/F\) of degree \(m'\) has \(h_E\) divisible by
From Leitzel [3, Theorem 2], we have if \( p | h_M \) and \( T/M \) is the constant extension of degree \( p \) then \( h_T \) is divisible by at least \( p^2 \), since the \( p \)-rank of \( h_M \) is larger than one. Thus \( h_E \) is divisible by \( p^s, s \geq 1 \), if \( E/F \) is the constant extension of degree \( m' = mp^{s-1} \), where \( m \) is the value determined in the above Theorem 1.

I am indebted to the referee for indicating the following more direct proof of this extended result: We have \( L(u) = \prod_{i=1}^{2g} (1 - w_i u) \) where the \( w_i \) are algebraic integers. Let \( L' \) be the splitting field of \( L(u) \) over \( Q \). Let \( P \) be a prime of \( L' \) dividing \( p \). Then \( P \nmid w_i \) for at least one \( i \) (since otherwise \( L(u) \equiv 1 \mod P \), and thus also \( \mod p \)). Let \( L' = Q(w_i) \) and \( P' \) the prime of \( L' \) divisible by \( P \). Then \( e'f' \leq 2g \) where \( e' \) and \( f' \) are ramification index and residue class degree of \( P' \) over \( Q \). Also, the order of the multiplicative group of the residue class ring of the integers in \( L' \) modulo \( P' \) is \( m = (p' - 1)p^{e'(s-1)+1} \). Thus \( w_i \equiv 1 \mod P' \) and so \( h_E = L_m(1) \equiv 0 \mod P' \). But then, \( h_E \equiv 0 \mod p^s \). Arguments similar to those of Theorem 1 can be applied to show that \( m \) can be taken as \( (p^{2g} - 1)/p \) in case (a) (where \( p \mid q \)) and \( (p^{2g} - 1)/p \) in case (b) (where \( p \mid q \)).

4. **An additional comment.** In §3 we discussed the situation where \( F/K \) is a function field of genus \( g \), \( p = \text{char } K \), and \( L^*(u) \neq 1 \) in \( Z_p[u] \). In this section we discuss the case \( L^*(u) \equiv 1 \) in \( Z_p[u] \).

Let \( F/K \) be a function field of genus \( g \) and \( p \) a prime. Suppose \( L(u) \), the polynomial numerator of the zeta function of \( F \) as given by (1), satisfies the condition

\[
a_i \equiv 0 \mod p, \quad i = 1, \ldots, g.
\]

Then \( L^*(u) = 1 + q^g u^{2g} \) in \( Z_p[u] \) if \( p \neq \text{char } K \) and \( L^*(u) \equiv 1 \) in \( Z_p[u] \) if \( p = \text{char } K \). For a function field satisfying the condition (14) we give an explicit congruence relation for the class number \( h_K \) of any constant extension \( E/F \). This is contained in

**Theorem 2.** Let \( F/K \) be a function field of genus \( g \) and \( p \) a prime. Suppose \( L^*(u) = 1 + q^g u^{2g} \) in \( Z_p[u] \) and \( E/F \) is a constant extension of degree \( m \). Then if \( d = \gcd(m, 2g) \) we have

\[
h_K \equiv [1 - (-1)^{m/d}q^{d|d|^g}] \mod p.
\]

**Proof.** Let \( S_n \) again denote the sum of the \( n \)-th powers of the reciprocals of the roots of \( L(u) \). From our assumption on \( L(u) \) and the relations of (4) we deduce

\[
S_n \equiv 0 \mod p, \quad \text{if } 2g \nmid n,
\]

\[
S_n \equiv (-1)^{2gq^{2g}} \mod p, \quad \text{if } n = 2gk.
\]

To compute \( h_K \) for \( E/F \) a constant extension of degree \( m \) it is necessary to determine the coefficients of \( L_m(u) \). These all require the computation of
the determinant of a matrix of the type (7). Because of the relations (16), nonzero entries occur only when \(jm\equiv0 (2g), j=1, \ldots, r\). If \(d=\gcd(m, 2g)\) and \(m=td, 2g=kd\), then the values of \(j\) which yield nonzero entries are precisely \(lk\) for \(1\leq l\leq[d/2]\). Thus using this observation we can express the coefficients as

\[
\frac{(-1)^{2lk-l}}{(lk)!} \frac{(lk-1)!}{k2k \ldots (l-1)k} \times \det \begin{pmatrix}
S_{km} & k & \cdots & 0 \\
S_{2km} & S_{km} & 2k & \cdots & 0 \\
& \ddots & \ddots & \ddots & \ddots \\
& & & S_{(l-1)km} & \cdots & (l-1)k \\
S_{tkm} & & & & & S_{km}
\end{pmatrix}
\tag{17}
\]

Here we have used (16) and cofactor expansions along rows to get the final form. Now apply Lemma 3 with \(x=2g=kd\) and \(a=(-q^\sigma)^{m/d}\). We have then

\[
b_{lk} \equiv \frac{(-1)^{2lk-l}}{l!k!} k'(-q^\sigma)^{m/d} \sum_{j=0}^{d-1} (d - j) (p).
\tag{18}
\]

Substituting this information in

\[
h_E = L_m(1) = 1 + q^\sigma + \sum_{i=1}^{\lfloor d/2 \rfloor} b_i(1 + q^{m(i-1)}) + b_s
\]

we find, for odd \(d\),

\[
h_E \equiv 1 + q^\sigma + \sum_{i=1}^{\lfloor d/2 \rfloor} b_i(1 + q^{m(i-k)}}(p)
\]
or

\[
h_E \equiv 1 + q^\sigma + \sum_{i=1}^{\lfloor d/2 \rfloor} (1 + q^{m(i-k)})\{-1\}^{2lk-l}(-q^\sigma)^{m/d}(d\text{ d}) (p).
\]

Since

\[
q^m(\sigma-k\sigma)(-1)^{l}(-q^\sigma)^{m/d}(d\text{ d}) = (-1)^{d-l}(-q^\sigma)^{m(d-1)/d}
\]

and \(m+d\equiv0 (2)\) this can be rewritten as

\[
h_E \equiv \sum_{l=0}^{d} (-1)^{l}(d\text{ d})((-1)^{m/d}q^\sigma)^{l} (p).
\tag{19}
\]
If $d$ is even a similar argument leads to the same formula. Hence

$$h_E \equiv [1 - (-1)^{m/d} q^{m/2}] (p).$$

**Corollary 1.** If $\gcd(m, 2g) = 1$, then $h_E \equiv 1 + q^{m/2} (p)$.

**Proof.** $(m, 2g) = 1$ forces $d = 1$ and $m \equiv 1 (2)$.

**Corollary 2.** If $2g | m$, then for $m = 2gt$ we have $h_E \equiv [1 - (-1)^{g^2}]^{2g} (p)$.

**Corollary 3.** If $p = \text{char} K$ and $L(u) \equiv 1$ in $\mathbb{Z}_p[u]$ then $p \nmid h_E$ for any constant extension $E/F$.

**Proof.** Clearly $h_E \equiv 1 (p)$ in this case.

**Bibliography**


