ACTA ARITHMETICA
LX.1 (1991)

On p-class groups of cyclic extensions of prime degree p of number fields

by

Frank Gerth III (Austin, Tex.)

1. Introduction. Let $\boldsymbol{Q}$ denote the field of rational numbers, and let F be a finite extension field of $\boldsymbol{Q}$. Let p be an odd prime number which does not divide the class number of F and for which $\zeta_p \notin F$, where ζ_p is a primitive pth root of unity. (Of course all but finitely many primes p satisfy these conditions for a given field F.) If I is a nonzero ideal in the ring of integers $\mathcal{O}_F$, let $N(I)$ denote the absolute norm of I. Equivalently, $N(I) = [\mathcal{O}_F : I]$. Let K be a cyclic extension of F of degree p, and let σ be a generator of $\mathrm{Gal}(K/F)$. Let C_K denote the p-class group of K (i.e., the Sylow p-subgroup of the ideal class group of K), and let $C_K^{(1-\sigma)^i} = \{a^{(1-\sigma)^i} : a \in C_K\}$ for $i = 1, 2, \ldots$ Since we have assumed p does not divide the class number of F, then it is easy to see that $C_K/C_K^{1-\sigma}$ is an elementary abelian p-group (which we may view as a vector space over the finite field $\boldsymbol{F}_p$), and

$$\dim_{\mathcal{F}_p}(C_K/C_K^{1-\sigma}) = t - 1 - \beta \tag{1.1}$$

where t is the number of primes that ramify in K/F, and

$$p^\beta = [E_F : (E_F \cap N_{K/F}K^*)] \tag{1.2}$$

(cf. [3]). Here E_F is the group of units of F, and $N_{K/F}$ is the norm map from K^* to F^*.

Since the structure of $C_K/C_K^{1-\sigma}$ is known, we focus our attention on $C_K^{1-\sigma}$. We let

$$r_K = \dim_{\mathcal{F}_p}(C_K^{1-\sigma}/C_K^{(1-\sigma)^2}) . \tag{1.3}$$

Equivalently r_K is the minimal number of generators of $C_K^{1-\sigma}$ as a module over $\mathrm{Gal}(K/F)$. We let $D_{K/F}$ denote the relative discriminant of K/F. For each positive integer t, each nonnegative integer i, and each positive real number x, we define

(1.4) $$A_t = \{\text{cyclic extensions } K \text{ of } F \text{ of degree } p \text{ with exactly } t \text{ primes of } F \text{ ramified in } K/F\},$$

(1.5) $$A_{t;x} = \{K \in A_t : N(D_{K/F}) \le x^{p-1}\},$$

(1.6) $$A_{t,i;x} = \{K \in A_{t;x} : r_K = i\},$$

(1.7) $$d_{t,i} = \lim_{x\to\infty} \frac{|A_{t,i;x}|}{|A_{t;x}|},$$

(1.8) $$d_{\infty,i} = \lim_{t\to\infty} d_{t,i}.$$

Here $|S|$ denotes the cardinality of a set S. Our goal is to prove the following theorem.

THEOREM 1. *Let F be a finite extension of $\boldsymbol{Q}$. Let p be an odd prime number which does not divide the class number of F and for which $\zeta_p \notin F$, where ζ_p is a primitive p-th root of unity. For each cyclic extension K of F of degree p, let $N(D_{K/F})$ denote the absolute norm of the relative discriminant of K/F. Let C_K denote the p-class group of K; let σ be a generator of* Gal(K/F); *and let r_K denote the minimal number of generators of $C_K^{1-\sigma}$ as a module over* Gal(K/F). *Let u denote the rank of the group of units of F. Finally let $d_{\infty,i}$ be the density defined by equation* (1.8). (*Also see equations* (1.4) *through* (1.7).) *Then*

$$d_{\infty,i} = \frac{p^{-i(i+u+1)}\prod_{k=1}^{\infty}(1-p^{-k})}{[\prod_{k=1}^{i}(1-p^{-k})][\prod_{k=1}^{i+u+1}(1-p^{-k})]} \quad \textit{for } i = 0,1,2,\ldots$$

Remark. Certain special cases of Theorem 1 have been proved in other papers; namely, the case where $F = \boldsymbol{Q}$ (see [5]) and the case where F is a quadratic extension of $\boldsymbol{Q}$ (see [7]). For some partial results when $\zeta_p \in F$, see [6] and [8].

Remark. As $p \to \infty$, $d_{\infty,0} \to 1$ and $d_{\infty,i} \to 0$ for $i \ge 1$. So $C_K^{1-\sigma}$ is very likely to be trivial for large p. Also $C_K^{1-\sigma}$ is very likely to be trivial if u is large. For numerical values of $d_{\infty,i}$ when $u = 0$ or 1, $p = 3, 5, 7$, or 11, and $i = 0, 1, 2, 3$, or 4, see the appendix of [7].

2. Proof of Theorem 1. We let notation be the same as in the previous section. Since Theorem 1 has already been proved when $F = \boldsymbol{Q}$ and when F is a quadratic extension of $\boldsymbol{Q}$, we may assume $[F : \boldsymbol{Q}] \ge 3$, and hence the group of units E_F of F is an infinite group. We let $\varepsilon_1, \ldots, \varepsilon_u$ be a system of fundamental units of F. Our method of proof is a generalization of the method used when F is a real quadratic extension of $\boldsymbol{Q}$ (see [7], Section 3). For a cyclic extension K of F of degree p, we let t denote the number of primes of F that ramify in K. Then $N(D_{K/F}) = p^a N(\mathfrak{p}_1 \ldots \mathfrak{p}_s)^{p-1}$, where

$a \geq 0$; $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are distinct primes of F with $N(\mathfrak{p}_i) \equiv 1 \pmod p$ for $1 \leq i \leq s$; and $s \leq t$. Furthermore $s = t$ precisely when $a = 0$. When calculating $d_{t,i}$ in equation (1.7), we may omit the fields where $a > 0$ since when $s < t$,

$$|\{p^a N(\mathfrak{p}_1 \ldots \mathfrak{p}_s)^{p-1} \leq x^{p-1}\}| = o(|\{N(\mathfrak{p}_1 \ldots \mathfrak{p}_t)^{p-1} \leq x^{p-1}\}|) \quad \text{as } x \to \infty.$$

So we may assume

$$N(D_{K/F}) = N(\mathfrak{p}_1 \ldots \mathfrak{p}_t)^{p-1} \quad \text{with } N(\mathfrak{p}_i) \equiv 1 \pmod p \quad \text{for } 1 \leq i \leq t.$$

Now we let $\mathfrak{q}_1, \ldots, \mathfrak{q}_u$ be primes of F satisfying the following conditions:

(i) $N(\mathfrak{q}_i) \equiv 1 \pmod p$ for $1 \leq i \leq u$;
(ii) ε_j is a pth power residue (mod $\mathfrak{q}_i$) for all $j \neq i$;
(iii) ε_i is a pth power nonresidue (mod $\mathfrak{q}_i$) for $1 \leq i \leq u$.

(Remark. To find such a prime $\mathfrak{q}_i$, we can proceed as follows. Let

$$F_i = F(\zeta_p, \sqrt[p]{\varepsilon_1}, \ldots, \sqrt[p]{\varepsilon_{i-1}}, \sqrt[p]{\varepsilon_{i+1}}, \ldots, \sqrt[p]{\varepsilon_u}).$$

Then $\mathfrak{q}_i$ is a prime of F which splits completely in F_i/F but for which a prime in F_i above $\mathfrak{q}_i$ is inert in $F_i(\sqrt[p]{\varepsilon_i})/F_i$.) The primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_u$ shall be fixed throughout this paper, and since

$$|\{N(\mathfrak{q}_1 \ldots \mathfrak{q}_u)^{p-1} N(\mathfrak{p}_1 \ldots \mathfrak{p}_s)^{p-1} \leq x^{p-1}\}| = o(|\{N(\mathfrak{p}_1 \ldots \mathfrak{p}_t)^{p-1} \leq x^{p-1}\}|) \quad \text{as } x \to \infty$$

if $s < t$, we may assume $\mathfrak{p}_i \neq \mathfrak{q}_j$ for all i and j.

Next we define groups G_i for $1 \leq i \leq t$ by

$$G_i = (\mathcal{O}_F/\mathfrak{p}_i \mathfrak{q}_1 \ldots \mathfrak{q}_u)^\times / (E_F/E_F') \tag{2.1}$$

where $\mathcal{O}_F$ is the ring of integers of F, and $E_F' = \{\varepsilon \in E_F : \varepsilon \equiv 1 \pmod{\mathfrak{p}_i \mathfrak{q}_1 \ldots \mathfrak{q}_u}\}$. Because of the way we have chosen $\mathfrak{q}_1, \ldots, \mathfrak{q}_u$, there is a unique cyclic extension K_i of F of degree p whose Galois group is isomorphic to a quotient group of G_i such that $\mathfrak{p}_i$ ramifies in K_i/F, but no other primes ramify in K_i/F except perhaps $\mathfrak{q}_1, \ldots, \mathfrak{q}_u$. (Remark. $\mathfrak{p}_i$ will be the only prime ramifying in K_i/F when ε_j is a pth power residue (mod $\mathfrak{p}_i$) for $1 \leq j \leq u$.) We let $F' = F(\zeta_p)$ and $L_i = K_i \cdot F'$ for $1 \leq i \leq t$. Since L_i/F' is a Kummer extension, there exists $\mu_i \in F'$ such that $L_i = F'(\sqrt[p]{\mu_i})$. Let $\mathfrak{P}_i$ be a prime of F' above $\mathfrak{p}_i$. By replacing μ_i by a suitable power of μ_i, we may assume that the power of $\mathfrak{P}_i$ dividing μ_i is $\mathfrak{P}_i^{b_i}$ with $b_i \equiv 1 \pmod p$. Now let $L = K \cdot F'$. Then $L = F'(\sqrt[p]{\mu})$ with

$$\mu = \mu_1^{a_1} \ldots \mu_t^{a_t} \tag{2.2}$$

for some integers a_i with $1 \leq a_i \leq p-1$ for $1 \leq i \leq t$.

Next we let h denote the class number of F. Since $p \nmid h$ by assumption, there exists a positive integer h' such that $hh' \equiv 1 \pmod p$. We let $\pi_j' \in \mathcal{O}_F$

satisfy

$$\mathfrak{p}_j^{hh'} = \pi'_j \mathcal{O}_F \tag{2.3}$$

for $1 \le j \le t$. Now recall that ε_i is a pth power nonresidue (mod $\mathfrak{q}_i$). So there exists an integer c_{ij} with $0 \le c_{ij} \le p-1$ such that $\varepsilon_i^{c_{ij}} \pi'_j$ is a pth power residue (mod $\mathfrak{q}_i$). Let

$$\pi_j = \varepsilon_1^{c_{1j}} \ldots \varepsilon_u^{c_{uj}} \pi'_j \tag{2.4}$$

for $1 \le j \le t$. Since ε_k is a pth power residue (mod $\mathfrak{q}_i$) for $k \ne i$, then π_j is a pth power residue (mod $\mathfrak{q}_i$) for $1 \le i \le u$ and $1 \le j \le t$. Also π_j is a generator of the ideal $\mathfrak{p}_j^{hh'}$ for $1 \le j \le t$.

Now we let M_K be the $t \times (u+t)$ matrix over $\boldsymbol{F}_p$ defined as follows:

$$M_K = [m_{ij}], \quad m_{ij} \in \boldsymbol{F}_p, \quad 1 \le i \le t,\ 1 \le j \le u+t, \tag{2.5}$$

$$\zeta_p^{m_{ij}} = \begin{cases} \left(\dfrac{\varepsilon_j, \mu}{\mathfrak{P}_i}\right) & \text{for } 1 \le i \le t \text{ and } 1 \le j \le u, \\ \left(\dfrac{\pi_{j-u}, \mu}{\mathfrak{P}_i}\right) & \text{for } 1 \le i \le t \text{ and } u+1 \le j \le u+t. \end{cases} \tag{2.6}$$

The Hilbert symbol $(\frac{\alpha,\mu}{\mathfrak{P}_i}) \in \langle \zeta_p \rangle$ is defined by

$$\left(\frac{\alpha, L/F'}{\mathfrak{P}_i}\right) \sqrt[p]{\mu} = \left(\frac{\alpha, \mu}{\mathfrak{P}_i}\right) \sqrt[p]{\mu}$$

where α is a nonzero element of F', and $\left(\frac{\alpha, L/F'}{\mathfrak{P}_i}\right)$ is the norm residue symbol. We note that the product formula for Hilbert symbols implies that the sum of the entries in each column of M_K is zero. Our matrix M_K is a generalization of the matrix M_K on p. 96 in [7] that was used in the case where F is a real quadratic fields. As in [7], the matrix M_K provides information about $\dim_{\mathcal{F}_p}(C_K/C_K^{1-\sigma})$ and $\dim_{\mathcal{F}_p}(C_K^{1-\sigma}/C_K^{(1-\sigma)^2})$. More precisely

$$\dim_{\mathcal{F}_p}(C_K/C_K^{1-\sigma}) = t - 1 - \operatorname{rank} M_0 \tag{2.7}$$

where M_0 is the $t \times u$ matrix consisting of the first u columns of M_K, and

$$r_K = \dim_{\mathcal{F}_p}(C_K^{1-\sigma}/C_K^{(1-\sigma)^2}) = t - 1 - \operatorname{rank} M_K - \omega \tag{2.8}$$

where $0 \le \omega \le u$. Also $\omega = 0$ when $\operatorname{rank} M_0 = u$. As $t \to \infty$, the probability approaches 1 that $\operatorname{rank} M_0 = u$. So the error introduced by disregarding ω disappears when we calculate the limit in equation (1.8).

Now from properties of Hilbert symbols (cf. [1, Chapter 12] or [2, pp. 348–354]),

$$\left(\frac{\varepsilon_j, \mu}{\mathfrak{P}_i}\right) = \left(\frac{\varepsilon_j, \mu_i^{a_i}}{\mathfrak{P}_i}\right) = \left(\frac{\mu_i, \varepsilon_j}{\mathfrak{P}_i}\right)^{-a_i} = \left(\frac{\varepsilon_j}{\mathfrak{P}_i}\right)^{-a_i} \tag{2.9}$$

for $1 \le i \le t$ and $1 \le j \le u$. Here $\left(\frac{\varepsilon_j}{\mathfrak{P}_i}\right) \in \langle \zeta_p \rangle$ is the pth power residue symbol defined by

$$\left(\frac{F'(\sqrt[p]{\varepsilon_j})/F'}{\mathfrak{P}_i}\right) \sqrt[p]{\varepsilon_j} = \left(\frac{\varepsilon_j}{\mathfrak{P}_i}\right) \sqrt[p]{\varepsilon_j}, \quad \text{and} \quad \left(\frac{F'(\sqrt[p]{\varepsilon_j})/F'}{\mathfrak{P}_i}\right)$$

is the Artin symbol. Similarly

$$\left(\frac{\pi_{j-u}, \mu}{\mathfrak{P}_i}\right) = \left(\frac{\pi_{j-u}, \mu_i^{a_i}}{\mathfrak{P}_i}\right) = \left(\frac{\mu_i, \pi_{j-u}}{\mathfrak{P}_i}\right)^{-a_i} = \left(\frac{\pi_{j-u}}{\mathfrak{P}_i}\right)^{-a_i} \tag{2.10}$$

for $1 \le i \le t$, $u+1 \le j \le u+t$, and $i \ne j-u$. Alternatively for $i \ne j-u$ we can start with

$$\left(\frac{\pi_{j-u}, \mu}{\mathfrak{P}_i}\right) = \left(\frac{\pi_{j-u}, \mu_i^{a_i}}{\mathfrak{P}_i}\right) = \left(\frac{\pi_{j-u}, \mu_i}{\mathfrak{P}_i}\right)^{a_i}. \tag{2.11}$$

We note that the product formula $\prod_{\mathfrak{P}} \left(\frac{\pi_{j-u}, \mu_i}{\mathfrak{P}}\right) = 1$ over all primes $\mathfrak{P}$ of F' reduces to

$$\left(\frac{\pi_{j-u}, \mu_i}{\mathfrak{P}_i}\right)^d \left(\frac{\pi_{j-u}, \mu_i}{\mathfrak{P}_{j-u}}\right)^d \left(\frac{\pi_{j-u}, \mu_i}{\mathfrak{Q}_1}\right)^d \cdots \left(\frac{\pi_{j-u}, \mu_i}{\mathfrak{Q}_u}\right)^d = 1 \tag{2.12}$$

where $\mathfrak{Q}_k$ is a prime of F' above $\mathfrak{q}_k$ for $1 \le k \le u$, and $d = [F' : F]$. However we recall that π_{j-u} was defined in equation (2.4) so that π_{j-u} is a pth power residue (mod $\mathfrak{q}_k$) for $u+1 \le j \le u+t$ and $1 \le k \le u$. Hence $\left(\frac{\pi_{j-u}, \mu_i}{\mathfrak{Q}_k}\right) = 1$ for $u+1 \le j \le u+t$ and $1 \le k \le u$. So from equation (2.12), we get

$$\left(\frac{\pi_{j-u}, \mu_i}{\mathfrak{P}_i}\right) \left(\frac{\pi_{j-u}, \mu_i}{\mathfrak{P}_{j-u}}\right) = 1. \tag{2.13}$$

Then from equations (2.11) and (2.13), we get

$$\left(\frac{\pi_{j-u}, \mu}{\mathfrak{P}_i}\right) = \left(\frac{\pi_{j-u}, \mu_i}{\mathfrak{P}_i}\right)^{a_i} = \left(\frac{\pi_{j-u}, \mu_i}{\mathfrak{P}_{j-u}}\right)^{-a_i} = \left(\frac{\mu_i}{\mathfrak{P}_{j-u}}\right)^{-a_i} \tag{2.14}$$

for $1 \le i \le t$, $u+1 \le j \le u+t$, and $i \ne j-u$.

We now define characters λ_i and ν_j as follows

$$\lambda_i(I) = \left(\frac{\mu_i}{I}\right)^{-1}, \quad 1 \le i \le t \tag{2.15}$$

for ideals I of F' relatively prime to $\mathfrak{p}_i \mathfrak{q}_1 \ldots \mathfrak{q}_u \mathcal{O}_{F'}$;

$$\nu_j(I) = \left(\frac{\varepsilon_j}{I}\right)^{-1}, \quad 1 \le j \le u \tag{2.16}$$

for ideals I of F' relatively prime to $p\mathcal{O}_{F'}$; and

$$\nu_j(I) = \left(\frac{\pi_{j-u}}{I}\right)^{-1}, \quad u+1 \le j \le u+t \tag{2.17}$$

for ideals I of F' relatively prime to $p\mathfrak{p}_{j-u}\mathcal{O}_{F'}$. Then from equations (2.6), (2.9), (2.10), and (2.14) through (2.17), we get

$$\zeta_p^{m_{ij}} = \begin{cases} (\nu_j(\mathfrak{P}_i))^{a_i} & \text{for } 1 \le i \le t \text{ and } 1 \le j \le u, \\ (\nu_j(\mathfrak{P}_i))^{a_i} & \text{for } j-u < i \le t \text{ and } u+1 \le j \le u+t-1, \\ (\lambda_i(\mathfrak{P}_{j-u}))^{a_i} & \text{for } 1 \le i \le t-1 \text{ and } u+i < j \le u+t. \end{cases} \tag{2.18}$$

Also

$$m_{(j-u)j} = -\sum_{\substack{k=1\\k\ne j-u}}^{t} m_{kj} \quad \text{for } u+1 \le j \le u+t \tag{2.19}$$

since the sum of the entries in each column of M_K is zero. We let a_i' be the integer with $1 \le a_i' \le p-1$ such that

$$a_i a_i' \equiv 1 \pmod p \quad \text{for } 1 \le i \le t. \tag{2.20}$$

By multiplying the ith row of M_K by a_i' for each i, we get a new matrix M_K' defined as follows.

$$M_K' = [m_{ij}'], \quad m_{ij}' \in \boldsymbol{F}_p, \quad 1 \le i \le t, \quad 1 \le j \le u+t, \tag{2.21}$$

with

$$\zeta_p^{m_{ij}'} = \begin{cases} \nu_j(\mathfrak{P}_i) & \text{for } 1 \le i \le t \text{ and } 1 \le j \le u, \\ \nu_j(\mathfrak{P}_i) & \text{for } j-u < i \le t \text{ and } u+1 \le j \le u+t-1, \\ \lambda_i(\mathfrak{P}_{j-u}) & \text{for } 1 \le i \le t-1 \text{ and } u+i < j \le u+t \end{cases} \tag{2.22}$$

and

$$m_{(j-u)j}' = -a_{j-u}' \sum_{\substack{k=1\\k\ne j-u}}^{t} a_k m_{kj}' \quad \text{for } u+1 \le j \le u+t.$$

Furthermore

$$\operatorname{rank} M_K' = \operatorname{rank} M_K. \tag{2.23}$$

We observe that $m_{(j-u)j}'$ is known if we know $a_1, \ldots, a_t$ and the values of m_{kj}' for $1 \le k \le t$ and $k \ne j-u$. Also m_{tj}' is known if we know $a_1, \ldots, a_t$ and the values m_{kj}' for $1 \le k \le t-1$; that is:

$$m_{tj}' = -a_t' \sum_{k=1}^{t-1} a_k m_{kj}' \quad \text{for } 1 \le j \le u+t. \tag{2.24}$$

Equations (2.21) through (2.24) are the analogs of equations (3.15) through (3.18) in [7]. (Remark. Because of the way we defined π_j in equation (2.4), $\theta_i(\mathfrak{P}_j)$ can be omitted from equation (3.16) in [7].)

The procedure now is very similar to the procedure used on pp. 99–101 in [7]. Hence we refer the reader to pp. 99–101 in [7] for the details. However we shall mention a few modifications. The matrix Γ will now be a $t\times(u+t)$ matrix with entries in $\boldsymbol{F}_p$ whose first $t-1$ rows are arbitrary and whose last row has entries determined by an equation analogous to equation (2.24). The quantities $\delta_0(\mathfrak{P}_i)$ and $\delta(\mathfrak{P}_i,\mathfrak{P}_j)$ will be replaced by

$$\delta_j(\mathfrak{P}_i)=\begin{cases}1 & \text{if } \nu_j(\mathfrak{P}_i)=\zeta_p^{\gamma_{ij}},\\ 0 & \text{otherwise,}\end{cases}\qquad \text{for } 1\le i\le t,\ 1\le j\le u;$$

$$\delta(\mathfrak{P}_i,\mathfrak{P}_j)=\begin{cases}1 & \text{if } \nu_j(\mathfrak{P}_i)=\zeta_p^{\gamma_{ij}},\\ 0 & \text{otherwise,}\end{cases}\qquad \begin{array}{l}\text{for } j-u<i\le t,\\ \quad u+1\le j\le u+t-1;\end{array}$$

$$\delta(\mathfrak{P}_i,\mathfrak{P}_j)=\begin{cases}1 & \text{if } \lambda_i(\mathfrak{P}_{j-u})=\zeta_p^{\gamma_{ij}},\\ 0 & \text{otherwise,}\end{cases}\qquad \text{for } 1\le i\le t-1,\ u+i<j\le u+t.$$

The analog of equation (3.33) in [7] is then

$$d_{\infty,i}=\lim_{t\to\infty} w_{t-1,u+t,i} \tag{2.25}$$

where $w_{t-1,u+t,i}$ is the probability that a randomly chosen $(t-1)\times(u+t)$ matrix over $\boldsymbol{F}_p$ has rank equal to $t-1-i$. The formula for $d_{\infty,i}$ in Theorem 1 then follows from equation (2.25) and from Theorem 1.4 in [4].

Remark. The formula for $d_{\infty,i}$ in Theorem 1 is not valid for certain fields F that contain a primitive pth root of unity ζ_p (cf. [6] and [8]). One difference between the case where $\zeta_p\notin F$ and the case where $\zeta_p\in F$ concerns the relationship between μ_i and π_i. (For definitions of μ_i and π_i, see discussion preceding equation (2.2) and equations (2.3) and (2.4).) If we let $F'=F(\zeta_p)$ when $\zeta_p\notin F$, then $F'(\sqrt[p]{\mu_i})$ and $F'(\sqrt[p]{\pi_i})$ are disjoint extensions of F' since $F'(\sqrt[p]{\mu_i})$ is an abelian extension of F, but $F'(\sqrt[p]{\pi_i})$ is not an abelian extension of F. However if $\zeta_p\in F$, then it could happen that $\mu_i=\pi_i$. For example, if $p=3$ and $F=\boldsymbol{Q}(\zeta_3)$, then μ_i and π_i can be chosen so that $\mu_i=\pi_i$ if (π_i) is a prime ideal with $N((\pi_i))\equiv 1 \pmod 9$.

References

[1] E. Artin and J. Tate, *Class Field Theory*, Benjamin, New York 1967.

[2] J. Cassels and A. Fröhlich, *Algebraic Number Theory*, Thompson, Washington, D.C., 1967.

[3] Y. Furuta, *The genus field and genus number in algebraic number fields*, Nagoya Math. J. 29 (1967), 281–285.

[4] F. Gerth, *Limit probabilities for coranks of matrices over* GF(q), Linear and Multilinear Algebra 19 (1986), 79–93.

[5] —, *Densities for ranks of certain parts of p-class groups*, Proc. Amer. Math. Soc. 99 (1987), 1–8.

[6] —, *Densities for* 3*-class ranks in certain cubic extensions*, J. Reine Angew. Math. 381 (1987), 161–180.

[7] F. Gerth, *On p-class groups of cyclic extensions of prime degree p of quadratic fields*, Mathematika 36 (1989), 89–102.

[8] —, *On p-class groups of cyclic extension of prime degree p of certain cyclotomic fields*, Manuscripta Math. 70 (1990), 39–50.

DEPARTMENT OF MATHEMATICS
THE UNIVERSITY OF TEXAS AT AUSTIN
AUSTIN, TEXAS 78712
U.S.A.

Received on 26.11.1990 (2100)