COLLOQUIUM MATHEMATICUM

VOL. XII 1964 FASC. 1

ON ALGEBRAIC NUMBER FIELDS WITH NON-UNIQUE FACTORIZATION

BY

W. NARKIEWICZ (WROCŁAW)

In [3] E. Fogels proved that in the field $R(i\cdot 5^{1/2})$ almost no rational integer has a unique factorization into irreducible factors. He also proved that almost every integer of this field has a non-unique factorization. His method makes it possible to prove the same for all quadratic fields having only one class of ideals in each genus.

Professor P. Turán proposed me to investigate this problem for other number fields. In this note I generalize the results of Fogels to all normal fields and prove moreover that in such fields for any fixed k almost every rational integer has at least k different factorizations.

In [1] L. Carlitz proved that if the class number of an algebraic number field is at least 3, then one can find integers in K having at least two factorizations of different lengths (i.e. $a = p_1 \dots p_k = r_1 \dots r_m$, where the p_i-s and r_i-s are irreducible and $k \neq m$). We shall prove that if the class number of K is at least 3, then for any fixed k almost every integer in K has factorizations of at least k different lengths.

THEOREM I. *Let K be any finite, algebraic, normal extension of the rationals, of degree n, with the class number $h \neq 1$. Denote by $S_k(x)$ the number of positive rational integers not greater than x, having at most k essentially different factorizations in K. Then $S_k(x) = O\left(x(\log\log x)^{a_k}(\log x)^{-b_k}\right)$, where*

$$a_k = (2hnt_k + t_k - 1)/2(hn + t_k), \qquad b_k = 1/(hn + t_k),$$

$$t_k = (kg-1)[\tfrac{1}{2}(1+\sqrt{8k-7})],$$

and g is the smallest prime number dividing h.

(Here and in the sequel we denote by $[x]$ the integral part of x).

THEOREM II. *Let K be a finite algebraic extension of the rationals with the class number $h \neq 1$. Denote by $T_k(x)$ the number of non-associated integers a in K with $|N(a)| \leqslant x$, having at most k essentially different factorizations in K. Then*

$$T_k(x) = O\left(x(\log\log x)^{c_k}(\log x)^{-d_k}\right),$$

where

$$d_k = 1/(1+h+t_k), \quad c_k = d_k\left(h+t_k\left(h+\frac{t_k+1}{2}\right)\right),$$

$$t_k = (\beta g-1)\left(g\left((k+1)/[g/2]-1\right)\right),$$

β is the least integer such that $(\beta g)!/(\beta!)^g g! > k$ and g is an arbitrarily chosen order of a class in the ideal class group of K.

THEOREM III. *Let K be a finite algebraic extension of the rationals with class number $h \neq 1, 2$. Denote by $U_k(x)$ the number of non-associated integers in K with $|N(a)| \leqslant x$, having factorizations of at most k different lengths. Then*

$$U_k(x) = O\left(x(\log\log x)^{e_k}(\log x)^{-f_k}\right),$$

where

$$e_k = (gk-1)\left(h+\frac{kg}{2}-1\right)\Big/(h+kg-1), \quad f_k = 1/(h+kg-1)$$

and g is the smallest order $\neq 2$ of a class in the ideal class group of K, if it exists, and $g = 2$ if $X^2 = E$ for all X in the ideal class group of K.

THEOREM IV. *Let K be a quadratic extension of the rationals with the class number $h \neq 1, 2$. Denote by $V_k(x)$ the number of rational positive integers not greater than x, having factorizations in K of at most k different lengths. Then*

$$V_k(x) = O\left(x(\log\log x)^{r_k}(\log x)^{-s_k}\right)$$

where

$$s_k = 1/(2h+kg-1), \quad r_k = s_k(kg-1)(kg+4h-1),$$

g being the smallest order $\neq 2$ of a class in the ideal class group of K, if it exists, and $g = 1$ in the other case.

We shall use the following results:

(i) For every ideal class X and for $\operatorname{Re} s > 1$ we have $\sum N(\mathfrak{p})^{-s} = h^{-1}\log\left(1/(s-1)\right)+G(s)$, where the summation is taken over all prime ideals (or over all prime ideals of the first degree) in X and $G(s)$ is regular for $\operatorname{Re} s \geqslant 1$ (see e.g. [4], p. 33).

(ii) If a_n is a sequence of non-negative real numbers, $f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ is convergent for $\operatorname{Re} s > 1$, and, for some $P \neq 0, -1, -2, \ldots$, $f(s) = g_1(s)(s-1)^{-P}+g_2(s)$ for $\operatorname{Re} s > 1$, where $g_1(s), g_2(s)$ are regular for $\operatorname{Re} s \geqslant 1$ and, moreover, $g_1(1) \neq 0$, then

$$\sum_{n\leqslant x} a_n = \frac{g_1(1)}{\Gamma(P)}x(\log x)^{P-1}+o\left(x(\log x)^{P-1}\right)$$

for $x \to \infty$ (see [2]).

LEMMA 1. *If* $A_j(x)$ $(j = 0, 1, \ldots)$ *is a sequence of real functions, satisfying the conditions*:

(a) $A_{j+1}(x) = O\big(\sum_{p \leqslant x} A_j(x/p)\big)$,

(b) $A_j(x) = O(x)$,

(c) $A_0(x) = O\big(x(\log x)^{-\beta}\big)$, $\beta > 0$,

then

$$A_j(x) = O\big(x(\log\log x)^{k_j}(\log x)^{-m_j}\big),$$

where $k_j = j\big(1+\beta(j-1)/2\big)/(1+j\beta)$, $m_j = \beta/(1+j\beta)$ *for* $j = 1, 2, \ldots$ *(the constants in* $O(\ldots)$ *depend on* j*).*

Proof. It suffices to prove that from

$$A_j(x) = O\big(x(\log\log x)^{\alpha}(\log x)^{-\gamma}\big) \qquad (\gamma > 0)$$

it follows

$$A_{j+1}(x) = O\big(x(\log\log x)^{(1+\alpha)/(1+\gamma)}\big)(\log x)^{-\gamma/(1+\gamma)}.$$

Put

$$\varepsilon(x) = (\log\log x)^{(1+\alpha)/(1+\gamma)}(\log x)^{-\gamma/(1+\gamma)}.$$

Then for sufficiently large x one has $1/2 > \varepsilon > 1/\log x$. Now

$$\sum_{p \leqslant x} A_j(x/p) = \sum_{1 \leqslant x/p < x^{\varepsilon}} A_j(x/p) + \sum_{x^{\varepsilon} \leqslant x/p \leqslant x} A_j(x/p) = S_1 + S_2,$$

$$S_1 = O\Big(x \sum_{x^{1-\varepsilon} < p \leqslant x} p^{-1}\Big) = O\big(x(\log\log x - \log(1-\varepsilon) - \log\log x\big) +$$

$$+ O(x/\log x) = O(\varepsilon x)$$

and

$$S_2 = O\Big(x(\log\log x)^{\alpha}\varepsilon(x)^{-\gamma}(\log x)^{-\gamma} \sum_{p \leqslant x^{1-\varepsilon}} p^{-1}\Big)$$

$$= O\big(x(\log\log x)^{1+\alpha}\varepsilon(x)^{-\gamma}(\log x)^{-\gamma}\big) = O(\varepsilon x),$$

whence

$$A_{j+1}(x) = O(S_1 + S_2) = O(\varepsilon x), \qquad \text{q.e.d.}$$

Proof of Theorem I. Let X be an ideal class with $X^g = E$, $X \neq E$. Let P be the set of all rational primes which are norms of prime ideals from X, and which are not ramified in K. Moreover, let $\omega_P(m)$ be the number of different prime factors of m belonging to the set P and $\Omega_P(m)$ the number of prime factors of m belonging to the set P, each counted according to its multiplicity. Finally, let $F(m)$ be the number of different factorizations of m into irreducible factors in K. For abbreviation, let us put $r = 1 + [(1/2)(1+\sqrt{8k-7})]$.

LEMMA 2. *If* $F(m) \leqslant k$, *then* $\Omega_P(m) \leqslant (kg-1)(r-1) = t_k$.

Proof. Let $p_1, \ldots, p_r$ be different primes from the set P. Then $p_i = \mathfrak{p}_i \mathfrak{q}_i$, where $\mathfrak{p}_i$ are prime ideals from X with $N\mathfrak{p}_i = p_i$ and $\mathfrak{q}_i$ are ideals from X^{-1} $(i = 1, 2, \ldots, r)$.

At first we shall prove that the number $p_1 \ldots p_r$ has at least $1 + (1+2+\ldots+(r-1)) > k$ different factorizations. Since $\mathfrak{p}_i \in X$ and $\mathfrak{q}_j \in X^{-1}$, we have $\mathfrak{p}_i \mathfrak{q}_j \in E$ for each pair i, j. Consider the factorizations $D_{i,j}$ arising from

$$p_1 \ldots p_r = (\mathfrak{p}_i \mathfrak{q}_j)(\mathfrak{p}_j \mathfrak{q}_i) p_1 \ldots p_{i-1} p_{i+1} \ldots p_{j-1} p_{j+1} \ldots p_r \qquad (1 \leqslant i < j \leqslant r)$$

by factorization of the terms inside brackets and of the p_k-s $(k \neq i, j)$ into irreducible elements. It suffices to prove that the factorizations $D_{i,j}$ are all different. Let us fix i and j $(i < j)$. Choose an ideal $\mathfrak{r} = \mathfrak{r}(i, j)$ in X^{-1} such that $\mathfrak{r}$ divides $\mathfrak{q}_j$ and no proper divisor of $\mathfrak{r}$ belongs to X^{-1}. Such a choice is always possible. Obviously, $\mathfrak{p}_i \mathfrak{r} \in E$ and $\mathfrak{r} \notin E$. We assert that $\mathfrak{p}_i \mathfrak{r}$ has no proper divisors from E. Indeed, if $\mathfrak{p}_i \mathfrak{r} = \mathfrak{a}\mathfrak{b}$ $(\mathfrak{a}, \mathfrak{b} \in E)$, then $\mathfrak{p}_i$ divides $\mathfrak{a}$ or $\mathfrak{b}$, say $\mathfrak{p}_i$ divides $\mathfrak{a}$, thus with some $\mathfrak{c} \in X^{-1}$ one has $\mathfrak{a} = \mathfrak{p}_i \mathfrak{c}$, whence $\mathfrak{p}_i \mathfrak{r} = \mathfrak{p}_i \mathfrak{c}\mathfrak{b}$ and $\mathfrak{r} = \mathfrak{c}\mathfrak{b}$. From the choice of $\mathfrak{r}$ it follows $\mathfrak{r} = \mathfrak{b} \in E$, whereas $\mathfrak{r} \in X^{-1} \neq E$, and so we get a contradiction. Consequently, $\mathfrak{p}_i \mathfrak{r}(i, j)$ is irreducible.

We see thus that in the factorization $D_{i,j}$ there must appear an irreducible factor $\mathfrak{p}_i \mathfrak{r}(i, j)$, where $\mathfrak{r} \in X^{-1}$, $\mathfrak{r}$ divides $\mathfrak{q}_j$, and no proper divisor of $\mathfrak{r}$ has both these properties. Suppose now that for some i, j, i_1, j_1 $(i \neq i_1$, or $j \neq j_1)$ the factorizations $D_{i,j}$ and D_{i_1,j_1} coincide. Then a factor $\alpha = \mathfrak{p}_i \mathfrak{r}(i, j)$ must occur in the factorization D_{i_1,j_1}. It cannot occur in factorizations of $p_1, \ldots, p_r$ for from $\mathfrak{p}_i \mid p_i$ it would follow $\mathfrak{p}_i \mathfrak{r}(i, j) = \alpha \mid p_i = \mathfrak{p}_i \mathfrak{q}_i$, whence $\mathfrak{r}(i, j) \mid \mathfrak{q}_i$, and simultaneously $\mathfrak{r}(i, j) \mid \mathfrak{q}_j$, which is impossible, since two different rational primes p_i and p_j cannot have an ideal divisor $\neq (1)$ in common. Consequently, α must occur in the factorization of $\mathfrak{p}_{i_1} \mathfrak{q}_{j_1}$ or in the factorization of $\mathfrak{p}_{j_1} \mathfrak{q}_{i_1}$. Suppose that α divides $\mathfrak{p}_{i_1} \mathfrak{q}_{j_1}$ (the second case is analogous). Then $\mathfrak{p}_i \mid \mathfrak{p}_{i_1} \mathfrak{q}_{j_1}$ and we must distinguish between two cases, $i \neq i_1$ and $i = i_1$.

1. $i \neq i_1$. In this case $\mathfrak{p}_i \mid \mathfrak{q}_{j_1} \mid p_{j_1}$, whence it must be $i = j_1$, and thus $\mathfrak{p}_{j_1}^2 \mid \mathfrak{p}_{j_1} \mathfrak{q}_{j_1} = p_{j_1}$, which is impossible, because p_{j_1} is not ramified.

2. $i = i_1$. In this case $j \neq j_1$ and $r(i, j)$ divides both $\mathfrak{q}_j$ and $\mathfrak{q}_{j_1}$, which is impossible.

Since the factorizations $D_{i,j}$ are all different, the number $p_1 \ldots p_r$ has at least $k+1$ different factorizations.

Taking into account that $F(ab) \geqslant \max\big(F(a), F(b)\big)$ we see that from $F(m) \leqslant k$ it follows $\omega_P(m) \leqslant r-1$. Remark now that the number

$p^{\beta\sigma}$ ($p \in P$, $p = \mathfrak{p}\mathfrak{q}$, $\mathfrak{p} \in X$, $N\mathfrak{P} = p$) has at least $\beta+1$ different factorizations arising from

$$p^{\beta\sigma} = (\mathfrak{p}^{\sigma})^{j}(\mathfrak{q}^{\sigma})^{j}(\mathfrak{p}\mathfrak{q})^{\sigma(\beta-j)} \qquad (j = 0, 1, \ldots, \beta)$$

in the same way as above. Consequently, from $F(m) \leqslant k$ follows $\Omega_P(m) \leqslant (kg-1)(r-1)$, q.e.d.

Let R be the set of all prime numbers which are not norms of prime ideals of the field K. The notation $\sum_{p \in S}^{*}$ will be used for sums ranging over all prime ideals of the first degree, belonging to a set S. If S is the set of all prime ideals of K, we shall write Σ^{*}. Moreover, by $g(s)$ we shall denote (may be different) functions regular for $\mathrm{Re}\, s \geqslant 1$.

As

$$n \sum_{p \notin R} p^{-s} = \sum^{*} N(\mathfrak{p})^{-s} = \log\big(1/(s-1)\big) + g(s),$$

$$\sum_{p} p^{-s} = \log\big(1/(s-1)\big) + g(s),$$

we have

$$\sum_{p \in R} p^{-s} = \frac{n-1}{n} \log\big((1/s-1)\big) + g(s) \qquad \text{for} \qquad \mathrm{Re}\, s > 1.$$

Let Y be the set of all prime ideals of the first degree which do not belong to X, but which are conjugated with a prime ideal in X.

Let us define for p in P, $f(p)$ as the number of prime ideals dividing p, which are not in X, and put $f(p) = 0$ for all other primes.

Moreover, let

$$\varepsilon(p) = \begin{cases} 0 & \text{for} \quad p \in P, \\ 1 & \text{for} \quad p \notin P. \end{cases}$$

Then we have

$$n \sum_{\substack{p \notin P \\ p \notin R}} p^{-s} = \sum_{\substack{\mathfrak{p} \notin X \\ \mathfrak{p} \notin Y}}^{*} N(\mathfrak{p})^{-s} = \sum_{\mathfrak{p} \notin X}^{*} N(\mathfrak{p})^{-s} - \sum_{\mathfrak{p} \in Y}^{*} N(\mathfrak{p})^{-s}$$

$$= \left(1 - \frac{1}{h}\right) \log\big(1/(s-1)\big) + g(s) - \sum_{p} \frac{f(p)}{p^{s}}$$

and so

$$\sum_{p \notin P} p^{-s} = \sum_{\substack{p \notin P \\ p \notin R}} p^{-s} + \sum_{p \in R} p^{-s} = \left(1 - \frac{1}{hn}\right) \log\big(1/(s-1)\big) + g(s) - \frac{1}{n} \sum_{p} f(p) p^{-s}$$

hence finally, if we put $f_1(p) = \varepsilon(p) + f(p)/n$ we shall have

$$\sum_{p} f_1(p) p^{-s} = \left(1 - \frac{1}{hn}\right) \log\big(1/(s-1)\big) + g(s). \tag{1}$$

Now define for $N = p_1^{a_1}\dots p_k^{a_k}$, $f_1(N) = f_1(p_1)\dots f_1(p_k)$. Then

$$\sum_{N=1}^{\infty} f_1(N)N^{-s} = \prod_p \left(1+f_1(p)p^{-s}+\dots\right) = \exp\left(\sum_p f_1(p)p^{-s}+g(s)\right)$$
$$= g(s)(s-1)^{1/hn-1}+g_1(s) \quad \text{for} \quad \operatorname{Re} s > 1.$$

Since obviously $f_1(N) = 1$ if $\Omega_p(N) = 0$ and $f_1(N)$ is non-negative, we obtain by (ii)

$$\sum_{\substack{N\leqslant x\\ \Omega_p(N)=0}} 1 \leqslant \sum_{N\leqslant x} f_1(N) = O\left(x(\log x)^{-1/hn}\right).$$

Since by lemma 2

$$S_k(x) \leqslant Q_0(x)+\dots+Q_{t_k}(x), \quad \text{where} \quad Q_i(x) = \sum_{\substack{N\leqslant x\\ \Omega_p(N)=1}} 1 \tag{2}$$

and obviously

$$Q_i(x) = \sum_{\substack{p\leqslant x\\ p\in P}} Q_{i-1}(x/p) \leqslant \sum_{p\leqslant x} Q_{i-1}(x/p), \tag{3}$$

one has but to apply Lemma 1 to achieve the proof.

Proof of Theorem II. Let X be an ideal class of order g ($X \neq E$). Let Z be the set of all prime ideals from X, and D the set of all ideals having no prime factor from Z. For an integral a in K, let $F(a)$ be the number of different factorizations of a into irreducible elements, for any ideal $\mathfrak{a}$ let $\omega_Z(\mathfrak{a})$ be the number of different prime ideals from Z dividing $\mathfrak{a}$, and $\Omega_Z(\mathfrak{a})$ the number of all prime ideals from Z dividing $\mathfrak{a}$, each counted according to its multiplicity.

Lemma 3. *If $F(a) \leqslant k$, then a has the form: $a = \mathfrak{p}^m\mathfrak{a}$, where $\mathfrak{p}\in Z$, m is a non-negative integer and $\Omega_Z(\mathfrak{a}) \leqslant t_k$ (t_k is defined in the statement of Theorem II).*

(Here and in the sequel we need not distinguish the number a, and the principal ideal generated by a.)

Proof. If $a = \mathfrak{p}_1\dots\mathfrak{p}_{jg}$ ($\mathfrak{p}_i\in Z$, all $\mathfrak{p}_i$ — different), then a has at least $(jg)!/(j!)^g g!$ factorizations:

$$a = (\mathfrak{p}_{i_1}\dots\mathfrak{p}_{i_g})\dots(\mathfrak{p}_{i_{jg-g+1}}\dots\mathfrak{p}_{i_{gj}}),$$

hence from $F(a) \leqslant k$ it follows $\omega_Z(a) \leqslant \beta g-1$.

If $a = \mathfrak{p}_1^{g\lambda_1}\mathfrak{p}_2^{g\lambda_2}$ ($\mathfrak{p}_1, \mathfrak{p}_2\in Z$), then a has at least $[g/2]\left(\min(\lambda_1, \lambda_2)+1\right)$ factorizations arising from

$$a = (\mathfrak{p}_1^g)^{\lambda_1-j}(\mathfrak{p}_2^g)^{\lambda_2-j}(\mathfrak{p}_1^i\mathfrak{p}_2^{g-i})^j(\mathfrak{p}_1^{g-i}\mathfrak{p}_2^i)^j$$

($i = 1, 2, \dots, [g/2]$; $j = 0, 1, \dots, \min(\lambda_1, \lambda_2)$).

Thus, if $F(a) \leqslant k$, then there can exist at most one prime ideal $\mathfrak{p} \in Z$ such that $\mathfrak{p}^m \mid a$ with some $m > g\big((k+1)/[g/2]-1\big)-1$ and, consequently, a has the required form.

Let now $G(m)$ be the number of ideals from D with the norm m. For $\operatorname{Re} s > 1$ we have

$$\sum_{m=1}^{\infty} G(m)m^{-s} = \sum_{\mathfrak{a} \in D} N(\mathfrak{a})^{-s} = \prod_{\mathfrak{p} \notin Z} \big(1+N(\mathfrak{p})^{-s}+\ldots\big)$$

$$= \exp\Big(\sum_{\mathfrak{p} \notin Z} N(\mathfrak{p})^{-s}+g(s)\Big) = g(s)(s-1)^{1/n-1}+g_1(s)$$

and by (ii)

$$\sum_{m \leqslant x} G(m) = O\big(x(\log x)^{-1/h}\big). \tag{4}$$

Let $R_j(x)$ be the number of ideals with norm not greater than x, for which $\Omega_Z(a) = j$. Let $T(x) = \sum_{j=0}^{t_k} R_j(x)$. Then

$$T_k(x) \leqslant T(x)+\sum_{\mathfrak{p} \in X,\, N(\mathfrak{p}^m) \leqslant x} T\big(x/N(\mathfrak{p}^m)\big). \tag{5}$$

Observe that

$$R_{j+1}(x) \leqslant \sum_{N(\mathfrak{p}) \leqslant x} R_j\big(x/N(\mathfrak{p})\big) \leqslant n \sum_{p \leqslant x} R_j(x/p).$$

From the last inequality, (4) and lemma 1 it follows that

$$T(x) = O\big(x(\log\log x)^{\varrho}(\log x)^{-\sigma}\big), \tag{6}$$

where

$$\varrho = t_k\big(h+\tfrac{1}{2}(t_k-1)\big)/(h+t_k), \qquad \sigma = 1/(h+t_k).$$

Finally

$$\sum_{\mathfrak{p} \in X,\, N(\mathfrak{p}^m) \leqslant x} T\big(x/N(\mathfrak{p}^m)\big) \leqslant \sum_{N(\mathfrak{p}^m) \leqslant x} T\big(x/N(\mathfrak{p}^m)\big)$$

$$\leqslant \sum_{p^m \leqslant x} \sum_{N(\mathfrak{p})=p} T(x/p^m) \leqslant n \sum_{p^m \leqslant x} T(x/p^m).$$

Let $\eta(x) = (\log\log x)^{(\varrho+1)/(\sigma+1)}(\log x)^{-\sigma/(\sigma+1)}$. Then

$$\sum_{p^m \leqslant x} T(x/p^m) = \sum_{1 \leqslant x/p^m \leqslant x^{\eta}} T(x/p^m)+\sum_{x^{\eta} < x/p^m \leqslant x} T(x/p^m).$$

Proceeding similarly as in lemma 1 and taking into account that

$$\sum_{p^m \leqslant x} p^{-m} = \log\log x+A+O(1/\log x)$$

we obtain $\sum_{p^m \leqslant x} T(x/p^m) = O(\eta x)$, which together with (5) and (6) proves Theorem II.

Proof of Theorem III. First case. There exists an ideal class X, such that $X^2 \neq E$.

Let $X^g = E$, $g > 2$, and, for $g' < g$, $X^{g'} \neq E$. Denote by P_1, P_2 the sets of all prime ideals of the first degree in X and in X^{-1} respectively, and by $\Omega_i(a)$ $(i = 1, 2)$ the number of prime ideals of P_i which divide a, each counted according to its multiplicity. Finally let $H(a)$ be the number of factorizations of a into irreducible factors with different lengths. At first let us remark that if $a = \mathfrak{p}_1 \dots \mathfrak{p}_{rg} \mathfrak{q}_1 \dots \mathfrak{q}_{rg}$ $(\mathfrak{p}_i \in P_1,\ \mathfrak{q}_i \in P_2)$, then $H(a) \geqslant 1 + r$ in view of the following decompositions:

$$a = \prod_{i=1}^{\lambda g} (\mathfrak{p}_i \mathfrak{q}_i) \prod_{j=\lambda}^{r-1} (\mathfrak{p}_{jg+1} \dots \mathfrak{p}_{jg+g}) \prod_{j=\lambda}^{r-1} (\mathfrak{q}_{jg+1} \dots \mathfrak{q}_{jg+g}), \qquad \lambda = 1, 2, \dots, r-1,$$

$$a = \prod_{j=0}^{r-1} (\mathfrak{p}_{jg+1} \dots \mathfrak{p}_{jg+g}) \prod_{j=0}^{r-1} (\mathfrak{q}_{jg+1} \dots \mathfrak{q}_{jg+g}),$$

$$a = \prod_{i=1}^{rg} (\mathfrak{p}_i \mathfrak{q}_i).$$

Since $H(ab) \geqslant \max\big(H(a), H(b)\big)$, we immediately conclude that if $H(a) \leqslant k$, then a is of the following form:

$$a = \mathfrak{p}_1 \dots \mathfrak{p}_j \mathfrak{P}_1' \quad \text{or} \quad a = \mathfrak{q}_1 \dots \mathfrak{q}_j \mathfrak{P}_2' \qquad (j \leqslant kg - 1), \tag{7}$$

where $\mathfrak{p}_i \in P_1$, $\mathfrak{q}_i \in P_2$, and $\mathfrak{P}_i'$ has no divisor from P_i $(i = 1, 2)$. Now

$$\sum_{\mathfrak{P}_i'} N(\mathfrak{P}_i')^{-s} = \prod_{\mathfrak{p} \notin P_i} \big(1 + N(\mathfrak{p})^{-s} + \dots\big)$$

$$= \exp\Big(\sum_{\mathfrak{p} \notin P_i} N(\mathfrak{p})^{-s} + g(s)\Big) = \frac{g(s)}{(s-1)^{1-1/h}} + g_1(s),$$

whence by (ii)

$$\sum_{N(\mathfrak{P}_i') \leqslant x} 1 = O\big(x(\log x)^{-1/h}\big) \qquad (i = 1, 2). \tag{8}$$

Let

$$B_j^{(i)}(x) = \sum_{N(\mathfrak{a}) \in x,\ \Omega_i(\mathfrak{a}) = j} 1 \qquad (i = 1, 2).$$

Then by (7)

$$U_k(x) \leqslant \sum_{j=0}^{kg-1} B_j^{(1)}(x) + \sum_{j=0}^{kg-1} B_j^{(2)}(x). \tag{9}$$

From

$$B_{j+1}^{(i)}(x) \leqslant \sum_{N(\mathfrak{p}) \leqslant x} B_j^{(i)}\big(x/N(\mathfrak{p})\big) \leqslant n \sum_{p \leqslant x} B_j^{(i)}(x/p),$$

and by (8), (9) and lemma 1 the theorem follows in the first case.

Second case. For every ideal class X, $X^2 = E$.

Let $X_i^2 = E$ $(i = 1, 2, 3)$, $X_1X_2 = X_3$, $X_1, X_2, X_3 \neq E$. Let P_i be the set of all prime ideals of the first degree from X_i. Define $\Omega_i(x)$ and $H(a)$ as in the previous case. Remark that if $H(a) \leqslant k$, then $\min_i\big(\Omega_i(a)\big) < 2k$. Indeed, for the number

$$b = \mathfrak{p}_1 \dots \mathfrak{p}_{2k} \mathfrak{q}_1 \dots \mathfrak{q}_{2k} \mathfrak{r}_1 \dots \mathfrak{r}_{2k} \qquad (\mathfrak{p}_i \in P_1,\ \mathfrak{q}_i \in P_2,\ \mathfrak{r}_i \in P_3)$$

one has $H(b) \geqslant k+1$ in view of the following decompositions:

$$(10)\quad \begin{cases} b = \prod_{i=1}^{\mu} (\mathfrak{p}_i \mathfrak{q}_i \mathfrak{r}_i) \prod_{i=1}^{\mu} (\mathfrak{p}_{k+i} \mathfrak{q}_{k+i} \mathfrak{r}_{k+i}) \prod_{j=1+\mu}^{k} (\mathfrak{p}_j \mathfrak{p}_{k+j})(\mathfrak{q}_j \mathfrak{q}_{k+j})(\mathfrak{r}_j \mathfrak{r}_{k+j}) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\mu = 1, 2, \dots, k-1), \\ b = \prod_{i=1}^{2k} (\mathfrak{p}_i \mathfrak{q}_i \mathfrak{r}_i), \\ b = \prod_{i=1}^{k} (\mathfrak{p}_j \mathfrak{p}_{k+j})(\mathfrak{q}_j \mathfrak{q}_{k+j})(\mathfrak{r}_j \mathfrak{r}_{k+j}), \end{cases}$$

and it remains to observe that $H(ab) \geqslant \max\big(H(a), H(b)\big)$.

It follows that every a with $H(a) \leqslant k$ is of the following form:

$$a = \mathfrak{p}_1 \dots \mathfrak{p}_j \mathfrak{P}_1' \quad \text{or} \quad a = \mathfrak{q}_1 \dots \mathfrak{q}_j \mathfrak{P}_2' \quad \text{or} \quad a = \mathfrak{r}_1 \dots \mathfrak{r}_j \mathfrak{P}_3',$$

where $0 \leqslant j \leqslant 2k-1$, $\mathfrak{p}_i \in P_1$, $\mathfrak{q}_i \in P_2$, $\mathfrak{r}_i \in P_3$ and $\mathfrak{P}_i'$ are ideals with no factor from P_i. The proof of the theorem can now be completed in the same way as in the previous case.

Proof of theorem IV. First case. There exists an ideal class X such that $X^2 \neq E$.

Let $X^g = E$, and $X^{g'} \neq E$, for $g' < g$. Let P be the set of all rational primes which are norms of prime ideals from X, $\Omega_P(m)$ — the number of primes from P dividing m, each counted according to its multiplicity, and $H(m)$ — the number of factorizations of the number m into irreducible factors in K of different lengths.

Let $p_1, \dots, p_{kg} \in P$. Then $p_i = \mathfrak{p}_i \mathfrak{q}_i$ $(\mathfrak{p}_i \in X,\ \mathfrak{q}_i \in X^{-1},\ \mathfrak{p}_i, \mathfrak{q}_i$ are prime ideals). For $m = p_1 \dots p_{kg}$ one has $H(m) \geqslant k+1$ in the same way as in the first case of Theorem III. It follows that if $H(m) \leqslant k$, then $\Omega_P(m) \leqslant kg-1$. By an argument analogous to the proof of Theorem I our theorem follows in this case.

Second case. For every ideal class X one has $X^2 = E$.

Choose $X_i \neq E$ $(i = 1, 2, 3)$ such that $X_1X_2 = X_3$. Let P_i be the set of all rational primes which are norms of prime ideals from X_i, $\Omega_i(m)$ — the number of primes from P_i dividing m, each counted according to

its multiplicity, and $H(m)$ — the number of factorizations of the number m into irreducible factors in K of different lengths. Let $p_i = \mathfrak{p}_i\mathfrak{p}_i' \in P_1$, $q_i = \mathfrak{q}_i\mathfrak{q}_i' \in P_2$, $r_i = \mathfrak{r}_i\mathfrak{r}_i' \in P_3$ $(i = 1, 2, \ldots, k)$. Then for the number $m = p_1 \ldots p_k q_1 \ldots q_k r_1 \ldots r_k$ one has $H(m) \geqslant k+1$ in the same way as in (10). Thus from $H(m) \leqslant k$ it follows that $\min \Omega_i(m) \leqslant k-1$. The theorem follows now by an argument analogous to the proof of Theorem I.

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 le théorème tauberien de Ikehara*, Comptes Rendus de l'Académie des Sciences, Paris, 232 (1951), p. 465-467.

[3] E. Fogels, *Zur Arithmetik quadratischer Zahlenkörper*, Ученые записки университета, Математика, Рига, 2 (1943), p. 23-46.

[4] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I, Jahresberichte der Deutschen Mathematiker-Vereinigung 35 (1926), p. 1-55.

MATHEMATICAL INSTITUTE OF THE WROCŁAW UNIVERSITY
MATHEMATICAL INSTITUTE OF THE POLISH ACADEMY OF SCIENCES

Reçu par la Rédaction le 26. 2. 1963