COLLOQUIUM MATHEMATICUM

VOL. XLVI 1982 FASC. 1

FINITE ABELIAN GROUPS AND FACTORIZATION PROBLEMS. II

BY

W. NARKIEWICZ AND J. ŚLIWA (WROCŁAW)

0. In [2] several combinatorial constants associated with finite abelian groups were defined. All of them were connected with factorization properties in algebraic number fields, arising as exponents of $\log x$ and $\log\log x$ in various asymptotic formulas. We pursue now this topic and consider the constant $a_1(A)$ which was defined as the maximal length of a complex with a strongly unique factorization in a finite abelian group A. We obtain a simpler equivalent definition of it, improve the upper bound obtained in [2], and compute the exact value for it in certain cases.

1. For convenience we repeat the needed definitions concerning $a_1(A)$. Let A be a finite abelian group written additively. A sequence $b = \{a_1, \ldots, a_k\}$ of its nonzero elements is called a *block* provided $a_1 + \ldots + a_k = 0$. We identify two blocks which differ only in the ordering. We define multiplication of two blocks by juxtaposition and call a block *irreducible* if it cannot be written as a product of two blocks. Clearly, a block is irreducible if and only if none of its proper subsums vanishes. By a *factorization* of b we shall understand any surjective map

$$\varphi\colon \{1, \ldots, k\} \to \{1, \ldots, t\}$$

with a certain positive $t = t(\varphi)$ such that for $j = 1, \ldots, t$ the sequences $b_j = \{a_i\colon \varphi(i) = j\}$ are blocks. If they all are irreducible, we speak about an *irreducible factorization* of b. Obviously, we have $b = b_1 \ldots b_t$. Two such factorizations φ and ψ are called *strongly equivalent* if $t(\varphi) = t(\psi)$ $(= t$, say) and for a suitable permutation σ the sets $\{i\colon \varphi(i) = j\}$ and $\{i\colon \psi(i) = \sigma(j)\}$ coincide for $j = 1, \ldots, t$. A block is said to have a *strongly unique factorization* if all its irreducible factorizations are strongly equivalent.

The reason for introducing these notions is explained by the following result proved in [2]:

PROPOSITION 1 ([2], Proposition 7). *Let a be an integer in an algebraic number field K not divisible by a square of a nonprincipal prime ideal and without principal prime ideal factors. Then a has a unique factorization in K if and only if the block in the class group H of K formed by the ideal classes containing the prime ideal factors of a (taken with multiplicities) has a strongly unique factorization.*

It follows that $a_1(H)$ gives an upper bound for the number of nonprincipal prime ideals dividing an integer with unique factorization generating a squarefree ideal. Now we prove that here the square-freeness is in fact irrelevant.

THEOREM. *Let a be an integer of K with unique factorization and let H be the class group of K. The principal ideal generated by a can be divisible by at most $a_1(H)$ distinct nonprincipal prime ideals and this bound can be attained.*

Proof. Write

$$a = p_1^{\alpha_1} \dots p_s^{\alpha_s} I,$$

where $p_1, \dots, p_s$ are distinct nonprincipal prime ideals and I is a product of principal prime ideals. Obviously, it suffices to consider the case $I = 1$.

Let $p_1^{\alpha_1}, \dots, p_r^{\alpha_r}$ be principal, $p_{r+1}^{\alpha_{r+1}}, \dots, p_s^{\alpha_s}$ nonprincipal, and let $g_i \in H$ be the class containing p_i (for $i = 1, \dots, r$), respectively $p_i^{\alpha_i}$ (for $i = r+1, \dots, s$).

For each $i = 1, \dots, s$ choose a prime ideal q_i from g_i and for $i = 1, \dots, r$ choose a prime ideal q_i' from g_i^{-1} so that all obtained prime ideals are different. This choice assures the principality of the ideal

$$J = q_1 \dots q_s q_1' \dots q_r'.$$

Let b be any generator of J. We claim that b has a unique factorization in K. Since J is squarefree, Proposition 1 will imply

$$s \leqslant s + r \leqslant a_1(H).$$

Denote by m_i the order of g_i ($i = 1, \dots, r$), let π_i be a generator (clearly irreducible) of the principal ideal $p_i^{m_i}$, and let $A_i = \alpha_i / m_i$. Then the number

$$a' = \pi_1^{A_1} \dots \pi_r^{A_r}$$

has a unique factorization, being a divisor of a. Hence the elements $g_1, \dots, g_r$ generate independent subgroups. Indeed, if $\prod_{i=1}^{r} g_i^{t_i} = 1$ with $0 \leqslant t_i \leqslant m_i$ ($i = 1, \dots, r$) and for at least one i we had $t_i \neq 0, m_i$, then the ideal $\prod_{i=1}^{r} p_i^{t_i}$ would be principal and any of its generators would be a divisor of a' not of the form $\prod_{i=1}^{r} \pi_i^{B_i}$ ($0 \leqslant B_i \leqslant A_i$, $i = 1, \dots, r$). It is also clear

that no nonunit product of elements $g_{r+1}, \ldots, g_s$ can lie in the group generated by $g_1, \ldots, g_r$. This shows that b cannot have another factorization into irreducibles than that induced by

$$J = (q_1 q_1') \ldots (q_r q_r') \ldots$$

To show that the bound is obtained it is enough to apply Proposition 1.

2. Now we show that it is possible to give a simpler definition of $a_1(A)$. To do this, denote by $S(b)$ for a block $b = (a_1, \ldots, a_m)$ the set of all possible sums $a_{i_1} + \ldots + a_{i_j}$ $(1 \leqslant i_1 < \ldots < i_j \leqslant m)$.

PROPOSITION 2. *Let $b = \{a_1, \ldots, a_k\} = b_1 \ldots b_r$ and let the blocks $b_1, \ldots, b_r$ be irreducible. Then the block b has a strongly unique factorization if and only if for all disjoint subsets X, Y of $\{1, \ldots, r\}$ we have*

$$S\Big(\prod_{i \in X} b_i\Big) \cap S\Big(\prod_{i \in Y} b_i\Big) = \{0\}. \tag{1}$$

Proof. The "only if" part of this proposition is contained in Lemma 1 of [3], so let us assume that condition (1) is satisfied. If $r = 1$, then the implication holds, as b is irreducible; so we may assume that $r \geqslant 2$ and the implication holds for all smaller values of r. Define $\varphi = \{1, \ldots, k\} \to \{1, \ldots, r\}$ by $\varphi(i) = j$ if $a_i \in b_j$. Let $\psi = \{1, \ldots, k\} \to \{1, \ldots, s\}$ be another irreducible factorization of b. We have to show that it is strongly equivalent to φ. (We may assume that $s \geqslant 2$, as otherwise b would be irreducible.) Put

$$A_i(\varphi) = \{j\colon \varphi(j) = i\} \quad \text{and} \quad A_i(\psi) = \{j\colon \psi(j) = i\}.$$

If $A_i(\varphi) = A_{i'}(\psi)$ for some i, i', then the block $b_1 \ldots b_{i-1} b_{i+1} \ldots b_r$ would satisfy (1) and have two strongly inequivalent factorizations, contrary to our choice of r. Thus, in particular, we must have $A_1(\psi) \neq A_\nu(\varphi)$, $1 \leqslant \nu \leqslant r$, and, of course, $A_1(\psi) \subset A_i(\psi)$ (for some i) is also excluded. Thus we may find $j_1 \neq j_2$ and $k_1 \neq k_2$ such that

$$\varphi(k_1) = j_1, \quad \varphi(k_2) = j_2, \quad \psi(k_1) = \psi(k_2) = 1;$$

hence the sets $B = A_{j_1}(\varphi) \cap A_1(\psi)$ and $C = A_1(\psi) \setminus B$ are both nonempty.

As

$$\sum_{r \in B} a_r + \sum_{r \in C} a_r = \sum_{r \in A_1(\psi)} a_r = 0,$$

we have

$$0 \neq \xi = \sum_{r \in B} a_r \in S(b_{j_1})$$

and

$$-\xi = \sum_{r\in C} a_r \in S(b_1 \dots b_{j_1-1}\, b_{j_1+1} \dots b_r) = T,$$

but T is closed under inverses, whence finally

$$\xi \in S(b_{j_1}) \cap T = \{0\},$$

a contradiction.

Observe that in Proposition 2 we can replace condition (1) by the following:

$$S(b_i) \cap S(b_1 \dots b_{i-1} b_{i+1} \dots b_r) = \{0\} \qquad (i = 1, \dots, r). \tag{2}$$

In fact, assume that (2) holds and we have the equality

$$a_{i_1} + \dots + a_{i_k} = a_{j_1} + \dots + a_{j_l} \neq 0 \tag{3}$$

with

$$a_{i_m} \in \prod_{i\in A} b_i, \qquad a_{j_n} \in \prod_{i\in B} b_i \qquad (m = 1, \dots, k;\ n = 1, \dots, l)$$

for A, B disjoint.

We may assume that no subsum of the left-hand side of (3) vanishes, as in that case we could remove it. Not all of the elements $a_{i_1}, \dots, a_{i_k}$ can lie in the same irreducible block, so we may assume that $a_{i_1}, \dots, a_{i_p} \in b_1$, whereas $a_{i_{p+1}}, \dots, a_{i_k} \notin b_1$. Then

$$0 \neq a_{i_1} + \dots + a_{i_p} = a_{j_1} + \dots + a_{j_l} - (a_{i_{p+1}} + \dots + a_{i_k}) \in S(b_1) \cap S(b_2 \dots b_r).$$

3. In [2] it was shown (Proposition 8) that $a_1(A)$ does not exceed the cardinality of A. Without much trouble one can show that $a_1(A) = |A|$ holds if and only if either A is cyclic or $A \simeq C_2^2$. Now we shall give another upper bound for this constant, involving the constant of Davenport, and this will enable us to compute $a_1(A)$ for groups C_2^n and C_3^n.

Denote by $D(A)$ the *Davenport constant* of A, i.e. the smallest integer n with the property that from each sequence of n elements of A one can extract a subsequence with vanishing sum. Olson [3] proved that if A is a p-group and

$$A = \bigoplus_{i=1}^{m} C_{p^{h_i}},$$

then

$$D(A) = 1 + \sum_{i=1}^{m} (p^{h_i} - 1).$$

The analogue fails for arbitrary abelian groups (cf. [1]).

PROPOSITION 3. *For all finite abelian groups A we have*

$$a_1(A) \leqslant 2\big(D(A)-1\big).$$

Moreover, if b is a block in A with strongly unique factorization, $b = b_1 \dots b_r$ (b_i — irreducible), then b can contain at most $D(A)+r-1$ elements.

Proof. Delete one element from each block b_i. The sequence obtained cannot have a subsequence with vanishing sum because of Proposition 2. Thus it contains at most $D(A)-1$ elements. As we delete r elements, the second part of our proposition holds. To obtain the first part it suffices to note that the deleted elements also form a sequence without a subsequence with vanishing sum.

COROLLARY 1. $a_1(C_2^n) = 2n$.

Proof. By Olson's result, $D(C_2^n) = 1+n$, and $a_1(C_2^n) \geqslant 2n$ by Proposition 9 of [2].

COROLLARY 2. $a_1(C_3^n) = 3n$.

Proof. Regard C_3^n as an n-dimensional space over GF(3). If $b = b_1 \dots b_r$ is a block with strongly unique factorization and we take one element from b_i, then the obtained set is linearly independent in view of Proposition 2. Thus r cannot exceed n, and as $D(C_3^n) = 1+2n$, we obtain $a_1(A) \leqslant 3n$. The converse inequality follows from Proposition 9 of [2].

It can be also seen that if q is a prime power, then $a_1(C_q^N)$ cannot exceed $2N(q-1)$, but the lower bound in this case is Nq and there remains a gap to be closed.

The following proposition describes the behaviour of $a_1(A)$ under homomorphisms.

PROPOSITION 4. *If $0 \to H \to G \xrightarrow{f} A \to 0$ is an exact sequence of finite abelian groups, then*

$$a_1(G) \geqslant a_1(A) + a_1(H).$$

Proof. Let $b = b_1 \dots b_s$ be a block with strongly unique factorization in A with $a_1(A)$ elements, and let $c = c_1 \dots c_t$ be such a block in H. If $b_i = \{x_1, \dots, x_m\}$, then we can select elements $y_1, \dots, y_m$ in G with

$$\sum_{i=1}^{m} y_i = 0 \quad \text{and} \quad f(y_i) = x_i.$$

Write $B = \{y_1, \dots, y_m\}$ and consider the block $B = B_1 \dots B_{t+s}$, where for $i = s+1, \dots, t+s$ we have $B_i = C_{s+i}$ in G. We claim that it has a strongly unique factorization. Indeed, the blocks B_i are obviously irreducible, and if for a nonempty set $A \subset \{1, \dots, s+t\}$ the intersection

$$S\Big(\prod_{i \in A} B_i\Big) \cap S\Big(\prod_{i \notin A} B_i\Big)$$

contains a nonzero element a, say

$$a = \sum_{j=1}^{M} \xi_j - \sum_{j=1}^{N} \eta_j = \sum_{j=1}^{P} \hat{\xi}_j + \sum_{j=1}^{Q} \eta_j, \tag{4}$$

where

$$\xi_j \in \prod_{\substack{i \in A \\ i \leqslant s}} B_i, \quad \hat{\xi}_j \in \prod_{\substack{i \notin A \\ i \leqslant s}} B_i, \quad \eta_j \in \prod_{\substack{i \in A \\ i > s}} B_i, \quad \hat{\eta}_j \in \prod_{\substack{i \notin A \\ i > s}} B_i,$$

then

$$f(a) = \sum_{j=1}^{M} f(\xi_j) = \sum_{j=1}^{P} f(\hat{\xi}_j) \in S\Big(\prod_{i \in A} b_i\Big) \cap S\Big(\prod_{\substack{i \notin A \\ i \leqslant s}} b_i\Big) = \{0\}.$$

Thus

$$\{f(\xi_1), \ldots, f(\xi_M)\} = b_{i_1} \ldots b_{i_k}, \quad \{f(\hat{\xi}_1), \ldots, f(\hat{\xi}_p)\} = b_{j_1} \ldots b_{j_l}$$

with suitable $i_1, \ldots, i_k, j_1, \ldots, j_l$, showing that

$$\{\xi_1, \ldots, \xi_M\} = B_{i_1} \ldots B_{i_k}, \quad \{\hat{\xi}_1, \ldots, \hat{\xi}_p\} = B_{j_1} \ldots B_{j_l},$$

and

$$\sum_{j=1}^{M} \xi_j = 0 = \sum_{j=1}^{P} \hat{\xi}_j.$$

Now (4) gives

$$a = \sum_{j=1}^{N} \eta_j = \sum_{j=1}^{P} \eta_j \in S\Big(\prod_{i \in A} c_{i-s}\Big) \cap S\Big(\prod_{\substack{i \in A \\ i > s}} c_{i-s}\Big) = \{0\},$$

leading finally to $a = 0$.

The next propositions are useful for computing $a_1(G)$ for given groups.

PROPOSITION 5. *If $b = b_1 \ldots b_r$ is a block with strongly unique factorization in G, $1 \leqslant t \leqslant r$, and there is a subgroup H of G such that $S(b_{t+1} \ldots b_r) \cap H = \{0\}$, then*

$$|b_{t+1} \ldots b_r| \leqslant a_1(G/H).$$

Proof. Let f be the canonical map of G onto G/H and consider the block $b' = f(b_{1+t}) \ldots f(b_r)$ induced in G/H by f. Observe first that the blocks $f(b_i)$ are for $i = 1+t, \ldots, r$ irreducible. In fact, if $b_i = \{g_1, \ldots, g_s\}$ and if $f(g_{i_1}) + \ldots + f(g_{i_k}) = 0$, then $g_{i_1} + \ldots + g_{i_k}$ lies in $S(b_{t+1} \ldots b_r) \cap H = \{0\}$, thus $\{i_1, \ldots, i_k\} = \{1, \ldots, s\}$.

To show that b' has a strongly unique factorization assume that there is a nonempty proper subset $A \subset \{1+t, 2+t, \ldots, r\}$ such that the inter-

section

$$S\Big(\prod_{i\in A} f(b_i)\Big)\cap S\Big(\prod_{\substack{i\geqslant t+1\\ i\notin A}} f(b_i)\Big)$$

contains an element a. Then we can write

$$a=\sum_{u=1}^{k} f(g_{i_u})=\sum_{v=1}^{l} f(h_{i_v})$$

with

$$\{g_{i_1},\dots,g_{i_k}\}\in\prod_{i\in A} b_i,\qquad \{h_{i_1},\dots,h_{i_l}\}\in\prod_{\substack{i\geqslant t+1\\ i\notin A}} b_i.$$

As all sets $S(B)$ are closed under inverses, the element

$$\sum_{u=1}^{k} g_{i_u}-\sum_{v=1}^{l} h_{i_v}$$

belongs to $S(b_{t+1}\dots b_r)\cap H=\{0\}$, i.e.

$$\sum_{u=1}^{k} g_{i_u}=\sum_{v=1}^{l} h_{i_v}\in S\Big(\prod_{i\in A} b_i\Big)\cap S\Big(\prod_{\substack{i\geqslant 1+t\\ i\notin A}} b_i\Big)=\{0\},$$

and we have $a=0$. The proposition results now immediately.

PROPOSITION 6. *Let $b=b_1\dots b_r$ be a block with strongly unique factorization in a group of N elements and let s_i for $i=1,\dots,r$ be the number of elements in the irreducible factor b_i of b. Then $s_1\dots s_r\leqslant N$.*

Proof. Observe that if $b_i=\{a_{i1},\dots,a_{is_i}\}$ $(i=1,\dots,r)$, then all $s_1\dots s_r$ sums

$$\sum_{i=1}^{r}\sum_{j=1}^{t_i} a_{ij}\qquad (1\leqslant t_i\leqslant s_i)$$

are distinct.

COROLLARY 1. *For all abelian groups A of order N we have*

$$a_1(A)\leqslant D(A)+\frac{\log N}{\log 2}-1.$$

Proof. Note that $2^r\leqslant s_1\dots s_r\leqslant N$ holds by Proposition 6 for all blocks with strongly unique factorization and apply Proposition 3.

COROLLARY 2. *If A is an abelian group of order N and m is the maximal order of an element in A, then*

$$a_1(A)\leqslant m\left(1+\frac{\log N}{\log m}\right)+\frac{\log N}{\log 2}-1.$$

Proof. In [1] it was proved that

$$D(A) \leqslant m\left(1+\frac{\log N}{\log m}\right);$$

hence it suffices to apply the preceding corollary.

Using the above propositions one can without trouble compute the value of $a_1(A)$ for small groups. The results lead to the conjecture that if

$$A = \bigoplus_{i=1}^{N} C_{n_i} \qquad (n_1 | n_2 | \ldots | n_N),$$

then $a_1(A) = n_1 + \ldots + n_N$. It was observed in [2] that the inequality $a_1(A) \geqslant n_1 + \ldots + n_N$ always holds, but the converse inequality was proved only in particular cases. The corollaries to Proposition 3 show that the conjecture is true for $A = C_2^N$ and C_3^N, and using Proposition 6 one can also establish it for $A = C_2^N \oplus C_4$ and $C_2^N \oplus C_4^2$. This can be done in the following way: if $b = b_1 \ldots b_r$ is a block with strongly unique factorization in $A = C_2^N \oplus C_4^2$ having more than $2N+9$ elements, and s_i denotes the number of elements in the block b_i, then from $s_i \geqslant 2$ and $s_1 \ldots s_r \leqslant 2^{N+4}$ we infer that $r \leqslant N+4$. On the other hand, $D(A) = N+7$ and Proposition 3 shows that $2N+9 \leqslant N+6+r$, whence $r \geqslant N+3$. Thus, finally, either $r = N+3$ or $r = N+4$. In the second case all s_i's have to be equal to 2, so b contains $2N+8$ elements, and in the first case we can notice that all solutions of $s_1 \ldots s_{N-3} \leqslant 2^{N+4}$ with $s_i \geqslant 2$ satisfy $s_1 + \ldots + s_{N-3} \leqslant 2N+8$.

REFERENCES

[1] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups, III*, Reports of the Mathematisch Centrum Amsterdam, ZW 1969-008.

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

[3] J. E. Olson, *A combinatorial problem on finite abelian groups*, Journal of Number Theory 1 (1969), p. 8-10.

Reçu par la Rédaction le 28. 10. 1979