ACTA ARITHMETICA
123.2 (2006)

On the number of integers represented by systems of Abelian norm forms

by

VALENTIN BLOMER (Toronto)
and JAN-CHRISTOPH SCHLAGE-PUCHTA (Freiburg)

1. Introduction and statement of results. In [11], Odoni gave (among other things) an asymptotic formula for the number $U_F(x)$ of positive integers not exceeding x that can be represented by a given norm form F. The error term, however, depends on the number field involved, and for applications often uniform results are required (see e.g. [1, 2]). In this paper we derive uniform estimates for $U_F(x)$ in the case of Abelian number fields. In fact, we consider the following more general situation:

Let $K_1, \ldots, K_m$ be finite Abelian extensions of $\mathbb{Q}$ of degrees $d_1, \ldots, d_m$ with pairwise coprime discriminants. For $j = 1, \ldots, m$ let $\mathcal{O}_j \subseteq K_j$ be the ring of integers. Choose an integral basis $\{\omega_{j,\nu} \mid 1 \le \nu \le d_j\}$ of $\mathcal{O}_j$ and let

$$F_j(\mathbf{x}) = N\Big(\sum_{\nu} \omega_{j,\nu} x_\nu\Big), \qquad \mathbf{x} = (x_\nu) \in \mathbb{Z}^{d_j},$$

be the corresponding norm form. A change of base in $\mathcal{O}_j$ yields a new form $F_j' = F_j \circ M$ with some $M \in \mathrm{GL}_{d_j}(\mathbb{Z})$. Thus F_j and F_j' represent the same integers. Let $U_{\mathbf{F}}(x)$ be the number of integers $n \le x$ such that the system of the m diophantine equations $|F_j(\mathbf{x}_j)| = n$ $(j = 1, \ldots, m)$ is solvable. In other words, $U_{\mathbf{F}}(x)$ is the number of integers $n \le x$ such that each field K_j contains an K_j-integer whose norm (in absolute value) is n.

The coprimality of the discriminants implies $K_i \cap K_j = \mathbb{Q}$ for $i \ne j$ (see e.g. [16, p. 322]). Let $L = K_1 \cdots K_m$. Then $\mathrm{Gal}(L/\mathbb{Q}) \cong \prod_{j=1}^m \mathrm{Gal}(K_j/\mathbb{Q})$ acts on $\underline{\mathfrak{C}} := \prod_{j=1}^m \mathfrak{C}_j$, the direct product of the class groups of the fields K_j. We write $h(k)$ for the class number of a number field k and define

$$\mathbf{h} := \prod_{j=1}^m h(K_j), \quad \Delta := |D_{L/\mathbb{Q}}|, \quad G := \mathrm{Gal}(L/\mathbb{Q}), \quad d_L := [L : \mathbb{Q}].$$

2000 *Mathematics Subject Classification*: 11D57, 11N25.
Key words and phrases: norm form equations, uniform asymptotic results.

Several times we shall use the bound $d_L \ll \log \Delta$. Here and henceforth all implicit and explicit constants do not depend on the fields involved, and they are also independent of m. Odoni's result implies (in the case $m = 1$)

$$U_{\mathbf{F}}(x) \sim c(\mathbf{F}) x (\log x)^{1/d_L - 1} \tag{1.1}$$

for fixed $K_1, \ldots, K_m$ and $x \to \infty$ where the constant $c(\mathbf{F})$ is neither very big nor very small. However, as we shall see below, in general this asymptotics becomes incorrect if Δ can increase (even moderately) with x.

In order to state the main result, we write, for $\alpha \in [0,1]$ and each subgroup $H \le G$,

$$E(\alpha, H) := -1 + \alpha(1 - \log(\alpha |H|)),$$
$$\operatorname{Fix} H := \{\mathbf{C} \in \underline{\mathfrak{C}} \mid \mathbf{C}^\sigma = \mathbf{C} \text{ for all } \sigma \in H\}.$$

We shall prove:

THEOREM 1. *Let $M > 0$ and $\varepsilon > 0$ be given. Let $x \ge x_0(M, \varepsilon)$, and assume $\Delta \le (\log x)^M$. Then*

$$U_{\mathbf{F}}(x) \gg_{M,\varepsilon} \max_{0 \le \alpha \le 1} \min_{H \le G} \frac{x (\log x)^{E(\alpha,H) - \varepsilon}}{|\operatorname{Fix} H|}. \tag{1.2}$$

If in addition $d_L = o(\log\log x)$, then

$$U_{\mathbf{F}}(x) \ll_{M,\varepsilon} \max_{0 \le \alpha \le 1} \min_{H \le G} \frac{x (\log x)^{E(\alpha,H) + \varepsilon}}{|\operatorname{Fix} H|}. \tag{1.3}$$

Theorem 1 follows directly from the following theorem. For $n \in \mathbb{N}$ and $\mathbf{C} = (C_1, \ldots, C_m) \in \underline{\mathfrak{C}}$ we write $n \in \mathcal{R}(\mathbf{C})$ and say that n is a *norm* in $\mathbf{C}$ if for each $j = 1, \ldots, m$ there is an ideal $\mathfrak{a}_j$ in the class C_j with norm n.

THEOREM 2. *Let $M > 0$, $\varepsilon > 0$, and $\mathbf{C}_0 \in \underline{\mathfrak{C}}$ be given. Let $U_{\mathbf{C}_0}(x)$ be the number of integers $n \le x$ such that n is the norm of some ideal in $\mathbf{C}_0$. Then for $x \ge x_0(M, \varepsilon)$ and $\Delta \le (\log x)^M$ we have*

$$U_{\mathbf{C}_0}(x) \gg_{M,\varepsilon} \max_{0 \le \alpha \le 1} \min_{H \le G} \frac{x (\log x)^{E(\alpha,H) - \varepsilon}}{|\operatorname{Fix} H|}.$$

If in addition $d_L = o(\log\log x)$, then

$$U_{\mathbf{C}_0}(x) \ll_{M,\varepsilon} \max_{0 \le \alpha \le 1} \min_{H \le G} \frac{x (\log x)^{E(\alpha,H) + \varepsilon}}{|\operatorname{Fix} H|}.$$

If we take $H = \{e\}$ and $H = G$, this contains the two upper bounds

$$U_{\mathbf{C}_0}(x) \ll \frac{x (\log x)^{\varepsilon}}{\mathbf{h}}$$

which can be obtained by counting norms of ideals *with multiplicity* of their occurrence (see e.g. [14]), and

$$U_{\mathbf{C}_0}(x) \ll x (\log x)^{1/d_L - 1 + \varepsilon}. \tag{1.4}$$

The bound (1.4), uniformly in $\Delta \leq (\log x)^M$, can be obtained by applying a Landau-type argument to $\zeta_L(s)^{1/d_L} H(s)$ where $H(s) \ll \prod_{p\mid\Delta}(1+p^{-s})$ in $\Re s \geq 2/3$. In general it might be hard to estimate $\operatorname{Fix} H$ for all subgroups H of G, but for example the following bound holds.

PROPOSITION 3. *Assume that $G_j := \mathrm{Gal}(K_j/\mathbb{Q})$ is cyclic, and let $H \leq G = \prod G_j$ be any subgroup. Let $\mathrm{pr}_j : G \to G_j$ be the canonical projection, define $H_j := \mathrm{pr}_j(H)$ and let $K_j^{H_j} \subseteq K_j$ be the fixed field of H_j. Then*

$$|\operatorname{Fix} H| \ll \Delta^{\varepsilon} \prod_{j=1}^{m} h(K_j^{H_j}).$$

A typical application of Theorem 2 is the following uniform version of (1.1):

COROLLARY 4. *With the above notation we have*

$$U_{\mathbf{C}_0}(x) = x(\log x)^{1/d_L - 1 + o(1)} \tag{1.5}$$

providing $x \gg \exp(\Delta^{\varepsilon}) + \exp(\mathbf{h}^{\varepsilon + d_L/\log 2}) + \exp(\exp(d_L \log d_L))$.

In general, (1.5) becomes incorrect for smaller x as can already be seen by taking imaginary quadratic fields [2]. The proof of Theorem 2 is a variant of the method in [1, 2], but we need some additional ideas to obtain uniformity in all parameters. Loosely speaking, if $\alpha_0 \in [0,1]$ is the number at which the maximum in (1.2), (1.3) is taken, then $\alpha_0 \log\log x$ is approximately the number of prime factors of a "generic" integer n counted by $U_{\mathbf{F}}(x)$. It is clear that we cannot drop the condition $(D_{K_i/\mathbb{Q}}, D_{K_j/\mathbb{Q}}) = 1$ for $i \neq j$ as one can already see for two quadratic extensions. The condition $d_L = o(\log\log x)$, however, is only for technical reasons and can perhaps be removed.

The first author would like to thank Dr. M. Spitzweck and Prof. U. Stuhler for helpful discussions.

2. Some lemmata. For a group G and subsets $A_1, \ldots, A_k$ define the product set

$$\prod_{j=1}^{k} A_j := \{a_1 \cdots a_k \mid a_1 \in A_1, \ldots, a_k \in A_k\}. \tag{2.1}$$

Then we have:

LEMMA 2.1. *A prime p is a norm in some $\mathbf{C} \in \underline{\mathfrak{C}}$ if and only if p is divisible by a prime ideal in L of degree 1. In this case p^{e_p} is a norm in all the classes in the product set $\{\mathbf{C}^{\sigma} \mid \sigma \in G\}^{e_p}$ and no others.*

Let $n = \prod_p p^{e_p}$ be the canonical prime factorization of n, and assume that p^{e_p} is a norm exactly in the set of classes $\emptyset \subseteq \mathcal{C}_p \subseteq \underline{\mathfrak{C}}$. Then n is a norm exactly in all the classes in the product set $\prod_p \mathcal{C}_p$ and no others.

Let $\mathfrak{C}(L)$ be the class group of L, and for any finite Abelian group G let $\widehat{G} := \{\chi : G \to \mathbb{C}^*\}$ be the dual group.

LEMMA 2.2. *We have an injective homomorphism of groups*

$$\widehat{\underline{\mathfrak{C}}} \hookrightarrow \widehat{\mathfrak{C}(L)}, \qquad (\chi_1, \dots, \chi_m) \mapsto \chi := \prod_{j=1}^{m} \chi_j \circ N_{L/K_j}.$$

Proof. It is clear that the map is a homomorphism from $\widehat{\underline{\mathfrak{C}}}$ to $\widehat{\mathfrak{C}(L)}$. We have to show that the kernel is trivial. To this end let χ_1, say, be nonprincipal, so that $\chi_1(C) \neq 1$ for some $C \in \mathfrak{C}_1$. For any number field $k/\mathbb{Q}$ let $\widetilde{k}$ be the class field. Since $(D_{K_i/\mathbb{Q}}, D_{K_j/\mathbb{Q}}) = 1$ for $i \neq j$, we have by properties of the Artin map (see [16, p. 400]) a commutative diagram

$$\begin{array}{ccc} \mathfrak{C}(L) & \xrightarrow{\cong} & \mathrm{Gal}(\widetilde{L}/L) \\ {\scriptstyle\text{norm}}\big\downarrow & & \big\downarrow \\ \underline{\mathfrak{C}} = \prod_{j=1}^{m} \mathfrak{C}_j & \xrightarrow{\cong} & \prod_{j=1}^{m} \mathrm{Gal}(\widetilde{K}_j/K_j) \end{array}$$

where the isomorphisms are given by the Artin map; the map on the right-hand side is given by

$$\mathrm{Gal}(\widetilde{L}/L) \xrightarrow{\text{restr.}} \mathrm{Gal}\Big(\prod \widetilde{K_j}/L\Big) \cong \prod \mathrm{Gal}(\widetilde{K_j}L/L) \cong \prod \mathrm{Gal}(\widetilde{K_j}/K_j)$$

and therefore obviously surjective. Thus also the norm is surjective and we have a preimage $\mathcal{C} \in \mathfrak{C}(L)$ of $(C, 1, \dots, 1)$ with $\chi(\mathcal{C}) \neq 1$, i.e. χ is nonprincipal.

For any Galois number field $k/\mathbb{Q}$ with discriminant D we know from results of Siegel [12] (upper bound), and Siegel–Brauer–Stark [13] (lower bound)

$$|D|^{-\varepsilon} \ll_{\varepsilon} \operatorname{res}_{s=1} \zeta_k(s) \ll \left(\frac{c_1 \log |D|}{d_L}\right)^{d_L} \ll |D|^{c_2} \tag{2.2}$$

for any $\varepsilon > 0$ and some absolute constants c_1, c_2, so that by the class number formula

$$h(k) \ll |D|^{c_3}. \tag{2.3}$$

Let

$$Q = Q_{\varepsilon} := \exp(\Delta^{\varepsilon}) \tag{2.4}$$

for some sufficiently small given $\varepsilon > 0$, and define

$$\begin{aligned} \mathbb{P}_Q &:= \{p > Q \mid p \text{ totally split in } L\}, \\ \mathcal{R}_Q(\mathbf{C}) &:= \mathcal{R}(\mathbf{C}) \cap \{n \in \mathbb{N} : p \mid n \Rightarrow p \in \mathbb{P}_Q\}. \end{aligned} \tag{2.5}$$

For $\chi \in \widehat{\mathfrak{C}(L)}$ let $L(s,\chi)$ be the Hecke L-function, and let

$$\widetilde{L}(s,Q,\chi) := \prod_{p\in\mathbb{P}_Q}\prod_{\mathfrak{P}|(p)} \exp\biggl(\frac{\chi(\mathfrak{P})}{p^s}\biggr)$$

where $\mathfrak{P}$ denotes a prime ideal in L.

LEMMA 2.3. *For any $\varepsilon > 0$ there are absolute positive constants c_4, $c_5(\varepsilon)$ such that for $\chi \in \widehat{\underline{\mathfrak{C}}}$ the functions $L(s,\chi)$, $\widetilde{L}(s,Q,\chi)$ are analytic and zero-free in the region*

$$R := \biggl\{ s = \sigma + it \in \mathbb{C} \;\biggl|\; \sigma \ge 1 - \frac{c_4}{d_L \log(\Delta(1+|t|))} \biggr\} \setminus (-\infty, 1 - c_5(\varepsilon)\Delta^{-\varepsilon}], \tag{2.6}$$

except for a simple pole at $s = 1$ if $\chi = \chi_0$. For $s \in R$, $|\sigma - 1| \le \min\bigl((\log Q)^{-1}, \frac{1}{3}\log^{-1}(\Delta(1+|t|))\bigr)$, we have

$$\left.\begin{matrix} \log \widetilde{L}(s,Q,\chi) \\ \log L(s,\chi) \end{matrix}\right\} - \delta_\chi \log^+\biggl(\frac{1}{|s-1|}\biggr) \ll_\varepsilon d_L \log\log(\Delta(1+|t|)) + \log \Delta^\varepsilon \tag{2.7}$$

where $\log^+(x) = \log(\max(1,x))$ and $\delta_\chi = 1$ if $\chi = \chi_0$ and zero otherwise. All constants are absolute (*but c_5 and the constant implied in* (2.7) *are ineffective*).

Proof. We first observe that $\widetilde{L}(s,Q,\chi) = L(s,\chi)G(s,Q,\chi)$ where the Euler product G is entire and zero-free in $\Re s > 1/2$ and $\log G(s,Q,\chi) \ll \log\log Q = \log \Delta^\varepsilon$ if $\Re s \ge 1 - (\log Q)^{-1}$. For complex χ or $|t| \ge 1$ the existence of a $c_4 > 0$ for the zero-free region for $L(s,\chi)$ is well known (see e.g. [9, Lemma 2.3]). For real $\chi \ne \chi_0$ we note that $L(s,\chi) = \zeta_{L'}(s)/\zeta_L(s)$ for some quadratic extension $L' \supseteq L$ (see [5]) with $D_{L'/\mathbb{Q}} \le \Delta^2$. Thus it follows from the theorems of Siegel–Brauer and Stark [13] that there is no zero

$$\beta \ge 1 - \max(c_6(\varepsilon)^{-d_L}\Delta^{-\varepsilon}, c_7 d_L^{-1}\Delta^{-2/d_L}),$$

which gives (2.6). To obtain (2.7), we choose $\delta = \log^{-1}(\Delta(1+|t|))$ in Lemma 4 of [4] getting

$$\frac{s-1}{s-2}\,\zeta_L(s), L(s,\chi) \ll \log^{d_L}(c_8\Delta(1+|t|))$$

uniformly in $1-\delta \le \sigma \le 1+\delta$ where χ denotes any nonprincipal character. By Carathéodory's inequality (see e.g. [10, §§73, 80]) and (2.4) we find

$$\begin{aligned}\log L(s,\chi) - \delta_\chi \log^+ \frac{1}{|s-1|} \\ &\ll d_L \log\log(\Delta(1+|t|)) + \left|\log L\left(1+\frac{\delta}{3}+it,\chi\right)\right| \\ &\ll d_L \log\log(\Delta(1+|t|)) + \log\frac{1}{\delta} + \log(\operatorname{res}_{s=1}\zeta_L(s)) \\ &\ll d_L \log\log(\Delta(1+|t|)) + \log \Delta^{\varepsilon}\end{aligned}$$

for $s \in R$, $1-\delta/3 \le \sigma \le 1+\delta$ and any $\chi \in \underline{\widehat{\mathfrak{C}}}$. After possibly reducing c_4, c_5 in (2.6), we obtain (2.7). By the remark at the beginning of the proof it also holds for $\widetilde{L}(s,Q,\chi)$.

LEMMA 2.4. *Let* $\mathfrak{C}$ *be any finite Abelian group of order* h, $G \le \operatorname{Aut}(\mathfrak{C})$ *finite*, $k \in \mathbb{N}$. *For* $\mathbf{C} = (C_1,\dots,C_k) \in \mathfrak{C}^k$ *define*

$$S_k(\mathbf{C}) := \# \prod_{\nu=1}^{k} \{C_\nu^\sigma \mid \sigma \in G\}$$

in the sense of (2.1). *Then*

$$\sum_{\mathbf{C}\in\mathfrak{C}^k} S_k(\mathbf{C}) \ge \frac{h^k}{\sum_{H\le G} 1} \min_{H\le G}\left(\frac{h}{|\operatorname{Fix} H|}\left(\frac{|G|}{|H|}\right)^k\right),$$

$$\max_{\mathbf{C}\in\mathfrak{C}^k} S_k(\mathbf{C}) \le \min_{H\le G}\left(\frac{h}{|\operatorname{Fix} H|}\left(\frac{|G|}{|H|}\right)^k\right).$$

Proof. To obtain the upper bound, we fix a subgroup $H \le G$. Let T be a transversal for H in G, so that, for any $\sigma_1,\dots,\sigma_k \in G$, $C_1,\dots,C_k \in \mathfrak{C}$,

$$\prod_{\nu=1}^{k} C_\nu^{\sigma_\nu} = \prod_{\nu=1}^{k} C_\nu \prod_{\nu=1}^{k} C_\nu^{t_\nu} \prod_{\nu=1}^{k} C_\nu^{\tau_\nu - 1}$$

for suitable $t_\nu \in T$, $\tau_\nu \in H$. (Note that $\sigma - 1$ is an endomorphism of $\mathfrak{C}$ for all $\sigma \in G$ since $\mathfrak{C}$ is Abelian.) Let $V = \langle \tau - 1 \mid \tau \in H\rangle \le \operatorname{End}(\mathfrak{C})$. Since $\bigcap_{v\in V} \ker(v) = \bigcap_{\tau\in H} \ker(\tau - 1) = \operatorname{Fix} H$, we have

$$\#\Big\{\prod_{\nu=1}^{k} C_\nu^{\tau_\nu - 1} \;\Big|\; \tau_\nu \in H\Big\} \le \frac{h}{|\operatorname{Fix} H|}.$$

This shows

$$S_k(\mathbf{C}) \le \frac{h|T|^k}{|\operatorname{Fix} H|} = \frac{h}{|\operatorname{Fix} H|}\left(\frac{|G|}{|H|}\right)^k$$

for any subgroup $H \le G$ and any $\mathbf{C} \in \mathfrak{C}^k$.

For the lower bound we define

$$N_{\mathbf{C}}(C)=N_{C_1,\ldots,C_k}(C):=\#\Big\{(\sigma_1,\ldots,\sigma_k)\in G^k \;\Big|\; \prod_{\nu=1}^{k} C_\nu^{\sigma_\nu}=C\Big\}$$

for $C\in\mathfrak{C}$ and $\mathbf{C}\in\mathfrak{C}^k$. By Cauchy's inequality,

$$\sum_{\mathbf{C}\in\mathfrak{C}} S_k(\mathbf{C})=\sum_{\mathbf{C}\in\mathfrak{C}^k}\sum_{\substack{C\in\mathfrak{C}\\ N_{\mathbf{C}}(C)\geq 1}} 1 \geq \frac{(\sum_{\mathbf{C}\in\mathfrak{C}^k}\sum_{C\in\mathfrak{C}} N_{\mathbf{C}}(C))^2}{\sum_{\mathbf{C}\in\mathfrak{C}^k}\sum_{C\in\mathfrak{C}} N_{\mathbf{C}}(C)^2}. \tag{2.8}$$

Clearly,

$$\sum_{\mathbf{C}\in\mathfrak{C}^k}\sum_{C\in\mathfrak{C}} N_{\mathbf{C}}(C)=|\mathfrak{C}|^k|G|^k \tag{2.9}$$

and

$$\begin{aligned}\sum_{\mathbf{C}\in\mathfrak{C}^k}\sum_{C\in\mathfrak{C}} N_{\mathbf{C}}(C)^2 &= \sum_{\mathbf{C}\in\mathfrak{C}^k}\sum_{\substack{(\sigma_1,\sigma_1',\ldots,\sigma_k,\sigma_k')\in G^{2k}\\ C_1^{\sigma_1}\cdots C_k^{\sigma_k}=C_1^{\sigma_1'}\cdots C_k^{\sigma_k'}}} 1\\ &= \sum_{(\sigma_1,\sigma_1',\ldots,\sigma_k,\sigma_k')\in G^{2k}} \#\{\mathbf{C}\in\mathfrak{C}^k \mid C_1^{\sigma_1}\cdots C_k^{\sigma_k}=C_1^{\sigma_1'}\cdots C_k^{\sigma_k'}\}\\ &= |G|^k\sum_{(\sigma_1,\ldots,\sigma_k)\in G^k}\#\{\mathbf{C}\in\mathfrak{C}^k \mid C_1^{\sigma_1-1}\cdots C_k^{\sigma_k-1}=1\}.\end{aligned} \tag{2.10}$$

For $H\leq G$ let

$$\varSigma_H:=\sum_{\substack{(\sigma_1,\ldots,\sigma_k)\in G^k\\ \langle\sigma_1,\ldots,\sigma_k\rangle=H}}\#\{\mathbf{C}\in\mathfrak{C}^k \mid C_1^{\sigma_1-1}\cdots C_k^{\sigma_k-1}=1\}.$$

Since the $\sigma_\nu-1$ are endomorphisms of $\mathfrak{C}$, we obtain

$$\begin{aligned}&\#\{\mathbf{C}\in\mathfrak{C}^k \mid C_1^{\sigma_1-1}\cdots C_k^{\sigma_k-1}=1\}\\ &\quad=\#\Big\{(C_1,\ldots,C_k)\in\prod_{\nu=1}^{k}\operatorname{im}(\sigma_\nu-1)\;\Big|\;\prod_{\nu=1}^{k}C_\nu=1\Big\}\prod_{\nu=1}^{k}|\ker(\sigma_\nu-1)|\end{aligned}$$

for any k-tuple $(\sigma_1,\ldots,\sigma_k)\in G^k$. Since $\mathfrak{C}$ is Abelian, the first factor equals

$$\frac{1}{|\langle\operatorname{im}(\sigma_1-1),\ldots,\operatorname{im}(\sigma_k-1)\rangle|}\prod_{\nu=1}^{k}|\operatorname{im}(\sigma_\nu-1)|.$$

If we substitute the last two displays in the definition of $\varSigma_H$, we obtain

$$\varSigma_H=\sum_{\substack{(\sigma_1,\ldots,\sigma_k)\in G^k\\ \langle\sigma_1,\ldots,\sigma_k\rangle=H}}\frac{|\mathfrak{C}|^k}{|\langle\operatorname{im}(\sigma_1-1),\ldots,\operatorname{im}(\sigma_k-1)\rangle|}\leq|\mathfrak{C}|^k\,\frac{|H|^k|\operatorname{Fix}H|}{|\mathfrak{C}|}.$$

Finally, we sum over all $H\leq G$ and use (2.8)–(2.10) to get the lower bound.

Next we restate Lemma 4.1 in [1].

LEMMA 2.5. *Let z_ν, $\nu = 1, \dots, k$, be k complex numbers with $\Im(z_\nu) < 0 < \Re(z_\nu)$ and let $z = \prod_{\nu=1}^{k} z_\nu$. Then $-\Im(z)$ is positive and increasing in all $\Re(z_\nu)$ as long as $k\Im(z_\nu)/\Re(z_\nu) > -\pi$ for all ν.*

LEMMA 2.6. *Let $\alpha \in [0,1]$, $\beta \in [1/2, 1]$, $\gamma > 0$, $r := \alpha \log\log x$, $J = [1 - (\log x)^{-\beta}, 1]$. If $\beta > \alpha$, then*

$$\frac{1}{\Gamma(r+1)} \int_J \left(\gamma \log \frac{1}{1-s}\right)^r ds \ll (\log x)^{-\beta+\alpha(1+\log(\gamma\beta/\alpha))+\varepsilon}$$

uniformly in α, β, γ.

Proof. By a change of variables $\widetilde{s} := (\log\log x)^2/\log\left(\frac{1}{1-s}\right)$ the left hand side equals

$$\frac{\gamma^r (\log\log x)^2}{\Gamma(r+1)} \int_0^{(\log\log x)/\beta} \left(\frac{(\log\log x)^2}{\widetilde{s}}\right)^r \exp\left(-\frac{(\log\log x)^2}{\widetilde{s}}\right) \frac{d\widetilde{s}}{\widetilde{s}^2}.$$

The integrand is increasing for $\widetilde{s} \le (\log\log x)^2/(r+2)$, and so is

$$\ll (\beta \log\log x)^r (\log x)^{-\beta}$$

since $\beta > \alpha$. The lemma follows now easily using Stirling's formula.

Finally, we need a general Siegel–Walfisz theorem for Galois number fields. For $\mathbf{C} \in \underline{\mathfrak{C}}$ let

$$\epsilon(\mathbf{C}) := \frac{1}{|G|} \#\{\sigma \in G \mid \mathbf{C}^\sigma = \mathbf{C}\} \tag{2.11}$$

be the normalized stabilizer of $\mathbf{C}$.

LEMMA 2.7. *For any $\mathbf{C} \in \underline{\mathfrak{C}}$ we have*

$$\epsilon(\mathbf{C}) \sum_{\substack{p \le \xi \\ p \in \mathcal{R}(\mathbf{C}) \\ p \text{ totally split in } L}} 1 = \frac{1}{d_L \mathbf{h}} \int_2^\xi \frac{dt}{\log t} + O(\xi \exp(-c_B (\log \xi)^{1/3})) \tag{2.12}$$

uniformly in $\Delta \le (\log \xi)^B$ for any constant $B > 0$. In particular,

$$U_{\mathbf{F}}(x) \gg \frac{x}{(\log x)^{1+\varepsilon \mathbf{h}}} \gg \frac{x}{(\log x)^{Bc_3+1+\varepsilon}} \tag{2.13}$$

uniformly in $\Delta \le (\log x)^B$ (cf. (2.3)).

Proof. This is standard by applying Perron's formula to

$$\Psi_{\mathbf{C}}(s) := -\frac{1}{d_L\mathbf{h}} \sum_{(\chi_1,\ldots,\chi_m)\in\widehat{\underline{\mathfrak{C}}}} \Big(\prod_{j=1}^{m} \bar{\chi}_j(C_j)\Big) \frac{L'(s,\chi)}{L(s,\chi)} \tag{2.14}$$
$$= \frac{1}{d_L} \sum_{p} \sum_{n\ge 1} \frac{f_p \log p}{p^{f_p n s}} \sum_{\substack{\mathfrak{P}\mid(p) \\ N_{L/K_j}\mathfrak{P}^n\in\mathfrak{C}_j}} 1.$$

Here $\mathfrak{P}$ is a prime ideal in L, f_p is the ramification index of p in L, and χ is as in Lemma 2.2. We can absorb the contribution of the p^n, $n > 1$, and the contribution of the nonsplit primes in the error term. We integrate over a suitable rectangle so that the main term comes from the residue of $\Psi_{\mathbf{C}}(s)$ at $s = 1$, which is $(d_L\mathbf{h})^{-1}$ by Lemma 2.2. Note that we have $d_L^{-1}\#\{\mathfrak{P} \mid (p) : N_{L/K_j}\mathfrak{P}^n \in \mathfrak{C}_j\} = \epsilon(\mathbf{C})$ for a totally split prime p. For further details see [6], where the integration is carried out in detail, and note that we can use Stark's result [13] to obtain a larger zero-free region as in [6] if d_L is large ($d_L \ge \sqrt{\log\log x}$, say).

3. Suitable Dirichlet series. The proof of the main theorem uses ideas from [1, 2], so we refer to these papers for some more details. We use a Dirichlet series to count numbers which are norms in a given class. We begin with a Dirichlet series that counts primes that are norms in a given class $\mathbf{C} = (C_1, \ldots, C_m)$. By orthogonality we have (cf. (2.14))

$$\frac{1}{d_L\mathbf{h}} \sum_{(\chi_1,\ldots,\chi_m)\in\widehat{\underline{\mathfrak{C}}}} \Big(\prod_{j=1}^{m} \bar{\chi}_j(C_j)\Big) \log \widetilde{L}(s,Q,\chi) = \epsilon(\mathbf{C}) \sum_{p\in\mathcal{R}_Q(\mathbf{C})} \frac{1}{p^s} \tag{3.1}$$
$$=: P_{\mathbf{C},Q}(s) =: \frac{1}{d_L\mathbf{h}} \log\zeta(s) + T(s,\mathbf{C},Q)$$

where χ is given by Lemma 2.2 and $\mathcal{R}_Q(\mathbf{C})$ by (2.5). From the definition we see that $T(s,\mathbf{C},Q)$ is a Dirichlet series with real coefficients, hence $T(s,\mathbf{C},Q) = \overline{T}(\bar{s},\mathbf{C},Q)$ on $(1,\infty]$. This identity holds wherever T is holomorphic; in particular T is real on $[2/3,1]\cap R$ by Lemma 2.3. For $\mathbf{C} \in \underline{\mathfrak{C}}$, $k \in \mathbb{N}$ let

$$M_k(\mathbf{C}) := \Big\{(\mathbf{C}_1,\ldots,\mathbf{C}_k) \in \underline{\mathfrak{C}}^k \;\Big|\; \mathbf{C} \in \prod_{\nu=1}^{k}\{\mathbf{C}_\nu^\sigma \mid \sigma\in G\}\Big\},$$

and

$$A_{\mathbf{C},k}(s) = \frac{1}{k!} \sum_{(\mathbf{C}_1,\ldots,\mathbf{C}_k)\in M_k(\mathbf{C})} \prod_{\nu=1}^{k} P_{\mathbf{C}_\nu,Q}(s) = \sum_{n=1}^{\infty} \frac{a_{\mathbf{C},k}(n)}{n^s} \quad \text{(say)}. \tag{3.2}$$

By Lemma 2.1 the coefficients $a_{\mathbf{C},k}$ satisfy

- $0 \leq a_{\mathbf{C},k}(n) \leq 1$ for all $n \in \mathbb{N}$,
- $a_{\mathbf{C},k}(n) > 0$ only if $n \in \mathcal{R}_Q(\mathbf{C})$ and $\Omega(n) = k$,
- $a_{\mathbf{C},k}(n) = 1$ if $n \in \mathcal{R}_Q(\mathbf{C})$, $\Omega(n) = k$ and $\mu^2(n) = 1$.

In fact, it is clear that $A_{\mathbf{C},k}(s)$ counts only $n \in \mathcal{R}_Q(\mathbf{C})$ with $\Omega(n) = k$. Furthermore, choose a fixed set of representatives of the quotient $G\backslash\underline{\mathfrak{C}}$, and for each $\mathbf{C} \in \underline{\mathfrak{C}}$ let $\widetilde{\mathbf{C}}$ be this representative. For k not necessarily distinct objects $X_1, \ldots, X_k$ let $\varrho(X_1, \ldots, X_k)$ be the number of rearrangements of the k-tuple $(X_1, \ldots, X_k)$. Then we observe that an $n = \prod_{\nu=1}^k p_\nu$ with not necessarily distinct $p_\nu \in \mathcal{R}_Q(\mathbf{D}_\nu)$, say, occurs as a denominator of a Dirichlet series $\prod_{\nu=1}^k P_{\mathbf{C}_\nu,Q}(s)$ for exactly $\varrho(\widetilde{\mathbf{D}}_1, \ldots, \widetilde{\mathbf{D}}_k) \prod_{\nu=1}^k \epsilon(\mathbf{D}_\nu)^{-1}$ k-tuples from $M_k(\mathbf{C})$. Therefore, $a_{\mathbf{C},k}(n) \leq 1$ with equality if $n \in \mathcal{R}_Q(\mathbf{C})$ is squarefree.

The preceding discussion gives

$$\sum_{n \leq x} a_{\mathbf{C}_0,k}(n) \leq U_{\mathbf{C}_0}(x) \tag{3.3}$$

for all $k \in \mathbb{N}$ and $\mathbf{C}_0 \in \underline{\mathfrak{C}}$. To obtain an upper bound, we have to include some more numbers in our Dirichlet series. To this end, let

$$Z_{\mathbf{C},Q}(s) = \epsilon(\mathbf{C}) \sum_{\substack{p \leq Q \\ p \in \mathcal{R}(\mathbf{C})}} \frac{1}{p^s}.$$

For $k, l \in \mathbb{N}_0$ let

$$\begin{aligned} A_{\mathbf{C},k,l}(s) &:= \frac{1}{k!}\frac{1}{l!} \sum_{\substack{(\mathbf{C}_1,\ldots,\mathbf{C}_k) \in \underline{\mathfrak{C}}^k \\ (\mathbf{D}_1,\ldots,\mathbf{D}_l) \in \underline{\mathfrak{C}}^l \\ (\mathbf{C}_1,\ldots,\mathbf{D}_l) \in M_{k+l}(\mathbf{C})}} \prod_{\nu=1}^k P_{\mathbf{C}_\nu,Q}(s) \prod_{\mu=1}^l Z_{\mathbf{D}_\mu,Q}(s) \\ &= \sum_{n=1}^\infty \frac{a_{\mathbf{C},k,l}(n)}{n^s} \qquad \text{(say)}. \end{aligned}$$

Then we see as before that $a_{\mathbf{C},k,l}(n) = 1$ if $n \in \mathcal{R}(\mathbf{C})$, $\mu^2(n) = 1$, and n has exactly l prime factors $\leq Q$ and k greater than Q.

Now we observe that by Lemma 2.1, if $n = n_1 n_2 \in \mathcal{R}(\mathbf{C})$ and $(n_1, n_2) = 1$, then $n_1 \in \mathcal{R}(\mathbf{C}_1)$ and $n_2 \in \mathcal{R}(\mathbf{C}_2)$ for some $\mathbf{C}_1\mathbf{C}_2 = \mathbf{C}$. This also holds if (n_1, n_2) consists only of totally split primes. Finally, let

$$B_{\mathbf{C}}(s) = \delta_{\mathbf{C}} + \sum_{\substack{n \in \mathcal{R}(\mathbf{C}) \\ n \text{ powerfull}}} \frac{1}{n^s}$$

where $\delta_{\mathbf{C}} = 1$ if $\mathbf{C} = 1 \in \underline{\mathfrak{C}}$ and else it vanishes. Then by the above discussion the coefficients of

$$\sum_{\mathbf{C}\in\underline{\mathfrak{C}}}\sum_{r\le R}\sum_{k+l=r} A_{\mathbf{C},k,l}(s)B_{\mathbf{C}^{-1}\mathbf{C}_0}(s)=\sum_{n=1}^{\infty}\frac{a_{\mathbf{C}_0}^{(R)}(n)}{n^s}\quad\text{(say)}\tag{3.4}$$

satisfy

$$\sum_{n\le x} a_{\mathbf{C}_0}^{(R)}(n)\ge U_{\mathbf{C}_0}^{(R)}(x)\tag{3.5}$$

where $U_{\mathbf{C}_0}^{(R)}(x)$ denotes those numbers $n\le x$, $n\in\mathcal{R}(\mathbf{C}_0)$ with $\Omega(n)\le R$. For $k=0$ we count numbers with multiplicity at most $\mathbf{h}$ that consist only of primes $p\le Q$, and by Corollary 1.3 of [8] there are, for sufficiently small ε in (2.4), at most $x\exp(-(\log x)^{3/4})$ numbers of this kind up to x. Thus we may assume $k>0$.

In preparation for Perron's formula let $S=\exp((\log x)^{1/2})$ and

$$\begin{aligned}\Gamma_{1,1}&:=[1-(\log x)^{-1+\varepsilon}+iS,1+(\log x)^{-1}+iS],\\ \Gamma_{2,1}&:=[1-(\log x)^{-1+\varepsilon},1-(\log x)^{-1+\varepsilon}+iS],\\ \Gamma_{3,1}&:=[1-\exp(-(\log\log x)^4),1-(\log x)^{-1+\varepsilon}],\\ \Gamma_{4}&:=\{s\in\mathbb{C}\mid |s-1|=\exp(-(\log\log x)^4)\}.\end{aligned}$$

Let $\Gamma_{\nu,2}$ $(1\le\nu\le3)$ be the image of $\Gamma_{\nu,1}$ under reflection on the real axis, oriented such that

$$\Gamma:=\Gamma_{1,2}\Gamma_{2,2}\Gamma_{3,2}\Gamma_4\Gamma_{3,1}\Gamma_{2,1}\Gamma_{1,1}$$

is homotopic to $[1+(\log x)^{-1}-iS,1+(\log x)^{-1}+iS]$. By (2.4), (2.6), (2.7) the functions $P_{\mathbf{C},Q}$ extend for sufficiently large x holomorphically to a neighbourhood of Γ, and we have $P_{\mathbf{C},Q}(s)\ll(\log\log x)^2$ on $\Gamma_{1,2}\Gamma_{2,2}\cup\Gamma_{2,1}\Gamma_{1,1}$ and $P_{\mathbf{C},Q}(s)\ll(\log\log x)^4$ on Γ_4, so that

$$A_{\mathbf{C},k}(s)\ll(\mathbf{h}(\log\log x)^4)^k\ll\exp((\log\log x)^3)\tag{3.6}$$

on $\widetilde{\Gamma}:=\Gamma_{1,2}\Gamma_{2,2}\cup\Gamma_4\cup\Gamma_{2,1}\Gamma_{1,1}$ for $k\ll\log\log x$ and $x>x_0(A)$. Likewise, since

$$Z_{\mathbf{C},Q}(s)\ll\sum_{p\le Q}\frac{1}{p^{1-(\log x)^{-1+\varepsilon}}}\ll\log\log Q\ll\log\log x$$

on Γ, we see that

$$A_{\mathbf{C},k,l}(s)\ll\exp((\log\log x)^3)\tag{3.7}$$

on $\widetilde{\Gamma}$ for $k+l\ll\log\log x$. For future reference we define

$$J=-\Gamma_{3,1}=[1-(\log x)^{-1+\varepsilon},1-\exp(-(\log\log x)^4)].\tag{3.8}$$

LEMMA 3.1. *For $\mathbf{C}\in\underline{\mathfrak{C}}$, $|\sigma-1|\le(\log x)^{-2/3}$ and $\varepsilon>0$ we have*

$$|T(\sigma,\mathbf{C},Q)|\le\frac{\varepsilon\log\Delta+O(1)}{d_L\mathbf{h}}$$

where T was defined in (3.1).

Proof (see Lemma 4.3 in [2] for details). For fixed $\mu \ge 0$ we have, by (3.1),

$$\frac{d^\mu}{ds^\mu} T(s, \mathbf{C}, Q)|_{s=1} = \lim_{\xi\to\infty}\biggl(\epsilon(\mathbf{C}) \sum_{p\in\mathcal{R}_Q(\mathbf{C}),\, p\le\xi} \frac{(-\log p)^\mu}{p} - \frac{1}{d_L\mathbf{h}} \sum_{p\le\xi} \frac{(-\log p)^\mu}{p}\biggr).$$

For $\xi \ge Q$ this can be evaluated by partial summation and (2.12), and we obtain

$$|T(1, \mathbf{C}, Q)| \le \frac{\varepsilon \log \Delta + O_\varepsilon(1)}{d_L\mathbf{h}} \quad \text{and} \quad |T^{(\mu)}(1, \mathbf{C}, Q)| \le \frac{\Delta^\varepsilon + O_\varepsilon(1)}{d_L\mathbf{h}}$$

for $\mu \ge 1$. The lemma follows now from Taylor's formula up to degree $\mu_0 := \lceil 2c_3M + 1\rceil$, say, where we use the trivial estimation

$$T^{(\mu_0)}(s, \mathbf{C}, Q) \ll \max_{\chi\ne\chi_0} \biggl| \frac{d^{\mu_0}}{ds^{\mu_0}} \log \widetilde{L}(s, Q, \chi)\biggr| \ll (\log x)^\varepsilon$$

together with (2.6) for $|s - 1| \le (\log x)^{-2/3}$.

4. The lower bound. We start with the lower bound. By Perron's formula, (3.2) and (3.3) we obtain

$$U_{\mathbf{C}_0}(x) \ge \max_{k\le(1-2\varepsilon)\log\log x} \frac{1}{2\pi i} \int_\Gamma A_{\mathbf{C}_0,k}(s)\, \frac{x^s}{s}\, ds + O\biggl(\frac{x \log x}{S}\biggr),$$

so that by (3.6),

$$U_{\mathbf{C}_0}(x) \ge \max_{k\le(1-2\varepsilon)\log\log x} \biggl(-\frac{1}{\pi}\Im \int_J A_{\mathbf{C}_0,k}(s)\, \frac{x^s}{s}\, ds\biggr) + O\biggl(\frac{x}{\exp((\log\log x)^3)}\biggr)$$

with J as in (3.8). Note that the integrand in $\Gamma_{3,1}$ is the complex conjugate of the integrand in $\Gamma_{3,2}$. We use Lemma 2.5 with $z_\nu = P_{\mathbf{C}_\nu,Q}(s)$. Note that by (3.1) and Lemma 3.1 the assumptions are satisfied for $x > x_0(M, \varepsilon)$. Therefore,

$$U_{\mathbf{C}_0}(x) \ge \max_{k\le(1-2\varepsilon)\log\log x} \biggl(-\frac{1}{\pi}\Im \int_{1-2/\log x}^{1-1/\log x} \frac{1}{k!}\biggl(\frac{\log\frac{1}{1-s} - \varepsilon\log\Delta - c_9 - i\pi}{d_L\mathbf{h}}\biggr)^k \times \#M_k(\mathbf{C}_0)\, \frac{x^s}{s}\, ds\biggr) + O\biggl(\frac{x}{\exp((\log\log x)^3)}\biggr)$$

for some positive constant c_9. To estimate $\#M_k(\mathbf{C}_0)$, we divide the sum over $\underline{\mathfrak{C}}^k$ into two sums over $\underline{\mathfrak{C}} \times \underline{\mathfrak{C}}^{k-1}$, obtaining

$$\#M_k(\mathbf{C}_0) \ge \sum_{\mathbf{C}\in\underline{\mathfrak{C}}} \#M_{k-1}(\mathbf{C}_0\mathbf{C}^{-1}) = \sum_{\mathbf{C}\in\underline{\mathfrak{C}}} \#M_{k-1}(\mathbf{C}) = \sum_{\mathbf{C}\in\underline{\mathfrak{C}}^{k-1}} S_{k-1}(\mathbf{C}),$$

so that by Lemma 2.4,

$$\begin{aligned}U_{\mathbf{C}_0}(x) \gg_{M,\varepsilon} \frac{x}{\log x} \max_{k\le(1-2\varepsilon)\log\log x} \frac{1}{k!}((1-\varepsilon)\log\log x)^k \sin\biggl(\frac{\pi k(1+o(1))}{\log\log x}\biggr) \\ \times \frac{1}{d_L\sum_{H\le G}1} \min_{H\le G}\biggl(\frac{1}{|H|^k|\mathrm{Fix}\,H|}\biggr) \\ \gg \frac{x}{(\log x)^{1+\varepsilon}} \max_{k\le(1-2\varepsilon)\log\log x} \frac{1}{k!}(\log\log x)^k \min_{H\le G}\biggl(\frac{1}{|H|^k|\mathrm{Fix}\,H|}\biggr)\end{aligned}$$

up to an error of $O(x/\exp((\log\log x)^3))$. In order to obtain a (crude) bound for $\sum_{H\le G}1$, we can observe that there are $\ll |G|$ nonisomorphic Abelian groups H of order $\le G$, and each H has at most $\Omega(|H|)$ generators and so can occur in at most $\Omega(|H|) \ll \log|G|$ ways in G. Thus $\sum_{H\le G}1 \ll |G|^{O(\log|G|)} \ll (\log x)^{\varepsilon}$.

At the cost of an additional factor $(\log x)^{-\varepsilon}$ we may extend the maximum over all real $k\in[0,\log\log x]$. Writing $k=\alpha\log\log x$, we obtain after a short calculation using Stirling's formula

$$U_{\mathbf{C}_0}(x) \gg \max_{0\le\alpha\le1}\min_{H\le G}\frac{x(\log x)^{E(\alpha,H)-\varepsilon}}{|\mathrm{Fix}\,H|}.$$

This gives the lower bound.

5. The upper bound. Let us first note that by our assumption $d_L = o(\log\log x)$ we have

$$\sum_{\mathbf{C}\in\underline{\mathfrak{C}}} B_{\mathbf{C}}(s) \ll \sum_{\mathbf{C}\in\underline{\mathfrak{C}}} B_{\mathbf{C}}\biggl(1-\frac{1}{(\log x)^{1-\varepsilon}}\biggr) \le c_{10}^{d_L} \ll (\log x)^{\varepsilon}$$

for $s\in\Gamma$. This is the only place where the additional assumption is needed. By Perron's formula, (3.4), (3.5) and (3.7), we therefore have as above

$$\begin{aligned}(5.1)\quad U_{\mathbf{C}_0}^{(R)}(x) \le \sum_{r\le R}\sum_{\substack{k+l=r\\k\ne0}} \frac{-1}{\pi}\Im\biggl(\int_J\sum_{\mathbf{C}\in\underline{\mathfrak{C}}} A_{\mathbf{C},k,l}(s)B_{\mathbf{C}^{-1}\mathbf{C}_0}(s)\,\frac{x^s}{s}\,ds\biggr) \\ + O\biggl(\frac{x}{\exp((\log\log x)^3)}\biggr) \\ \ll x(\log x)^{\varepsilon}\sum_{r\le R}\sum_{\substack{k+l=r\\k\ne0}}\int_J\max_{\mathbf{C}\in\underline{\mathfrak{C}}}|A_{\mathbf{C},k,l}(s)|\,ds + \frac{x}{\exp((\log\log x)^3)}.\end{aligned}$$

Writing $\underline{\mathfrak{C}}^k = \underline{\mathfrak{C}}\times\underline{\mathfrak{C}}^{k-1}$, we see that

$$|A_{\mathbf{C},k,l}(s)| \le \frac{1}{k!}\frac{1}{l!}\sum_{\sigma\in G}\sum_{\mathbf{C}_1\in\underline{\mathfrak{C}}}|P_{\mathbf{C}_1,Q}(s)| \\ \times \sum_{\substack{(\mathbf{C}_2,\ldots,\mathbf{C}_k)\in\underline{\mathfrak{C}}^{k-1}\\(\mathbf{D}_1,\ldots,\mathbf{D}_l)\in\underline{\mathfrak{C}}^l\\(\mathbf{C}_2,\ldots,\mathbf{D}_l)\in M_{k-1+l}(\mathbf{C}\mathbf{C}_1^\sigma)}}\prod_{\nu=2}^{k}|P_{\mathbf{C}_\nu,Q}(s)|\prod_{\mu=1}^{l}|Z_{\mathbf{D}_\mu,Q}(s)|.$$

We relabel the summation variable $\mathbf{C}_1 \leftarrow \mathbf{C}\mathbf{C}_1^\sigma$. By Lemma 3.1 we have

$$|P_{\mathbf{C},Q}(s)| \le \frac{1+\varepsilon}{d_L\mathbf{h}}\log\frac{1}{1-s} \quad \text{on } J.$$

Changing the order of summation, we see that

$$|A_{\mathbf{C},k,l}(s)| \ll \frac{(\log\log x)^4}{\mathbf{h}k!l!}\Big(\sum_{\mathbf{C}\in\underline{\mathfrak{C}}}|P_{\mathbf{C},Q}(s)|\Big)^{k-1}\Big(\sum_{\mathbf{D}\in\underline{\mathfrak{C}}}Z_{\mathbf{D},Q}(s)\Big)^{l} \\ \times \max_{(\mathbf{C}_2,\ldots,\mathbf{D}_l)\in\underline{\mathfrak{C}}^{k-1+l}} S_{k-1+l}((\mathbf{C}_2,\ldots,\mathbf{D}_l)) \tag{5.2}$$

on J (note that $Z_{\mathbf{D},Q}(s) > 0$ there), so that by Lemma 2.4, (5.1) and (5.2),

$$U^{(R)}_{\mathbf{C}_0}(x) \ll x(\log x)^\varepsilon \max_{r\le R}\min_{H\le G}\left(\frac{d_L^{r-1}}{|H|^{r-1}|\mathrm{Fix}\,H|}\right)\frac{1}{r!} \\ \times \int_J\Big(\sum_{\mathbf{C}\in\underline{\mathfrak{C}}}|P_{\mathbf{C},Q}(s)| + Z_{\mathbf{C},Q}(s)\Big)^r ds + \frac{x}{\exp((\log\log x)^3)}. \tag{5.3}$$

By (3.1) we have $\sum_{\mathbf{C}\in\underline{\mathfrak{C}}}(|P_{\mathbf{C},Q}(s)| - P_{\mathbf{C},Q}(s)) = \pi/d_L$. Using orthogonality, the same calculation as in (3.1) shows

$$\frac{1}{d_L}\log\zeta_L(s) = \sum_{\mathbf{C}\in\underline{\mathfrak{C}}}\frac{1}{\mathbf{h}}\sum_{(\chi_1,\ldots,\chi_m)\in\widehat{\underline{\mathfrak{C}}}}\Big(\prod_{j=1}^{m}\bar{\chi}_j(C_j)\Big)\log L(s,\chi) \\ = \sum_{\mathbf{C}\in\underline{\mathfrak{C}}}\sum_{p\in\mathcal{R}(\mathbf{C})}\frac{1}{p^s} + O\Big(1+\sum_{p\mid\Delta}\frac{1}{p^s}\Big)$$

on J. From (2.7) we thus infer

$$\Big|\sum_{\mathbf{C}\in\underline{\mathfrak{C}}}(|P_{\mathbf{C},Q}(s)| + Z_{\mathbf{C},Q}(s))\Big| \le \frac{1+\varepsilon}{d_L}\log\frac{1}{1-s} + \log\log\Delta \tag{5.4}$$

on J ($x \ge x_0(\varepsilon)$). Let us first assume $d_L \le \sqrt{\log\log x}$. Then

$$\Big|\sum_{\mathbf{C}\in\underline{\mathfrak{C}}}(|P_{\mathbf{C},Q}(s)| + Z_{\mathbf{C},Q}(s))\Big| \le \frac{1+\varepsilon}{d_L}\log\frac{1}{1-s},$$

so that by (5.3),

$$U^{(R)}_{\mathbf{C}_0}(x) \ll x(\log x)^{\varepsilon} \max_{r\le \log\log x} \min_{H\le G} \left(\frac{1}{|H|^r |\mathrm{Fix}\, H|}\right) \frac{1}{r!} \int_J \left(\log \frac{1}{1-s}\right)^r ds \ll x \max_{\alpha\in[0,1]} \min_{H\le G} \frac{(\log x)^{E(\alpha,H)+\varepsilon}}{|\mathrm{Fix}\, H|} \tag{5.5}$$

by Lemma 2.6.

Now assume $d_L \ge \sqrt{\log\log x}$ and let $c_{11} = Mc_3 + 2$,

$$\varrho = \frac{2c_{11}}{\log\log\log x}.$$

Firstly we show that the contribution of those r in (5.3) with $\varrho \log\log x \le r \le R$ is negligible. In fact, if we consider in (5.3) only the case $H = G$, then by (5.4) and Lemma 2.6 their contribution is at most

$$\begin{aligned} U^{(R)}_1(x) &\ll x(\log x)^{\varepsilon} \max_{r\ge \varrho\log\log x} \frac{1}{r!} \int_J \left(\frac{1+\varepsilon}{d_L} \log \frac{1}{1-s} + \log\log \Delta\right)^r ds \\ &\ll x(\log x)^{\varepsilon} \max_{r\ge \varrho\log\log x} \frac{1}{r!} \int_J \left(\frac{c_{12}}{\sqrt{\log\log x}} \log \frac{1}{1-s}\right)^r ds \\ &\ll x(\log x)^{-c_{11}+\varepsilon} \end{aligned}$$

for sufficiently large x which is admissible by (2.13). On the other hand, those r with $r \le \varrho \log\log x$ contribute at most

$$x(\log x)^{\varepsilon} \max_{r\le \varrho\log\log x} \min_{H\le G} \left(\frac{1}{|H|^r |\mathrm{Fix}\, H|}\right) \int_J \frac{1}{r!} \left(c_{13}(\log\log \Delta) \log \frac{1}{1-s}\right)^r ds.$$

Since $\varrho \log(c_{13} \log\log \Delta) = o(1)$, we find by Lemma 2.6 that

$$U^{(R)}_{\mathbf{C}_0}(x) \ll x \max_{\alpha\le\varrho} \min_{H\le G} \frac{(\log x)^{E(\alpha,H)+\varepsilon}}{|\mathrm{Fix}\, H|}. \tag{5.6}$$

Now we choose $R := c_{14} \log\log x$ with $c_{14} = (\log 2)^{-1}(Mc_3 + 4)$ and bound trivially the number of integers $n \le x$ with $\Omega(n) \ge c_{12} \log\log x$. By [3, Corollary 1], there are at most $O(x(\log x)^{-Mc_3-2})$ numbers of this kind. By (2.13) this yields an admissible error. By (5.5) and (5.6) the proof is complete.

6. Proof of Proposition 3 and Corollary 4. Since each group $G_j = \mathrm{Gal}(K_j/\mathbb{Q})$ is cyclic, every $\mathbf{C} \in \mathrm{Fix}\, H$ contains an m-tuple of ideals $(\mathfrak{a}_1, \ldots, \mathfrak{a}_m)$ that remains fixed under the action of H. Indeed, let σ_j be a generator of H_j. If $(\mathfrak{b}_1, \ldots, \mathfrak{b}_m)$ is any m-tuple of ideals in a class $\mathbf{C} = (C_1, \ldots, C_m) \in \mathrm{Fix}\, H$, then C_j is fixed by H_j, and so $(\mathfrak{b}_1^{\sigma_1}, \ldots, \mathfrak{b}_m^{\sigma_m}) =$

$((\lambda_1)\mathfrak{b}_1, \ldots, (\lambda_m)\mathfrak{b}_m)$ for some principal ideals (λ_j). By Hilbert's Theorem 90 we can write $\lambda_j = \mu_j^{1-\sigma_j}$ (e.g. [7, §13]), so that $\mathfrak{a}_j := (\mu_j)\mathfrak{b}_j$ gives the desired ideal tuple. But up to a product of powers of ramified prime ideals, the $\mathfrak{a}_j$ are lifted ideals from the fixed field $K_j^{H_j}$, and so (cf. e.g. [15, Theorem 1.6])

$$|\mathrm{Fix}\, H| \leq \prod_{j=1}^{m} \Big(h(K_j^{H_j}) \prod_{\mathfrak{p} \subseteq K_j^{H_j}} e(\mathfrak{p}) \Big)$$

where as usual $e(\mathfrak{p})$ denotes the ramification index of $\mathfrak{p}$ in K_j. By Dedekind's discriminant theorem we know

$$\prod_{\mathfrak{p} \subseteq K_j^{H_j}} e(\mathfrak{p}) \leq \prod_{p^e \| D_{K/\mathbb{Q}}} (e+1) \ll (D_{K/\mathbb{Q}})^{\varepsilon}.$$

This gives the proposition.

The corollary follows immediately from Theorem 2: For each subgroup $H \neq G$ we estimate $E(\alpha, H) \geq -1 + \alpha(1 - \log(\alpha d_L/2))$ and $\mathrm{Fix}\, H \leq \mathbf{h}$ getting

$$\begin{aligned} U_{\mathbf{C}_0}(x) & \\ &\gg \max_{0 \leq \alpha \leq 1} \min\left(x(\log x)^{-1+\alpha(1-\log(\alpha d_L))-\varepsilon}, \frac{x(\log x)^{-1+\alpha(1-\log(\alpha d_L/2))-\varepsilon}}{\mathbf{h}} \right) \\ &\geq x(\log x)^{1/d_L - 1 - \varepsilon} \end{aligned}$$

if $\mathbf{h} \leq (\log x)^{(\log 2)/d_L}$ as can be seen by taking $\alpha = 1/d_L$. The upper bound in (1.5) follows from (1.4) for $x \gg \exp(\Delta^{\varepsilon})$.

References

[1] V. Blomer, *Binary quadratic forms with large discriminants and sums of two squarefull numbers*, J. Reine Angew. Math. 569 (2004), 213–234.

[2] —, *Binary quadratic forms with large discriminants and sums of two squarefull numbers II*, J. London Math. Soc. 71 (2005), 69–84.

[3] P. Erdős and A. Sárközy, *On the number of prime factors of integers*, Acta Sci. Math. (Szeged) 42 (1980), 237–246.

[4] E. Fogels, *On the zeros of Hecke's L-functions I*, Acta Arith. 7 (1962), 87–106.

[5] —, *Über die Ausnahmenullstelle der Heckeschen L-Funktionen*, ibid. 8 (1963), 307–309.

[6] L. J. Goldstein, *A generalization of the Siegel–Walfisz theorem*, Trans. Amer. Math. Soc. 149 (1970), 417–429.

[7] H. Hasse, *Vorlesungen über Klassenkörpertheorie*, Würzburg, 1967.

[8] A. Hildebrand and G. Tenenbaum, *Integers without large prime factors*, J. Théor. Nombres Bordeaux 5 (1993), 411–484.

[9] J. C. Lagarias, H. L. Montgomery and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. 54 (1979), 271–296.

[10] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, 2. Bd., Leipzig, 1909.

[11] R. W. K. Odoni, *On the norms of algebraic integers*, Mathematika 22 (1975), 71–80.

[12] C. L. Siegel, *Abschätzungen von Einheiten*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II 1969, 71–86.

[13] H. M. Stark, *Some effective cases of the Brauer–Siegel theorem*, Invent. Math. 23 (1974), 135–152.

[14] A. I. Vinogradov, *On the extension to the left halfplane of the scalar product of Hecke L-series with magnitude characters*, Izv. Akad. Nauk SSSR Ser. Mat. 29 (1965), 485–492 (in Russian); English transl.: Amer. Math. Soc. Transl. (2) 82 (1969), 1–9.

[15] C. Walter, *The ambiguous class group and the genus class group of certain non-normal extensions*, Mathematika 26 (1979), 113–124.

[16] L. Washington, *Introduction to Cyclotomic Fields*, Springer, 1997.

Erindale College
University of Toronto
3359 Missisauga Road N
Missisauga, Ontario
Canada L5L 1C6
E-mail: vblomer@math.toronto.edu

Fachbereich Mathematik
Mathematisches Institut
Albert-Ludwigs-Universität
Eckerstr. 1
D-79104 Freiburg, Germany
E-mail: jcp@math.uni-freiburg.de

Received on 20.5.2005
and in revised form on 1.12.2005 (4992)