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 $N \geq 3$.

References


INSTITUTE OF MATHEMATICS, WROCŁAW UNIVERSITY
Wrocław, Poland

Received on 10. 9. 1976

(768)

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 finite 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–Borch theorem that the number of classes of degree 0 is finite. In this case, 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 André 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 $\text{Gal}(K/k(x))$ has order $n_0 p^n$, where $p$ is the characteristic of the field and $n_0$ is relatively prime to $p$; and for which the $p$-primary part of $\text{Gal}(K/k(x))$ 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 $n_0 p^n$, 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. Helbronn [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,

$$\lim_{|d| \to \infty} \frac{\log h}{\log |d|} = 1$$

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. Kisielewski [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 in 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 $K$ be the constant field extension of $K$ which has the algebraic closure $k$ of $k$ as its field of constants. There is a one-to-one morphism from the Jacobian variety of $K$ onto the divisor classes of degree 0 of $K$. 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 [15].

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

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

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

$$0 < \lambda_i < p^n, \quad t_1 = 1, 2, \ldots, l.$$ 

The decomposition of a prime divisor of $k(x)$ in $Z$ can easily be 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 $l$ factors each of degree $t_i$ (this is the only possible type of decomposition since $k$ contains the $p^n$-th roots of 1), then the prime $p_{\lambda_i}(x)$ of $k(x)$, associated with $p(x)$, decomposes in $Z$ as

$$p_{\lambda_i}(x) = p_1 \cdot p_2 \cdots p_l \quad \text{where} \quad \deg_{x(x)}(p_i) = t_i.$$ 

**Theorem 2.** With the notation as above, if $p_i(x)$ is a prime polynomial which divides $f(x)$, then the prime $p_{\lambda_i}(x)$ 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 $Z' = k(x, y'^t)$.
3. Further, if $\mathfrak{p}$ is any prime of $Z$ which lies over $p_{\lambda_i}(x)$, the contribution of $\mathfrak{p}$ to the different of $Z/k(x)$ is

$$\delta(\mathfrak{p}) = p_i^{e_i - 1}.$$ 

The decomposition of a ramified prime $p_{\lambda_i}(x)$ of $k(x)$ can be completely determined by applying Theorem 1 to the extension $Z' = k(x, y'^t)$ 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 exten-
The exponent of class groups in congruence function fields

\[ v_{\mathcal{O}}(\theta) = v_{\mathcal{O}} \left( \frac{y^j}{\prod p_i(x)^{r_i}} \right) = \frac{j v_{\mathcal{O}}(y) - \sum_{i} r_i v_{\mathcal{O}}(p_i(x))}{p^n v_{\mathcal{O}}(y^p) - \epsilon v_{\mathcal{O}}(y)}, \]

\[ \frac{j \lambda_i \lambda_i}{p^n} - \epsilon \left[ \frac{j \lambda_i}{p^n} \right] > 0. \]

So, this basis consists of elements that are integral with respect to all prime divisors of \( E \) except those that lie over the infinite prime of \( k(x) \). Thus, the elements \( \theta_i \) 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:

\[ \Delta(E) = \Delta(1, y, y^2, \ldots, y^{p^n-1}) = f(x)^{p^n-1}. \]

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

\[ \Delta(E) = (\text{det} \bar{M}^2) \Delta(E(y)) = \prod_{i=1}^{p^n-1} \left[ \frac{j \lambda_i}{p^n} \right] = \prod_{i=1}^{p^n-1} \left[ \frac{j \lambda_i}{p^n} \right] \left( \frac{j \lambda_i}{p^n} \right). \]

Now, evaluating the sum:

\[ \sum_{i=0}^{p^n-1} \lambda_i \left( \frac{p^n}{d_i} \right) = \sum_{i=0}^{p^n-1} \left[ \frac{j \lambda_i}{p^n} \right] = \sum_{i=0}^{p^n-1} \left( \left[ \frac{j \lambda_i}{p^n} \right] \right) \left( \left[ \frac{j \lambda_i}{p^n} \right] \right) \]

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

\[ \sum_{i=0}^{p^n-1} \lambda_i = \sum_{i=0}^{p^n-1} \left( \left[ \frac{j \lambda_i}{p^n} \right] \right) \left( \left[ \frac{j \lambda_i}{p^n} \right] \right) \]

But \( \lambda'_i \) is relatively prime to \( \frac{p^n}{d_i} \) and so \( j \lambda'_i \) is a complete residue system modulo \( \frac{p^n}{d_i} \).

Thus, the greatest integer not exceeding \( j \lambda'_i \) is

\[ \sum_{i=0}^{p^n-1} \lambda_i = \sum_{i=0}^{p^n-1} \left( \left[ \frac{j \lambda_i}{p^n} \right] \right) \left( \left[ \frac{j \lambda_i}{p^n} \right] \right) \]

But \( \lambda'_i \) is relatively prime to \( \frac{p^n}{d_i} \) and so \( j \lambda'_i \) is a complete residue system modulo \( \frac{p^n}{d_i} \).

Therefore,

\[ \sum_{i=0}^{p^n-1} \lambda_i = \sum_{i=0}^{p^n-1} \left( \left[ \frac{j \lambda_i}{p^n} \right] \right) \left( \left[ \frac{j \lambda_i}{p^n} \right] \right) \]

But \( \lambda'_i \) is relatively prime to \( \frac{p^n}{d_i} \) and so \( j \lambda'_i \) is a complete residue system modulo \( \frac{p^n}{d_i} \).
Substituting (3) into (1) yields

$$
\Delta (\mathcal{D}_k) = \prod_{i=1}^{l} p_i(x)^{d_i-1} 
$$

However, this (after being converted to an ideal and then injected into the divisor group) is exactly that part \( \mathcal{D}_k \) 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,

$$
\mathcal{D}_k(p_i(x)) = N \left( \prod_{\mathfrak{p}_k} \mathcal{D}_k(\mathfrak{p}_k) \right)
$$

where \( \mathfrak{p}_k \) are the primes of \( K \) above the divisor associated with \( p_i(x) \), \( N \) denotes the norm of \( K \) to \( k(x) \) and \( \mathcal{D}_k(\mathfrak{p}_k) \) is the contribution of \( p_i(x) \) to the discriminant. Thus,

$$
\Delta (\mathcal{D}_k(p_i(x))) = N \left( \prod_{\mathfrak{p}_k} \mathcal{D}_k(\mathfrak{p}_k)^{\gamma-1} \right) = (p_i(x))^{d_i (\gamma-1)}.
$$

This completes the proof of Theorem 3.

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

$$
v_{\mathfrak{p}_\alpha}(\alpha) = e_\alpha - 1 - \frac{2e_\alpha}{p} - \frac{2G e_\alpha}{p^2 (p^n-1)}
$$

where \( G \) is the genus of \( K \) and \( e_\alpha \) is the ramification index of \( \mathfrak{p}_\alpha \).

**Proof.** Let the decomposition of \( \mathfrak{p}_\alpha \) in \( K \) be given by

$$
\mathfrak{p}_\alpha = (\mathfrak{p}_1, \ldots, \mathfrak{p}_s)^{e_\alpha},
$$

where \( \deg_{Z/k(x)}(\mathfrak{p}_i) = f_i \).

By the previous theorem every \( \alpha \in \mathcal{O} \) can be written as

$$
\alpha = a_0(x) \theta_0 + a_1(x) \theta_1 + \ldots + a_{n-1}(x) \theta_{n-1},
$$

and then, for all the primes \( \mathfrak{p}_i \),

$$
v_{\mathfrak{p}_i}(\alpha) = \min \left\{ v_{\mathfrak{p}_i}(a_i(x) \theta_j) \right\},
$$

(3)

By the definition of \( \theta_j \), it is clear that

$$
v_{\mathfrak{p}_i}(\theta_j) = v_{\mathfrak{p}_i}(\theta_0)
$$

for all possible \( h, i \) 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

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

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

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

where \( 0 \leq i \leq p^n \). Now multiplying the \( i \)-th equation by \( \zeta^{-i} \), these equations become:

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

For any \( p^n \)-th root of 1, \( \zeta \), not equal to 1

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

Thus adding these equations yields

$$
p^n \sigma_{j_0}(x) \theta_{j_0} = \sum_{j=0}^{p^n-1} (\zeta^{-i} \sigma^i \alpha).
$$

And then taking the valuation \( v_{\mathfrak{p}_i} \) of both sides gives

$$
m = v_{\mathfrak{p}_i}(p^n \sigma_{j_0}(x) \theta_{j_0}) = v_{\mathfrak{p}_i} \left( \sum_{i=0}^{p^n-1} (\zeta^{-i} \sigma^i \alpha) \right) \geq \min \left\{ v_{\mathfrak{p}_i}(\sigma^i \alpha) \right\}
$$

$$
\geq \min \left\{ v_{\mathfrak{p}_i}(a_i(x) \theta_j) \right\} \geq \min \left\{ v_{\mathfrak{p}_i}(a_i(x)) \right\} = m
$$

by (3).

Thus there is a prime \( \mathfrak{p}_\alpha \) lying over \( \mathfrak{p}_\alpha \) such that

$$
v_{\mathfrak{p}_\alpha}(\alpha) = m = \min \left\{ v_{\mathfrak{p}_\alpha}(a_i(x) \theta_j) \right\},
$$

(4)

Consider now \( v_{\mathfrak{p}_\alpha}(a_i(x) \theta_j) \) for any prime \( \mathfrak{p}_\alpha \) over \( \mathfrak{p}_\alpha \). If \( a_i(x) \) is any non-zero polynomial over \( k \), then \( v_{\mathfrak{p}_\alpha}(a_i(x)) \leq 0 \), and so

$$
v_{\mathfrak{p}_\alpha}(a_i(x) \theta_j) = v_{\mathfrak{p}_\alpha}(a_i(x)) - v_{\mathfrak{p}_\alpha}(y) - \frac{1}{p} \sum_{j=0}^{p^n-1} v_{\mathfrak{p}_\alpha}(p_j(x) \theta_j)
$$

$$
\leq -\frac{1}{p} \sum_{j=0}^{p^n-1} v_{\mathfrak{p}_\alpha}(p_j(x) \theta_j)
$$

$$
\leq -\frac{1}{p} \sum_{j=0}^{p^n-1} v_{\mathfrak{p}_\alpha}(p_j(x) \theta_j) - \sum_{j=0}^{p^n-1} v_{\mathfrak{p}_\alpha}(a_j(x) \theta_j)
$$

$$
\leq -\frac{1}{p^n} \left( \sum_{j=0}^{p^n-1} v_{\mathfrak{p}_\alpha}(j \theta_j) \right) \deg p_j(x),
$$

(5)
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 \( (j, p) = 1 \), \( j \lambda \lambda_j \) is not an integer, and so

\[
\frac{j \lambda}{p^n} \left( \left\lfloor \frac{j}{p^n} \right\rfloor \right) > \frac{1}{p^n}.
\]

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

\[
v_{\mathfrak{P}_\infty}(a) = \min_{0 < j < p^n} \{v_{\mathfrak{P}_\infty}(a_j(x) \mathfrak{D})\} \leq \frac{e_\infty}{p^n} \sum_{l=1}^{l=d} \deg p_l(x)
\]

\[
\leq -\frac{e_\infty}{p^n} \sum_{l=1}^{l=d} \frac{p^n - d_l}{p^n - 1} \deg p_l(x), \quad \text{where} \quad d_l = (p^n, \lambda_l),
\]

\[
\leq -\frac{e_\infty}{p^n} \left( \prod_{l=1}^{l=d} p_l(x)^{p^n - d_l} \right)
\]

\[
\leq -\frac{e_\infty}{p^n} \deg(A_\infty),
\]

where \( A_\infty \) is the Dedekind discriminant,

\[
(7)
\]

\[
\leq -\frac{e_\infty}{p^n} \left( \deg_{\mathfrak{P}_\infty}(d) - \left( p^n - \frac{p^n}{e_\infty} \right) \right),
\]

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

\[
v_{\mathfrak{P}_\infty}(a) \leq -\frac{e_\infty}{p^n} \left( 2G + 2(p^n - 1) - \left( p^n - \frac{p^n}{e_\infty} \right) \right)
\]

\[
\leq \frac{e_\infty - 1}{p^n - 1} \frac{2e_\infty}{p^n - 1} \frac{2G e_\infty}{p^n(p^n - 1)}
\]

for some \( \mathfrak{P}_m \) of \( Z \) lying over \( \mathfrak{p}_{1m} \). 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 \( \mathfrak{a} \) 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

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

where \( G \) is the genus of \( Z \) and \( e_\infty \) 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 \( \mathfrak{p}_{1m} \) of \( k'(x) \) such that

\[
v_{\mathfrak{P}_\infty}(a) = v_{\mathfrak{P}_\infty}(a) \leq \frac{e_\infty - 1}{p^n - 1} \frac{2e_\infty}{p^n - 1} \frac{2G e_\infty}{p^n(p^n - 1)}
\]

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 \( \mathfrak{a} \) of \( k(x) \) which splits completely in \( Z \) and which has degree less than \( m_\alpha \), where \( m_\alpha = m_\alpha + 2 \) for any positive \( m_\alpha \) which satisfies

\[
q^{m_\alpha} - 2G q^{m_\alpha} - 2m_\alpha (\theta + p^n) > 0.
\]

**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 \( \mathfrak{P}_m \) is the prime under \( \mathfrak{P}_m \) in \( Z \), then

\[
\deg_{\mathfrak{P}_m}(\mathfrak{P}) = 1.
\]

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

\[
\deg_{\mathfrak{p}}(\mathfrak{P}) = p^f \deg_{\mathfrak{P}_m}(\mathfrak{P}) = p^f \deg p(x).
\]
And then,
\[ \deg_{Z_m}(\mathcal{P}_m) \cdot m = \deg_{Z_{m+2}}(\mathcal{P}_m) \deg_2(\mathcal{P}) = \deg_{Z_m}(\mathcal{P}_m) \cdot p^e \cdot \deg p(\mathcal{P}). \]

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

Proof of Theorem 6. A prime \(\mathcal{P}\) in \(Z\) can have relative degree 1 in only two ways:
(1) the prime \(p_{\mathcal{P}(z)}\) lying under \(\mathcal{P}\) in \(k(\sigma)\) is ramified in \(Z\);
(2) the prime \(p_{\mathcal{P}(z)}\) lying under \(\mathcal{P}\) in \(k(\sigma)\) 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 \(k(\sigma)\), then there must be a prime of degree 1 in \(Z_m\) which lies over a prime \(p_{\mathcal{P}(z)}\) of \(k(\sigma)\) which is split completely in \(Z\). Now the degree of \(p_{\mathcal{P}(z)}\) cannot exceed \(m\), for it lies under a prime of degree 1 in \(k(\sigma)\), a degree \(m\) constant extension of \(k(\sigma)\). 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 Riemann hypothesis;
\[ |N_m - (p^m + 1)| \leq 2Gq^{m^2}. \]

And so,
\[ N_m \geq p^m - 2Gq^{m^2} + 1. \tag{8} \]

Next, the number of primes of \(Z\) that have ramified from \(k(\sigma)\) is less than or equal to the degree of the different of the extension \(Z/k(\sigma)\). By the genus formula, this degree is
\[ 2G + (p^e - 1). \]

Now each of these primes of \(Z\) that have ramified from \(k(\sigma)\) can have at most \(m\) primes over it in \(Z_m\). Thus the number of primes of \(Z_m\) which lie over primes of \(k(\sigma)\) that ramify in \(Z\) is at most
\[ 2m(G + p^e - 1). \]

Thus, if \(m\) is chosen such that \((m, p) = 1\) and
\[ q^m - 2Gq^{m^2} + 1 > 2m(G + p^e - 1), \]
then there is a prime of \(k(\sigma)\) 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 \(k(\sigma)\) of degree \(p^e\), where \(p\) is a prime other than the characteristic of \(k\). If \(G\) is the genus of \(Z\), \(e_\infty\) is the ramification index of a prime of \(Z\) over the infinite prime of \(k(\sigma)\), \(m = m_0\)
of Theorem 6, and \(E\) is the exponent of the null class group of \(Z\), then
\[ E \geq \frac{1}{m} \left( \frac{2G e_\infty}{p^e} - \frac{2e_\infty}{p^e} - \frac{e_\infty - 1}{p^e - 1} \right). \]

Proof. Let \(p\) be a prime divisor of \(k(\sigma)\) of smallest degree which splits completely in \(Z\). Then by Theorem 6,
\[ \deg_{Z_m}(\mathcal{P}_m) \leq m. \]

Let \(\mathcal{P}_1\) be any prime of \(Z\) which lies over \(p\); then \(\mathcal{P}_1\) has \(p^e\) distinct conjugates under the action of the Galois group. If \(\mathcal{P}_o\) is any prime of \(Z\) (other than \(\mathcal{P}_1\)) which lies over the infinite prime of \(k(\sigma)\), then
\[ \deg_{Z_m}(\mathcal{P}_o) \leq \frac{q^{m^2} e_\infty}{q^{m^2} e_\infty + 1} E_{k(\sigma)}. \]

Therefore, since \(E\) is the exponent of \(D_k(Z)/E(Z)\), the null class group,
\[ \mathcal{P}_1 \deg_{Z_m}(\mathcal{P}_o) \mathcal{P}_o = (a) \in E(Z), \quad a \in \mathcal{Z}. \]

The function \(a\) has its only pole at \(p\) over the infinite prime of \(k(\sigma)\); so \(a\) is integral over \(k(\sigma)\). Also \(a\) has \(p^e\) distinct conjugates under the action of the Galois group of \(Z/k(\sigma)\); thus, \(a\) is a primitive element for this extension. By Theorem 5,
\[ -E \deg_{Z}(\mathcal{P}_1) \leq \frac{e_\infty - 1}{p^e - 1} - \frac{2e_\infty}{p^e} - \frac{2G e_\infty}{p^e(p^e - 1)}. \]

But \(\deg_{Z}(\mathcal{P}_1) = \deg_{Z_m}(\mathcal{P}_m) \leq m\). Therefore
\[ E \geq \frac{1}{m} \left( \frac{2G e_\infty}{p^e} - \frac{2e_\infty}{p^e} - \frac{e_\infty - 1}{p^e - 1} \right). \]

**Corollary.** In the class of finite, cyclic, geometric extensions \(Z\) of \(k(\sigma)\) of fixed degree \(p^e\), 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 \(e_\infty \geq 1,\)
\[ \frac{2e_\infty}{p^e} - \frac{e_\infty - 1}{p^e - 1} = \frac{p^e e_\infty - 2e_\infty}{p^e(p^e - 1)} \geq \frac{p^e - 1}{p^e(p^e - 1)} \geq \frac{2}{p^e}, \]
and so
\[ E \geq \frac{1}{m} \left( \frac{2G}{p^e} + \frac{2}{p^e} \right). \]
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
$$(q^{m_1} - 2G) = G^2 - 2G > 1,$$
for $G$ large enough. Thus,
$$q^{m_1}(q^{m_1} - 2G) - 2m_1(G + p^n) > q^{m_1} - 2m_1(G + p^n),$$
or, after plugging in the value suggested for $m_1$,
$$q^{m_1}(q^{m_2} - 2G) - 2m_1(G + p^n) > G^2 - \frac{12}{\log q} (\log G)(G + p^n).$$
If $G$ is large enough, this is positive; so $m_2 = \frac{6\log G}{\log q}$ satisfies the inequality of Theorem 6. Now,
$$m = m_0 = m_1 + 2 = \frac{6\log G}{\log q} + 2 \leq \frac{7\log G}{\log q},$$
if $G$ is large enough.

Putting this in (10) gives
$$E \geq \frac{\log q}{7\log G} \left( \frac{2G}{p^n(p^n - 1)} + \frac{2}{p^n} \right).$$
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 $E$ be a cyclic geometric extension of $k(x)$ of degree $p$ where $p$ is the characteristic of $k$; then $E$ 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 $E = k(x, y)$ where
$$y^p - y = f(x) = \prod_{i=1}^{t} p_i(x)^{\mu_i}, \quad \mu_i \in Z.$$  

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
$$y^p - y = f(x), \quad (f(x) = \frac{\Omega}{p_1(x)^{\lambda_1}p_2(x)^{\lambda_2} \cdots p_t(x)^{\lambda_t}}, \quad (\lambda_i, p) = 1 \quad \text{for} \quad i = 1, 2, \ldots, t.$$
Also $\Omega$ 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
$$y^p - y = f(x) = \prod_{i=1}^{t} p_i(x)^{r_i}p_2(x)^{r_2} \cdots p_t(x)^{r_t}, \quad (\lambda_i, p) = 1;$$
and, in keeping with the standard form of $f(x)$,
$$\lambda = \begin{cases} \deg f(x), & \text{if} \quad \deg f(x) > 0, \\ 0, & \text{if} \quad \deg f(x) \leq 0. \end{cases}$$

Thus $(\lambda, p) = 1$, if $\lambda \neq 0$. Further, for any prime divisor $p$ of $k(x)$:

1. If $p$ is ramified, if and only if $p$ divides the (divisor) denominator of $f(x)$. The contribution of the prime $p$ of $Z$ above $p$ to the different is
$$\delta(p) = \begin{cases} \delta(p) = \Omega^{(l_p + \lambda_p - 1)}, & \text{if} \quad p \text{ is not an infinite prime,} \\ \delta(p) = \Omega^{(l_p + \lambda_p - 1)}, & \text{if} \quad p \text{ is the infinite prime.} \end{cases}$$
2. If $p$ is an unramified prime, then
$$y^p - y = f(x)$$
is an integral polynomial with respect to $p$. The decomposition of $p$ in $Z$ mirrors the decomposition of this polynomial modulo $p$. That is, $p$ is inert if $y^p - y - f(x)$ is irreducible in $\mathcal{O}_p/I_p$ and is split if the polynomial factors there.

In an Artin–Schreier extension, there is an automorphism $\sigma$ which generates $\operatorname{Gal}(Z/k(x))$ such that
$$\sigma(y) = y + 1.$$

With the notation in Theorem 8, let $\mathcal{E}$ 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
$$y^p - y = f(x) = \frac{\Omega}{p_1(x)^{\lambda_1}p_2(x)^{\lambda_2} \cdots p_t(x)^{\lambda_t}}.$$
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

\[
\theta_j = y^j \prod_{i=1}^s p_i(x)^{\nu_{ij}}, \quad \text{for} \quad \nu_{ij} = \begin{cases} 1 + \left\lfloor \frac{j \lambda_i}{p} \right\rfloor, & \text{if } j \neq 0, \\ 0, & \text{if } j = 0. \end{cases}
\]

Proof. \( \theta_j \) is clearly integral for all the primes of \( Z \) except possible those lying over ramified primes or the infinite prime. If \( \Psi_i \) is a prime of \( Z \) lying over \( p_i(x) \), the prime divisor of \( k(x) \) associated with \( p_i(x) \), then

\[
v_{\Psi_i}(y) < 0.
\]

Therefore,

\[
v_{\Psi_i}(y) = v_{\Psi_i}(y + 1) = v_{\Psi_i}(y + 2) = \ldots = v_{\Psi_i}(y + p - 1).
\]

This gives immediately

\[
v_{\Psi_i}(y) = -\frac{1}{p} v_{\Psi_i}(y^p - y) = -\frac{1}{p} v_{\Psi_i}(f(x)) = -\lambda_i,
\]

and, using the definition,

\[
v_{\Psi_i}(\theta_j) = v_{\Psi_i}\left(y^j \prod_{i=1}^s p_i(x)^{\nu_{ij}}\right) = -j\lambda_i + \nu_{ij}p.
\]

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

To compute the discriminant of the basis \( \{ \theta_j \} \), let \( M \) be the matrix of coefficients in the linear equations expressing \( \theta_j \) in terms of \( \{ y^j \} \). Then,

\[
A_z(\theta_j) = [\det M]^2 A_z(y^j).
\]

But \( A_z(y^j) \) is the discriminant of the polynomial \( y^p - y - f(x) \), which is 1. So,

\[
A_z(\theta_j) = \prod_{i=1}^s p_i(x)^{\nu_{ij} - 1}.
\]

(13)

Now,

\[
\sum_{j=0}^{p-1} \nu_{ij} = \sum_{j=0}^{p-1} \left(1 + \left\lfloor \frac{j \lambda_i}{p} \right\rfloor\right) = (p - 1) + \frac{\lambda_i}{2} (p - 1) - \frac{1}{2} (p - 1) = \frac{1}{2} (\lambda_i + 1) (p - 1).
\]

(14)

Then (13) and (14) together give

\[
A_z(\theta_j) = \prod_{i=1}^s p_i(x)^{\nu_{ij} - 1} = \prod_{i=1}^s p_i(x)^{\nu_{ij} - 1}.
\]

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

\[
A_x(\theta_j) = A_x(Z),
\]

where \( A_x(Z) \) is the Dedekind discriminant of \( Z \) over \( k(x) \). Thus \( \{ \theta_j \} \) 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 \( \alpha \in Z \) which is a primitive element of the extension \( Z \) over \( k(x) \), there is a prime divisor \( \Psi_\infty \) of \( Z \) lying over the infinite prime \( p_{\infty} \) of \( k(x) \) such that

\[
v_{\Psi_\infty}(\alpha) \leq -\varepsilon_0 \left(\frac{2G}{p(p-1)} + \frac{1}{p}\right),
\]

where \( \varepsilon_0 \) is the ramification index of \( \Psi_\infty \) and \( G \) is the genus of \( Z \).

Proof. If \( \alpha \not\in \mathcal{O} \), then by the previous theorem \( \alpha \) can be written as

\[
\alpha = a_0(x) \theta_0 + a_1(x) \theta_1 + \ldots + a_{p-1}(x) \theta_{p-1}
\]

where \( a_i(x) \in k[x] \) and \( b_i(x) = a_i(x) \prod_{j \neq i} p_j(x)^{\nu_{ij}} \). As in the proof of Theorem 4, it is necessary to evaluate \( v_{\Psi_\infty}(\alpha) \) for some \( \Psi_\infty \) lying over \( p_{\infty} \). It is convenient to do this in the form of

Lemma 2. For a \( \alpha \) as in the theorem, there is a \( \Psi_\infty \) lying over the infinite prime \( p_{\infty} \) of \( k(x) \) such that

\[
v_{\Psi_\infty}(\alpha) = m,
\]

where

\[
m = \begin{cases} \min \left\{ v_{\Psi_\infty}(b_j(x)^{\nu_{ij}}) \right\}, & \text{if } p_{\infty} \text{ is ramified in } Z, \\ \min \left\{ v_{\Psi_{\infty}}(b_j(x)) \right\}, & \text{if } p_{\infty} \text{ is unramified in } Z. \end{cases}
\]

Proof of Lemma 2. The proof is given in two parts. First, if \( p_{\infty} \) is ramified in \( Z \), then there is only one prime \( \Psi_\infty \) of \( Z \) over \( p_{\infty} \), and \( v_{\Psi_\infty}(\alpha) = -\lambda_\infty \). Now,

\[
v_{\Psi_\infty}(b_j(x)^{\nu_{ij}}) = v_{\Psi_\infty}(b_j(x)) + v_{\Psi_{\infty}}(\nu_{ij}) = p v_{p_{\infty}}(b_j(x)) - j\lambda_\infty.
\]

However, since \( p_{\infty} \) is ramified, \( \lambda_\infty \equiv 0 \mod p \), and so the set

\[
\{ v_{\Psi_\infty}(b_j(x)^{\nu_{ij}}) \mid 0 \leq j < p \}
\]
is a complete residue system modulo $p$. Therefore, this set has a distinct minimum, and so,

$$v_{p_0}(a) = m.$$  

Next is the case where $p_{1_{\infty}}$ is unramified in $Z$. If $\Psi_1$ is any prime of $Z$ over $p_{1\infty}$, then

$$v_{\Psi_1}(y) \geq 0.$$  

Thus for all the primes $\Psi$ over $p_{1\infty}$,

$$v_{\Psi}(\alpha) = v_{\Psi}(b_0(\alpha) + b_1(\alpha)y + \ldots + b_{p-1}(\alpha)y^{p-1}) \geq \min_{0 < j < p} \{ v_{\Psi}(b_j(\alpha)y^j) \} \geq \min_{0 < j < p} \{ v_{\Psi}(b_j(\alpha)) + jv_{\Psi}(y) \} \geq \min_{0 < j < p} \{ v_{\Psi}(b_j(\alpha)) \} \geq m.$$  

Notice here, that there is some prime $\Psi_1$ over $p_{1\infty}$ such that $v_{\Psi_1}(y) = 0$. For suppose $v_{\Psi_1}(y) > 0$, then $v_{p_{1\infty}}(f(x)) > 0$, and so $p_{1\infty}$ must split over $Z$. Then

$$v_{\Psi_1}(y) = v_{\Psi_1}(y + 1) = \min \{ v_{\Psi_1}(y), 0 \} = 0.$$  

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

$$v_{\Psi_1}(\alpha) = \min_{0 < j < p} \{ v_{\Psi_1}(b_j(\alpha)y^j) \} = m$$

for that prime $\Psi_1$ over $p_{1\infty}$ for which $v_{\Psi_1}(y) = 0$. Consider then

$$y^{p-1-j_0} = b_0(\alpha)y^{p-1-j_0} + b_1(\alpha)y^{p-1-j_0} + \ldots + b_{j_0}(\alpha)y^{j_0} + \ldots + b_{p-1}(\alpha)y^{p-1}.$$  

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 $k(\alpha)$ (denoted by $Tr(\alpha)$) acts on these powers of $y$ in the following way:

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

Therefore, (16) gives, for any prime $\Psi_1$ above $p_{1\infty}$,

$$m = v_{p_{1\infty}}(b_0(\alpha)) = v_{\Psi_1}(b_0(\alpha)) = v_{\Psi_1}(Tr(y^{p-1-j_0})).$$

This, together with (15) gives

$$m \geq \min_{\Psi \text{ above } p_{1\infty}} \{ (p - 1 - j_0)v_{\Psi}(y) + v_{\Psi}(\alpha) \} \geq m.$$  

Thus, there is a prime $\Psi_\infty$ in $Z$ above $p_{1\infty}$ such that $v_{\Psi_\infty}(\alpha) = m$, and this proves the lemma.

**Proof of Theorem 10.** It remains to estimate the value of $m$ in the lemma. For a primitive element $\alpha$ in the extension $Z$ over $k(\alpha)$, there is an index $j_1$ such that $a_j(\alpha) \neq 0$ and $f_1 \neq 0$. When $p_{1\infty}$ is ramified this gives

$$m = \min_{0 < j < p} \{ v_{\Psi_\infty}(b_j(\alpha)y^j) \} \leq v_{\Psi_\infty}(a_j(\alpha)) + \sum_{i=1}^{j-1} p_i(\alpha)^{j_i} - j_1 \lambda_0 \leq \sum_{i=1}^{j-1} p_i(\alpha)^{j_i} - \lambda_0.$$  

When $p_{1\infty}$ is unramified,

$$m = \min_{0 < j < p} \{ v_{p_{1\infty}}(b_j(\alpha)) \} \leq v_{p_{1\infty}}(a_j(\alpha)) + v_{p_{1\infty}}(\sum_{i=1}^{j-1} p_i(\alpha)^{j_i}) \leq v_{p_{1\infty}}(\sum_{i=1}^{j-1} p_i(\alpha)^{j_i}).$$

In both cases it is necessary to approximate $v_{p_{1\infty}}(\sum_{i=1}^{j-1} p_i(\alpha)^{j_i})$, for $j \neq 0; j \geq -p$:

$$v_{p_{1\infty}}(\sum_{i=1}^{j} p_i(\alpha)^{j_i}) = -\deg(\sum_{i=1}^{j} p_i(\alpha)^{j_i}) = -\sum_{i=1}^{j} \deg p_i(\alpha)$$

$$\leq -\sum_{i=1}^{j} \left( \frac{j_i}{p} \right) \deg p_i(\alpha) \leq -\sum_{i=1}^{j} \left( \frac{j_i}{p} + \frac{1}{p} \right) \deg p_i(\alpha),$$

$$\leq -\frac{1}{p} \sum_{i=1}^{j} (j_i + 1) \deg p_i(\alpha)$$

(20)

$$\leq -\frac{1}{p} \sum_{i=1}^{j} (j_i + 1) \deg p_i(\alpha)$$

(21)
where \( A_\kappa \) is the ideal discriminant of \( Z \). When \( p_\kappa \) is unramified
\[
\deg A_\kappa = \deg_{\kappa(\mathbf{a})} A,
\]
where \( A \) is the divisor discriminant, and so, by the genus formula, (19), and (21),
\[
m \leq -\frac{1}{p(p-1)} \deg A = -\frac{2G}{p(p-1)} - \frac{2}{p}.
\]
When \( p_\kappa \) is ramified,
\[
A = (A_\kappa)^{\left(p^{e_\kappa}(\mathbf{a})\right)},
\]
and so
\[
\deg A_\kappa = \deg A - (p-1)(\lambda_\infty + 1).
\]
Using the genus formula, it follows from (18) and (21) that
\[
m \leq -p \left( \frac{\deg A - (p-1)(\lambda_\infty + 1)}{p(p-1)} \right) - \lambda_\infty \\
\leq -\frac{1}{p-1} \left( 2G - 2(p-1) - (p-1)(\lambda_\infty + 1) + \lambda_\infty (p-1) \right) \leq -\frac{2G}{p-1} - 1.
\]
In either case there is a prime \( \mathfrak{p}_\infty \) of \( Z \) lying over \( p_\kappa \) such that
\[
\nu_{\mathfrak{p}_\infty}(a) = m = -e_\infty \left( \frac{2G}{p(p-1)} + \frac{1}{p} \right),
\]
where \( e_\infty \) is the ramification index of \( \mathfrak{p}_\infty \). This completes the proof of Theorem 10.

Since Theorem 6 holds for all cyclic extensions of \( k(a) \) of prime power degree, there is a bound on the minimum degree of a prime of \( k(a) \) 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 \( k(a) \). If \( G \) is the genus of \( Z \), \( e_\infty \) is the ramification index of a prime over the infinite prime, \( m = m_{\kappa} \) of Theorem 6, and \( E \) is the exponent of the null class group of \( Z \), then
\[
E \geq \frac{e_\infty}{m} \left( \frac{2G}{p(p-1)} + \frac{1}{p} \right).
\]

**Corollary.** In the class of Artin–Schreier extensions of \( k(a) \) 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
\[
E \geq \frac{\log q}{\log G} \left( \frac{2G}{p(p-1)} + \frac{1}{p} \right).
\]

Thus
\[
\lim_{G \to \infty} E = \infty.
\]

**4. The main result.** The next step is to combine the results of Section 3 with the results of Section 3 to show that, for a special class of extensions of \( k(a) \), 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 \( k(a) \) of fixed degree where the \( p \)-primary part of the Galois group is elementary abelian. These are exactly those extensions of \( k(a) \) 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 \( K/k(a) \) be an extension as described above, and let \( G \) be its genus. Then,
\[
\text{Gal}(K/k(a)) = C_1 \times C_2 \times \cdots \times C_n,
\]
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
\[
\text{Gal}(Z_i/k(a)) = C_i.
\]

These subfields are, therefore, either cyclic geometric extensions of \( k(a) \) of prime power degree for primes other than the characteristic or are Artin–Schreier extensions of \( k(a) \). 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 \( k(a) \) such that \( Z_i \subseteq K \) for \( i = 1, 2 \), and such that
\[
\text{Gal}(K/k(a)) = \text{Gal}(Z_1/k(a)) \times \text{Gal}(Z_2/k(a)).
\]

Then, as divisors of \( K \),
\[
\delta(K/Z_1) \text{ divides } \delta(Z_1/k(a))
\]
and
\[
\delta(K/Z_2) \text{ divides } \delta(Z_2/k(a)),
\]
where \( \delta \) denotes the different of the proper extension.
The exponent of class groups in congruence function fields

Proof. Let \( \theta_1, \theta_2, \ldots, \theta_n \) be the respective integral closures of \( k(x) \) in \( Z_1, Z_2, \ldots, \) and \( K \). Also let \( \delta_1(K/Z_1) \) and \( \delta_2(Z_2/k(x)) \) be the Dedekind differents in the respective extensions. It is well-known that \( \delta_2(Z_2/k(x)) \) is the greatest common divisor of the different of all the elements of \( \theta_2 \). However

\[
\text{Gal}(K/Z_1) \cong \text{Gal}(K/k(x))/\text{Gal}(Z_2/k(x)) \cong \text{Gal}(Z_2/k(x)),
\]

and \( \theta_2 \subseteq \theta_1 \). Thus the different of an element of \( \theta_2 \) in the extension \( Z_2/k(x) \) can also be considered as the different of an element of \( \theta_1 \) in the extension \( K/Z_1 \). Therefore,

\[
\delta_2(K/Z_1) \text{ divides } \delta_2(Z_2/k(x)).
\]

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

\[
\delta(K/Z_2) \text{ divides } \delta(Z_2/k(x)).
\]

**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. \( \text{Gal}(K/k(x)) = \text{Gal}(Z_1/k(x)) \times \text{Gal}(Z_2/k(x)) \times \cdots \times \text{Gal}(Z_h/k(x)) \).

Then for some field \( Z_i \), say \( Z_1 \),

\[
G_1 \geq \frac{1}{n} \left( G - (h-1)n + \sum_{i=1}^{h} n_i - 1 \right).
\]

Proof. For the purposes of this proof, \( Z_1, Z_2, \ldots, Z_h \) will denote the smallest subfield of \( K \) containing the fields \( Z_1, Z_2, \ldots, Z_h \). In this particular case,

\[
\text{Gal}(Z_1Z_2 \cdots Z_h/k(x)) = \text{Gal}(Z_1/k(x)) \times \text{Gal}(Z_2/k(x)) \times \cdots \times \text{Gal}(Z_h/k(x)).
\]

Now in the tower of fields \( K \supseteq Z_i \supseteq k(x) \),

\[
\delta(K/k(x)) = \delta(Z_i/k(x)) \delta(K/Z_1),
\]

considered as divisors of \( K \). Now, by the lemma,

\[
\delta(K/Z_1) \text{ divides } \delta(Z_2Z_3 \cdots Z_h/k(x)),
\]

and so

\[
\delta(K/k(x)) \text{ divides } \delta(Z_1/k(x)) \delta(Z_2Z_3 \cdots Z_h/k(x)).
\]

Similarly,

\[
\delta(K/k(x)) \text{ divides } \delta(Z_1/k(x)) \delta(Z_2Z_3 \cdots Z_h/k(x)).
\]

This can be continued until

\[
\delta(K/k(x)) \text{ divides } \delta(Z_1/k(x)) \delta(Z_2/k(x)) \cdots \delta(Z_h/k(x)).
\]

Taking degrees in \( K \) gives:

\[
\text{deg}_K(\delta(K/k(x))) \leq \sum_{i=1}^{h} \text{deg}_K(\delta(Z_i/k(x))) \leq \sum_{i=1}^{h} n_i^{*}\text{deg}_K(\delta(Z_i/k(x)))
\]

where \( n_i^{*} \equiv \frac{n_i}{n} \), \( i = 1, 2, \ldots, k \). After applying the genus formula, this gives

\[
2G + 2(n-1) \leq \sum_{i=1}^{h} n_i^{*} \left[ 2G_i + 2(n_i - 1) \right],
\]

and so,

\[
\sum_{i=1}^{h} n_i^{*} \geq G - (h-1)n + \sum_{i=1}^{h} n_i^{*} - 1.
\]

Since \( n \geq n_i^{*} \), there must be some \( G_i \), say \( G_1 \), such that

\[
G_1 \geq \left( \frac{1}{n} \left( G - (h-1)n + \sum_{i=1}^{h} n_i^{*} - 1 \right) \right)
\]

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

\[
E \geq C \frac{G}{\log \left( \frac{G}{n^* + M} \right)},
\]

where \( C \) and \( M \) are constants.

Proof. Let

\[
\text{Gal}(K/k(x)) = C_1 \times C_2 \times \cdots \times C_h,
\]

...
where each \( C_i \) is a group of prime power order, and let \( Z_i \) be the subfield of \( K \) for which
\[
\text{Gal}(Z_i/k(x)) = C_i, \quad i = 1, 2, \ldots, h.
\]
Then by Theorem 12, \( C_i \) can be chosen such that its genus \( G_i \), is bounded by
\[
G_i \geq \frac{1}{n^i} \left( G - (k-1) + \sum_{i=1}^{h} \frac{n_i}{n_i} - 1 \right)
\]
where \( n = [K : k(x)] \) and \( n_i = [Z_i : k(x)] \), \( i = 1, 2, \ldots, h \). Since \( n \geq h \) this can be written as
\[
G_i \geq \frac{G}{n^i} + M, \quad \text{for some constant } M.
\]

Now \( Z_i \) 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)),
\[
E_i \geq \frac{\log q}{7n_1} \left( \frac{2G_1}{n_1(n_1-1)} + \frac{1}{n_1} \right) \geq \frac{2\log q}{7n_1(n_1-1)} \frac{G_1}{\log G_1}.
\]
However, if \( \delta \) is large enough, \( \frac{\theta}{\log G} \) is an increasing function, and so,
\[
E_i \geq \frac{2\log q}{7n_1(n_1-1)} \frac{G_1}{\log \left( \frac{G}{n^i} + M \right)}.
\]
Also since \( n \geq n_1 \),
\[
E_i \geq \frac{2\log q}{7n(n-1)} \frac{G_1}{\log \left( \frac{G}{n^i} + M \right)}.
\]
Thus, when the genus of \( K \) is large, there is a subextension \( Z_i \) of \( k(x) \) whose null class group \( C_0(Z_i) \) has equally large exponent. The group \( C_0(Z_i) \) is mapped in a canonical way into \( C_0(K) \). This map (called the conorm) has the following property [3]
\[
[K : k(x)] \text{ divides } \text{Gal}(Z_i/k(x)).
\]
In this particular case,
\[
[K : k(x)] = n.
\]

But then the null class group \( C_0(K) \) of \( K \) contains a subgroup,
\[
C_0(Z_i)/\text{Ker(conorm)},
\]
whose exponent is greater than or equal to \( \frac{E_i}{n} \). Thus by (23),
\[
E_i \geq \frac{E_i}{n} \geq \frac{2\log q}{7n^i(n-1)} \frac{\left( \frac{G}{n^i} + M \right)}{\log \left( \frac{G}{n^i} + M \right)}.
\]
This completes the proof of the main theorem.

References


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

Received on 25. 9. 1975 (770)