distributed (mod N) for all N is still unanswered.) Let L_m be the sequence of all progressions with the first term prime to the difference and let $P = \bigcup_{m=1}^{\infty} P_m$ be a partition of the set P of all primes into disjoint subsets with the property $\sum_{p \in P_m} 1/p = \infty$ $(m = 1, 2, \ldots)$. If now f is any multiplicative function such that for primes $p \in P_m$ the number $f(p)$ is a prime from L_m distinct from p and all numbers $f(q)$ for primes q less than p, then by Theorem III such a function will be WUD (mod N) for all $N \geqslant 3$.

References

[1] H. Delange, *Sur la distribution des valeurs des fonctions additives*, C. R. Acad. Sci. Paris 275 (1972), pp. A1139–A1142.

[2] W. Narkiewicz, *On distribution of values of multiplicative functions in residue classes*, Acta Arith. 12 (1967), pp. 269–279.

[3] W. Narkiewicz and J. Śliwa, *On a kind of uniform distribution of values of multiplicative functions in residue classes*, ibid., 31(1976), pp. 297–300.

[4] E. Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen, II*, Acta Math. Acad. Sci. Hungar. 18 (1967), pp. 411–467.

INSTITUTE OF MATHEMATICS, WROCŁAW UNIVERSITY
Wrocław, Poland

Received on 10. 9. 1975 (768)

ACTA ARITHMETICA
XXXII (1977)

The exponent of class groups in congruence function fields

by

MANOHAR L. MADAN and DANIEL J. MADDEN (Columbus, Ohio)

1. Introduction. For a finitely generated extension K of a field k with transcendence degree 1, the divisor class group is infinite and the null class group (the subgroup of divisor classes of degree 0) is, in general, also infinite. However, if k is finite, it is a consequence of the Riemann–Roch theorem that the number of classes of degree 0 is finite. In this, the case of congruence function fields, the order of the null class group is called the class number of the field. This null class group is analogous to the ideal class group in the case of algebraic number fields, and it plays an important role in all algebraic, arithmetic, and geometric studies of congruence function fields.

In the theory of congruence function fields, the "Riemann Hypothesis" plays an essential role. This "hypothesis" determines the real part of the zeros of the zeta function of a congruence function field. It was proved in complete generality by Andre Weil [10] after H. Hasse [7] had given a proof in the elliptic case. This result gives bounds on the class number of a congruence function field; however, while there are bounds on the order of the null class group, not much is known about its structure. The purpose here is to study the exponent of this group for congruence function fields of a particular type. These are fields K which are abelian extensions of $k(x)$, the rational function field over k, for which $\mathrm{Gal}\big(K/k(x)\big)$ has order $n_0 p^{r_0}$, where p is the characteristic of the field and n_0 is relatively prime to p; and for which the p-primary part of $\mathrm{Gal}\big(K/k(x)\big)$ is elementary abelian. The main object of this paper is to give a lower bound for the exponent of the null class group of a field of this type. A consequence of this will be that for a fixed finite field k and a fixed degree $n_0 p^{r_0}$, the exponent will approach infinity as the genus of the field goes to infinity.

It is well-known that there is a strong similarity between the theory of congruence function fields and the theory of algebraic number fields; the two together form the class of global fields, and class field theory holds for them. It would be interesting to obtain analogous results for some special class of algebraic number fields. No such definitive result is known; for the class of imaginary quadratic number fields, H. Heilbronn [8] proved that the class number becomes infinitely large with the absolute value of the discriminant. In fact, C. L. Siegel [9] proved that for imaginary quadratic fields,

$$\lim \frac{\log h}{\log \sqrt{|d|}} = 1$$

as $|d|$ tends to infinity (where h is the class number and d is the discriminant). Attempting to improve upon this result, D. Boyd and H. Kisielevsky [1] and P. Weinberger [11] proved that the exponent of the class group becomes infinitely large with the absolute value of the discriminant if one assumes the truth of the extended Riemann Hypothesis. This is analogous to the result of this work because the Hurwitz genus formula for extensions of fixed degree gives that the genus grows infinitely large with the degree of the discriminant.

Section 2 of this paper deals with cyclic extensions of $k(x)$ of prime power degree for primes other than the characteristic of the field; Section 3 deals with Artin–Schreier extensions of $k(x)$, i.e., extensions of degree p, where p is the characteristic. And in Section 4 the results of Section 2 and Section 3 are combined to give the main result. This is accomplished by studying the relationship between the null class group of a field whose Galois group is the direct product of two groups and the null class groups of the two subfields associated with the factors.

Finally, while the methods and results of this paper are completely arithmetic and algebraic, there is a natural geometric interpretation of the results. If K is a congruence function field over the field of constants k, let $\bar{K}$ be the constant field extension of K which has the algebraic closure $\bar{k}$ of k as its field of constants. There is a one-to-one morphism from the Jacobian variety of $\bar{K}$ onto the divisor classes of degree 0 of $\bar{K}$. Through this morphism, the k-rational points on the variety are mapped onto the null class group of K.

2. Cyclic extensions of $k(x)$ of prime power degree. Hasse's paper [6] contains a very clear presentation of the arithmetic theory of Kummer extensions and of Artin–Schreier extensions. For the convenience of the reader and in order to fix notation, the principal results about the decomposition of primes in these extensions are stated here and in the beginning of Section 3. For the standard results of the theory, the reader is referred to [4] or [5].

Let k be a finite field with q elements, and let Z be a cyclic extension of $k(x)$ of degree p^n, where p is a prime other than the characteristic. Then Z is a congruence function field over the exact field of constants k. Further, if p^n divides $q-1$, then k contains the p^n-th roots of 1. This type of extension, a cyclic Kummer extension, can be realized as $Z = k(x, y)$ where

$$y^{p^n} = f(x) = \prod_{i=1}^{l} p_i(x)^{\lambda_i}, \quad \lambda_i \in \mathbf{Z}.$$

However, if $\lambda_i < 0$ or $\lambda_i \geqslant p^n$, then a transformation $y' = y \cdot p_i(x)^{\gamma}$, for a suitable $\gamma \in \mathbf{Z}$, can be used to put this generating equation into a standard form in which

$$0 < \lambda_i < p^n, \quad i = 1, 2, \ldots, l.$$

The decomposition of a prime divisor of $k(x)$ in Z can be easily computed using the following two theorems:

THEOREM 1. *If, with the notation as above, $Z = k(x, y)$, where the generating equation is in standard form, then for a prime $p(x)$ which does not divide $f(x)$:*

(1) *The prime divisor of $k(x)$ associated with $p(x)$ is unramified.*

(2) *If the polynomial $y^{p^n} - f(x)$ modulo $p(x)$ decomposes into g factors each of degree f (this is the only possible type of decomposition since k contains the p^n-th roots of 1), then the prime $\mathfrak{p}_{p(x)}$ of $k(x)$, associated with $p(x)$, decomposes in Z as*

$$\mathfrak{p}_{p(x)} = \mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_g \quad \textit{where} \quad \deg_{Z/k(x)}(\mathfrak{P}_i) = f.$$

THEOREM 2. *With the notation as above, if $p_i(x)$ is a prime polynomial which divides $f(x)$, then the prime $\mathfrak{p}_{p_i(x)}$ of $k(x)$ associated with $p_i(x)$:*

(1) *ramifies in Z and has ramification index e_i, where*

$$e_i = \frac{p^n}{(p^n, \lambda_i)};$$

(2) *is unramified in the subfield $Z' = k(x, y^{e_i})$.*

(3) *Further, if $\mathfrak{P}_i$ is any prime of Z which lies over $\mathfrak{p}_{p_i(x)}$, the contribution of $\mathfrak{P}_i$ to the different of $Z/k(x)$ is*

$$\delta(\mathfrak{P}_i) = \mathfrak{P}_i^{e_i - 1}.$$

The decomposition of a ramified prime $\mathfrak{p}_{p_i(x)}$ of $k(x)$ can be completely determined by applying Theorem 1 to the extension $Z' = k(x, y^{e_i})$ over $k(x)$.

There is, of course, one prime of $k(x)$ which is not explicitly covered in these two theorems. However, the decomposition of this infinite prime is exactly the decomposition of the prime associated with x in the extension generated by the equation

$$y^{p^n} = f\left(\frac{1}{x}\right).$$

The extension generated by this equation is Z, and, for this reason, the infinite prime of $k(x)$ is often called the prime divisor associated with $\frac{1}{x}$. It is useful, however, to give the decomposition of this prime directly from the standard form of the generating equation.

Corollary. *With the notation as above, let*

$$\lambda_\infty = -\deg f(x) \quad \textit{and} \quad e_\infty = \frac{p^n}{(p^n, \lambda_\infty)}.$$

(1) *If $e_\infty = 1$, then $\mathfrak{p}_{1/x}$ is unramified in Z, and its decomposition into primes is determined by the decomposition of the polynomial $y^{p^n} - a$ in $k[x]$, where a is the leading coefficient of $f(x)$.*

(2) *If $e_\infty > 1$, then $\mathfrak{p}_{1/x}$ is ramified in Z with ramification index e_∞; the contribution to the different of any prime $\mathfrak{P}_\infty$ of Z over $\mathfrak{p}_{1/x}$ is given by*

$$\delta(\mathfrak{P}_\infty) = \mathfrak{P}_\infty^{e_\infty - 1}.$$

The precise decomposition of $\mathfrak{p}_{1/x}$ is obtained by considering the $Z' = k(x, y^{e_\infty})$ in which $\mathfrak{p}_{1/x}$ is unramified.

Poles of integral functions. The object now is to show that a primitive integral element of a cyclic extension $Z/k(x)$ of degree p^n must have some infinite prime as a pole of large order if the genus of Z is large. To that end a special type of integral basis is constructed for cyclic Kummer extensions of prime power degree which can be used to determine the values of an integral element at an infinite valuation in terms of the coefficients in its representation.

Theorem 3. *Let Z be a cyclic geometric extension of $k(x)$ of degree p^n, where p is not the characteristic of k and where k contains the p^n-th roots of 1. Further, let $Z = k(x, y)$ where*

$$y^{p^n} = f(x) = \prod_{i=1}^{l} p_i(x)^{\lambda_i}, \quad 0 < \lambda_i < p^n, \quad i = 1, 2, \ldots, l.$$

Then $\{\theta_0, \theta_1, \theta_2, \ldots, \theta_{p^n-1}\}$ is an integral basis of Z over $k(x)$, where

$$\theta_j = \frac{y^j}{\prod_{i=1}^{l} \mathfrak{p}_i(x)^{r_{ij}}} \quad \textit{for} \quad r_{ij} = \left[\left|\frac{j\lambda_i}{p^n}\right|\right],$$

the greatest integer not exceeding $j\lambda_i/p^n$.

Proof. If $\mathfrak{P}_i$ is any prime of Z lying over the prime divisor of $k(x)$ associated with $p_i(x)$, then

$$v_{\mathfrak{P}_i}(\theta_j) = v_{\mathfrak{P}_i}\left(\frac{y^j}{\prod_{h=1}^{l} \mathfrak{p}_h(x)^{r_{hj}}}\right) = j v_{\mathfrak{P}_i}(y) - r_{ij} v_{\mathfrak{P}_i}(p_i(x)) = \frac{j}{p^n} v_{\mathfrak{P}_i}(y^{p^n}) - e_i r_{ij}$$

$$= \frac{j e_i \lambda_i}{p^n} - e_i\left[\left|\frac{j\lambda_i}{p^n}\right|\right] \geqslant 0.$$

So, this basis consists of elements that are integral with respect to all prime divisors of Z except those that lie over the infinite prime of $k(x)$. Thus, the elements θ_i are integral over $k[x]$.

Consider the field basis $\{1, y, y^2, \ldots, y^{p^n-1}\}$. The discriminant of this basis is given by the following equation if we disregard a constant which plays no role in our arguments

$$\Delta_x\{y^i\} = \Delta_x\{1, y, y^2, \ldots, y^{p^n-1}\} = f(x)^{p^n-1}.$$

Let M be the resulting matrix of coefficients when the elements of the basis $\{\theta_j\}$ are expressed in terms of the basis $\{y^i\}$. Then, the discriminant of the basis $\{\theta_i\}$ is given by

$$\text{(1)} \qquad \Delta_x\{\theta_i\} = (\det M)^2(\Delta_x\{y^i\})$$

$$= (\det M)^2 f(x)^{p^n-1} = \prod_{i=1}^{l} p_i(x)^{\lambda_i(p^n-1) - 2\sum_{j=0}^{p^n-1} r_{ij}}.$$

Now, evaluating the sum:

$$\sum_{j=0}^{p^n-1} r_{ij} = \sum_{j=0}^{p^n-1}\left[\left|\frac{j\lambda_i}{p^n}\right|\right] = \sum_{j=0}^{p^n-1}\frac{j\lambda_i}{p^n} - \sum_{j=0}^{p^n-1}\left\{\left|\frac{j\lambda_i}{p^n}\right|\right\}$$

(the fractional part).

Let $d_i = (\lambda_i, p^n)$ and $\lambda_i = d_i\lambda_i'$. Then

$$\sum_{j=0}^{p^n-1} r_{ij} = \frac{1}{2}\lambda_i(p^n-1) - \sum_{j=0}^{p^n-1}\left\{\left|\frac{j\lambda_i'}{\frac{p^n}{d_i}}\right|\right\}.$$

But λ_i' is relatively prime to $\frac{p^n}{d_i}$, and so $\left\{j\lambda_i' \mid 0 \leqslant j < \frac{p^n}{d_i}\right\}$ is a complete residue system modulo $\frac{p^n}{d_i}$.

$$\text{(2)} \qquad \therefore \sum_{j=0}^{p^n-1} r_{ij} = \frac{1}{2}\lambda_i(p^n-1) - d_i\sum_{j=0}^{\frac{p^n}{d_i}-1}\frac{j}{\frac{p^n}{d_i}}$$

$$= \frac{1}{2}\lambda_i(p^n-1) - d_i\cdot\frac{d_i}{p^n}\cdot\frac{1}{2}\left(\frac{p^n}{d_i}-1\right)\frac{p^n}{d_i} = \frac{1}{2}\lambda_i(p^n-1) - \frac{1}{2}(p^n-d_i).$$

Substituting (2) into (1) yields

$$\Delta_x\{\theta_i\} = \prod_{i=1}^{l} p_i(x)^{\lambda_i(p^n-1)-\lambda_i(p^n-1)+(p^n-d_i)} = \prod_{i=1}^{l} p_i(x)^{p^n-d_i}.$$

However, this (after being converted to an ideal and then injected into the divisor group) is exactly that part Δ_x of the divisor discriminant of the extension which is based on the finite primes. For consider the contribution of $p_i(x)$ to the discriminant,

$$\Delta_x\big(p_i(x)\big) = N\Big(\prod_{h=1}^{g} \delta_x(\mathfrak{P}_h)\Big)$$

where $\mathfrak{P}_h$ are the primes of Z above the divisor associated with $p_i(x)$, N denotes the norm of Z to $k(x)$ and $\delta_x(\mathfrak{p}_h)$ is the contribution of $\mathfrak{p}_h$ to the different. Thus,

$$\Delta_x\big(p_i(x)\big) = N\Big(\prod_{h=1}^{g} \mathfrak{P}_h^{e_i-1}\Big) = \prod_{h=1}^{g} \big(N(\mathfrak{P}_h)\big)^{e_i-1} = \big(p_i(x)\big)^{d_i(e_i-1)}.$$

This completes the proof of Theorem 3.

THEOREM 4. *Let Z be a congruence function field as in Theorem 3. Then, for any $a \in \mathcal{O}$, the integral closure of $k[x]$ in Z, which is a primitive element for the extension $Z/k(x)$, there is prime $\mathfrak{P}_\infty$ lying over the infinite prime of $k(x)$, $\mathfrak{p}_{1/x}$, such that*

$$v_{\mathfrak{P}_\infty}(a) \leqslant \frac{e_\infty - 1}{p^n - 1} - \frac{2e_\infty}{p^n} - \frac{2G e_\infty}{p^n(p^n-1)}$$

where G is the genus of Z and e_∞ is the ramification index of $\mathfrak{P}_\infty$.

Proof. Let the decomposition of $\mathfrak{p}_{1/x}$ in Z be given by

$$\mathfrak{p}_{1/x} = (\mathfrak{P}_1\mathfrak{P}_2\ldots\mathfrak{P}_g)^{e_\infty}, \qquad \deg_{Z/k(x)}(\mathfrak{P}_i) = f.$$

By the previous theorem every $a \in \mathcal{O}$ can be written as

$$a = a_0(x)\theta_0 + a_1(x)\theta_1 + \ldots + a_{p^n-1}(x)\theta_{p^n-1}, \qquad a_i(x) \in k[x],$$

and then, for all the primes $\mathfrak{P}_i$,

(3) $$v_{\mathfrak{P}_i}(a) \geqslant \min_{0\leqslant j<p^n} \big\{v_{\mathfrak{P}_i}\big(a_j(x)\theta_j\big)\big\}.$$

By the definition of θ_j, it is clear that

$$v_{\mathfrak{P}_i}(\theta_j) = v_{\mathfrak{P}_h}(\theta_j) \text{ for all possible } h,\ i \text{ and } j;$$

so there is only one minimum as in (3). Let m denote this minimum, and let j_0 be an index such that

$$v_{\mathfrak{P}_i}\big(a_{j_0}(x)\theta_{j_0}\big) = m.$$

Let σ be a generating automorphism in $\mathrm{Gal}\big(Z/k(x)\big)$. The action of the Galois group on θ_j is given by $\sigma^i\theta_j = \zeta^{ij}\theta_j$ where ζ is a primitive p^n-th root of 1 in k. Consider, then, the system of equations:

$$\sigma^i a = \sum_{j=0}^{p^n-1} a_j(x)\sigma^i\theta_j = \sum_{j=0}^{p^n-1} a_j(x)\zeta^{ij}\theta_j,$$

where $0 \leqslant i \leqslant p^n$. Now multiplying the ith equation by ζ^{-ij_0} these equations become:

$$\zeta^{-ij_0}\sigma^i a = \sum_{j=0}^{p^n-1} a_j(x)\zeta^{i(j-j_0)}\theta_j.$$

For any p^n-th root of 1, ζ', not equal to 1

$$\sum_{i=0}^{p^n-1} (\zeta')^i = 0.$$

Thus adding these equations yields

$$p^n a_{j_0}(x)\theta_{j_0} = \sum_{i=0}^{p^n-1} (\zeta^{-ij_0}\sigma^i a).$$

And then taking the valuation $v_{\mathfrak{P}_1}$ of both sides gives

$$m = v_{\mathfrak{P}_1}\big(p^n a_{j_0}(x)\theta_{j_0}\big) = v_{\mathfrak{P}_1}\Big(\sum_{i=0}^{p^n-1}(\zeta^{-ij_0}\sigma^i a)\Big) \geqslant \min_{0\leqslant i<p^n}\{v_{\mathfrak{P}_1}(\sigma^i a)\}$$
$$\geqslant \min_{0\leqslant i<p^n}\{v_{\sigma^i\mathfrak{P}_1}(a)\} \geqslant \min_{1\leqslant i\leqslant g}\{v_{\mathfrak{P}_i}(a)\} \geqslant m \qquad \text{by (3)}.$$

Thus there is a prime $\mathfrak{P}_\infty$ lying over $\mathfrak{p}_{1/x}$ such that

(4) $$v_{\mathfrak{P}_\infty}(a) = m = \min_{0\leqslant j<p^n}\big\{v_{\mathfrak{P}_\infty}\big(a_j(x)\theta_j\big)\big\}.$$

Consider now $v_{\mathfrak{P}_\infty}\big(a_j(x)\theta_j\big)$ for any prime $\mathfrak{P}_\infty$ over $\mathfrak{p}_{1/x}$. If $a_j(x)$ is any non-zero polynomial over k, then $v_{\mathfrak{P}_\infty}\big(a_j(x)\big) \leqslant 0$, and so

(5) $$v_{\mathfrak{P}_\infty}\big(a_j(x)\theta_j\big) \leqslant v_{\mathfrak{P}_\infty}(\theta_j) \leqslant v_{\mathfrak{P}_\infty}(y^j) - v_{\mathfrak{P}_\infty}\Big(\prod_{i=1}^{l} p_i(x)^{r_{ij}}\Big)$$
$$\leqslant \frac{j}{p^n} v_{\mathfrak{P}_\infty}(y^{p^n}) - \sum_{i=1}^{l} r_{ij} v_{\mathfrak{P}_\infty}\big(p_i(x)\big)$$
$$\leqslant \frac{j}{p^n} e_\infty v_{\mathfrak{p}_{1/x}}\Big(\prod_{i=1}^{l} p_i(x)^{\lambda_i}\Big) - \sum_{i=1}^{l} r_{ij} e_\infty v_{\mathfrak{p}_{1/x}}\big(p_i(x)\big)$$
$$\leqslant -e_\infty \sum_{i=1}^{l}\left(\frac{j\lambda_i}{p^n} - \left[\!\left[\frac{j\lambda_i}{p^n}\right]\!\right]\right)\deg p_i(x).$$

Since a is also a primitive element in the extension Z over $k(x)$, there must be an index j relatively prime to p such that $a_j(x) \neq 0$, otherwise a would be contained in the subfield $k(x, y^p)$. But then, if $(j, p) = 1$, $j\lambda_i/p^n$ is not an integer, and so

$$\frac{j\lambda_i}{p^n} - \left[\left|\frac{j\lambda_i}{p^n}\right|\right] \geqslant \frac{1}{p^n}.$$

Thus (4) and (5) imply, for some prime $\mathfrak{P}_\infty$ lying over $\mathfrak{p}_{1/x}$,

$$v_{\mathfrak{P}_\infty}(a) = \min_{0\leqslant j<p^n} \{v_{\mathfrak{P}_\infty}(a_j(x)\theta_j)\} \leqslant -\frac{e_\infty}{p^n}\sum_{i=1}^{l}\deg p_i(x)$$

(6) $$\leqslant -\frac{e_\infty}{p^n}\sum_{i=1}^{l}\frac{p^n-d_i}{p^n-1}\deg p_i(x), \quad \text{where } d_i = (p^n, \lambda_i),$$

$$\leqslant -\frac{e_\infty}{p^n(p^n-1)}\deg\Big(\prod_{i=1}^{l} p_i(x)^{p^n-d_i}\Big)$$

$$\leqslant -\frac{e_\infty}{p^n(p^n-1)}\deg(\Delta_x),$$

where Δ_x is the Dedekind discriminant,

(7) $$\leqslant -\frac{e_\infty}{p^n(p^n-1)}\Big(\deg_{k(x)}(\Delta) - \Big(p^n - \frac{p^n}{e_\infty}\Big)\Big),$$

where Δ is the divisor discriminant of the extension $Z/k(x)$. By the Hurwitz genus formula this gives:

$$v_{\mathfrak{P}_\infty}(a) \leqslant -\frac{e_\infty}{p^n(p^n-1)}\Big(2G+2(p^n-1) - \Big(p^n - \frac{p^n}{e_\infty}\Big)\Big)$$

$$\leqslant \frac{e_\infty-1}{p^n-1} - \frac{2e_\infty}{p^n} - \frac{2Ge_\infty}{p^n(p^n-1)}$$

for some $\mathfrak{P}_\infty$ of Z lying over $\mathfrak{p}_{1/x}$. Thus Theorem 4 is proved.

Next, Theorem 4 is generalized to include cyclic extensions of $k(x)$ of degree p^n in which p^n-th roots of 1 are not necessarily present:

THEOREM 5. *Let Z be a cyclic geometric extension of $k(x)$ of degree p^n, where p is a prime other than the characteristic of k. Then, for any a integral over $k[x]$ which is a primitive element of the extension $Z/k(x)$, there is a prime $\mathfrak{P}_\infty$ of Z lying over the infinite prime of $k(x)$ such that*

$$v_{\mathfrak{P}_\infty}(a) \leqslant \frac{e_\infty-1}{p^n-1} - \frac{2e_\infty}{p^n} - \frac{2Ge_\infty}{p^n(p^n-1)}$$

where G is the genus of Z and e_∞ is the ramification index of $\mathfrak{P}_\infty$.

Proof. Let k' be the smallest extension of k which contains the p^n-th roots of 1, and let Z' be the constant field extensions of Z with constant field k'. Any primitive element a for the extension $Z/k(x)$ satisfies a p^n-th degree polynomial that is irreducible over $k[x]$. Since $Z/k(x)$ is geometric and has k for its exact field of constants, the polynomial is also irreducible in $k'[x]$. Thus a is also a primitive element for the extension $Z'/k'(x)$. If a is integral over $k[x]$, it is also integral over $k'[x]$. Finally Z'/Z is a constant field extension and k is perfect; so the genus of Z' is the genus of Z. Thus by Theorem 4 there is a prime $\mathfrak{P}'_\infty$ of Z' which lies over the infinite prime $\mathfrak{p}'_{1/x}$ of $k'(x)$ such that

$$v_{\mathfrak{P}'_\infty}(a) \leqslant \frac{e'_\infty-1}{p^n-1} - \frac{2e'_\infty}{p^n} - \frac{2Ge'_\infty}{p^n(p^n-1)},$$

where e'_∞ is the ramification index of $\mathfrak{P}'_\infty$ over $k'(x)$. Now $\mathfrak{P}'_\infty$ lies over some $\mathfrak{P}_\infty$ in Z, and, since Z'/Z is unramified, the ramification index of $\mathfrak{P}_\infty$ over $\mathfrak{p}_{1/x}$ is e'_∞. Thus

$$v_{\mathfrak{P}_\infty}(a) = v_{\mathfrak{P}'_\infty}(a) \leqslant \frac{e_\infty-1}{p^n-1} - \frac{2e_\infty}{p^n} - \frac{2Ge_\infty}{p^n(p^n-1)},$$

completing the proof of Theorem 5.

The main result in a special case. To prove the main result for cyclic extensions of $k(x)$, it is necessary to estimate the minimum degree of a prime of $k(x)$ that splits in Z. Such an estimate is given by:

THEOREM 6. *If Z is a cyclic geometric extension of $k(x)$ of degree p^n where p is any prime (including the characteristic of k), then there exists a prime divisor in $k(x)$ which splits completely in Z and which has degree less than m_0, where $m_0 = m_1+2$ for any positive m_1 which satisfies*

$$q^{m_1} - 2Gq^{m_1/2} - 2m_1(G+p^n) \geqslant 0.$$

LEMMA 1. *Let Z_m be the constant field extension of Z of degree m for m relatively prime to p. If $\mathfrak{P}_m$ is a prime divisor of Z_m of degree 1, and if $\mathfrak{P}$ is the prime under $\mathfrak{P}_m$ in Z, then*

$$\deg_{Z/k(x)}(\mathfrak{P}) = 1.$$

Proof of Lemma 1. Suppose $\deg_{Z/k(x)}(\mathfrak{P}) \neq 1$. Let $\mathfrak{P}$ lie over $\mathfrak{p}_{p(x)}$ in $k(x)$. Then since the degree of the extension $Z/k(x)$ is p^n, $\deg_{Z/k(x)}(\mathfrak{P}) = p^f$ for some $f \geqslant 1$. This follows from the fact that in a normal extension the relative degree of any prime divides the degree of the extension. And therefore,

$$\deg_Z(\mathfrak{P}) = p^f \deg_{k(x)}(\mathfrak{p}_{p(x)}) = p^f \deg p(x).$$

And then,

$$\deg_{Z_m}(\mathfrak{P}_m)\cdot m = \deg_{Z_m/Z}(\mathfrak{P}_m)\deg_Z(\mathfrak{P}) = \deg_{Z_m/Z}(\mathfrak{P}_m)\cdot p^f\cdot \deg p(x).$$

But $(m,p)=1$, so p must divide $\deg_{Z_m}(\mathfrak{P}_m)$; thus it cannot be 1.

Proof of Theorem 6. A prime $\mathfrak{P}$ in Z can have relative degree 1 in only two ways:

(1) the prime $\mathfrak{p}_{p(x)}$ lying under $\mathfrak{P}$ in $k(x)$ is ramified in Z;

(2) the prime $\mathfrak{p}_{p(x)}$ lying under $\mathfrak{P}$ in $k(x)$ is split completely in Z.

Thus if m is chosen large enough to ensure that there are more primes of degree 1 in Z_m than could lie over ramified primes of $k(x)$, then there must be a prime of degree 1 in Z_m which lies over a prime $\mathfrak{p}_{p(x)}$ of $k(x)$ which is split completely in Z. Now the degree of $\mathfrak{p}_{p(x)}$ cannot exceed m, for it lies under a prime of degree 1 in $k'(x)$, a degree m constant extension of $k(x)$. Thus, it is only necessary to choose the proper m.

First, let N_m be the number of primes of degree 1 in Z_m. N_m can be estimated using the Rieman hypothesis;

$$|N_m-(q^m+1)|\leqslant 2Gq^{m/2}.$$

And so,

$$N_m\geqslant q^m-2Gq^{m/2}+1. \tag{8}$$

Next, the number of primes of Z that have ramified from $k(x)$ is less than or equal to the degree of the different of the extension $Z/k(x)$. By the genus formula, this degree is

$$2G+2(p^n-1).$$

Now each of these primes of Z that have ramified from $k(x)$ can have at most m primes over it in Z_m. Thus the number of primes of Z_m which lie over primes of $k(x)$ that ramify in Z is at most

$$2m(G+p^n-1).$$

Thus, if m is chosen such that $(m,p)=1$ and

$$q^m-2Gq^{m/2}+1>2m(G+p^n-1),$$

then there is a prime of $k(x)$ which splits completely in Z and has degree at most m. Such an m can be chosen less than the m_0 in the statement of the theorem. We omit this easy calculation.

It is now possible to prove the main result of the paper in a special case.

THEOREM 7. *Let Z be a cyclic geometric extension of $k(x)$ of degree p^n, where p is a prime other than the characteristic of k. If G is the genus of Z, e_∞ is the ramification index of a prime of Z over the infinite prime of $k(x)$, $m=m_0$ of Theorem 6, and E is the exponent of the null class group of Z, then*

$$E\geqslant\frac{1}{m}\left(\frac{2Ge_\infty}{p^n(p^n-1)}+\frac{2e_\infty}{p^n}-\frac{e_\infty-1}{p^n-1}\right). \tag{9}$$

Proof. Let $\mathfrak{p}$ be a prime divisor of $k(x)$ of smallest degree which splits completely in Z. Then by Theorem 6,

$$\deg_{k(x)}\mathfrak{p}\leqslant m.$$

Let $\mathfrak{P}_1$ be any prime of Z which lies over $\mathfrak{p}$; then $\mathfrak{P}_1$ has p^n distinct conjugates under the action of the Galois group. If $\mathfrak{P}_\infty$ is any prime of Z (other than $\mathfrak{P}_1$) which lies over the infinite prime of $k(x)$, then

$$\frac{\mathfrak{P}_1^{\deg_Z\mathfrak{P}_\infty}}{\mathfrak{P}_\infty^{\deg_Z\mathfrak{P}_1}}\in D_0(Z).$$

Therefore, since E is the exponent of $D_0(Z)/E(Z)$, the null class group,

$$\frac{\mathfrak{P}_1^{E\deg_Z\mathfrak{P}_\infty}}{\mathfrak{P}_\infty^{E\deg_Z\mathfrak{P}_1}}=(a)\in E(Z),\qquad a\in Z.$$

The function a has its only pole at a prime over the infinite prime of $k(x)$; so a is integral over $k[x]$. Also a has p^n distinct conjugates under the action of the Galois group of $Z/k(x)$; thus, a is a primitive element for this extension. By Theorem 5,

$$-E\deg_Z(\mathfrak{P}_1)\leqslant\frac{e_\infty-1}{p^n-1}-\frac{2e_\infty}{p^n}-\frac{2Ge_\infty}{p^n(p^n-1)}.$$

But $\deg_Z(\mathfrak{P}_1)=\deg_{k(x)}\mathfrak{p}\leqslant m$. Therefore

$$E\geqslant\frac{1}{m}\left(\frac{2Ge_\infty}{p^n(p^n-1)}+\frac{2e_\infty}{p^n}-\frac{e_\infty-1}{p^n-1}\right).\ \blacksquare$$

COROLLARY. *In the class of finite, cyclic, geometric extensions Z of $k(x)$ of fixed degree p^n, where p is a prime other than the characteristic of the finite field k, the exponent of the null class group approaches infinity as the genus of Z goes to infinity.*

Proof. Since $e_\infty\geqslant 1$,

$$\frac{2e_\infty}{p^n}-\frac{e_\infty-1}{p^n-1}=\frac{p^ne_\infty-2e_\infty+p^n}{p^n(p^n-1)}\geqslant\frac{p^n-2+p^n}{p^n(p^n-1)}\geqslant\frac{2}{p^n},$$

and so

$$E\geqslant\frac{1}{m}\left(\frac{2G}{p^n(p^n-1)}+\frac{2}{p^n}\right). \tag{10}$$

For G large enough, the m in Theorem 6 can be taken as

$$m_1 = \frac{6\log G}{\log q}.$$

This is easily seen since

$$(q^{m_1/2} - 2G) = G^3 - 2G > 1,$$

for G large enough. Thus,

$$q^{m_1/2}(q^{m_1/2} - 2G) - 2m_1(G+p^n) > q^{m_1/2} - 2m_1(G+p^n),$$

or, after plugging in the value suggested for m_1,

$$q^{m_1/2}(q^{m_1/2} - 2G) - 2m_1(G+p^n) > G^3 - \frac{12}{\log q}(\log G)(G+p^n).$$

If G is large enough, this is positive; so $m_1 = \dfrac{6\log G}{\log q}$ satisfies the inequality of Theorem 6. Now,

$$m = m_0 = m_1 + 2 = \frac{6\log G}{\log q} + 2 \leqslant \frac{7\log G}{\log q},$$

if G is large enough.

Putting this in (10) gives

$$E \geqslant \frac{\log q}{7\log G}\left(\frac{2G}{p^n(p^n-1)} + \frac{2}{p^n}\right). \tag{11}$$

Therefore,

$$\lim_{G\to\infty} E = \infty.$$

3. Artin–Schreier extensions. In this section, results analogous to those proved in Section 2 for extensions of prime power degree are obtained for Artin–Schreier extensions.

Let Z be a cyclic geometric extension of $k(x)$ of degree p where p is the characteristic of k; then Z is a congruence function field over the exact field of constants k, if k is finite. Let k be finite and $|k| = q$; this type of extension, an Artin–Schreier extension, can be realized as $Z = k(x, y)$ where

$$y^p - y = f(x) = \prod_{i=1}^{l} p_i(x)^{\mu_i}, \quad \mu_i \in \mathbf{Z}.$$

There is a standard form of such an equation that can be reached through the transformation $y = y' + a(x)$ for suitable $a(x)$; it can be assumed

that the generating equation of Z over $k(x)$ is

$$y^p - y = f(x), \quad \text{where} \quad (f(x)) = \frac{\mathfrak{Q}}{\mathfrak{p}_1^{\lambda_1}\mathfrak{p}_2^{\lambda_2}\cdots\mathfrak{p}_l^{\lambda_l}},$$

$$(\lambda_i, p) = 1 \quad \text{for} \quad i = 1, 2, \ldots, l.$$

Also $\mathfrak{Q}$ is an integral divisor of $k(x)$ and relatively prime to the denominator of $f(x)$. Note that the standard form of an Artin–Schreier extension treats all the prime divisors of $k(x)$ equally, unlike the standard form of a Kummer extension.

THEOREM 8. *If, with the notation as above, $Z = k(x, y)$, where the generating equation is in standard form, then*

$$y^p - y = f(x) = \frac{q(x)}{p_1(x)^{\lambda_1}p_2(x)^{\lambda_2}\cdots p_l(x)^{\lambda_l}}, \quad (\lambda_i, p) = 1;$$

and, in keeping with the standard form of $f(x)$,

$$\lambda_\infty = \begin{cases} \deg f(x), & \text{if} \quad \deg f(x) > 0, \\ 0, & \text{if} \quad \deg f(x) \leqslant 0. \end{cases}$$

Thus $(\lambda_\infty, p) = 1$, if $\lambda_\infty \neq 0$. Further, for any prime divisor $\mathfrak{p}$ of $k(x)$:

(1) *$\mathfrak{p}$ is ramified if and only if $\mathfrak{p}$ divides the (divisor) denominator of $f(x)$. The contribution of the prime $\mathfrak{P}$ of Z above $\mathfrak{p}$ to the different is*

(12) (a) $\delta(\mathfrak{P}) = \mathfrak{P}^{(\lambda_i+1)(p-1)}$, *if $\mathfrak{p}$ is not the infinite prime,*
(b) $\delta(\mathfrak{P}) = \mathfrak{P}^{(\lambda_\infty+1)(p-1)}$, *if $\mathfrak{p}$ is the infinite prime.*

(2) *If $\mathfrak{p}$ is an unramified prime, then*

$$y^p - y - f(x)$$

is an integral polynomial with respect to $\mathfrak{p}$. The decomposition of $\mathfrak{p}$ in Z mirrors the decomposition of this polynomial modulo $\mathfrak{p}$. That is, $\mathfrak{p}$ is inert if $y^p - y - f(x)$ is irreducible in $\mathcal{O}_\mathfrak{p}/I_\mathfrak{p}$ and is split if the polynomial factors there.

In an Artin–Schreier extension, there is an automorphism σ which generates $\mathrm{Gal}(Z/k(x))$ such that

$$\sigma(y) = y + 1.$$

With the notation in Theorem 8, let $\mathcal{O}$ be the integral closure of $k[x]$ in Z. We shall, now, construct a special integral basis and use it to prove for Artin–Schreier extensions a theorem similar to Theorem 4.

THEOREM 9. *Let Z be an Artin–Schreier extension of $k(x)$, and let*

$$y^p - y = f(x) = \frac{q(x)}{p_1(x)^{\lambda_1}p_2(x)^{\lambda_2}\cdots p_l(x)^{\lambda_l}}$$

be the generating equation in standard form (the notation as in Theorem 8). *Then* $\{\theta_0, \theta_1, \theta_2, \ldots, \theta_{p-1}\}$ *is an integral basis of* Z *over* $k(x)$, *where*

$$\theta_j = y^j \prod_{i=1}^{l} p_i(x)^{r_{ij}}, \quad \textit{for} \quad r_{ij} = \begin{cases} 1 + \left[\left|\dfrac{j\lambda_i}{p}\right|\right], & \textit{if } j \neq 0, \\ 0, & \textit{if } j = 0. \end{cases}$$

Proof. θ_j is clearly integral for all the primes of Z except possible those lying over ramified primes or the infinite prime. If $\mathfrak{P}_i$ is a prime of Z lying over $\mathfrak{p}_{p_i(x)}$, the prime divisor of $k(x)$ associated with $p_i(x)$, then

$$v_{\mathfrak{P}_i}(y) < 0.$$

Therefore,

$$v_{\mathfrak{P}_i}(y) = v_{\mathfrak{P}_i}(y+1) = v_{\mathfrak{P}_i}(y+2) = \ldots = v_{\mathfrak{P}_i}(y+p-1).$$

This gives immediately

$$v_{\mathfrak{P}_i}(y) = \frac{1}{p} v_{\mathfrak{P}_i}(y^p - y) = \frac{1}{p} v_{\mathfrak{P}_i}\big(f(x)\big) = -\lambda_i,$$

and, using the definition,

$$v_{\mathfrak{P}_i}(\theta_j) = v_{\mathfrak{P}_i}\Big(y^j \prod p_h(x)^{r_{hj}}\Big) = -j\lambda_i + r_{ij}p.$$

Therefore, $v_{\mathfrak{P}_i}(\theta_j) \geqslant 0$ for all the primes $\mathfrak{P}_i$ that have ramified from $k(x)$ and which are associated with polynomials in $k(x)$. In fact, if $j \neq 0$, then $v_{\mathfrak{P}_i}(\theta_j) > 0$. This gives that the elements of the basis $\{\theta_i\}$ are integral over $k[x]$.

To compute the discriminant of the basis $\{\theta_i\}$, let M be the matrix of coefficients in the linear equations expressing $\{\theta_i\}$ in terms of $\{y^i\}$. Then,

$$\Delta_x\{\theta_i\} = [\det M]^2 \Delta_x\{y^i\}.$$

But $\Delta_x\{y^i\}$ is the discriminant of the polynomial $y^p - y - f(x)$, which is 1. So,

$$\Delta_x\{\theta_i\} = \prod_{i=1}^{l} p_i(x)^{2\sum_{j=0}^{p-1} r_{ij}}. \tag{13}$$

Now,

$$\sum_{j=0}^{p-1} r_{ij} = \sum_{j=1}^{p-1} \left(1 + \left[\left|\frac{j\lambda_i}{p}\right|\right]\right) \tag{14}$$
$$= (p-1) + \frac{\lambda_i}{2}(p-1) - \frac{1}{2}(p-1) = \frac{1}{2}(\lambda_i + 1)(p-1).$$

Then (13) and (14) together give

$$\Delta_x\{\theta_i\} = \prod_{i=1}^{l} p_i(x)^{(\lambda_i+1)(p-1)}.$$

However, this (after being made an ideal and then a divisor) is exactly the finite part of the norm of the different as given by (12). So

$$\Delta_x\{\theta_i\} = \Delta_x(Z),$$

where $\Delta_x(Z)$ is the Dedekind discriminant of Z over $k(x)$. Thus $\{\theta_i\}$ is an integral basis and the theorem is proved.

THEOREM 10. *Let* Z *be an Artin–Schreier extension with the notation as in Theorems* 8 *and* 9; *then, for any* $\alpha \in \mathcal{O}$ *which is a primitive element of he extension* Z *over* $k(x)$, *there is a prime divisor* $\mathfrak{P}_\infty$ *of* Z *lying over the infinite prime* $\mathfrak{p}_{1/x}$ *of* $k(x)$ *such that*

$$v_{\mathfrak{P}_\infty}(\alpha) \leqslant -e_\infty \left(\frac{2G}{p(p-1)} + \frac{1}{p}\right),$$

where e_∞ *is the ramification index of* $\mathfrak{P}_\infty$ *and* G *is the genus of* Z.

Proof. If $\alpha \in \mathcal{O}$, then by the previous theorem α can be written as

$$\begin{aligned} \alpha &= a_0(x)\theta_0 + a_1(x)\theta_1 + a_2(x)\theta_2 + \ldots + a_{p-1}(x)\theta_{p-1} \\ &= b_0(x) + b_1(x)y + b_2(x)y^2 + \ldots + b_{p-1}(x)y^{p-1}, \end{aligned}$$

where $a_j(x) \in k[x]$ and $b_j(x) = a_j(x) \prod_{i=1}^{l} p_i(x)^{r_{ij}}$. As in the proof of Theorem 4, it is necessary to evaluate $v_{\mathfrak{P}_\infty}(\alpha)$ for some $\mathfrak{P}_\infty$ lying over $\mathfrak{p}_{1/x}$. It is convenient to do this in the form of

LEMMA 2. *For* α *as in the theorem, there is a* $\mathfrak{P}_\infty$ *lying over the infinite prime* $\mathfrak{p}_{1/x}$ *of* $k(x)$ *such that*

$$v_{\mathfrak{P}_\infty}(\alpha) = m,$$

where

$$m = \begin{cases} \min\limits_{0 \leqslant j < p} \{v_{\mathfrak{P}_\infty}\big(b_j(x)y^j\big)\}, & \textit{if} \quad \mathfrak{p}_{1/x} \textit{ is ramified in } Z, \\ \min\limits_{0 \leqslant j < p} \{v_{\mathfrak{p}_{1/x}}\big(b_j(x)\big)\}, & \textit{if} \quad \mathfrak{p}_{1/x} \textit{ is unramified in } Z. \end{cases}$$

Proof of Lemma 2. The proof is given in two parts. First, if $\mathfrak{p}_{1/x}$ is ramified in Z, then there is only one prime $\mathfrak{P}_\infty$ of Z over $\mathfrak{p}_{1/x}$, and $v_{\mathfrak{P}_\infty}(y) = -\lambda_\infty$. Now,

$$v_{\mathfrak{P}_\infty}\big(b_j(x)y^j\big) = v_{\mathfrak{P}_\infty}\big(b_j(x)\big) + v_{\mathfrak{P}_\infty}(y^j) = pv_{\mathfrak{p}_{1/x}}\big(b_j(x)\big) - j\lambda_\infty.$$

However, since $\mathfrak{p}_{1/x}$ is ramified, $\lambda_\infty \not\equiv 0 \pmod{p}$, and so the set

$$\{v_{\mathfrak{P}_\infty}\big(b_j(x)y^j\big) \mid 0 \leqslant j < p\}$$

is a complete residue system modulo p. Therefore, this set has a distinct minimum, and so,

$$v_{\mathfrak{P}_\infty}(\alpha) = m.$$

Next is the case where $\mathfrak{p}_{1/x}$ is unramified in Z. If $\mathfrak{P}_1$ is any prime of Z over $\mathfrak{p}_{1/x}$, then

$$v_{\mathfrak{P}_1}(y) \geqslant 0.$$

Thus for all the primes $\mathfrak{P}_i$ over $\mathfrak{p}_{1/x}$,

$$\begin{aligned}(15)\quad v_{\mathfrak{P}_i}(\alpha) &= v_{\mathfrak{P}_i}\big(b_0(x)+b_1(x)y+\ldots+b_{p-1}(x)y^{p-1}\big) \geqslant \min_{0\leqslant j<p}\{v_{\mathfrak{P}_i}\big(b_j(x)y^j\big)\} \\ &\geqslant \min_{0\leqslant j<p}\{v_{\mathfrak{P}_i}\big(b_j(x)\big)+jv_{\mathfrak{P}_i}(y)\} \geqslant \min_{0\leqslant j<p}\{v_{\mathfrak{p}_{1/x}}\big(b_j(x)\big)\} \geqslant m.\end{aligned}$$

Notice here, that there is some prime $\mathfrak{P}_1$ over $\mathfrak{p}_{1/x}$ such that $v_{\mathfrak{P}_1}(y) = 0$. For suppose $v_{\mathfrak{P}_1}(y) > 0$, then $v_{\mathfrak{p}_{1/x}}\big(f(x)\big) > 0$, and so $\mathfrak{p}_{1/x}$ must split over Z. Then

$$v_{\sigma\mathfrak{P}_1}(y) = v_{\mathfrak{P}_1}(y+1) = \min\{v_{\mathfrak{P}_1}(y), 0\} = 0.$$

Let j_0 be an index such that $v_{\mathfrak{p}_{1/x}}\big(b_{j_0}(x)\big) = m$. It can be assumed that $j_0 \neq 0$; for if 0 is the only index where this minimum occurs, it follows immediately that

$$v_{\mathfrak{P}_1}(\alpha) = \min_{0\leqslant j<0}\{v_{\mathfrak{P}_1}\big(b_j(x)y^j\big)\} = m$$

for that prime $\mathfrak{P}_1$ over $\mathfrak{p}_{1/x}$ for which $v_{\mathfrak{P}_1}(y) = 0$. Consider then

$$\begin{aligned}(16)\quad y^{p-1-j_0}\alpha = b_0(x)y^{p-1-j_0}+b_1(x)y^{p-j_0}+\ldots+ \\ +b_{j_0}(x)y^{p-1}+\ldots+b_{p-1}(x)y^{2(p-1)-j_0}.\end{aligned}$$

Now since $j_0 \neq 0$, the highest power of y that can occur in this sum is $2p-3$. By Newton's formulae ([2], p. 437), it is easy to see that the trace from Z to $k(x)$ (denoted by $\mathrm{Tr}(\alpha)$) acts on these powers of y in the following way:

$$\mathrm{Tr}(y^h) = \begin{cases}0, & \text{if} \quad 0 \leqslant h < 2p-1 \text{ and } h \neq p-1,\\ -1, & \text{if} \quad h = p-1.\end{cases}$$

Therefore, (16) gives, for any prime $\mathfrak{P}_1$ above $\mathfrak{p}_{1/x}$,

$$\begin{aligned}(17)\quad m &= v_{\mathfrak{p}_{1/x}}\big(b_{j_0}(x)\big) = v_{\mathfrak{P}_1}\big(b_{j_0}(x)\big) = v_{\mathfrak{P}_1}\big(\mathrm{Tr}(y^{p-1-j_0}\alpha)\big) \\ &\geqslant \min_{\sigma\in\mathrm{Gal}(Z/k(x))}\{v_{\mathfrak{P}_1}\big(\sigma(y^{p-1-j_0}\alpha)\big)\} \geqslant \min_{\mathfrak{P}_i \text{ above } \mathfrak{p}_{1/x}}\{v_{\mathfrak{P}_i}(y^{p-1-j_0}\alpha)\} \\ &\geqslant \min_{\mathfrak{P}_i \text{ above } \mathfrak{p}_{1/x}}\{(p-1-j_0)v_{\mathfrak{P}_i}(y)+v_{\mathfrak{P}_i}(\alpha)\}.\end{aligned}$$

But $v_{\mathfrak{P}_i}(y) \geqslant 0$, $(p-1-j_0) \geqslant 0$, and $v_{\mathfrak{P}_i}(\alpha) \geqslant m$ for all the primes $\mathfrak{P}_i$ of Z above $\mathfrak{p}_{1/x}$, and this together with (15) gives

$$m \geqslant \min_{\mathfrak{P}_i \text{ above } \mathfrak{p}_{1/x}}\{(p-1-j_0)v_{\mathfrak{P}_i}(y)+v_{\mathfrak{P}_i}(\alpha)\} \geqslant m.$$

Thus, there is a prime $\mathfrak{P}_\infty$ in Z above $\mathfrak{p}_{1/x}$ such that $v_{\mathfrak{P}_\infty}(\alpha) = m$, and this proves the lemma.

Proof of Theorem 10. It remains to estimate the value of m in the lemma. For a primitive element α in the extension Z over $k(x)$, there is an index j_1 such that $a_{j_1}(x) \neq 0$ and $j_1 \neq 0$. When $\mathfrak{p}_{1/x}$ is ramified this gives

$$\begin{aligned}(18)\quad m &= \min_{0\leqslant j<p}\{v_{\mathfrak{P}_\infty}\big(b_j(x)y^j\big)\} \leqslant v_{\mathfrak{P}_\infty}\big(b_{j_1}(x)y^{j_1}\big) \\ &\leqslant v_{\mathfrak{P}_\infty}\big(a_{j_1}(x)\big)+v_{\mathfrak{P}_\infty}\Big(\prod_{i=1}^{l} p_i(x)^{r_{ij_1}}\Big)-j_1\lambda_\infty \leqslant pv_{\mathfrak{p}_{1/x}}\Big(\prod_{i=1}^{l} p_i(x)^{r_{ij_1}}\Big)-\lambda_\infty.\end{aligned}$$

When $\mathfrak{p}_{1/x}$ is unramified,

$$\begin{aligned}(19)\quad m &= \min_{0\leqslant j<p}\{v_{\mathfrak{p}_{1/x}}\big(b_j(x)\big)\} \leqslant v_{\mathfrak{p}_{1/x}}\big(b_{j_1}(x)\big) \leqslant v_{\mathfrak{p}_{1/x}}\big(a_{j_1}(x)\big)+v_{\mathfrak{p}_{1/x}}\Big(\prod_{i=1}^{l} p_i(x)^{r_{ij_1}}\Big) \\ &\leqslant v_{\mathfrak{p}_{1/x}}\Big(\prod_{i=1}^{l} p_i(x)^{r_{ij_1}}\Big).\end{aligned}$$

In both cases it is necessary to approximate $v_{\mathfrak{p}_{1/x}}\big(\prod_{i=1}^{l} p_i(x)^{r_{ij}}\big)$, for $j \neq 0$;

$$\begin{aligned} v_{\mathfrak{p}_{1/x}}\Big(\prod_{i=1}^{l} p_i(x)^{r_{ij}}\Big) &= -\deg\Big(\prod_{i=1}^{l} p_i(x)^{r_{ij}}\Big) = -\sum_{i=1}^{l} r_{ij}\deg p_i(x) \\ &= -\sum_{i=1}^{l}\Big(1+\Big[\Big|\frac{j\lambda_i}{p}\Big|\Big]\Big)\deg p_i(x) \\ &\leqslant -\sum_{i=1}^{l}\Big(\frac{j\lambda_i}{p}+\frac{1}{p}\Big)\deg p_i(x), \qquad \because p \nmid \lambda_i, \\ &\leqslant -\frac{1}{p}\sum_{i=1}^{l}(j\lambda_i+1)\deg p_i(x) \\ (20)\quad &\leqslant -\frac{1}{p}\sum_{i=1}^{l}(\lambda_i+1)\deg p_i(x) \\ &\leqslant -\frac{1}{p(p-1)}\sum_{i=1}^{l}(\lambda_i+1)(p-1)\deg p_i(x) \\ &\leqslant -\frac{1}{p(p-1)}\deg\Big(\prod_{i=1}^{l} p_i(x)^{(p-1)(\lambda_i+1)}\Big) \\ (21)\quad &\leqslant -\frac{1}{p(p-1)}\deg(\Delta_x),\end{aligned}$$

where Δ_x is the ideal discriminant of Z. When $\mathfrak{p}_{1/x}$ is unramified

$$\deg \Delta_x = \deg_{k(x)} \Delta,$$

where Δ is the divisor discriminant, and so, by the genus formula, (19), and (21),

$$m \leqslant -\frac{1}{p(p-1)} \deg \Delta = -\frac{2G}{p(p-1)} - \frac{2}{p}.$$

When $\mathfrak{p}_{1/x}$ is ramified,

$$\Delta = (\Delta_x) \mathfrak{p}_{1/x}^{(p-1)(\lambda_\infty+1)},$$

and so

$$\deg \Delta_x = \deg \Delta - (p-1)(\lambda_\infty + 1).$$

Using the genus formula, it follows from (18) and (21) that

$$m \leqslant -p\left(\frac{\deg \Delta - (p-1)(\lambda_\infty+1)}{p(p-1)}\right) - \lambda_\infty$$

$$\leqslant \frac{-1}{p-1}\big(2G - 2(p-1) - (p-1)(\lambda_\infty+1) + \lambda_\infty(p-1)\big) \leqslant -\frac{2G}{p-1} - 1.$$

In either case there is a prime $\mathfrak{P}_\infty$ of Z lying over $\mathfrak{p}_{1/x}$ such that

$$v_{\mathfrak{P}_\infty}(a) \leqslant m \leqslant -e_\infty\left(\frac{2G}{p(p-1)} + \frac{1}{p}\right),$$

where e_∞ is the ramification index of $\mathfrak{P}_\infty$. This completes the proof of Theorem 10.

Since Theorem 6 holds for all cyclic extensions of $k(x)$ of prime power degree, there is a bound on the minimum degree of a prime of $k(x)$ which splits completely in an Artin–Schreier extension. This, together with the bound given by Theorem 10, gives the following:

THEOREM 11. *Let Z be an Artin–Schreier extension of $k(x)$. If G is the genus of Z, e_∞ is the ramification index of a prime over the infinite prime, $m = m_0$ of Theorem 6, and E is the exponent of the null class group of Z, then*

$$E \geqslant \frac{e_\infty}{m}\left(\frac{2G}{p(p-1)} + \frac{1}{p}\right).$$

COROLLARY. *In the class of Artin–Schreier extensions of $k(x)$ for a fixed finite field k, the exponent of the null class group approaches infinity as the genus of the field goes to infinity.*

The proof of Theorem 11 parallels the proof of Theorem 7, and the approximation for m used in the proof of the corollary of that theorem gives

$$(22) \qquad E \geqslant \frac{\log q}{7 \log G}\left(\frac{2G}{p(p-1)} + \frac{1}{p}\right).$$

Thus

$$\lim_{G\to\infty} E = \infty.$$

4. The main result. The next step is to combine the results of Section 2 with the results of Section 3 to show that, for a special class of extensions of $k(x)$, the exponent of the null class group approaches infinity as the genus of the field goes to infinity. This special class of extensions consists of these geometric abelian extensions Z of $k(x)$ of fixed degree where the p-primary part of the Galois group is elementary abelian. These are exactly those extensions of $k(x)$ whose Galois group is the direct product of cyclic groups of prime power order for primes other than the characteristic and groups of order equal to the characteristic.

Let $K/k(x)$ be an extension as described above, and let G be its genus. Then,

$$\mathrm{Gal}\big(K/k(x)\big) = C_1 \times C_2 \times C_3 \times \ldots \times C_n,$$

where each C_i is a cyclic group of the proper type. There is a subfield Z_i corresponding to each C_i such that

$$\mathrm{Gal}\big(Z_i/k(x)\big) = C_i.$$

These subfields are, therefore, either cyclic geometric extensions of $k(x)$ of prime power degree for primes other than the characteristic or are Artin–Schreier extensions of $k(x)$. Thus, the result has been established for all of the subfields Z_i of K. The first step in extending this result to K is to show that, if G is large, then the genus G_i of some Z_i is also large. To this purpose a lemma and Theorem 12 are proved.

LEMMA 3. *Let Z_1, Z_2, and K be extensions of $k(x)$ such that $Z_i \subseteq K$, for $i = 1, 2$, and such that*

$$\mathrm{Gal}\big(K/k(x)\big) = \mathrm{Gal}\big(Z_1/k(x)\big) \times \mathrm{Gal}\big(Z_2/k(x)\big).$$

Then, as divisors of K,

$$\delta(K/Z_1) \text{ divides } \delta\big(Z_2/k(x)\big)$$

and

$$\delta(K/Z_2) \text{ divides } \delta\big(Z_1/k(x)\big),$$

where δ denotes the different of the proper extension.

Proof. Let $\mathcal{O}_1$, $\mathcal{O}_2$, and $\mathcal{O}$ be the respective integral closures of $k[x$ in Z_1, Z_2, and K. Also let $\delta_x(K/Z_1)$ and $\delta_x(Z_2/k(x))$ be the Dedekind differ ents in the respective extension. It is well-known that $\delta_x(Z_2/k(x))$ is th greatest common divisor of the differents of all the elements of $\mathcal{O}_2$. However

$$\mathrm{Gal}(K/Z_1) \cong \mathrm{Gal}(K/k(x))/\mathrm{Gal}(Z_2/k(x)) \cong \mathrm{Gal}(Z_2/k(x)),$$

and $\mathcal{O}_2 \subseteq \mathcal{O}$. Thus the different of an element of $\mathcal{O}_2$ in the extension $Z_2/k(x$ can also be considered as the different of an element of $\mathcal{O}$ in the extensio K/Z_1. Therefore,

$$\delta_x(K/Z_1) \text{ divides } \delta_x(Z_2/k(x)).$$

This completes the proof for all prime divisors of K that do not lie ove the infinite prime of $k(x)$. For the complete proof of the lemma, it i necessary to extend the divisibility to include the infinite primes. Thi is done by observing that $k(x) = k\left(\frac{1}{x}\right)$ and that the global differen is the product of the local differents. Therefore,

$$\delta(K/Z_1) \quad \text{divides} \quad \delta(Z_2/k(x)).$$

THEOREM 12. *Let K and Z_i, $i = 1, 2, \ldots, h$, be geometric extension of $k(x)$ such that:*

(1) *$[K: k(x)] = n$ and $[Z_i: k(x)] = n_i$, $i = 1, 2, \ldots, h$;*
(2) *K has genus G, and Z_i has genus G_i, $i = 1, 2, \ldots, h$;*
(3) *$Z_i \subseteq K$, for $i = 1, 2, \ldots, h$;*
(4) *$\mathrm{Gal}(K/k(x)) = \mathrm{Gal}(Z_1/k(x)) \times \mathrm{Gal}(Z_2/k(x)) \times \ldots \times \mathrm{Gal}(Z_h/k(x))$.*

Then for some field Z_i, say Z_1,

$$G_1 \geqslant \frac{1}{n^2}\left(G-(h-1)n+\sum_{i=1}^{h}\frac{n}{n_i}-1\right).$$

Proof. For the purposes of this proof, $Z_{i_1}Z_{i_2}\ldots Z_{i_s}$ will denote th smallest subfield of K containing the fields $Z_{i_1}Z_{i_2}\ldots Z_{i_s}$. In this par ticular case,

$$\mathrm{Gal}(Z_{i_1}Z_{i_2}\ldots Z_{i_s}/k(x)) = \mathrm{Gal}(Z_{i_1}/k(x)) \times \mathrm{Gal}(Z_{i_2}/k(x)) \times \ldots \times \mathrm{Gal}(Z_{i_s}/k(x)).$$

Now in the tower of fields $K \geqslant Z_1 \geqslant k(x)$,

$$\delta(K/k(x)) = \delta(Z_1/k(x))\,\delta(K/Z_1),$$

considered as divisors of K. Now, by the lemma,

$$\delta(K/Z_1) \quad \text{divides} \quad \delta(Z_2Z_3\ldots Z_h/k(x)),$$

and so

$$\delta(K/k(x)) \text{ divides } \delta(Z_1/k(x))\,\delta(Z_2Z_3\ldots Z_h/k(x)).$$

Similarly,

$$\delta(K/k(x)) \text{ divides } \delta(Z_1/k(x))\,\delta(Z_2/k(x))\,\delta(Z_3Z_4\ldots Z_h/k(x)).$$

This can be continued until

$$\delta(K/k(x)) \text{ divides } \delta(Z_1/k(x))\,\delta(Z_2/k(x))\ldots\delta(Z_h/k(x)).$$

Taking degrees in K gives:

$$\deg_K\big(\delta(K/k(x))\big) \leqslant \sum_{i=1}^{h}\deg_K\big(\delta(Z_i/k(x))\big) \leqslant \sum_{i=1}^{h} n_i^*\deg_{Z_i}\big(\delta(Z_i/k(x))\big)$$

where $n_i^* = \frac{n}{n_i}$, $i = 1, 2, \ldots, h$. After applying the genus formula, this gives

$$2G+2(n-1) \leqslant \sum_{i=1}^{h} n_i^*\big(2G_i+2(n_i-1)\big),$$

and so,

$$\sum_{i=1}^{h} n_i^* G_i \geqslant G-(h-1)n+\sum_{i=1}^{h} n_i^*-1.$$

Since $n \geqslant n_i^*$, there must be some G_i, say G_1, such that

$$G_1 \geqslant \frac{1}{n^2}\left(G-(h-1)n+\sum_{i=1}^{h} n_i^*-1\right)$$

and this completes the proof.

THEOREM 13. *In the class of abelian geometric extensions of $k(x)$ of fixed degree n, where k is a fixed finite field with characteristic p, in which the p-primary part of the Galois group is elementary abelian, the exponent of the null class group approaches infinity as the genus of the field approaches infinity. In fact if K is a field in this class with genus G large enough, the exponent E of the null class group is bounded by*

$$E \geqslant C\,\frac{\frac{G}{n^2}+M}{\log\left(\frac{G}{n^2}+M\right)}, \quad \textit{where } C \textit{ and } M \textit{ are constants.}$$

Proof. Let

$$\mathrm{Gal}(K/k(x)) = C_1 \times C_2 \times \ldots \times C_h,$$

where each C_i is a group of prime power order, and let Z_i be the subfield of K for which

$$\mathrm{Gal}(Z_i/k(x)) = C_i, \quad i = 1, 2, \ldots, h.$$

Then by Theorem 12, C_1 can be chosen such that its genus G_1, is bounded by

$$G_1 \geqslant \frac{1}{n^2}\Big(G-(h-1)n+\sum_{i=1}^{h}\frac{n}{n_i}-1\Big)$$

where $n = [K\colon k(x)]$ and $n_i = [Z_i\colon k(x)]$, $i = 1, 2, \ldots, h$. Since $n \geqslant h$ this can be written as

$$G_1 \geqslant \frac{G}{n^2}+M, \quad \text{for some constant } M.$$

Now Z_1 must be either a cyclic geometric extension of prime power degree or an Artin–Schreier extension of $k(x)$. Thus by Theorems 7 and 11 (in particular (11) and (22)),

$$E_1 \geqslant \frac{\log q}{7\log G_1}\Big(\frac{2G_1}{n_1(n_1-1)}+\frac{1}{n_1}\Big) \geqslant \frac{2\log q}{7n_1(n_1-1)}\,\frac{G_1}{\log G_1}.$$

However, if G is large enough, $\dfrac{G}{\log G}$ is an increasing function, and so,

$$E_1 \geqslant \frac{2\log q}{7n_1(n_1-1)}\cdot\frac{\left(\frac{G}{n^2}+M\right)}{\log\left(\frac{G}{n^2}+M\right)}.$$

Also since $n \geqslant n_1$,

$$E_1 \geqslant \frac{2\log q}{7n(n-1)}\cdot\frac{\left(\frac{G}{n^2}+M\right)}{\log\left(\frac{G}{n^2}+M\right)}. \tag{23}$$

Thus, when the genus of K is large, there is a subextension Z_1 of $k(x)$ whose null class group $C_0(Z_1)$ has equally large exponent. The group $C_0(Z_1)$ is mapped in a canonical way into $C_0(K)$. This map (called the conorm) has the following property [3]

$$|\mathrm{Ker}(\mathrm{conorm})| \text{ divides } [K\colon Z_1].$$

In this particular case,

$$|\mathrm{Ker}(\mathrm{conorm})| < [K\colon k(x)] = n.$$

But then the null class group $C_0(K)$ of K contains a subgroup,

$$C_0(Z_1)/|\mathrm{Ker}(\mathrm{conorm})|,$$

whose exponent is greater than or equal to $\dfrac{E_1}{n}$. Thus by (23),

$$E \geqslant \frac{E_1}{n} \geqslant \frac{2\log q}{7n^2(n-1)}\cdot\frac{\left(\frac{G}{n^2}+M\right)}{\log\left(\frac{G}{n^2}+M\right)}.$$

This completes the proof of the main theorem.

References

[1] David Boyd and H. Kisielevsky, *On the exponent of the ideal class group of complex quadratic fields*, Proc. Amer. Math. Soc. 31 (1972), pp. 433–436.

[2] G. Chrystal, *A textbook of algebra*, Vol. I, A. and C. Black, Edinburgh 1889; reprint of 6th ed. Chelsea, New York.

[3] M. Deuring, *Zur arithmetischen Theorie der algebraischen Funktionen*, Math. Ann. 106 (1932), pp. 77–102.

[4] — *Lectures on the theory of algebraic functions of one variable*, Tata Institute (Bombay), 1959.

[5] M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Academic Press, New York and London 1966.

[6] H. Hasse, *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstatenkörper*, Journ. Reine Angew. Math.

[7] — *Zur Theorie der abstrakten elliptischen Funktionenkörper*, Journ. Reine Angew. Math. 175 (1936), II: pp. 69–88, III: pp. 193–208.

[8] H. Heilbronn, *On the class-number in imaginary quadratic fields*, Quart. J. Math. Oxford 2, 5 (1934), pp. 150–160.

[9] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), pp. 83–86.

[10] Andre Weil, *Sur les courbes algébriques et les variétés qui s'en deduisent*, Actualités Scil Ind. No. 1041, 1948.

[11] P. J. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta Arith. 22 (1973), pp. 117–124.

DEPARTMENT OF MATHEMATICS
THE OHIO STATE UNIVERSITY
Columbus, Ohio, USA

Received on 25. 9. 1975 (770)