ACTA ARITHMETICA
LVII (1991)

Factorization of natural numbers in algebraic number fields

by

A. GEROLDINGER (Graz)

1. Let R be the ring of integers of an algebraic number field K with ideal class group G and class number h. If for some $a \in R \backslash (R^{\times} \cup \{0\})$ $a = u_1 \ldots u_k$ is a factorization into irreducibles, then k is called *length* of the factorization. Let $g(a)$ denote the number of distinct lengths of possible factorizations of a. In the case $h \geqslant 3$ the function

$$G'_m(x) = \# \{n \in N \mid n \leqslant x, g(n) \leqslant m\}$$

was studied for every $m \geqslant 1$ (see [8]–[12], [14]–[16], [1], [23]) and it was proved that

$$G'_m(x) = \big(C + o(1)\big) x (\log x)^{-\eta'(K,m)} (\log \log x)^{\psi'(K,m)}$$

with non-negative constants $\eta'(K,m)$ and $\psi'(K,m)$ ([22]).

In this paper we determine these constants and especially we show $\eta'(K,m) = \eta'(K)$. Thus the exponents in the asymptotic formulae for all four functions which were introduced by W. Narkiewicz in 1964 ([8]) are known: concerning

$G'_m(x)$ see Theorem 1,

$G_m(x) = \# \{(a) \mid N(a) \leqslant x,\ g(a) \leqslant m\}$ see [4],

$F_m(x) = \# \{(a) \mid N(a) \leqslant x,\ f(a) \leqslant m\}$ see [13],

$F'_m(x) = \# \{n \in N \mid n \leqslant x,\ f(n) \leqslant m\}$ see [18], [21].

Here $f(a)$ denotes the number of distinct factorizations of some $a \in R \backslash (R^{\times} \cup \{0\})$.

In [7] the remainder terms of the asymptotic formulae of these functions are studied. In Section 4 we use these results to obtain an asymptotic formula for $\bar{F}_m(x) = \# \{(a) \mid N(a) \leqslant x,\ f(a) = m\}$.

2. Let $h \geqslant 3$. For a non-empty subset $G_0 \subset G$ let $\mathscr{F}(G_0)$ denote the free abelian semigroup generated by G_0. An element $B \in \mathscr{F}(G_0)$ has the form $B = \prod_{g \in G_0} g^{v_g(B)}$ with $v_g(B) \in N$. B is called a *block* if $\sum_{g \in G_0} v_g(B)\, g = 0$. The set of all blocks $\mathscr{B}(G_0) \subset \mathscr{F}(G_0)$ is a subsemigroup. Thus it is commutative, regular and we have the usual notions of divisibility. For $B \in \mathscr{B}(G_0)$ let $L(B) = \{k \mid B$ has a factorization into k irreducible blocks$\}$. Further let $\Delta(L(B)) = \{s-r \mid r, s \in L(B),\ r < s$ and $t \notin L(B)$ for $r < t < s\}$ and $\Delta(G_0) = \bigcup_{B \in \mathscr{B}(G_0)} \Delta(L(B))$. If for some $a \in R \setminus (R^\times \cup \{0\})$ $aR = \mathfrak{p}_1 \ldots \mathfrak{p}_r$ is its prime ideal decomposition then $B(a) = \prod_{g \in G} g^{\#\{\mathfrak{p}_i \mid \mathfrak{p}_i \in g, 1 \leqslant i \leqslant r\}} = \langle [\mathfrak{p}_1], \ldots, [\mathfrak{p}_r] \rangle$ denotes the corresponding block (see [3]). Obviously $\mathscr{B}(\boldsymbol{P}) = \{B(p) \mid p \in \boldsymbol{P}\}$ is finite. Let $\mathscr{B}(\boldsymbol{P}) = \{B_1, \ldots, B_\varrho\}$.

When studying $G'_m(x)$ invariant subsets $G_0 \subset G$ with $\Delta(G_0) = \emptyset$ are of decisive importance; here, a subset $G_0 \subset G$ is called *invariant* if $G_0 = G_I = \bigcup_{i \in I} \{g \mid v_g(B_i) > 0\}$ for some $I \subset \{1, \ldots, \varrho\}$.

Remarks. 1. Let $G_0 \subset G$; then by definition $\Delta(G_0) = \emptyset$ if and only if $\mathscr{B}(G_0)$ is half-factorial. In connection with the problem of describing half-factorial Dedekind domains L. Skula proves ([20], Theorem 3.1): $\Delta(G_0) = \emptyset$ if and only if $\sum_{g \in G} v_g(B)/\mathrm{ord}(g) = 1$ for every irreducible block $B \in \mathscr{B}(G_0)$. If G is cyclic of prime power order he derives an explicit characterization of subsets $G_0 \subset G$ with $\Delta(G_0) = \emptyset$ ([20], Proposition 3.4). These subsets also play a central part in the investigation of $G_m(x)$ ([4]).

2. If $K/\boldsymbol{Q}$ is Galois then $G_0 \subset G$ is invariant if and only if G_0 is invariant under the action of the Galois group.

For a block $B \in \mathscr{B}(G)$ let $P(B) = \{p \in \boldsymbol{P} \mid B(p) = B\}$ and for a subset $M \subset \boldsymbol{P}$ let $q(M)$ denote the Dirichlet density of M, if it exists.

LEMMA 1. *$P(B)$ is either finite or it is a regular set with positive Dirichlet density. If p is unramified then $P(B(p))$ has positive Dirichlet density.*

Proof. See Lemma 11 in [22] and Section 2 in [19]. ■

Remark. Lemma 1 and Proposition 7.9 in [15] imply: if there is an unramified prime $p \in \boldsymbol{P}$ remaining irreducible in R, then

$$\#\{n \leqslant x \mid n \text{ is irreducible in } R\} = Cx(\log x)^{-1} + o\left(x(\log x)^{-1}\right).$$

For $i \in \{1, \ldots, \varrho\}$ let $q_i = q(P(B_i))$ (if $P(B_i)$ is finite then $q_i = 0$). Therefore $\sum_{i=1}^{\varrho} q_i = 1$. For $I \subset \{1, \ldots, \varrho\}$ let $q_I = \sum_{i \in I} q_i$ and for an invariant subset $G_0 \subset G$ let

$$q(K, G_0) = \sum_{\substack{1 \leqslant i \leqslant \varrho \\ B_i \in \mathscr{B}(G_0)}} q_i.$$

Further let

$$q(K) = \max\{q(K, G_0) \mid G_0 \subset G \text{ invariant},\ \Delta(G_0) = \emptyset\}.$$

LEMMA 2. $0 < q(K) < 1$.

Proof. (i) Let p be a prime which splits completely in the Hilbert class field of K. Then $B(p) = \langle 0, \ldots, 0 \rangle$. Thus $\{0\}$ is an invariant subset and $q(K) > 0$.

(ii) Let $G_0 \subset G$ be invariant with $\Delta(G_0) = \emptyset$. Since $h \geqslant 3$ there is a $g \in G \backslash G_0$. Let $p \in P$ be unramified having a prime ideal divisor $\mathfrak{p} \in g$. Then $q(B(p)) > 0$, $B(p) \notin \mathscr{B}(G_0)$ and so $q(K, G_0) < 1$. ∎

$\mathscr{G} = \{G_0 \subset G \mid G_0$ invariant and $\Delta(G_0) = \emptyset\}$ is partially ordered with respect to the set-theoretical inclusion. Let $G_1, G_2 \in \mathscr{G}$. Then $G_1 \subset G_2$ implies $q(K, G_1) \leqslant q(K, G_2)$. If $q(K, G_1) = q(K)$ then there is a maximal subset $G_0 \in \mathscr{G}$ with $G_1 \subset G_0$ and $q(K, G_1) = q(K, G_0) = q(K)$. If K/Q is Galois then $G_1 \subset G_2$, $G_1 \neq G_2$ implies $q(K, G_1) < q(K, G_2)$ and the subsets $G_0 \in \mathscr{G}$ with $q(K, G_0) = q(K)$ are maximal in $\mathscr{G}$.

For $n = \prod_{p \in P} p^{v_p(n)} \in N$ let $v_i(n) = \sum_{\substack{p \in P \\ B(p) = B_i}} v_p(n)$ for every $i \in \{1, \ldots, \varrho\}$. For $s = (s_i)_{i \in I^c} \in N^{I^c}$ with $I \subset \{1, \ldots, \varrho\}$ and $I^c = \{1, \ldots, \varrho\} \backslash I$ let $\psi'(s) = \sum_{\substack{i \in I^c \\ q_i > 0}} s_i$.

Let $I \in \mathscr{I} = \{I \mid I \subset \{1, \ldots, \varrho\},\ q_I = q(K)$ and $\Delta(G_I) = \emptyset\}$. For every $m \geqslant 1$ let $S(I, m)$ be the set of all $s \in N^{I^c}$ with

$$\{n \mid v_i(n) = s_i \text{ for every } i \in I^c\} \subset \{n \mid g(n) \leqslant m\}.$$

LEMMA 3. *If for some $j \in I^c$, $\{s_j \mid s \in S(I, m)\}$ is infinite, then $q_j = 0$.*

Proof. Let $j \in I^c$ and suppose $\{s_j \mid s \in S(I, m)\}$ is infinite. Then $\Delta(G_{I'}) = \emptyset$ with $I' = I \cup \{j\}$. Since $q(K) \geqslant q_{I'} = q_I + q_j = q(K) + q_j$ it follows that $q_j = 0$. ∎

Thus the following definitions make sense:

$$\psi'(K, I, m) = \max\{\psi'(s) \mid s \in S(I, m)\},$$

$$\psi'(K, m) = \max\{\psi'(K, I, m) \mid I \in \mathscr{I}\}.$$

The constants $q(K)$ ($\psi'(K, m)$ respectively) just depend on the orbit structure of G (and on m respectively) which we define as the sequence of blocks $B_1, \ldots, B_\varrho \in \mathscr{B}(G)$ and the corresponding sequence of densities $q_1, \ldots, q_\varrho \in [0, 1)$ with $\sum_{i=1}^{\varrho} q_i = 1$.

The following lemma provides the analytic tool for Theorem 1.

LEMMA 4. *Let $I \subset \{1, \ldots, \varrho\}$ with $q_I > 0$ and let $s \in N^{I^c}$. Then*

$$\# \{n \leqslant x \mid v_i(n) = s_i \text{ for every } i \in I^c\} = (C + o(1))x(\log x)^{-1+q_I}(\log\log x)^{\psi'(s)}.$$

Proof. See Lemma 12 in [22] and Lemma 7 in [11]. ∎

THEOREM 1. *For $m \geqslant 1$*

$$G'_m(x) = (C + o(1))\, x(\log x)^{-1+q(K)}(\log\log x)^{\psi'(K,m)}.$$

Proof. 1. Let $I \subset \{1, \ldots, \varrho\}$ with $\Delta(G_I) \neq \emptyset$. There is an $n^I \in N$ with $B(n^I) \in \mathscr{B}(G_I)$ and $g(n^I) > m$. Then for every $n \in N$, $g(nn^I) > m$.

For every $i \in \{1, \ldots, \varrho\}$ let $w_i = \max\{v_i(n^I) \mid I \subset \{1, \ldots, \varrho\}$ with $\Delta(G_I) \neq \emptyset\}$. These constants have the following property: if for $n \in N$, $\Delta\big(\bigcup_{\substack{1 \leqslant i \leqslant \varrho \\ v_i(n) \geqslant w_i}} \{g \mid v_g(B_i) > 0\}\big) \neq \emptyset$, then $g(n) > m$.

2. For $I \in \mathscr{I}$ let $T(I, m) = N^{I^c} \backslash S(I, m)$; $T(I, m)$ is the set of all $t \in N^{I^c}$ such that

$$\{n \mid g(n) > m\} \cap \{n \mid v_i(n) = t_i \text{ for every } i \in I^c\} \neq \emptyset.$$

According to Theorem 9.18 in [2] there are only finitely many minimal elements in $T(I, m)$: $t_1^I, \ldots, t_{\lambda_I}^I$. For $j \in \{1, \ldots, \lambda_I\}$ let $n_j^I \in N$ with $g(n_j^I) > m$ and $v_i(n_j^I) = t_{j,i}^I$ for every $i \in I^c$.

For every $i \in \{1, \ldots, \varrho\}$ let $u_i = \max\{v_i(n_j^I) \mid 1 \leqslant j \leqslant \lambda_I, I \in \mathscr{I}\}$. Then for every $I \in \mathscr{I}$ and for every $t \in T(I, m)$

$$\{n \mid v_i(n) \geqslant u_i \text{ for } i \in I,\ v_i(n) = t_i \text{ for } i \in I^c\} \cap \{n \mid g(n) \leqslant m\} = \emptyset.$$

3. For every $i \in \{1, \ldots, \varrho\}$ let $z_i = \max\{u_i, w_i\}$. Then

$$\bigcup_{I \in \mathscr{I}} \bigcup_{\substack{s \in S(I,m),\\ s_i \leqslant \psi'(K,I,m)\\ \text{for every } i \in I^c}} \{n \leqslant x \mid v_i(n) = s_i \text{ for every } i \in I^c\} \subset \{n \leqslant x \mid g(n) \leqslant m\}$$

$$= \bigcup_I \{n \leqslant x \mid g(n) \leqslant m,\ v_i(n) \geqslant z_i \text{ for } i \in I,\ v_i(n) < z_i \text{ for } i \in I^c\}$$

$$\overset{(1)}{=} \bigcup_{I, \Delta(G_I) = \emptyset} \{n \leqslant x \mid g(n) \leqslant m,\ v_i(n) \geqslant z_i \text{ for } i \in I,\ v_i(n) < z_i \text{ for } i \in I^c\}$$

$$= \bigcup_{\substack{I, q_I < q(K)\\ \Delta(G_I) = \emptyset}} \{\ldots\} \cup \bigcup_{I \in \mathscr{I}} \{\ldots\}$$

$$\overset{(2)}{=} \bigcup_{\substack{I, q_I < q(K)\\ \Delta(G_I) = \emptyset}} \{\cdots\} \cup \bigcup_{I \in \mathscr{I}} \bigcup_{\substack{s \in S(I,m),\\ s_i < z_i\\ \text{for every } i \in I^c}} \{n \leqslant x \mid v_i(n) \geqslant z_i \text{ for } i \in I,\ v_i(n) = s_i \text{ for } i \in I^c\}$$

$$\subset \bigcup_{\substack{I, q_I < q(K)\\ \Delta(G_I) = \emptyset}} \{\cdots\} \cup \bigcup_{I \in \mathscr{I}} \bigcup_{\substack{s \in S(I,m),\\ s_i < \max\{z_i, \psi'(K,I,m)\}\\ \text{for every } i \in I^c}} \{n \leqslant x \mid v_i(n) = s_i \text{ for every } i \in I^c\}.$$

Now Lemma 4 implies the assertion. ∎

3. In this section $q(K)$ will be further investigated. Due to J. Śliwa ([21])

$$F_m'(x) = (C + o(1))\, x (\log x)^{-1 + q_0(K)} (\log\log x)^{\varphi'(K,m)}$$

with $q_0(K)$ being the density of primes which have only principal ideals in their prime ideal decomposition. The following proposition deals with $q_0(K)$ and $q(K)$.

Proposition 1. 1. $q_0(K) = q(K, \{0\}) \leqslant q(K)$.

2. *Let* $\{B(p) \mid p$ *is unramified and has a non-principal prime ideal divisor*$\}$ $= \{B_1, \ldots, B_{\varrho'}\}$. *Then the following conditions are equivalent*:

(a) $q_0(K) = q(K)$.

(b) $\Delta(\{g \mid v_g(B_i) > 0\}) \neq \emptyset$ *for every* $i \in \{1, \ldots, \varrho'\}$.

(c) $\sum_{g \in G} v_g(A)/\mathrm{ord}(g) = 1$ *for every irreducible* $A \in (\mathscr{B}\{g \mid v_g(B_i) > 0\})$ *for every* $i \in \{1, \ldots, \varrho'\}$.

3. *If* $p \nmid h$ *for every prime* $p \leqslant [K : Q]$, *then* $q_0(K) = q(K)$.

Proof. 2(a) and (b) are equivalent by definition; (b) and (c) are equivalent by [20], Theorem 3.1.

3. Let $\langle 0\rangle^k B = \langle 0\rangle^k \langle g_1, \ldots, g_r\rangle \in \{B_1, \ldots, B_{\varrho'}\}$ with $k \in N$ and $g_1, \ldots, g_r \in G\backslash\{0\}$. Then $B^s = \prod_{i=1}^{r} \langle g_1, \ldots, g_i\rangle^{s/\mathrm{ord}(g_i)}$ with $s = \mathrm{lcm}\{\mathrm{ord}(g_i) \mid 1 \leqslant i \leqslant r\}$. Since $[K:Q] < \mathrm{ord}(g_i)$ it follows

$$s \sum_{i=1}^{r} \frac{1}{\mathrm{ord}(g_i)} < sr \frac{1}{[K:Q]} \leqslant s.$$

Thus $\Delta(\{g \mid v_g(B) > 0\}) \neq \emptyset$, and so 2(b) implies the assertion. ∎

From now on till the end of this section all number fields K are Galois and Γ denotes the Galois group of K over Q.

PROPOSITION 2. *If for every $g \in G\backslash G^\Gamma$ there exists a $\gamma \in \Gamma$ with $g \neq g^\gamma$ such that g and g^γ are in the same cyclic subgroup of G, then*

$$q(K) = \max\{q(K, G_0) \mid G_0 \subset G^\Gamma, \Delta(G_0) = \emptyset\}.$$

Proof. It suffices to show: if $G_0 \subset G$ is invariant and $G_0 \not\subset G^\Gamma$ then $\Delta(G_0) \neq \emptyset$. Let $g \in G_0\backslash G^\Gamma$, $\gamma \in \Gamma$ with $g \neq g^\gamma$ and $g = a + nZ$, $g^\gamma = b + nZ \in Z/nZ < G$. We have

$$\frac{n}{\gcd(a, n)} = \mathrm{ord}(a+nZ) = \mathrm{ord}(b+nZ) = \frac{n}{\gcd(b, n)}$$

and so

$$\gcd(a, n) = \gcd(b, n) = k.$$

According to Proposition 5 in [5] $\Delta(\{a+nZ, b+nZ\}) = \emptyset$ if and only if

$$\frac{a}{k} \equiv \frac{b}{k} \bmod \left(\frac{n}{k}\right) \quad \text{or} \quad \frac{n}{k} \leqslant 2.$$

Since neither of the two conditions holds $\emptyset \neq \Delta(\{a+nZ, b+nZ\}) \subset \Delta(G_0)$. ∎

For $d \in N_+$ let $G[d] = \{g \in G \mid dg = 0\}$.

PROPOSITION 3. *Let $k \subset K$ with k/Q Galois, Hilbert class field $H(k) \subset K$ and $[K:k] = d$. Then*

$$q(K) = \max\{q(K, G_0) \mid G_0 \subset G[d],\ G_0 \text{ invariant},\ \Delta(G_0) = \emptyset\}.$$

Proof. Let $\Gamma' = \mathrm{Gal}(K/k) \subset \mathrm{Gal}(K/Q) = \Gamma$, $\# \Gamma = n$, $G_0 \subset G$ invariant, $\Delta(G_0) = \emptyset$ and $0 \neq g \in G_0$. Let $\mathfrak{p} \in g$ be a prime ideal of first degree and let $\mathfrak{p} \cap Z = pZ$. Then p splits completely in K and since $H(k) \subset K$, p splits into principal prime ideals in k. Therefore $B(p) = \langle g^\gamma \mid \gamma \in \Gamma\rangle = \prod_{i=1}^{n/d} B_i$ with $B_i = \langle g^{\gamma_i\gamma'} \mid \gamma' \in \Gamma'\rangle$ and $\Gamma = \bigcup_{i=1}^{n/d} \gamma_i \Gamma'$. Because of $\Gamma' \lhd \Gamma$

$$B_1^{\gamma_1^{-1}\gamma_i} = \langle g^{\gamma_1\gamma'} \mid \gamma' \in \Gamma'\rangle^{\gamma_1^{-1}\gamma_i} = \langle g^{\gamma_1\gamma'\gamma_1^{-1}\gamma_i} \mid \gamma' \in \Gamma'\rangle = B_i$$

for every $1 \leqslant i \leqslant n$. Therefore, if B_1 has a factorization into e irreducible blocks, then so has B_i for every $1 \leqslant i \leqslant n$. Thus $B(p)$ is a product of $(n/d)e$ irreducible blocks. On the other hand $B(p)^{\mathrm{ord}(g)} = \prod_{\gamma \in \Gamma} \langle g^\gamma, \ldots, g^\gamma\rangle$. Since $\Delta(G_0) = \emptyset$ it follows that $(n/d)e \cdot \mathrm{ord}(g) = n$, i.e. $\mathrm{ord}(g) \mid d$. ∎

COROLLARY 1. *If* $\# \Gamma = n$ *then*

$$q(K) = \max\{q(K, G_0) \mid G_0 \subset G[n],\ G_0 \text{ invariant},\ \Delta(G_0) = \emptyset\}.$$

Proof. Choose $k = \mathbf{Q}$. ∎

In the sequel we write $q(B)$ instead of $q(P(B))$ for a block B.

LEMMA 5. *Let* $K/\mathbf{Q}$ *be cyclic with prime degree* l.

1. *If* $p \in \mathbf{P}$ *is unramified in* K *then* $B(p) = \langle 0 \rangle$ *or* $B(p) = \langle g, \ldots, g \rangle$ *with* $g \in G^\Gamma$ *or* $B(p) = \langle g, g^\gamma, \ldots, g^{\gamma^{l-1}} \rangle$ *with* $g \in G \setminus G^\Gamma$ *and* $\gamma \in \Gamma$.
2. (a) $q(\langle 0 \rangle) = (l-1)/l$.
   (b) $q(\langle g^\gamma \mid \gamma \in \Gamma \rangle) = 1/h$ *for every* $g \in G \setminus G^\Gamma$.
   (c) $q(\langle g, \ldots, g \rangle) = 1/(lh)$ *for every* $g \in G^\Gamma$.
3. $q_0(K) = (l-1)/l + 1/(lh)$.
4. $q(K, G_0) = (l-1)/l + \# G_0/(lh)$ *for every invariant* $G_0 \subset G$ *with* $0 \in G_0$.

Proof. 1. Obvious.

2. (a) Since $\{p \in \mathbf{P} \mid B(p) = \langle 0 \rangle\} = \{p \in \mathbf{P} \mid p \text{ does not split}\}$ the assertion follows by Corollary 5, p. 324 in [15].

(b), (c). Let $H(K)$ be the Hilbert class field of K and let $\varphi: G \to \mathrm{Gal}(H(K)/K)$ be the Artin isomorphism. Then $\Gamma = \mathrm{Gal}(K/\mathbf{Q}) = \mathrm{Gal}(H(K)/\mathbf{Q})/\mathrm{Gal}(H(K)/K)$ and $\varphi(g^\gamma) = \gamma\varphi(g)\gamma^{-1}$ for every $g \in G$ and every $\gamma \in \Gamma$. For an unramified $p \in \mathbf{P}$ let $F(p) \subset \mathrm{Gal}(H(K)/\mathbf{Q})$ denote the conjugate class of Frobenius automorphisms associated with prime divisors $\mathfrak{p}$ of p in $H(K)$. Then, by Chebotarev's density theorem we obtain (see, for example Theorem 7.10 in [15]):

(i) for every $g \in G \setminus G^\Gamma$

$$q(\langle g^\gamma \mid \gamma \in \Gamma \rangle) = q(\{p \in \mathbf{P} \mid F(p) = \{\gamma\varphi(g)\gamma^{-1} \mid \gamma \in \Gamma\}\})$$
$$= \frac{\# \{\gamma\varphi(g)\gamma^{-1} \mid \gamma \in \Gamma\}}{lh} = \frac{1}{h}.$$

(ii) for every $g \in G^\Gamma$

$$q(\langle g, \ldots, g \rangle) = q(\{p \in \mathbf{P} \mid F(p) = \{\varphi(g)\}\}) = 1/(lh).$$

3. $q_0(K) = q(\langle 0 \rangle) + q(\langle 0, \ldots, 0 \rangle)$.

4. Let $G_0 \subset G$ be invariant and $0 \in G_0$. Since

$$\mathscr{B}(G_0) \cap \mathscr{B}(\mathbf{P}) = \{\langle 0 \rangle\} \cup \{\langle g, \ldots, g \rangle \mid g \in G_0^\Gamma\} \cup \{\langle g^\gamma \mid \gamma \in \Gamma \rangle \mid g \in G_0 \setminus G_0^\Gamma\}$$

the assertion follows by 2. ∎

For a finite group Γ and a finite Γ-module G let

$$\mu_\Gamma(G) = \max\{\# G_0 \mid G_0 \subset G\ \Gamma\text{-invariant},\ \Delta(G_0) = \emptyset\}.$$

If Γ acts trivially on G then $\mu_\Gamma(G) = \mu(G) = \max\{\# G_0 \mid \Delta(G_0) = \emptyset\}$. Obviously $1 \leqslant \mu(G^\Gamma) \leqslant \mu_\Gamma(G) \leqslant \mu(G)$. Furthermore, if the condition in Proposition 2 holds (especially, if G is cyclic), then $\mu_\Gamma(G) = \mu(G^\Gamma)$. For $p \in \boldsymbol{P}$, $\mu(C_{p^n}) = n+1$ ([20], Proposition 3.4) and if G is an elementary 2-group then $\mu(G) = \mathrm{rk}(G)+1$ ([23], Section 5). For further results on $\mu(G)$ see [22], Lemma 1, and [17], Section 2.

LEMMA 6. *Let Γ be cyclic with prime degree l and let G be an elementary l group. If* $\mathrm{rk}(G) - \mathrm{rk}(G^\Gamma) \leqslant l-1$, *then* $\mu_\Gamma(G) = \mu(G^\Gamma)$.

Proof. Let $G_0 \subset G$ be invariant with $\Delta(G_0) = \emptyset$. It suffices to show $G_0 \subset G^\Gamma$. Assume to the contrary, there is an element $g_1 \in G_0 \setminus G^\Gamma$. Then $g_1, g_2 = g_1^\gamma, \ldots, g_l = g_1^{\gamma^{l-1}}$ are pairwise distinct for $\gamma \in \Gamma$. Let $G = G^\Gamma \times G_1$. Since

$$l\left(\mathrm{rk}(G)-\mathrm{rk}(G^\Gamma)\right) = \# G_1 \geqslant \# \bigcup_{i=1}^{l} \{g_i, 2g_i, \ldots, (l-1)g_i\}+1$$

it follows that

$$\# \bigcup_{i=1}^{l} \{g_i, \ldots, (l-1)g_i\} < l(l-1).$$

Therefore there are g_i, g_j with $g_i \neq g_j$ and m_i, $m_j \in \{1, \ldots, l-1\}$ with $m_i g_i + m_j g_j = 0$. Let $m_i' \in \{1, \ldots, l-1\}$ with $m_i m_i' \equiv 1 \bmod l$ and let $m_j' \in \{1, \ldots, l-1\}$ with $m_j' \equiv m_j m_i' \bmod l$. Then $g_i + m_j' g_j = 0$ and $B = \langle g_i, g_j, \ldots, g_j \rangle$ is irreducible. $B^l = \langle g_i, \ldots, g_i \rangle \langle g_j, \ldots, g_j \rangle^{m_j'}$ implies $m_j' = l-1$. Thus $g_i = g_j$, a contradiction. ■

PROPOSITION 4. *If K/Q is cyclic with prime degree l, then*

$$q(K) = \frac{l-1}{l} + \frac{1}{lh}\mu_\Gamma(G[l]).$$

Proof. The proof follows immediately by Corollary 1 and Lemma 5. ■
The final corollary is due to W. Narkiewicz ([11], Theorem 4).

COROLLARY 2. *If K is a quadratic number field, then*

$$q(K) = \frac{1}{2} + \frac{1}{2h}\left(\mathrm{rk}_2(G)+1\right).$$

Proof. Since Γ acts trivially on $G[2]$

$$\mu_\Gamma(G[2]) = \mu(G[2]) = \mathrm{rk}_2(G)+1. \ ■$$

4. Let $h \geqslant 2$ and $m \geqslant 1$. In order to get an asymptotic formula for $\bar{F}_m(x) = \# \{(a) \mid N(a) \leqslant x, f(a) = m\}$ we improve the asymptotic formula for $F_m(x)$ given in [13] with the methods of [7].

THEOREM 2.

1. $F_m(x) = x(\log x)^{-1+1/h} W_m(\log\log x) + O\left(x(\log x)^{-2+1/h}(\log\log x)^{c_m}\right)$ *with* $0 \neq W_m \in C[X]$ *and* $c_m \geqslant 0$.

2. $\bar{F}_m(x) = x(\log x)^{-1+1/h}\bar{W}_m(\log\log x) + O\left(x(\log x)^{-2+1/h}(\log\log x)^{\bar{c}_m}\right)$ *with* $0 \neq \bar{W}_m \in C[X]$ *and* $\bar{c}_m \geq 0$.

Proof. 1. If we apply in Section 5 of [13] the so-called Main Lemma of [7] (Case II with $q = 0$) we get the above formula. (Proposition 1 in [7] and the formulae appearing in the proofs of the corollaries in [13] guarantee that the assumptions of the Main Lemma are satisfied.)

2. Let $m \geq 2$. First we show that there exists an $a_0 \in R$ with $f(a_0) = m$. Let $g \in G$ with $\mathrm{ord}(g) = n \geq 2$, let $p_1 \in g$, $p_2 \in -g$ be distinct prime ideals, $p_1^n = a_1 R$, $p_2^n = a_2 R$ and $p_1 p_2 = bR$. Since $a_0 = a_1^{m-1} a_2^{m-1} = a_1^{m-1-i} a_2^{m-1-i} b^{ni}$ for every $i \in \{0, \ldots, m-1\}$ and since there are no more factorizations of a_0, it follows that $f(a_0) = m$.

Let $M = \{a \in R \mid (a)$ is a product of principal prime ideals$\}$. Then $\#\{(a) \mid a \in M, N(a) \leq x\} \geq C_1 x(\log x)^{-1+1/h}$ ([7], Lemma 2). Since for every $a \in M$, $f(aa_0) = m$ we obtain $\bar{F}_m(x) \geq C_2 x(\log x)^{-1+1/h}$. But $\bar{F}_m(x) = F_m(x) - F_{m-1}(x) \geq C_2 x(\log x)^{-1+1/h}$ implies $W_m - W_{m-1} \neq 0$, and thus 2 holds with $\bar{W}_m = W_m - W_{m-1}$. ■

Remark. It is possible to proceed with $F'_m(x)$ and $\bar{F}'_m(x) = \#\{n \leq x \mid f(n) = m\}$ in the same way as above, to obtain an asymptotic formula for $\bar{F}'_m(x)$ (from [18] it follows that the assumptions of the Main Lemma in [7] are satisfied; further use [21], resp. [13] 3.b).

5. Finally we consider those natural numbers which have simple sets of lengths: for $n \in N$ let $L(n)$ denote the set of lengths of possible factorizations of n, i.e. $L(n) = \{k \mid n$ has a factorization of length $k\}$. $L(n)$ is called *simple* if there are $y, k \in N$ such that $L(n) = \{y, y+1, \ldots, y+k\}$. Lemma 4 and Lemma 7 in [3] imply that

$$\#\{n \leq x \mid L(n) \text{ is simple}\} = \left(1 + o(1)\right)x.$$

There are algebraic number fields with class number $h > 3$ such that $L(n)$ is simple for every $n \in N$ ([6]).

Acknowledgement. I would like to thank Professor F. Halter-Koch for valuable discussions on $q(K)$.

References

[1] S. Allen, *On the factorisations of natural numbers in an algebraic number field*, J. London Math. Soc. (2) 11 (1975), 294–300.

[2] A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups*, Vol. II, Providence, Rhode Island 1967.

[3] A. Geroldinger, *Über nicht-eindeutige Zerlegungen in irreduzible Elemente*, Math. Z. 197 (1988), 505–529.

[4] —, *Ein quantitatives Resultat über Faktorisierungen verschiedener Länge in algebraischen Zahlkörpern*, ibid. 205 (1990), 159–162.

[5] —, *On non-unique factorizations into irreducible elements II*, in *Number Theory*, Vol. II, Coll. Math. Soc. J. Bolyai 51, Budapest 1987, 723–757.

[6] —, *Factorizations of algebraic integers*, in *Number Theory*, Ulm 1987, Springer Lecture Notes 1380, 63–74.

[7] J. Kaczorowski, *Some remarks on factorization in algebraic number fields*, Acta Arith. 43 (1983), 53–68.

[8] W. Narkiewicz, *On algebraic number fields with non-unique factorization*, Colloq. Math. 12 (1964), 59–68.

[9] —, *On algebraic number fields with non-unique factorization II*, ibid. 15 (1966), 49–58.

[10] —, *On natural numbers having unique factorization in a quadratic number field*, Bull. Acad. Polon. Sci. 14 (1966), 17–18.

[11] —, *On natural numbers having unique factorization in a quadratic number field*, Acta Arith. 12 (1966), 1–22.

[12] —, *On natural numbers having unique factorization in a quadratic number field II*, ibid. 13 (1967), 123–129.

[13] —, *Numbers with unique factorization in an algebraic number field*, ibid. 21 (1972), 313–322.

[14] —, *A note on numbers with good factorization properties*, Colloq. Math. 27 (1973), 275–276.

[15] —, *Elementary and Analytic Theory of Algebraic Numbers*, PWN, Warszawa 1974.

[16] —, *Numbers with all factorizations of the same length in a quadratic number field*, Colloq. Math. 45 (1981), 71–74.

[17] —, *Finite abelian groups and factorization problems*, ibid. 42 (1979), 319–330.

[18] R. W. K. Odoni, *On a problem of Narkiewicz*, J. Reine Angew. Math. 288 (1976), 160–167.

[19] J. Rosiński and J. Śliwa, *The number of factorizations in an algebraic number field*, Bull. Acad. Polon. Sci. 24 (1976), 821–826.

[20] L. Skula, *On c-semigroups*, Acta Arith. 31 (1976), 247–257.

[21] J. Śliwa, *A note on factorizations in algebraic number fields*, Bull. Acad. Polon. Sci. 24 (1976), 313–314.

[22] —, *Factorizations of distinct lengths in algebraic number fields*, Acta Arith. 31 (1976), 399–417.

[23] —, *Remarks on factorizations in algebraic number fields*, Colloq. Math. 46 (1982), 123–130.

INSTITUT FÜR MATHEMATIK
KARL-FRANZENS-UNIVERSITÄT
Halbärthgasse 1/I
A-8010 Graz, Österreich

Received on 6.6.1989
and in revised form on 21.2.1990 (1944)