COLLOQUIUM MATHEMATICUM

VOL. LXV 1993 FASC. 2

FACTORIZATION PROBLEMS IN CLASS NUMBER TWO

BY

FRANZ HALTER-KOCH (GRAZ)

Introduction. Let K be an algebraic number field, R its ring of integers, G its ideal class group and $N = \#G > 1$ its class number. For $k \ge 1$ and $x \in \mathbb{R}_{>0}$, let $F_k(x)$ be the number of elements $\alpha \in R$ (up to associates) having at most k different factorizations into irreducible elements of R. W. Narkiewicz [9] obtained the asymptotic expression

$$F_k(x) \sim c_k x\,(\log x)^{-1+1/N}(\log\log x)^{a_k}\,,$$

where $c_k \in \mathbb{R}_{>0}$ depends on k and K, and $a_k \in \mathbb{N}$ depends only on k and G. In [4], this was generalized to abstract arithmetical formations, emphasizing applications to algebraic function fields and to arithmetical semigroups (e.g. Hilbert semigroups $1 + f\mathbb{N}_0$ and, more generally, ray class semigroups in algebraic number fields).

In this paper we give an explicit description of a_k and c_k in the simplest non-trivial case $N = 2$. For a_k, this is a purely combinatorial problem, settled in Theorems 2 and 3. For the calculation of c_k, it is necessary to handle some infinite sums and products involving primes, which might be of independent interest (Propositions 1 and 2). We formulate our investigations in the frame of arithmetical formations having zeta functions; the analytical main results are Theorems 1 and 4.

1. Arithmetical formations. We introduce the concept of an arithmetical formation following [6]. By a *semigroup* we always mean a commutative monoid satisfying the cancellation law; the identity element is denoted by 1.

Definition. A *formation* consists of

1) a free abelian semigroup D with basis $P \ne \emptyset$, together with a congruence relation $\sim$ on D such that $G = D/\!\sim$ is a finite abelian group (written additively) of order $N \ge 2$,

2) a completely multiplicative function $|\cdot| : D \to \mathbb{N}$ with the following three properties:

(i) $|a| > 1$ for all $a \in D \setminus \{1\}$;

(ii) there exist real numbers $\lambda > 0$ and $0 < \delta < 1$ such that, for all $g \in G$ and $x \in \mathbb{R}_{>0}$,

$$\#\{a \in g \mid |a| \le x\} = \lambda x + O(x^{1-\delta});$$

(iii) Axiom (A**), to be explained below.

Let $G^* = \mathrm{Hom}(G, \mathbb{C}^\times)$ be the character group of G and $\chi_0 \in G^*$ the principal character. For $a \in D$, we denote by $[a] \in G$ the class of a, and for $\chi \in G^*$ we set $\chi(a) = \chi([a])$. We introduce the Hecke–Landau zeta functions

$$Z(s,\chi) = \sum_{a \in D} \chi(a)|a|^{-s};$$

the defining Dirichlet series converge for $\Re s > 1$ and have an Euler product expansion

$$Z(s,\chi) = \prod_{p \in P} (1 - \chi(p)|p|^{-s})^{-1}.$$

The functions $Z(s,\chi)$ have analytic continuations to meromorphic functions in the half-plane $\Re s > 1-\delta$. For $\chi \ne \chi_0$, $Z(s,\chi)$ is holomorphic in $\Re s > 1-\delta$, and $Z(s) = Z(s,\chi_0)$ has a simple pole at $s = 1$ with residue λ. We have $Z(1+it,\chi) \ne 0$ for all $t \in \mathbb{R}$ and $\chi \in G^*$ unless $t = 0$ and $\chi^2 = \chi_0$; for this special case, we introduce

Axiom (A**). $Z(1,\chi) \ne 0$.

Taking logarithms in the Euler product of $Z(s,\chi)$ and applying the orthogonality relations for characters, we obtain for every $g \in G$ and $\Re s > 1$,

$$\sum_{p \in P \cap g} |p|^{-s} = \frac{1}{N} \log \frac{1}{s-1} + h_g(s),$$

where

$$\begin{aligned} h_g(s) = {}& \frac{1}{N} \log\{(s-1)Z(s)\} \\ &+ \frac{1}{N} \sum_{\substack{\chi \in G^* \\ \chi \ne \chi_0}} \overline{\chi}(g) \log Z(s,\chi) - \sum_{p \in P \cap g} \sum_{\nu=2}^{\infty} |p|^{-\nu s}. \end{aligned}$$

The functions $h_g(s)$ are regular in the closed half-plane $\Re s \ge 1$. Therefore an arithmetical formation as introduced above is a formation in the sense of [4], and the algebra of all complex functions which are analytic in $\Re s \ge 1$ is suitable for this formation.

For an arithmetical formation as introduced above, our main interest lies in the arithmetic of the semigroup

$$H = \{a \in D \mid a \sim 1\} = \{a \in D \mid [a] = 0 \in G\}.$$

The injection $H \hookrightarrow D$ is a divisor theory [4, Lemma 1], and therefore D and G are uniquely determined by H [2, Bemerkung 4]. In the sequel, we shall speak about *the arithmetical formation* $[D,H]$, and we shall tacitly use the notations $P, |\cdot|, G, N, Z$ as above.

The most important examples of arithmetical formations to be considered in this paper are ray class semigroups in algebraic number fields (see [2, Beispiel 4] and [8, Ch. VI, §1]):

Let K be an algebraic number field, $\mathfrak{c}$ a cycle of K, $\mathcal{I}(\mathfrak{c})$ the group of fractional ideals of K relatively prime to $\mathfrak{c}$, $\mathcal{I}_0(\mathfrak{c})$ the semigroup of integral ideals in $\mathcal{I}(\mathfrak{c})$, $K(\mathfrak{c}) = \{(\alpha) \in \mathcal{I}(\mathfrak{c}) \mid \alpha \in K^\times, \alpha \equiv 1 \bmod^\times \mathfrak{c}\}$, $\mathcal{S}(\mathfrak{c}) = \mathcal{I}(\mathfrak{c})/K(\mathfrak{c})$ the ray class group modulo $\mathfrak{c}$ and $\Gamma \subset \mathcal{S}(\mathfrak{c})$ a subgroup. Then

$$\mathcal{I}^\Gamma(\mathfrak{c}) = \{\mathfrak{a} \in \mathcal{I}_0(\mathfrak{c}) \mid \mathfrak{a}K(\mathfrak{c}) \in \Gamma\}$$

is a subsemigroup of $\mathcal{I}_0(\mathfrak{c})$. We set $D = \mathcal{I}_0(\mathfrak{c})$, $H = \mathcal{I}^\Gamma(\mathfrak{c})$ and $|\mathfrak{a}| = \mathfrak{N}(\mathfrak{a})$; then $[D,H]$ becomes a formation with divisor class group $G \simeq \mathcal{S}(\mathfrak{c})/\Gamma$ (see [7, Sätze LXIV, XCVI] and [8, Ch. XIII, §3]).

Every character $\chi \in G^*$ induces a (not necessarily primitive) ideal character χ_1 mod $\mathfrak{c}$ by

$$\chi_1(\mathfrak{a}) = \begin{cases} \chi(\mathfrak{a}K(\mathfrak{c})\Gamma) & \text{if } \mathfrak{a} \in \mathcal{I}(\mathfrak{c}), \\ 0 & \text{if } \mathfrak{a} \notin \mathcal{I}(\mathfrak{c}), \end{cases}$$

and

$$Z(s,\chi) = \zeta_K(s,\chi_1)$$

is the classical Hecke zeta function for χ_1. If $\mathfrak{c} = 1$, then $\mathcal{S}(\mathfrak{c})$ is the usual ideal class group, and if $\Gamma = \{1\}$, then $H = \mathcal{I}^\Gamma(\mathfrak{c})$ is the semigroup of non-zero principal ideals of K (which reflects the arithmetic in the ring of integers in K).

The following special case will be dealt with in detail: Let φ be a (primitive) Hecke character of order 2 with conductor $\mathfrak{c}$, identify φ with the induced homomorphism $\varphi : \mathcal{S}(\mathfrak{c}) \to \{\pm 1\}$, set $\Gamma = \mathrm{Ker}(\varphi) \subset \mathcal{S}(\mathfrak{c})$ and $H_\varphi = \mathcal{I}^\Gamma(\mathfrak{c})$. Then $[\mathcal{I}_0(\mathfrak{c}), H_\varphi]$ is an arithmetical formation whose class group G is of order $N = 2$, and φ induces the non-trivial character on G. Associated with this arithmetical formation, there are two zeta functions, $Z(s)$ and $Z(s,\varphi)$, and we obtain

$$Z(s) = \zeta_K(s) \prod_{\mathfrak{p} \mid \mathfrak{c}} (1 - \mathfrak{N}(\mathfrak{p})^{-s}) \quad \text{and} \quad Z(s,\varphi) = L(s,\varphi)\,;$$

here ζ_K is the Dedekind zeta function of K, $L(s,\varphi)$ is the usual L-series, and consequently $\zeta_{K(\varphi)}(s) = \zeta_K(s)L(s,\varphi)$, where $K(\varphi)$ is the quadratic extension field of K attached to φ by class field theory. The following examples will be reconsidered at the end of §4.

EXAMPLE 1. $K=\mathbb{Q}$, $\mathfrak{c}=4\infty$, $\mathcal{I}_0(\mathfrak{c})=\{a\in\mathbb{N}\mid a\equiv 1 \bmod 2\}$, $\varphi=\left(\frac{-4}{\bullet}\right)$, $H_\varphi=1+4\mathbb{N}_0$, $Z(s)=(1-2^{-s})\zeta(s)$, $Z(s,\varphi)=L(s,\varphi)$ and $K(\varphi)=\mathbb{Q}(\sqrt{-1})$.

EXAMPLE 2. $K=\mathbb{Q}$, $\mathfrak{c}=5$, $\mathcal{I}_0(\mathfrak{c})=\{a\in\mathbb{N}\mid a\not\equiv 0 \bmod 5\}$, $\varphi=\left(\frac{5}{\bullet}\right)$, $H_\varphi=\{a\in\mathbb{N}\mid a\equiv\pm1 \bmod 5\}$, $Z(s)=(1-5^{-s})\zeta(s)$, $Z(s,\varphi)=L(s,\varphi)$ and $K(\varphi)=\mathbb{Q}(\sqrt{5})$.

EXAMPLE 3. $K=\mathbb{Q}(\sqrt{-5})$, $\mathfrak{c}=(1)$, $\mathcal{I}_0(\mathfrak{c})$ is the semigroup of all non-zero ideals of $\mathbb{Z}[\sqrt{-5}]$, H_φ is the semigroup of all non-zero principal ideals of $\mathbb{Z}[\sqrt{-5}]$, φ is the non-trivial character on the ideal class group of K, $Z(s)=\zeta_K(s)$ and $K(\varphi)=\mathbb{Q}(\sqrt{5},\sqrt{-5})$.

2. Factorizations and types. Let $[D,H]$ be an arithmetical formation. For H, we use the notions of divisibility theory as introduced in [1, §6]. We are interested in the number $\mathbf{f}(\alpha)$ of distinct factorizations of an element $\alpha\in H$ into irreducibles (two factorizations are called distinct if they differ not only in the order of their factors). For $k\in\mathbb{N}$, we consider the function

$$F_k(x)=\#\{\alpha\in H\mid |\alpha|\le x,\ \mathbf{f}(\alpha)\le k\}\,.$$

For the determination of its asymptotic behaviour, we introduce the notion of types (cf. [9], [4] and [3] for a more systematical treatment of this concept).

DEFINITION. A *type* is a sequence

$$t=((t_{g,\nu})_{\nu\in\mathbb{N}})_{0\ne g\in G}\,,$$

where $t_{g,\nu}\in\mathbb{N}_0$, $t_{g,\nu}=0$ for almost all indices (g,ν), and

$$\sum_{0\ne g\in G}\ \sum_{\nu\ge1} t_{g,\nu}\, g=0\in G\,;$$

the number

$$\delta(t)=\#\{(g,\nu)\mid t_{g,\nu}=1\}\in\mathbb{N}_0$$

is called the *depth* of t. Under componentwise addition, the set of types is a semigroup $\mathcal{T}(G)$, and we adopt the notions of divisibility theory also for $\mathcal{T}(G)$. Every $t\in\mathcal{T}(G)$ has a factorization into irreducible elements of $\mathcal{T}(G)$, and we denote by $\mathbf{f}(t)$ the number of distinct such factorizations.

A type $t=((t_{g,\nu})_{\nu\ge1})_{0\ne g\in G}\in\mathcal{T}(G)$ is called *normalized* if for every $0\ne g\in G$ there exists an integer $\lambda_g\in\mathbb{N}_0$ such that $1\le t_{g,1}\le t_{g,2}\le\ldots\le t_{g,\lambda_g}$ and $t_{g,\nu}=0$ for $\nu>\lambda_g$; in this case we write $t=((t_{g,\nu})_{\nu\le\lambda_g})_{0\ne g\in G}$.

Now let $[D,H]$ be an arbitrary arithmetical formation. We are going to describe factorizations in H by means of $\mathcal{T}(G)$. For $\alpha\in H$, we set

$$\alpha=\prod_{g\in G}\prod_{\nu=1}^{\lambda_g} p_{g,\nu}^{t_{g,\nu}}$$

where $\lambda_g \in \mathbb{N}_0$, $p_{g,1}, \ldots, p_{g,\lambda_g} \in P \cap g$ are distinct, $t_{g,\nu} \in \mathbb{N}$ and $1 \le t_{g,1} \le t_{g,2} \le \ldots \le t_{g,\lambda_g}$; we call

$$\boldsymbol{\tau}(\alpha) = ((t_{g,\nu})_{\nu \le \lambda_g})_{0 \ne g \in G} \in \mathcal{T}(G)$$

the *type of* α. It is not difficult to see that $\mathbf{f}(\alpha) = \mathbf{f}(\boldsymbol{\tau}(\alpha))$ (cf. [3] for details).

For $k \in \mathbb{N}$, we set

$$\mathcal{T}_k(G) = \{t \in \mathcal{T}(G) \mid \mathbf{f}(t) \le k\}\,;$$

then we obviously have, for $x \in \mathbb{R}_{>0}$,

$$F_k(x) = \#\{\alpha \in H \mid |\alpha| \le x,\ \boldsymbol{\tau}(\alpha) \in \mathcal{T}_k(G)\}\,,$$

and it was proved in [9] (see also [4], [3]) that

$$a_k = a_k(G) = \sup\{\delta(t) \mid t \in \mathcal{T}_k(G)\}$$

is a positive integer. Now we are able to state the theorem concerning the asymptotic behaviour of $F_k(x)$ in arithmetical formations.

THEOREM 1. *Let* $[D, H]$ *be an arithmetical formation*, $k \in \mathbb{N}$ *and* $a_k = a_k(G)$. *Then we have, as* $x \to \infty$,

$$F_k(x) \sim c_k x\,(\log x)^{-1+1/N}(\log\log x)^{a_k}\,,$$

where

$$c_k = \frac{G(1)}{N^d \Gamma(1/N)} \sum_t \kappa_t C_t\,;$$

here we have

$$G(s) = (s-1)^{-1/N} \prod_{p \in P \cap H} (1 - |p|^{-s})^{-1}\,,$$

the sum is over all normalized types $t \in \mathcal{T}_k(G)$ *such that* $\delta(t) = a_k$, *and for a normalized type* $t = ((t_{g,\nu})_{\nu \le \lambda_g})_{0 \ne g \in G}$ *the quantities* κ_t *and* C_t *are defined as follows*:

$$\kappa_t = \prod_{0 \ne g \in G} \#\{\pi \in \mathfrak{S}_{\lambda_t} \mid t_{g,\pi(\nu)} = t_{g,\nu} \text{ for all } \nu \le \lambda_g\}^{-1}\,,$$

and if $d_g \in \mathbb{N}_0$ *are integers defined by* $t_{g,\nu} = 1$ *for* $1 \le \nu \le d_g$ *and* $t_{g,\nu} > 1$ *for* $d_g < \nu \le \lambda_g$, *then*

$$C_t = \prod_{0 \ne g \in G} \sum_{(\mathbf{q};g)} \prod_{\nu = d_g+1}^{\lambda_g} |q_\nu|^{-t_{g,\nu}}\,,$$

where $(\mathbf{q}; g)$ *denotes the sum over all tuples* $(q_{d_g+1}, \ldots, q_{\lambda_g})$ *of distinct primes* $q_j \in P \cap g$.

Proof. See [4, Theorem 1]; there the constant c_k is not given explicitly, but it can be reconstructed from the proof. ∎

Remark. Using the methods of [5], the assertion of Theorem 1 can be refined by giving further terms of the asymptotic expansion of $F_k(x)$ if $[D,H]$ arises from a ray class semigroup in an algebraic number field.

To make Theorem 1 more explicit, it is necessary to calculate $a_k(G)$, determine all normalized types $t \in \mathcal{T}_k(G)$ with $\delta(t) = a_k(G)$ and manage the calculation of the infinite series occurring in the definition of C_t. In this paper we shall solve these problems for the simplest non-trivial case, where $G = C_2$ is a group of 2 elements.

3. Combinatorial theory of types over C_2. Let $G = C_2$ be a group of two elements. Then $\mathcal{T}(C_2)$ consists of all sequences $(t_\nu)_{\nu\ge 1}$, where $t_\nu \in \mathbb{N}_0$, $t_\nu = 0$ for almost all $\nu \ge 1$ and $\sum_{\nu\ge1} t_\nu \equiv 0 \bmod 2$; the normalized types are finite sequences $(t_1,\dots,t_\lambda)$ in $\mathbb{N}$ satisfying $t_1+\ldots+t_\lambda \equiv 0 \bmod 2$.

For $n,k \in \mathbb{N}_0$, $n+k>0$, $n+k \equiv 0 \bmod 2$, we set

$$t^{(n,k)} = (\underbrace{1,\dots,1}_{n}, k) \in \mathcal{T}(C_2) \quad \text{and} \quad C(n,k) = \mathbf{f}(t^{(n,k)})\,.$$

Theorem 2. *For $n,k \in \mathbb{N}_0$, $n+k>0$, $n+k \equiv 0 \bmod 2$, we have*

$$C(n,k) = \sum_{\nu=0}^{[k/2]} \binom{n}{k-2\nu} (n-k+2\nu-1)!!\,,$$

where

$$l\,!! = \begin{cases} 1\cdot 3\cdot 5\cdot\ldots\cdot l & \text{if } l \in \mathbb{N} \text{ is odd,}\\ 1 & \text{otherwise.}\end{cases}$$

Proof. For $n \ge 1$, every factorization of $t^{(n,k)}$ into irreducible types contains exactly one irreducible factor of the form $(1,0,\dots,0,1,0,\dots,0)$. Therefore the numbers $C(n,k)$ satisfy the following recursion formulas:

$$\begin{aligned} C(1,k) &= C(0,k) = 1 && \text{for } k \ge 0\,;\\ C(n+1,0) &= C(n,1) && \text{for } n \ge 1\,;\\ C(n,0) &= (n-1)C(n-2,0) && \text{for } n \ge 2\,;\\ C(n,k) &= (n-1)C(n-2,k) + C(n-1,k-1) && \text{for } n \ge 2,\ k \ge 1\,. \end{aligned}$$

These are satisfied by the expression given in Theorem 1. ■

Theorem 3. *For $k \in \mathbb{N}$, let $n \in \mathbb{N}$ be maximal such that $(2n-1)!! \le k$. Then*

$$a_k(C_2) = 2n\,,$$

and

$$\{t \in \mathcal{T}_k(C_2) \mid \ t \text{ normalized},\ \delta(t) = 2n\} = \{t^{(2n,2j)} \mid j \in J_k\}\,,$$

where J_k is given as follows:

$J_k = \{0\}$ *if* $k = 1$, $3 \le k \le 8$, $15 \le k \le 59$, $105 \le k \le 524$, $945 \le k \le 5669$, $10395 \le k \le 72764$ *or* $n \ge 7$, $(2n-1)!! \le k < (2n-1)!!\,(n+1)$;

$J_k = \{0,1\}$ *if* $k = 9$, $60 \le k \le 74$, $525 \le k \le 734$, $5670 \le k \le 8819$, $72765 \le k \le 124739$ *or* $n \ge 7$, $(2n-1)!!\,(n+1) \le k < (2n+1)!!$;

$J_k = \{0,1,2\}$ *if* $k = 75$, $735 \le k \le 762$, $8820 \le k \le 9449$ *or* $124740 \le k \le 135134$;

$J_k = \{0,1,2,3\}$ *if* $k = 763$ *or* $9450 \le k \le 9494$;

$J_k = \{0,1,2,3,4\}$ *if* $k = 9495$;

$J_k = \mathbb{N}_0$ *if* $k = 2$, $10 \le k \le 14$, $76 \le k \le 104$, $764 \le k \le 944$ *or* $9496 \le k \le 10394$.

Proof. Let $k \in \mathbb{N}$ be given, and let $n \in \mathbb{N}$ be maximal such that $(2n-1)!! \le k$.

By Theorem 2, $\mathbf{f}(t^{(2n,0)}) = (2n-1)!!$ and $\delta(t^{(2n,0)}) = 2n$. Therefore we must prove that $\delta(t) > 2n$ implies $\mathbf{f}(t) > k$ for every normalized type t; but if $\delta(t) > 2n$, then $t^{(2n+2,0)}$ divides t, and therefore $\mathbf{f}(t) \ge \mathbf{f}(t^{(2n+2,0)}) = (2n+1)!! > k$.

By the same argument, every normalized type $t \in \mathcal{T}(C_2)$ satisfying $\mathbf{f}(t) \le k$ and $\delta(t) = 2n$ is of the form $t = t^{(2n,2l)}$ for some $l \in \mathbb{N}_0$. In order to finish the proof of Theorem 3, we must determine all $l \in \mathbb{N}_0$ satisfying $C(2n,2l) \le k$.

$n = 1 : k \le 2$, $C(2,0) = 1$, $C(2,2l) = 2$ for all $l \ge 1$; therefore $J_1 = \{0\}$ and $J_2 = \mathbb{N}_0$.

$n = 2 : 3 \le k \le 14$, $C(4,0) = 3$, $C(4,2) = 9$, $C(4,2l) = 10$ for all $l \ge 2$; therefore $J_k = \{0\}$ for $3 \le k \le 8$, $J_9 = \{0,1\}$ and $J_k = \mathbb{N}_0$ for $10 \le k \le 14$.

$n = 3 : 15 \le k \le 104$, $C(6,0) = 15$, $C(6,2) = 60$, $C(6,4) = 75$, $C(6,2l) = 76$ for all $l \ge 3$; therefore $J_k = \{0\}$ for $15 \le k \le 59$, $J_k = \{0,1\}$ for $60 \le k \le 74$, $J_k = \{0,1,2\}$ for $k = 75$ and $J_k = \mathbb{N}_0$ for $76 \le k \le 104$.

$n = 4,5,6$: Similar.

$n \ge 7 : C(2n,2) = (2n-1)!!\,(n+1) < (2n+1)!!$, and $C(2n,4) = (2n-1)!!(n^2+5n+6)/6 \ge (2n+1)!!$; therefore we obtain $J_k = \{0\}$ for $(2n-1)!! \le k < (2n-1)!!\,(n+1)$, and $J_k = \{0,1\}$ for $(2n-1)!!\,(n+1) \le k < (2n+1)!!$. ∎

4. Analytical theory of factorizations in class number two. From Theorems 1 and 3 we deduce:

THEOREM 4. *Let* $[D,H]$ *be an arithmetical formation with class group of order* $N = 2$, *and* $k \in \mathbb{N}$. *Let* $n \in \mathbb{N}$ *be maximal with* $(2n-1)!! \le k$. *Then we have*, *as* $k \to \infty$,

$$F_k(x) \sim c_k \frac{x}{\sqrt{\log x}} (\log\log x)^{2n}\,,$$

where

$$c_k = \frac{G(1)}{2^{2n}(2n)!\sqrt{\pi}} \sum_{j \in J_k} S_{2j}\,,$$

$$S_0 = 1, \qquad S_l = \sum_{p \in P \setminus H} |p|^{-l} \quad \textit{for } l \geq 2\,,$$

and

$$G(s) = (s-1)^{1/2} \prod_{p \in P \cap H} (1 - |p|^{-s})^{-1}\,.$$

Though c_k is given explicitly in Theorem 4, $G(1)$ cannot be calculated from the definition of $G(s)$, and for small j the series defining S_{2j} converge very slowly. Therefore we shall now describe techniques which allow us to compute c_k in specific examples.

Let $[D, H]$ be an arithmetical formation whose class group G is of order $N = 2$, and let χ be the non-trivial character of G. Then the formation has two zeta functions, $Z(s)$ and $Z(s, \chi)$, and we define its *total zeta function* by

$$Z^*(s) = Z(s)Z(s,\chi)\,.$$

$Z^*(s)$ is a meromorphic function in the half-plane $\Re s > 1 - \delta$, having a simple pole at $s = 1$, and we set

$$K = \operatorname{Res}\{Z^*(s) : s = 1\}\,.$$

If

$$G_0(s) = \prod_{p \in P \cap H} (1 - |p|^{-s})^{-1}\,,$$

then the following formulas permit a calculation of $G(1)$.

Proposition 1. *Let notations be as above and $m \in \mathbb{N}$. Then we have*

$$G(1) = \sqrt{\frac{K}{Z(2)}} \prod_{p \in P \cap H} \frac{|p|}{\sqrt{|p|^2 - 1}} = \sqrt{K} \prod_{p \in P \setminus H} \frac{\sqrt{|p|^2 - 1}}{|p|}$$

$$= \sqrt{\frac{K}{Z(2)}} \prod_{j=1}^{m-1} \left\{ \frac{Z^*(2^j)}{Z(2^{j+1})} \right\}^{2^{-j-1}} G_0(2^m)^{2^{-m}}\,,$$

and moreover

$$G(1) = \sqrt{\frac{K}{Z(2)}} \prod_{j=1}^{\infty} \left\{ \frac{Z^*(2^j)}{Z(2^{j+1})} \right\}^{2^{-j-1}}\,.$$

Proof. From the identity

$$G_0(s)^2 = \frac{Z^*(s)}{Z(2s)} G_0(2s)$$

we obtain

$$G(1) = \lim_{s\to 1}(s-1)^{1/2}G_0(s) = \sqrt{\frac{K}{Z(2)}G_0(2)}\,,$$

which implies the first formula. The second one follows by induction on m; for the third one observe that

$$\lim_{m\to\infty} G_0(2^m)^{2^{-m}} = 1\,. \ \blacksquare$$

For the calculation of S_l for $l \ge 2$ we introduce the function

$$H(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \log \frac{Z(ns,\chi)}{Z(ns)}\,,$$

where μ denotes the Möbius function. It is connected with the sums S_l by the following formulas.

PROPOSITION 2. *Let notations be as above.*

(i) *For $l > 1$, we have*

$$H(l) = S_{2l} - 2S_l\,;$$

(ii) *For $l > 1$ and $m \in \mathbb{N}$,*

$$S_l = -\sum_{\nu=0}^{m-1} 2^{-\nu-1} H(2^\nu l) + 2^{-m} S_{2^m l}\,,$$

and

$$S_l = -\sum_{\nu=0}^{\infty} 2^{-\nu-1} H(2^l \nu)\,.$$

P r o o f. (i) From

$$\frac{Z(ns,\chi)}{Z(ns)} = \prod_{p\in P\setminus H} \frac{(1+|p|^{-ns})^{-1}}{(1-|p|^{-ns})^{-1}}$$

we obtain

$$\log \frac{Z(ns,\chi)}{Z(ns)} = \sum_{p\in P\setminus H} \sum_{\substack{k=1\\ k\equiv 1 \bmod 2}}^{\infty} \frac{-2}{k}|p|^{-kns}\,,$$

and consequently

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} \log \frac{Z(ns,\chi)}{Z(ns)} = \sum_{p\in P\setminus H} \sum_{m=1}^{\infty} \frac{-2}{m}|p|^{-ms} \sum_{\substack{1\le k\mid m\\ k\equiv 1 \bmod 2}} \mu\left(\frac{m}{k}\right).$$

It is easily checked that

$$\sum_{\substack{1\le k\mid m\\ k\equiv 1 \bmod 2}} \mu\Big(\frac{m}{k}\Big) = \begin{cases} 1 & \text{if } m=1,\\ -1 & \text{if } m=2,\\ 0 & \text{if } m>2,\end{cases}$$

which gives the result.

(ii) follows from (i) by induction on m, observing that $\lim_{m\to\infty} 2^{-m} S_{2^m l} = 0$. ■

Remark. The infinite product in Proposition 1 and the infinite series in Proposition 2 turn out to converge very rapidly. They have been used for the calculations in the subsequent examples.

EXAMPLE 1. $H = 1+4\mathbb{N}_0$, $D = 1+2\mathbb{N}_0$, $\varphi = \big(\frac{-4}{\bullet}\big)$, $Z(s) = (1-2^{-s})\zeta(s)$, $Z(s,\varphi) = L(s,\varphi)$ and $Z^*(s) = (1-2^{-s})\zeta_{\mathbb{Q}(\sqrt{-1})}(s)$; $K = \frac{\pi}{8}$.

$G(1)$	S_2	S_4	S_6	S_8
0.5798	0.1484	0.0128	0.0014	0.0002

EXAMPLE 2. $H = \{a \in \mathbb{N} \mid a \equiv \pm 1 \bmod 5\}$, $D = \{a \in \mathbb{N} \mid a \not\equiv 0 \bmod 5\}$, $\varphi = \big(\frac{5}{\bullet}\big)$, $Z(s) = (1-5^{-s})\zeta(s)$, $Z(s,\varphi) = L(s,\varphi)$ and $Z^*(s) = (1-5^{-s})\zeta_{\mathbb{Q}(\sqrt{r})}(s)$; $K = \frac{2}{5\sqrt5}\log\frac{1+\sqrt5}{2}$.

$G(1)$	S_2	S_4	S_6	S_8	S_{10}	S_{12}
0.2353	0.3965	0.0753	0.0170	0.0041	0.0010	0.0002

EXAMPLE 3. H is the semigroup of non-zero principal ideals of $\mathbb{Z}[\sqrt{-5}]$, D is the semigroup of all non-zero ideals of $\mathbb{Z}[\sqrt{-5}]$, G is the ideal class group of $\mathbb{Z}[\sqrt{-5}]$ and φ is the non-trivial ideal class character, $\varphi : D \to \{\pm 1\}$, $H = \varphi^{-1}(1)$; $Z(s) = \zeta_{\mathbb{Q}(\sqrt{-5})}(s) = \zeta(s)L(s,\chi)$, where $\chi = \big(\frac{-20}{\bullet}\big)$; we set $\psi = \big(\frac{5}{\bullet}\big)$, $\theta = \big(\frac{-4}{\bullet}\big)$ and obtain

$$Z^*(s) = \zeta_{\mathbb{Q}(\sqrt5,\sqrt{-5})}(s) = \zeta(s)L(s,\chi)L(s,\psi)L(s,\theta)\,,$$

whence $Z(s,\varphi) = L(s,\psi)L(s,\theta)$; $K = \frac15\log\frac{1+\sqrt5}{2}$.

$G(1)$	S_2	S_4	S_6	S_8
0.2331	0.1353	0.0128	0.0014	0.0002

REFERENCES

[1] R. Gilmer, *Commutative Semigroup Rings*, Univ. of Chicago Press, Chicago 1984.
[2] F. Halter-Koch, *Halbgruppen mit Divisorentheorie*, Exposition. Math. 8 (1990), 29–66.
[3] —, *Typenhalbgruppen und Faktorisierungsprobleme*, Resultate Math. 22 (1992), 545–559.
[4] F. Halter-Koch and W. Müller, *Quantitative aspects of non-unique factorization: A general theory with applications to algebraic function fields*, J. Reine Angew. Math. 421 (1991), 159–188.
[5] J. Kaczorowski, *Some remarks on factorizations in algebraic number fields*, Acta Arith. 43 (1983), 53–68.
[6] J. Knopfmacher, *Abstract Analytic Number Theory*, North-Holland, 1975.
[7] E. Landau, *Über Ideale und Primideale in Idealklassen*, Math. Z. 2 (1918), 52–154.
[8] S. Lang, *Algebraic Number Theory*, Addison-Wesley, 1970.
[9] W. Narkiewicz, *Numbers with unique factorization in an algebraic number field*, Acta Arith. 21 (1972), 313–322.

INSTITUT FÜR MATHEMATIK
KARL-FRANZENS-UNIVERSITÄT
HEINRICHSTRASSE 36/IV
A-8010 GRAZ, ÖSTERREICH

Reçu par la Rédaction le 17.6.1992;
en version modifiée le 25.1.1993