Astérisque

WOLFGANG M. SCHMIDT

Number fields of given degree and bounded discriminant

Astérisque, tome 228 (1995), p. 189-195

<http://www.numdam.org/item?id=AST_1995__228__189_0>

NUMBER FIELDS OF GIVEN DEGREE AND BOUNDED DISCRIMINANT

Wolfgang M. Schmidt[†]

1. Introduction. Let $N(d;X)$ be the number of algebraic number fields of degree d and discriminant Δ with $|\Delta| \leqq X$. It has been conjectured (but I don't know to whom to attribute this conjecture) that for each fixed $d > 1$ we have $N(d;X) \sim c_d X$ as $X \to \infty$, with a constant $c_d > 0$. This is easy to see when $d = 2$, and has been established for $d = 3$ by Davenport and Heilbronn [3]. For $d = 4$ Bailey [1] could show that $X \ll N(4;X) \ll X^{3/2}(\log X)^4$. The goal of the present note is an easy proof of

$$N(d;X) \ll X^{(d+2)/4}. \tag{1.1}$$

For $d = 4$ this improves slightly upon Bailey. In fact, for given $d_1 > 1, \ldots, d_t > 1$ and a number field L, let $N(L; d_1, \ldots, d_t; X)$ be the number of chains of fields $L = K_0 \subset K_1 \subset \cdots \subset K_t = K$ with degrees $[K_j : K_{j-1}] = d_j$ $(j = 1, \ldots, t)$ and with discriminant $\Delta(K)$ of modulus $\leqq X$. We will show that

$$N(L; d_1, \ldots, d_t; X) \ll (X/|\Delta(L)|)^{(d+2)/4} |\Delta(L)|^{-1/2\ell}, \tag{1.2}$$

where $d = \max(d_1, \ldots, d_t)$, $\ell = \deg L$, and where the constant in $\ll$ depends only on d, t, ℓ. The case when $L = \mathbb{Q}$, $t = 2$, $d_1 = d_2 = 2$ is contained in Bailey's work [1]. In many cases when $d_t < d$, the exponent $(d+2)/4$ could be reduced. The exponent $-1/2\ell$ of $|\Delta(L)|$ could always be reduced; in fact the main purpose of the factor $|\Delta(L)|^{-1/2\ell}$ will be to be able to carry out an induction on t.

Related to our topic is the important work of D. J. Wright [4] on abelian extensions. Given a finite abelian group G of order $|G|$ and with

---

AMS Classification Number: 11R04 (Algebraic Number Theory: general)

[†] Supported in part by NSF grant DMS–9108581.

Q the smallest prime divisor of $|G|$, set $\alpha(G) = |G|(1 - Q^{-1})$. Then the number of abelian number fields with Galois group G and discriminant of modulus $\leqq X$ is $\sim cX^{1/\alpha}(\log X)^{\beta}$ where $c = c(G) > 0$, $\beta = \beta(G) \geqq 0$. Therefore if the above mentioned conjecture is correct, the main contribution to the asymptotic formula would come from nonabelian extensions.

2. Geometry of Number Fields. When K is a number field of degree k and $\sigma_1, \dots, \sigma_k$ are the embeddings of K into $\mathbb{C}$, write $k = r + 2s$ and suppose that $\sigma_1, \dots, \sigma_r$ are real, and $\sigma_{r+i}, \sigma_{r+s+i}$ for $i = 1, \dots, s$ are pairs of complex conjugates. For $\alpha \in K$ set $\alpha^{(j)} = \sigma_j(\alpha)$ $(j = 1, \dots, k)$. Let $\underline{\underline{\varphi}}_K$ be the map $K \rightarrow \mathbb{R}^k$ with

$$\underline{\underline{\varphi}}_K(\alpha) = (\alpha^{(1)}, \dots, \alpha^{(r)}, \sqrt{2}\,\mathrm{Re}\,\alpha^{(r+1)}, \sqrt{2}\,\mathrm{Im}\,\alpha^{(r+1)}, \dots, \sqrt{2}\,\mathrm{Re}\,\alpha^{(r+s)},$$
$$\sqrt{2}\,\mathrm{Im}\,\alpha^{(r+s)}).$$

Let $\mathfrak{O}_K$ be the ring of integers in K; then $\underline{\underline{\varphi}}_K(\mathfrak{O}_K) = \Lambda_K$, say, is a lattice in $\mathbb{R}^k$ of determinant

$$\mathrm{Det}\,\Lambda_K = |\Delta(K)|^{1/2}.$$

Finally, let $\kappa_1, \dots, \kappa_k$ be the successive minima of Λ_K (with respect to the Euclidean norm) in the sense of Minkowski. There are $\alpha_1, \dots, \alpha_k$ in $\mathfrak{O}_K$, linearly independent over $\mathbb{Q}$, with

$$|\underline{\underline{\varphi}}_K(\alpha_j)| = \kappa_j \qquad (j = 1, \dots, k), \tag{2.1}$$

where $|\cdot|$ denotes the Euclidean norm. As is well known,

$$\kappa_1 \cdots \kappa_k \gg\ll \mathrm{Det}\,\Lambda_K = |\Delta(K)|^{1/2} \tag{2.2}$$

where the implied constants depend on k only. Each $\alpha \in \mathbb{Q}$ has

$$|\underline{\underline{\varphi}}_K(\alpha)| = \sqrt{k}\,|\alpha|, \tag{2.3}$$

in particular $|\underline{\underline{\varphi}}_K(1)| = \sqrt{k}$, so that $\kappa_1 \leqq \sqrt{k}$. On the other hand, $\alpha \neq 0$ in $\mathfrak{O}_K$ has

$|\alpha^{(1)} \cdots \alpha^{(r)}||\alpha^{(r+1)} \cdots \alpha^{(r+s)}|^2 \geqq 1$, so that by the arithmetic–geometric inequality

$$|\alpha^{(1)}|^2 + \cdots + |\alpha^{(r)}|^2 + 2|\alpha^{(r+1)}|^2 + \cdots + 2|\alpha^{(r+s)}|^2 \geqq k,$$

i.e., $|\underline{\underline{\varphi}}_K(\alpha)|^2 \geqq k$. We may conclude that

$$\kappa_1 = \sqrt{k}\ . \tag{2.4}$$

Let L be a subfield of K of degree ℓ. Denote the conjugates of $\alpha \in L$ by $\alpha^{[1]}, \ldots, \alpha^{[\ell]}$. (We can't write them as $\alpha^{(1)}, \ldots, \alpha^{(\ell)}$ since the maps $\sigma_1, \ldots, \sigma_\ell$ (among the maps $\sigma_1, \ldots, \sigma_k$ given above) do not necessarily give the distinct embeddings of L into $\mathbb{C}$.) We define $\underline{\underline{\varphi}}_L$, Λ_L and successive minima $\lambda_1, \ldots, \lambda_\ell$ in the obvious way. It is easily seen that $\alpha \in L$ has $|\underline{\underline{\varphi}}_K(\alpha)| = \sqrt{d}\ |\underline{\underline{\varphi}}_L(\alpha)|$ where $d = [K : L]$; this generalizes (2.3). The image $\Lambda'_L = \underline{\underline{\varphi}}_K(\mathfrak{O}_L)$ is therefore isometric to $\sqrt{d}\ \Lambda_L$, and the minima $\lambda'_1, \ldots, \lambda'_\ell$ of Λ'_L have

$$\lambda'_j = \sqrt{d}\ \lambda_j \qquad (j = 1, \ldots, \ell). \tag{2.5}$$

LEMMA 1.

$$\lambda_{\ell-j} \ll \kappa_{k-j} \qquad (0 \leqq j < \ell).$$

Proof. Let Tr denote the trace from K to L. It is a $\mathbb{Q}$-linear map whose image is L, so that its kernel (as a $\mathbb{Q}$-vector space) has dimension $\deg K - \deg L = k - \ell$. Let $\alpha_1, \ldots, \alpha_k$ be as in (2.1). Among $\beta_q = \operatorname{Tr} \alpha_q$ with $q = 1, \ldots, k-j$, there must therefore be at least $k - j - (k - \ell) = \ell - j$ linearly independent ones; say for $q_1, \ldots, q_{\ell-j}$. Then $\beta_{q_1}, \ldots, \beta_{q_{\ell-j}}$ are $\mathbb{Q}$-linearly independent elements of $\mathfrak{O}_L$ with

$$|\beta^{[i]}_{q_u}| \ll \max_t |\alpha^{(t)}_{q_u}| \leqq |\underline{\underline{\varphi}}_K(\alpha_{q_u})| = \kappa_{q_u} \leqq \kappa_{k-j}.$$

Therefore $|\underline{\underline{\varphi}}_L(\beta_{q_u})| \ll \kappa_{k-j}$ $(u = 1, \ldots, \ell - j)$, and the lemma follows.

By the argument leading to (2.4) we may set $\alpha_1 = 1$, so that $\alpha_1 \in \mathbb{Q} \subset L$.

LEMMA 2. *Let m be least with $\alpha_{m+1} \notin L$. Then*

$$|\Delta(L)|^{1/2}\kappa_{m+1}^{k-\ell} \ll |\Delta(K)|^{1/2}.$$

Proof. $\alpha_1, \dots, \alpha_m$ lie in L, and therefore $\lambda'_j = \kappa_j$, hence by (2.5), $\lambda_j \leqq \kappa_j$ for $j = 1, \dots, m$. On the other hand, $\lambda_{m+1} \cdots \lambda_\ell \ll \kappa_{k-\ell+m+1} \cdots \kappa_k$ by Lemma 1. Thus

$$|\Delta(L)|^{1/2} = \operatorname{Det} \Lambda_L \ll \lambda_1 \cdots \lambda_\ell \ll (\kappa_1 \cdots \kappa_m)(\kappa_{k-\ell+m+1} \cdots \kappa_k).$$

There are exactly $k - \ell$ integers strictly between m and $k - \ell + m + 1$, so that

$$|\Delta(L)|^{1/2}\kappa_{m+1}^{k-\ell} \ll \kappa_1 \cdots \kappa_k \ll |\Delta(K)|^{1/2}.$$

3. Proof of the main result. When the chain $L = K_0 \subset \cdots \subset K_t = K$ is refined by inserting extra fields, the quantity d can only decrease. Therefore we may restrict ourselves to saturated chains, i.e., chains where there is no field strictly between K_{j-1} and K_j $(j = 1, \dots, t)$. We will first deal with the case $t = 1$. Thus we consider fields $K \supset L$ with $[K : L] = d$ and no field strictly between L and K.

The lattice Λ_L has a basis $\underline{\underline{b}}_1, \dots, \underline{\underline{b}}_\ell$ with $\lambda_j \leqq |\underline{\underline{b}}_j| \ll \lambda_j$ $(j = 1, \dots, \ell)$ ([2, §VIII.5.2]), and such a basis has

$$|\underline{\underline{b}}_1| \cdots |\underline{\underline{b}}_\ell| \ll \operatorname{Det} \Lambda_L. \tag{3.1}$$

Let $\underline{\underline{b}}_1^*, \dots, \underline{\underline{b}}_\ell^*$ be the dual basis, so that the inner products $\underline{\underline{b}}_i \underline{\underline{b}}_j^* = \delta_{ij}$ $(1 \leqq i,\ j \leqq \ell)$, with δ_{ij} the Kronecker symbol. Further, with $\wedge$ denoting the exterior product,

$$\underline{\underline{b}}_j^* = (\underline{\underline{b}}_1 \wedge \cdots \wedge \underline{\underline{b}}_{j-1} \wedge \underline{\underline{b}}_{j+1} \wedge \cdots \wedge \underline{\underline{b}}_\ell)/\operatorname{Det} \Lambda_L,$$

so that

$$|\underline{\underline{b}}_j||\underline{\underline{b}}_j^*| \leqq |\underline{\underline{b}}_1| \cdots |\underline{\underline{b}}_\ell|/\operatorname{Det} \Lambda_L \ll 1 \tag{3.2}$$

by (3.1). Let $\beta_1, \dots, \beta_\ell$ be the elements in L with $\underline{\underline{\varphi}}_L(\beta_j) = \underline{\underline{b}}_j$ $(j = 1, \dots, \ell)$; then $\beta_1, \dots, \beta_\ell$ are a $\mathbb{Z}$-basis of $\mathfrak{O}_L$.

As in the last section, let m be least with $\alpha_{m+1} \notin L$. Set $\beta = \operatorname{Tr} \alpha_{m+1}$ and $\underline{\underline{b}} = \underline{\underline{\varphi}}_L(\beta)$. We may write $\beta = c_1\beta_1 + \cdots + c_\ell\beta_\ell$ with $c_j \in \mathbb{Z}$ $(j = 1, \dots, \ell)$, and then

$$(3.3) \qquad \underline{\underline{b}} = c_1\underline{\underline{b}}_1 + \cdots + c_\ell\underline{\underline{b}}_\ell.$$

Since $|\underline{\underline{\varphi}}_K(\alpha_{m+1})| = \kappa_{m+1}$, each conjugate of α_{m+1} has modulus $\leqq \kappa_{m+1}$, therefore each conjugate of β is $\ll \kappa_{m+1}$, and $|\underline{\underline{b}}| \ll \kappa_{m+1}$. The inner product of (3.3) with $\underline{\underline{b}}_j^*$ gives $\underline{\underline{b}}\underline{\underline{b}}_j^* = c_j$, so that

$$(3.4) \qquad |c_j| \ll \kappa_{m+1}|\underline{\underline{b}}_j^*| \ll \kappa_{m+1}/|\underline{\underline{b}}_j| \ll \kappa_{m+1}/\lambda_j$$

by (3.2). Set

$$\alpha = \alpha_{m+1} - [c_1/d]\beta_1 - \cdots - [c_\ell/d]\beta_\ell,$$

where [ ] denotes integer parts. Then

$$(3.5) \qquad \operatorname{Tr} \alpha = (c_1 - d[c_1/d])\beta_1 + \cdots + (c_\ell - d[c_\ell/d])\beta_\ell.$$

We also note that

$$(3.6) \qquad |\underline{\underline{\varphi}}_K(\alpha)| \ll \kappa_{m+1},$$

since $|\underline{\underline{\varphi}}_K(\alpha_{m+1})| = \kappa_{m+1}$, since $|\underline{\underline{\varphi}}_K(\beta_j)| = \sqrt{d}\ |\underline{\underline{\varphi}}_L(\beta_j)| = \sqrt{d}\ |\underline{\underline{b}}_j| \ll |\underline{\underline{b}}_j|$, and since $|c_j||\underline{\underline{b}}_j| \ll (\kappa_{m+1}/\lambda_j)\lambda_j$ by (3.4).

Now α satisfies

$$\alpha^d + \tau_1\alpha^{d-1} + \cdots + \tau_d = 0,$$

where $(-1)^j\tau_j$ is the j-th elementary symmetric polynomial in the conjugates of α over L. Here τ_j is in $\mathfrak{O}_L$, so that we may write

$$\tau_j = c_{j1}\beta_1 + \cdots + c_{j\ell}\beta_\ell \qquad (j = 1, \dots, d)$$

with coefficients $c_{jh} \in \mathbb{Z}$. Since $\tau_1 = -\operatorname{Tr} \alpha$, (3.5) shows that

$$(3.7) \qquad |c_{1h}| \leqq d \ll 1 \qquad (1 \leqq h \leqq \ell).$$

In view of (3.6), each conjugate of α is $\ll \kappa_{m+1}$, therefore each conjugate of τ_j is $\ll \kappa_{m+1}^j$, and $|\underline{\underline{\varphi}}_L(\tau_j)| \ll \kappa_{m+1}^j$. But

$$\underline{\underline{\varphi}}_L(\tau_j) = c_{j1}\underline{\underline{b}}_1 + \cdots + c_{j\ell}\underline{\underline{b}}_\ell,$$

and taking the inner product with $\underline{\underline{b}}_h^*$ we get

$$|c_{jh}| \leqq |\underline{\underline{\varphi}}_L(\tau_j)||\underline{\underline{b}}_h^*| \ll \kappa_{m+1}^j/\lambda_h \quad (2 \leqq j \leqq d,\ 1 \leqq h \leqq \ell) \tag{3.8}$$

by (3.2).

The number of possibilities for each c_{1h} is $\ll 1$ by (3.7), and the number of possibilities for c_{jh} with $2 \leqq j \leqq d$ is $\ll \kappa_{m+1}^j$, where we have not used the extra factor $1/\lambda_h$ in (3.8). The total number of possibilities for the coefficients c_{jh} is

$$\ll \kappa_{m+1}^{(2+3+\cdots+d)\ell} = \kappa_{m+1}^{\ell(d-1)(d+2)/2},$$

and by Lemma 2 this is

$$\ll (X/|\Delta(L)|)^{(d+2)/4}, \tag{3.9}$$

since $k - \ell = \ell(d-1)$ and since we consider fields K with $|\Delta(K)| \leqq X$. The number of possibilities for α is bounded by (3.9). But since $L \subset K$ is saturated and $\alpha \notin L$, we have $K = L(\alpha)$, so that K is determined by α.

To get the extra factor $|\Delta(L)|^{-1/2\ell}$ we proceed as follows. Either $\kappa_{m+1}^d \geqq \lambda_\ell$. Then by (3.8) the number of possibilities for c_{dh} is $\ll \kappa_{m+1}^d/\lambda_h$ ($h = 1, \ldots, \ell$), and altogether we save by a factor $(\lambda_1 \cdots \lambda_\ell)^{-1} \ll |\Delta(L)|^{-1/2}$. Or $\kappa_{m+1}^d < \lambda_\ell$, so that $\kappa_{m+1}^j < \lambda_\ell$ for $j = 2, \ldots, d$. By (3.8), the number of possibilities for $c_{j\ell}$ is $\ll 1$. Thus we save by a factor $(\kappa_{m+1}^{2+3+\cdots+d})^{-1}$, and the total number of possibilities for K is

$$\ll \kappa_{m+1}^{(2+3+\cdots+d)(\ell-1)} \ll (X/|\Delta(L)|)^{(1-(1/\ell))(d+2)/4}$$

by Lemma 2. Now it is well known that $\Delta(L)^d$ divides $\Delta(K)$, so that (if there is any field K as required) $X \geqq |\Delta(K)| \geqq |\Delta(L)|^d$, and we save (from (3.9)) by a factor

$$\ll (X/|\Delta(L)|)^{-(d+2)/4\ell} \ll |\Delta(L)|^{-(d-1)(d+2)/4\ell} \leqq |\Delta(L)|^{-1/\ell}.$$

This finishes the case $t = 1$.

To do an inductive argument from $t-1$ to t, we initially consider only chains $L = K_0 \subset K_1 \subset \cdots \subset K_{t-1} \subset K_t = K$ with $A \leqq |\Delta(K_{t-1})| < eA$, where A is given. The number of possibilities for $K_1, \ldots, K_{t-1}$ is

$$\ll (A/|\Delta(L)|)^{(d+2)/4} |\Delta(L)|^{-1/2\ell}.$$

Given K_{t-1}, the number of possibilities for K_t with $|\Delta(K_t)| \leqq X$ is

$$\ll (X/A)^{(d+2)/4} A^{-1/2\ell'},$$

where $\ell' = \deg K_{t-1} = \ell d_1 \cdots d_{t-1}$. Taking the product we get

$$\ll (X/|\Delta(L)|)^{(d+2)/4} |\Delta(L)|^{-1/2\ell} A^{-1/2\ell'}.$$

Taking the sum over $A = e^\nu$ with $\nu = 0, 1, \ldots$ we obtain (1.2).

References.

[1] A. M. Bailey. *On the density of discriminants of quartic fields*, J. Reine Angew. Math. **315** (1980), 190–210.

[2] J. W. S. Cassels. *An Introduction to the Geometry of Numbers*, Springer Grundlehren **99** (1959).

[3] H. Davenport and H. Heilbronn. *On the density of discriminants of cubic fields II.* Proc. Roy. Soc. London A322 (1971).

[4] D. J. Wright. *Distribution of discriminants of abelian extensions*, Proc. London Math. Soc., (3) **58** (1989), 17–50.

Wolfgang M. Schmidt
University of Colorado
Department of Mathematics
Boulder, Colorado 80309–0395 U.S.A.