CLASS NUMBER IN CONSTANT EXTENSIONS OF ELLIPTIC FUNCTION FIELDS

JAMES R. C. LEITZEL

ABSTRACT. For F/K a function field of genus one having the finite field K as field of constants and E the constant extension of degree n we give explicitly the class number of the field E as a polynomial expression in terms of the class number of F and the order of the field K. Applications are made to determine the degree of a constant extension E necessary to have a predetermined prime p occur as a divisor of the class number of the field E.

Let F/K be a function field in one variable with exact field of constants K, a finite field having q elements. The order of the finite group of divisor classes of degree zero is the class number h_F. Let E denote the constant extension of degree n and h_E the class number of E. It is known that $h_E = kh_F$ for some integer k. In this note we give an explicit determination of k in the particular case that F has genus one and give several applications of it. Precisely, we prove the

THEOREM. *If F/K is a function field with genus one and E/F is the constant extension of degree n then*

$$h_E = \sum_{l=1}^{n} (-1)^{l-1} c_l h_F^l$$

where

$$c_l = \sum_{j=0}^{[n-l/2]} (-1)^j \frac{n}{n-j} \binom{n-j}{j} \binom{n-2j}{l} q^j (1+q)^{n-2j-l}.$$

The applications give the degree of a constant extension E that must be made for a given prime p to occur as a divisor of h_E.

We begin with some preliminary observations on the zeta function of F and some results on binomial expansions. For a field F as described above, the zeta function is given by

$$\zeta_F(s) = \frac{L(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

where $L(u)$ is a polynomial with rational integral coefficients of degree $2g$, g the genus of F, [2]. It is known that $L(1) = h_F$. In fact if $L(u) = \sum_{i=0}^{2g} a_i u^i = \prod_{i=1}^{2g} (1 - \alpha_i u)$ we have $a_0 = 1$, $a_{2g} = q^g$, and

Received by the editors September 2, 1969.

AMS Subject Classifications. Primary 1078; Secondary 1278, 1435.

Key Words and Phrases. Genus one, constant extension, binomial expansions.

$a_1 = N_1 - (1+q)$. Here N_1 denotes the number of prime divisors of degree one for the field F. In a constant extension of degree n the polynomial numerator is given by

$$L_n(u) = \prod_{i=1}^{2g} (1 - \alpha_i^n u).$$

Thus the number of prime divisors of degree one in the extension of degree n is given

$$N_n = 1 + q^n - \sum_{i=1}^{2g} \alpha_i^n. \tag{1}$$

If we assume that F has genus one, then also E has genus one since F is conservative. Hence $L_n(u)$ is a quadratic polynomial for all n and the class number is precisely N_n, the number of prime divisors of degree one. In particular we have $L_F(u) = 1 - [1+q-h_F]u + qu^2$. The formula (1) involves the reciprocals of the roots; hence in our further work we shall be concerned with the following two relations:

(2) $L^*(x) = x^2 - [1+q-h_F]x + q$ with roots α, β.

(3) $h_E = 1 + q^n - (\alpha^n + \beta^n)$ giving the class number for a constant extension of degree n.

As a first step we collect some results on the roots of a quadratic polynomial such as (2). Since we can be more general, we assume we have given a polynomial $x^2 = Px - Q$ with P and Q not necessarily relatively prime. Our discussion is adapted from Lucas [**5**], and we repeat his proofs for convenience. If α, β denote the roots of $x^2 - Px + Q = 0$ then, setting $\delta = \alpha - \beta$, we have the following relations:

$$\begin{aligned} \alpha + \beta &= P, & 2\alpha &= P + \delta, \\ \alpha\beta &= Q, & 2\beta &= P - \delta, \\ \Delta &= P^2 - 4Q, & \delta^2 &= \Delta. \end{aligned} \tag{4}$$

We define $V_n = \alpha^n + \beta^n$ and it is easy to check that we have the following recursion: $V_{n+2} = PV_{n+1} - QV_n$.

In the discussion which follows we make use of two identities which can be found in Chrystal [**1**, pp. 178–179].

$$X^n + Y^n = \sum_{j=0}^{[n/2]} (-1)^j \frac{n}{n-j} \binom{n-j}{j} (XY)^j (X+Y)^{n-2j}, \tag{5}$$

$$\frac{X^{n+1} - Y^{n+1}}{X - Y} = \sum_{j=0}^{[n/2]} (-1)^j \binom{n-j}{j} (XY)^j (X+Y)^{n-2j}. \tag{6}$$

From the relations in (4) we have

$$2^n\alpha^n = (P+\delta)^n = \sum_{\nu=0}^{n}\binom{n}{\nu}P^{n-\nu}\delta^\nu, \tag{7}$$

$$2^n\beta^n = (P-\delta)^n = \sum_{\nu=0}^{n}(-1)^\nu\binom{n}{\nu}P^{n-\nu}\delta^\nu. \tag{8}$$

Adding these we conclude, using the definition of V_n and (4),

$$2^nV_n = (P+\delta)^n + (P-\delta)^n = 2\sum_{\nu=0}^{n}\binom{n}{\nu}P^{n-\nu}\delta^\nu \qquad (\nu \text{ even}) \tag{9}$$

which gives

$$2^{n-1}V_n = \sum_{j=0}^{[n/2]}\binom{n}{2j}P^{n-2j}\Delta^j. \tag{10}$$

On the other hand if we set $X=P+\delta$, $Y=P-\delta$ in (5) we conclude

$$2^nV_n = \sum_{j=0}^{[n/2]}(-1)^j\frac{n}{n-j}\binom{n-j}{j}(4Q)^j(2P)^{n-2j} \tag{11}$$

which after simplification yields

$$V_n = \sum_{j=0}^{[n/2]}(-1)^j\frac{n}{n-j}\binom{n-j}{j}Q^jP^{n-2j}. \tag{12}$$

LEMMA 1. *If p is a prime and $p|P$, then $V_n\equiv(-Q)^{n/2}V_0(p)$ if n is even and $V_n\equiv 0\ (p)$ if n is odd.*

PROOF. From the recursion relations on V_n we see $V_2\equiv -QV_0\ (p)$, $V_3\equiv 0\ (p)$ and the result follows by induction.

LEMMA 2. *If p is an odd prime, then*
(a) *if $(\Delta/p)=1$ we have $V_{p-1}\equiv 2\ (p)$ and*
(b) *if $(\Delta/p)=-1$ we have $V_{p+1}\equiv 2Q\ (p)$.*

PROOF. (a) Since $\Delta^{(p-1)/2}\equiv 1\ (p)$ setting $n=p-1$ in (10) gives

$$2^{p-2}V_{p-1} = P^{p-1} + \binom{p-1}{2}P^{p-3}\Delta + \cdots + \Delta^{(p-1)/2}.$$

But

$$\binom{p-1}{2j} \equiv 1\ (p);$$

thus we have

$$2^{p-2}V_{p-1} \equiv \frac{P^{p+1} - \Delta^{(p+1)/2}}{P^2 - \Delta} \ (p).$$

Now $P^{p+1} \equiv P^2 \ (p)$ and $\Delta^{(p+1)/2} \equiv \Delta \ (p)$; thus

$$2^{p-2}V_{p-1} \equiv 1 \ (p)$$

and (a) follows.

If $(\Delta/p) = -1$ then $\Delta^{(p-1)/2} \equiv -1 \ (p)$ and setting $n = p+1$ in (10) gives

$$2^pV_{p+1} = P^{p+1} + \binom{p+1}{2} P^{p-1}\Delta + \cdots + \Delta^{(p+1)/2}$$

but

$$\binom{p+1}{2j} \equiv 0 \ (p).$$

Thus $2V_{p+1} \equiv 2^pV_{p+1} \equiv P^2 - \Delta \equiv 4Q \ (p)$ and (b) follows.

Proof of theorem. Specializing these comments now to (2) we have $P = 1 + q - h_F$ and $Q = q$. Thus from (12) we get

$$(13) \qquad V_n = \sum_{j=0}^{[n/2]} (-1)^j \frac{n}{n-j} \binom{n-j}{j} q^j [1 + q - h_F]^{n-2j}.$$

Rearranging terms in (13) to give a polynomial expression in h_F we find

$$(14) \qquad V_n = \sum_{l=0}^{n} (-1)^l c_l h_F^l$$

where

$$(15) \qquad c_l = \sum_{j=0}^{[n-l/2]} (-1)^j \frac{n}{n-j} \binom{n-j}{j} \binom{n-2j}{l} q^j (1+q)^{n-2j-l}.$$

The c_l are rational integers since

$$\frac{n}{n-j}\binom{n-j}{j} = \frac{n}{j}\binom{n-j-1}{j-1} = 2\binom{n-j}{j} - \binom{n-j-1}{j}.$$

It is easy to check that $c_n = 1$ and $c_{n-1} = n(1+q)$. Using the identity (5) we find $c_0 = 1 + q^n$ and (6) gives $c_1 = n((q^n - 1)/(q-1))$. Substituting (14) and the value of c_0 in (3) we find

$$(16) \qquad h_E = \sum_{l=1}^{n} (-1)^{l-1} c_l h_F^l.$$

Consequently since $h_E = kh_F$ we have explicitly determined k as a polynomial expression in h_F; namely

$$k = \sum_{l=1}^{n} (-1)^{l-1} c_l h_F^{l-1}. \tag{17}$$

We state our applications of these results in the following propositions:

Proposition 1. *If $p = \mathrm{char}\ F$ then*

(a) *if $h_F \equiv 1$ (p) we have $h_E \equiv 1$ (p) for all finite constant extensions E;*

(b) *if $h_F \not\equiv 1$ (p) and $f = \mathrm{ord}\ (1-h_F) \bmod p$ then $h_E = 0$ (p) for $\deg(E/F) = f$.*

Proof. From (15) we find $c_l \equiv \binom{n}{l}$ (p) since $q \equiv 0$ (p). Thus from (16) we get

$$h_E \equiv \sum_{l=1}^{n} (-1)^{l-1} \binom{n}{l} h_F^{l} \ (p), \tag{18}$$

which after rewriting becomes

$$h_E \equiv 1 - (1 - h_F)^n \ (p) \tag{19}$$

and the proposition follows.

Note. These conclusions are compatible with statements on the p-rank of the group of divisor classes of degree zero in elliptic function fields of characteristic p over an algebraically closed field of constants as given by Hasse [3].

Proposition 2. *If p is a prime and $p^m \| h_F$, $m \geqq 1$, then $p^{m+1} | h_E$ for a constant extension E/F of degree n if and only if $p | n((q^n - 1)/(q-1))$.*

Proof. From (17) since $p | h_F$ we have $p | k$ if and only if $p | c_1$ and

$$c_1 = n((q^n - 1)/(q - 1)).$$

Corollary. *If $p = \mathrm{char}\ F$ then $p^{m+1} | h_E$ if and only if $p | n$ (Leitzel [4]).*

Proposition 3. *If $p | 1 + q - h_F$ then for a constant extension E of degree n we have*

(a) *$h_E \equiv 1 + q^n$ (p) if n is odd,*

(b) *$h_E \equiv (1 + q^{n/2})^2$ (p) if $n \equiv 2$ (4),*

(c) *$h_E \equiv (1 - q^{n/2})^2$ (p) if $n \equiv 0$ (4).*

Proof. $h_E = 1 + q^n - V_n$ so this follows directly from Lemma 1, and $V_0 = 2$.

PROPOSITION 4. *If* char $F \neq 2$ *and* E/F *is the constant extension of degree* 3 *then* $h_E \equiv 0$ (2).

PROOF. We may assume $2 \nmid h_F$. Then $q \equiv 1$ (2) and from (17) we have $k = c_1 + c_2 h_F + c_3 h_F^2$, with $h_F \equiv c_1 \equiv c_3 \equiv 1$ (2), $c_2 \equiv 0$ (2).

PROPOSITION 5. *Let* p *be an odd prime,* $p \neq$ char F, *and such that* $|K| = q \equiv 1$ (p). *If* $p \nmid h_F$ *then* $p \mid h_E$ *for* E/F *a constant extension of degree dividing* $(p^2-1)/2$.

PROOF. As earlier let $\Delta = [1+q-h_F]^2 - 4q$. Then since $h_E = 1 + q^n - V_n$ we see from Lemma 2 that if $(\Delta/p) = 1$, $n = p-1$ suffices and if $(\Delta/p) = -1$, $n = p+1$ since $q \equiv 1$ (p). If $p \mid \Delta$ then $(1+q-h_F)^2 - 4q \equiv 0$ (p), and since $q \equiv 1$ (p) we conclude $h_F(4-h_F) \equiv 0$ (p). By hypothesis $p \nmid h_F$ so $h_F \equiv 4$ (p). From (17) with $n = 2$ we find $k = 2(q+1) - h_F$; thus $k \equiv 0$ (p) if $h_F \equiv 4$ (p), and in this case an extension of degree 2 suffices. In all three possibilities $n \mid (p^2-1)/2$.

COROLLARY. *If* p *is an odd prime,* $p \neq$ char F, *then* $p \mid h_E$ *for a constant extension* E/F *of degree dividing* $f((p^2-1)/2)$ *where* $f =$ ord q (p).

BIBLIOGRAPHY

1. G. Chrystal, *A textbook of algebra*. Vol. II, A. and C. Black, Edinburgh, 1889; reprint of 6th ed., Chelsea, New York.

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. H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper*. I, J. Reine Angew. Math. **175** (1936), 55–62.

4. J. Leitzel, *Galois cohomology and class number in constant extensions of algebraic function fields*, Proc. Amer. Math. Soc. 22 (1969), 206–208.

5. E. Lucas, *Théorie des fonctions numériques simplement pérodiques*, Amer. J. Math. **1** (1878), 184–239; 289–321.

OHIO STATE UNIVERSITY, COLUMBUS, OHIO 43210