COLLOQUIUM MATHEMATICUM

XLII DÉDIÉ À LA MÉMOIRE D'EDWARD MARCZEWSKI 1979

FINITE ABELIAN GROUPS AND FACTORIZATION PROBLEMS

BY

W. NARKIEWICZ (WROCŁAW)

0. In this paper we formulate several open questions of combinatorial nature which concern finite abelian groups and which arose with investigations of various factorization properties in algebraic number fields.

Let K be an algebraic number field with the classnumber h and classgroup H. Denote by R its ring of integers and let, for $k = 1, 2, \ldots,$ F_k be the set of all elements of R which have at most k distinct factorizations into irreducibles. Similarly, let G_k be the set of all elements of R which have at most k such factorizations of distinct length. It is well known that $F_1 = R$ holds only in the case $h = 1$, and $G_1 = R$ holds if and only if h is either 1 or 2. Suitably defined counting functions of the sets F_k and G_k, as well as of $F_k \cap Z$ and $G_k \cap Z$, were studied in [1], [3]-[7], [8] (ch. IX), [9] and [12], and it turned out that asymptotically they behave like

$$Cx\frac{\log\log^M x}{\log^a x},$$

where C is positive, and a and M are nonnegative constants depending on K, in most cases having a combinatorial interpretation. It is the aim of this paper to point out some purely combinatorial problems arising here.

1. For most arithmetical problems, quoted above, the field K itself is irrelevant and only the structure of its classgroup is of importance. We now give a general scheme which permits a translation of those problems into the language of group theory and thus leads to a study of factorization properties via abelian groups.

Let G be an arbitrary abelian group of h elements. We shall consider finite systems $\langle g_1, \ldots, g_n\rangle$ of nonzero elements of G, i.e. sequences in which the order is disregarded. Such a system will be called a *block* if $g_1 + \ldots + g_n = 0$, and n will be called its *length*. We denote by $B(G)$ the set of all blocks. Note that it has a natural semigroup structure with juxtaposition as multiplication.

A block is called *irreducible* if it cannot be written as a product of two blocks. It is clear that many notions connected with factorization in R, such as unique factorization, the length of a factorization etc., have their counterparts in $B(H)$.

For any group G let $a(G)$ be the maximal length of an irreducible block. It is, clearly, the least integer a with the property that if $g_1, g_2, \ldots, g_{1+a}$ is an arbitrary sequence of nonzero elements of G with vanishing sum, then one can select a subsequence of at most a elements also with vanishing sum. Recall that the constant of Davenport, $D(G)$, is defined as the least integer b such that from any b elements of G one can extract a subsequence with zero sum. Thus, clearly, $a(G) \leqslant D(G)$. However, as noted by Davenport, both constants are equal.

PROPOSITION 1. *For all abelian groups*, $a(G) = D(G)$.

Proof. Assume $a(G) < D(G)$ and let $g_1, \ldots, g_a$ ($a = a(G)$) be a sequence without a subsequence with vanishing sum. Let $h = -g_1 - g_2 - \ldots - g_a$ and consider the sequence $g_1, \ldots, g_a, h$. By the definition of $a(G)$, it must have a subsequence of at most a elements whose sum vanishes. It must be of the form $g_{i_1}, \ldots, g_{i_r}, h$, thus $g_{i_1} + \ldots + g_{i_r} + h = 0$, and hence

$$\sum_{k \neq i_1, \ldots, i_r} g_k = 0,$$

contrary to our assumption.

COROLLARY (H. Davenport). *The maximal number of nonprincipal prime ideal factors of an irreducible element of R equals $D(H)$.*

Note (cf. theorem 9.6 of [8]) that this corollary implies that the number of nonassociated irreducible elements of R with absolute value of norm bounded by x is asymptotically equal to

$$C(K)x \frac{(\log\log x)^{D(H)-1}}{\log x}$$

with a positive $C(K)$.

PROBLEM I. Evaluate $D(G)$. (**P 1141**)

This problem was proposed first by Davenport and its solution is known for all p-groups and groups which are direct sums of at most two cyclic groups ([10] and [2]). In those cases, if

$$G = \bigoplus_{i=1}^{t} C_{d_i} \quad (d_1 | d_2 | \ldots | d_t),$$

then

$$D(G) = 1 + \sum_{i=1}^{t} (d_i - 1).$$

It was conjectured that this equality holds for all groups, but $C_2^4 \oplus C_6$ can serve as a counterexample (P. C. Baayen).

We conclude this section with a geometrical interpretation of $D(G)$. Denote by Q_r the cube

$$\{\langle x_1, \ldots, x_r \rangle: |x_i| \leqslant 1, \ i = 1, \ldots, r\}$$

in the real r-space and let Q_r^+ be its subset consisting of all points with nonnegative coordinates. Then we have

PROPOSITION 2. *For any finite abelian group the constant $D(G)$ is equal to the minimal integer r with the property that every sublattice Λ of Z^r, which satisfies $Z^r/\Lambda < G$, contains at least one nonzero point of Q_r^+.*

Proof. Let $g_1, \ldots, g_r$ be a sequence of elements of G and let Λ be the kernel of f: $Z^r \to G$ defined by

$$f: \langle n_1, \ldots, n_r \rangle \mapsto \sum_{i=1}^{r} n_i g_i.$$

Obviously, there is a common nonzero point of Λ and Q_r^+ if and only if there is a subsequence of the g_i's with zero sum and it suffices to note that this correspondence between sequences of r elements of G and sublattices Λ of Z^r with $Z^r/\Lambda < G$ is one-to-one.

2. For an algebraic number field K let $\beta(K)$ be the maximal cardinality of a subset A of the classgroup H with the property that for all integers a of K, whose all prime ideal factors lie in the classes from A, the length of any factorization into irreducibles depends only on a and not on a particular factorization. It was shown by Śliwa [12] that the number of nonassociated integers a of K with $|N(a)| \leqslant x$ and all factorizations of the same length behaves asymptotically like

$$Cx \frac{(\log\log x)^c}{\log^d x}$$

with C positive, c nonnegative and $d = 1 - \beta(K)/h$.

Śliwa also considered the following property (C) of subsets of an abelian group:

A subset $\{g_1, \ldots, g_t\}$ of G is said to have the *property* (C), provided the following implication is true:

If $n_1 g_1 + \ldots + n_t g_t = 0$ (n_i — nonnegative integers) and this equality is minimal, i.e., if from $m_1 g_1 + \ldots + m_t g_t = 0$ with $0 \leqslant m_i \leqslant n_i$, $m_i \in Z$, it follows that either all m_i's are zero or $m_i = n_i$ for $i = 1, \ldots, t$, then

$$\sum_{i=1}^{t} \frac{n_i}{o(g_i)} = 1,$$

where $o(g)$ denotes the order of g. (Conditions of this type were also considered in [11] and [14].)

Define $\beta_0(G)$ as the maximal cardinality of a subset of G with the property (C). The following result lies hidden in the proof of lemma 2 in [12]:

PROPOSITION 3. $\beta(K) = \beta_0(H)$.

PROBLEM II. Evaluate $\beta_0(G)$. (**P 1142**)

The solution is known only for cyclic groups of prime-power order, where

$$\beta_0(C_{p^n}) = 1+n,$$

as shown by Śliwa ([12], lemma 1, (iii)).

Note that in the case $G = C_p^N$ (in which case we may treat G as a linear space over $GF(p)$), if $A \subset G$ has the property (C) and $u_1, \ldots, u_r$ is a maximal linearly independent subset of A, then A can contain only elements of the form

$$(1) \qquad \sum_{k=1}^{r} (p-a_k)u_k \qquad (1 \leqslant a_k \leqslant p)$$

with

$$(2) \qquad \sum_{\substack{k \\ a_k \neq p}} a_k = p-1$$

(cf. [12], lemma 1 (iv)).

This implies immediately the equality $\beta_0(C_2^N) = 1+N$, because in this case the set of nonzero elements of a set with the property (C) must be linearly independent. The following problem arises:

PROBLEM III. Let $u_1, \ldots, u_N$ be a basis of C_p^N and let A consist of all elements of the form (1) satisfying (2) (with $r = N$). Does A have the property (C)? (**P 1143**)

If the answer is affirmative, then

$$\beta_0(C_p^N) = 1+\binom{N+p-2}{p-1}.$$

Property (C) (and hence problems II and III) admits a geometrical interpretation. Let B be any subset of Z^N and let B^+ denote the subset of B consisting of all nonzero points with nonnegative coordinates. A point $P = \langle x_1, \ldots, x_N \rangle$ is called *minimal* if P lies in B^+ and there is no point

$\langle y_1, \ldots, y_N\rangle$ in B^+, distinct from P, and satisfying $x_i \geqslant y_i$, $i = 1, 2, \ldots, N$. For a finite abelian group G and $A = \{g_1, \ldots, g_t\} \subset G$, let Λ_A denote the lattice

$$\Big\{\langle n_1, \ldots, n_t\rangle \in Z^t \colon \sum_{i=1}^{t} n_i g_i = 0\Big\} \subset Z^t.$$

PROPOSITION 4. *The set A has the property* (C) *if and only if all minimal points of Λ_A^+ lie in a hyperplane.*

Proof. If A has the property (C), then all points of Λ_A^+, which are minimal, lie in the hyperplane

$$\sum_{j=1}^{t} \frac{x_j}{o(g_j)} = 1. \tag{3}$$

The points $P_i = \langle 0, \ldots, 0, o(g_i), 0, \ldots, 0\rangle$ ($i = 1, 2, \ldots, t$) are clearly minimal in Λ_A^+ and so if all minimal points of it lie on a hyperplane, this must be the hyperplane spanned by $P_1, \ldots, P_t$, thus its equation is (3). Hence A has the property (C).

This proposition leads to the following question:

PROBLEM IV. Describe all lattices in Z^N whose all minimal points lie on a hyperplane. (**P 1144**)

Now we can give a geometrical definition of $\beta_0(G)$.

PROPOSITION 5. *$\beta_0(G)$ is the maximal integer t with the property that there is a lattice $\Lambda < Z^t$ such that all its minimal points lie on a hyperplane, $Z^t/\Lambda < G$ and the points $e_1, \ldots, e_t$ are distinct* mod Λ. *Here e_i is the point whose i-th coordinate is* 1 *and the remaining coordinates vanish.*

Proof follows directly from the preceding proposition.

3. To deal with questions of unique factorization it is convenient to reformulate the notion of a factorization in $B(G)$.

Let $b = \langle g_1, \ldots, g_n\rangle$ be a given block in $B(G)$ and let an ordering of its elements be fixed. By a *factorization* of b we shall understand, for a certain positive $t = t(\Phi)$, any surjective map

$$\Phi\colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, t\}$$

such that if $A_i = A_i(\Phi)$ denotes the counterimage of i for $i = 1, 2, \ldots, t$, then

$$\sum_{j\in A_i} g_j = 0 \quad \text{for } i = 1, 2, \ldots, t,$$

i.e. the systems b_i formed by the elements g_j with j in A_i are blocks.

It is obvious that for any such factorization we have $b = b_1(\Phi)\ldots b_t(\Phi)$.

If all blocks $b_i(\Phi)$ are irreducible, we call Φ an *irreducible factorization*. We say that two factorizations Φ and Ψ are *equivalent* if $t(\Phi) = t(\Psi) = t$ and for a suitable permutation σ of $\{1, 2, \dots, t\}$ the blocks $b_i(\Phi)$ and $b_{\sigma(i)}(\Psi)$ coincide. Two equivalent factorizations are called *strongly equivalent* if, moreover, the sets $A_i(\Phi)$ and $A_{\sigma(i)}(\Psi)$ coincide. A complex is said to have a *unique factorization* if all its irreducible factorizations are equivalent and it is said to have a *strongly unique factorization* if all such factorizations are strongly equivalent.

Those properties are independent of the ordering of b.

Let $a_1(G)$ be the maximal length of a complex in $B(G)$ with a strongly unique factorization and, more generally, let $a_k(G)$ $(k = 1, 2, \dots)$ be the maximal length of a complex in $B(G)$ with at most k strongly inequivalent irreducible factorizations.

PROPOSITION 6. *If H is the classgroup of K, then $a_k(H)$ equals the maximal number of nonprincipal prime ideals which can divide a squarefree element of R with at most k distinct factorizations into irreducible elements.*

(An element of R is called *squarefree* if the principal ideal generated by it is not divisible by a square of a prime ideal.)

Proof. Let a be a squarefree element of R and let

$$aR = p_1 \dots p_s I,$$

where I is an ideal whose all prime ideal factors are principal and $p_1, \dots, p_s$ are nonprincipal prime ideals. Denote by g_i (for $i = 1, 2, \dots, s$) the class of H which contains p_i. Then $b = \langle g_1, \dots, g_s \rangle$ is a block in $B(H)$. If now

$$a = \pi_1 \dots \pi_t$$

is a factorization of a into irreducibles,

$$\pi_l = \prod_{j=1}^{k_l} p_{i(l,j)},$$

where $k_1, \dots, k_t$ are all distinct and not less than $1, 1 \leqslant i(l, j) \leqslant s$, and $k_1 + \dots + k_t = s$, then we can obtain a factorization of b by putting $\Phi(i) = l$ whenever $i(l, j) = i$ holds for a certain j. One sees immediately that distinct factorizations of a correspond in this way to strongly inequivalent irreducible factorizations of b, and conversely. Thus the proposition follows.

The knowledge of $a_k(G)$ would give an explicit asymptotical value for the number of nonassociated integers of K with absolute values of their norms bounded by x, which have at most k distinct factorizations into irreducibles. In [7] it was shown that this number is asymptotically equal to

$$Cx\frac{(\log\log x)^M}{\log^{1-1/h}x},$$

where C is positive and $M = M_k(K)$ equals the maximal number of nonprincipal prime ideal factors occurring with exponent 1 in the factorization of the ideal generated by a number with at most k distinct factorizations and we have the following

PROPOSITION 7. *For all fields K we have $M_k(K) = a_k(H)$.*

Proof. The preceding proposition implies $M_k(K) \geqslant a_k(H)$. To prove the converse inequality take any element a with at most k distinct factorizations and write

$$aR = p_1 \dots p_s q_1^{a_1} \dots q_t^{a_t} I,$$

where $p_1, \dots, p_s, q_1, \dots, q_t$ are distinct nonprincipal prime ideals, $t \geqslant 0$, $a_i \geqslant 2$ for $i = 1, 2, \dots, t$, and all prime ideal factors of I are principal.

Let p_0 be any prime ideal distinct from $p_1, \dots, p_s, q_1, \dots, q_t$ and lying in the class determined by $q_1^{a_1} \dots q_t^{a_t}$. The ideal $p_0 p_1 \dots p_s$ is principal and squarefree. Take any generator of it, say b, and note that it has at most k distinct factorizations into irreducibles. Applying proposition 6 we get $1+s \leqslant a_k(H)$ in the case where p_0 is nonprincipal and $s \leqslant a_k(H)$ in the case where p_0 is principal. Thus $s \leqslant a_k(H)$ holds in all cases and $M_k(K) \leqslant a_k(H)$ follows.

An upper bound for $a_1(G)$ is given by the following result:

PROPOSITION 8. *For all abelian groups G one has $a_1(G) \leqslant |G|$. If, moreover, G is cyclic, then $a_1(G) = |G|$.*

Proof. For any block $\langle g_1, \dots, g_t\rangle = b$ denote by $S(b)$ the set of all nonzero sums of the form

$$\sum_{j=1}^{t} \varepsilon_j g_j \qquad (\varepsilon_j = 0, 1).$$

LEMMA 1. *If the block b has a strongly unique irreducible factorization*

$$b = b_1 \dots b_n, \tag{4}$$

then for all disjoint subsets A, B of $\{1, 2, \dots, n\}$ we have

$$S\Big(\prod_{i\in A} b_i\Big) \cap S\Big(\prod_{i\in B} b_i\Big) = \emptyset.$$

Proof. Put

$$X_A = \prod_{i\in A} b_i, \qquad X_B = \prod_{i\in B} b_i.$$

If $h_1, \ldots, h_r$ are in X_A, $h'_1, \ldots, h'_s$ are in X_B and

$$h_1 + \ldots + h_r = h'_1 + \ldots + h'_s \neq 0,$$

then exchanging the elements $h_1, \ldots, h_r$ and $h'_1, \ldots, h'_s$ in X_A and X_B . and taking irreducible factorizations of the resulting blocks, we get a factorization of b which is strongly inequivalent to (4).

Lemma 2. *For any irreducible block b we have $|S(b)| \geqslant |b|$, save b of the form $\langle g, g, \ldots, g\rangle$ in which case $S(b)$ has $|b|-1$ elements and $S(b) \cup \{0\}$ is the cyclic group generated by g.*

Proof. Call a block *bad* if it has the form $\langle g, g, \ldots, g\rangle$.

If b is irreducible and not bad, then we can write

$$b = \langle g_1, g_2, \ldots, g_r\rangle \quad \text{with } g_1 \neq g_2.$$

In this case the r elements $g_1, g_2, g_1+g_2, \ldots, g_1+g_2+\ldots+g_{r-1}$ are distinct and nonzero and they are all members of $S(b)$. If, however, b is irreducible and bad, say, $b = \langle g, \ldots, g\rangle$ (m times), then m equals the order of g and $S(b) = \{g, 2g, \ldots, (m-1)g\}$.

Corollary 1. *If $b = b_1 \ldots b_t$ is a strongly unique irreducible factorization and none of the blocks b_i is bad, then $|S(b)| \geqslant |b|$.*

Proof. By lemma 1 the sets $S(b_i)$ are pairwise disjoint and as they all are contained in $S(b)$, the corollary follows from lemma 2.

Corollary 2. *If $b = b_1 \ldots b_t$ is a strongly unique irreducible factorization and all blocks b_i are bad, then*

$$|S(b)| \geqslant \prod_{i=1}^{t} |b_i| - 1.$$

Proof. Lemma 1 implies that if $b_i = \langle g_i, \ldots, g_i\rangle$, $i = 1, \ldots, t$, then all elements $g_1, \ldots, g_t$ are distinct and lemma 2 shows that all nonzero elements of the product

$$\prod_{i=1}^{t} gp\{g_i\}$$

lie in $S(b)$.

Proof of proposition 8. Let $b = b_1 \ldots b_t$ be a strongly unique irreducible factorization and let $b_1, \ldots, b_k$ be all bad blocks occurring in it. Let $N_i = |b_i|$ ($i = 1, 2, \ldots, t$). Then by corollaries 1 and 2 we get

$$S\Big(\prod_{i=1}^{k} b_i\Big) \geqslant N_1 \ldots N_k - 1 \tag{5}$$

and

$$S\Big(\prod_{i=1+k}^{t} b_i\Big) \geqslant N_{1+k} + \ldots + N_t. \tag{6}$$

If the proposition is false and the block b serves as a counterexample to it, then we must have $N_1+\ldots+N_t \geqslant 1+h$, but (5), (6) and lemma 1 imply

$$N_{1+k}+\ldots+N_t+N_1N_2\ldots N_k-1 < h$$

and so for $k = 0$ we have already a contradiction and for $k \neq 0$ we obtain

$$N_1N_2\ldots N_k < N_1+\ldots+N_k$$

which never happens to be true. The obtained contradiction establishes our proposition, the cyclic case being trivial.

An evident lower bound for $a_1(G)$ is contained in the following

Proposition 9. *If*

$$G = \bigoplus_{i=1}^{t} C_{n_i},$$

then

$$a_1(G) \geqslant \sum_{i=1}^{t} n_i.$$

Proof. It suffices to observe that if $g_1, \ldots, g_t$ are generators of the cyclic summands of G, then the product of bad blocks containing $g_1, \ldots, g_t$ has a strongly unique irreducible factorization.

The exact value of $a_1(G)$ is still unknown, so we have

Problem V. Determine $a_1(G)$ and, more generally, $a_k(G)$ for $k = 1, 2, \ldots$ **(P 1145)**

4. Another combinatorial constant which is, as we shall see, very similar to the constant of Davenport, arises when we consider factorizations of rational positive integers in quadratic fields. It was shown in [5] that the number of positive rational integers less than x, which in a given quadratic number field K have a unique factorization into irreducibles, is asymptotically equal to

$$Cx\frac{\log\log^M x}{(\log x)^{1/2-1/2h}},$$

where C is positive and depends on K, M is also positive, depends only on the classgroup H of K and was defined in [5] in a rather complicated way. We shall now show that this constant can be defined in a very simple way and give a geometrical interpretation of it similar to the interpretation of $D(G)$ given in proposition 2.

We start with recalling the definition of $M = M(H)$. Write

$$H = \bigoplus_{j=1}^{t} C_{h_j}, \tag{7}$$

where all summands are cyclic of $h_1, \ldots, h_t$ elements. For a given integer a and $i = 1, 2, \ldots, t$ put $[a]_i = h_i - a$ if $a \neq 0$ and $[a]_i = 0$ if $a = 0$. Consider now sequences $\{a_1, \ldots, a_t\}$ of rational integers satisfying

(i) $0 \leqslant a_i \leqslant h_i - 1$ for $i = 1, 2, \ldots, t$,

(ii) $a_1 \leqslant [a_1]_1$ and if for a certain k we have $a_i = [a_i]_i$ for $i = 1, 2, \ldots \ldots, k-1$, then $a_k \leqslant [a_k]_k$.

A set of sequences

$$\{a_1^{(j)}, \ldots, a_t^{(j)}\} \quad (j = 1, 2, \ldots, T),$$

satisfying (i) and (ii), is called *admissible* provided for any two distinct 0-1 sequences $\{\varepsilon_1, \ldots, \varepsilon_T\}$, $\{\eta_1, \ldots, \eta_T\}$ there is an index i, $1 \leqslant i \leqslant t$, such that

$$\sum_{k=1}^{T} \varepsilon_k a_i^{(k)} \not\equiv \sum_{k=1}^{T} \eta_k a_i^{(k)} \pmod{h_i}. \tag{8}$$

The constant M equals the maximal cardinality of an admissible set. The next proposition shows that this definition can be simplified:

PROPOSITION 10. *The constant M equals the maximal cardinality of a subset $\{g_1, \ldots, g_n\}$ of H with the property that all sums*

$$\sum_{k=1}^{n} \varepsilon_k g_k \quad (\varepsilon_k = 0, 1;\ k = 1, \ldots, n) \tag{9}$$

are distinct.

Proof. Let $A_1, \ldots, A_t$ be fixed generators of the cyclic summands of G. It was noted already in [5] that the orbits of G under $g \mapsto -g$ are in a one-to-one correspondence with sequences $\{n_1, \ldots, n_t\}$ satisfying (i) and (ii) given by

$$\{n_1, \ldots, n_t\} \mapsto \Big\langle \sum_{i=1}^{t} n_i A_i, -\sum_{i=1}^{t} n_i A_i \Big\rangle.$$

Now let $g_1, \ldots, g_n$ be such that all sums (9) are distinct. Write each g_i in the form

$$g_i = \sum_{j=1}^{t} m_j^{(i)} A_j \quad (i = 1, \ldots, n)$$

and let the sequences $m_1^{(i)}, \ldots, m_t^{(i)}$ satisfy (i) and (ii) for $i = 1, 2, \ldots, R$ but not for $i = R+1, \ldots, n$.

Consider the sequence $g_1, \ldots, g_R, -g_{R+1}, \ldots, -g_n$ and let us prove that all sums formed by subsequences of it are distinct. Indeed, let

$$g_{i_1} + \ldots + g_{i_a} + (-g_{j_1}) + \ldots + (-g_{j_b}) = g_{k_1} + \ldots + g_{k_c} + (-g_{l_1}) + \ldots + (-g_{l_d})$$

be a nontrivial equality. We may assume that no cancellation is possible here, thus

$$\{i_1, \ldots, i_a\} \cap \{k_1, \ldots, k_c\} = \{j_1, \ldots, j_b\} \cap \{l_1, \ldots, l_d\} = \emptyset.$$

As for $\alpha \leqslant a$, $\beta \leqslant b$, $\gamma \leqslant c$, $\delta \leqslant d$ we have $i_\alpha, k_\gamma \leqslant R < j_\beta, l_\delta$, all four sets of indices are disjoint and we arrive at a nontrivial identity

$$\sum_{\alpha=1}^{a} g_{i_\alpha} + \sum_{\delta=1}^{d} g_{l_\delta} = \sum_{\beta=1}^{b} g_{j_\beta} + \sum_{\gamma=1}^{c} g_{k_\gamma},$$

contrary to our assumption.

The sequences of integers subject to (i) and (ii), associated with orbits of $g_1, \ldots, g_R, -g_{R+1}, \ldots, -g_N$, evidently satisfy (8) and so the inequality $n \leqslant M$ follows. The converse inequality is immediate: if the orbits $(g_1, -g_1), \ldots, (g_n, -g_n)$ are such that the corresponding sequences realize (8), then all sums (9) are distinct.

Now define $M(G)$ for an arbitrary finite abelian group G as the maximal cardinality of a subset $\{g_1, \ldots, g_n\}$ of G for which all sums (9) are distinct.

One sees immediately that $M(G)$ is equal to the maximal cardinality of a subset $\{g_1, \ldots, g_n\}$ of G with the property that the sum

$$\sum_{i=1}^{n} \varepsilon_i g_i \quad \text{with } \varepsilon_i = 0, 1, -1$$

can vanish only if $\varepsilon_i = 0$ for $i = 1, \ldots, n$.

If $G = C_m^k$, this constant was considered recently by Stein [13] in connection with the graph theory. He showed that for odd m the following inequality holds:

$$M(C_m^k) \leqslant \frac{\log\left(m^{k-1}(m-1)\right)}{\log 2}.$$

The following proposition gives the trivial bounds for $M(G)$:

Proposition 11 (lemma 14 of [5]). *If*

$$G = \bigoplus_{i=1}^{t} C_{N_i},$$

then

$$\sum_{i=1}^{t} \left[\frac{\log N_i}{\log 2}\right] \leqslant M(G) \leqslant \left[\frac{\log |G|}{\log 2}\right].$$

It results that if G is a 2-group, then $M(G) = \log|G|/\log 2$ and it is clear that $M(C_3^N) = N$, as G is in this case a linear space over $GF(3)$ and $M(G)$ is the maximal cardinality of a linearly independent subset of G.

PROBLEM VI. Determine $M(G)$. (P 1146)

We conclude with a geometrical interpretation for $M(G)$:

PROPOSITION 12. *The constant $M(G)$ equals the minimal integer r with the property that there exists a sublattice Λ of Z^r not containing any nonzero point of Q_r and for which $Z^r/\Lambda < G$.*

Proof. Copy the proof of proposition 2, replacing Q_r^+ by Q_r.

REFERENCES

[1] S. Allen, *On the factorizations of natural numbers in an algebraic number fieid,* Journal of the London Mathematical Society 11 (1975), p. 294-300.

[2] P. van Emde Boas, *A combinatorial problem on finite abelian groups, II,* Reports of the Mathematisch Centrum Amsterdam, ZW-1969-007.

[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. 59-68; 15 (1966), p. 49-58.

[5] — *On natural numbers having unique factorization in a quadratic number field,* Acta Arithmetica 12 (1966), p. 1-22; 13 (1967), p. 123-129.

[6] — *A note on factorizations in quadratic fields,* ibidem 15 (1968), p. 19-22.

[7] — *Numbers with unique factorization in an algebraic number field,* ibidem 21 (1972), p. 313-322.

[8] — *Elementary and analytic theory of algebraic numbers,* Warszawa 1974.

[9] R. W. K. Odoni, *On a problem of Narkiewicz,* Journal für die reine und angewandte Mathematik 288 (1976), p. 160-167.

[10] J. E. Olson, *A combinatorial problem in finite abelian groups,* Journal of Number Theory 1 (1969), p. 8-10 and p. 195-199.

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

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

[13] S. K. Stein, *Modified linear dependence and the capacity of a cyclic graph,* Linear Algebra and its Applications 17 (1977), p. 191-195.

[14] A. Zaks, *Half factorial domains,* Bulletin of the American Mathematical Society 82 (1976), p. 721-723 and p. 965.

INSTITUTE OF MATHEMATICS, WROCŁAW UNIVERSITY

Reçu par la Rédaction le 24. 11. 1977