ACTA ARITHMETICA
XXI (1972)

Numbers with unique factorization in an algebraic number field

by

W. Narkiewicz (Wrocław)

*Dedicated to the memory of
Professor Wacław Sierpiński*

1. It is well-known (see [2]) that if K is an algebraic number field with the class-number $h \neq 1$ then almost all its integers have non-unique factorization. This means that if one denotes by $F(x)$ the number of nonassociated integers of K whose norms do not exceed x in absolute value and which have in K a unique factorization into irreducibles then the ratio $F(x)/x$ tends to zero as x goes to infinity.

In this paper we improve this, giving an asymptotic formula for $F(x)$ as well as for the number $F_k(x)$ of nonassociated integers a of K with $|N(a)| \leqslant x$ and at most k distinct factorizations. We obtain these formulas as a special case of a more general result, which we are now going to describe.

Let I be any ideal which has no principal prime ideal divisors and factorize it into prime ideals;

$$I = \mathfrak{p}_{11}^{a_{11}} \ldots \mathfrak{p}_{1c_1}^{a_{1c_1}} \ldots \mathfrak{p}_{h-1,1}^{a_{h-1,1}} \ldots \mathfrak{p}_{h-1,c_{h-1}}^{a_{h-1,c_{h-1}}},$$

with $\mathfrak{p}_{ij} \in X_i$, $X_1, \ldots, X_{h-1}$ being the non-principal ideal classes of K.

We shall say that the system

$$\tau = \tau(I) = \langle \{a_{11}, \ldots, a_{1c_1}\}, \ldots, \{a_{h-1,1}, \ldots, a_{h-1,c_{h-1}}\} \rangle \tag{1}$$

is the *type* of I. Two types: τ, given by (1) and

$$\tau' = \langle \{\beta_{11}, \ldots, \beta_{1c_1'}\}, \ldots, \{\beta_{h-1,1}, \ldots, \beta_{h-1,c_{h-1}'}\} \rangle$$

are considered equal, if for each i we have $c_i = c_i'$ and the systems

$$\{a_{i1}, \ldots, a_{ic_i}\},\ \{\beta_{i1}, \ldots, \beta_{ic_i}\}$$

differ only in the ordering.

We have to admit also the possibility of some c_i being 0. In this case we write Ø instead of $\{a_{i1}, \ldots, a_{ic_i}\}$.

So the type τ is determined unambigously by I.

If τ is a type of the form (1), then we define its *length* $l(\tau)$ by

$$l(\tau) = c_1 + \ldots + c_{h-1}$$

and its *depth* $d(\tau)$ by

$$d(\tau) = \mathcal{N}\{a_{ij} = 1:\ 1 \leqslant i \leqslant h-1,\ 1 \leqslant j \leqslant c_i\}.$$

Our main result consists in the following

THEOREM 1. *Let $\mathcal{A}$ be any set of principal ideals satisfying the following conditions:*

(i) *If $I \in \mathcal{A}$ and $\tau(J) = \tau(I)$ then $J \in \mathcal{A}$,*

(ii) *$\mathcal{A}$ contains every ideal all prime ideal factors of which are principal,*

(iii) *There is a constant B such that $I \in \mathcal{A}$ implies $d(\tau(I)) \leqslant B$.*

Then for the number $A(x)$ of ideals in $\mathcal{A}$ with $N(I) \leqslant x$ one has

$$A(x) = \big(C + o(1)\big)\frac{x(\log\log x)^M}{(\log x)^{1-1/h}}$$

where $C = C(\mathcal{A})$ is a positive constant, and

$$M = \max\{d(\tau(I)):\ I \in \mathcal{A}\} \leqslant B.$$

2. Before giving the proof we show how this theorem implies results for $F(x)$ and $F_k(x)$.

Note first that every class of associated integers determines uniquely a principal ideal and the divisibility and factorization properties of integers are reflected by those of principal ideals. So we may look for principal ideals with at most k factorizations into principal ideals, which cannot be factorized into principal ideals.

We apply the theorem with $\mathcal{A} = \mathcal{A}_k$ being the set of such ideals. The properties (i), (ii) being obviously satisfied, it suffices to prove (iii). This is done in

LEMMA 1. *Let for $i = 1, 2, \ldots, h-1$, $\omega_i(I)$ denote the number of distinct prime ideals from X_i dividing I. If $I \in \mathcal{A}_k$ then for $i = 1, 2, \ldots, h-1$ one has $\omega_i(I) \leqslant h(k+1)-1$.*

Proof. Let I be an ideal with $\omega_i(I) \geqslant h(k+1)$ for some i. Let g be the order of X_i and let $\mathfrak{p}_{11}, \ldots, \mathfrak{p}_{1g}, \mathfrak{p}_{21}, \ldots, \mathfrak{p}_{k+1,g} \in X_i$ divide I. Then the ideal $I_0 = \prod_{i,j} \mathfrak{p}_{ij}$ is principal and divides I, and

$$I_0 = \prod_{i=1}^{k+1} (\mathfrak{p}_{i1} \ldots \mathfrak{p}_{ig})$$

is one of its factorization into irreducibles. But interchanging here $\mathfrak{p}_{11}$ consecutively with $\mathfrak{p}_{21}, \mathfrak{p}_{31}, \ldots, \mathfrak{p}_{k+1,g}$ we get $k+1$ factorizations of I_0, and so $I \notin \mathcal{A}_k$. □

The application of Theorem 1 leads now to

THEOREM 2. *If $h(K) > 1$ one has*

$$F_k(x) = \big(C + o(1)\big)\frac{x(\log\log x)^{M_k}}{(\log x)^{1-1/h}}$$

where M_k is the maximal number of nonprincipal prime ideal factors which can occur in the factorization of a number with $\leqslant k$ factorization with the exponent one.

3. Note also that in principle the same reasoning as that given in sequel (with trivial changes), leads to similar theorems:

(a) One can in the definition of the type take in account also the principal class. In this case assumption (ii) of the theorem can be waved and the assertion will take the form

$$A(x) = \big(C + o(1)\big)\frac{x(\log\log x)^{M-1}}{\log x}, \quad C > 0.$$

(b) Instead of considering absolute ideal classes one can consider any partition of the prime ideals into a finite number of classes $X_1, \ldots, X_m$, such that the condition

$$\sum_{\mathfrak{p}\in X_i} \frac{1}{N\mathfrak{p}^s} = a_i \log\frac{1}{s-1} + g_i(s),$$

with $g_i(s)$ regular for $\operatorname{Re} s \geqslant 1$ and $a_i > 0$, is satisfied for $i = 1, 2, \ldots, m$.

The definition of a type should be modified correspondingly.

In this case the assertion takes the form

$$A(x) = \big(C + o(1)\big)\frac{x(\log\log x)^M}{(\log x)^{1-a_m}} \quad (C > 0)$$

if the class X_m plays the rôle of the principal class in the assumption (ii), and

$$A(x) = \big(C + o(1)\big)\frac{x(\log\log x)^{M-1}}{\log x}$$

if we extend the definition of a type as done in (a).

4. Denote by $S(\tau)$ the set of all ideals of the type τ, and by $\bar{S}(\tau)$ the set of all ideals of the form $J \cdot J_1$ with $J \in S(\tau)$ and with J_1 having all its prime ideal factors principal. Then by the condition (i) of Theorem 1 we obtain the existence of a set T of types, such that

$$A = \bigcup_{\tau \epsilon T} \bar{S}(\tau). \tag{2}$$

By the condition (iii) every $\tau \epsilon T$ satifies $d(\tau) \leqslant B$.

To get insight into behavior of $S(\tau)$ we prove.

LEMMA 2. *Let X be an ideal class, $d \geqslant 0$, $n \geqslant 0$, and $F_1(t), \ldots, F_u(t)$ real functions with $0 < F_i(t) \ll t^{-2}$. Let $S(s) = S(s; X; F_1, \ldots, F_u)$ denote the sum (well-defined for* $\operatorname{Re} s > 1$)

$$\sum_{\substack{\mathfrak{p}_1, \ldots, \mathfrak{p}_d \epsilon X \\ \text{distinct}}} \frac{1}{N\mathfrak{p}_1^s \ldots N\mathfrak{p}_d^s} \sum_{\substack{\mathfrak{q}_1, \ldots, \mathfrak{q}_u \epsilon X \\ \mathfrak{q}_i \neq \mathfrak{p}_j \text{ distinct}}} F_1(N\mathfrak{q}_1^s) \ldots F_u(N\mathfrak{q}_u^s).$$

Then for $\operatorname{Re} s > 1$ *we have*

$$S = P\left(\log \frac{1}{s-1}\right)$$

where $P(t)$ is a polynomial of degree d over the ring Ω of functions regular in $\operatorname{Re} s \geqslant 1$, with leading coefficient positive at $s = 1$. (Needless to say that the coefficients depend on $X, F_1, \ldots, F_u$.)

Proof. We utilise induction on d. For $d = 0$ and every u clearly $S(s) \epsilon \Omega(s)$ and

$$S(1) = \sum_{\substack{\mathfrak{q}_1, \ldots, \mathfrak{q}_u \epsilon X \\ \text{distinct}}} F_1(N\mathfrak{q}_1) \ldots F_u(N\mathfrak{q}_u) > 0.$$

Assume thus the truth of the lemma for all $\delta < d$, all u, and all functions $F_1, \ldots, F_u$ subject to $0 < F_i(t) \ll t^{-2}$. Then one can write

$$S(s) = S_1(s) - S_2(s)$$

where

$$S_1(s) = \sum_{\substack{\mathfrak{p}_1, \ldots, \mathfrak{p}_d \epsilon X \\ \text{distinct}}} \frac{1}{N\mathfrak{p}_1^s \ldots N\mathfrak{p}_d^s} \sum_{\substack{\mathfrak{q}_1, \ldots, \mathfrak{q}_u \epsilon X \\ \text{distinct}}} F_1(N\mathfrak{q}_1^s) \ldots F_u(N\mathfrak{q}_u^s), \tag{3}$$

and

$$S_2(s) = \sum_{\substack{\mathfrak{p}_1, \ldots, \mathfrak{p}_d \epsilon X \\ \text{distinct}}} \frac{1}{N\mathfrak{p}_1^s \ldots N\mathfrak{p}_d^s} \sum F_1(N\mathfrak{q}_1^s) \ldots F_s(N\mathfrak{q}_u^s)$$

where in the last inner sum the summation is carried over all prime ideals $\mathfrak{q}_i \epsilon X$ which are distinct, but at least one of them is equal to some $\mathfrak{p}_i$.

We deal first with $S_2(x)$. Take any non-void subset A of $\{1, 2, \ldots, u\}$ and consider the family F_A of all injective maps $f\colon A \to \{1, 2, \ldots, d\}$. With every such map associate the sum

$$S_f^{(s)} = \sum_{\substack{\mathfrak{p}_1, \ldots, \mathfrak{p}_d \epsilon X \\ \text{distinct}}} \frac{1}{N\mathfrak{p}_1^s \ldots N\mathfrak{p}_d^s} \sum F_1(N\mathfrak{q}_1^s) \ldots F_u(N\mathfrak{q}_u^s)$$

the inner summation carried over all distinct prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_u \epsilon X$ for which

(i) if $i \epsilon A$ then $\mathfrak{q}_i = \mathfrak{p}_{f(i)}$,

(ii) if $i \notin A$ then $\mathfrak{q}_i \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_d$.

Clearly

$$S_2(s) = \sum_{A \neq \emptyset} \sum_{f \epsilon F_A} S_f(s)$$

but

$$S_f(s) = \sum_{\substack{\mathfrak{p}_i \epsilon X \\ \text{distinct } i \notin A}} \frac{1}{\prod_{i \notin A} N\mathfrak{p}_i^s} \sum_{\substack{\mathfrak{q}_1, \ldots, \mathfrak{q}_u \epsilon X \\ \text{distinct} \\ \mathfrak{q}_i \neq \mathfrak{p}_j (j \notin A)}} \left(\prod_{i \notin A} F_i(N\mathfrak{q}_i^s) \prod_{i \notin A} \frac{F_i(N\mathfrak{q}_i^s)}{N\mathfrak{q}_i^s} \right)$$

$$= \sum_{\substack{\mathfrak{p}_i \epsilon X \\ \text{distinct} \\ i \notin A}} \frac{1}{\prod_{i \notin A} N\mathfrak{p}_i^s} \sum_{\substack{\mathfrak{q}_1, \ldots, \mathfrak{q}_u \epsilon X \\ \text{distinct} \\ \mathfrak{q}_i \neq \mathfrak{p}_j (j \notin A)}} G_1(N\mathfrak{q}_1^s) \ldots G_u(N\mathfrak{q}_u^s),$$

where

$$G_i(t) = \begin{cases} F_i(t), & i \notin A, \\ \dfrac{F_i(t)}{t} & i \epsilon A. \end{cases}$$

To the last sum we may apply the inductive assumption and so it turns out that $S_2(s)$ is a polynomial in $\log \dfrac{1}{s-1}$ over Ω of degree at most equal to $d-1$.

It remains to deal with $S_1(s)$. As the inner sum in (3) is independent on $\mathfrak{p}_1, \ldots, \mathfrak{p}_d$ and is obviously an element of Ω it suffices to consider

$$S_3(s) = \sum_{\substack{\mathfrak{p}_1, \ldots, \mathfrak{p}_d \epsilon X \\ \text{distinct}}} \frac{1}{N\mathfrak{p}_1^s \ldots N\mathfrak{p}_d^s}.$$

Obviously

$$S_4(s) = \sum_{\mathfrak{p}_1, \ldots, \mathfrak{p}_d \epsilon X} \frac{1}{N\mathfrak{p}_1^s \ldots N\mathfrak{p}_d^s} = \prod_{i=1}^{d} \sum_{\mathfrak{p}_i \epsilon X} \frac{1}{N\mathfrak{p}_i^s}$$

is a polynomial of degree d in $\log\frac{1}{s-1}$ over Ω with the highest coefficient equal to $1/h^d$ and we consider now the difference $S_4(s)-S_3(s)$. It equals the sum

$$\sum \frac{1}{N\mathfrak{p}_1^s \ldots N\mathfrak{p}_d^s}$$

taken over $\mathfrak{p}_1, \ldots, \mathfrak{p}_d \epsilon X$, at least two of them being equal. Let P be the set of all partitions of $\{1, 2, \ldots, d\}$ into disjoint non-void subsets at least one of which has $\geqslant 2$ elements. Let

$$\Gamma\colon \{i_1, \ldots, i_{l_1}\} \cup \{i_{l_1+1}, \ldots, i_{l_2}\} \cup \ldots \cup \{i_{l_{z-1}+1}, \ldots, i_{l_z}\}$$

be a typical representative of P.

If

$$A_\Gamma(s) = \sum_{\substack{\mathfrak{p}_{i_1}=\ldots=\mathfrak{p}_{i_{l_1}}\epsilon X \\ \cdots\cdots\cdots \\ \mathfrak{p}_{i_{l_{z-1}}}=\ldots=\mathfrak{p}_{i_{l_z}}\epsilon X \\ (\mathfrak{p}_{i_{l_1}},\ldots,\mathfrak{p}_{i_{l_z}}\text{ distinct})}} \frac{1}{N\mathfrak{p}_1^s \ldots N\mathfrak{p}_d^s},$$

then clearly

$$S_4(s)-S_3(s) = \sum_{\Gamma \epsilon P} A_\Gamma(s).$$

Considering a particular Γ, we may assume that $l_1 = \ldots = l_r = 1$; $l_{r+1}, \ldots, l_z > 1$ $(0 \leqslant r \leqslant z-1)$ and, permuting the indices if necessary, that $i_k = k$. Then $A_\Gamma(s)$ becomes

$$\sum_{\substack{\mathfrak{p}_1,\ldots,\mathfrak{p}_r \epsilon X \\ \text{distinct}}} \frac{1}{N\mathfrak{p}_1^s \ldots N\mathfrak{p}_r^s} \sum_{\substack{\mathfrak{q}_{1+r},\ldots,\mathfrak{q}_z \epsilon X \\ \text{distinct}}} \frac{1}{N\mathfrak{q}_{r+1}^{l_{r+1}s} \ldots N\mathfrak{q}_z^{l_z s}}$$

which is, according to the inductive assumption, a polynomial in $\log\frac{1}{s-1}$ over Ω of degree $r \leqslant d-1$.

Hence $S_3(s) = S_4(s) - \sum_{\Gamma\epsilon P} A_\Gamma(s)$ is a polynomial of degree d in $\frac{1}{s-1}$ over Ω and its highest coefficient equals

$$\frac{1}{h^d} \sum_{\substack{\mathfrak{q}_1,\ldots,\mathfrak{q}_u \epsilon X \\ \text{distinct}}} F_1(N\mathfrak{q}_1^s) \ldots F_u(N\mathfrak{q}_u^s)$$

at so has a positive value at $s=1$. □

Corollary 1. *If X_j is a given non-principal class and*

$$\tau = (\emptyset, \ldots, \emptyset, \{a_{j1}, \ldots, a_{jc_j}\}, \emptyset, \ldots, \emptyset)$$

then for $\operatorname{Re} s > 1$

$$\sum_{I\epsilon S(\tau)} \frac{1}{N(I)^s} = \mathscr{V}_\tau\left(\log\frac{1}{s-1}\right)$$

where $\mathscr{V}_T(t)$ is a polynomial over Ω. The degree of $\mathscr{V}_T$ equals the depth $d(\tau)$ and the value of leading coefficient at $s=1$ is positive.

Proof. Assume freely, that $a_{j1} = \ldots = a_{jd} = 1$, with $d = d(\tau)$. Moreover let $r(\tau)$ be the number of permutations π of the set $\{1, \ldots, c_j\}$ for which

$$a_{j\pi(k)} = a_{jk}.$$

Then we have

$$\sum_{I\epsilon S(\tau)} \frac{1}{N(I)^s} = \frac{1}{r(\tau)} \sum_{\substack{\mathfrak{p}_1,\ldots,\mathfrak{p}_d \epsilon X \\ \text{distinct}}} \frac{1}{N\mathfrak{p}_1^s \ldots N\mathfrak{p}_d^s} \sum_{\substack{\mathfrak{p}_{d+1},\ldots,\mathfrak{p}_{c_j} \epsilon X \\ \text{distinct} \\ \text{and} \neq \mathfrak{p}_i (i \leqslant d)}} \frac{1}{N\mathfrak{p}_{d+1}^{a_{j,d+1}s} \ldots N\mathfrak{p}_{c_j}^{a_{jc_j}s}}$$

and so the lemma is applicable with

$$F_j(t) = t^{-a_{j,d+j}}. \ \square$$

Corollary 2. *If τ is an arbitrary type, given in the form* (1), *then for* $\operatorname{Re} s > 1$ *one has*

$$\sum_{I\epsilon S(\tau)} \frac{1}{N(I)^s} = \mathscr{V}_\tau\left(\log\frac{1}{s-1}\right)$$

with $\mathscr{V}_\tau(t)$ being a polynomial over Ω, of degree $d(\tau)$, and highest coefficient positive at $s=1$.

Proof. In fact, if

$$\tau_j = \langle \emptyset, \ldots, \emptyset, \{a_{j1}, \ldots, a_{jc_j}\}, \emptyset, \ldots \rangle$$

then

$$\sum_{I\epsilon S(\tau)} \frac{1}{N(I)^s} = \prod_{j=1}^{h-1} \sum_{I\epsilon S(\tau_j)} \frac{1}{N(I)^s} = \prod_{j=1}^{h-1} \mathscr{V}_{\tau_j}\left(\log\frac{1}{s-1}\right)$$

by Corollary 1. □

Corollary 3. *If τ is any type, then for* $\operatorname{Re} s > 1$ *one has*

$$\sum_{I\epsilon \overline{S}(\tau)} \frac{1}{N(I)^s} = g(s) \frac{\mathscr{V}_\tau\left(\log\frac{1}{s-1}\right)}{(s-1)^{1/h}}$$

where $g(s) \in \Omega$ is independent on τ, $g(1) > 0$ and $\mathscr{V}_\tau$ is the polynomial from Corollary 2.

Proof. Write

$$\sum_{I \in \bar{S}(\tau)} \frac{1}{N(I)^s} = \prod_{\mathfrak{p} \in E} \frac{1}{1 - \dfrac{1}{N\mathfrak{p}^s}} \sum_{I \in S(\tau)} \frac{1}{N(I)^s},$$

observe that

$$\prod_{\mathfrak{p} \in E} \frac{1}{1 - \dfrac{1}{N\mathfrak{p}^s}} = \frac{g(s)}{(s-1)^{1/h}} \qquad (g \in \Omega,\ g(1) > 0)$$

and apply Corollary 2. □

Corollary 4. *Let $\mathscr{A}$ be any set of types of the same depth d. Then for* $\operatorname{Re} s > 1$ *one has*

$$C(S) = \sum_{\tau \in \mathscr{A}} \sum_{I \in S(\tau)} \frac{1}{N(I)^s} = \mathscr{V}_{\mathscr{A}}\left(\log \frac{1}{s-1}\right)$$

where $\mathscr{V}_{\mathscr{A}}(t)$ is a polynomial over Ω of degree d with the leading coefficient positive at $s = 1$.

Proof. Let $\mathscr{A}_{d_1, \ldots, d_{h-1}}$ be the set of all types τ of the form (1) with

$$\mathscr{N}\{a_{jk} = 1\colon 1 \leqslant k \leqslant c_j\} = d_j.$$

Then

$$\mathscr{A} = \bigcup_{d_1 + \ldots + d_{h-1} = d} \mathscr{A}_{d_1, \ldots, d_{h-1}} \cap \mathscr{A}$$

and so it is sufficient to prove our assertion separately for each set $\mathscr{A}_{d_1, \ldots, d_{h-1}} \cap \mathscr{A} = \mathscr{A}'$.

We use induction in d. If $d = 0$, then

$$C(S) \in \Omega$$

as the series is majorized for $\operatorname{Re} s > \frac{1}{2}$ by $\sum\limits_{I} \dfrac{1}{N(I)^s}$ in which the sum is taken over all ideals I with $\mathfrak{p} | I \rightarrow \mathfrak{p}^2 | I$.

Assume the truth for all $\delta < d$ and write our sum in the form

$$\frac{1}{d_1!\, d_2! \ldots d_{n-1}!} \sum_{\substack{\mathfrak{p}_1, \ldots, \mathfrak{p}_{d_1} \in X_1 \\ \mathfrak{p}_{1+d_1}, \ldots, \mathfrak{p}_{d_2+d_1} \in X_2 \\ \cdots\cdots\cdots \\ \text{distinct}}} \frac{1}{N\mathfrak{p}_1^s \ldots N\mathfrak{p}_d^s} \times$$

$$\times \sum_{u=0}^{\infty} \sum_{\substack{\tau \in A' \\ l(\tau) = u+d}} \frac{1}{c(\tau)} \sum_{\mathfrak{q}_1, \ldots, \mathfrak{q}_u} \frac{1}{\mathfrak{q}_1^{s\beta_1} \ldots \mathfrak{q}_u^{s\beta_u}}$$

where the last inner sum is taken over distinct (and $\neq \mathfrak{p}_1, \ldots, \mathfrak{p}_d$) prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_u$ lying in classes prescribed by τ and the exponents $\beta_1, \ldots, \beta_u \geqslant 2$ are also prescribed by τ. The coefficient $c(\tau)$ denotes the number of permutations π of $\{1, 2, \ldots, n\}$ such that if

$$\begin{gathered} \mathfrak{q}_1, \ldots, \mathfrak{q}_{l_1} \in X_1, \\ \mathfrak{q}_{1+l_1}, \ldots, \mathfrak{q}_{l_2} \in X_2, \\ \cdots\cdots\cdots\cdots \end{gathered}$$

are the conditions given by τ, then the sets $\{1, \ldots, l_1\}$, $\{1 + l_1, \ldots, l_2\}, \ldots$ are stable under π and moreover $\beta_{\pi(j)} = \beta_j$.

Now the last sum equals

$$\sum_{\substack{\mathfrak{q}_1, \ldots, \mathfrak{q}_u \\ \text{distinct}}} \frac{1}{\mathfrak{q}_1^{s\beta_1} \ldots \mathfrak{q}_u^{s\beta_u}} - \sum_{\substack{\mathfrak{q}_1, \ldots, \mathfrak{q}_u \\ \text{distinct} \\ \text{some equal to} \\ \text{certain } \mathfrak{p}_j\text{–}s}} \frac{1}{\mathfrak{q}_1^{s\beta_1} \ldots \mathfrak{q}_u^{s\beta_u}} = B_1(s) - B_2(s).$$

But

$$\sum_{u=0}^{\infty} \sum_{\substack{\tau \in A \\ l(\tau) = u+d}} B_1(s) \in \Omega$$

and

$$\sum_{\substack{\mathfrak{p}_1, \ldots, \mathfrak{p}_{d_1} \in X_1 \\ \cdots\cdots\cdots}} \frac{1}{N(\mathfrak{p}_1^s) \ldots N(\mathfrak{p}_d^s)} \sum_{u=0}^{\infty} \sum_{\substack{\tau \in A' \\ l(\tau) = u+d}} B_2(s)$$

can be dealt with in the same way as $S_2(s)$ in the proof of the lemma. We arrive thus at

$$C(s) = B_1(s) \sum_{\substack{\mathfrak{p}_1, \ldots, \mathfrak{p}_{d_1} \in X_1 \\ \cdots\cdots\cdots}} \frac{1}{N\mathfrak{p}_1^s \ldots N\mathfrak{p}_d^s} + Q\left(\log \frac{1}{s-1}\right)$$

where $Q(t)$ is a polynomial of degree $\leqslant d-1$ over Ω. Utilizing Corollary 2 and the obvious inequality $B_1(1) > 0$ we arrive at our assertion. □

Corollary 5. *Let $\mathscr{A}$ be any set of types of the same depth d. Then for* $\operatorname{Re} s > 1$ *one has*

$$\sum_{\tau \in \mathscr{A}} \sum_{I \in \bar{S}(\tau)} \frac{1}{N(I)^s} = \frac{g(s) \mathscr{V}_{A}\left(\log \dfrac{1}{s-1}\right)}{(s-1)^{1/h}}.$$

Proof. Immediate. □

5. Proof of the theorem. For $\mathrm{Re}\, s > 1$ we have

$$\sum_{I\in\mathscr{A}} \frac{1}{N(I)^s} = \sum_{\tau\in T} \sum_{I\in S(\tau)} \frac{1}{N(I)^s}$$

with $d(\tau) \leqslant M$ for each $\tau\in T$, thus

$$\sum_{I\in\mathscr{A}} \frac{1}{N(I)^s} = \sum_{j=0}^{M} \sum_{\substack{\tau\in T\\ d(\tau)=j}} \sum_{I\in\bar{S}(\tau)} \frac{1}{N(I)^s}$$

and by the last corollary this equals

$$\frac{g(s)\mathscr{V}\left(\log\dfrac{1}{s-1}\right)}{(s-1)^{1/h}}$$

with $\mathscr{V}(t)$ being a polynomial over Ω of degree M, with leading coefficient positive at $s=1$ and $g(1)>0$. Applying the tauberian theorem of H. Delange ([1]) we get our assertion.

References

[1] H. Delange, *Généralisation du théorème de Ikehara*, Ann. Sci. Ec. Norm. Sup. 71 (1954), pp. 213–242.

[2] W. Narkiewicz, *On algebraic number fields with nonunique factorization*, Colloq. Math. 12 (1964), pp. 59–68.

MATHEMATICAL INSTITUTE, WROCŁAW UNIVERSITY
UNIVERSITÈ BORDEAUX I

Received on 2. 8. 1971 (201)

ACTA ARITHMETICA
XXI (1972)

Über die Idealklassengruppe des Dirichletschen biquadratischen Zahlenkörpers

von

HANS REICHARDT (Berlin)

Zum Gedenken an W. Sierpiński

Gauß hat seine komplexen ganzen Zahlen nicht nur um ihrer selbst willen eingeführt, sondern um eine Theorie der biquadratischen Reste in Analogie zu der der quadratischen Reste aufzubauen, was ihm, solange er viele Jahre im Bereich der rationalen Zahlen blieb, nicht in befriedigender Weise gelingen wollte, aber dann im Komplexen sofort zum Reziprozitätsgesetz nebst Ergänzungssätzen für die 4. Potenzreste führte. Im Gegensatz zu Gauß schlug Dirichlet [1] vor, die ganzen Gaußschen Zahlen als selbständiges Forschungsobjekt zu betrachten und deren Theorie ganz nach dem Muster der Theorie der rationalen Zahlen soweit wie möglich aufzubauen. Es lag für ihn natürlich besonders nahe, seine eigenen neuen Methoden, vor allem die analytische Bestimmung der Klassenzahl quadratischer Formen, zu übertragen, also die Klassenzahlen solcher quadratischen Formen zu berechnen, deren Koeffizienten und deren Variable ganze Gaußsche Zahlen sind. Das für ihn überraschendste und schönste Ergebnis war die Erkenntnis, ausgedrückt in unserer heutigen idealtheoretischen Betrachtungsweise, daß die Klassenzahl h eines Körpers B, der von i und $\sqrt{D}$, wobei D die Diskriminante eines quadratischen Zahlkörpers über dem Körper Q der rationalen Zahlen ist, über Q erzeugt wird, gleich h_1h_2 oder $h_1h_2/2$ ist, wobei h_1 die Klassenzahl von $Q_1 = Q(\sqrt{D})$ und h_2 die von $Q_2 = Q(\sqrt{-D})$ ist. Dafür, welcher der beiden Fälle vorliegt, gab er ein einfaches Kriterium an.

Später hat Hilbert [3] den Vorschlag von Dirichlet weiterverfolgt und eine zur Gaußschen Geschlechtertheorie Q analoge über $Q_0 = Q(i)$ aufgebaut. Die Ergebnisse konnte er zu einem neuen und rein arithmetischen Beweis des Resultats von Dirichlet verwerten. Zwar lautet das Hilbertsche Kriterium anders als das von Dirichlet, doch lassen sich beide leicht ineinander überführen.