ACTA ARITHMETICA
LXXII.4 (1995)

On the exponent of the ideal class groups of imaginary extensions of $\mathbb{F}_q(x)$

by

HERSHY KISILEVSKY (Montréal, Qué.) and
FRANCESCO PAPPALARDI (Roma)

1. Introduction. Let d be a square-free positive integer. We denote by $\mathcal{C}(d)$ the ideal class group of the imaginary field $\mathbb{Q}(\sqrt{-d})$ and by $e(d)$ the exponent of $\mathcal{C}(d)$, that is, the least positive integer e such that

$$x^e = 1 \quad \text{for all } x \in \mathcal{C}(d).$$

In 1969, at the Stony Brook conference, K. Iwasawa asked whether

$$\lim_{d\to\infty} e(d) = \infty.$$

In 1972, Boyd and the first author (see [1]) showed under the assumption of the Extended Riemann Hypothesis that for all $\varepsilon > 0$, there exists $d(\varepsilon)$ such that for all $d > d(\varepsilon)$, one has

$$e(d) > \frac{\log d}{(2+\varepsilon)\log\log d}, \tag{1.1}$$

which is a conditional positive answer to Iwasawa's original question. As we will see, this result is ineffective due to the inexpliciteness of the error term in the Chebotarev Density Theorem.

In 1992, the second author (see [4]) proved that the inequality (1.1) holds (unconditionally) for almost all discriminants d.

The proof of the estimate in (1.1) consists of two steps:

(a) One notes that if α is an integer of $\mathbb{Q}(\sqrt{-d})$ which is not in $\mathbb{Z}$, then

$$N(\alpha) > d/4. \tag{1.2}$$

(b) One uses the fact that the least rational prime p which splits in $\mathbb{Q}(\sqrt{-d})$ is less than $(\log d)^{2+\varepsilon}$ for all d large enough.

1991 *Mathematics Subject Classification*: Primary 11R29; Secondary 11N37.
Research of the first author supported in part by grants from NSERC and FCAR.
Research of the second author supported by CICMA.

Finally, if $\mathfrak{p}$ is a prime above the split prime p then the ideal $\mathfrak{p}^{e(d)}$ is a principal ideal (α) $(\alpha \notin \mathbb{Z})$. Taking norms one has by the first step

$$N(\mathfrak{p}^e) \geq N(\alpha) > d/4;$$

and by the second step

$$N(\mathfrak{p}^e) = p^e \leq (\log d)^{e(2+\varepsilon)}.$$

These two inequalities imply (1.1).

Step (a) is possible since in $\mathbb{Q}(\sqrt{-d})$ the group of units is finite. Step (b) can be deduced rather directly from the version of the Chebotarev Density Theorem proven under the assumption of the Riemann Hypothesis. In the case of function fields, the Riemann Hypothesis is known to be true and this is the basic motivation of this article.

Let q be a power of a prime, let $F = \mathbb{F}_q(x)$ be a function field in one variable over the finite field with q elements and let $\mathcal{O} = \mathbb{F}_q[x]$ denote the polynomial ring. An extension E/F is said to be *imaginary* if there is a unique place of E above the place $\mathfrak{p}_\infty$ associated with the valuation at ∞ of $\mathcal{O}$.

For any extension E over F we denote by $\mathcal{O}_E$ the integral closure of $\mathcal{O}$ in E. Then $\mathcal{O}_E$ is a Dedekind domain and it is called the *ring of integers* of E.

Note that if E is an imaginary extension of F, then the group of units of $\mathcal{O}_E$ is finite.

In the case where E is quadratic over F, $\mathrm{char}(F) \neq 2$, then

$$E = \mathbb{F}_q(x, y), \quad y^2 = f(x), \quad f(x) \in \mathcal{O}$$

and $f(x)$ is not a square in $\mathbb{F}_q((1/x))$. Note that $\mathbb{F}_q((1/x))$ is the completion of $\mathcal{O}$ at the valuation at ∞.

In this case the analogous property to the inequality (1.2) of the first step of the proof of (1.1) is shown in the following:

PROPOSITION 1.1. *Suppose* $\mathrm{char}(F) > 2$ *and let* $E = \mathbb{F}_q(x, y)$ *be an imaginary quadratic extension of* F. *If* $y^2 = f(x)$ *with* $f(x) \in \mathcal{O}$ *square-free, then for all* $\alpha \in \mathcal{O}_E \setminus \mathcal{O}$ *we have*

$$\deg N_{E/F}(\alpha) \geq \deg f.$$

Proof. Suppose $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, then

$$f(x) = x^n a_n \left(1 + b_{n-1}\frac{1}{x} + \ldots + b_0 \frac{1}{x^n}\right)$$

with $b_j = a_j/a_n$. Since every Laurent polynomial congruent to 1 $(\mathrm{mod}\, \mathfrak{p}_\infty)$ is a square in $\mathbb{F}_q((1/x))$, we see that $f(x)$ is a square in $\mathbb{F}_q((1/x))$ if and only if n is even and a_n is a square in $\mathbb{F}_q$. Hence E/F is imaginary if and only if either $\deg f$ is odd or $\deg f$ is even and $a_n \notin (\mathbb{F}_q)^2$.

Now we can write

$$\alpha = g + hy$$

and

$$N_{E/F}(\alpha) = g^2 - h^2y^2 = g^2 - h^2 f \in \mathcal{O}$$

with $g, h \in \mathcal{O}$ and $h \neq 0$.

If $\deg(g^2) \neq \deg(h^2 f)$, then $\deg(g^2 - h^2 f) \geq \deg f$ as $h \neq 0$.

If $\deg(g^2) = \deg(h^2 f)$, then $\deg f$ is even thus $a_n \notin (\mathbb{F}_q)^2$. This implies that if c and d are the coefficients of the term with highest degree of g and h, the term with highest degree of $g^2 - h^2 f$ is $c^2 - d^2 a_n$, which is not zero since otherwise a_n would be a square in $\mathbb{F}_q$.

So in either case we have the assertion. ∎

2. The Chebotarev Density Theorem. The norm $N(\mathfrak{p})$ of a prime $\mathfrak{p}$ of $\mathcal{O}$ is defined as the number of elements in the residue field of the completion of F at $\mathfrak{p}$. The degree $\deg \mathfrak{p}$ is defined by the identity

$$N(\mathfrak{p}) = q^{\deg \mathfrak{p}}.$$

If $\mathfrak{p}$ is the principal ideal $(g(x))$, then the above degree coincides with the usual degree of the polynomial $g(x)$.

Now suppose that E is a finite Galois extension of F and set

$$C_k(E/F) = \#\{\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}) \mid \deg \mathfrak{p} = k,\ \mathfrak{p} \text{ splits completely in } E/F\}.$$

Then the Riemann Hypothesis for function fields allows one to prove the following:

THEOREM 2.1. *Let L be the algebraic closure of $\mathbb{F}_q$ in E and let*

$$n = [L : \mathbb{F}_q], \qquad m = [E : LF].$$

Then for all k for which $n \mid k$,

$$\left| C_k(E/F) - \frac{1}{m}\frac{q^k}{k} \right| < 4q^{k/2}\left(1 + \frac{g_E}{km}\right),$$

where g_E is the genus of E. If $n \nmid k$ then $C_k(E/F) = 0$.

Proof. See Proposition 5.16 in Fried and Jarden [2]. ∎

We will use the Chebotarev Density Theorem in the following form:

COROLLARY 2.2. *With the same notation as above, let*

$$r = 4\left(g_E + mn + m\frac{14\log(g_E + mn)}{\log q}\right).$$

Then there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ which splits completely in $\mathcal{O}_E$ and $N(\mathfrak{p}) \leq r^2$.

Proof. In order to have $C_k(E/F) > 1$ we must assure that the main term in Theorem 2.1 bounds the error term.

Indeed,

$$C_k(E/F) > \frac{q^k}{mk} - 4q^{k/2}\left(1 + \frac{g_E}{km}\right) = \frac{q^{k/2}}{mk}(q^{k/2} - 4(mk + g_E)).$$

Let k_0 be the least integer such that $n \mid k_0$ and $q^{k_0} > r^2$. Then

$$\frac{2\log r}{\log q} < k_0 \leq \frac{2\log r}{\log q} + n$$

and therefore

$$\begin{aligned} C_{k_0}(E/F) &> \frac{r}{k_0 m}\left(r - 4m\left(\frac{2\log r}{\log q} + n\right) - 4g_E\right) \\ &= \frac{8r}{k_0 \log q}(7\log(g_E + mn) - \log r) > 0. \end{aligned}$$

The last inequality holds since $(g_E + mn)^7 > r$ for all g_E, m, n and q. Therefore $C_k(E/F) \geq 1$ for some $k < k_0$. Hence there is a prime in $\mathcal{O}$ that splits completely in $\mathcal{O}_E$ with norm less than r^2. ∎

We can now state the first result:

THEOREM 2.3. *Suppose that* $\mathrm{char}(F) > 2$, *let* $E = \mathbb{F}_q(x, y)$ *be an imaginary quadratic extension of* F *and let* $y^2 = f(x)$ *with* $f(x) \in \mathcal{O}$ *square-free. Let* $e(f)$ *be the exponent of the ideal class group of the Dedekind domain* $\mathcal{O}_E$. *Then*

$$e(f) \geq \frac{\deg f \log q}{2\log(72 \deg f)}.$$

Proof. From Corollary 2.2, we see that there exists a prime ideal $\mathfrak{p}_0$ of $\mathcal{O}$ that splits completely in E with degree such that

$$\begin{aligned} q^{\deg \mathfrak{p}_0} &\leq \left(4\left(g_E + 2 + 28\frac{\log(g_E + 2)}{\log q}\right)\right)^2 \\ &\leq (4((28/\log 3 + 1)g_E + 28/\log 3 + 2))^2. \end{aligned}$$

Now let $\mathfrak{P}_0$ be a prime above $\mathfrak{p}_0$. As in the case of $\mathbb{Q}(\sqrt{-d})$ we see that $\mathfrak{P}_0^{e(f)}$ is a principal ideal (α), hence by Proposition 1.1,

$$q^{e(f)\deg \mathfrak{p}_0} = N_{E/F}(\mathfrak{P}_0^{e(f)}) = N_{E/F}(\alpha) \geq q^{\deg f},$$

which by taking logarithms gives

$$e(f) \geq \frac{\deg f \log q}{2\log(4((28/\log 3 + 1)g_E + 28/\log 3 + 2))}.$$

Finally, by the Riemann–Hurwitz formula we have

$$g_E \leq \frac{\deg f - 1}{2}$$

and since $\deg f \geq 3$, the statement is proved. ∎

3. The relation with the Jacobian. In this section we want to compare the estimate for the exponent obtained by this method (algebraic estimate) with the geometric estimate.

Suppose that E is the function field of a curve $X/\mathbb{F}_q$, and let $J_0(E)$ denote the points in the Jacobian of X rational over $\mathbb{F}_q$. Then $J_0(E)$ is isomorphic to the group of divisor classes of degree 0 of E. The ideal class group $\mathcal{C}(\mathcal{O}_E)$ can be related to $J_0(E)$:

PROPOSITION 3.1. *Suppose E is an imaginary extension of F of degree m and let $\mathfrak{P}_\infty$ denote the unique prime of E dividing $\mathfrak{p}_\infty$ of F. If $h = \deg \mathfrak{P}_\infty$ and d is the least degree of a prime divisor of E/F then*

$$\mathcal{C}(\mathcal{O}_E)/J_0(E) \simeq \mathbb{Z}/(h/d)\mathbb{Z}.$$

Proof. Let $\mathcal{D}(E)$ be the divisor group and $\mathcal{P}(E)$ be the group of principal divisors. By considering the exact sequence

$$\begin{array}{ccccccccc} 0 & \to & \langle \mathfrak{P}_\infty \rangle \mathcal{P}(E) & \to & \mathcal{D}(E) & \to & \mathcal{C}(\mathcal{O}_E) & \to & 0, \\ & & & & n_\infty \mathfrak{P}_\infty + \sum n_\mathfrak{P} \mathfrak{P} & \mapsto & \left[\prod \mathfrak{P}^{n_\mathfrak{P}}\right] & & \end{array}$$

we have the isomorphism

$$\mathcal{C}(\mathcal{O}_E) \simeq \frac{\mathcal{D}(E)}{\langle \mathfrak{P}_\infty \rangle \mathcal{P}(E)}.$$

On the other hand, consider the exact sequence

$$0 \to \mathcal{D}_0(E) \to \mathcal{D}(E) \to d\mathbb{Z} \to 0,$$

where the second map is the degree and first map is the inclusion of the group $\mathcal{D}_0(E)$ of divisors of degree 0 in $\mathcal{D}(E)$. Since $\mathcal{P}(E) \subset \mathcal{D}_0(E)$, we have that

$$\mathcal{P}(E)\langle \mathfrak{P}_\infty \rangle \subset \mathcal{D}_0(E)\langle \mathfrak{P}_\infty \rangle \subset \mathcal{D}(E),$$

therefore

$$0 \to \frac{\mathcal{D}_0(E)\langle \mathfrak{P}_\infty \rangle}{\mathcal{P}(E)\langle \mathfrak{P}_\infty \rangle} \to \frac{\mathcal{D}(E)}{\mathcal{P}(E)\langle \mathfrak{P}_\infty \rangle} \to \frac{\mathcal{D}(E)}{\mathcal{D}_0(E)\langle \mathfrak{P}_\infty \rangle} \to 0$$

and finally

$$0 \to J_0(E) \to \mathcal{C}(\mathcal{O}_E) \to \frac{(\deg \mathcal{D}(E))\mathbb{Z}}{(\deg \mathfrak{P}_\infty)\mathbb{Z}} \to 0. \tag{3.1}$$

Now, since $\deg \mathfrak{P}_\infty = h$ and $\deg \mathcal{D}(E) = d\mathbb{Z}$, we get the assertion. ∎

Now let us turn our attention to the exponent of $J_0(E)$. If $L(s)$ is the L-function of X, then it is known that

$$|J_0(E)| = L(1) = \prod_{i=1}^{2g_E}(1-\alpha_i).$$

By the Riemann Hypothesis for function fields, $|\alpha_i| = \sqrt{q}$, and thus it follows that

$$|J_0(E)| \geq (\sqrt{q}-1)^{2g_E}.$$

It follows from the theory of Riemann surfaces that $J_0(E)$ has at most $2g_E$ generators, therefore the exponent $e(E)$ of $J_0(E)$ is not smaller than

$$e(E) \geq |J_0(E)|^{1/(2g_E)} \geq \sqrt{q}-1. \tag{3.2}$$

In the case of Theorem 2.3 we have $\deg \mathfrak{P}_\infty \leq 2$ and therefore

$$|\mathcal{C}(\mathcal{O}_E)/J_0(E)| \leq 2.$$

If $\deg f$ is large with respect to q, more precisely if $\deg f \gg \sqrt{q}$, then the estimate of Theorem 2.3 is sharper than (3.2).

4. Application to the exponent. From now on we will suppose that E is an imaginary extension of F of degree m in which ∞ is totally ramified. That is, if $\mathfrak{p}_\infty$ is the prime at infinity of $\mathcal{O}$ and $\mathfrak{P}_\infty$ is the unique prime of $\mathcal{O}_E$ above $\mathfrak{p}_\infty$, then $\mathfrak{P}_\infty = \mathfrak{p}_\infty^m$. Let g_E denote the genus of E.

We note that since $\mathfrak{p}_\infty$ is totally ramified, for $\alpha \in \mathcal{O}_E$ we have

$$\deg N_{E/F}(\alpha) = -v_{\mathfrak{p}_\infty}(N_{E/F}(\alpha)) = -v_{\mathfrak{P}_\infty}(\alpha).$$

We can extend the result of Proposition 1.1 to a special class of such fields:

THEOREM 4.1. *Let $E = \mathbb{F}_q(x,y)$, $y^m = f(x)$ where $\mathrm{char}(F)$ does not divide m, and where $f(x)$ is a polynomial such that every prime divisor of $f(x)$ divides it to a power coprime to m. Suppose also that $(\deg f, m) = 1$. If $\alpha \in \mathcal{O}_E \setminus \mathcal{O}$, we have*

$$\deg N_{E/F}(\alpha) \geq \frac{2g_E}{m-1} + 1.$$

Proof. First we note that the condition $(\deg f, m) = 1$ implies that $\mathfrak{p}_\infty$ is totally ramified in E and so E is imaginary over F. Let $f = \prod_{j=1}^t p_j^{a_j}$ with $p_j \in \mathbb{F}_q[x]$ irreducible, $(a_j, m) = 1$, and $1 \leq a_j \leq m-1$, and let $f_1 = \prod_{j=1}^t p_j$.

The Riemann–Hurwitz formula then gives

$$g_E = \frac{(m-1)(\deg f_1 - 1)}{2}.$$

Let $\mathfrak{P}_i$ be the prime of E dividing $\mathfrak{p}_i = (p_i(x))$. Then since $(a_i, m) = 1$, it follows that $\mathfrak{P}_i$ is totally ramified in E/F, and that $\mathfrak{P}_i^m = \mathfrak{p}_i$ for $1 \leq i \leq t$.

Hence

$$(y) = y \cdot \mathcal{O}_E = \prod_{i=1}^{t} \mathfrak{P}_i^{a_i}.$$

For $1 \leq k \leq m-1$, write

$$a_i k = m q_{ik} + r_{ik} \quad \text{with } 1 \leq r_{ik} \leq m-1.$$

Then, for each fixed i, as k ranges over the distinct non-zero residue classes modulo m so does r_{ik}, since $(a_i, m) = 1$. For each $k, 1 \leq k \leq m-1$,

$$(y^k) = \prod_{i=1}^{t} \mathfrak{p}_i^{q_{ik}} \prod_{i=1}^{t} \mathfrak{P}_i^{r_{ik}} = (c_k) \prod_{i=1}^{t} \mathfrak{P}_i^{r_{ik}}$$

for some $c_k \in \mathcal{O}$, with $(c_k) = \prod_{i=1}^{t} \mathfrak{p}_i^{q_{ik}}$. Let $y_k = y^k/c_k$. Set $y_0 = 1$ and let $\mathcal{A} = \sum_{k=0}^{m-1} \mathcal{O} y_k$. We claim that the ring of integers is

$$\mathcal{O}_E = \mathcal{A}, \tag{4.1}$$

and we will prove this later. Now if $\alpha \in \mathcal{O}_E \backslash \mathcal{O}$, we have $\alpha = \sum_{k=0}^{m-1} g_k y_k$ with $g_k \in \mathcal{O}$, and $g_k \neq 0$ for some $k \geq 1$. Then since the valuations $v_{\mathfrak{P}_\infty}(g_k y_k)$ are distinct (modulo m), we have

$$v_{\mathfrak{P}_\infty}(\alpha) = \min_{0<k\leq m-1} v_{\mathfrak{P}_\infty}(g_k y_k) \leq \min_{0<k\leq m-1} v_{\mathfrak{P}_\infty}(y_k).$$

Taking norms and noting that $r_{ik} \geq 1$, we obtain

$$v_{\mathfrak{p}_\infty}(N_{E/F}(\alpha)) \leq \min_{0<k\leq m-1} v_{\mathfrak{p}_\infty}(N_{E/F}(y_k)) \leq v_{\mathfrak{p}_\infty}(f_1(x))$$

which is equivalent to

$$\deg N_{E/F}(\alpha) \geq \deg(f_1(x)).$$

We need only prove (4.1). For this, let $\beta \in \mathcal{O}_E$. Then we can write β as $\beta = \sum_{k=0}^{m-1} b_k y_k$, where $b_k \in F$ and we want to show that the b_k are elements of $\mathcal{O}$. We note that the trace $\mathrm{Tr}(y_k) = \mathrm{Tr}(y^k) = 0$ for $1 \leq k \leq m-1$, and $\mathrm{Tr}(y^m) = mf$. Therefore, $\mathrm{Tr}(\beta) = m b_0$ and hence $b_0 \in \mathcal{O}$ since $m \in \mathcal{O}^\times$. Similarly, for all $1 \leq k \leq m-1$,

$$\mathrm{Tr}(y_{m-k}\beta) = \mathrm{Tr}(b_k y_k y_{m-k}) = mf b_k/(c_{m-k}c_k)$$

and therefore $f b_k \in \mathcal{O}$. Now write

$$f\beta = e_0 + e_1 y + \ldots + e_{m-1} y_{m-1}$$

with $e_k \in \mathcal{O}$ and $e_0 \in f\mathcal{O}$. If $\mathfrak{p}_i$ is a prime factor of f and $\mathfrak{P}_i$ is a prime ideal of E above $\mathfrak{p}_i$, then

$$v_{\mathfrak{P}_i}(f\beta) \geq v_{\mathfrak{P}_i}(f) = m a_i. \tag{4.2}$$

On the other hand, since the valuations $v_{\mathfrak{P}_i}(e_k y_k)$ are all distinct (modulo m) and hence distinct, we have for each i, $1 \le i \le t$,

$$v_{\mathfrak{P}_i}(e_0 + e_1 y + \ldots + e_{m-1} y_{m-1}) = \min_{k \ge 0} v_{\mathfrak{P}_i}(e_k y_k).$$

Since $r_{ik} \le m-1$, it follows from (4.2) that

$$v_{\mathfrak{P}_i}(e_k) \ge m a_i - r_{ik} > m(a_i - 1).$$

But since $v_{\mathfrak{P}_i}(e_k) \equiv 0 \pmod m$, we see that $v_{\mathfrak{P}_i}(e_k) \ge m a_i$, and conclude that $f \mid e_k$ for all k. This implies that $b_k \in \mathcal{O}$ for all k and proves the statement. ∎

As a consequence we have the following:

COROLLARY 4.2. *With the same notations as in Theorem* 4.1, *let*

$$r = 4\left(g_E + m\varphi(m) + 14m \frac{\log(g_E + m\varphi(m))}{\log q} \right).$$

Then

$$e(\mathcal{O}_E) > \frac{g_E \log q}{(m-1)\log r}.$$

Proof. We first note that a prime ideal splits completely in E if and only if it splits completely in the Galois closure $\overline{E}$ of E.

In this case, if L is the algebraic closure of $\mathbb{F}_q$ in $\overline{E}$, then

$$[L : \mathbb{F}_q] \le \varphi(m) \quad \text{and} \quad m = [E : F] = [\overline{E} : F],$$

since $\overline{E} = EL$. Thus the genus of $\overline{E}$ equals g_E.

If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$ with least norm that splits completely in E then by Corollary 2.2, we have $N(\mathfrak{p}) \le r^2$. Hence if $\mathfrak{P}$ is a prime of E above $\mathfrak{p}$, we see as in the proof of Theorem 2.3 that $\mathfrak{P}^{e(\mathcal{O}_E)}$ is a principal ideal α and finally that

$$e(\mathcal{O}_E) \ge \frac{\log N_{E/F}(\alpha)}{\log N(\mathfrak{p})} \ge \frac{(2g_E/(m-1))\log q}{2\log r}. \quad ∎$$

A different method allows us to calculate a similar bound as in Theorem 4.1 for another family of extensions of F which are not necessarily tame. This case was not treated in Theorems 2.3 and 4.1.

THEOREM 4.3. *Let E be an imaginary extension of F of prime degree m and genus g_E, in which ∞ is totally ramified. Then for all $\alpha \in \mathcal{O}_E \setminus \mathcal{O}$, we have*

$$\deg N_{E/F}(\alpha) \ge \frac{2(g_E - 1)}{m-1}.$$

Proof. If $\mathfrak{D} \in \mathcal{D}(E)$ is a divisor of E, then $\mathcal{L}(\mathfrak{D})$ will denote as usual

$$\mathcal{L}(\mathfrak{D}) = \{ f \in E \mid v_{\mathfrak{P}}(f) \ge -v_{\mathfrak{P}}(\mathfrak{D}) \text{ for all prime } \mathfrak{P} \in \mathcal{D}(E) \}$$

and we let $l(\mathfrak{D}) = \dim_{\mathbb{F}_q}(L(\mathfrak{D}))$. Note that for any n,

$$l(n\mathfrak{P}_\infty) - l((n-1)\mathfrak{P}_\infty) \leq \deg \mathfrak{P}_\infty = 1.$$

Consider the *Weierstrass semigroup* of $\mathfrak{P}_\infty$ defined by

$$\mathcal{W} = \{n \in \mathbb{N} \mid \exists \alpha \in E, \text{ with } v_{\mathfrak{P}_\infty}(\alpha) = -n, \text{ and } v_{\mathfrak{P}}(\alpha) \geq 0 \text{ for } \mathfrak{P} \neq \mathfrak{P}_\infty\}.$$

We have $0 \in \mathcal{W}$ as $1 \in E$, and since by the Riemann–Roch Theorem,

$$l(n\mathfrak{P}_\infty) = n - g_E + 1 \quad \text{for } n \geq 2g_E - 1, \tag{4.3}$$

it follows that $2g_E, 2g_E + 1, \ldots \in \mathcal{W}$. Since $v_{\mathfrak{P}_\infty}(x^k) = -km$, we see that $0, m, 2m, \ldots \in \mathcal{W}$. If we let $\mathcal{H} = \mathcal{W} \cap \{0, 1, \ldots, 2g_E - 1\}$, then $|\mathcal{H}| = g_E$ as $l((2g_E - 1)\mathfrak{P}_\infty) = g_E$ by (4.3).

Let a be minimal with respect to the property that $\mathcal{L}(a\mathfrak{P}_\infty)$ contains an element $\alpha \notin F$. Then a cannot be a multiple of m since if it were km, then both α and x^k would be elements of $\mathcal{L}(a\mathfrak{P}_\infty) \setminus \mathcal{L}((a-1)\mathfrak{P}_\infty)$ and since $l(a\mathfrak{P}_\infty) - l((a-1)\mathfrak{P}_\infty) \leq 1$, this implies that $\{\alpha, x^k, x^{k-1}, \ldots, x, 1\}$ are linearly dependent over $\mathbb{F}_q$ and so $\alpha \in F$.

Hence since m is prime, $(a, m) = 1$. If we let, for $0 \leq j \leq m-1$,

$$\mathcal{W}_j = \left\{ ja + km \,\middle|\, 0 \leq k \leq \frac{2g_E - 1 - ja}{m} \right\},$$

then the elements of $\bigcup_{j=0}^{m-1} \mathcal{W}_j$ are distinct and all lie in $\mathcal{H}$. But then

$$\left| \bigcup_{j=0}^{m-1} \mathcal{W}_j \right| \geq \sum_{j=0}^{m-1} \frac{2g_E - 1 - ja}{m} = (2g_E - 1) - a\frac{m-1}{2}. \tag{4.4}$$

Since $|\mathcal{H}| = g_E$, (4.4) implies that

$$a \geq \frac{2(g_E - 1)}{m - 1}$$

and the assertion follows. ∎

We let $\overline{m}$ and $\overline{n}$ denote the dimension of the Galois closure $\overline{E}$ of E over F and the dimension over $\mathbb{F}_q$ of the algebraic closure of $\mathbb{F}_q$ in $\overline{E}$ respectively.

In the case where $\overline{E}$ is a tamely ramified extension of F, then E is a tamely ramified extension of F and the genus of $\overline{E}$ can be related to the genus of E:

LEMMA 4.4. *If $\overline{E}$ is a tamely ramified extension of F, then*

$$2g_{\overline{E}} - 2 \leq 2\overline{m}\left(\frac{2g_E - 2}{m} + 1\right).$$

Proof. By the Riemann–Hurwitz formula we have that

$$2g_{\overline{E}} - 2 = -2\overline{m} + \sum_{\overline{\mathfrak{P}}} v_{\overline{\mathfrak{P}}}(\mathfrak{D}(E/F)),$$

where the sum is over all primes that ramify in $\overline{E}/F$, including ∞, and $\mathfrak{D}(E/F)$ is the ramification divisor. Since $\overline{E}$ over F is tamely ramified, if $\mathfrak{p}$ is a prime of F such that $\overline{\mathfrak{P}}$ divides $\mathfrak{p}$, then

$$v_{\bar{\mathfrak{P}}}(\mathfrak{D}(E/F)) = (e(\overline{\mathfrak{P}}/\mathfrak{p}) - 1)\deg(\overline{\mathfrak{P}}/\mathfrak{p}) \leq e(\overline{\mathfrak{P}}/\mathfrak{p})f(\overline{\mathfrak{P}}/\mathfrak{p}). \tag{4.5}$$

Let $\mathfrak{P}$ be a prime of E dividing $\mathfrak{p}$. Then the right hand side of (4.5) equals

$$e(\overline{\mathfrak{P}}/\mathfrak{P})f(\overline{\mathfrak{P}}/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}).$$

Now note that $\mathfrak{p}$ is ramified in $\overline{E}$ if and only if it ramifies in E, and therefore

$$\begin{aligned}\sum_{\bar{\mathfrak{P}}} v_{\bar{\mathfrak{P}}}(\mathfrak{D}(E/F)) &\leq \sum_{\mathfrak{P}} e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})\Big(\sum_{\bar{\mathfrak{P}}|\mathfrak{P}} e(\overline{\mathfrak{P}}/\mathfrak{P})f(\overline{\mathfrak{P}}/\mathfrak{P})\Big) \\ &= \frac{\overline{m}}{m}\sum_{\mathfrak{P}} e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) \\ &\leq 2\frac{\overline{m}}{m}\sum_{\mathfrak{P}}(e(\mathfrak{P}/\mathfrak{p}) - 1)\deg(\mathfrak{P}/\mathfrak{p}).\end{aligned} \tag{4.6}$$

Finally, using the Riemann–Hurwitz formula for the extension E/F we conclude that the right hand side of (4.6) equals

$$\frac{2\overline{m}}{m}(2g_E - 2 + 2m)$$

and the result follows. ∎

COROLLARY 4.5. *With the same notations as in Theorem* 4.3, *let*

$$r = 4\left(g_{\bar{E}} + \overline{m}\overline{n} + \overline{m}\frac{14\log(g_{\bar{E}} + \overline{m}\overline{n})}{\log q}\right).$$

Then

$$e(\mathcal{O}_E) \geq \frac{(g_E - 1)\log q}{(m-1)\log r}.$$

In particular, if $\overline{E}$ *is tamely ramified over* F, *then*

$$e(\mathcal{O}_E) \geq \frac{(g_E - 1)\log q}{(m-1)\log(120\overline{m}^2(g_E/m + \overline{n}))}. \quad ∎$$

Vijaya Kumar Murty and John Scherk [3] have recently proven a new version of the Chebotarev Density Theorem for function fields. Their result gives a slightly better bound for the least norm of a prime that splits completely in a function field Galois extension. The same argument of Theorem 2.3 and Corollary 4.2 applies.

Acknowledgments. The authors would like to thank Chantal David and Kumar Murty for some useful discussions. The second author would like to thank CICMA for the hospitality and support during the preparation of this paper.

References

[1] D. W. Boyd and H. Kisilevsky, *On the exponent of the ideal class groups of complex quadratic fields*, Proc. Amer. Math. Soc. 31 (1972), 433–436.

[2] M. D. Fried and M. Jarden, *Field Arithmetic*, Springer, 1986.

[3] V. K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields*, C. R. Acad. Sci. Paris Sér. I 319 (1994), 523–528.

[4] F. Pappalardi, *On the exponent of the ideal class group of* $\mathbb{Q}(\sqrt{-d})$, Proc. Amer. Math. Soc., to appear.

DEPARTMENT OF MATHEMATICS
AND STATISTICS AND CICMA
CONCORDIA UNIVERSITY
1455 DE MAISONNEUVE BLVD. WEST
MONTRÉAL, QUÉBEC
H3G 1M8, CANADA
E-mail: KISILEV@ABACUS.CONCORDIA.CA

DIPARTIMENTO DI MATEMATICA
TERZA UNIVERSITÀ DEGLI STUDI DI ROMA
VIA C. SEGRE, 2/6
00146 ROMA, ITALY
E-mail: PAPPA@MATRM3.MAT.UNIROMA3.IT

Received on 19.4.1994
and in revised form on 12.12.1994 (2601)