ACTA ARITHMETICA
XLVI (1986)

Densities for 3-class ranks of pure cubic fields

by

FRANK GERTH III (Austin, Tex.)

1. Galois cubic case. Let K be a Galois cubic extension of the field of rational numbers Q such that exactly t primes ramify in K/Q. Then if D_K is the discriminant of K, we have

$$D_K = (f_K)^2 \tag{1.1}$$

where f_K is the conductor of K and satisfies

$$f_K = \begin{cases} p_1 \dots p_t & \text{with distinct primes } p_i \equiv 1 \pmod 3 \text{ if } 3 \nmid D_K, \\ 9p_1 \dots p_{t-1} & \text{with distinct primes } p_i \equiv 1 \pmod 3 \text{ if } 3 \mid D_K. \end{cases} \tag{1.2}$$

Let A_K denote the 3-class group of K; i.e., the Sylow 3-subgroup of the ideal class group of K. Then the 3-class rank of K is given by $\operatorname{rank} A_K = \operatorname{din}_{F_3}(A_K/A_K^3)$, where F_3 is the finite field with three elements, and we are viewing the elementary abelian 3-group A_K/A_K^3 as a vector space over F_3. It is known that $t-1 \leqslant \operatorname{rank} A_K \leqslant 2(t-1)$. (See [9], Satz 30.) So we may write

$$\operatorname{rank} A_K = t-1+c \quad \text{with } 0 \leqslant c \leqslant t-1. \tag{1.3}$$

We consider the following question: how likely is $\operatorname{rank} A_K = t-1$, $\operatorname{rank} A_K = t$, $\operatorname{rank} A_K = t+1$, etc.? To be more precise, we proceed as follows: for each positive integer t, each nonnegative integer $c \leqslant t-1$, and each positive real number x, we let

$$S'_{t;x} = \{\text{Galois cubic extensions } K \text{ of } Q \text{ with exactly } t \text{ ramified primes and } f_K \leqslant x\}; \tag{1.4}$$

$$S'_{t,c;x} = \{K \in S'_{t;x} \colon \operatorname{rank} A_K = t-1+c\}. \tag{1.5}$$

Then we define the density $d'_{t,c}$ by

$$d'_{t,c} = \lim_{x\to\infty} \frac{|S'_{t,c;x}|}{|S'_{t;x}|}. \tag{1.6}$$

Here $|S|$ denotes the cardinality of a set S. So $d'_{t,c}$ specifies how likely it is for $\operatorname{rank} A_K = t-1+c$. The following result is proved in [6], which depends on calculations in [5].

Proposition 1.1 (cf. [6], Proposition 3.1). *Let t be a positive integer, and let c be an integer with $0 \leqslant c \leqslant t-1$. Let $d'_{t,c}$ be defined by equation* (1.6). *Then*

$$d'_{t,c} = \left[\prod_{j=1}^{t-1-c}\left(1-\frac{1}{3^{t+1-j}}\right)\right]\cdot\frac{1}{3^{tc}}\cdot\sum_{\substack{i_1+\ldots+i_{t-1-c}\leqslant c\\ \text{each } i_s\geqslant 0}}\left[\prod_{s=1}^{t-1-c}3^{si_s}\right].$$

Corollary 1.2 (cf. [7]). *Let notations be as in Proposition* 1.1. *Then*

$$\lim_{t\to\infty} d'_{t,c} = \frac{3^{-c(c+1)}\prod\limits_{j=c+1}^{\infty}(1-3^{-j})}{\prod\limits_{j=1}^{c+1}(1-3^{-j})} \quad \textit{for} \quad c = 0, 1, 2, \ldots$$

In Table I of the appendix, we list some values of $d'_{t,c}$. We note that $c = 0$ is most likely for all t. Hence for a Galois cubic field with exactly t ramified primes, the most likely 3-class rank is $t-1$.

2. Preliminary results for pure cubic case. Our goal for the pure cubic case is to obtain results analogous to Proposition 1.1 and Corollary 1.2. Some of the techniques we shall use are very similar to the techniques we used in [5], [6], and [7] to handle the Galois cubic case, and hence sometimes we shall refer the reader to these references rather than repeat lengthy arguments that appear in the references.

Let L be a pure cubic extension of $\boldsymbol{Q}$; i.e., $L = \boldsymbol{Q}(n^{1/3})$ for some cube-free integer n. Suppose exactly t primes are totally ramified in $L/\boldsymbol{Q}$, and let D_L denote the discriminant of L. Then

$$D_L = -3(g_L)^2 \tag{2.1}$$

where g_L satisfies

$$g_L = \begin{cases} p_1 \ldots p_t & \text{with distinct primes } p_i \equiv \pm 1 \pmod 3 \\ & \text{if } n \equiv \pm 1 \pmod 9, \\ 3^e p_1 \ldots p_{t-1} & \text{with distinct primes } p_i \equiv \pm 1 \pmod 3, \\ & e = 1 \text{ or } 2, \text{ if } n \not\equiv \pm 1 \pmod 9 \end{cases} \tag{2.2}$$

(cf. [2], Section 4). Since

$$\sum_{3^e p_1 \ldots p_{t-1} \leqslant x} 1 = o\Big(\sum_{p_1 \ldots p_t \leqslant x} 1\Big),$$

it suffices to consider $g_L = p_1 \ldots p_t$ with distinct primes $p_i \equiv \pm 1 \pmod 3$ in our counting arguments. We relabel the primes as follows:

$$g_L = p_1 \ldots p_u q_{u+1} \ldots q_t \quad \text{with each } p_i \equiv 1 \pmod 3 \text{ and each } q_i \equiv -1 \pmod 3. \tag{2.3}$$

For convenience we assume $p_i < p_j$ if $i < j$, and $q_i < q_j$ if $i < j$. Of course we may have some $q_i < p_j$. We note that

$$n = p_1^{a_1} \ldots p_u^{a_u} q_{u+1}^{a_{u+1}} \ldots q_t^{a_t} \quad \text{with each } a_i = 1 \text{ or } 2. \tag{2.4}$$

If ζ is a primitive cube root of unity, then in $\boldsymbol{Q}(\zeta)$, each $p_i = \pi_i \bar{\pi}_i$, where π_i and $\bar{\pi}_i$ are prime elements in $\boldsymbol{Q}(\zeta)$ with $\bar{\pi}_i$ the complex conjugate of π_i.

Next we let A_L denote the 3-class group of L. In [3] and [4] we have specified algorithms for computing $\operatorname{rank} A_L$. In this paper we shall use the algorithm in [4], Theorem 3.6. (Remark: The t in [4] corresponds to $t+u$ in this paper.) We thus have

$$\operatorname{rank} A_L = t+u-1-\operatorname{rank} M_1, \tag{2.5}$$

where M_1 is a certain matrix of norm residue symbols. Using the notation of [4], we let $F = \boldsymbol{Q}(\zeta)$ and $K = F(n^{1/3})$. Because the extension K/F is a Kummer extension, we can replace the norm residue symbols by cubic Hilbert symbols to obtain the following matrix M_1.

$$M_1 = [m'_{ij}], \quad 1 \leqslant i \leqslant t+u-1,\ 0 \leqslant j \leqslant u,$$

where

$$m'_{ij} = \begin{cases} \left(\dfrac{x_j, n}{(\pi_{(i+1)/2})}\right) & \text{for} \quad i = 1, 3, 5, \ldots, 2u-1 \text{ and } 0 \leqslant j \leqslant u, \\ \left(\dfrac{x_j, n}{(\bar{\pi}_{i/2})}\right) & \text{for} \quad i = 2, 4, 6, \ldots, 2u \text{ and } 0 \leqslant j \leqslant u, \\ \left(\dfrac{x_j, n}{(q_{i-u})}\right) & \text{for} \quad 2u+1 \leqslant i \leqslant t+u-1 \text{ and } 0 \leqslant j \leqslant u \end{cases}$$

and

$$x_j = \begin{cases} \zeta & \text{if} \quad j = 0, \\ \pi_j \bar{\pi}_j^2 & \text{if} \quad 1 \leqslant j \leqslant u. \end{cases}$$

Each element of M_1 is ζ^0, ζ^1, or ζ^2, and we view M_1 as a matrix over $\boldsymbol{F}_3$. The cubic Hilbert symbol $\left(\dfrac{x_j, n}{(\pi_i)}\right)$, for example, is defined by

$$\left(\frac{x_j, K/F}{(\pi_i)}\right) n^{1/3} = \left(\frac{x_j, n}{(\pi_i)}\right) n^{1/3},$$

where $\left(\dfrac{x_j, K/F}{(\pi_i)}\right)$ is the norm residue symbol.

Let M_2 be the $(t+u)\times(u+1)$ matrix over $\boldsymbol{F}_3$ whose first $(t+u-1)$ rows are the same as the rows of M_1, and whose $(t+u, j)$ entry is $\left(\dfrac{x_j, n}{(q_t)}\right)$ for $0 \leqslant j \leqslant u$. The product formula for Hilbert symbols implies that the product of the entries in each column of M_2 is 1. It then follows that $\operatorname{rank} M_2 = \operatorname{rank} M_1$. Now standard properties of cubic Hilbert symbols show that

$$\left(\frac{x_j,\, n}{(\bar{\pi}_i)}\right) = \left(\frac{x_j,\, n}{(\pi_i)}\right) \quad \text{for all } j.$$

(See [8] for basic properties of Hilbert symbols.) So rows $2, 4, \ldots, 2u$ are the same as rows $1, 3, \ldots, 2u-1$, respectively. Hence we may delete rows $2, 4, \ldots, 2u$ from M_2 to obtain a new matrix M, where M is a $t \times (u+1)$ matrix over F_3 with $\operatorname{rank} M = \operatorname{rank} M_2 = \operatorname{rank} M_1$. Explicitly

(2.6) $$M = [m_{ij}], \quad 1 \leqslant i \leqslant t,\ 0 \leqslant j \leqslant u,$$

where each $m_{ij} \in W = \{\zeta^0, \zeta^1, \zeta^2\}$ is defined by

(2.7) $$m_{ij} = \begin{cases} \left(\dfrac{x_j,\, n}{(\pi_i)}\right) & \text{for} \quad 1 \leqslant i \leqslant u,\ 0 \leqslant j \leqslant u, \\ \left(\dfrac{x_j,\, n}{(q_i)}\right) & \text{for} \quad u+1 \leqslant i \leqslant t,\ 0 \leqslant j \leqslant u, \end{cases}$$

(2.8) $$x_j = \begin{cases} \zeta & \text{for} \quad j = 0, \\ \pi_j \bar{\pi}_j^2 & \text{for} \quad 1 \leqslant j \leqslant u, \end{cases}$$

and n is given by (2.4).

We let

(2.9) $$c = u + 1 - \operatorname{rank} M.$$

Then the analog of equation (1.3) is

(2.10) $$\operatorname{rank} A_L = t - 2 + c \quad \text{with} \quad 0 \leqslant c \leqslant u+1.$$

For each positive integer t, each nonnegative integer $c \leqslant t+1$, and each positive real number x, we obtain the following analogs of equations (1.4), (1.5) and (1.6):

(2.11) $S_{t;x} = \{$pure cubic extensions L of Q with exactly t totally ramified primes and $g_L \leqslant x\}$;

(2.12) $$S_{t,c;x} = \{L \in S_{t;x}\colon \operatorname{rank} A_L = t-2+c\};$$

(2.13) $$d_{t,c} = \lim_{x \to \infty} \frac{|S_{t,c;x}|}{|S_{t;x}|}.$$

Thus our goal is to determine the density $d_{t,c}$.

3. Certain asymptotic formulas for the pure cubic case. Let notations be the same as in Section 2. We can now employ techniques similar to those we used in [5], Sections 3 and 4. The following lemma is the analog of Lemma 1 in [5].

LEMMA 3.1. *Let g_L be given by equation (2.3). Then there are 2^{t-1} pure cubic extensions L of Q with the same discriminant $D_L = -3(g_L)^2$.*

Our next step is to introduce certain characters related to the Hilbert symbols (cf. [5], p. 198). If x_j is given by equation (2.8) and n is given by equation (2.4), then if $1 \leqslant i \leqslant u$, $1 \leqslant j \leqslant u$, and $i \neq j$, we have

$$\left(\frac{x_j,\, n}{(\pi_i)}\right) = \left(\frac{x_j,\, p_i^{a_i}}{(\pi_i)}\right) = \left(\frac{p_i,\, x_j}{(\pi_i)}\right)^{-a_i} = \left(\frac{x_j}{(\pi_i)}\right)^{-a_i},$$

where $\left(\frac{x_j}{(\pi_i)}\right) \in W$ is the cubic power residue symbol defined by

$$\left(\frac{F(x_j^{1/3})/F}{(\pi_i)}\right) x_j^{1/3} = \left(\frac{x_j}{(\pi_i)}\right) x_j^{1/3},$$

and $\left(\frac{F(x_j^{1/3})/F}{(\pi_i)}\right) \in \operatorname{Gal}(F(x_j^{1/3})/F)$ is the Artin symbol. Similarly

$$\left(\frac{x_j,\, n}{(q_i)}\right) = \left(\frac{x_j}{(q_i)}\right)^{-a_i}.$$

We define the characters

$$\lambda_j(I) = \left(\frac{x_j}{I}\right)^{-1}, \quad 1 \leqslant j \leqslant u,$$

for all ideals I of F relatively prime to (x_j). The conductor of λ_j is (p_j); in fact, $\lambda_j((\pi_i)) = \theta(p_i)$, where θ is a cubic Dirichlet character with conductor p_j. In the matrix M we then have

(3.1) $$\left(\frac{x_j,\, n}{(\pi_i)}\right) = \lambda_j^{a_i}((\pi_i)) \quad \text{for} \quad 1 \leqslant i \leqslant u,\ 1 \leqslant j \leqslant u,\ i \neq j,$$

and

(3.2) $$\left(\frac{x_j,\, n}{(q_i)}\right) = \lambda_j^{a_i}((q_i)) \quad \text{for} \quad u+1 \leqslant i \leqslant t,\ 1 \leqslant j \leqslant u.$$

Next we note that for $1 \leqslant i \leqslant u$, $1 \leqslant j \leqslant u$, and $i \neq j$, we have

$$\left(\frac{x_j,\, n}{(\pi_i)}\right) = \left(\frac{x_j,\, p_i^{a_i}}{(\pi_i)}\right) = \left(\frac{p_i,\, x_j}{(\pi_i)}\right)^{-a_i} = \left(\frac{x_j,\, p_i}{(\pi_j)}\right)^{-a_i} = \left(\frac{p_i}{(\pi_j)}\right)^{-a_i}$$

where $\left(\frac{p_i}{(\pi_j)}\right) \in W$ is the cubic power residue symbol defined by

$$\left(\frac{F(p_i^{1/3})/F}{(\pi_j)}\right) p_i^{1/3} = \left(\frac{p_i}{(\pi_j)}\right) p_i^{1/3},$$

where $\left(\frac{F(p_i^{1/3})/F}{(\pi_j)}\right) \in \mathrm{Gal}\left(F(p_i^{1/3})/F\right)$ is the Artin symbol. Similarly

$$\left(\frac{x_j,\, n}{(q_i)}\right) = \left(\frac{q_i}{(\pi_j)}\right)^{a_i}.$$

We define the characters

$$\omega_i(I) = \left(\frac{p_i}{I}\right)^{-1}, \quad 1 \leqslant i \leqslant u,$$

for all ideals I of F relatively prime to $(p_i(1-\zeta))$. The conductor of the character ω_i is $(p_i(1-\zeta)^{l_i})$ for some integer l_i with $0 \leqslant l_i \leqslant 3$ (cf. [1], p. 91). Similarly we define the characters

$$\omega_i(I) = \left(\frac{q_i}{I}\right), \quad u+1 \leqslant i \leqslant t,$$

for all ideals I of F relatively prime to $(q_i(1-\zeta))$. The conductor of this ω_i is $(q_i(1-\zeta)^{l_i})$ for some integer l_i with $0 \leqslant l_i \leqslant 3$. In the matrix M we then have

$$\text{(3.3)} \qquad \left(\frac{x_j,\, n}{(\pi_i)}\right) = \omega_i^{a_i}((\pi_j)) \quad \text{for} \quad 1 \leqslant i \leqslant u,\ 1 \leqslant j \leqslant u,\ i \neq j,$$

and

$$\text{(3.4)} \qquad \left(\frac{x_j,\, n}{(q_i)}\right) = \omega_i^{a_i}((\pi_j)) \quad \text{for} \quad u+1 \leqslant i \leqslant t,\ 1 \leqslant j \leqslant u.$$

For $j = 0$, we have

$$\left(\frac{x_0,\, n}{(\pi_i)}\right) = \left(\frac{\zeta,\, p_i^{a_i}}{(\pi_i)}\right) = \left(\frac{p_i,\, \zeta}{(\pi_i)}\right)^{-a_i} = \left(\frac{\zeta}{(\pi_i)}\right)^{-a_i}.$$

Similarly $\left(\frac{x_0,\, n}{(q_i)}\right) = \left(\frac{\zeta}{(q_i)}\right)^{-a_i}$. We define the character λ_0 with conductor $(1-\zeta)^3$ by $\lambda_0(I) = \left(\frac{\zeta}{I}\right)^{-1}$ for all ideals I relatively prime to $(1-\zeta)$. So

$$\text{(3.5)} \qquad \left(\frac{x_0,\, n}{(\pi_i)}\right) = \lambda_0^{a_i}((\pi_i)) \quad \text{for} \quad 1 \leqslant i \leqslant u;$$

$$\text{(3.6)} \qquad \left(\frac{x_0,\, n}{(q_i)}\right) = \lambda_0^{a_i}((q_i)) \quad \text{for} \quad u+1 \leqslant i \leqslant t.$$

Finally we note that the (j, j) entry for $1 \leqslant j \leqslant u$ is determined from a knowledge of the other entries in the jth column because of the product formula. (Remark: By comparing the matrices M and M_2, we note that for fixed j with $0 \leqslant j \leqslant u$, the product of the squares of the (i, j) entries for $1 \leqslant i \leqslant u$ times the product of the (i, j) entries for $u+1 \leqslant i \leqslant t$ equals 1.)

Now let G be an arbitrary $t \times (u+1)$ matrix with entries in W such that for fixed j with $0 \leqslant j \leqslant u$, the product of the squares of the (i, j) entries for $1 \leqslant i \leqslant u$ times the product of the (i, j) entries for $u+1 \leqslant i \leqslant t$ equals 1. Let

$$\text{(3.7)} \qquad S_{t;x}(G) = \{L \in S_{t;x}\colon \text{the matrix } M \text{ associated to } L \text{ equals } G\}$$

(cf. equations (2.6) and (2.11)). Suppose we consider one pure cubic field L_1 in $S_{t;x}(G)$. We may write $L_1 = \boldsymbol{Q}(n_1^{1/3})$, where

$$n_1 = (p_1'')^{a_1''} \ldots (p_u'')^{a_u''} (q_{u+1}'')^{a_{u+1}''} \ldots (q_t'')^{a_t''}$$

with each $p_i'' \equiv 1 \pmod 3$, each $q_i'' \equiv -1 \pmod 3$, and $1 \leqslant a_i'' \leqslant 2$ for each i. As usual we suppose $p_i'' < p_j''$ if $i < j$, and $q_i'' < q_j''$ if $i < j$. However we may have some $q_i'' < p_j''$. So we write the prime factorization of n_1 in the following way:

$$n_1 = (p_1')^{a_1'} \ldots (p_t')^{a_t'} \quad \text{with primes } p_1' < \ldots < p_t',$$

$1 \leqslant a_i' \leqslant 2$ for each i, and exactly u of the $p_i' \equiv 1 \pmod 3$. If $p_i' \equiv 1 \pmod 3$, we recall that $p_i' = \pi_i' \bar{\pi}_i'$ in $\boldsymbol{Q}(\zeta)$. Now let

$$\text{(3.8)} \qquad S_{t;x}(G, L_1) = \{L = \boldsymbol{Q}(n^{1/3}) \in S_{t;x}(G)\colon n \text{ has prime divisors } p_1 < \ldots < p_t \text{ with } p_i \equiv p_i' \pmod 3 \text{ for } 1 \leqslant i \leqslant t\}.$$

We shall obtain asymptotic formulas for $|S_{t;x}(G, L_1)|$ and $|S_{t;x}(G)|$. (Remark: Our asymptotic formula for $|S_{t;x}(G, L_1)|$ will be the appropriate analog of Lemma 3 in [5].)

Now suppose $p_k \neq 3$ and $p_l \neq 3$ are rational primes with $p_k < p_l$; and suppose $1 \leqslant a_k \leqslant 2$ and $1 \leqslant a_l \leqslant 2$. If p_k [resp., p_l] is congruent to $1 \pmod 3$, recall that $p_k = \pi_k \bar{\pi}_k$ [resp., $p_l = \pi_l \bar{\pi}_l$] in $\boldsymbol{Q}(\zeta)$. Suppose that at least one of p_k and p_l is congruent to $1 \pmod 3$. Then we define

$$\text{(3.9)} \qquad h_{a_k,a_l}(p_k, p_l) = \begin{cases} (\lambda_k^{a_l}((\pi_l)),\ \omega_k^{a_k}((\pi_l)) \in W \times W & \text{if} \quad p_k \equiv p_l \equiv 1 \pmod 3, \\ \lambda_k^{a_l}((p_l)) \in W & \text{if} \quad p_k \equiv 1 \pmod 3,\ p_l \equiv -1 \pmod 3, \\ \omega_k^{a_k}((\pi_l)) \in W & \text{if} \quad p_k \equiv -1 \pmod 3,\ p_l \equiv 1 \pmod 3. \end{cases}$$

We also define

$$\text{(3.10)} \qquad h_{a_l}(p_l) = \begin{cases} \lambda_0^{a_l}((\pi_l)) & \text{if} \quad p_l \equiv 1 \pmod 3, \\ \lambda_0^{a_l}((p_l)) & \text{if} \quad p_l \equiv -1 \pmod 3. \end{cases}$$

Now suppose $L = \boldsymbol{Q}(n^{1/3})$, where $n = p_1^{a_1} \ldots p_t^{a_t}$ with primes $p_1 < \ldots < p_t$ and $1 \leqslant a_i \leqslant 2$ for each i. Then from equations (3.1) through (3.10), we see that $L \in S_{t;x}(G, L_1)$ if and only if

(i) $p_l \equiv p_l' \pmod 3$ for $1 \leqslant l \leqslant t$;

(ii) $h_{a_k,a_l}(p_k, p_l) = h_{a'_k,a'_l}(p'_k, p'_l)$ for $1 \leqslant k < l \leqslant t$ whenever at least one of p_k and p_l is congruent to $1 \pmod 3$; and

(iii) $h_{a_l}(p_l) = h_{a'_l}(p'_l)$ for $1 \leqslant l \leqslant t$.

Suppose at least one of p_k and p_l is congruent to $1 \pmod 3$. We define

$$\delta_{a_k,a_l}(p_k, p_l) = \begin{cases} 1 & \text{if} \quad h_{a_k,a_l}(p_k, p_l) = h_{a'_k,a'_l}(p'_k, p'_l); \\ 0 & \text{otherwise.} \end{cases}$$

If both $p_k \equiv -1 \pmod 3$ and $p_l \equiv -1 \pmod 3$, we define $\delta_{a_k,a_l}(p_k, p_l) = 1$. For $1 \leqslant l \leqslant t$, we define

$$\delta_{a_l}(p_l) = \begin{cases} 1 & \text{if} \quad h_{a_l}(p_l) = h_{a'_l}(p'_l); \\ 0 & \text{otherwise.} \end{cases}$$

Then we have

$$(3.11) \qquad |S_{t;x}(G, L_1)| = \sum_{\substack{p_1 \leqslant x^{1/t} \\ p_1 \equiv p'_1 \pmod 3}} \sum_{a_1=1}^{1} \sum_{\substack{p_1 < p_2 \leqslant (x/p_1)^{1/(t-1)} \\ p_2 \equiv p'_2 \pmod 3}} Y_2 \ldots \sum_{\substack{p_{t-1} < p_t \leqslant x/p_1 \ldots p_{t-1} \\ p_t \equiv p'_t \pmod 3}} Y_t$$

where

$$(3.12) \qquad Y_j = \sum_{a_j=1}^{2} \delta_{a_j}(p_j) \prod_{i_j=1}^{j-1} \delta_{a_{i_j},a_j}(p_{i_j}, p_j) \quad \text{for} \quad j = 2, 3, \ldots, t$$

(cf. [5], equations (4) and (5)). Then we can proceed to obtain the following analog of Lemma 3 in [5].

Lemma 3.2.

$$|S_{t;x}(G, L_1)| = \frac{1}{2 \cdot 3^{(t-1)(u+1)}} \cdot \frac{1}{(t-1)!} \frac{x(\log\log x)^{t-1}}{\log x} + o\left(\frac{x(\log\log x)^{t-1}}{\log x}\right),$$

where t is the number of totally ramified primes in L_1/Q, and u is the number of these totally ramified primes that are congruent to $1 \pmod 3$.

Remark. The formula for $|S_{t;x}(G, L_1)|$ is valid for every $t \times (u+1)$ matrix G having the properties listed in the discussion preceding equation (3.7), and the formula is valid for every L_1 in $S_{t;x}(G)$.

We shall briefly describe in an intuitive way how the factors in the main term in Lemma 3.2 arise (cf. [5], p. 202). Each $\delta_{a_{i_j},a_j}(p_{i_j}, p_j) = 1$ with probability 1/9 if $p_{i_j} \equiv p_j \equiv 1 \pmod 3$, with probability 1 if $p_{i_j} \equiv p_j \equiv -1 \pmod 3$, and with probability 1/3 otherwise. Each $\delta_{a_j}(p_j) = 1$ with probability 1/3. All of these δ terms combine to contribute the factor $1/3^{(t-1)(u+1)}$. Each sum $\sum_{a_j=1}^{2}$ contributes a factor of 2, but each congruence condition $p_i \equiv p'_i \pmod 3$ contributes a factor of 1/2. We thus get the factor $2^{t-1}(1/2^t) = 1/2$. Finally we note that

$$\sum_{\substack{p_1 \ldots p_t \leqslant x \\ p_1 < \ldots < p_t}} 1 \sim \frac{1}{(t-1)!} \frac{x(\log\log x)^{t-1}}{\log x}.$$

The actual proof of Lemma 3.2 is quite lengthy, but the ideas required are the same as those used in proving Lemma 3 in [5]; hence we refer the reader to [5] for details. We remark that a key part of the proof is showing that various character sums are $o\left(\frac{x(\log\log x)^{t-1}}{\log x}\right)$.

From equations (3.7) and (3.8) and from the remark following Lemma 3.2, we have the following result.

Corollary 3.3. $|S_{t;x}(G)| \sim \binom{t}{u} |S_{t;x}(G, L_1)|$, *where* $\binom{t}{u}$ *is the binomial coefficient* $(t!)/(u!)((t-u)!)$.

Now recall that G is a $t \times (u+1)$ matrix with entries in $W = \{\zeta^0, \zeta^1, \zeta^2\}$ such that for fixed j with $0 \leqslant j \leqslant u$, the product of the squares of the (i, j) entries for $1 \leqslant i \leqslant u$ times the product of the (i, j) entries for $u+1 \leqslant i \leqslant t$ equals 1. Thus G is determined by the entries in its first $(t-1)$ rows, and those entries can be arbitrary elements of W. For t a positive integer, nonnegative integers $u \leqslant t$ and $c \leqslant u+1$, and x a positive real number, we let

$$(3.13) \qquad S_{t,u,c;x} = \bigcup_G S_{t;x}(G),$$

where G ranges over all these special $t \times (u+1)$ matrices such that rank $G = u+1-c$ when G is viewed as a matrix over $\boldsymbol{F}_3$. Then

$$(3.14) \qquad |S_{t,u,c;x}| \sim N_{t-1,u+1,c} |S_{t;x}(G)|,$$

where $N_{t-1,u+1,c}$ is the number of $(t-1) \times (u+1)$ matrices over $\boldsymbol{F}_3$ with rank $= u+1-c$. (When $t = 1$, we define $N_{0,u+1,c} = 1$ if $c = u+1$; otherwise $N_{0,u+1,c} = 0$.) Finally using equations (2.9) through (2.12) and equation (3.13), we have

$$(3.15) \qquad |S_{t,c;x}| = \sum_{u=0}^{t} |S_{t,u,c;x}|$$

and

$$(3.16) \qquad |S_{t;x}| = \sum_{c=0}^{t+1} |S_{t,c;x}|.$$

4. Density results for pure cubic case. We let notations be as in previous sections. Our goal in this section is to compute the density $d_{t,c}$ given by equation (2.13) and to compute $\lim_{t\to\infty} d_{t,c}$. From Lemma 3.2, Corollary 3.3, and formulas (3.14) through (3.16), we have

$$(4.1)\qquad |S_{t,c;x}| \sim \sum_{u=0}^{t} \binom{t}{u} \frac{N_{t-1,u+1,c}}{2\cdot 3^{(t-1)(u+1)}} \cdot \frac{1}{(t-1)!} \frac{x(\log\log x)^{t-1}}{\log x}$$

and

$$(4.2)\qquad |S_{t;x}| \sim \sum_{c=0}^{t+1} \sum_{u=0}^{t} \binom{t}{u} \frac{N_{t-1,u+1,c}}{2\cdot 3^{(t-1)(u+1)}} \cdot \frac{1}{(t-1)!} \frac{x(\log\log x)^{t-1}}{\log x}.$$

We recall that $N_{t-1,u+1,c}$ is the number of $(t-1)\times(u+1)$ matrices over F_3 with rank $= u+1-c$. Now we note that $\sum_{c=0}^{t+1} N_{t-1,u+1,c} = 3^{(t-1)(u+1)}$, the total number of $(t-1)\times(u+1)$ matrices over F_3. Hence formula (4.2) becomes

$$(4.3)\qquad |S_{t;x}| \sim \sum_{u=0}^{t} \binom{t}{u} \cdot \frac{1}{2} \cdot \frac{1}{(t-1)!} \frac{x(\log\log x)^{t-1}}{\log x}.$$

Now if we sum all binomial coefficients, we have $\sum_{u=0}^{t} \binom{t}{u} = 2^t$. So formula (4.3) becomes

$$(4.4)\qquad |S_{t;x}| \sim 2^{t-1} \cdot \frac{1}{(t-1)!} \frac{x(\log\log x)^{t-1}}{\log x}.$$

Then using equation (2.13) and formulas (4.1) and (4.4), we have

$$(4.5)\qquad d_{t,c} = \sum_{u=0}^{t} b_{t,u} f_{t-1,u+1,c},$$

where

$$(4.6)\qquad b_{t,u} = \binom{t}{u} \cdot 2^{-t}$$

and

$$(4.7)\qquad f_{t-1,u+1,c} = \frac{N_{t-1,u+1,c}}{3^{(t-1)(u+1)}}.$$

We note that $b_{t,u}$ is a binomial probability, and $\sum_{u=0}^{t} b_{t,u} = 1$. Also $f_{t-1,u+1,c}$ is the probability that a randomly selected $(t-1)\times(u+1)$ matrix over F_3 has rank $= u+1-c$. If $c > u+1$, then $f_{t-1,u+1,c} = 0$. If $c = u+1$, then

$f_{t-1,u+1,c} = 3^{-(t-1)(u+1)}$. If $0 \leqslant c \leqslant u$, we can use [10] to get

$$\begin{aligned} f_{t-1,u+1,c} &= \frac{1}{3^{(t-1)(u+1)}} \prod_{i=0}^{u-c} \frac{(3^{u+1}-3^i)(3^{t-1-i}-1)}{(3^{i+1}-1)} \\ &= \frac{3^{(u-c+1)(u+1)} \cdot 3^{(t-1)(u-c+1)-(u-c)(u-c+1)/2}}{3^{(t-1)(u+1)} \cdot 3^{(u-c+1)(u-c+2)/2}} \times \\ &\qquad \times \prod_{i=0}^{u-c} \frac{(1-3^{i-u-1})(1-3^{i+1-t})}{(1-3^{-i-1})} \\ &= 3^{-c(c+t-u-2)} \prod_{i=0}^{u-c} \frac{(1-3^{i-u-1})(1-3^{i+1-t})}{(1-3^{-i-1})}. \end{aligned}$$

We let $j = u+1-i$. Then for $0 \leqslant c \leqslant u$,

$$(4.8)\qquad f_{t-1,u+1,c} = 3^{-c(c+t-u-2)} \prod_{j=c+1}^{u+1} \frac{(1-3^{-j})(1-3^{2-j-(t-u)})}{(1-3^{j-u-2})}.$$

So we obtain the following result.

THEOREM 4.1. *Let t be a positive integer. Let $d_{t,c}$ be the density of pure cubic extensions of Q with t totally ramified primes having 3-class rank equal to $t-2+c$ among all pure cubic fields with t totally ramified primes. Here $0 \leqslant c \leqslant t+1$. Then*

$$d_{t,c} = \sum_{u=0}^{t} \binom{t}{u} \cdot 2^{-t} \cdot f_{t-1,u+1,c},$$

where $\binom{t}{u} = (t!)/(u!)((t-u)!)$; $f_{t-1,u+1,c}$ is given by equation (4.8) if $0 \leqslant c \leqslant u$;

$$f_{t-1,u+1,c} = \begin{cases} 3^{-(t-1)(u+1)} & \textit{if} \quad c = u+1; \\ 0 & \textit{if} \quad c > u+1. \end{cases}$$

In Table II in the appendix, we list some values for $d_{t,c}$. Suppose we have a pure cubic field with exactly t totally ramified primes. For $t = 1$, c is equally likely to be 1 or 2, and hence the 3-class rank is equally likely to be 0 or 1. For $t = 2$ and 3, the 3-class rank is most likely to be $t-1$. For $t \geqslant 4$, the 3-class rank is most likely to be $t-2$.

It remains to determine the behavior of $d_{t,c}$ as t becomes large. Before computing $\lim_{t\to\infty} d_{t,c}$, we examine certain subclasses of pure cubic fields. For $0 \leqslant v \leqslant t$, we let

$$S_{t;x}^{(v)} = \{L \in S_{t;x}\colon \text{exactly } v \text{ of the totally ramified primes in } L/Q \text{ are not congruent to } 1 \pmod 3\}.$$

Then we let

$$S_{t,c;x}^{(v)} = \{L \in S_{t;x}^{(v)}: \text{the 3-class rank of } L \text{ is } t-2+c\}.$$

We define the density $\Delta_{t,c}^{(v)}$ by

$$(4.9) \qquad \Delta_{t,c}^{(v)} = \lim_{x \to x} \frac{|S_{t,c;x}^{(v)}|}{|S_{t;x}^{(v)}|}.$$

So $\Delta_{t,c}^{(v)}$ tells us how likely it is for a pure cubic field with exactly t totally ramified primes, exactly v of which are not congruent to $1 \pmod 3$, to have 3-class rank equal to $t-2+c$. From Sections 2 and 3 we see that we can replace $|S_{t,c;x}^{(v)}|$ by $|S_{t,t-v,c;x}|$. (See equation (3.13).) Also we can replace $|S_{t;x}^{(v)}|$ by $\sum_c |S_{t,t-v,c;x}|$. Then from Lemma 3.2, Corollary 3.3, and formulas (3.14), (4.7), and (4.9), we get

$$(4.10) \qquad \Delta_{t,c}^{(v)} = f_{t-1,t-v+1,c}.$$

If $c \leqslant t-v$, then using equation (4.8), we get

$$(4.11) \quad \Delta_{t,c}^{(v)} = 3^{-c(c+v-2)} \prod_{j=c+1}^{t-v+1} \frac{(1-3^{-j})(1-3^{2-j-v})}{(1-3^{j-t+v-2})}$$

$$= 3^{-c(c+v-2)} \Big[\prod_{j=c+1}^{t-v+1} (1-3^{-j})\Big] \frac{(1-3^{-c-v+1})(1-3^{-c-v}) \dots (1-3^{-t+1})}{(1-3^{c-t+v-1})(1-3^{c-t+v}) \dots (1-3^{-1})}.$$

We now have the following result.

Proposition 4.2. *Let t be a positive integer and v a nonnegative integer with $v \leqslant t$. Let $\Delta_{t,c}^{(v)}$ be the density of pure cubic extensions of Q with t totally ramified primes, v of which are not congruent to* $1 \pmod 3$, *having 3-class rank equal to $t-2+c$ among all pure cubic fields with t totally ramified primes, v of which are not congruent to* $1 \pmod 3$. *Here $0 \leqslant c \leqslant t+1$. Then $\Delta_{t,c}^{(v)}$ is given by equation* (4.11) *if $c \leqslant t-v$; $\Delta_{t,c}^{(v)} = 3^{-(t-1)(t-v+1)}$ if $c = t-v+1$; and $\Delta_{t,c}^{(v)} = 0$ if $c > t-v+1$. Furthermore if c and v are fixed, then*

$$\lim_{t \to \infty} \Delta_{t,c}^{(v)} = \frac{3^{-c(c+v-2)} \prod\limits_{j=c+v-1}^{\infty} (1-3^{-j})}{\prod\limits_{j=1}^{c} (1-3^{-j})}.$$

(If $c = 0$, the factor $\prod_{j=1}^{c} (1-3^{-j})$ is omitted.)

Remark. In Section 1 we observed that Galois cubic fields with exactly t ramified primes have 3-class ranks $= t-1+c$ with density $d'_{t,c}$ given by Proposition 1.1. Also $\lim_{t \to \infty} d'_{t,c}$ is given by Corollary 1.2. Suppose we let $v = 1$ and $c' = c-1$ in Proposition 4.2. So we are considering pure cubic fields with exactly t totally ramified primes, exactly one of which is not congruent to $1 \pmod 3$. Such fields have 3-class ranks equal to $t-1+c'$ with density $\Delta_{t,c'+1}^{(1)}$. From Corollary 1.2 and Proposition 4.2, we have the interesting result that $\lim_{t \to \infty} \Delta_{t,c'+1}^{(1)} = \lim_{t \to \infty} d'_{t,c'}$ for $c' = 0, 1, 2, \dots$ Furthermore by induction one can even show that $\Delta_{t,c'+1}^{(1)} = d'_{t,c'}$ for all t and $0 \leqslant c' \leqslant t-1$. So as far as our densities of 3-class ranks are concerned, the set of pure cubic fields with exactly t totally ramified primes, exactly one of which is not congruent to $1 \pmod 3$, provides a perfect analog to the set of Galois cubic fields with exactly t ramified primes.

In equation (4.11) if we keep c fixed but require $v \to \infty$ in a certain way when $t \to \infty$, we obtain the following result.

Proposition 4.3. *Let notations be as in Proposition 4.2. Suppose α is a fixed real number with $0 < \alpha \leqslant 1$. If $\alpha t \leqslant v \leqslant t$, then*

$$\lim_{t \to x} \Delta_{t,c}^{(v)} = \begin{cases} 1 & \text{if } c = 0, \\ 0 & \text{if } c > 0. \end{cases}$$

Remark. So for example if $\alpha = 1/4$ in Proposition 4.3, then $v \geqslant \alpha t$ means that the number of totally ramified primes not congruent to $1 \pmod 3$ is at least 1/4 of the number of totally ramified primes. Since the 3-class rank is $t-2+c$ with density $\Delta_{t,c}^{(v)}$ for a pure cubic field with exactly t totally ramified primes, exactly v of which are not congruent to $1 \pmod 3$, we see from Proposition 4.3 that the 3-class rank is very likely to be $t-2$ if t is large and $v \geqslant \alpha t$ for some fixed $\alpha > 0$.

We finally return to the calculation of $\lim_{t \to \infty} d_{t,c}$. Here we must consider all nonnegative integers u and v such that $u+v = t$. However Proposition 4.3 is a key result we shall need for our calculation. We start with equations (4.5) through (4.7). We let X_t be the random variable which takes on the value u (for $0 \leqslant u \leqslant t$) with probability $b_{t,u}$ (see equation (4.6)). A standard calculation shows that the binomial random variable X_t has expected value $t/2$ and standard deviation $\sqrt{t}/2$. For large t, X_t is approximately normally distributed. Since the standard deviation $\sqrt{t}/2$ is much smaller than the expected value $t/2$ for large t, then if

$$B_t(j) = \sum_{0 \leqslant u \leqslant j} b_{t,u} \quad \text{(the cumulative probability for } X_t\text{)},$$

we can choose t sufficiently large so that $(1-B_t(3t/4))$ is arbitrarily small. Now we write $d_{t,c} = R_1 + R_2$ with

$$R_1 = \sum_{0 \leqslant u \leqslant 3t/4} b_{t,u} f_{t-1,u+1,c}$$

and

$$R_2 = \sum_{3t/4 < u \leqslant t} b_{t,u} f_{t-1,u+1,c}.$$

Suppose $\varepsilon > 0$ is given. We choose a positive number T_1 so that for $t \geqslant T_1$,

$$(1 - B_t(3t/4)) < \varepsilon/2.$$

Then since $f_{t-1,u+1,c} \leqslant 1$, we have

$$R_2 \leqslant \sum_{3t/4 < u \leqslant t} b_{t,u} = 1 - B_t(3t/4) < \varepsilon/2.$$

Now suppose $c > 0$. With $v = t-u$, we see that $v \geqslant t/4$ in the sum R_1. So from equation (4.10) and Proposition 4.3, we can choose a positive number T_2 so that for $t \geqslant T_2$, $f_{t-1,u+1,c} < \varepsilon/2$ for all $0 \leqslant u \leqslant 3t/4$ if $c > 0$. Then for $t \geqslant T_2$,

$$R_1 < \sum_{0 \leqslant u \leqslant 3t/4} b_{t,u}(\varepsilon/2) = (\varepsilon/2)\, B_t(3t/4) \leqslant \varepsilon/2.$$

Then for $t \geqslant \max(T_1, T_2)$, $d_{t,c} = R_1 + R_2 < \varepsilon$ if $c > 0$. If $c = 0$, then we choose T_2 so that for $t \geqslant T_2$, $f_{t-1,u+1,c} > 1-(\varepsilon/2)$ for $0 \leqslant u \leqslant 3t/4$. Then for $t \geqslant \max(T_1, T_2)$,

$$R_1 > \sum_{0 \leqslant u \leqslant 3t/4} b_{t,u}\big(1-(\varepsilon/2)\big)$$
$$= \big(1-(\varepsilon/2)\big) B_t(3t/4) > \big(1-(\varepsilon/2)\big)\big(1-(\varepsilon/2)\big) > 1-\varepsilon.$$

So for $t \geqslant \max(T_1, T_2)$, we have $d_{t,c} = R_1 + R_2 \geqslant R_1 > 1-\varepsilon$ if $c = 0$. Hence we have our final result.

THEOREM 4.4. *Let notations be as in Theorem* 4.1. *Then*

$$\lim_{t\to\infty} d_{t,c} = \begin{cases} 1 & \textit{if} \quad c = 0, \\ 0 & \textit{if} \quad c > 0. \end{cases}$$

Remark. Galois cubic fields and pure cubic fields present an interesting contrast. For every $c \geqslant 0$, $\lim_{t\to\infty} d'_{t,c} > 0$ in the Galois cubic case. So all possible 3-class ranks $t-1+c$ for $0 \leqslant c \leqslant t-1$ occur with densities that do not go to zero as $t \to \infty$. Yet in the pure cubic case $\lim_{t\to\infty} d_{t,c} = 0$ for all $c > 0$, and hence for the 3-class ranks greater than $t-2$, the densities go to zero as $t \to \infty$.

APPENDIX

In Table I, t denotes the number of ramified primes in a Galois cubic field; c is the integer such that the 3-class rank of the Galois cubic field is $t-1+c$; and $d'_{t,c}$ is the density defined by equation (1.6). Also $d'_{\infty,c} = \lim_{t\to\infty} d'_{t,c}$.

Table I. Values of $d'_{t,c}$

c t	0	1	2	3	4	5
1	1.000000					
2	.888889	.111111				
3	.855967	.142661	.001372			
4	.845400	.152642	.001957	1.9×10^{-6}		
5	.841921	.155911	.002165	2.8×10^{-6}	2.9×10^{-10}	
6	.840766	.156995	.002236	3.1×10^{-6}	4.3×10^{-10}	4.9×10^{-15}
7	.840381	.157355	.002260	3.2×10^{-6}	4.8×10^{-10}	7.3×10^{-15}
8	.840253	.157475	.002268	3.3×10^{-6}	5.0×10^{-10}	8.2×10^{-15}
9	.840210	.157515	.002271	3.3×10^{-6}	5.0×10^{-10}	8.5×10^{-15}
10	.840196	.157529	.002272	3.3×10^{-6}	5.1×10^{-10}	8.6×10^{-15}
⋮						
15	.840189	.157535	.002272	3.3×10^{-6}	5.1×10^{-10}	8.6×10^{-15}
⋮						
20	.840189	.157535	.002272	3.3×10^{-6}	5.1×10^{-10}	8.6×10^{-15}
⋮						
∞	.840189	.157535	.002272	3.3×10^{-6}	5.1×10^{-10}	8.6×10^{-15}

In Table II, t denotes the number of totally ramified primes in a pure cubic field; c is the integer such that the 3-class rank of the pure cubic field is $t-2+c$; and $d_{t,c}$ is the density defined by equation (2.13). Also $d_{\infty,c} = \lim_{t\to\infty} d_{t,c}$.

Table II. Values of $d_{t,c}$

c t	0	1	2	3	4	5
1	0	.500000	.500000			
2	.166667	.527778	.296296	.009259		
3	.333333	.483025	.177012	.006611	1.9×10^{-5}	
4	.488169	.403880	.104140	.003797	1.4×10^{-5}	4.4×10^{-9}
5	.619782	.317720	.060444	.002046	8.0×10^{-6}	3.3×10^{-9}
6	.724413	.239735	.034769	.001079	4.2×10^{-6}	1.8×10^{-9}
7	.803828	.175718	.019888	.000564	2.2×10^{-6}	9.6×10^{-10}
8	.862217	.126155	.011333	.000294	1.1×10^{-6}	4.9×10^{-10}
9	.904203	.089203	.006441	.000153	5.6×10^{-7}	2.5×10^{-10}
10	.933914	.062353	.003653	.000080	2.8×10^{-7}	1.2×10^{-10}
⋮						
15	.990389	.009399	.000209	3.0×10^{-6}	9.4×10^{-9}	4.0×10^{-12}
⋮						
20	.998683	.001305	.000012	1.2×10^{-7}	3.1×10^{-10}	1.3×10^{-13}
⋮						
∞	1.00000	0	0	0	0	0

References

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

[2] R. Dedekind, *Ueber die Anzahl der Idealklassen in reinen kubischen Zahlkörpern*, J. Reine Angew. Math. 121 (1900), pp. 40–123.

[3] F. Gerth, *On 3-class groups of pure cubic fields*, ibid. 278/279 (1975), pp. 52–62.

[4] — *Ranks of* 3-*class groups of non-Galois cubic fields*, Acta Arith. 30 (1976), pp. 307–322.

[5] — *Counting certain number fields with prescribed l-class numbers*, J. Reine Angew. Math. 337 (1982), pp. 195–207.

[6] — *An application of matrices over finite fields to algebraic number theory*, Math. Comp. 41 (1983), pp. 229–234.

[7] — *Densities for ranks of certain parts of p-class groups*, to appear.

[8] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. II*, Jahresber. Deutsch. Math.-Verein. 39 (1930), pp. 1–204.

[9] E. Inaba, *Über die Struktur der l-Klassengruppe zyklischer Zahlkörper von Primzahlgrad l*, J. Fac. Sci. Imp. Univ. Tokyo, Sect. I, 4 (1940), pp. 61–115.

[10] G. Landsberg, *Ueber eine Anzahlbestimmung und eine damit zusammenhängende Reihe*, J. Reine Angew. Math. 111 (1893), pp. 87–88.

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

Received on 3.9.1984
and in revised form on 31.1.1985 (1449)

ACTA ARITHMETICA
XLVI (1986)

Galois representations of Iwasawa modules

by

ROBERT GOLD and MANOHAR MADAN (Columbus, Ohio)

1. Introduction. A finite group of automorphisms of an algebraic function field of one variable over the complex numbers operates in a natural way on the space of holomorphic differentials. The representation thus obtained was given by Chevalley and Weil [1]. Iwasawa [5] obtained analogous results for p-adic galois representations in number fields. In his situation, L/K is a finite p-extension of Z_p-fields of CM-type and $\mathrm{Gal}(L/K)$ operates on A_L^-, the minus part of the p-class group of L. Iwasawa determined the representation on $A_L^- \otimes_{Z_p} Q_p$ (Th. 4, Th. 5). His immediate object was to give a proof of a theorem of Kida [6]. The classical Riemann–Hurwitz genus formula and the well-known orthogonality relations on characters are the critical tools in the treatment of Chevalley and Weil. Kida's theorem is an analogue of the genus formula and it can be proved easily. In Section 2, we give a unified proof of Iwasawa's two theorems in the spirit of Chevalley and Weil. This is Theorem 2. In the special case when $[L:K] = p$, we determine even the integral representations, i.e. the structure of A_L^- as a $Z_p[G]$-module, $G = \mathrm{Gal}(L/K)$. This gives in particular the basis for induction in the proof of Theorem 2.

In Section 3, we determine the modular representations in the case when L/K is a cyclic p-extension and the module consists of elements of order dividing p in A_L^-. This result is analogous to the one proved in [4] for function fields.

To generalize Theorem 1 to arbitrary p-extensions is an interesting open problem. For the special case when G is cyclic of order p^2, the indecomposable $Z_p[G]$-modules have been classified. Using this, we have been able to extend Theorem 1 to this case, Theorem 4 in Section 4.

We are particularly indebted to Alfredo Jones for the information summarized in Table 1.

2. Let p be an odd prime. Let Q_n be the unique cyclic extension of degree p^{n-1} contained in the cyclotomic field of p^n-th roots of unity and $Q_\infty = \bigcup_{n>0} Q_n$. A Z_p-field is the composite of Q_∞ with a finite extension of Q.