ACTA ARITHMETICA
118.1 (2005)

Steinitz classes and discriminant counting

by

Ebru Bekyel (Istanbul)

1. Introduction. Let k be a number field. For a finite extension k'/k let $\Delta(k'/k)$ be the discriminant idèle first defined by Fröhlich in [4], where it is also shown that k' has a relative integral basis over k if and only if $\Delta(k'/k)$ is principal. If the class number of k is odd, this condition is equivalent to the discriminant ideal $(\Delta(k'/k))$ being principal. In this paper we determine how often this happens for extensions with a fixed abelian group G. More generally, let $\mathfrak{c}$ be an element of the ideal class group Cl_k of k and let $N(k, G, \mathfrak{c}; X)$ be the number of normal extensions k'/k with Galois group isomorphic to G, $(\Delta(k'/k)) \in \mathfrak{c}$ and the norm of $(\Delta(k'/k))$ less than or equal to X. We want to determine the behavior of $N(k, G, \mathfrak{c}; X)$ as $X \to \infty$. We prove the following theorem:

Theorem 1. *Let k be a number field and G be a finite abelian group. Let $\mathfrak{c}$ be an element of the ideal class group of k. If there exists an extension k'/k such that* $\mathrm{Gal}(k'/k) \cong G$ *and $(\Delta(k'/k)) \in \mathfrak{c}$ then there exists a positive number $c_1(k, G, \mathfrak{c})$ such that*

$$N(k, G, \mathfrak{c}; X) \sim c_1(k, G, \mathfrak{c}) X^a (\log X)^b$$

as $X \to \infty$, where a and b are constants depending on G and k.

The question of whether there exists an extension k'/k such that $\mathrm{Gal}(k'/k) \cong G$ and $(\Delta(k'/k)) \in \mathfrak{c}$ is settled completely for G abelian by McCulloh in [5]. The counting of extensions of a global field k with a given Galois group G was done by Wright in [9], where it is proven that

$$\sum_{\mathfrak{c}} c_1(k, G, \mathfrak{c}) > 0.$$

The method used to prove the above statement in [9] is to study the associated Dirichlet series. In fact the author proves results about a more general series of quasicharacters which he later specializes for his own purposes. In

2000 *Mathematics Subject Classification*: Primary 11R45; Secondary 11R37, 11R33.
Key words and phrases: Stenitz class, discriminant counting.

order to prove our theorem, we are going to use this more general series so we start by summarizing in Section 2 some of the results from [9]. Then in Section 3 we prove our main theorem. In the final section we calculate $c_1(k, G, \mathfrak{c})$ in the case of cyclic extensions of prime order as an example.

2. Results on discriminant series. The results of this section are due to Wright. We summarize the necessary definitions and constructions, in particular those necessary for the statement of Proposition 5.5 of [9]. Let k be a number field. We denote by $A^\times$ the idèle group of k and by C_k the idèle class group $A^\times/k^\times$. Let M_k be the set of primes of k and let M_∞ be the set of infinite primes. For any prime v, k_v is the completion of k at v. For a finite prime v the valuation ring and the unit group of k_v are denoted by O_v and $O_v^\times$ respectively. In this case, a basis for the topology of $k_v^\times$ is given by the sets $U_v^{(n)} = 1 + \pi_v^n O_v^\times$, where π_v is a generator of the unique prime ideal $\mathfrak{p}_v$ of O_v and $n \geq 1$. We let $U_v^{(0)} = O_v^\times$. For an open subgroup $U \subset k_v^\times$ the conductor of U denoted by $\Phi(U)$ is π_v^n, where n is the smallest integer such that $U_v^{(n)} \subset U$. If v is infinite and complex, then $k_v^\times = \mathbb{C}^\times$, which has no open subgroups but itself whose conductor is defined to be 1. In the case $k_v = \mathbb{R}$, $\Phi(\mathbb{R}^\times) = 1$ and $\Phi(\mathbb{R}^+) = -1$. For an open subgroup U of $A^\times$ the conductor is the idèle whose local components are the conductors of the open subgroups $U_v = U \cap k_v^\times$ of $k_v^\times$. For a continuous character χ of $A^\times$ or of $k_v^\times$ for any prime v, the conductor $\Phi(\chi)$ is defined to be the conductor of the kernel of χ.

Let ω be a quasicharacter on the idèles $A^\times$ of k which is trivial on $k^\times$, i.e. a continuous $\mathbb{C}^\times$-valued homomorphism on C_k. For a fixed finite abelian group G the generating series of discriminants is defined by

$$D_G(\omega) = \sum_{\mathrm{Gal}(k'/k) \cong G} \omega(\Delta(k'/k)), \tag{1}$$

where the sum is over all extensions k'/k with Galois group isomorphic to G. We will see below that this series can be written as a finite sum of series which converge for $\mathrm{Re}(\omega)$ large enough. The first step in that direction is to write this series as a combination of conductor series. Since G is a finite abelian group, it has a unique representation of the form

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_l\mathbb{Z},$$

where n_j are integers greater than 1 such that $n_{j+1} \mid n_j$ for $j = 1, \ldots, l-1$. For a locally compact abelian group X let $C_n(X)$ be the group of all continuous characters χ of X such that $\chi^n = 1$. Define

$$C_G(X) = C_{n_1}(X) \times \cdots \times C_{n_l}(X).$$

Now for any character $\chi = (\chi_1, \dots, \chi_l) \in C_G(C_k)$ let

$$\Phi_G(\chi) = \prod_{0 \le a_1 < n_1} \cdots \prod_{0 \le a_l < n_l} \Phi(\chi_1^{a_1} \cdots \chi_l^{a_l}).$$

The relation between the generating series for conductors defined by

$$F_G(\omega) = \sum_{\chi \in C_G(C_k)} \omega(\Phi_G(\chi))$$

and the discriminant series given by (1) is

$$D_G(\omega) = \frac{1}{\phi(G)} \sum_{H \subset G} \mu(G/H) F_H(\omega^{|G|/|H|}), \tag{2}$$

where $\phi(G)$ is the cardinality of the group of automorphism of G, the sum is over all subgroups H of G, and μ is the Möbius function on finite abelian groups defined in [3] with the property that

$$\sum_{H \subset J \subset G} \mu(J/H) = \sum_{H \subset J \subset G} \mu(G/J) = \begin{cases} 1 & \text{if } G = H, \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

The equality (2) is a result of the conductor-discriminant formula and inversion given by (3). Before we carry on, we should remark that since the local discriminants are defined up to multiplication by squares of units and the local conductors are defined up to multiplication by units, we require the quasicharacter ω to be trivial on $A_0 = \prod_{v \notin M_\infty} O_v^\times$. This is the reason why we can only count extensions with $(\Delta(k'/k)) \in \mathfrak{c}$. Ideally, one would like to single out those extensions where $\Delta(k'/k)$ is principal which guarantees that k'/k has an integral basis.

Next we give an expression of the conductor series as a combination of Euler products. Let S be a set of primes containing the infinite ones such that

$$O_S^\times = \{x \in k^\times : v(x) \ge 0 \text{ for all } v \notin S\}$$

is a principal ideal domain and let O_S^n be the subgroup of nth powers in $O_S^\times$. Define

$$\mathcal{E}_G(S) = O_S^\times / O_S^{n_1} \times \cdots \times O_S^\times / O_S^{n_l}$$

and let $e_G(S)$ be the order of $\mathcal{E}_G(S)$. Then

$$F_G(\omega) = \frac{1}{e_G(S)} \sum_{\varepsilon \in \mathcal{E}_G(S)} F_{G,S}(\omega; \varepsilon), \tag{4}$$

where each $F_{G,S}(\omega; \varepsilon)$ is an Euler product

$$F_{G,S}(\omega; \varepsilon) = \prod_v F_{G,v}(\omega; \varepsilon). \tag{5}$$

The individual Euler factors of the Euler products are given by

$$F_{G,v}(\omega;\varepsilon) = \begin{cases} \displaystyle\sum_{\chi\in C_G(k_v^\times)} \chi(\varepsilon)\omega_v(\Phi_G(\chi)) & \text{if } v\in S, \\ \displaystyle\sum_{\chi\in C_G(O_v^\times)} \chi(\varepsilon)\omega_v(\Phi_G(\chi)) & \text{if } v\notin S. \end{cases} \tag{6}$$

The convergence properties of $F_{G,S}(\omega;\varepsilon)$ are described through comparison to certain L-series. Let T be a finite set of places of k containing all the infinite places and places where ω_v is ramified. Let

$$L_{k,T}(\omega) = \prod_{v\notin T}(1-\omega_v(\pi_v))^{-1}$$

and for an arbitrary finite Galois extension K/k let

$$L_{K,T}(\omega) = L_{K,T'}(\omega\circ N_{K/k}),$$

where T' is the set of primes of K above T and $N_{K/k}$ is the relative idèle norm. The set T does not affect convergence and is omitted from the notation for simplicity. It is well known that (see for example [8]), for any extension K/k, the series $L_K(\omega)$ converges absolutely and locally uniformly in $\mathrm{Re}(\omega)>1$ and it may be continued to a holomorphic function except for simple poles when $\omega\circ N_{K/k}$ is trivial on idèles of norm 1 and $s(\omega)=1$.

Now let Q be the smallest prime dividing the order of the group G, β be the largest integer such that $(\mathbb{Z}/Q\mathbb{Z})^\beta \subseteq G$, and let $\alpha(G)=|G|(1-Q^{-1})$. Also define $k_0=k(\zeta_Q)$ with ζ_Q a primitive Qth root of unity and let d be the degree of the extension k_0/k. We are ready to state the main proposition regarding the convergence of $F_{G,S}(\omega;\varepsilon)$.

Proposition 2 ([9, Proposition 5.5]). *The Euler product $F_{G,S}(\omega;\varepsilon)$ converges absolutely and uniformly for $\mathrm{Re}(\omega)>1/\alpha(G)$. Also, $F_{G,S}(\omega;\varepsilon)$ has an analytic continuation to $\mathrm{Re}(\omega)>1/(\alpha(G)+1)$, which is equal to a holomorphic function $\phi(\omega)$ multiplied by*

$$(L_{k_\varepsilon}(\omega^{\alpha(G)}))^{(Q^{\beta-m}-1)/d}\left\{\frac{L_{k_\varepsilon}(\omega^{\alpha(G)})}{L_{k_0}(\omega^{\alpha(G)})}\right\}^{1/d}, \tag{7}$$

where $k_\varepsilon = k_0(\varepsilon_1^{1/Q},\dots,\varepsilon_l^{1/Q})$ and $Q^m=[k_\varepsilon : k_0]$. In addition, all zeros of $\phi(\omega)$ occur at solutions to the factors $F_{G,v}(\omega;\varepsilon)$ of the Euler product $F_{G,S}(\omega;\varepsilon)$ for finitely many places v.

3. Density of extensions. Let $\mathfrak{c}$ be an ideal class in the class group Cl_k of k. For an idèle $x=(x_v)\in A^\times$ let (x) be the corresponding ideal and let

$$|x| = \prod_v |x_v|_v$$

be the idèle norm. We want to calculate the Dirichlet series

$$D_{G,\mathfrak{c}}(s) = \sum_{\mathrm{Gal}(k'/k)\cong G,\,(\Delta(k'/k))\in\mathfrak{c}} |\Delta(k'/k)|^s$$

summed over extensions with Galois group isomorphic to G and the discriminant ideal belonging to $\mathfrak{c}$. Note that the idèle norm $|\Delta(k'/k)|$ is the reciprocal of the norm of the corresponding ideal $(\Delta(k'/k))$ so the above series is a Dirichlet series. Define the quasicharacters

$$\omega_{\psi,s}(x) = \psi((x))|x|^s$$

on $A^\times$, where ψ is a character of the ideal class group of k. We write ω_s in place of $\omega_{1,s}$. Then by orthogonality of characters on the ideal class group Cl_k we can write

$$D_{G,\mathfrak{c}}(s) = \frac{1}{h_k}\sum_{\psi} \psi(\mathfrak{c}^{-1}) D_G(\omega_{\psi,s}), \tag{8}$$

where the sum is over all characters ψ of Cl_k and $D_G(\omega)$ is the discriminant series given by (1). We will see below that $D_G(\omega)$ converges for $\mathrm{Re}(\omega) > 1/\alpha$ with a possible pole at $s = 1/\alpha$. Since our aim is to find a density result, we will be content with finding an analytic continuation of $D_G(\omega)$ to some open set containing $\mathrm{Re}(\omega) \geq 1/\alpha$ so that we can apply the Ikehara–Delange Tauberian theorem to the series $D_{G,\mathfrak{c}}(s)$. For $\omega = \omega_s$, $D_G(\omega)$ has an analytic continuation to $\mathrm{Re}(\omega) > 1/(\alpha+1)$ as shown in [9].

Proposition 3. *Let $\alpha = |G|(1-Q^{-1})$, where Q is the smallest prime divisor of $|G|$. Let $d = [k(\zeta_Q) : k]$, $\phi_Q(G)$ be the number of elements of G of order Q and $\nu = \phi_Q(G)/d$. For any quasicharacter $\omega = \omega_{\psi,s}$ the discriminant series $D_G(\omega)$ can be written in the form*

$$D_G(\omega) = \frac{g_0(s)}{(s-1/\alpha)^\nu} + \sum_{j=1}^{N} \frac{g_j(s)}{(s-1/\alpha)^{a_j}} + g(s) \tag{9}$$

for $\mathrm{Re}(s) > 1/\alpha$, where $g(s), g_0(s), \ldots, g_N(s)$ are analytic in the half-plane $\mathrm{Re}(s) \geq 1/\alpha$ and a_j are non-negative rational numbers less than ν.

Proof. Combining (2) and (4) we see that the discriminant series $D_G(\omega)$ can be written as a combination of Euler products $F_{H,S}(\omega^{|G|/|H|};\varepsilon)$, where H is a subgroup of G and $\varepsilon \in \mathcal{E}_H(S)$, which converge uniformly for $\mathrm{Re}(\omega^{|G|/|H|}) > 1/\alpha(H)$ or equivalently for $\mathrm{Re}(\omega) > 1/|G|(1-Q_H^{-1})$, where Q_H is the largest prime divisor of the order of H. Therefore the Euler products coming from subgroups H whose order is not divisible by Q are analytic for $\mathrm{Re}(\omega) \geq 1/\alpha$ and thus contribute to $g(s)$. Now assume Q divides the order of H so that $\alpha(H)|G|/|H| = \alpha$ and let β_H be the largest integer such that $(\mathbb{Z}/Q\mathbb{Z})^{\beta_H} \subset H$. Note that $L_{k_0}(\omega^\alpha)$ and $L_{k_\varepsilon}(\omega^\alpha)$ are non-zero for

$\mathrm{Re}(\omega) \geq 1/\alpha$. Therefore if $L_{k_\varepsilon}(\omega^\alpha)$ does not have a pole at $s = 1/\alpha$ then the dth root of the quotient in (7) can be defined as a single-valued analytic function for $\mathrm{Re}(\omega) \geq 1/\alpha$. In that case $F_{H,S}(\omega^{|G|/|H|}; \varepsilon)$ has an analytic continuation to $\mathrm{Re}(\omega) \geq 1/\alpha$ and so it contributes to the analytic part $g(s)$ of $D_G(\omega)$.

Now assume $L_{k_\varepsilon}(\omega^\alpha)$ has a simple pole at $s = 1/\alpha$ which is possible if and only if $\omega^\alpha \circ N_{k_\varepsilon/k}$ is trivial on idèles of k_ε of norm one. In this case we have two different situations. If $\omega^\alpha \circ N_{k_0/k}$ is trivial on idèles of k_0 of norm one then $L_{k_0}(\omega^\alpha)$ has also a simple pole at $s = 1/\alpha$. Then the poles cancel and the quotient $L_{k_\varepsilon}(\omega^\alpha)/L_{k_0}(\omega^\alpha)$ is a non-zero analytic function for $\mathrm{Re}(\omega) \geq 1/\alpha$. Once again a single-valued dth root can be defined. Hence $F_{H,S}(\omega^{|G|/|H|}; \varepsilon)$ has a pole of order at most $(Q^{\beta_H - m} - 1)/d$ at $s = 1/\alpha$. The maximum possible order of the pole is $\nu = (Q^\beta - 1)/d$. Therefore $F_{H,S}(\omega^{|G|/|H|}; \varepsilon)$ with $\beta_H = \beta$ and $k_0 = k_\varepsilon$ contribute to $g_0(s)/(s - 1/\alpha)^\nu$ and the rest to $g_j(s)/(s - 1/\alpha)^{a_j}$ with $a_j = (Q^{j-1} - 1)/d$ for $1 \leq j \leq \beta$.

The only case left is when $L_{k_\varepsilon}(\omega^\alpha)$ has a pole at $s = 1/\alpha$ but $L_{k_0}(\omega^\alpha)$ does not. In this case since $k_\varepsilon \neq k_0$ we have $m \geq 1$. Since $(s - 1/\alpha) L_{k_\varepsilon}(\omega^\alpha) L_{k_0}(\omega^\alpha)^{-1}$ is analytic and non-zero for $\mathrm{Re}(\omega) \geq 1/\alpha$ it is possible to define a single-valued analytic branch of the dth root. Then we can write $F_{H,S}(\omega^{|G|/|H|}; \varepsilon) = (s - 1/\alpha)^{-Q^{\beta_H - m}/d} \widetilde{g}(s)$ for $\mathrm{Re}(\omega) > 1/\alpha$ for some function $\widetilde{g}(s)$ analytic for $\mathrm{Re}(s) \geq 1/\alpha$, where $1 \leq m \leq \beta_H$. So $F_{H,S}(\omega^{|G|/|H|}; \varepsilon)$ contributes to $g(s)$ if $m = \beta_H$ and to one of the $g_j(s)/(s - 1/\alpha)^{a_j}$ with $a_j = Q^{j-\beta}/d$ for $\beta + 1 \leq j \leq 2\beta - 1$ otherwise. Note that the maximum of such a_j is less than ν. ∎

Since $D_{G,\mathfrak{c}}(s)$ is a linear combination of $D_G(\omega)$'s we see that

$$c(k, G, \mathfrak{c}) = \lim_{s \to 1/\alpha} (s - 1/\alpha)^\nu D_{G,\mathfrak{c}}(s)$$

exists. First we will show that the above limit is non-negative. Then we will determine the ideal classes for which it is positive.

We will follow the same line of thought as in [9] except that we will have twists by characters ψ of Cl_k. Let $L(s) = \zeta_{k_0}(s)$ and $r_0 = \mathrm{res}_{s=1} \zeta_{k_0}(s)$. We can rewrite $c(k, G, \mathfrak{c})$ as

$$c(k, G, \mathfrak{c}) = \left(\frac{r_0}{\alpha}\right)^\nu \lim_{s \to 1/\alpha} \frac{D_{G,\mathfrak{c}}(s)}{L(\alpha s)^\nu}.$$

Then, putting (8), (2) and (4) together we get

$$c(k, G, \mathfrak{c}) = \frac{(r_0 \alpha^{-1})^\nu}{\phi(G) h_k} \sum_{\psi \in \widehat{Cl}_k,\, H \subset G} \psi(\mathfrak{c}^{-1}) \frac{\mu(G/H)}{e_H(S)} \sum_{\varepsilon \in \mathcal{E}_H(S)} r_S(H; \psi; \varepsilon),$$

where

$$r_S(H;\psi;\varepsilon)=\prod_v \frac{F_{H,v}(\omega_{\psi,1/\alpha}^{|G|/|H|};\varepsilon)}{L_v(1/\alpha)} \tag{10}$$

with $F_{H,v}(\omega;\varepsilon)$ and $L_v(s)$ being the individual factors in the Euler product decompositions of $F_{H,S}(\omega;\varepsilon)$ and $\zeta_{k_0}(s)$ respectively and the product is over all primes v of k. We know that the product in (10) converges by the argument above. Now let

$$R(\mathfrak{c})=\frac{1}{h_k}\sum_{\psi}\psi(\mathfrak{c}^{-1})\sum_{H\subset G}\frac{\mu(G/H)}{e_H(S)}\sum_{\varepsilon\in\mathcal{E}_H(S)} r_S(H;\psi;\varepsilon).$$

We know that $\sum_{\mathfrak{c}} R(\mathfrak{c})$ is positive by the proof of Theorem 6.1 in [9]. We will show below that each $R(\mathfrak{c})\geq 0$. The question is then to determine the classes $\mathfrak{c}$ for which we get a positive value for $R(\mathfrak{c})$. Let T be a set of primes containing S and look at a combination of partial products given by

$$R_T(\mathfrak{c})=\frac{1}{h_k}\sum_{\psi}\psi(\mathfrak{c}^{-1})\sum_{H\subset G}\frac{\mu(G/H)}{e_H(S)}\sum_{\varepsilon\in E_H(S)} r_S^T(H;\psi;\varepsilon), \tag{11}$$

where the definition of $r_S^T(H;\psi;\varepsilon)$ is similar to the definition of $r_S(H;\psi;\varepsilon)$ given by (10) with the product being restricted to the primes of T. We start by simplifying the factors in the product of $r_S^T(H;\psi;\varepsilon)$. From (6) we have

$$F_{H,v}(\omega_{\psi,1/\alpha}^{|G|/|H|};\varepsilon)=\sum_{\chi}\chi(\varepsilon)(\omega_{\psi,1/\alpha}^{|G|/|H|})_v(\Phi_H(\chi)),$$

where the sum is over characters in $C_H(k_v^\times)$ if $v\in S$ and over characters in $C_H(O_v^\times)$ otherwise. Then the local conductor-discriminant formula implies that

$$F_{H,v}(\omega_{\psi,1/\alpha}^{|G|/|H|};\varepsilon)=\sum_{\chi}\chi(\varepsilon)(\omega_{\psi,1/\alpha}^{|G|/|H|})_v(\Delta(K_\chi/k_v)^{|H|/|J|}),$$

where K_χ is the extension corresponding to $U_\chi=\bigcap_{1\leq j\leq l}\ker\chi_j$ provided by local class field theory and J is the Galois group of K_χ/k_v. After simplification we get

$$\frac{F_{H,v}(\omega_{\psi,1/\alpha}^{|G|/|H|};\varepsilon)}{L_v(1/\alpha)}=\sum_{\chi}\chi(\varepsilon)\mathcal{D}(\chi,\psi),$$

where

$$\mathcal{D}(\chi,\psi_v)=L_v(1/\alpha)^{-1}\psi_v^{|G|/|J|}(\Delta(K_\chi/k_v))|\Delta(K_\chi/k_v)|_v^{1/|J|(1-Q^{-1})}.$$

Note that $\mathcal{D}(\chi,\psi)$ depends only on ψ and U_χ. Now let

$$k_T^\times=\prod_{v\in S}k_v^\times\times\prod_{v\in T\setminus S}O_v^\times$$

and for $\chi = (\chi_v) \in C_H(k_T^\times)$ let $\mathcal{D}(\chi, \psi) = \prod_{v\in T} \mathcal{D}(\chi_v, \psi_v)$. Similarly define $\chi(\varepsilon) = \prod_{v\in T} \chi_v(\varepsilon)$ for any $\varepsilon \in O_S^\times$. We have

$$r_S^T(H; \psi; \varepsilon) = \sum_{\chi\in C_H(k_T^\times)} \chi(\varepsilon)\mathcal{D}(\chi, \psi).$$

Substituting this expression into (11), using orthogonality of characters χ and interchanging the order of summation we get

$$R_T(\mathfrak{c}) = \sum_{H\subset G} \mu(G/H) \sum_{\substack{\chi\in C_H(k_T^\times)\\ U_\chi\supset O_S^\times}} \Big(\frac{1}{h_k} \sum_{\psi} \psi(\mathfrak{c}^{-1})\mathcal{D}(\chi, \psi)\Big).$$

This time we use the orthogonality of the characters ψ. For an open subgroup $U \subset k_T^\times$ let

$$\widetilde{\mathfrak{c}}(U) = \text{class of } \Big(\prod_{v\in T} \Delta(K_{U_v}/k_v)^{|G|/|J|}\Big) \tag{12}$$

in the ideal class group, where $U_v = k_v^\times \cap U$, K_{U_v} is the extension corresponding to U_v and J is the Galois group of K_{U_v}/k_v. Then

$$R_T(\mathfrak{c}) = \sum_{H\subset G} \mu(G/H) \sum_{\substack{\chi\in C_H(k_T^\times)\\ U_\chi\supset O_S^\times, \widetilde{\mathfrak{c}}(U_\chi)=\mathfrak{c}}} \mathcal{D}(\chi, 1).$$

Since $\mathcal{D}(\chi, 1)$ depends only on U_χ we write $\mathcal{D}(\chi, 1) = \mathcal{D}(U_\chi)$ and then $R_T(\mathfrak{c})$ becomes

$$R_T(\mathfrak{c}) = \sum_{H\subset G} \mu(G/H) \sum_{J\subset H} \phi(J) \sum_{\substack{k_T^\times/U\cong J\\ U\supset O_S^\times, \widetilde{\mathfrak{c}}(U)=\mathfrak{c}}} \mathcal{D}(U)$$

and finally applying Möbius inversion we get

$$R_T(\mathfrak{c}) = \phi(G) \sum_{\substack{k_T^\times/U\cong G\\ U\supset O_S^\times, \widetilde{\mathfrak{c}}(U)=\mathfrak{c}}} \mathcal{D}(U). \tag{13}$$

Clearly, this expression is non-negative. Whether or not it is positive depends on the existence of subgroups U with the desired properties. We will come back to this question shortly. First, we exhibit the relation between the positivity of $R_T(\mathfrak{c})$ and that of $R(\mathfrak{c}) = \lim_{T\to M_k} R_T(\mathfrak{c})$.

PROPOSITION 4. *Let T be a set of primes containing S, and let $R_T(\mathfrak{c})$ and $R(\mathfrak{c})$ be defined as above. Then $R(\mathfrak{c}) > 0$ if and only if $R_{T_0}(\mathfrak{c}) > 0$ for some T_0.*

Proof. Since $R(\mathfrak{c}) = \lim_{T\to M_k} R_T(\mathfrak{c})$ one way is clear. For the converse, assume there exists a T_0 with $R_{T_0}(\mathfrak{c}) > 0$. Then there exists a $U_0 \subset k_{T_0}^\times$

such that $k_{T_0}^\times/U_0 \cong G$, $U_0 \supset O_S^\times$ and $\widetilde{\mathfrak{c}}(U_0) = \mathfrak{c}$. Let T be any set of primes containing T_0 and let $n = n_1$ be the exponent of G. For a complete set of representatives $\{a_1, \dots, a_r\}$ of $O_S^\times/O_S^n$ and ζ_n a primitive nth root of unity, define $\widetilde{k} = k(\zeta_n, \sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$. Let H_k be the Hilbert class field of k. Let $\widetilde{T}$ be the set of primes of k which split completely in the compositum $\widetilde{k}H_k$. Then for any prime v in $\widetilde{T}$, $q_v \equiv 1 \pmod n$ and $a_i^{(q_v-1)/n} \equiv 1 \pmod v$. Also since v splits in H_k it is principal. Now for any $U \subset k_T^\times$ such that $U \cap k_{T_0}^\times = U_0$ we have $k_T^\times/U \cong G$. Moreover, if $U_v = O_v^\times$ for any $v \notin T_0 \cup \widetilde{T}$ then $\widetilde{\mathfrak{c}}(U) = \widetilde{\mathfrak{c}}(U_0) = \mathfrak{c}$ and $O_S^\times \subset U$. Restricting the sum in (13) to such open U we have

$$R_T(\mathfrak{c}) \geq \Phi(G) \sum_U \mathcal{D}(U).$$

Taking the limit as $T \to M_k$ we have

$$R(\mathfrak{c}) \geq \Phi(G)\mathcal{D}(U_0) \prod_{v \in \widetilde{T} \setminus T_0} \Big(\sum_{\chi \in C_G(O_v^\times)} |\Phi_G(\chi)|_v \Big)$$

and the right hand side is positive. ∎

Now we return to the question of determining the classes $\mathfrak{c}$ which have $R(\mathfrak{c}) > 0$ and prove our main theorem.

THEOREM 5. *Let k be a number field, G be an abelian group and $\mathfrak{c}$ an element of the ideal class group of k. Let $N(k, g, \mathfrak{c}; X)$ be the number of normal extensions k'/k with Galois group isomorphic to G, $(\Delta(k'/k)) \in \mathfrak{c}$ and the norm of $(\Delta(k'/k))$ be less than or equal to X. If there exists an extension k'/k such that $\mathrm{Gal}(k'/k) \cong G$ and $(\Delta(k'/k)) \in \mathfrak{c}$ then there exists a constant $c(k, G, \mathfrak{c}) > 0$ such that*

$$N(k, G, \mathfrak{c}; X) \sim \frac{c(k, G, \mathfrak{c})\alpha}{(\nu - 1)!} X^{1/\alpha} (\log X)^{\nu - 1}$$

as $X \to \infty$, where α and ν are the constants depending on G and k defined above.

Proof. Let k'/k be an extension such that $\mathrm{Gal}(k'/k) \cong G$ and $(\Delta(k'/k)) \in \mathfrak{c}$. Let $U \subset A_k^\times$ be the corresponding open subgroup containing $k^\times$ provided by class field theory. Let S be a set of primes containing the infinite primes and the primes dividing $(\Delta(k'/k))$ such that $O_S^\times$ is a principal ideal domain. For $T = S$ let $k_v^\times = \prod_{v \in T} k_v^\times$ and let $U_T = U \cap k_T^\times$. Then the components of the discriminant idèle $\Delta(k'/k)$ are given by

$$\Delta(k'/k)_v = \Delta(K_{U_v}/k_v)^{|G|/|J|},$$

where $U_v = k_v^\times \cap U = k_v^\times \cap U_T$, K_{U_v} is the extension corresponding to U_v by class field theory and J is the Galois group of K_{U_v}/k_v. Since T contains all

the primes for which $\Delta(k'/k)_v$ might be a non-unit, from (12) we see that $\widetilde{\mathfrak{c}}(U_T) = \mathfrak{c}$. The map

$$A_k^\times \to k_T^\times / U_T, \qquad (x_v)_{v\in M_k} \mapsto (x_v)_{v\in T} \bmod U_T,$$

is surjective and has kernel U by construction so $G \cong \mathrm{Gal}(k'/k) \cong A^\times/U \cong k_T^\times/U_T$. Finally, since $k^\times \subset U$ we have $O_S^\times \subset U_T$. Now by Proposition 4 above, $R(\mathfrak{c}) > 0$, which implies that $c(k, G, \mathfrak{c}) > 0$. Now by a standard Tauberian argument (see for example [7, Appendix I]) we get the desired result. ∎

4. Cyclic extensions of prime degree. In general $c(k, G, \mathfrak{c})$ is a complicated expression. Even

$$c(k, G) = \lim_{s\to 1/\alpha} (s - 1/\alpha)^\nu D_G(s),$$

which gives the density of extensions with a given abelian Galois group, is very hard to compute in general. See [2] for the case of cyclic extensions of prime order and [1] for a survey of discriminant counting in general. In the simplest case $G = \mathbb{Z}/Q\mathbb{Z}$, where Q is a prime number. In this case $\alpha = Q - 1$. Since G has only two subgroups, the trivial subgroup and itself, we only need two terms for the sum in (4). For the trivial subgroup, $F_1(\omega) = 1$ for any ω which does not contribute to the singularity. In order to calculate $F_G(\omega)$ let S be a set of primes of k containing the infinite ones and the ones above the prime Q such that $O_S^\times$ is a principal ideal. Let $\varepsilon \in O_S^\times / O_S^Q$. From the discussion in the proof of Proposition 3 in calculating $c(k, G, \mathfrak{c})$ we can restrict the sum in (8) to the characters ψ with the property $\psi^{Q-1} \circ N_{k_0/k} = 1$ and the sum in (4) to ε such that $k_\varepsilon = k_0$, where $k_0 = k(\zeta_Q)$ and $k_\varepsilon = k_0(\sqrt[Q]{\varepsilon})$. We make these assumptions when we calculate the terms of the Euler products below. Also for any $\chi \in C_G(O_v^\times)$ we have $\Phi_G(\chi) = \Phi(\chi)^{Q-1}$ because $\ker \chi^i = \ker \chi$ for $1 \le i \le Q - 1$.

For $v \notin S$ the Euler factor of $F_G(\omega; \varepsilon)$ corresponding to v is given by

$$\sum_{\chi\in C_G(O_v^\times)} \chi(\varepsilon)\omega_v(\Phi_G(\chi))$$

in (6). Since v does not divide Q there will be a non-trivial character in $C_G(O_v^\times)$ if and only if $Q \,|\, (q_v - 1)$ and its conductor will be π_v. If χ is one such character all the others will be given by $\sigma \circ \chi$, where σ runs through automorphisms of the Qth roots of unity. When $Q \,|\, (q_v - 1)$ the prime v splits in k_0. But we are assuming that $k_\varepsilon = k_0$ so ε is a Qth power in $O_v^\times$ and therefore $\chi(\varepsilon) = 1$ for all χ. Since we are also assuming $\psi^{Q-1} \circ N_{k_0/k} = 1$

we have

$$F_{G,v}(\omega_{\psi,s};\varepsilon)=\begin{cases}1+(Q-1)q_v^{(1-Q)s} & \text{if } v \text{ splits in } k_0,\\ 1 & \text{otherwise,}\end{cases}$$

independently of ψ and ε.

For the infinite primes we have two cases. If $k_v=\mathbb{C}$ then $F_{G,v}(\omega;\varepsilon)=1$ for any G, ω and ε. If $k_v=\mathbb{R}$ and Q is odd then $F_{G,v}(\omega_{\psi,s};\varepsilon)=1$ for any ω and ε. If $k_v=\mathbb{R}$ and $Q=2$ then $F_{G,v}(\omega_{\psi,s};\varepsilon)=1+\operatorname{sign}(\sigma_v(\varepsilon))$ for any of the ω_ψ, where σ_v is the embedding of k into $\mathbb{R}$ defining v. Therefore $F_{G,v}(\omega_{\psi,s};1)=2$ if $G=\mathbb{Z}/2\mathbb{Z}$ since in this case $k=k_0=k_\varepsilon$ implies ε is a square.

For the finite primes in S not dividing Q a character of $C_G(k_v^\times)$ is given by a character of $C_G(O_v^\times)$ multiplied by a character of order dividing Q on the infinite cyclic group generated by π_v. The former are constructed as in the case of $v\notin S$ above. If v does not split in k_0 then $C_G(O_v^\times)=1$. The latter are given by $\pi_v^n\to\zeta_Q^{ni}$ where ζ_Q is a primitive Qth root of unity and $0\le i\le Q-1$. We have

$$F_{G,v}(\omega_{\psi,s};\varepsilon)=\begin{cases}Q(1+(Q-1)q_v^{(1-Q)s}) & \text{if } v \text{ splits in } k_0,\\ Q & \text{otherwise.}\end{cases}$$

Now let

$$F_Q(\omega;\varepsilon)=\prod_{v\mid Q}F_{G,v}(\omega;\varepsilon).$$

Also define

$$H_0=\{\psi\in Cl_k:\psi^{Q-1}\circ N_{k_0/k}=1\},$$
$$L=\{\varepsilon\in O_s^\times/O_s^Q:k_\varepsilon=k_0\}.$$

Since $F_{G,v}(\omega_{\psi,s};\varepsilon)=F_{G,v}(\omega_s;1)$ independently of ψ and ε, when $v\nmid Q$ we get

$$D_{G,\mathfrak{c}}(s)=\frac{1}{\phi(G)h_k}\prod_{v\nmid Q}F_{G,v}(\omega_s;1)\sum_{\psi\in H_0,\,\varepsilon\in L}\frac{\psi(\mathfrak{c}^{-1})}{e_G(S)}F_Q(\omega_{\psi,s};\varepsilon)+g_1(s)$$

for some $g_1(s)$ with $\lim_{s\to1/\alpha}(s-1/\alpha)^v g_1(s)=0$. Similarly

$$D_G(s)=\frac{1}{\phi(G)}\prod_{v\nmid Q}F_{G,v}(\omega_s;1)\,\frac{1}{e_G(S)}\sum_{\varepsilon\in L}F_Q(\omega_s;\varepsilon)+g_2(s)$$

for some $g_2(s)$ with $\lim_{s\to1/\alpha}(s-1/\alpha)^v g_2(s)=0$. Therefore we have

$$c(k,G,\mathfrak{c})=c(k,G)\,\frac{\frac{1}{h_k}\sum_{\psi\in H_0,\,\varepsilon\in L}\psi(\mathfrak{c}^{-1})F_Q(\omega_{\psi,1/(Q-1)};\varepsilon)}{\sum_{\varepsilon\in L}F_Q(\omega_{1/(Q-1)};\varepsilon)}.$$

Although this is a messy expression, it is a finite calculation which gives a positive result if $\mathfrak{c}$ is a realizable class by Theorem 5. In the simpler case when k contains a primitive Qth root of unity, we have $k = k_0$ so $k_\varepsilon = k$ means $\varepsilon \in O_S^\times$ and hence we can take $L = \{1\}$. In that case we get

$$c(k, G, \mathfrak{c}) = c(k, G)\,\frac{|Cl_k/Cl_k^{Q-1}|}{h_k},$$

where Cl_k is the ideal class group of k and Cl_k^{Q-1} is its subgroup consisting of $(Q-1)$st powers.

Since we have most of the ingredients we will finish by calculating $c(k, G)$ in this simple case where k contains the Qth roots of unity. We only need to determine $F_{G,v}(\omega_s; 1)$ for $v \mid Q$ since the other factors are already determined above. We know

$$F_{G,v}(\omega_s; 1) = Q \sum_{\chi \in C_G(O_v^\times)} |\Phi(\chi)|_v^{(Q-1)s}.$$

Since Q is prime to $q_v - 1$, if a character χ of $O_v^\times$ has conductor π_v^n then $n \geq 2$. Let c_n be the number of open subgroups U of $O_v^\times$ such that $U \supseteq 1 + \pi_v^n O_v^\times$ and $O_v^\times/U \cong \mathbb{Z}/Q\mathbb{Z}$. Then c_n is equal to the number of surjective maps $O_v^\times/(1+\pi_v^n O_v^\times) \to \mathbb{Z}/Q\mathbb{Z}$, which by duality is the number of subgroups of $O_v^\times/(1+\pi_v^n O_v^\times)$ of order Q. Therefore $(Q-1)c_n$ is the number of elements of $O_v^\times/(1+\pi_v^n O_v^\times)$ of order Q. The structure of the group $O_v^\times/(1+\pi_v^n O_v^\times)$ is completely determined in [6]. In particular the Q-rank r_n of $O_v^\times/(1+\pi_v^n O_v^\times)$ is given by

$$r_n = \begin{cases} \left((n-1) - \left\lfloor \dfrac{n-1}{Q} \right\rfloor\right) f & \text{if } 1 \leq n \leq \dfrac{eQ}{Q-1}, \\ ef + 1 & \text{if } n > \dfrac{eQ}{Q-1}, \end{cases}$$

where $\lfloor \cdot \rfloor$ denotes the greatest integer function, e is the absolute ramification of the prime v over the rational prime Q and f is its degree. Note that since $k_0 = k$ we have $(Q-1) \mid e$. Therefore,

$$F_{G,v}(\omega_s; 1) = Q\left(1 + \sum_{n=2}^{eQ/(Q-1)} \frac{Q^{r_n} - Q^{r_{n-1}}}{q_v^{(Q-1)s}}\right),$$

which after simplification gives

$$F_{G,v}(\omega_s; 1) = Q\left(1 + \frac{Q-1}{q_v^{(Q-1)s}}\right).$$

Finally, putting all the terms together and substituting $\alpha = \nu = Q - 1$ we

have

$$\begin{aligned} c(k,G) &= \lim_{s\to 1/\alpha} (s-1/\alpha)^{\nu} D_G(s) \\ &= \frac{1}{\alpha^{\nu}} \frac{1}{\phi(G)e_G(S)} \lim_{s\to 1/\alpha} (\alpha s-1)^{\nu} \prod_v F_{G,v}(\omega_s;1) \\ &= \frac{1}{\alpha^{\nu}} \frac{Q^{|S|-r_2}}{\phi(G)e_G(S)} \lim_{s\to 1}(s-1)^{\nu} \prod_{v\notin M_\infty} (1+(Q-1)q_v^{(1-Q)s}) \\ &= \frac{\zeta_k(1)^{Q-1}Q^{1-r_2}}{(Q-1)^Q} \prod_{v\notin M_\infty} \left(1+\frac{Q-1}{q_v^{(Q-1)s}}\right)\left(1-\frac{1}{q_v}\right)^{Q-1}. \end{aligned}$$

We have proven

PROPOSITION 6. *Let Q be a prime number, $G=\mathbb{Z}/\mathbb{Z}Q$ and let k be a number field containing the Qth roots of unity. Let $N(k,G;X)$ be the number of Galois extensions k'/k with Galois group isomorphic to G and norm of the discriminant less than or equal to X. Then*

$$N(k,G;X) \sim \frac{\kappa^{\alpha}(\alpha+1)^{1-r_2}}{\alpha^{\alpha-1}\alpha!} \prod_v \left(\left(1+\frac{\alpha}{q_v^{\alpha}}\right)\left(1-\frac{1}{q_v}\right)^{\alpha}\right) X^{1/\alpha}(\log X)^{\alpha-1}$$

as $X\to\infty$, where r_2 is the number of pairs of complex places of k, $\alpha=Q-1$, $\kappa=\operatorname{res}_{s=1}\zeta_k(s)$ and the product is over the finite primes of k.

The above proposition appears as a corollary to the main theorem in [2] where the general case of prime cyclic extensions without the restriction that k contains the Qth roots of unity is solved.

References

[1] H. Cohen, *Constructing and counting number fields*, in: Proceedings of the International Congress of Mathematicians (Beijing, 2002), Vol. II, Higher Ed. Press, Beijing, 2002, 129–138.

[2] H. Cohen, F. Diaz y Diaz and M. Olivier, *On the density of cyclic extensions of prime degree*, J. Reine Angew. Math. 550 (2002), 169–209.

[3] S. Delsarte, *Fonctions de Möbius sur les groupes abéliens finis*, Ann. of Math. (2) 49 (1948), 600–609.

[4] A. Fröhlich, *Discriminants of algebraic number fields*, Math. Z. 74 (1960), 18–28.

[5] L. R. McCulloh, *Galois module structure of abelian extensions*, J. Reine Angew. Math. 375/376 (1987), 259–306.

[6] N. Nakagoshi, *The structure of the multiplicative group of residue classes modulo $\mathfrak{p}^{N+1}$*, Nagoya Math. J. 73 (1979), 41–60.

[7] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, PWN–Polish Sci. Publ., Warszawa, 1974.

[8] A. Weil, *Basic Number Theory*, Springer, Berlin, 1995.

[9] D. Wright, *Discriminants of abelian extensions*, Proc. London Math. Soc. (3) 58 (1989), 17–50.

Faculty of Engineering and Natural Sciences
Sabanci University
Orhanli, Tuzla
34956 Istanbul, Turkey
E-mail: ebekyel@sabanciuniv.edu

Received on 5.2.2004
and in revised form on 2.8.2004 (4711)