COLLOQUIUM MATHEMATICUM

VOL. XLVI 1982 FASC. 1

REMARKS ON FACTORIZATIONS IN ALGEBRAIC NUMBER FIELDS

BY

JAN ŚLIWA (WROCŁAW)

1. In this note we investigate some problems connected with factorizations in algebraic number fields, which were stated in [1] and [3].

Let K denote an algebraic number field, R_K its ring of integers, H the class group, and h the class number of K. By G_m we denote the set of all elements of R_K with factorizations of m distinct lengths and by G'_m the set of all positive rational integers contained in G_m. The number of non-associated integers a in G_m with $|N(a)| \leqslant x$ will be denoted by $G_m(x)$ and, similarly, the number of positive integers less than or equal to x lying in G'_m by $G'_m(x)$. If X is an element of H and $a \in R_K$, then $\Omega_X(a)$ will denote the number of prime ideal divisors of aR_K lying in the class X and counted according to their multiplicities. By $\mathfrak{p}$, $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ we always mean prime ideals. Finally, if k and N are positive integers, then C_k will denote the cyclic group of k elements and C_k^N the product of N copies of C_k.

2. It is well known that $G_m = G'_m = \emptyset$ if $h \leqslant 2$ and $m \geqslant 2$. In [3] it was shown that for $h \geqslant 3$ either $G_m = \emptyset$ or

$$G_m(x) \sim C(m, K)x(\log\log x)^{B(m,H)}(\log x)^{-A(m,H)},$$

where $C(m, K)$, $A(m, H)$ are positive and $B(m, H)$ non-negative.

A similar result was obtained also for G'_m and $G'_m(x)$.

Now we prove that for the set G_m the first alternative never occurs.

THEOREM 1. *If $h \geqslant 3$, then $G_m \neq \emptyset$ for $m = 1, 2, \ldots$*

Proof. For any subset U of H we denote by $R(U)$ the set of those integers in R_K which generate ideals not divisible by prime ideals of classes belonging to $H \setminus U$.

If H contains an element X of order $t \geqslant 3$, we take $U = \{X, X^{-1}\}$ and we will show that $R(U)$ contains elements with any prescribed number of distinct lengths of factorizations.

Let m be a positive integer. Choose $a \in R(U)$ such that

$$\Omega_X(a) = \Omega_{X^{-1}}(a) = t(m-1).$$

Let

$$a = d_1 d_2 \dots d_r \tag{1}$$

be a factorization of a into irreducibles.

From the definition of $R(U)$ it follows that each irreducible factor appearing in (1) generates an ideal of one of the following types:

1. $\mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1 \in X$, $\mathfrak{p}_2 \in X^{-1}$;
2. $\mathfrak{p}_1 \dots \mathfrak{p}_t$, $\mathfrak{p}_i \in X$;
3. $\mathfrak{p}_1 \dots \mathfrak{p}_t$, $\mathfrak{p}_i \in X^{-1}$.

Let u_i $(1 \leqslant i \leqslant 3)$ denote the number of d_j's in (1) which correspond to the i-th type. Then

$$u_1 + tu_2 = u_1 + tu_3 = t(m-1), \tag{2}$$

and the length of factorization (1) equals

$$r = u_1 + u_2 + u_3 = \frac{1}{t}\big(2t(m-1) + (t-2)u_1\big).$$

Hence this number is equal to the number of non-negative values of u_1 for which (2) has a non-negative solution u_2, u_3. Obviously, the last can happen only for $u_1 \in \{0, t, 2t, \dots, (m-1)t\}$. This proves that $a \in G_m$.

If H contains only elements of order 2 and $h \geqslant 3$, then we take $U = \{X, Y, XY\}$, where X, Y are distinct non-unit elements of H. If $a \in R(U)$ with

$$\Omega_X(a) = \Omega_Y(a) = \Omega_{XY}(a) = 2(m-1)$$

has factorization (1), then only the following types of irreducibles can occur:

1. $\mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1, \mathfrak{p}_2 \in X$;
2. $\mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1, \mathfrak{p}_2 \in Y$;
3. $\mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1, \mathfrak{p}_2 \in XY$;
4. $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{p}_1 \in X$, $\mathfrak{p}_2 \in Y$, $\mathfrak{p}_3 \in XY$.

Let u_i $(1 \leqslant i \leqslant 4)$ be the number of d_j's in (1) of the i-th type. We get a system of equations

$$2u_1 + u_4 = 2u_2 + u_4 = 2u_3 + u_4 = 2(m-1),$$
$$r = u_1 + u_2 + u_3 + u_4 = 3(m-1) - \tfrac{1}{2}u_4,$$

and we infer easily that the set of admissible values for u_4 is $\{0, 2, \dots, 2(m-1)\}$, so $a \in G_m$.

For the set G'_m we can prove a similar result only in the quadratic case.

THEOREM 2. *If K is a quadratic number field and $h \geqslant 3$, then $G'_m \neq \emptyset$ for $m = 1, 2, \ldots$*

Proof. If H contains an element X of order $t \geqslant 3$ and $\mathfrak{p} \in X$, then $N(\mathfrak{p}) = \mathfrak{p}\mathfrak{p}_1$, where $\mathfrak{p}_1$ is a prime ideal in X^{-1}. Thus the rational integer $n = (N(\mathfrak{p}))^{t(m-1)}$ belongs to $R(\{X, X^{-1}\})$, $\Omega_X(n) = \Omega_{X^{-1}}(n) = t(m-1)$, and as in the proof of Theorem 1 we get $n \in G'_m$.

If $H = C_2^k$, $k \geqslant 2$, $X \neq Y$ are non-unit elements, and $\mathfrak{p}_1 \in X$, $\mathfrak{p}_2 \in Y$, $\mathfrak{p}_3 \in XY$, then $n = (N(\mathfrak{p}_1)N(\mathfrak{p}_2)N(\mathfrak{p}_3))^{m-1}$ is contained in $R(\{X, Y, XY\})$, $\Omega_X(n) = \Omega_Y(n) = \Omega_{XY}(n) = 2(m-1)$. Consequently, as in the proof of Theorem 1 we obtain $n \in G'_m$.

3. In [3] it was noted that in the case $H = C_3$ we have

$$A(m, H) = \tfrac{1}{3}, \qquad B(m, H) = 3m-1.$$

In the same way it can be proved that

$$A(m, C_2^2) = \tfrac{1}{4}, \qquad B(m, C_2^2) = 2m-1$$

and

$$A(m, C_4) = \tfrac{1}{4}, \qquad B(m, C_4) = 2m-1.$$

A direct computation of those constants for other groups is rather complicated as the number of minimal equalities in H increases very quickly with h. But, nevertheless, we state the following

CONJECTURE (**P 1247**). One has

$$A(m, H) = A(1, H) = 1 - \frac{t(H)}{h} \qquad \text{and} \qquad B(m, H) = A(H)m + B(H),$$

where $A(H)$, $B(H)$ are rational integers, and $t(H)$ is a combinatorial constant which was defined in [3] (This constant will be discussed later on.)

4. Let G be a finite abelian group. If $g_1, \ldots, g_k \in G$ and

$$g_1^{n_1} \ldots g_k^{n_k} = 1, \tag{3}$$

then this equality will be called *minimal* if

1° $n_i \geqslant 0$ for $1 \leqslant i \leqslant k$ and $(n_1, \ldots, n_k) \neq (0, \ldots, 0)$;

2° if $0 \leqslant m_i \leqslant n_i$ $(1 \leqslant i \leqslant k)$ and $g_1^{m_1} \ldots g_k^{m_k} = 1$, then either all m_i's are zero or $m_i = n_i$ for $i = 1, \ldots, k$.

We say (as in [1]-[3]) that the minimal equality (3) satisfies *condition* (C) if

$$\sum_{i=1}^{k} \frac{n_i}{\operatorname{ord} g_i} = 1.$$

A subset U of G is said to have *property* (C) (in such a case we write $U \in (C)$) if every minimal equality of the form (3) with $g_1, \ldots, g_k \in U$ satisfies condition (C).

By $t(G)$ we denote the maximal cardinality of a set $U \in (C)$.

Property (C) is closely connected with factorizational properties of integers in K; namely, if U is a subset of class group of K, then $R(U) \subset G_1$ if and only if $U \in (C)$.

In [3] it was shown that

$$t(C_{p^n}) = n+1 \quad \text{and} \quad t(C_p^n) \leqslant \binom{n+p-2}{p-1} + 1.$$

To investigate further the values of $t(G)$ we consider a weaker property of minimal equalities than (C); namely, we say that the minimal equality (3) satisfies *condition* (C_0) if

$$\sum_{i=1}^{k} \frac{n_i}{\operatorname{ord} g_i} \in Z.$$

Similarly as before we define property (C_0) of subsets of G and the corresponding constant $t_0(G)$. Obviously,

$$t(G) \leqslant t_0(G). \tag{4}$$

Let m be the exponent of G and f a homomorphism of G to $m^{-1}Z/Z$. Put

$$G_f = \left\{ g \in G\colon f(g) = \frac{1}{\operatorname{ord} g} \right\}.$$

LEMMA 1. *A subset U of G has property* (C_0) *if and only if there exists* $f \in \operatorname{Hom}(G, m^{-1}Z/Z)$ *such that* $U \subset G_f$.

Proof. Let $U = \{g_1, \ldots, g_k\} \in (C_0)$ and let $f\colon U \to m^{-1}Z/Z$ be defined by

$$f(g_i) = \frac{1}{\operatorname{ord} g_i}.$$

Obviously, f can be extended to a homomorphism of G if and only if $g_1^{s_1} \ldots g_k^{s_k} = 1$ implies

$$\sum_{i=1}^{k} \frac{s_i}{\operatorname{ord} g_i} \in Z.$$

But there exist integers $w_1, \ldots, w_k$ such that the equality

$$g_1^{w_1 \operatorname{ord} g_1 + s_1} \ldots g_k^{w_k \operatorname{ord} g_k + s_k} = 1$$

has positive exponents, and so is a product of minimal equalities. Therefore

$$\sum_{i=1}^{k} \frac{w_i \operatorname{ord} g_i + s_i}{\operatorname{ord} g_i} \in Z.$$

The converse is trivial as each G_f has property (C_0).

Now let $G = C_{n_1} \oplus \ldots \oplus C_{n_k}$ with $n_1 | \ldots | n_k = m$ and let X_i denote a generator of C_{n_i}.

LEMMA 2. *If $A = (a_1, \ldots, a_k)$ is a k-tuple with $0 \leqslant a_i < n_i$ and*

$$U_A = \left\{ X_1^{b_1} \ldots X_k^{b_k} : \sum_{i=1}^{k} \frac{a_i b_i}{n_i} \equiv \min_{1 \leqslant i \leqslant k} \frac{(b_i, a_i)}{n_i} \pmod 1 \right\},$$

then $U_A \in (C_0)$. Conversely, for each U with property (C_0) there exists a k-tuple A such that $U \subset U_A$.

Proof. Observe that each $f \in \operatorname{Hom}(G, m^{-1}Z/Z)$ is uniquely determined by a k-tuple $(a_1, \ldots, a_k)$, $0 \leqslant a_i < n_i$, and $f(X_i) = a_i/n_i$. But

$$\operatorname{ord}(X_1^{b_1} \ldots X_k^{b_k}) = \max_{1 \leqslant i \leqslant k} \left\{ \frac{n_i}{(n_i, b_i)} \right\},$$

and comparing this with Lemma 1 we get our assertion.

COROLLARY. *$t_0(C_n) = d(n)$ (the number of divisors of n) and $t_0(C_n^2) = n+1$.*

THEOREM 3. *$d(n) \geqslant t(C_n) \geqslant \Omega(n)+1$, where $\Omega(n)$ denotes the number of prime divisors of n counted according to their multiplicities.*

Proof. The left-hand inequality follows from (4) and the Corollary.

Let $d_1, \ldots, d_k$ be a set of divisors of n with $d_1 | \ldots | d_k$, and g a generator of C_n. We shall show that the set $\{g^{d_1}, \ldots, g^{d_k}\}$ has property (C).

If $(g^{d_1})^{n_1} \ldots (g^{d_k})^{n_k} = 1$ with positive integers $n_1, \ldots, n_k$, then $n | n_1 d_1 + \ldots + n_k d_k$, and this implies that for some $n_1, \ldots, n_k$

(5)

$$n_1 = \frac{d_2}{d_1} n_1', \quad n_{s-1}' + n_s = \frac{d_{s+1}}{d_s} n_s' \ (2 \leqslant s \leqslant k-1), \quad n_{k-1}' + n_k = \frac{n}{d_k} n_k'.$$

Indeed, if $n | n_1 d_1 + \ldots + n_k d_k$, then

$$\frac{n}{d_1} \Big| n_1 + n_2 \frac{d_2}{d_1} + \ldots + n_k \frac{d_k}{d_1},$$

and as

$$\frac{d_2}{d_1} \Big| \frac{n}{d_1}, \quad \frac{d_2}{d_1} \Big| \frac{d_s}{d_1} \ (s = 2, \ldots, k),$$

there exists n_1' such that

$$n_1 = \frac{d_2}{d_1} n_1' \quad \text{and} \quad \frac{n}{d_2} \Big| (n_1' + n_2) + n_3 \frac{d_3}{d_2} + \ldots + n_k \frac{d_k}{d_2}.$$

Continuing this process we obtain (5).

Further

$$\sum_{i=1}^{k} \frac{n_i}{\operatorname{ord} g^{d_i}} = \frac{1}{n} \sum_{i=1}^{k} n_i d_i = n_k'.$$

Taking $m_k' = 1$ we can determine $0 \leqslant m_k \leqslant n_k$ and $m_{k-1}' \geqslant 0$ such that

$$m_{k-1}' + m_k = \frac{n}{d_k} m_k' = \frac{n}{d_k}.$$

Proceeding further in this way we obtain $0 \leqslant m_i \leqslant n_i$ $(0 \leqslant i \leqslant k)$, not all equal to zero, and non-negative integers $m_1', \ldots, m_k'$ such that equations (5) are satisfied if we replace n_i, n_i' by m_i, m_i'. Thus

$$(g^{d_1})^{m_1} \ldots (g^{d_k})^{m_k} = 1 \quad \text{and} \quad \sum_{i=1}^{k} \frac{m_i}{\operatorname{ord} g^{d_i}} = 1;$$

hence our set has property (C).

Remark. As can be seen from Lemma 2 the set $\{g^d\}_{d|n}$ has property (C_0). For some n it has also property (C). But as the following example of a minimal equality in C_{60} shows:

$$(g^5)^1 (g^6)^1 (g^{12})^2 (g^{15})^1 (g^{20})^2 (g^{30})^1 = 1,$$

it does not always have property (C).

5. Now let $G = C_p^N$. We may treat this group as a linear space over $\mathrm{GF}(p)$. Let $u_1, \ldots, u_N$ be a basis of this space and let A be the set of elements of the form

$$\sum_{k=1}^{N} (p - a_k) u_k, \quad 1 \leqslant a_k \leqslant p,$$

with

$$\sum_{a_k \neq p} a_k = p - 1.$$

Narkiewicz ([1], P 1143) has asked whether this set has property (C). If the answer were affirmative, then

$$t(C_p^N) = \binom{N+p-2}{p-1} + 1.$$

Obviously, this is the case for $p = 2$ and all N.

THEOREM 4. *If $p \geqslant 3$, then $A \in (C)$ if and only if $N \leqslant 2$.*

Proof. Let $p \geqslant 3$ and $N \geqslant 3$. We shall determine a subset of A which does not have property (C). Let $v_1 = (p-1)u_2 + 2u_3$, $v_2 = u_2$, $v_3 = (p-1)u_1 + 2u_3$, $v_4 = u_1$. Obviously, $v_1, v_2, v_3, v_4 \in A$ and

$$(p-1)v_1 + (p-1)v_2 + v_3 + v_4 = 0. \tag{6}$$

If there existed d_1, d_2, d_3, d_4 such that $0 \leqslant d_1 \leqslant p-1$, $0 \leqslant d_2 \leqslant p-1$, $0 \leqslant d_3 \leqslant 1$, $0 \leqslant d_4 \leqslant 1$ and $d_1v_1 + d_2v_2 + d_3v_3 + d_4v_4 = 0$, then we would have

$$(d_2 - d_1)u_2 + 2d_1u_3 = \begin{cases} (p-2)u_3 & \text{if } d_3 = d_4 = 1, \\ (p-1)u_1 & \text{if } d_3 = 0, d_4 = 1, \\ u_1 + (p-2)u_3 & \text{if } d_3 = 1, d_4 = 0, \\ 0 & \text{if } d_3 = d_4 = 0. \end{cases}$$

This can take place only for $d_1 = d_2 = p-1$, $d_3 = d_4 = 1$ or $d_1 = d_2 = d_3 = d_4 = 0$, and hence equality (6) is minimal but certainly does not satisfy (C).

If $N = 2$, then the set A can be written in the form

$$\{w_k = kv_1 + v_2 \colon k = 0, 1, \ldots, p-1\}, \quad \text{where } v_1 = u_2 - u_1,\ v_2 = u_2.$$

If for non-negative $d_0, d_1, \ldots, d_{p-1} \in Z$

$$d_0w_0 + \ldots + d_{p-1}w_{p-1} = 0, \tag{7}$$

then

$$\sum_{k=0}^{p-1} kd_k \equiv 0 \pmod{p} \quad \text{and} \quad \sum_{k=0}^{p-1} d_k \equiv 0 \pmod{p}. \tag{8}$$

If equality (7) does not satisfy (C), then by (8) we have

$$\sum_{k=0}^{p-1} d_k \geqslant 2p.$$

We shall prove a lemma, a very special case of which we shall need, but as it seems interesting, we state it in full generality.

Let $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_m)$ be elements of Z^m. We write $x \leqslant y$ if $x_i \leqslant y_i$ for $i = 1, \ldots, m$. Let $L_1, \ldots, L_k$ denote linear forms on Z^m with integer coefficients. By $D(G)$ we denote the Davenport constant of the group G, e.g. the least integer r such that from any r elements of G one can extract a subsequence with unit product.

LEMMA 3. *If $n_1, \ldots, n_k$ are positive integers and $x = (x_1, \ldots, x_m) \in Z^m$ is such that $\sum x_i \geqslant D(C_{n_1} \oplus \ldots \oplus C_{n_k})$, $x > (0, \ldots, 0)$, then there exists $z \in Z^m$, $(0, \ldots, 0) < z \leqslant x$, for which $L_i(z) \equiv 0 \pmod{n_i}$, $i = 1, \ldots, k$.*

Proof. For $i = 1, \ldots, m$ we put

$$e_i = (0, \ldots, 1, \ldots, 0), \quad f_i = \big(L_1(e_1), \ldots, L_k(e_i)\big).$$

Let us consider the system $f_1, \ldots, f_m$ (where each f_i occurs x_i times, $i = 1, \ldots, m$) of elements of $C_{n_1} \oplus \ldots \oplus C_{n_k}$. As this system has $\sum x_i \geqslant D(C_{n_1} \oplus \ldots \oplus C_{n_k})$ elements, there are t_i, $0 \leqslant t_i \leqslant x_i$ $(1 \leqslant i \leqslant n)$, not all equal to zero, such that $t_1 f_1 + \ldots + t_m f_m = 0$. Hence

$$\big(L_1(t_1, \ldots, t_m), \ldots, L_k(t_1, \ldots, t_m)\big) = 0$$

and this is the assertion of Lemma 3.

In our case we take $k = 2$, $n_1 = n_2 = p-1$, and

$$L_1(x_0, \ldots, x_{p-1}) = \sum_{i=0}^{p-1} i x_i, \qquad L_2(x_0, \ldots, x_{p-1}) = \sum_{i=0}^{p-2} x_i.$$

As $d_{i_0} > 0$ for some i_0, and $\sum d_j - 1 \geqslant 2p-1 = D(C_p^2)$, we can take $x = (d_0, \ldots, d_{i_0} - 1, \ldots, d_{p-1})$ and apply Lemma 3. The existence of $z \in Z^p$ with $(0, \ldots, 0) < z \leqslant x$ and $L_1(z) \equiv L_2(z) \equiv 0 \pmod p$ implies that equality (7) is not minimal.

REFERENCES

[1] W. Narkiewicz, *Finite abelian groups and factorization problems*, Colloquium Mathematicum 42 (1979), p. 319-330.

[2] L. Skula, *On c-semigroups*, Acta Arithmetica 31 (1976), p. 247-257.

[3] J. Śliwa, *Factorizations of distinct lengths in algebraic number fields*, ibidem 31 (1976), p. 399-417.

Reçu par la Rédaction le 28. 2. 1979