MATHEMATICS OF COMPUTATION
VOLUME 46, NUMBER 173
JANUARY 1986, PAGES 337-340

Class Numbers of Cyclotomic Function Fields

By K. F. Ireland and R. D. Small

Abstract. Using results of Galovich and Rosen the plus and minus factors for the class number of the cyclotomic function field associated with irreducibles of degree three and four over the field with three elements are computed. As a consequence it is shown that the analogue to a result of Kummer on the p-divisibility of these factors is false.

Consider an odd prime p and let $\mathbf{F}_p$ denote the finite field with p elements. To each monic irreducible polynomial $P(T)$ of degree d with coefficients in $\mathbf{F}_p$ one can associate a cyclic extension K_P of $\mathbf{F}_p(T)$ that enjoys properties analogous to those of the classical cyclotomic number fields $\mathbf{Q}(\zeta_p)$, $\zeta_p = e^{2\pi i/p}$. Such fields were discovered by L. Carlitz in the 1930's and have been studied intensively in recent years by D. Hayes, M. Rosen, S. Galovich, D. Goss and others. If $\mathbf{D}$ is the integral closure of $\mathbf{F}_p[T]$ in K_P, then one has the diagram:

$$\begin{tikzcd} & K_P \arrow[d, dash] \\ \mathbf{D} \arrow[ur, dash] \arrow[d, dash] & \mathbf{F}_p(T) \\ \mathbf{F}_p[T] \arrow[ur, dash] & \end{tikzcd}$$

The following properties hold:

(a) K_P has degree $p^d - 1$ over $\mathbf{F}_p(T)$.

(b) $P(T)$ completely ramifies in K_P.

(c) If $Q(T)$ is monic irreducible, $Q^f \equiv 1\ (P)$, f minimal, then $Q\mathbf{D} = P_1 \cdots P_s$, $s = (p^d - 1)/f$, P_i of relative degree f.

(d) $(1/T)\tilde{\mathbf{D}} = (P_1 \cdots P_r)^{p-1}$, $r = (p^d - 1)/(p - 1)$, where $\tilde{\mathbf{D}}$ is the integral closure of $\mathbf{F}_p[1/T]$ in K_P and P_i are distinct primes of degree 1.

(e) The Galois group of $K_P/\mathbf{F}_p(T)$ can be canonically identified with the multiplicative cyclic group $(\mathbf{F}_p[T]/P(T))^*$.

To explain the important property (e), we define the Carlitz action on the algebraic closure $\mathbf{F}_p(T)^{\mathrm{alg}}$ of $\mathbf{F}_p(T)$. Define operators ψ and μ on $\mathbf{F}_p(T)^{\mathrm{alg}}$ by $\psi(\alpha) = \alpha^p$ and $\mu(\alpha) = T\alpha$. Then ψ and μ are noncommuting operators and one may consider $P(\psi + \mu)u = u^{P(T)}$. It can be shown that $u^{P(T)}/u$ is irreducible. The splitting field of this polynomial is K_P. The action $\alpha \to \alpha^{A(T)}$ gives the additive group of $\mathbf{F}_p(T)^{\mathrm{alg}}$ the structure of a $\mathbf{F}_p[T]$ module. This construction is due to Carlitz. If λ is a fixed root of $u^{P(T)}/u$, then the automorphisms of K_P are given by $\lambda \to \lambda^{A(T)}$ where $A(T) \in (\mathbf{F}_p[T]/P(T))^*$. This explains (e). The arithmetic of the unique quadratic subfield was treated by E. Artin in his thesis [1].

Received July 27, 1984.

1980 *Mathematics Subject Classification*. Primary 12A35, 12A50, 12A90.

If K^+ denotes the maximal subfield in which $1/T$ splits completely, then K^+ has degree $(p^d - 1)/(p - 1)$ and is the fixed field under the subgroup $\mathbf{F}_p^*$ of the Galois group. This field is the correct analogue of the maximal real subfield in the classical case.

For each integer s dividing $p^d - 1$ there is a unique subfield of degree s, denoted by K_s. Thus $K^+ = K_{(p^d-1)/(p-1)}$. Denote by $Z(u, K_s)$ the congruence zeta function of the extension $K_s/\mathbf{F}_p$. Then, according to A. Weil [4, p. 154], one has

$$Z(u, K_s) = \frac{f_s(u)}{(1-u)(1-pu)},$$

where $f_s(u)$ is a polynomial with integer coefficients of degree twice the genus of K_s. The value of $f_s(u)$ at $u = 1$ is the number of divisor classes of degree zero on K_s. We denote this divisor class number by h_s. Let $G = (\mathbf{F}_p[T]/P(T))^*$ and consider the nontrivial complex-valued characters χ on G, that is $\operatorname{Hom}(G, \mathbf{C}^*)$, $\chi \neq \mathrm{id}$. To each such character define the quantities

$$s_j(\chi) = \Sigma\chi(A),$$

the sum being over all elements A of G that are monic and of degree j. Put

$$L^*(u,\chi) = \begin{cases} \sum_{j=0}^{d-1} s_j(\chi)u^j, & \operatorname{ord}\chi \nmid (p^d-1)/(p-1), \\ \sum_{j=0}^{d-1} s_j(\chi)u^j/(1-u), & \operatorname{ord}\chi \mid (p^d-1)/(p-1). \end{cases}$$

Then one can show that

$$Z(u, K_s) = \frac{\Pi L^*(u,\chi)}{(1-u)(1-pu)}, \qquad \operatorname{ord}\chi | s,\ \chi \neq \mathrm{id}.$$

Put $h^+ =$ divisor class number of K^+ and define h^- by $h = h^+h^-$. In the case of cyclotomic number fields it is a well-known conjecture that p never divides $h^+(\mathbf{Q}(\zeta_p))$. This is the so-called Vandiver conjecture. Furthermore, it is a known result of Kummer that if $p | h^+(\mathbf{Q}(\zeta_p))$, then $p | h^-(\mathbf{Q}(\zeta_p))$. These two statements refer, of course, to the ring of integers in $\mathbf{Q}(\zeta_p)$. In the case of function fields there is in general a nontrivial divisor class group concentrated on the primes at infinity. The order of this group is known as the regulator and it is the quotient of the divisor class number given by the zeta function by the regulator that is the class number of the associated ring of integers.

In E. Artin's thesis it is shown that for $p = 3$ and $P(T) = 2 + T^2 + T^4$ the class number of the ring of integers is 3. Since the extensions are totally ramified at P, it can be shown (Rosen [6] and Iwasawa [5]) that 3 also divides the class number of the ring of integers in K^+. Using a program devised by R. D. Small, we found that, in this case,

$$h^+ = 2^7 \cdot 3 \cdot 11^2 \cdot 17 \cdot 29^2 \cdot 421^2 \cdot 191969^2.$$

Needless to say, the regulator has not been computed. In the classical case this is difficult even for cubic extensions! Furthermore, the machine calculation showed that

$$h^- = 2^{39} \cdot 241 \cdot 3329 \cdot 65521 \cdot 1322641,$$

which is not divisible by 3. Thus the analogue of Kummer's Theorem is false!

A computer program has been written by R. D. Small that calculates the divisor class numbers for all subfields of $K_{P(T)}$. We conclude this note with a short table of some of the results. Namely, we give the prime decomposition of h^+ and h^- for all cubic and quartic polynomials modulo 3. Several observations are in order. Notice that 3 never divides h^- in the quartic case. Furthermore 3 does not divide the total class number h^+h^- for $2 + 2T + T^4$. Such $P(T)$ are called regular by D. Goss, and for such irreducibles he has proved an analogue of Fermat's last theorem. The power of 2 dividing h^- is consistent with a result of Rosen and Galovich on the unit group that implies $(p-1)^r \mid h^-$, where $r = (p^d - 1)/(p-1) - 1$. Thus for cubics $2^{12} \mid h^-$ and for quartics $2^{39} \mid h^-$. The explicit calculations show, in fact, that these estimates are exact. It would be interesting to know if this is true in general.

$P(T)$	h^+	h^-
$2 + T^2 + T^3$	$53 \cdot 313$	$2^{12} \cdot 5 \cdot 79$
$2 + T + T^2 + T^3$	$53 \cdot 313$	$2^{12} \cdot 5 \cdot 79$
$1 + 2T + T^2 + T^3$	$53 \cdot 313$	$2^{12} \cdot 5 \cdot 79$
$1 + T + 2T^2 + T^3$	$53 \cdot 313$	$2^{12} \cdot 3 \cdot 131$
$2 + 2T + 2T^2 + T^3$	$53 \cdot 313$	$2^{12} \cdot 3 \cdot 131$
$1 + 2T^2 + T^3$	$53 \cdot 313$	$2^{12} \cdot 3 \cdot 131$
$2 + 2T + T^3$	3^9	$2^{12} \cdot 3 \cdot 7$
$1 + 2T + T^3$	3^9	$2^{12} \cdot 3^6$

$p = 3, \deg P(T) = 4$

$P(T) = 1 + 2T + T^2 + T^4$
$h^+ = 2^{22} \cdot 3^3 \cdot 5^4 \cdot 11^2 \cdot 17 \cdot 41 \cdot 101 \cdot 5468921$
$h^- = 2^{39} \cdot 17^2 \cdot 13921 \cdot 18743655761$
$3 \mid h^+, 3 \mid h^-$

$P(T) = 2 + 2T + T^4$
$h^+ = 2^4 \cdot 11^2 \cdot 17 \cdot 41 \cdot 71 \cdot 97 \cdot 491 \cdot 881 \cdot 1464361$
$h^- = 2^{39} \cdot 17 \cdot 97 \cdot 63648628175761$

$P(T) = 2 + 2T^2 + T^4$
$h^+ = 2^7 \cdot 3^4 \cdot 5^3 \cdot 17 \cdot 19^2 \cdot 29^2 \cdot 89^4 \cdot 101^2$
$h^- = 2^{39} \cdot 17^3 \cdot 12046669609441$
$3 \mid \mathrm{h}^+, 3 \nmid h^-$

$P(T) = 2 + T^2 + T^4$
$h^+ = 2^7 \cdot 3 \cdot 11^2 \cdot 17 \cdot 29^2 \cdot 421^2 \cdot 191969^2$
$h^- = 2^{39} \cdot 241 \cdot 3329 \cdot 65521 \cdot 1322641$
$3 \mid h^+, 3 \nmid h^-$

$P(T) = 2 + T + T^4$
$h^+ = 2^4 \cdot 11^2 \cdot 17 \cdot 41 \cdot 71 \cdot 97 \cdot 491 \cdot 881 \cdot 1464361$
$h^- = 2^{39} \cdot 241 \cdot 641 \cdot 881 \cdot 532611841$

$P(T) = 1 + T + T^2 + T^4$
$h^+ = 2^{22} \cdot 3^3 \cdot 5^4 \cdot 11^2 \cdot 17 \cdot 41 \cdot 101 \cdot 5468921$
$h^- = 2^{39} \cdot 17^2 \cdot 853111437361$

Department of Mathematics and Statistics
University of New Brunswick
P.O. Box 4400
Fredericton, N.B.
Canada E3B 5A3

1. E. Artin, "Quadratische Körper im Gebiet der höheren Kongruenzen. I, II," *Math. Z.*, v. 19, 1924, pp. 153–246.

2. S. Galovich & M. Rosen, "The class number of cyclotomic function fields," *J. Number Theory*, v. 13, 1981, pp. 363–375.

3. D. Hayes, "Explicit class field theory for rational function fields," *Trans. Amer. Math. Soc.*, v. 189, 1979, pp. 77–91.

4. K. Ireland & Michael Rosen, *A Classical Introduction to Number Theory*, Graduate Texts in Mathematics, Springer-Verlag, New York, Heidelberg, Berlin, 1982.

5. K. Iwasawa, "A note on class numbers of algebraic number fields," *Abh. Math. Sem. Univ. Hamburg*, v. 20, 1955, pp. 257–258.

6. M. Rosen, "Ambiguous divisor classes in function fields," *J. Number Theory*, v. 9, 1977, pp. 160–174.