PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 36, Number 1, November 1972

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

$$(1)\qquad \begin{aligned} L(u) = 1 &+ a_1u + a_2u^2 + \cdots \\ &+ a_gu^g + qa_{g-1}u^{g+1} + \cdots + q^{g-1}a_1u^{2g-1} + q^gu^{2g} \end{aligned}$$

and $L(u) \in Z[u]$, 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

$$(2)\qquad L_n(u) = 1 + b_1u + \cdots + b_gu^g + q^nb_{g-1}u^{g+1} + \cdots + q^{ng}u^{2g}$$

where the coefficients b_j $(j=1, \cdots, g)$ are, with appropriate sign, the elementary symmetric functions of the nth 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

Received by the editors September 10, 1971 and, in revised form, March 12, 1972.
AMS 1969 *subject classifications*. Primary 1078; Secondary 1278, 1435.
Key words and phrases. Zeta function, constant extension, reciprocal polynomials.

divisor of the class number h_E. Precisely, we prove

THEOREM 1. *Let F/K be a function field of genus g and p a rational prime. If $p\nmid h_F$ then $p|h_E$ for E a constant extension of F of degree m where*
(a) $m=f(p^{2r(g)}-1)$ *if* $p\neq\text{char } K$ *and* $f=\text{ord}\, q\ (p)$.
(b) $m=p^{r(g)}-1$ *if* $p=\text{char } K$ *and* $L(u)\not\equiv 1$ *in* $Z_p[u]$.
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 $f(x)=x^{\deg f}f(1/x)$ [**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 $[E:K]|2r(m)$, where $r(m)$ is the least common multiple of the integers* $1, 2, \cdots, m$.

PROOF. Suppose

$$f(x)=x^{2m}+a_1x^{2m-1}+\cdots+a_mx^m+\cdots+a_1x+1.$$

Dividing by x^m and combining terms we get

$$f(x)/x^m=(x^m+1/x^m)+a_1(x^{m-1}+1/x^{m-1}) + \cdots + a_{m-1}(x+1/x)+a_m. \tag{3}$$

Set $z=x+1/x$ and for nonnegative integers s, $W_s=x^s+1/x^s$. It is easy to verify that $W_{s+1}=zW_s-W_{s-1}$. 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 $\alpha_1,\cdots,\alpha_n$ are the roots of $f(x)$ in a splitting field the sums of the kth powers of these roots are elements in K. In fact if we let $S_k=\sum_{i=1}^n\alpha_i^k$, then the following relations hold [**4**, p. 81]:

$$\begin{aligned} S_k &= S_{k-1}\sigma_1-S_{k-2}\sigma_2+\cdots+(-1)^{k+1}k\sigma_k \qquad \text{for } k\leqq n,\\ S_k &= S_{k-1}\sigma_1-S_{k-2}\sigma_2+\cdots+(-1)^{n+1}S_{k-n}\sigma_n \quad \text{for } k>n \end{aligned} \tag{4}$$

where σ_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 kth powers of the roots of $f(x)$ ($f^*(x)$). Then for all k we have $S_k \equiv S_k^*$ (p).*

PROOF. Let σ_i (σ_i^*), $i=1, \cdots, \deg f$, 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 $\sigma_i \equiv \sigma_i^*$ (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*

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

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,

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

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 $r=1, \cdots, n$ we have

$$r!\, a_r = (-1)^r \det A_r \tag{5}$$

where A_r is the $r \times r$ matrix given by

$$A_r = \begin{pmatrix} S_1 & 1 & 0 & \cdots & 0 \\ S_2 & S_1 & 2 & \cdots & 0 \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ S_{r-1} & S_{r-2} & & \cdots & r-1 \\ S_r & S_{r-1} & & \cdots & S_1 \end{pmatrix}. \tag{6}$$

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 $k|x$, say $x=ky$. Let A be the $r\times r$ matrix*

$$A = \begin{pmatrix} xa & k & 0 & \cdots & 0 \\ xa^2 & xa & 2k & \cdots & 0 \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ xa^{r-1} & xa^{r-2} & & \cdots & (r-1)k \\ xa^r & xa^{r-1} & & \cdots & xa \end{pmatrix};$$

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 $f=\operatorname{ord} q\ (p)$. Thus without loss of generality we assume that F/K is a function field with $|K|=q\equiv 1\ (p)$ and $p\neq \operatorname{char} K$. 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 nth powers of the reciprocals of the roots of $L(u)$,

$$S_{k(p^{2r(g)}-1)} \equiv 2g\ (p), \qquad k\in Z^+.$$

Let $m=p^{2r(g)}-1$. The coefficients of $L_m(u)$ can be computed from (5); namely, $r!\,b_r=(-1)^r \det A_r^{(m)}$, where

(7) $$A_r^{(m)} = \begin{pmatrix} S_m & 1 & & \cdots & 0 \\ S_{2m} & S_m & 2 & \cdots & 0 \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ S_{rm} & S_{(r-1)m} & & \cdots & S_m \end{pmatrix}.$$

Using $S_{km}\equiv 2g\ (p)$ and Lemma 3 with $x=2g$, $a=k=1$, we deduce

(8) $$b_r \equiv (-1)^r \binom{2g}{r}\ (p).$$

Moreover

$$h_E = L_m(1) = 1 + q^{mg} + \sum_{i=1}^{g-1} (1 + q^{m(g-i)})b_i + b_g.$$

Substituting from (8) we get

$$(9) \qquad h_E \equiv 2 + 2\sum_{i=1}^{g-1} (-1)^i \binom{2g}{i} + (-1)^g \binom{2g}{g} \ (p).$$

Observing that $(-1)^i\binom{2g}{i} = (-1)^{2g-i}\binom{2g}{2g-i}$ we conclude

$$(10) \qquad h_E \equiv \sum_{i=0}^{2g} (-1)^i \binom{2g}{i} \equiv 0 \ (p).$$

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 $1 \leqq t \leqq g$. 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 nth powers of the reciprocals of the roots of $L^*(u)$, we have, as in Corollary 2.1,

$$(11) \qquad S_{k(p^{r(t)}-1)} \equiv t \ (p), \qquad k \in Z^+.$$

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

From Lemma 3 with $x = t$, $a = k = 1$ we see

$$(12) \qquad \begin{aligned} b_j &\equiv (-1)^j \binom{t}{j} \ (p), \qquad && j = 1, \cdots, t, \\ b_j &\equiv 0 \ (p), && j = t + 1, \cdots, g. \end{aligned}$$

Then

$$h_E = L_m(1) = 1 + q^{mg} + \sum_{i=1}^{g-1} b_i(1 + q^{m(g-i)}) + b_g$$

gives, after substitution from (12) and $q \equiv 0 \ (p)$,

$$(13) \qquad h_E \equiv 1 + \sum_{i=1}^{t} (-1)^i \binom{t}{i} \ (p),$$

i.e., $h_E \equiv \sum_{i=0}^{t} (-1)^i \binom{t}{i} \equiv 0 \ (p)$. Since $p^{r(t)} - 1 \mid p^{r(g)} - 1$ 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

p^s, $s \geqq 1$. 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, $s \geqq 1$, 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 $L(u) \equiv 1 \pmod P$, and thus also $\pmod p$)). Let $L' = Q(w_i)$ and P' the prime of L' divisible by P. Then $e'f' \leqq 2g$ 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 $P'^{e'(s-1)+1}$ is $m = (p^{f'} - 1)p^{e'f'(s-1)}$. Thus $w_i^m \equiv 1 \pmod{P'^{e'(s-1)+1}}$ and so $h_E = L_m(1) \equiv 0 \pmod{P'^{e'(s-1)+1}}$. But then, $h_E \equiv 0 \pmod{p^s}$. Arguments similar to those of Theorem 1 can be applied to show that m can be taken as $f(p^{2r(g)} - 1)p^{2g(s-1)}$ in case (a) (where $p \nmid q$) and $(p^{r(g)} - 1)^{pg(s-1)}$ in case (b) (where $p|q$).

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 $L^*(u) \not\equiv 1$ 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

$$a_i \equiv 0 \ (p), \qquad i = 1, \cdots, g. \tag{14}$$

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_E 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*

$$h_E \equiv [1 - (-1)^{m/d} q^{gm/d}]^d \ (p). \tag{15}$$

PROOF. Let S_n again denote the sum of the nth powers of the reciprocals of the roots of $L(u)$. From our assumption on $L(u)$ and the relations of (4) we deduce

$$\begin{aligned} S_n &\equiv 0 \ (p) && \text{if } 2g \nmid n, \\ S_n &\equiv (-1)^k 2g q^{kg} \ (p) && \text{if } n = 2gk. \end{aligned} \tag{16}$$

To compute h_E 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 $jm \equiv 0\ (2g)$, $j=1, \cdots, r$. If $d=\gcd(m, 2g)$ and $m=td$, $2g=kd$, then the values of j which yield nonzero entries are precisely lk for $1 \leqq l \leqq [d/2]$. Thus using this observation we can express the coefficients as

$$b_{lk} \equiv \frac{(-1)^{2lk-l}}{(lk)!} \frac{(lk-1)!}{k2k \cdots (l-1)k} \times \det \begin{pmatrix} S_{km} & k & & \cdots & 0 \\ S_{2km} & S_{km} & 2k & \cdots & 0 \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ S_{(l-1)km} & & & \cdots & (l-1)k \\ S_{lkm} & & & \cdots & S_{km} \end{pmatrix} (p). \tag{17}$$

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

$$\begin{aligned} b_{lk} &\equiv \frac{(-1)^{2lk-l}}{l!k^l} k^l(-q^g)^{ml/d} \prod_{j=0}^{l-1} (d-j)\,(p) \\ &\equiv (-1)^{2lk-l}(-q^g)^{ml/d}\binom{d}{l}\,(p). \end{aligned} \tag{18}$$

Substituting this information in

$$h_E = L_m(1) = 1 + q^{mg} + \sum_{i=1}^{g-1} b_i(1+q^{m(g-i)}) + b_g$$

we find, for odd d,

$$h_E \equiv 1 + q^{mg} + \sum_{l=1}^{[d/2]} b_{kl}(1+q^{m(g-kl)})\,(p)$$

or

$$h_E \equiv 1 + q^{mg} + \sum_{l=1}^{[d/2]} (1+q^{m(g-kl)})(-1)^{2lk-l}(-q^g)^{ml/d}\binom{d}{l}\,(p).$$

Since

$$q^{m(g-kl)}(-1)^l(-q^g)^{ml/d}\binom{d}{l} = (-1)^{d-l}\binom{d}{d-l}(-q^g)^{m(d-l)/d}$$

and $m+d \equiv 0\ (2)$ this can be rewritten as

$$h_E \equiv \sum_{l=0}^{d} (-1)^l \binom{d}{l}((-1)^{m/d}q^{mg/d})^l\,(p). \tag{19}$$

If d is even a similar argument leads to the same formula. Hence

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

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

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

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

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

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

BIBLIOGRAPHY

1. W. S. Burnside and A. W. Panton, *The theory of equations: With an introduction to the theory of binary algebraic forms*. Vols. 1, 2, Dover, New York, 1960. MR **22** #6784.

2. M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Birkhäuser, Basel, 1963; English transl., Pure and Appl. Math., vol. 23, Academic Press, New York, 1966. MR **29** #5821; MR **35** #160.

3. J. R. C. Leitzel, *Galois cohomology and class number in constant extensions of algebraic function fields*, Proc. Amer. Math. Soc. **22** (1969), 206–208. MR **39** #4126.

4. B. L. van der Waerden, *Moderne Algebra*. Vol. 1, 2nd rev. ed., English transl., Ungar, New York, 1953.

DEPARTMENT OF MATHEMATICS, OHIO STATE UNIVERSITY, COLUMBUS, OHIO 43210