Combining (1.4) and (5.5) we obtain

$$(5.6)\qquad c|s_i|^{\varkappa_i-1} \geqslant \prod_{\tau=1}^{t_i} |s_i|_{p_{\tau i}} \quad (1 \leqslant i \leqslant n+1).$$

Since the components s_i have the same order of size, we may conclude by (5.6)

$$(5.7)\qquad c_5\|\mathfrak{s}\|^{\varkappa_i-1} \geqslant \prod_{\tau=1}^{t_i} |s_i|_{p_{\tau i}} \quad (1 \leqslant i \leqslant n+1),$$

and the corollary follows.

References

[1] K. Mahler, *Lectures on diophantine approximations*, University of Notre Dame, 1961.
[2] D. Ridout, *Rational approximations to algebraic numbers*, Mathematika 4 (1957), pp. 125–131.
[3] — *The p-adic generalization of the Thue–Siegel–Roth Theorem*, Mathematika 5 (1958), pp. 40–48.
[4] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), pp. 1–20.
[5] H. P. Schlickewei, *Die p-adische Verallgemeinerung des Satzes von Thue–Siegel–Roth–Schmidt*, J. Reine Angew. Math. (to appear).
[6] — *Linearformen mit algebraischen Koeffizienten*, Manuscripta Math. 18 (1976), pp. 147–185.
[7] W. M. Schmidt, *Simultaneous approximation to algebraic numbers by rationals*, Acta Math. 125 (1970), pp. 189–201.
[8] — *Linear forms with algebraic coefficients I*, J. Number Theory 3 (1971), pp. 253–277.
[9] — *Norm form equations*, Ann. of Math. 96 (1972), pp. 526–551.
[10] — *Simultaneous approximation to algebraic numbers by elements of a number field*, Monatsh. Math. 79 (1975), pp. 55–66.

MATHEMATISCHES INSTITUT DER UNIVERSITÄT
Freiburg i. Br.,

Received on 19. 5. 1975 (712)

ACTA ARITHMETICA
XXXI (1976)

Factorizations of distinct lengths in algebraic number fields

by

JAN ŚLIWA (Wrocław)

1. Let K be an algebraic number field. We shall denote by R_K its ring of integers, by P the set of all prime ideals of R_K, by H the classgroup of K and by h the classnumber.

It is known (L. Carlitz [1]) that in the case $h \geqslant 3$ some elements of R_K have factorizations into irreducibles of distinct lengths. In this paper we shall study the asymptotic distribution of numbers with factorizations of $m \geqslant 1$ distinct lengths. The set of all such numbers will be denoted by $G_m(K)$. In the case $m = 1$ we shall write also $G_1(K) = G(K)$.

Let $G_m(x)$ be the number of non-associated integers a in $G_m(K)$ with $|N(a)| \leqslant x$. We shall determine the asymptotic behaviour of $G_m(x)$ (Theorem 4) and in particular we shall prove that

$$G_1(x) = \big(C(K)+o(1)\big)\frac{x(\log\log x)^a}{(\log x)^{1-\frac{t}{h}}},$$

where $C(K) > 0$, a is a non-negative integer and $t = t(H)$ is a positive integer, which has a combinatorial meaning. We shall also obtain a similar result for natural numbers $\leqslant x$ lying in $G_m(K)$ (Theorem 5).

I am very grateful to Professor W. Narkiewicz for valuable remarks and guidance in the preparation of this paper.

2. To begin with we define two combinatorial constants attached to a given finite abelian group A which we shall write multiplicatively.

If $g_1, \ldots, g_k \in A$, $n_1, \ldots, n_k \in Z$ and

$$(1)\qquad g_1^{n_1}\ldots g_k^{n_k} = 1$$

then (1) will be called a *minimal equality*, provided

1° $0 \leqslant n_i \leqslant r_i =$ order of g_i $(i = 1, \ldots, k)$ and

$$\langle n_1, \ldots, n_k\rangle \neq \langle 0, \ldots, 0\rangle.$$

2° If $0 \leqslant m_i \leqslant n_i$ $(i = 1, \ldots, k)$ and $g_1^{m_1} \ldots g_k^{m_k} = 1$ then the k-tuple $\langle m_1, \ldots, m_k \rangle$ equals either $\langle n_1, \ldots, n_k \rangle$ or $\langle 0, \ldots, 0 \rangle$.

We shall say, that the minimal equality (1) *satisfies the condition* C, provided

$$\sum_{i=1}^{k} \frac{n_i}{r_i} = 1. \tag{2}$$

(This condition has been also considered by L. Skula [7].)

Now let U be any subset of A. We shall write $U \in C$, provided every minimal equality of the form (1) with $g_1, \ldots, g_k \in U$ satisfies the condition C.

Note that for $U = \{g\} \subset A$ one has trivially $U \in C$. Hence we can always write

$$A = \bigcup_{i=1}^{n} U_i \tag{3}$$

with suitable $U_i \in C$.

The minimal number n of summands needed in (3) will be denoted by $l(A)$. By $t(A)$ we shall denote the maximal cardinality of a set $U \in C$.

Clearly one has

$$1 \leqslant l(A) \leqslant |A| - 1$$

and

$$2 \leqslant t(A) \leqslant |A| \quad (\text{if } |A| \geqslant 2).$$

The following lemma lists the simplest properties of $l(A)$ and $t(A)$.

LEMMA 1. (i) *If H is a subgroup of A, then*

$$l(H) \leqslant l(A), \quad t(H) \leqslant t(A).$$

(ii) *If C_n is the cyclic group of n elements then $l(C_n) \geqslant \varphi(n)$.*

(iii) *For a prime p and $n \geqslant 1$ one has*

$$l(C_{p^n}) = \varphi(p^n) = p^{n-1}(p-1), \quad t(C_{p^n}) = n.$$

(iv) *For prime p and $n \geqslant 1$ one has*

$$t(C_p^n) \leqslant \binom{n+p-2}{p-1} + 1,$$

and moreover any $U \in C$ can contain at most $\binom{n+p-2}{p-1}$ elements which are $\neq 1$.

Proof. (i) Is obvious.

(ii) As C_n has $\varphi(n)$ generators, it suffices to observe that if g_1, g_2 are distinct generators of C_n and $g_1, g_2 \in U \subset C_n$ then $U \notin C$. Indeed, as $g_2 = g_1^m$ $((m, n) = 1,\ 1 < m < n)$, the equality $g_1^{n-m} g_2 = 1$ is minimal and does not satisfy C.

(iii) In view of (ii) it is enough to note that for any g generating C_{p^n} one has

$$\{1, g, g^p, g^{p^2}, \ldots, g^{p^{n-1}}\} \in C.$$

(iv) We can consider $A = C_p^n$ as an n-dimensional vector space over $GF(p)$. Let U be a subset of A, $U \in C$ and let $v_1, \ldots, v_s$ be a linearly independent subset of U.

If

$$x = \sum_{k=1}^{s} (p - a_k) v_k \quad (1 \leqslant a_i \leqslant p-1)$$

lies in U then from the minimality of

$$x + \sum_{k=1}^{s} a_k v_k = 0$$

we infer that

$$\sum_{k=1}^{s} a_k = p - 1.$$

Let $v_1, \ldots, v_t$ be a maximal linearly independent subset of U and put

$$U' = \Big\{ \sum_{k=1}^{t} (p - a_k) v_k \colon 0 \leqslant a_i \leqslant p-1,\ \sum_{i=1}^{t} a_i = p-1 \Big\}.$$

As $U \setminus \{0\} \subset U'$, $t \leqslant n$ and the equation $x_1 + \ldots + x_t = l$ has $\binom{t+l-1}{l}$ solutions in non-negative integers, we obtain

$$|U \setminus \{0\}| \leqslant |U'| = \binom{t+p-2}{p-1} \leqslant \binom{n+p-2}{p-1}.$$

COROLLARY.

(i) $l(A) = 1 \Leftrightarrow |A| = 1, 2$.

(ii) $l(A) = 2 \Leftrightarrow |A| = 3, 4, 6$.

(iii) $l(A) = 3 \Leftrightarrow A = C_2 \oplus C_2$, $C_2 \oplus C_2 \oplus C_2$ *or* $C_3 \oplus C_3$.

Proof. If $l(A) \leqslant 3$, then A cannot contain subgroups C_p with $p \geqslant 5$. Moreover

$$l(C_{2^k}) = 2^{k-1} > 3 \ (k \geqslant 3), \quad l(C_{3^k}) = 2 \cdot 3^{k-1} > 3 \ (k \geqslant 2).$$

So

$$A = C_2^k \oplus C_3^l \oplus C_4^m \quad \text{with} \quad k \leqslant 3,\ l \leqslant 2,\ m \leqslant 3.$$

Computing directly $l(A)$ for those groups one obtains the assertion. Lemma 1 enables us to obtain an asymptotic lower bound of $l(A)$:

THEOREM 1. *There exists positive constants C_1 and C_2 such that*

$$l(A) \geqslant C_1 \exp(C_2 \log^{1/2} N), \quad \textit{where} \quad N = |A|.$$

Proof. First we prove, that with suitable $C > 0$, $\theta > 1$ one has

$$l(C_p^k) \geqslant C\cdot\theta^k \quad (p \text{ — prime}, \ k = 1, 2, \ldots). \tag{4}$$

Lemma 1(iv) implies

$$l(C_p^k) \geqslant \frac{p^k-1}{\binom{k+p-2}{p-1}}$$

hence

$$l(C_2^k) \geqslant \frac{2^k-1}{k} \geqslant A_1\left(\frac{3}{2}\right)^k, \tag{5}$$

$$l(C_3^k) \geqslant \frac{3^k-1}{\binom{k+1}{2}} \geqslant A_2\left(\frac{3}{2}\right)^k \tag{5'}$$

with suitable $A_1, A_2 > 0$.

For $p \geqslant 5$ and $k \geqslant p$ one has

$$l(C_p^k) \geqslant \frac{p^k-1}{2^{2(k-1)}} \geqslant \frac{4}{5}\left(\frac{5}{4}\right)^k \tag{6}$$

and finally for $p \geqslant 5$, $k \leqslant p-1$ we have

$$\binom{k+p-2}{p-1} \leqslant \left(\frac{3p}{4}\right)^{k-1},$$

hence for $p \geqslant 5$ and all $k \geqslant 1$ $(k \leqslant p-1)$

$$l(C_p^k) \geqslant \frac{3}{4}\left(\frac{4}{3}\right)^k. \tag{7}$$

The inequalities (5), (5′), (6), (7) imply (4).

Now let

$$A = \bigoplus_{i=1}^{k} C_{n_i}$$

be a decomposition of A into cyclic factors with $n_1 | n_2 | \ldots | n_k$. Then

$$|A| = n_1 \ldots n_k \leqslant n_k^k$$

hence

$$\log|A| \leqslant k \log n_k.$$

If now p denotes the minimal prime factor of n_1, then by Lemma 1 and (4) we get

$$l(A) \geqslant \max\{l(C_p^k), l(C_{n_k})\} \geqslant \max\{C\cdot\theta^k, \varphi(n_k)\}.$$

Using the evaluation

$$\varphi(m) \geqslant \frac{m}{\log\log m}$$

we arrive at our assertion.

3. If H is the classgroup of K, then we shall write $l(K)$ instead o. $l(H)$. We present now two arithmetical interpretations of $l(K)$.

Let $\{A_i\}$ $(i \in I)$ be a family of subsets of R_K. We shall say it is a *decomposition* of R_K provided the following conditions are satisfied:

(i) If $x, y \in A_i$ then $xy \in A_i$ and if $x \in A_i$, $y|x$, then $y \in A_i$.

(ii) There exists $m \geqslant 1$ such that for every $x \in R_K$ one has

$$x^m = \prod_{i \in I} x_i,$$

where $x_i \in A_i$ and only finitely many numbers x_i are $\neq 1$.

A decomposition $\{A_i\}_{i\in I}$ will be called a *good decomposition*, provided $\bigcup_{i\in I} A_i \subset G(K)$.

THEOREM 2. *The minimal number l for which there exists a good decomposition $\{A_i\}_{i\in I}$ of R_K with $|I| = l$ equals $l(K)$.*

Proof. We start with a lemma relating the property C with the set $G(K)$:

LEMMA 2. *Let U be a subset of H. Write $I(U) = P(K) \cap U$, and let $R_K(U)$ denotes the set of all integers of K whose all prime ideal divisors belong to $I(U)$.*

Then $R_K(U) \subset G(K)$ holds if and only if $U \in C$.

Proof. Note first that $a \in R_K$ is irreducible if and only if the equality

$$\prod_{X \in H} X^{\Omega_X(a)} = 1$$

(where $\Omega_X(a)$ denotes the number of prime ideal divisors of a lying in the class X and counted according to their multiplicities) is minimal.

Let $X_1, \ldots, X_l \in U$, n_i = order of X_i and let

$$X_1^{m_1} \ldots X_l^{m_l} = 1$$

be a minimal equality which does not satisfy C. Choose $\mathfrak{p}_1, \ldots, \mathfrak{p}_l \in P(K)$ such that $\mathfrak{p}_i \in X_i$, $i = 1, \ldots, l$, and let

$$\mathfrak{p}_i^{n_i} = (a_i) \ (i = 1, \ldots, l), \quad \mathfrak{p}_1^{m_1} \ldots \mathfrak{p}_l^{m_l} = (a).$$

Obviously $a_1, \ldots, a_l, a$ are irreducible elements of $R_K(U)$. If $M = n_1 \ldots n_l$ then

$$(a^M) = \prod_{i=1}^{l} (a_i)^{Mm_i/n_i}.$$

As $1 \neq \sum (m_i/n_i)$ hence $a^M \in R_K(U) \setminus G(K)$.

Assume now that

$$U = \{X_1, \ldots, X_k\} \in C \quad \text{and} \quad a \in R_K(U).$$

Let

$$(8) \qquad \begin{array}{c} X_1^{m_1^{(1)}} \ldots X_k^{m_k^{(1)}} = 1, \\ \cdots\cdots\cdots \\ X_1^{m_1^{(s)}} \ldots X_k^{m_k^{(s)}} = 1 \end{array}$$

be all minimal equalities between the elements of U.

Let

$$(9) \qquad a = d_1 \ldots d_u$$

be a factorization of a into irreducibles. To every d occurring in (9) there corresponds the minimal equality

$$\prod_{i=1}^{k} X_i^{\Omega_{X_i}(d)} = 1.$$

Assume that to the ith equality in (8) correspond in that way u_i irreducibles from (9). Then

$$\Omega_{X_i}(a) = \sum_{j=1}^{s} u_j m_i^{(j)} \quad (i = 1, \ldots, k)$$

and $U \in C$ implies

$$\sum_{i=1}^{k} \frac{m_i^{(j)}}{n_i} = 1 \quad (j = 1, \ldots, s),$$

thus

$$u = \sum_{i=1}^{s} u_i = \sum_{j=1}^{k} \frac{\Omega_{X_j}(a)}{n_j}$$

is independent of the chosen factorization (9). Hence $a \in G(K)$.

The theorem follows now from the lemma and the observation that if $\{A_i\}_{i \in I}$ is a decomposition of R_K, and for $i \in I$ we denote by U_i the set of all classes of H containing a prime ideal dividing a number $a \in A_i$, then $R_K(U_i) = A_i$.

Let S be the set of all integers a of K such that in the factorization into prime ideals

$$aR_K = \prod_{i=1}^{s} \mathfrak{p}_i^{a_i} \quad (\mathfrak{p}_i \text{ — prime ideal}, \ a_i \geqslant 0)$$

the ideals $\mathfrak{p}_i^{a_i}$ $(i = 1, \ldots, s)$ are all principal. (Note that the hth powers of integers of K lie in S.)

Our second characterization of $l(K)$ is contained in the following theorem:

THEOREM 3. *The minimal number l such that every integer from S can be written as a product of l integers from $G(K)$ equals $l(K)$.*

Proof. We need a lemma.

LEMMA 3. *For any $a \in R_K$ put*

$$H(a) = \{X \in H\colon \ \Omega_X(a) > 0\}.$$

If $a \in G_m(K)$, $U \subset H(a)$ and $U \notin C$, then there exists a class $X \in U$ with

$$\Omega_X(a) < mh^2.$$

Proof. Let first $m = 1$. Choose $X_1, \ldots, X_k \in U$ and $m_1, \ldots, m_k \geqslant 0$ such that

$$\prod_{i=1}^{k} X_i^{m_i} = 1$$

is a minimal equality which does not satisfy condition C. Assume, tha for $i = 1, \ldots, k$ one has

$$\Omega_{X_i}(a) \geqslant h^2.$$

If n_i denotes the order of X_i, M is the least common multiple of $n_1, \ldots, n_k$ and $r_i = Mm_i/n_i$ then one may choose irreducible integers

$$b_1, \ldots, b_M, a_{ij} \quad (1 \leqslant i \leqslant k, \ 1 \leqslant j \leqslant r_i)$$

such that

1° $\Omega_{X_i}(b_j) = m_i$ $(i = 1, \ldots, k, \ j = 1, \ldots, M)$,
$\Omega_X(b_j) = 0$ $(X \neq X_1, \ldots, X_k, \ j = 1, \ldots, M)$;

2° $\prod_{j=1}^{M} b_j$ divides a;

3° $$\Omega_X(a_{ij}) = \begin{cases} n_i, & X = X_i, \\ 0, & X \neq X_i \end{cases}$$

and

4° $$b_1 \ldots b_M R_K = \Big(\prod_{i=1}^{k} \prod_{j=1}^{r_i} a_{ij}\Big) R_K.$$

The condition 4° implies $b_1 \dots b_M \notin G(K)$ and so $a \notin G(K)$ in view of 2°. This settles the case $m = 1$.

In the general case observe first that if a has factorizations of k distinct lengths, and b has factorization of l distinct lengths, then ab has at least $k+l-1$ factorizations of distinct lengths. Now we use the induction on m. If for all $X \in U$ there is

$$\Omega_X(a) \geqslant (m+1)h^2$$

then we can find $a_1, a_2 \in R_K$ such that $a_1 a_2 | a$ and

$$\Omega_X(a_1) \geqslant mh^2, \quad \Omega_X(a_2) \geqslant h^2$$

for all $X \in U$. Using the above remark and the inductive assumption we obtain that $a_1 a_2$ has at least $(m+1)+2-1 = m+2$ factorizations of distinct lengths. This proves our lemma.

Proof of Theorem 3. Observe first, that if $A_1, \dots, A_l$ is a good decomposition of R_K, then

$$S \subset A_1 A_2 \dots A_l, \quad A_i \subset G(K).$$

Indeed, if $a \in S$ and $aR_K = \prod_{\mathfrak{p}} \mathfrak{p}^{m_\mathfrak{p}}$, then for

$$H_i = \{\mathfrak{p} \in P(K) \colon \exists a \in A_i,\ \mathfrak{p} | aR_K\} \quad (i = 1, \dots, l)$$

and

$$a_1 = \prod_{\substack{\mathfrak{p} \in H_1 \\ \mathfrak{p} | (a)}} \mathfrak{p}^{m_\mathfrak{p}}, \quad a_2 = \prod_{\substack{\mathfrak{p} \in H_2 \\ \mathfrak{p} | \left(\frac{a}{a_1}\right)}} \mathfrak{p}^{m_\mathfrak{p}}, \quad \dots, \quad a_{l-1} = \prod_{\substack{\mathfrak{p} \in H_{l-1} \\ \mathfrak{p} | \left(\frac{a}{a_1 \dots a_{l-2}}\right)}} \mathfrak{p}^{m_\mathfrak{p}},$$

$$a_l = \frac{a}{a_1 \dots a_{l-1}}$$

one has $a = a_1 \dots a_l$ and $a_i \in G(K)$ $(i = 1, \dots, l)$.

On the other hand, if we choose $a \in S$ with $\Omega_X(a) > h^3$ for all $X \in H$ and $a = a_1 \dots a_n$, $n \leqslant l(K)$, $a_i \in G(K)$, then by Lemma 3 we have

$$U_i = \{X \colon \Omega_X(a_i) > h^2\} \in C.$$

If for some $X \in H$ we would have

$$\Omega_X(a_i) \leqslant h^2 \quad \text{for} \quad i = 1, \dots, n$$

then $\Omega_X(a) < nh^2 \leqslant l(K)h^2 \leqslant h^3$, a contradiction.

Hence

$$H \subset \bigcup_{i=1}^{n} U_i$$

and so $n \geqslant l(K)$.

4. Now we turn to the asymptotical behaviour of $G_m(x)$ and show:

THEOREM 4. *If K is a finite extension of the rationals, and $m \geqslant 1$, then either*

$$G_m(K) = \emptyset$$

or

$$G_m(x) = \big(C + o(1)\big)\frac{x(\log\log x)^B}{(\log x)^A},$$

where $C = C(m, K) > 0$, $A = A(m, H)$ and $B = B(m, H)$ are non-negative, and in the case $h \geqslant 3$, $A > 0$.

Proof. Any pair $S = \langle U, A \rangle$ where $U \subset H$, $U \in C$ and $A = \{A_X \colon X \in H \setminus U\}$, A_X – positive integers, will be called a *system*. The length of S is defined as $|U|$. For any system S and $d \geqslant 0$ let us put

$$N_S = \{a \in R_K \colon \Omega_X(a) = A_X \ (X \notin U)\},$$
$$N_S(d) = \{a \in N_S \colon \Omega_X(a) > d \ (X \in U)\}.$$

LEMMA 4. *There exists a finite set W of systems such that*

$$G_m(K) \subset \bigcup_{S \in W} N_S.$$

Proof. Let

$$W = \{S = \langle U, A_U \rangle \colon \text{for } X \notin U,\ A_X \leqslant mh^2\}.$$

If $a \in G_m(K)$ and $U = \{X \in H \colon \Omega_X(a) > mh^2\}$, $A_X = \Omega_X(a)$ for $X \notin U$, then by Lemma 3 we obtain $U \in C$, hence $\langle U, \{A_X\} \rangle$ is a system, which lies in W. As $a \in N_S$ and W is finite, our lemma is proved.

LEMMA 5. *If S is a system, then we can find a number $d = d(S)$ such that either*

$$N_S(d) \subset G_m(K) \quad \text{or} \quad N_S(d) \cap G_m(K) = \emptyset.$$

Proof. Let $S = \langle U, A_U \rangle$ with

$$U = \{X_1, \dots, X_t\}, \quad H \setminus U = \{X_{t+1}, \dots, X_h\} \quad \text{and} \quad A_U = \{A_{t+1}, \dots, A_h\}.$$

Let us write all possible minimal equalities in H:

$$\text{(I)} \qquad \prod_{i=1}^{t} X_i^{n_i(k)} = 1 \quad (k = 1, \dots, s),$$

$$\text{(II)} \qquad \prod_{i=1}^{h} X_i^{n_i(k)} = 1 \quad (k = s+1, \dots, s_1),$$

$$\text{(III)} \qquad \prod_{i=t+1}^{h} X_i^{n_i(k)} = 1 \quad (k = s_1+1, \dots, s_2).$$

Let $a \in N_S$, and for $1 \leqslant k \leqslant s_2$ denote by u_k the number of irreducible factors in $a = d_1 \ldots d_w$ (d_i irreducible) which correspond to the kth minimal equality in the same way as in the proof of Lemma 2. Then we get

$$(10) \qquad \sum_{k=1}^{s_2} u_k n_i(k) = \Omega_{X_i}(a) \qquad (i = 1, \ldots, t)$$

and

$$(11) \qquad \sum_{k=s+1}^{s_2} u_k n_i(k) = \Omega_{X_i}(a) = A_i \qquad (i = t+1, \ldots, h)$$

hence

$$w = u_1 + \ldots + u_{s_2} = \sum_{j=1}^{h} \frac{1}{n_j} \Omega_{X_j}(a) + \sum_{k=s+1}^{s_2} u_k \left(1 - \sum_{j=1}^{h} \frac{n_j(k)}{n_j}\right)$$

(n_j = order of X_j), as $\{X_1, \ldots, X_t\} \in C$.

If V_S is the set of all non-negative solutions $u_{s+1}, \ldots, u_{s_2}$ of (11),

$$d(S) = \max_{\substack{1 \leqslant i \leqslant t \\ (x_{s+1}, \ldots, x_{s_2}) \in V_S}} \sum_{j=s+1}^{s_2} x_j n_i(j)$$

and a was chosen to satisfy

$$\Omega_{X_i}(a) > d(S) \qquad (i = 1, \ldots, t)$$

then the number of distinct values of the linear form

$$\sum_{i=s+1}^{s_2} x_i \left(1 - \sum_{j=1}^{h} \frac{n_j(i)}{n_j}\right)$$

attained in V_S equals to the number of distinct lengths of factorizations of a.

This implies that all integers in $N_S\big(d(S)\big)$ have the same number of distinct lengths of factorizations and the lemma follows.

LEMMA 6. *Let S be a system. One can find systems $S_1, \ldots, S_n$ ($n = n(S)$) such that*

$$N_S \subset \bigcup_{j=1}^{n} N_{S_j}(d_j),$$

where $d_j = d(S_j)$ are taken from the last lemma.

Proof. We use induction on the length of S. If it equals 1, then

$$S = \langle \{X\}, A_2, \ldots, A_h \rangle$$

and if we put for $j = 0, 1, \ldots, d = d(S)$

$$S_j = \langle \emptyset, j, A_2, \ldots, A_h \rangle,$$

we obtain $d_j = d(S_j) = 0$, $N_{S_j}(d_j) = N_{S_j}$ and

$$N_S \subset N_S(d) \cup \bigcup_{j=0}^{d} N_{S_j}(d_j)$$

as asserted.

If now $S = \langle U, A \rangle$ is of length t, then

$$N_s \subset N_s(d) \cup \bigcup_{\substack{1 \leqslant i_1 < \ldots < i_j \leqslant t \\ j \geqslant 1}} \bigcup_{k_{i_1}=0}^{d} \cdots \bigcup_{k_{i_j}=0}^{d} N_{S_{i_1, \ldots, i_j, k_{i_1}, \ldots, k_{i_j}}}$$

where $d = d(S)$ and

$$(12) \qquad S_{i_1, \ldots, i_j, k_{i_1}, \ldots, k_{i_j}} = \langle \{X \in U \colon X \neq X_{i_1}, \ldots, X_{i_j}\}; k_{i_1}, \ldots, k_{i_j}, \{A\} \rangle.$$

As the length of (12) is $\leqslant t-1$ we may apply induction.

COROLLARY. *There exists a finite set L of systems such that with suitable integers d_S ($S \in L$) one has*

$$G_m(K) = \bigcup_{S \in L} N_S(d_S).$$

5. The last corollary clearly shows, that in order to solve the problem of the asymptotical behaviour of $G_m(x)$ we have to do the same for the sets $N_S(d_S)$. We shall accomplish this with the use of the tauberian theorem of H. Delange ([2]), which we state as

LEMMA 7. *Assume that the series*

$$\sum_{n=1}^{\infty} a_n n^{-s}$$

has all its coefficients real and non-negative and that it converges in $\operatorname{Re} s > 1$ *defining a function $f(s)$ regular there. Assume, moreover, that in the same half-plane we can write*

$$f(s) = g_0(s) \left(\log \frac{1}{s-1}\right)^{b_0} (s-1)^{-a_0} + \sum_{j=1}^{q} g_j(s) \left(\log \frac{1}{s-1}\right)^{b_j} (s-1)^{-a_j} + g(s),$$

where $g(s), g_0(s), \ldots, g_q(s)$ are regular in closed half-plane $\operatorname{Re} s \geqslant 1$, *$b_0, b_1, \ldots \ldots, b_q$ are non-negative rational integers, $a_1, \ldots, a_q$ are complex numbers* *whose real parts are smaller than a_0, which is a positive real number, and finally $g_0(1) \neq 0$. Then for $S(x) = \sum_{n \leqslant x} a_n$ we have for x tending to infinity, the asymptotic expression:*

$$S(x) = \big(g_0(1)\Gamma(a_0)^{-1} + o(1)\big)x(\log x)^{a_0-1}(\log\log x)^{b_0}.$$

However, if $f(s)$ satisfies the same assumptions with the following change: $a_0 = 0$, $b_0 \neq 0$, then we get

$$S(x) = \big(b_0 g_0(1) + o(1)\big)x(\log x)^{-1}(\log\log x)^{b_0-1}.$$

6. The system S with $N_S\big(d(S)\big) \subset G_m(K)$ will be called *m-admissible*. An m-admissible system

$$S = \langle U, A\rangle, \quad U = \{X_1, \ldots, X_l\}, \quad A = \{A_{l+1}, \ldots, A_h\}$$

will be called a *maximal m-admissible* system if N_S is non-empty, the length of S is the maximal possible, say equal to M, and $\sum_{i=l+1}^{h} A_i$ attains its maximal value amongst all m-admissible systems with length M.

Note, that $N_S \neq \emptyset$ if and only if

$$X_{l+1}^{A_{l+1}} \ldots X_h^{A_h}$$

lies in the group generated by $\{X_1, \ldots, X_l\}$.

Let now $X_1, \ldots, X_m$ be given distinct classes of H and let $c_i \geqslant 0$ $(i = 1, \ldots, m)$. In the case $m = h$ we assume moreover, that not all c_i vanish. Let $Y \in H$ and let $F_Y(x, c_1, \ldots, c_m)$ denote the number of ideals of norms $\leqslant x$, lying in Y and satisfying $\Omega_{X_i}(I) = c_i$ $(i = 1, \ldots, m)$. Then the following modification of Theorem 9.4 in [3] holds:

LEMMA 8. (i) *If $X_1^{c_1} \ldots X_m^{c_m} Y^{-1}$ does not belong to the subgroup of H generated by $H \setminus \{X_1, \ldots, X_m\}$, then for all $x > 0$*

$$F_Y(x, c_1, \ldots, c_m) = 0.$$

(ii) *Otherwise*

$$F_Y(x, c_1, \ldots, c_m) = \begin{cases} \big(C + o(1)\big)x(\log x)^{-m/h}(\log\log x)^{c_1+\ldots+c_m}, & m < h, \\ \big(C + o(1)\big)x(\log x)^{-1}(\log\log x)^{c_1+\ldots+c_m-1}, & m = h, \end{cases}$$

where C are positive constants, depending on $Y, c_1, \ldots, c_m$.

Proof. We prove only (ii), (i) being obvious.

In the same way as in [3] we arrive at the following identity valid for $\operatorname{Re} s > 1$:

$$(13) \quad \sum_{\substack{I \in Y \\ \Omega_{X_i}(I) = c_i}} N(I)^{-s} = (s-1)^{\frac{m}{h}-1}\left(\frac{1}{h}A^{(\chi_0)}(s)\left(\frac{\log\frac{1}{s-1}}{h}\right)^{c_1+\ldots+c_m}\right)\prod_{i=1}^{m}(c_i!)^{-1} + \frac{1}{h}\sum_{\chi \neq \chi_0}\overline{\chi(Y)}(s-1)^{b(\chi)}\left(\frac{\log\frac{1}{s-1}}{h}\right)^{c_1+\ldots+c_m} A^{(\chi)}(s) \times$$
$$\times \chi(X_1)^{c_1} \ldots \chi(X_m)^{c_m}\prod_{i=1}^{m}(c_i!)^{-1} + (s-1)^{\frac{m}{h}-1}P_0\left(\log\frac{1}{s-1}\right) + \sum_{\chi \neq \chi_0}(s-1)^{b(\chi)}P_\chi\left(\log\frac{1}{s-1}\right)$$

where χ runs over all characters of H, χ_0 the trivial character, $P_0(u)$, $P_\chi(u)$ are polynomials over the ring Ω of all functions regular in $\operatorname{Re} s \geqslant 1$ and of degrees $< c_1 + \ldots + c_m$, $A^{(\chi)}(s)$ lie in Ω and are positive at $s = 1$. Finally

$$b(\chi) = \frac{1}{h}\sum_{i=1}^{m}\chi(X_i).$$

Observe that $\operatorname{Re}\big(-b(\chi)\big) \leqslant 1 - m/h$ and the equality will hold here if and only if

$$(14) \quad \chi(X) = 1 \quad \text{for all } X \in H \setminus \{X_1, \ldots, X_l\}.$$

In this case we get $-b(\chi) = 1 - m/h$. If T denote the set of all characters χ, $\chi \neq \chi_0$ for which (14) holds, then for all $\chi \in T$ we have

$$\overline{\chi(Y)}\chi(X_1)^{c_1} \ldots \chi(X_m)^{c_m} = 1.$$

Now (13) implies

$$\sum_{\substack{I \in Y \\ \Omega_{X_i}(I) = c_i \\ 1 \leqslant i \leqslant m}} N(I)^{-s} = (s-1)^{\frac{m}{h}-1}\frac{1}{h}\left(\frac{1}{h}\log\frac{1}{s-1}\right)^{c_1+\ldots+c_m}\prod_{i=1}^{m}(c_i!)^{-1} + \Big(\sum_{\chi \in T \cup \{\chi_0\}} A^{(\chi)}(s)\Big) + $$
$$+ (s-1)^{\frac{m}{h}-1}P_0\left(\log\frac{1}{s-1}\right) + \sum_{\substack{\chi \notin T \\ \chi \neq \chi_0}}(s-1)^{b(\chi)}P_\chi\left(\log\frac{1}{s-1}\right).$$

As $\mathrm{Re}(-b(\chi)) < 1-m/h$ for $\chi \notin T$ and the degree of $P_0(u)$ is less than $c_1+\ldots+c_m$ we may apply Lemma 7 to obtain our assertion.

If M is any subset of R_K then by $M(x)$ we shall denote the number of non-associated elements of M whose norms do not exceed x in absolute value.

Observe that if $G_m(K) \neq \emptyset$ then there exists m-admissible systems whose lengts are positive, as we always can assume that $X = 1$ belongs to U.

Now let $S = \langle U, A\rangle$ be a system with $U = \{X_1, \ldots, X_t\}$, $A = \{A_{t+1}, \ldots, A_h\}$, $t \geq 1$, $N_S \neq \emptyset$ and let $d \geq 0$ be a positive integer.

LEMMA 9. *For x tending to infinity*

$$N_S(d)(x) = N_S(x) = \big(C+o(1)\big)x(\log x)^{-1+\frac{|U|}{h}}(\log\log x)^{\sum_{i=t+1}^{h} A_i},$$

where C is some positive constant.

Proof. For any sequence $1 \leq i_1 < \ldots < i_j \leq t$ define

$$B_S(i_1, \ldots, i_j) = \{a \in R_K\colon \Omega_{X_i}(a) = A_i \text{ for } i = t+1, \ldots, h \text{ and } \Omega_{X_i}(a) \leq d \text{ for } i = i_1, \ldots, i_j\},$$

and observe that

$$N_S(d)(x) = N_S(x) + \sum_{j=1}^{t}(-1)^j \sum_{1\leq i_1<\ldots<i_j\leq t} B_S(i_1, \ldots, i_j)(x) \tag{15}$$

(see [3]). As

$$B_S(i_1, \ldots, i_j) = \bigcup_{\substack{0\leq l_{i_k}\leq d\\ 1\leq k\leq j}} \{a \in R_K\colon \Omega_{X_i}(a) = A_i\ (i \geq t+1),\ \Omega_{X_i}(a) = l_i\ (i = i_1, \ldots, i_k)\}$$

therefore Lemma 8 implies

$$B_S(i_1, \ldots, i_j)(x) = O\big(x(\log x)^{-1+\frac{t-j}{h}}(\log\log x)^{jd+\sum_{i=t+1}^{h} A_i}\big).$$

As

$$N_S(x) = \big(C+o(1)\big)x(\log x)^{-1+\frac{|U|}{h}}(\log\log x)^{\sum_{i=t+1}^{h} A_i}$$

(15) implies the lemma.

Proof of Theorem 4. Let S_1, S_2 be two distinct m-admissible systems:

$$S_1 = \{(X_{i_1}, \ldots, X_{i_r});\ A_j, j \neq i_1, \ldots, i_r\},$$
$$S_2 = \{(X_{i_1'}, \ldots, X_{i_{r'}'});\ A_j', j \neq i_1', \ldots, i_{r'}'\}$$

and assume that $r, r' \geq 1$ and the sets N_{S_1}, N_{S_2} are both non-empty. Of course $N_{S_1} \cap N_{S_2} \neq \emptyset$ only if $A_j = A_j'$ for $j \neq i_1, \ldots, i_r, i_1', \ldots, i_{r'}'$ and in this case we have $N_{S_1} \cap N_{S_2} = N_S$ with

$$S = \{(X_{i_1''}, \ldots, X_{i_{r''}''}), A_j'', j \neq i_1'', \ldots, i_{r''}''\},$$

$$\{i_1'', \ldots, i_{r''}''\} = \{i_1, \ldots, i_r\} \cap \{i_1', \ldots, i_{r'}'\}$$

and

$$A_j'' = \begin{cases} A_j & \text{for } j \neq i_1, \ldots, i_r, \\ A_j' & \text{for } j \neq i_1', \ldots, i_{r'}'. \end{cases}$$

As $S_1 \neq S_2$ we must have $r'' < \max\{r, r'\}$ and Lemma 8 gives

$$(N_{S_1} \cap N_{S_2})(x) = N_S(x) = o\big(\max\{N_{S_1}(x), N_{S_2}(x)\}\big)$$

for x tending to infinity. Lemma 9 implies now that for $d_1, d_2 \geq 0$

$$\big(N_{S_1}(d_1) \cup N_{S_2}(d_2)\big)(x) \sim N_{S_1}(x) + N_{S_2}(x).$$

Applying Lemmas 8 and 9 and Corollary to Lemma 6 we get

$$G_m(x) = \big(C+o(1)\big)x(\log x)^{-1+\frac{M}{h}}(\log\log x)^{\Sigma A_i}$$

where C is a positive constant.

Obviously, if there are no m-admissible systems S, for which $N_S \neq \emptyset$ then $G_m(K) = \emptyset$.

COROLLARY 1. *For x tending to infinity*

$$G(x) = \big(C(K)+o(1)\big)\frac{x(\log\log x)^a}{(\log x)^{1-\frac{t(H)}{h}}},$$

where $t(H)$ is the constant introduced in Section 2, a is a constant, depending on H and satisfying $0 \leq a \leq h^2(h-t(H))$.

Proof. Let U be a subset of H satisfying C with $t(H)$ elements. Then the system $S = \langle U, \{0, \ldots, 0\}\rangle$ is 1-admissible and the maximal 1-admissible systems have to be sought among the systems of the form $\langle U, \{A_{t+1}, \ldots, A_h\}\rangle$ $(t = t(H),\ 0 \leq A_i \leq h^2)$.

COROLLARY 2. *If $h = 3$, then*

$$G_m(x) = \big(C(m, K)+o(1)\big)\frac{x(\log\log x)^{3m-1}}{(\log x)^{1/3}}.$$

Proof. It suffices to observe, that if $H = \{1, X, Y\}$ then the only maximal m-admissible systems are

$$\langle\{1, X\}, 3m-1\rangle \quad\text{and}\quad \langle\{1, Y\}, 3m-1\rangle.$$

7. In this section we shall study the asymptotic behaviour of

$$G'_m(x) = \sum_{\substack{n\leqslant x \\ n\in G'_m(K)}} 1$$

where

$$G'_m(K) = G_m(K)\cap \mathcal{N}.$$

We prove

THEOREM 5. *If K is a finite extension of the rationals and $m\geqslant 1$, then either*

$$G'_m(K) = \emptyset$$

or

$$G'_m(x) = \big(C+o(1)\big)\frac{x(\log\log x)^B}{(\log x)^A},$$

where A, B, C are constants, depending on K and m, B is a non-negative integer, $A\geqslant 0$, $C>0$ and in the case $h\geqslant 3$ also $A>0$.

Proof. Let p be a rational prime and let $pR_K = \mathfrak{p}_1\ldots\mathfrak{p}_n$ be its decomposition into prime ideals. If $\mathfrak{p}_i\in X_i\in H$ $(i=1,\ldots,n)$ then $(X_1,\ldots,X_n)$ will be called the *orbit* of p. If O is such an orbit and $X\in H$ then we write $\Omega_X(O)$ for number of $1\leqslant j\leqslant n$, for which $X_j = X$, and P_O for the set of all rationals primes which have O as its orbit. If $V=\{O_1,\ldots,O_s\}$ is a set of orbits, then by U_V we denote the set of all distinct elements in $O_1\cup\ldots\cup O_s$. Let V be such that $U_V\in C$ and let $O_{s+1},\ldots,O_m$ denote all remaining orbits. If $B_{s+1},\ldots,B_m$ are non-negative integers then the pair

$$Z = \langle V, \{B_{s+1},\ldots,B_m\}\rangle$$

will be called a *system* in $\mathcal{N}$ and $|V|$ will be called the *length* of Z.

To each such system there corresponds a set $M_Z\subset\mathcal{N}$ defined by

$$M_Z = \{n\in\mathcal{N}\colon\ \Omega_{P_j}(n) = B_j,\ j=s+1,\ldots,m\},$$

where $P_j = P_{O_j}$ and $\Omega_{P_j}(n)$ denotes the number of primes of P_j dividing n, each counted according to its multiplicity. For $d\geqslant 0$ let

$$M_Z(d) = \{n\in M_Z\colon\ \Omega_{P_j}(n) > d \text{ for } 1\leqslant j\leqslant s\}.$$

If $U_V = \{X_1,\ldots,X_t\}$ and $X_{t+1},\ldots,X_h$ denote the remaining elements of H, then for $n\in M_Z$, $l\geqslant 1+t$ we have

$$\Omega_{X_l}(n) = \sum_{=s+1}^{m}\Omega_{X_l}(O_j)B_j = A_l,\ \text{say}.$$

With Z we may associate a system S_Z in R_K putting

$$S_Z = \langle U_V, \{A_{t+1},\ldots,A_h\}\rangle.$$

Note, that

$$M_Z\subset N_{S_Z}\cap\mathcal{N}. \tag{16}$$

We prove now

LEMMA 10. *There exists a finite set W' of systems such that*

$$G'_m(K)\subset\bigcup_{Z\in W'} M_Z.$$

Proof. We prove that the set

$$W = \{Z = \langle V, \boldsymbol{B}\rangle\colon\ B\in\boldsymbol{B}\to B\leqslant mh^2\}$$

has the required property.

Let $n\in G'_m(K)$ and

$$V_n = \{O\colon\ \Omega_{P_O}(n) > mh^2\}.$$

For $X\in U_{V_n}$ we have

$$\Omega_X(n) = \sum_O \Omega_X(O)\,\Omega_{P_O}(n)\geqslant mh^2$$

and the Lemma 3 implies $U_{V_n}\in C$. Consider the system

$$Z_n = \langle V_n\colon\ \{\Omega_{P_O}(n)\}(O\notin V_n)\rangle.$$

Of course $Z_n\in W$, $n\in M_{Z_n}$.

Lemma 5 implies that there exists $d = d(S_Z)$ such that

$$N_{S_Z}(d)\subset G_m(K)\quad\text{or}\quad N_{S_Z}(d)\cap G_m(K) = \emptyset.$$

From (16) it follows that for some $d' = d'(d)$ one has

$$M_Z(d')\subset N_{S_Z}(d)\cap\mathcal{N}.$$

Hence for any system Z in $\mathcal{N}$, there exists $d = d(Z)$ such that

$$M_Z(d)\subset G'_m(K)\quad\text{or}\quad M_Z(d)\cap G'_m(K) = \emptyset.$$

In the same way as in Section 4, one gets

COROLLARY. *There exists a finite set L' of systems in $\mathcal{N}$, such that with suitable integers d_Z $(Z\in L')$ one has*

$$G'_m(K) = \bigcup_{Z\in L'} M_Z(d_Z).$$

The system Z with $M'_Z\big(d(Z)\big)\subset G'_m(K)$ will be called m-admissible.

To apply analytical methods to our problem we need more information about primes belonging to a given orbit. This will be done in the following lemma, the proof of which will be omitted, as it is a simple modification of the proof of a similar result, obtained by R. Odoni ([6]).

LEMMA 11. *If O denotes an orbit, then either P_O is finite or*

$$\sum_{p\in P_O} p^{-s} = q(0)\log\frac{1}{s-1} + g_O(s)$$

where $q(0) > 0$ and $g_O(s)$ is regular for $\operatorname{Re} s \geqslant 1$.

The final step of our proof will utilize the following lemma:

LEMMA 12 (see [5], Lemma 7). *Suppose $P_1, \ldots, P_r$ are disjoint regular sets of rational primes with positive densities $q_1, \ldots, q_r$ respectively, satisfying $q_1 + \ldots + q_r < 1$ and $T_1, \ldots, T_k$ are disjoint finite sets and disjoint with $P_1 \cup \ldots \cup P_r$. Suppose further that $c_1, \ldots, c_r, b_1, \ldots, b_k$ are given non-negative integers. Denote by $F(x) = F(x, c_1, \ldots, c_r, b_1, \ldots, b_k)$ the number of positive integers not exceeding x for which*

$$\Omega_{P_i}(n) = c_i, \quad \Omega_{T_j}(n) = b_j \quad (1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant k).$$

Then for some constant $C > 0$ and x tending to infinity

$$F(x) = \big(C + o(1)\big)x(\log x)^{-(q_1+\ldots+q_r)}(\log\log x)^{c_1+\ldots+c_r}.$$

The m-admissible system $T = \langle V, \boldsymbol{B}\rangle$ we will call a *maximal m-admissible* system if

1° $q(Z) = \sum_{O\in V} q(0)$ is maximal among m-admissible systems ($q(0)$ defined as in Lemma 11, in case P_O finite we put $q(0) = 0$).

2° $s(Z) = \sum_{B\in\boldsymbol{B}} B$ is maximal among m-admissible systems Z with maximal value of $q(Z)$.

Observe that if $G'_m(K) \neq \emptyset$ then there exist m-admissible systems Z with $q(Z) > 0$. This is a consequence of the fact that the rational primes which have in decomposition into prime ideals only principal ideals, have a positive density ([6]).

For system of this type we get using Lemma 12

$$M_Z(x) = \big(C_Z + o(1)\big)x(\log x)^{q(Z)-1}(\log\log x)^{s(Z)}$$

with some positive C_Z.

Proceeding now as in the proof of Lemma 9 we get for any $d \geqslant 0$

$$M_Z(d)(x) = \big(C_Z(d) + o(1)\big)x(\log x)^{q(Z)-1}(\log\log x)^{s(Z)}$$

and now corollary to Lemma 10 implies our assertion, with $A = 1 - q(Z)$ $B = s(Z)$, where Z is any maximal m-admissible system in $\mathcal{N}$.

Our proof does not give any information about the constants A, B. But in some particular cases, exact values of these constants are known.

If K is a quadratic field and $h \neq 1, 2$ then ([4], [5]) $A = (h-g-1)/2h$ where g denotes number of even invariants of H. If moreover H is cyclic then in the case of even h $B = (h-2)/2$, and in the case of odd h $B = h-1$.

References

[1] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. 11 (1960), pp. 391–392.

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

[3] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Warszawa 1974 (Chapter IX).

[4] — *Factorization on natural numbers in some quadratic number fields*, Colloq. Math. 16 (1967), pp. 257–268.

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

[6] R. Odoni, *On a problem of Narkiewicz*, to appear in Journ. Reine Angew. Math.

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

INSTYTUT MATEMATYCZNY UNIWERSYTETU WROCŁAWSKIEGO IM. B. BIERUTA
MATHEMATICAL INSTITUTE, WROCŁAW UNIVERSITY

Received on 30. 6. 1975 (736)