COLLOQUIUM MATHEMATICUM

VOL. XV 1966 FASC. 1

ON ALGEBRAIC NUMBER FIELDS WITH NON-UNIQUE FACTORIZATION, II

BY

W. NARKIEWICZ (WROCŁAW)

1. It was proved in [4] that in an algebraic number field with the class-number $h > 1$ almost all integers have non-unique factorization into irreducible factors, and if the field in question is normal then almost all rational integers have non-unique factorization.

L. Carlitz proved in [1] that in fields with $h > 2$ there are integers which have factorizations into irreducible factors with different lengths. (The length of a factorization is the number of irreducible non-unit factors occuring in it.) In [4] it was proved that almost all integers have this property and that in the case of a quadratic number field almost all rational integers share this property as well.

In this note* we prove the last result for all normal extensions of the rationals with the class-number at least 3.

2. Let $\mathcal{K}$ be a normal algebraic number field of degree N with Galois group G and class-group $H \neq C_2$. By E we shall denote the unit element of H and h will be the class-number of $\mathcal{K}$. Evidently every element of G induces an automorphism of H. For every $X \in H$ let $O(X)$ be the orbit of X under G, i. e. $O(X) = \{sX: s \in G\}$. We shall write the orbits in the form $O = (X_1, \ldots, X_N)$, where $X_i = s_i(X_1)$ and $s_1, \ldots, s_N$ is an ordering of G which usually will be arbitrary but fixed independently of the choice of X_1. Let W be the number of different orbits $\neq O(E)$, $m(X)$ the order of X in H and $s(X)$ the number of elements of G which leave X invariant. Obviously $m(X)$ and $s(X)$ depend only on the orbit to which X belongs, so that for any orbit O, $s(O)$ and $m(O)$ are well-defined. Let m^* be the least common multiple of the numbers $m(X)$ $(X \in H)$, $M = \max_{X \in H} m(X)$, A — the number of orbits $O \neq O(E)$ such that $X \in O$ implies $X^{-1} \in O$, and $B = \sum m(O)$, where the sum is extended over

* During the preparation of this paper the author held a British Council Scholarship at the University College, London.

all such orbits. Let $t_k = 2k/N$ if N divides $2k$ and $t_k = [2k/N]+1$ if not. (Here k is an arbitrary natural number.) Let $C = \sum_{O \neq O(E)} m(O)$ and finally let

$$V = \frac{1}{2} \sum_{O=O(X)\neq O(X^{-1})} s(O)^{-1} + \sum_{\substack{O=O(X)=O(X^{-1}) \\ m(O)\neq 2}} s(O)^{-1}.$$

We shall say that a rational prime p *belongs to the orbit* O if $p = \mathfrak{p}_1 \ldots \mathfrak{p}_N$, where $\mathfrak{p}_i \in X_i$ and $O = (X_1, \ldots, X_N)$. For such a prime we shall write $p \sim O$. (This definition applies only to primes which are norms of a prime ideal of the first degree, but they are the only ones which are important for us.)

By a *factorization* of an orbit $O = (X_1, \ldots, X_N)$ we shall understand any decomposition

$$E = (X_{i_1^{(1)}} \ldots X_{i_{k_1}^{(1)}}) \ldots (X_{i_1^{(z)}} \ldots X_{i_{k_z}^{(z)}}),$$

where $i_1^{(1)}, \ldots, i_{k_z}^{(z)}$ is a permutation of the set $\{1, 2, \ldots, N\}$ such that for $j = 1, 2, \ldots, z$ we have

$$X_{i_1^{(j)}} \ldots X_{i_{k_j}^{(j)}} = E$$

and where the equality

$$X_{i_{t_1}^{(j)}} \ldots X_{i_{t_v}^{(j)}} = E$$

for some $\{t_1, \ldots, t_v\} \subset \{1, \ldots, k_j\}$ with all t_i-s distinct implies $\{t_1, \ldots, t_v\} = \{1, \ldots, k_j\}$.

We shall call z the *length of the factorization*. Evidently every factorization of an orbit induces a factorization (with the same length) of any prime belonging to this orbit, and conversely.

Let K be the number of orbits $\neq O(E)$ which have a factorization of the length different from $N/2$ (if N is odd, then $K = W$) and let $Z = \sum s(O)^{-1}$ where the sum is extended over all such orbits.

By $f(n)$ we denote the number of factorizations of the rational positive integer n, which have different lengths. Finally, for any set of rational primes P we shall denote by $\Omega_P(n)$ the number of primes in P, which divide n, each counted according to its multiplicity.

We can now state our result:

THEOREM. *Let $\mathcal{K}$ be a normal algebraic number field with the class-number $h > 2$. Let $F_k(x)$ be the number of rational positive integers not greater than x, with at most k factorizations of different lengths. Then $F_k(x) = o(x)$.*

More precisely $F_k(x) = O\{x(\log\log x)^{b_k}(\log x)^{-a_k}\}$, where a_k and b_k are defined as follows:

(i) *If* $(h, 2N) = 1$, *then* $a_k = (h-1)/hN$, $b_k = \min(2Ck - W, k(W-1)m^* + 2Mk - W)$,

(ii) *if* $(h, 2N) > 1$, *but* $H \neq C_2 \times C_2 \times \ldots \times C_2$, *then* $a_k = V/h$, $b_k = t_k B - A + (W-A)(k-1)/2$,

(iii) *if* $H = C_2 \times \ldots \times C_2$, *and* $K > 0$, *then* $a_k = Z/h$, $b_k = K(2k-1)$,

(iv) *if* $H = C_2 \times \ldots \times C_2$ *and* $K = 0$, *then* $a_k = T/h$, *where* T *is defined in a rather complicated way by* (4), *and* $b_k = W(k-1)$.

(It should be remarked that a_k does not depend on k at all, and so in the case of a quadratic field we get here an improvement of the result obtained in [4]).

The proof is based on the following result of H. Delange:

(*) *Let* P *be a set of rational primes such that for* $\operatorname{Re} s > 1$

$$\sum_{p \in P} p^{-s} = \lambda \log\bigl(1/(s-1)\bigr) + g(s),$$

where λ *is positive and* $g(s)$ *is a function regular for* $\operatorname{Re} s \geqslant 1$.

Then

$$\sum_{\substack{n \leqslant x \\ \Omega_P(n) \leqslant k}} 1 = Cx(\log\log x)^k (\log x)^{-\lambda} + o\bigl(x(\log\log x)^k (\log x)^{-\lambda}\bigr)$$

where C *is some positive constant depending on* k *and the set* P (see [2], th. 36).

Moreover, we shall use the following well-known result:

(**) *If* O *is any orbit, then for* $\operatorname{Re} s > 1$ *we have*

$$\sum_{P \sim O} p^{-s} = \frac{1}{hs(O)} \log\bigl(1/(s-1)\bigr) + g(s)$$

with some $g(s)$ *regular for* $\operatorname{Re} s \geqslant 1$.

Let us remark that with the use of (*) one can improve the exponents in the theorem I in [4], which will take thus the following form:

Let K be a finite algebraic normal extension of the rationals with the classnumber $h \neq 1$. Denote by $S_k(x)$ the number of rational positive integers not greater than x, having at most k essentially different factorizations in K. Then

$$S_k(x) \ll x(\log\log x)^{(r-1)(kC-W)} (\log x)^{-(h-1)/hN},$$

where r is the least integer greater than $\frac{1}{2}(1+\sqrt{8k-7})$.

In the case of the field $Q(\sqrt{-5})$ and $k = 1$ we obtain

$$S_1(x) \ll x(\log\log x)(\log x)^{-1/4}. \tag{1}$$

This improves a result of Fogels, who proved in [3]

$$S_1(x) \ll x(\log\log x)^{4/5} (\log x)^{-1/5}.$$

It is easy to see that (1) cannot be improved, as every rational integer having in $Q(\sqrt{-5})$ at most one rational prime divisor which is a product of two non-principal prime ideals must have a unique factorization, and the number of such positive rational integers which are not greater than x is by (*) and (**) $\geqslant x(\log\log x)(\log x)^{-1/4}$.

2. LEMMA 1. *If* $(h, 2N) = 1$, *and* $f(n) \leqslant k$, *then* $\Omega_P(n) \leqslant \min\big(2Ck - W, k(W-1)m^* + 2Mk - W\big)$, *where* P *is the set of all rational primes which are norms of non-principal prime ideals.*

Proof. Let $X, Y \in H$ ($X, Y \neq E$, but we do not assume $X \neq Y$). Let $(X_1, \ldots, X_N) = O_1$ be the orbit of X and $(Y_1, \ldots, Y_N) = O_2$ the orbit of Y. Let $m(X) = m_1$, $m(Y) = m_2$, $[m_1, m_2] = R$. Consider now arbitrary factorizations of the orbits O_1 and O_2:

$$X_1 \ldots X_{j_1} = X_{j_1+1} \ldots X_{j_2} = \ldots = X_{j_{s-1}+1} \ldots X_N = E,$$
$$Y_1 \ldots Y_{i_1} = Y_{i_1+1} \ldots Y_{i_2} = \ldots = Y_{i_{s'-1}+1} \ldots Y_N = E$$

of lengths s and s' respectively.

If now $p_r \sim O_1$, $q_r \sim O_2$ ($r = 1, 2, \ldots, kR$), then since

$$p_r = \prod_{i=1}^{N} \mathfrak{p}_i^{(r)} \quad (\mathfrak{p}_i^{(r)} \in X_i), \qquad q_r = \prod_{i=1}^{N} \mathfrak{q}_i^{(r)} \quad (\mathfrak{q}_i^{(r)} \in Y_i)$$

we have, for $n = p_1 q_1 \ldots p_{Rk} q_{Rk}$, the following factorizations:

$$\begin{aligned} n = \prod_{\mu=1}^{wR} (\mathfrak{p}_1^{(\mu)} \ldots \mathfrak{p}_{j_1}^{(\mu)}) \ldots (\mathfrak{p}_{j_{s-1}+1}^{(\mu)} \ldots \mathfrak{p}_N^{(\mu)}) \times \\ \times \prod_{\mu=1}^{wR} (\mathfrak{q}_1^{(\mu)} \ldots \mathfrak{q}_{i_1}^{(\mu)}) \ldots (\mathfrak{q}_{i_{s'-1}}^{\mu} \ldots \mathfrak{q}_N^{(\mu)}) \times \\ \times \prod_{\lambda=1}^{w} (\mathfrak{p}_\lambda^{(wR+1)} \ldots \mathfrak{p}_\lambda^{(wR+m_1)}) \ldots (\mathfrak{p}_\lambda^{(Rk-m_1+1)} \ldots \mathfrak{p}_\lambda^{(Rk)}) \times \\ \times \prod_{\lambda=1}^{N} (\mathfrak{q}_\lambda^{(wR+1)} \ldots \mathfrak{q}_\lambda^{(wR+m_2)}) \ldots (\mathfrak{q}_\lambda^{(Rk-m_2+1)} \ldots \mathfrak{q}_\lambda^{(Rk)}) \end{aligned}$$

for $w = 0, 1, 2, \ldots, k$. The length of such a factorization is evidently equal to $wR\big((s+s') - N(m_1^{-1} + m_2^{-1})\big) + RNk(m_1^{-1} + m_2^{-1})$.

If $s + s' = N(m_1^{-1} + m_2^{-1})$, then $(s+s')m_1 m_2 = N(m_1 + m_2)$, and so m_1 divides Nm_2 and m_2 divides Nm_1. As m_1 divides h and $(h, N) = 1$, it follows that $m_1 = m_2$ and so $(s+s')m_1 = 2N$, whence m_1 divides $2N$ and finally m_1 must be equal to 1. But this is impossible, as $X \neq E$. Then $s + s' \neq N(m_1^{-1} + m_2^{-1})$ and so all the factorizations (2) have different lengths. Hence $f(n) \geqslant 1 + k$.

Consequently, if $f(m) \leqslant k$ for some m, then for every orbit $O \neq O(E)$, m one can have at most $2km(O)-1$ prime factors $p \sim O$ and, moreover, there is at most one orbit $O \neq O(E)$ such that m has at least km^* prime factors belonging to it. The lemma follows now easily.

To prove the theorem in the case (i) let us observe that the Dirichlet density of the set of all rational primes which are norms of non-principal prime ideals is by (**) equal to $(h-1)/hN$. The application of (*) and lemma 1 gives us the desired result.

3. Now let us turn to the case (ii). Thus we assume that $H \neq C_2 \times \ldots \times C_2$. (In what follows, the case $(h, 2N) = 1$ is not formally excluded, but obviously the result obtained in this case is much weaker than the foregoing.)

LEMMA 2. *If $f(n) \leqslant k$, and $X \in H$ is such that $X^2 \neq E$, $O(X) \neq O(X^{-1})$, then $n = p_1 \ldots p_j q_1 \ldots q_j \cdot Q$, where $p_i \sim O(X)$, $q_i \sim O(X^{-1})$, $\min(j, j') \leqslant k-1$, and Q has no prime divisors belonging to either of the orbits $O(X)$, $O(X^{-1})$.*

Proof. Let $O(X) = (X_1, \ldots, X_N)$, $O(X^{-1}) = (Y_1, \ldots, Y_N)$ where $Y_i = X_i^{-1}$ $(i = 1, 2, \ldots, N)$. Suppose that the orbits are ordered in such a way that $E = X_1 \ldots X_{j_1} = \ldots = X_{i_{s-1}} \ldots X_N$ is a factorization of $O(X)$. Then obviously $E = Y_1 \ldots Y_{j_1} = \ldots = Y_{j_{s-1}} \ldots Y_N$ is a factorization of $O(X^{-1})$. If now

$$p_i = \prod_{j=1}^{N} \mathfrak{p}_j^{(i)} \sim O(X), \qquad q_i = \prod_{j=1}^{N} \mathfrak{q}_j^{(j)} \sim O(X^{-1})$$

$$(\mathfrak{p}_j^{(i)} \in X_j,\ \mathfrak{q}_j^{(i)} \in Y_j,\ j = 1, \ldots, N),$$

then the number $n = p_1 \ldots p_k q_1 \ldots q_k$ will have the following factorizations

$$n = \prod_{i=1}^{r} \prod_{t=0}^{s-1} (\mathfrak{p}_{j_t+1}^{(i)} \ldots \mathfrak{p}_{j_{t+1}}^{(i)})(\mathfrak{q}_{j_t+1}^{(i)} \ldots \mathfrak{q}_{j_{t+1}}^{(i)}) \prod_{i=1+r}^{k} \prod_{t=1}^{N} (\mathfrak{p}_t^{(i)} \mathfrak{q}_t^{(i)})$$

for $r = 0, 1, \ldots, k$. The length of such a factorization is equal to $r(2s-N) + kN$, and so $f(n)$ will be at least $1+k$, provided $2s \neq N$. But observe that the equality $j_{t+1} - j_t = 1$ for some t would imply $X_{j_{t+1}} = E$, and $j_{t+1} - j_t = 2$ would imply $X_{j_{t+1}} = X_{j_t+1}^{-1} = Y_{j_t+1}$. In both cases a contradiction, as $X_i \neq E$ and the orbits $O(X)$ and $O(X^{-1})$ are disjoint. Hence $j_{t+1} - j_t \geqslant 3$ holds for all t. Consequently $N = (N - j_{s-1}) + (j_{s-1} - j_{s-2}) + \ldots + (j_2 - j_1) \geqslant 3s$, and so $N \neq 2s$, and the lemma follows.

LEMMA 3. *If $f(n) \leqslant k$, and $X \in H$ is such that $X^2 \neq E$ and $O(X) = O(X^{-1})$, then $n = p_1 \ldots p_j Q$, where $p_i \sim O(X)$, Q has no prime divisors belonging to the orbit $O(X)$, and $j \leqslant t_k m(X) - 1$.*

Proof. In our case $Y \in O(X)$ implies $Y^{-1} \in O(X)$, and so the orbit $O(X)$ has the form $(X_1, X_1^{-1}, \dots, X_{N/2}, X_{N/2}^{-1})$. If now

$$p_i = \prod_{j=1}^{N/2} \mathfrak{p}_j^{(i)} \prod_{j=1}^{N/2} \mathfrak{q}_j^{(i)} \sim O(X) \qquad (\mathfrak{p}_j^{(i)} \in X_j,\ \mathfrak{q}_j^{(i)} \in X_j^{-1}),$$

then the number $n = p_1 \dots p_{m(X)}$ has the following factorizations:

$$n = \prod_{i=1}^{m(X)} (\mathfrak{p}_1^{(i)} \mathfrak{q}_1^{(i)}) \dots (\mathfrak{p}_r^{(i)} \mathfrak{q}_r^{(i)}) \prod_{j=1}^{N/2-r} \left(\prod_{i=1}^{m(X)} \mathfrak{p}_{r+j}^{(i)} \right) \prod_{j=1}^{N/2-r} \prod_{i=1}^{m(X)} \left(\mathfrak{q}_{r+j}^{(i)} \right)$$

for $r = 0, 1, 2, \dots, N/2$. The length of such a factorization is equal to $r(m(X)-2)+N$, and as $m(X) \neq 2$, it follows that $f(n) \geqslant 1+N/2$.

If now the number m has the form $m = p_1 \dots p_{t_k m(X)}$ $(p_i \sim O(X))$, then for every $j = 0, 1, \dots, t_k-1$ there exist factorizations of the number $p_{jm(X)+1} \dots p_{(j+1)m(X)}$ with the lengths $r_j(m(X)-2)+N$, where r_j is any number from the interval $[0, N/2]$. By putting them together, we obtain a factorization of m with the length equal to $(r_0+\dots+r_{t_k-1}) \times (m(X)-2)+t_k N$. As there are $t_k N/2+1$ different numbers here, it follows that $f(m) \geqslant Nt_k/2+1 \geqslant k+1$, and the lemma easily follows.

Now we can prove our theorem in the case (ii). Let $O_i = O(X_i)$ be all orbits $\neq O(E)$ such that $O(X_i) \neq O(X_i^{-1})$. Here $i = 1, 2, \dots, W-A$. We can assume that they are numbered in such way that $O(X_{A'+i}) = O(X^{-1})$ for $i = 1, 2, \dots, A'$, where $A' = (W-A)/2$.

Now let

$$P_0 = \bigcup_{\substack{X \\ O(X) = O(X^{-1}) \\ X^2 \neq E}} \{p : p \sim O(X)\}, \qquad P_j^{(+1)} = \{p : p \sim O_j\},$$

$$P_j^{(-1)} = \{p : p \sim O_{j+A'}\} \qquad (j = 1, 2, \dots, A').$$

From lemmas 2 and 3 it follows that if $f(n) \leqslant k$, then

$$\Omega_{P_0}(n) \leqslant \sum_{\substack{O(X) \neq O(E), O(X) = O(X^{-1}) \\ m(O) \neq 2}} (t_k m(O)-1) \leqslant \sum_{\substack{O \neq O(E) \\ O(X) \neq O(X^{-1})}} (t_k m(O)-1) \leqslant t_k B - A$$

and, moreover, $\min\left(\Omega_{P_i^{(+1)}}(n), \Omega_{P_i^{(-1)}}(n)\right) \leqslant k-1$ for $j = 1, \dots, A'$.

For every sequence $e = \{e_1, \dots, e_{A'}\}$ $(e_i = \pm 1)$ let us put

$$P^{(e)} = \bigcup_{j=1}^{A'} P_j^{(e)_j}.$$

For every n with $f(n) \leqslant k$ there is such a sequence e with $\Omega_{P^{(e)}}(n) \leqslant A'(k-1)$ and so if we finally define $\bar{P}^{(e)} = P^{(e)} \cup P_0$ we will have

$$\Omega_{\bar{P}^{(e)}}(n) \leqslant A'(k-1)+t_k B - A.$$

Hence

$$\sum_{\substack{n\leqslant x\\ f(n)\leqslant k}} 1 \leqslant \sum_{e} \sum_{\substack{n\leqslant x\\ \Omega_{\overline{P}(e)}(n)\leqslant t_k B-A+A'(k-1)}} 1. \tag{3}$$

Since for $\mathrm{Re}\, s > 1$, we have by (**)

$$\sum_{p\in P(e)} p^{-s} = \left(\frac{1}{n}\sum_{j=1}^{A'} s^{-1}(O_j)\right)\log\frac{1}{s-1} + g(s)$$

with some $g(s)$ regular for $\mathrm{Re}\, s \geqslant 1$; we have for $\mathrm{Re}\, s > 1$

$$\sum_{p\in\overline{P}(e)} p^{-s} = \frac{1}{h}\left(\frac{1}{2}\sum_{\substack{O=O(x)\\ \neq O(x^{-1})}} s^{-1}(O) + \sum_{\substack{O(X)=O(X^{-1})\\ m(O)\neq 2}} s^{-1}(O)\right)\log\frac{1}{s-1} + g_1(s)$$

$$= \frac{v}{h}\log\frac{1}{s-1} + g_1(s)$$

with some $g_1(s)$ regular for $\mathrm{Re}\, s \geqslant 1$, and consequently by (3) and (*) the theorem follows in the case (ii).

4. Now let us consider the case (iii), i. e. we assume that $H = C_2\times\ldots\times C_2 \neq C_2$ and $K \neq 0$. Let $O = (X_1, \ldots, X_N)$ be one of the orbits which have a factorization of the length different from $N/2$. Let $p_i = \mathfrak{p}_1^{(i)}\ldots\mathfrak{p}_N^{(i)}\sim O$ $(i = 1, 2;\ \mathfrak{p}_j^{(i)}\in X_j)$. The number $n = p_1p_2$ has a factorization of the length different from N induced by the factorization of O, the existence of which we assumed, and moreover it has a factorization of the length N:

$$n = \prod_{j=1}^{N}(\mathfrak{p}_j^{(1)}\mathfrak{p}_j^{(2)}).$$

In the same way as in lemma 3 we infer that the number $m = p_1\ldots p_{2k}$ $(p_i\sim O,\ i = 1, 2, \ldots, 2k)$ has at least $k+1$ factorizations of different lengths. Hence from $f(n)\leqslant k$ it will follow that n has at most $2k-1$ prime divisors belonging to the orbit O, and we get $\Omega_P(n) \leqslant K(2k-1)$, where

$$P = \bigcup_{O}\{p: p\sim O\}.$$

and the sum is extended over all such orbits which have a factorization of the length different from $N/2$.

As for $\mathrm{Re}\, s > 1$ we have

$$\sum_{p\in P} p^{-s} = \left(\frac{1}{h}\sum_{i=1}^{k} s(O_i)^{-1}\right)\log\frac{1}{s-1} + g(s) = \frac{Z}{h}\log\frac{1}{s-1} + g(s)$$

with a suitable function $g(s)$ regular for $\mathrm{Re}\, s \geqslant 1$, we can use (*) and the theorem in the case (iii) follows immediately.

5. Finally consider the case $H = C_2 \times \ldots \times C_2 \neq C_2$ and $K = 0$. Now every orbit $\neq O(E)$ has factorizations only of the length $N/2$, i. e. every irreducible factor of every factorization of an orbit must have the length 2. There exist at least two different orbits, because otherwise the only existing orbit $\neq O(E)$, say $(X_1, \ldots, X_N)$ (here the X_i-s are not necessarily distinct, but as $H \neq C_2$ we can arrange them in such way that $X_1 \neq X_2$, and $X_3 = X_1 X_2$), would have a factorization of a length $\neq N/2$. Indeed, $X_1 X_2 X_3 = E$, and obviously $X_1 X_2 X_3$ is irreducible, so if we factorize $X_4 \ldots X_N$ in an arbitrary way, say $(X_4 \ldots X_{i_1}) \ldots (X_{i_j+1} \ldots X_N)$, then the factorization $(X_1 X_2 X_3)(X_4 \ldots X_{i_1}) \ldots (X_{i_j+1} \ldots X_N)$ of the orbit $(X_1, \ldots, X_N)$ will have the length $< N/2$.

Let now $O' = (X_1, \ldots, X_N)$, $O'' = (Y_1, \ldots, Y_N)$ be two different orbits $\neq O(E)$, and let $O = (X_1 Y_1, \ldots, X_N Y_N)$. If

$$p = \prod_{i=1}^{N} \mathfrak{p}_i \sim O' \qquad (\mathfrak{p}_i \in X_i),$$

$$q = \prod_{i=1}^{N} \mathfrak{q}_i \sim O'' \qquad (\mathfrak{q}_i \in Y^i) \qquad \text{and} \qquad r = \prod_{i=1}^{N} \mathfrak{r}_i \sim O \qquad (\mathfrak{r}_i \in X_i Y_i),$$

then the number pqr will have a factorization of the length $3N/2$ induced by the factorizations of the orbits and moreover a factorization of the length N:

$$pqr = \prod_{i=1}^{N} (\mathfrak{p}_i \mathfrak{q}_i \mathfrak{r}_i).$$

Similarly, as in lemma 3, we infer that if $p_i \sim O'$, $q_i \sim O''$ and $r_i \sim O$ $(i = 1, 2, \ldots, k)$, then $f(p_1 q_1 r_1 \ldots p_k q_k r_k) \geqslant 1 + k$, and so, if we define $P' = \{p: p \sim O'\}$, $P'' = \{p: p \sim O''\}$ and $P = \{p: p \sim O\}$, we see that $f(n) \leqslant k$ implies

$$\min\left(\Omega_{P'}(n), \Omega_{P''}(n), \Omega_P(n)\right) \leqslant k-1.$$

Let now O_1 be an arbitrary orbit $\neq O(E)$ and let $O_2, \ldots, O_W$ be the remaining orbits $\neq O(E)$. Let us define $P_i = \{p: p \sim O_i\}$ $(i = 1, 2, \ldots, W)$. The result obtained above tells us that there exists a function β: $(2, \ldots, W) \to (1, 2, \ldots, W)$ such that, for every $i = 2, \ldots, W$, $f(n) \leqslant k$ implies

$$\min\left(\Omega_{P_1}(n), \Omega_{P_i}(n), \Omega_{P_{\beta(i)}}(n)\right) \leqslant k-1.$$

For every sequence $e = (e_2, \ldots, e_W)$, $e_i = \pm 1$, let

$$P^{(e)} = \bigcup_{\substack{2 \leqslant i \leqslant W \\ e_i = +1}} P_i \cup \bigcup_{\substack{2 \leqslant i \leqslant W \\ e_i = -1}} P_{\beta(i)}.$$

To every n with $f(n) \leqslant k$ and $\Omega_{P_1}(n) \geqslant k$ there corresponds such a sequence defined by

$$e_i = \begin{cases} 1 & \text{if} \quad \Omega_{P_i}(n) \leqslant k-1, \\ -1 & \text{if} \quad \Omega_{P_i}(n) > k-1,\ \Omega_{P_{\beta(i)}}(n) \leqslant k-1. \end{cases}$$

Evidently, for this sequence (e), $\Omega_{P(e)}(n) \leqslant (W-1)(k-1)$.

Now for $\mathrm{Re}\, s > 1$ we have by (**)

$$\sum_{p \in P(e)} p^{-s} = \frac{1}{h}\Big(\sum_{\substack{i \\ c_i = +1}} s(O_i)^{-1} + \sum_{\substack{i \\ e_i=-1 \\ e_{\beta(i)}=-1}}^{*} s(O_{\beta(i)})^{-1}\Big) \log \frac{1}{s-1} + g(s)$$

with a suitable $g(s)$ regular for $\mathrm{Re}\, s \geqslant 1$. (Here $\sum^*$ indicates that if for some i-s, say for $i_1, \ldots, i_v$, we have $\beta(i_1) = \ldots = \beta(i_v)$, $e_{i_1} = \ldots = e_{i_v} = -1$, $e_{\beta(i_j)} = -1$ $(j = 1, \ldots, v)$, then we count the corresponding $s(O_{\beta(i_j)})^{-1}$ only once in the sum.)

Now let

$$T_1 = T_1(O_1) = \min_{(e)} \Big\{ \sum_{\substack{i \\ e_i=1}} s(O_i)^{-1} + \sum_{\substack{i \\ e_i=-1 \\ e_{\beta(i)}=-1}}^{*} s(O_{\beta(i)})^{-1} \Big\}.$$

By (*) it follows now that

$$\sum_{\substack{n \leqslant x \\ f(n) \leqslant k \\ \Omega_{P_1}(n) \geqslant k}} 1 \ll x(\log\log x)^{(W-1)(k-1)} (\log x)^{-T_1/h}.$$

If we repeat now the same procedure with O_i instead O_1, we will have

$$\sum_{\substack{n \leqslant x \\ f(n) \leqslant k \\ \Omega_{P_i}(n) \geqslant k}} 1 \ll x(\log\log x)^{(W-1)(K-1)} (\log x)^{-T_i/h},$$

where T_i is defined analogously to T_1 (take O_i instead O_1). If now

$$T = \min(T_1, \ldots, T_W), \tag{4}$$

then

$$\sum_{\substack{n \leqslant x \\ f(n) \leqslant k \\ \Omega_{P_i}(n) \geqslant k}} 1 \ll x(\log\log x)^{(W-1)(k-1)} (\log x)^{-T/h} \qquad (i = 1, \ldots, W).$$

But

$$F_k(x) \ll \sum_{i=1}^{N} \sum_{\substack{n \leqslant x \\ f(n) \leqslant k \\ \Omega_{P_i}(n) \geqslant k}} 1 + \sum_{\substack{n \leqslant x \\ f(n) \leqslant k \\ \Omega_{P_1}(n) \leqslant k-1 \\ \Omega_{P_2}(n) \leqslant k-1 \\ \ldots\ldots\ldots\ldots \\ \Omega_{P_W}(n) \leqslant k-1}} 1,$$

and the second sum is at most equal to

$$\sum_{\substack{n\leqslant x \\ \Omega_P(n)\leqslant(k-1)W}} 1 \ll x(\log\log x)^{W(k-1)}(\log x)^{-(h-1)/hN} \qquad \left(\text{where } P = \bigcup_{i=1}^{N} P_i\right)$$

by (*) and (**).

As $(h-1)/hN \geqslant T/h$, it results

$$F_k(x) \ll x(\log\log x)^{W(k-1)}(\log x)^{-T/h}$$

and so the theorem is proved in the last case.

REFERENCES

[1] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proceedings of the American Mathematical Society 11 (1960), p. 391-392.

[2] H. Delange, *Sur la distribution des entiers ayant certaines propriétés*, Annales Scientifiques de l'École Normale Supérieure 73 (1956), p. 15-74.

[3] E. Fogels, *Zur Arithmetik quadratischer Zahlenkörper*, Wissenschaftliche Abhandlungen der Universität, Riga, Kl. Math., Abt. 1 (1943) p. 23-47.

[4] W. Narkiewicz, *On algebraic number fields with non-unique factorization*, Colloquium Mathematicum 12 (1964), p. 59-67.

INSTITUTE OF MATHEMATCS OF THE WROCŁAW UNIVERSITY
INSTITUTE OF MATHEMATICS OF THE POLISH ACADEMY OF SCIENCES
UNIVERSITY COLLEGE, LONDON

Reçu par la Rédaction le 15. 10. 1964