stichting
mathematisch
centrum

MC

AFDELING ZUIVERE WISKUNDE ZW 31 JANUARI

P. VAN EMDE BOAS AND D. KRUYSWIJK
A COMBINATORIAL PROBLEM ON FINITE ABELIAN GROUPS III

PREPRINT OF ZW 1969-008

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

A note of the editors

This preprint consists of the sections II, III and IV of report ZW 1969-008, which will appear together with an introduction by P.C. Baayen in the near future.
For definitions stated in this introduction the reader is referred to [2].

II. Some groups for which $\lambda(G) = \Lambda(G)$.

§ 1. Introduction.

In [2] the equality $\lambda(G) = \Lambda(G)$ was proved for the following cases:

I G is an Abelian p-group.

II $G = C_a \oplus C_{ab}$

III $G = H \oplus C_{q^n m}$ where H is a p-group of order q^j such that $q^n \geq M(H)$

IV $G = C_{2\,p^{n_1}} \oplus C_{2\,p^{n_2}} \oplus C_{2\,p^{n_3}}$ with p prime

V $G = C_2 \oplus C_{2n\,m_1} \oplus C_{2n\,m_2}$ with $n = 2^{k_1} 3^{k_2} 5^{k_3} 7^{k_4}$ and either $m_1 = 1$ m_2 arbitrary or $m_1 = p^r$, $m_2 = p^s$ p prime

In [1] was shown that $\lambda = \Lambda$ holds for

VI $G = C_2 \oplus C_2 \oplus C_2 \oplus C_{2m}$ (for odd m)

In this section we extend the above list by three new series.

VII : $G = C_3 \oplus C_3 \oplus C_{6m}$ for $3 \nmid m$

VIII: $G = C_{3.2^{n_1}} \oplus C_{3.2^{n_2}} \oplus C_{3.2^{n_3}}$

IX : $G = C_3 \oplus C_{6n\,m_1} \oplus C_{6n\,m_2}$ with n, m_1 and m_2 like in series V.

The proof of these series is based on a couple of lemma's and theorems which we formulate below. First we repeat some of the definitions of notions we use in the sequel which were given in [2].

Let $G = C_{d_1} \oplus \ldots \oplus C_{d_k}$, $d_1 \mid d_2 \mid \ldots \mid d_k$.

A short zero-sequence S is a zero-sequence with length $\leq d_k$.

By $\mu_B(G)$ we denote the smallest integer n such that any G-sequence S of length $\geq$ n contains a short zero-subsequence. We always have $\mu(G) \leq \mu_B(G) \leq (d_k-1)(\omega(G) - 1) + 1$.

A hole of a G-sequence S is an element $\neq 0$ of G which does not appear as the sum of a subsequence of S.

By $\nu(G)$ we denote the smallest integer n such that for any primitive non-maximal G-sequence S of length n there exists a subgroup $N \subset G$ so that all holes of S are contained in a proper coset $x + N \quad x \notin N$.
We always have $\lambda(G) - 1 \leq \nu(G) \leq \lambda(G)$.

A new notion we use in this section is the following property (Q) :

For any primitive non maximal G-sequence S of length $\nu(G)$ there exists a subgroup $N \subset G$ of index 2 so that all holes of S are contained in the proper coset $G \setminus N$.

Property (Q) puts a restriction on the subgroups N which are supposed to exist by the definition of $\nu(G)$.
Now we state our lemma's and theorems:

Lemma (1,1): The equality $\lambda(G) = \Lambda(G)$ holds for $G = C_3 \oplus C_3 \oplus C_6$

Lemma (1,2): $\mu_B(C_3 \oplus C_3 \oplus C_3) = 17$

Any $C_3 \oplus C_3 \oplus C_3$ - sequence S with length 14 and value zero contains a short-zero-sequence.

Lemma (1,3): Property (Q) is shared by groups of the following types:

a) $G = C_{2m}$

b) $G = C_{2^{n_1}} \oplus C_{2^{n_2}} \oplus C_{2^{n_3}}$

c) $G = C_{2n\,m_1} \oplus C_{2n\,m_2}$

$n = 2^{k_1} 3^{k_2} 5^{k_3} 7^{k_4}$ and
either $m_1 = 1$ m_2 arbitrary
or $m_1 = p^r$ $m_2 = p^s$.

Theorem (1,4): Let $H = C_{n_1} \oplus C_{n_2} \oplus C_{n_3}$. If $\nu(H) = \Lambda(H) - 1$ and if H shares property (Q) then for $G = C_{3n_1} \oplus C_{3n_2} \oplus C_{3n_3}$ the equality $\lambda(G) = \Lambda(G)$ is true.

The proof of Th(1,4) depends on Lemma (1,1). Therefore we treat the case $C_3 \oplus C_3 \oplus C_6$ separately; see § 2, and also [3].
For Lemma (1,2) we give no proof in this report. It depends on some propositions treating the structure of $C_3 \oplus C_3 \oplus C_3$ which have been proved by trying out all possibilities. The proof will appear in the seperate report [4]. For more details see § 3.
For Lemma (1,3) we only give a sketch of a proof. A complete proof would demand an almost complete transcription of proofs given in [2]. We only give indications how the proofs given there have to be modified; see § 3.
The proof of Th (1,4) is given in § 4.

It is known from the results in [2] that for groups of types a) b) and c) in (1,3) the equality $\nu(G) = \Lambda(G) - 1$ holds.
By application of (1,3) and (1,4) one easily sees that the equality $\lambda(G) = \Lambda(G)$ holds for groups of the type's VII, VIII and IX.

§ 2. The case $G = C_3 \oplus C_3 \oplus C_6$

Lemma (1,1) : For $G = C_3 \oplus C_3 \oplus C_6$ the equality $\lambda(G) = \Lambda(G)$ holds.

proof: We write G in the shape $G = C_3 \oplus C_3 \oplus C_3 \oplus C_2$.
Elements from G are written as columns $\binom{x}{y}$ with
$x \in (C_3)^3$, $y = 0,1$.

We have $\Lambda(G) = 9$. It is therefore sufficient to show $\lambda(G) < 10$.
Let S therefore be a G-sequence of length 10. We prove that
S is not primitive.

Put $S = \left(\binom{x_1}{y_1}, \ldots\ldots, \binom{x_{10}}{y_{10}}\right)$

Suppose first that the $(C_3)^3$-sequence $S' = (x_1, \ldots, x_{10})$
contains two disjoint zero-subsequences T' , V'.
Then S is not primitive. For let T and V be the corresponding
subsequences of S then we have

$$|T| = \binom{0}{a} \qquad |V| = \binom{0}{b} \qquad \text{and} \qquad |T \cup V| = \binom{0}{a+b} .$$

Hence T, V or $T \cup V$ is a zero-subsequences of S. The above
situation certainly arises if S' contains a short zero-sub-
sequence as the remaining ≥ 7 elements in S' cannot form a
primitive sequence for $\left(\lambda((C_3)^3) = 6\right)$.

(The argument presented above is a special case of the argument
from [2] § 3).

Without loss of generality we may assume $y_1 = y_2 = \ldots = y_r = 1$,
$y_{r+1} = \ldots = y_{10} = 0$, $0 \leq r \leq 10$.
We consider subcases for the problem depending on the value of r.

case 1: $r \leq 6$.

Let $t = \lceil r/2 \rceil$ and form the sequence:

$$T = \left(\begin{pmatrix} x_1+x_2 \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} x_{2t-1}+x_{2t} \\ 0 \end{pmatrix}, \begin{pmatrix} x_{r+1} \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} x_{10} \\ 0 \end{pmatrix}\right)$$

This is a H-sequence of length ≥ 7 where H is the subgroup of all $\binom{x}{y}$ with $y = 0$. As $H \cong (C_3)^3$ we have $\lambda(H) = 6$. Hence T and therefore S also is not primitive

case 2: $r \geq 9$

Consider the sequence $S' = \left(\begin{pmatrix} x_1 \\ 1 \end{pmatrix}, \ldots\ldots, \begin{pmatrix} x_9 \\ 1 \end{pmatrix}\right)$ to be a $(C_3)^3 \oplus C_3$ sequence! We have $\lambda((C_3)^4) = 8$, hence S' is not primitive as $(C_3)^4$ sequence. We conclude that the sequence $(x_1, \ldots, x_9)$ contains a zero-subsequence of length $k = 3$, 6 or 9.

If $k = 3$ we have a short zero-sequence which makes S to be not primitive. If $k = 6$ the corresponding subsequence of S' is a $(C_3)^3 \oplus C_2$ zero-subsequence of S as well. Finally if $k = 9$ the corresponding $(C_3)^3$ - zero-sequence is not irreducible. Hence $(x_1, \ldots., x_{10})$ contains two disjoint zero-subsequences. Again S is not primitive.

case 3: $r = 8$.

Again we consider the sequence $S' = \left(\begin{pmatrix} x_1 \\ 1 \end{pmatrix}, \ldots., \begin{pmatrix} x_8 \\ 1 \end{pmatrix}\right)$ to be a $(C_3)^4$ - sequence.

If S' is not primitive we conclude that S is not primitive like in case 2. If S' however is primitive it is a maximal $(C_3)^4$-sequence and all elements $\neq 0$ in $(C_3)^4$ are the sum of some subsequence of S'.

Let $t = x_1 + x_2 + \ldots. + x_{10}$. Now there exists a subsequence T' of S' with $|T'| = \binom{t}{1}$ (calculating in $(C_3)^4$!).

We conclude that $(x_1, \ldots, x_8)$ contains a subsequence with sum t and length $k = 1, 4$ or 7. We may assume $|(x_1, \ldots, x_k)| = t$.

If $k = 1$ then $(x_2, \ldots, x_{10})$ is a zero-sequence of length 9 which cannot be irreducible. It is therefore the union of two disjoint zero-subsequences.

If $k = 7$ then (x_8, x_9, x_{10}) is a short zero sequence. We conclude that S is not primitive if $k = 1$ or 7.

If $k = 4$ however the subsequence

$$V = \left(\binom{x_5}{1}\binom{x_6}{1}\binom{x_7}{1}\binom{x_8}{1}\binom{x_9}{0}\binom{x_{10}}{0}\right)$$

is a zero-subsequence of S.

case 4: $r = 7$.

Let $t = -(x_1 + x_2 + \ldots + x_{10})$. If S is primitive then the sequence $S \cup \{\binom{t}{1}\}$ is an irreducible zero-sequence.

This implies that all subsequences of $S \cup \{\binom{t}{1}\}$ are primitive. Consider the following sequence

$$S' = \left(\binom{x_1}{1}, \ldots, \binom{x_7}{1}, \binom{t}{1}\binom{x_8}{0}, \binom{x_9}{0}\right)$$

S' is a subsequence of length 10 of $S \cup \{\binom{t}{1}\}$.
It has however $r = 8$. Therefore S' is not primitive as has been shown in case 3.
Again we conclude that S is not primitive.

This completes the proof of Lemma (1,1).

§ 3. Background information for theorem (1,4).

In this section no complete proofs are given. Readers willing to accept Lemma (1,2) and (1,3) as being true can proceed to § 4 straight away.

Let $G = C_3 \oplus C_3 \oplus C_3$. A short G- zero-sequence has length ≤ 3. We have the following types of short zero-sequences:

length 1 : (0)

length 2 : (x, -x)

length 3 : (x, x, x) or (x, x+a, x-a)

From this we see that in a short zero-sequence all elements are distinct except for the case of length 3 that the three elements are equal. For the presence of a short zero-sequence in some G-sequence S it makes therefore no difference whether some element x is contained one or two times. One needs only to consider G-sequences consisting of distinct elements.

Now the following properties are shared by $G = C_3 \oplus C_3 \oplus C_3$.

Property 1: The maximal length of a G-sequence of distinct elements containing no short zero-sequence is 8.

Property 2: Any G-sequence of length 8, consisting of distinct elements and containing no short zero-subsequence is a zero-sequence.

Property 3: No G-sequence of length 7, consisting of distinct elements and containing no short zero-subsequence is a zero-sequence.

These properties are shown in [4].

Lemma (1,2) is easily derived from properties 1, 2 and 3.

Let S be a G-sequence of 8 distinct elements not containing a short zero-subsequence then $S \cup S$ has length 16 and contains no short zero-subsequence. Hence $\mu_B(G) \geq 17$.

Any sequence of length 17 not containing some element three times contains ≥ 9 distinct elements; hence $\mu_B(G) \leq 17$.

Let S be a sequence of length 14 containing no short zero-sequence. Then it contains at least 7 and at most 8 distinct elements.
In the first case $S = T \cup T$ where T is a sequence as described in property 3. $|T| \neq 0$ and therefore $|S| \neq 0$.
In the second case $S = T \cup V$ where T is a sequence as described in property 2 and V is a subsequence of T of length 6. Now $|T| = 0$ and $|V| \neq 0$ (else $T \setminus V$ is a short zero-sequence) and therefore $|S| \neq 0$.

Next we treat Lemma (1,3). For any of the three types of groups the equality $v(G) = \Lambda(G) - 1$ is proved in [2]. We consider these proofs in details.

<u>case a)</u> : $G = C_{2m}$. See [2] prop (1,19).

It is shown there that any non maximal primitive C_{2m}-sequence S of length $2m - 2$ consists of a fixed generator $a \in C_{2m}$ taken $2m - 2$ times. The unique hole of S is the element $-a$. Now take $N = \{ka \mid k \text{ is even}\}$. Then N is a subgroup in C_{2m} of index 2 and $-a \in C_{2m} \setminus N$.
It follows that G has property (Q).

case b) : $G = C_{2^{n_1}} \oplus C_{2^{n_2}} \oplus C_{2^{n_3}}$. See [2] th (2,8).

It is shown there that for any p-group $G = C_{p^{n_1}} \oplus \ldots \oplus C_{p^{n_k}}$ and for any G-sequence S of length $\Lambda(G) - 1$ which is primitive and not maximal, there exist constants $c_1, \ldots, c_k \in \mathbb{F}_p$ (the finite field of p elements) not all being zero such that the following implication holds:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \text{is a hole of } S \implies c_1 x_1 + \ldots + c_k x_k \equiv -1 \pmod{p}$$

Now we have in this special case p = 2. Then the equation $c_1 x_1 + \ldots + c_k x_k \equiv 0$ determines a subgroup N in G of index 2 and the equation $c_1 x_1 + \ldots + c_k x_k \equiv 1$ determines its unique coset.

case c) : $G = C_{2n\,m_1} \oplus C_{2n\,m_2}$. See [2] prop (5,5).

The equality $\nu(G) = \Lambda(G) - 1$ is proved by complete induction. We perform this induction in such a way that the latest application of th (5,4) is in a situation represented by the following short exact sequence:

$$0 \to C_{n\,m_1} \oplus C_{n\,m_2} \xrightarrow{i} C_{2n\,m_1} \oplus C_{2n\,m_2} \xrightarrow{\pi} C_2 \oplus C_2 \to 0$$

In the proof of (5,4) the coset $x' + \pi^{-1}(N)$ containing the holes from S is the complete original under π of a proper coset $x + N$ in $C_p \oplus C_p$.
For our special case we have p = 2. Then the index of N in $C_2 \oplus C_2$ is two, and by the surjectivity of π the same holds in G : index $[\pi^{-1}(N) : G] = 2$.

This completes our sketch of a proof of Lemma (1,3).

In the formulation of property (Q) the fact that index $[N : G]$ is even presupposes that the order of G is even. This is however not sufficient.
Consider for example $G = C_3 \oplus C_6$. Then $\omega(G) = 18$ is even.
The equality $\nu(G) = \Lambda(G) - 1$ follows by [2] prop (5,5).
Take for S the sequence $S = \left(\binom{1}{0}, \binom{0}{1}, \binom{0}{1}, \binom{0}{1}, \binom{0}{1}, \binom{0}{1}\right)$. The holes of S form the proper coset $\left\{ \binom{x}{y} \;\middle|\; x = 2 \right\}$. This collection however has a non empty intersection with any subgroup of index 2.
It is unknown whether or not $\nu(G) = \Lambda(G) - 1$ implies (Q) for groups $G = C_{n_1} \oplus C_{n_2} \oplus \ldots \oplus C_{n_k}$ for which all n_i are even.

§ 4 Proof of theorem (1,4).

We consider an exact sequence

$$0 \to C_{n_1} \oplus C_{n_2} \oplus C_{n_3} \xrightarrow{i} C_{3n_1} \oplus C_{3n_2} \oplus C_{3n_3} \xrightarrow{\pi} C_3 \oplus C_3 \oplus C_3 \to 0$$

We denote $H = C_{n_1} \oplus C_{n_2} \oplus C_{n_3}$, $G = C_{3n_1} \oplus C_{3n_2} \oplus C_{3n_3}$.

In order to show $\lambda(G) = \Lambda(G)$ we prove $\mu(G) = M(G)$. We take a zero-sequence S of length $M(G) + 1$ and prove that S is not irreducible.

Let S be a G-zero-sequence of length $M(G) + 1 = 3(n_1+n_2+n_3) - 1$.
We have by Lemma (1,2) $\mu_B(C_3 \oplus C_3 \oplus C_3) = 17$. Hence πS contains at least $n_1 + n_2 + n_3 - 5$ disjoint short zero-subsequences, say $\pi S_1, \ldots, \pi S_{r-1}$. The corresponding subsequences $S_1, \ldots, S_{r-1}$ therefore have values in i(H).

Let T be the sequence of the remaining ≥ 14 elements. We may assume that the length of T is 14. If not we take the first 13 elements and the sum of the remaining elements producing in this way a sequence T' of length 14, such that $|T| = |T'|$.
In fact we change the sequence S by taking some elements together. However, if we prove that the resulting sequence S' is not irreducible then S is not irreducible either.

Now π T has length 14 and further $|\pi T| = 0$. By Lemma (1,2) we conclude that π T contains another short zero-subsequence πS_r. Let S_r be the corresponding subsequence of T and let $T_2 = T \setminus S_r$. Then T_2 contains At least 11 elements. Further $|\pi T_2| = 0$.

We have $r \geq n_1 + n_2 + n_3 - 4$.
By assumption we have $\nu(H) = \Lambda(H) - 1 = n_1 + n_2 + n_3 - 4$. Further we have assumed that H has property (Q).

Consider the H-sequence $V = (i^{-1}|S_1|, \ldots, i^{-1}|S_r|)$

If V is not primitive then V contains a zero-subsequence. This implies that S contains a proper subsequence with value zero hence S is not irreducible.

If V is maximal then $\pi\, T_2$ contains another proper zero-subsequence say $\pi\, S_{\nu+1}$ for $11 > \mu((C_3)^3) = 7$. But then $V \cup \{i^{-1} \mid S_{r+1}\}$ contains a zero-subsequence. We conclude that S contains a proper zero-subsequence, hence S is not irreducible.

Finally we suppose that V is not maximal. Then there exist a subgroup $N \subset H$ of index 2 such that all holes of V are contained in $H \setminus N$. Let K be the group $G / i(N)$. It is easy to see that K is an 54 element group which can be mapped homomorphically onto $(C_3)^3$ by the map $x + i(N) \longmapsto x + i(H)$. Therefore

$$K \overset{\sim}{=} C_3 \oplus C_3 \oplus C_3 \oplus C_2 = C_3 \oplus C_3 \oplus C_6.$$

Let τ be the natural projection from G onto K. The sequence $\tau\, T_2$ has length 11. As $\lambda(K) = 9$ (Lemma (1,1)) we conclude that $\tau\, T_2$ is not primitive or irreducible.

$\tau\, T_2$ contains a proper zero-subsequence $\tau\, U$ of length ≤ 10. Let U be the corresponding proper subsequence of T_2 then $|U| \in i(N)$. As all holes of V were contained in $H \setminus N$ we conclude that $V \cup \{i^{-1} \mid U|\}$ is not primitive. Again we derive that S is not irreducible.

This completes the proof of theorem (1,4).

Corollary (1,5): The equality $\lambda(G) = \Lambda(G)$ holds for the following series of groups:

VII : $G = C_3 \oplus C_3 \oplus C_{6m}$ $\qquad 3 \nmid m$

VIII: $G = C_{3.2^{n_1}} \oplus C_{3.2^{n_2}} \oplus C_{3.2^{n_3}}$

IV : $G = C_3 \oplus C_{6n\, m_1} \oplus C_{6n\, m_2}$ $\qquad n = 2^{k_1} 3^{k_2} 5^{k_3} 7^{k_4}$ and either $m_1 = 1$, m_2 arbitrary or $m_1 = p^r$, $m_2 = p^s$.

proof: by (1,3) and (1,4).

remark: The equality $\lambda(G) = \Lambda(G)$ is known to be true for all groups of dimension 1 and 2 (Type II). For dimension 4 there exists an example of a group for which $\lambda(G) \geq \Lambda(G) + 1$ ($G = C_3 \oplus C_3 \oplus C_3 \oplus C_6$). The problem whether or not the equality is generally true for groups of dimension 3 remains open. After the results of this section the smallest groups of dimension 3 for which it is unknown whether or not $\lambda = \Lambda$ are

G	ω	Λ
$C_3 \oplus C_3 \oplus C_{15}$	135	18
$C_3 \oplus C_3 \oplus C_{21}$	189	24
$C_5 \oplus C_5 \oplus C_{10}$	250	17
$C_3 \oplus C_3 \oplus C_{33}$	297	36
$C_4 \oplus C_4 \oplus C_{20}$	320	25
$C_3 \oplus C_3 \oplus C_{39}$	351	42
$C_5 \oplus C_5 \oplus C_{15}$	375	22
$C_3 \oplus C_3 \oplus C_{45}$	405	48
$C_4 \oplus C_4 \oplus C_{28}$	448	33
$C_3 \oplus C_3 \oplus C_{51}$	459	54
$C_3 \oplus C_9 \oplus C_{18}$	486	27
$C_5 \oplus C_5 \oplus C_{20}$	500	27
$C_5 \oplus C_{10} \oplus C_{10}$	500	22

In this list the group $C_4 \oplus C_4 \oplus C_{12}$ is missing although this group is not contained in any of the series I upto IX. The equality $\lambda = \Lambda$ however can be derived for this group by from the equality $\nu(C_2 \oplus C_2 \oplus C_6) = \Lambda(C_2 \oplus C_2 \oplus C_6) - 1$. See [2] th (4,2). The latter equality can be verified "by brute force" (i.e. checking all possibilities).

III. Some groups for which $\lambda(G) > \Lambda(G)$.

§ 5. Some series of excessive groups

The function $\lambda - \Lambda$ will be called the excess. A group G will be called excessive iff $\lambda(G) - \Lambda(G) \geq 1$.

Theorem (5,1): Let $n \geq 2$, $k \geq 2$, $(n,k) = 1$, then we have:

(5,1) a) $C_n^{kn-1} \oplus C_{nk}$ is excessive

(5,1) b) $C_n^{kn-n+2} \oplus C_{nk}$ is excessive

(5,1) c) If either $(k, n+1) \geq 2$ or $k \geq n^2-n+1$ then the group $C_n^{(k-1)n} \oplus C_{kn}$ is excessive.

Theorem (5,1) c) confirms BAAYEN's excessive example $C_2^4 \oplus C_6$ and yields the excessive group $C_3^3 \oplus C_6$. This group is four-dimensional. We do not know whether there are 3-dimensional groups (three-cyclic groups) with a positive excess. We shall prove theorem (5,1) with help of the following complicated statement:

Theorem (5,2): Let $n \geq 2$, $k \geq 2$, $(n,k) = 1$ and let

(1) $$G = C_n^{(k-1)n+\rho} \oplus C_{kn} \quad (0 \leq \rho \leq n-1).$$

Then we have:

(5,2) a) G has an excess $\geq \rho$ if $1 \leq \rho \leq n-1$ and $\rho \not\equiv n \mod k$.

(5,2) b) G has an excess $\geq \rho+1$ if $0 \leq \rho \leq n-2$, provided that

(2) $$x(n-\rho+1) \not\equiv n \text{ modulo } k$$

for $x = 1, 2, \ldots, n-1$.

Remarks (5,2) a) implies (5,1) a), because $n-1 \not\equiv n \mod k$.

(5,2) b), restricted to the case $\rho = 0$, gives

the following statement (which we call (5,2) c):

(5,2) c) $C_n^{(k-1)n} \oplus C_{kn}$ has a positive excess if k does not divide any term of the finite arithmetic sequence

$$1,\ n+2\ ,\ 2n+3,\ \ldots\ldots,\ n^2-n-1,\ n^2.$$

This statement implies (5,1) c). For the proof of (5,1) b) we distinguish three cases:

(p). $\underline{n = 3,\ k = 2}$. Here (5,1) a), which has just been proved, coïncides with (5,1) b) , even with "better" excess.

(q). $\underline{n \geq 4,\ n \equiv 1 \bmod k.}$ We take $\rho = 2$ in (5,2) b) . Then (2) shrinks to $0 \not\equiv n \bmod k$, which cannot fail to be true. Excess ≥ 3.

(r). $\underline{n \not\equiv 1 \bmod k}$. Here (5,2) a) gives a positive excess for $\rho = 1$. Does it follow that the same holds true if the exponent is nk-k+2? Yes. Let us consider canonical extensions of an arbitrary group G, by a cyclic component C_{m^*} . Here the word "canonical" means that m^* should fit somewhere in the divisor chain of G. Then Λ increases by m^*-1 and it can be seen that λ increases by at least m^*-1 [see [2] (1.16)] . It follows that the excess does not diminish, and I_b is true. [We mention further that the extension procedure proves at once the inequality $\lambda(G) \geq \Lambda(G)$ for all G]

We have derived by now theorem (5,1) from (5,2). Further exploration of the contents of (5,2) seems worth while, but can be tedious. The following observations reduce the number of calculations, especially if $k < n$.

. (5,2) a) is without meaning and (5,2) b) is useless for all those cases where $\rho \equiv n$ modulo k.

  In such a case one should proceed by canonical extension from downward.

. (5,2) b) is useless for $\rho = 1$ and for all further cases where $\rho \equiv 1 \bmod k$.

Example : $n = 8$, $k = 5$

ρ ..... →	0	1	2	3	4	5	6	7 .
excess by (5,2) a)$\geq$	-	1	2	-	4	5	6	7
excess by (5,2) b)$\geq$	0	-	0	-	5	0	-	-
Hence, excess $\geq$	0	1	2	2	5	5	6	7.

§ 6 Proof of Theorem (5,2)

We define T by:

(3) $$T = (k-1)n + \rho \qquad (0 \leq \rho \leq n-1)$$

and note that we have $T \geq 3$, besides:

(4) $$T \equiv \rho - n \quad \text{modulo } k.$$

The elements of the group C_n^T will be presented as vectors

(5) $$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_T \end{pmatrix} \quad \text{modulo } n.$$

That basic vector which has $\alpha_\mu \equiv 1$ and the remaining marks zero, is denoted by e_μ.
The vector in which all α_μ are 1 is denoted by f. Let S be the following structure (= sequence) over C_n^T :

(6) $$S = \underbrace{e_1 \ldots e_1}_{B_1}\ \underbrace{e_2 \ldots e_2}_{B_2} \cdots\cdots \underbrace{e_T \ldots e_T}_{B_T}\ \underbrace{f \ldots f}_{B^*} \quad ,$$

where each of the blocks B_i has n terms and where B^* has n^* terms. Here n^* has the following definition:

(7) n^* is either n or n-1. The choice is free for $0 \leq \rho \leq n-2$, but if $\rho = n-1$, then n^* must be n-1.

A simple calculation shows, by (3), that we have:

(8) $$l_S - \Lambda(C_n^T \oplus C_{kn}) = \begin{cases} \rho+1 & \text{if } n^* = n \\ \rho & \text{if } n^* = n-1, \end{cases}$$

where l_S is the length of S. This gives a certain hope that we shall succeed.

Before doing so, we study the zero-structures (subsequences with vanishing sum) in S.

Let Z be any zero structure in S and let the intersection of Z and B^* be a sequence of α elements ($0 \leq \alpha \leq n^*$) Then there are three possibilities:

P1) $\alpha = 0$. In order to obtain the sumvalue zero, Z must necessarily be the union of one or more blocks of type B_i.
Hence we find:

- There is a ν with $1 \leq \nu \leq nk-1$ such that Z consists of ν blocks, and such that B^* is not among these blocks.

P2) $\alpha = n$. Then we have $n^* = n$ and according to (7) :
$\rho \leq n-2$. By analoguous argument as in the foregoing case we find now:

- There is a μ with $1 \leq \mu \leq nk-1$ such that Z consists of μ blocks and where B^*, with $n^* = n$, may be present among these blocks.

P3) $1 < \alpha < n-1$. Besides the α elements from B^*, Z must now contain $n-\alpha$ elements from each one of the other blocks.
It follows:

- There is an x with $1 \leq x \leq n-1$ such that Z consists of Tx elements outside B^* and n-x elements inside B^*.

after these preparings we define a structure R over $C_n^T \oplus C_{kn}$ by canonical extension, as designed in (9) and (10)

(9) $$R = \underbrace{\binom{e_1}{k+1}\binom{e_1}{1}..\binom{e_1}{1}}_{n \text{ terms}} \cdots \underbrace{\binom{e_r}{k+1}\binom{e_r}{1}..\binom{e_r}{1}}_{n \text{ terms}} \underbrace{\binom{f}{\tau_1}\binom{f}{\tau_2}..\binom{f}{\tau_{n^*}}}_{n^* \text{ terms.}}$$

(10) If $n^* = n-1$, take $\tau_1 \equiv \ldots \equiv \tau_{n-1} \equiv T \bmod nk$
If $n^* = n$, take $\tau_1 \equiv k+1$, $\tau_2 \equiv \ldots \equiv \tau_n \equiv 1 \bmod nk$

There can be no ambiguity, as $n \geq 2$ and $n^* \geq 1$.

Let Q(Z) be a substructure of R, which is the extension of some zero-structure Z in (6).

In case P 1) we find that the sum-value of Q(Z) is $\binom{0}{\nu(k+n)}$ for some ν with $1 \leq \nu \leq nk-1$.

In case P 2) we have $n^* = n$ and find the value $\binom{0}{\mu(k+n)}$ for some μ with $1 \leq \mu \leq nk-1$.

These sums are not zero, as n + k is a generator of the additive group modulo kn (n coprime with k).

Hence R has no zero-substructures of type P 1) and type P 2).

In case P 3) let $\binom{0}{q}$ be the sum-value of Q(Z).

Here we are not able to evaluate q modulo nk, but we can do it modulo k.

If $n^* = n-1$, we find by (9) and (10):

$$q \equiv Tx.1 + (n-x)T \equiv nT \bmod k.$$

Hence, by (4), $q \equiv n(\rho-n) \bmod k$.

This cannot be zero if $\rho \not\equiv n \bmod k$.

If $n^* = n$ (which in case P 3) is certainly possible), we find:

$$q \equiv Tx.1 + (n-x).1 \equiv n-x(n-\rho+1) \bmod k.$$

This cannot vanish if condition (2) is fulfilled.

Hence, under the conditions of theorem (5,2) R is primitive over the group $C_n^T \oplus C_{nk}$.

On account of (8) the proof is now complete.

IV Upper estimates for $\lambda(G)$.

§ 7 Introduction.

Let G be an Abelian group with order $\Omega = \Omega(G)$ and with maximal element-order $m = m(G)$.

Let $\mu(G) = \lambda(G) + 1$, hence $\mu(G)$ is the minimal positive μ such that

$$g_1, g_2, \cdots, g_\mu \qquad (g_i \in G)$$

has always a subsequence which, under the operation in G, has the unit-element in G as its value. We shall prove:

Theorem (7,1)

$$\mu(G) \leq m(1 + \log \frac{\Omega}{m}).$$

Equality in this formula holds for cyclic groups, for there we have $\mu(G) = m$. For non-cyclic groups the sign $\leq$ improves itself to $<$, due to the irrationality of the right-hand member. The latter function is moreover $\leq \Omega$ as we have $\log x \leq x-1$ for $x \geq 1$. A further discussion will be given in § 12.

Theorem (7,1) will be proved, indirectly, by complete induction with regard to Ω , for a fixed value of m. This is not done by adding successive prime-factors, but by stepping from Ω to $\Omega+1$, where $\Omega+1$ of course is a pseudo-order. Exposition:

Theorem (7,2)

Let $\tau(l,m)$ $(l \geq 1,\ m \geq 1)$ be the combinatorial function which is to be defined in § 8 below. Then we have:

(11) $$\tau(l,m) \leq m(1 + \log \frac{l}{m}) \text{ for } l \geq m.$$

Theorem (7,3)

Let $\Omega = \Omega(G)$, $m = m(G)$, then

(12) $$\mu(G) \leq \tau(\Omega, m).$$

It is clear that (7,2) and (7,3) imply theorem (7,1).

§ 8 Description of the function $\tau(l,m)$.

We consider a finite matrix M with arbitrary things as elements, and define as a track in M any sequence which can be constructed under the following device:

> Choose, from left to right, one element from each column of M, such that identity holds for any two elements, which are taken from one and the same row.

Examples:

(13)
$$M_1 = \begin{matrix} a & a & a & a & b & c \\ d & e & d & e & d & f \\ p & q & p & q & p & q \end{matrix} \qquad M_2 = \begin{matrix} 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{matrix}$$

Among the tracks of M_1 are a a a a d q, d q d q b q and d q d q d q, but not p a d a p f. Matrix M_2 has tracks which are exactly situated like those in M_1. In fact, the two matrices are equivalent as to the problem of finding tracks, but M_1 is softer on the eye.

A matrix is called tractable if it has it least one track. Square and upstanding matrices are always tractable. The above notions are weatherbox-proof in both directions, hence by row-interchange and column-interchange any track can be presented as starting in the upper left corner of the matrix and ending somewhere in the final column, without ascendings underway.

A matrix M with length l and heigth h is called of type (l, h, m), if each row in M has <u>at most</u> m different elements. ($l \geq 1$, $h \geq 1$, $m \geq 1$). The same M belongs clearly to type (l, h, m+1) then. The triple of integers (l, h, m) is called tractable if all matrices of type (l, h, m) are tractable.

Together with (l, h, m) the triples (l-1, h, m), (l, h+1, m) and (l, h, m-1) will be tractable ($l \geq 2$, $m \geq 2$).

Triple (l, h, m) with $l \leq h$ is always tractable, but if $h < l \leq m$, the triple is not tractable , (take matrix with lh different elements).

Definition. $\tau(l,m)$ is the least positive integer h such that the triple (l,h,m) is tractable.

Basic properties: $\tau(l,m)$ is a non decreasing function in l and m separately. Further:

$$\begin{cases} \tau(l,m) \leq l \ ; \\ \tau(l,m) = l \quad \text{for } l \leq m \end{cases} \tag{14}$$

$$\tau(l,1) = 1 \tag{15}$$

$$\tau(m,m) = \tau(m+1, m) = m. \tag{16}$$

The function is interesting, if so, only for $l \geq m \geq 2$.

Lemma (8,1) Given $m \geq 2$ and $L \geq m+2$, there is an L^* with

$$m \leq L^* \leq \frac{m-1}{m} L \tag{17}$$

such that we have:

$$\tau(L,m) \leq \tau(L^*,m) + 1 \tag{18}$$

Proof: Put $L = qm + \sigma$ with $1 \leq \sigma \leq m$ and define L^* by $L^* = L - (q+1)$. Then we have:

$$\frac{L^*}{L} = 1 - \frac{q+1}{qm+\sigma} \leq 1 - \frac{1}{m} .$$

Further $L^* = q(m-1) + \sigma - 1 \geq m-1$. Here the sign of equality cannot hold, it would imply $q = 1$, $\sigma = 1$ and hence $L = m+1$, contradictory to our assumption $L \geq m+2$.
We have now proved that L^* satisfies (17).

Next we choose h so large that the triple (L^*, h, m) is tractable and we consider a matrice M of type $(L, h+1, m)$. Its first row contains a subsequence, say S, consisting of $q+1$ equal elements, otherwise we would have $L \leq qm$. We cancel those columns of M which intersect S and we cancel forthwith the whole first row of M. Now we are left with a matrix M^* of type (L^*, h, m), hence M^* is tractable. If we undo the cancellings, any track in M^*, united with S, becomes a track in M. Taking in particular $h = \tau(L^*,m)$, we find (18).

§ 9 Interlude for puzzlers.

The algorithm of the foregoing proof:

$$\left.\begin{array}{l} L = qm+\sigma \\ 1 \leq \sigma \leq m \end{array}\right\} \qquad L^{*} = L - (q+1)$$

is not uncommon in cocoa-nut-puzzles, where m missionaries take part in a store of cocoa-nuts, but an ape spoils the outcome every night, by taking away one of the participating nuts.

In our problem, the determination of $\tau(1,m)$, we deal with a fixed m (though in special cases m can be lowered during the work). By iteration procedure $(L, L^{*}, L^{**}, \ldots\ldots)$ one will find that $(2^k, k+1, 2)$ and $(9, 5, 3)$ are tractable. Hence $\tau(2^k,2) \leq k+1$ and $\tau(9,3) \leq 5$. The algorithm is too weak to show that $(6, 4, 4)$ is tractable, but this can be amended by direct verification. Then the algorithm gives that $(16, 7, 4)$ is tractable and it follows that $\tau(16, 4) \leq 7$. Those who are acquainted with the group-problem which is the subject of this report, will certainly have seen, that in the above three cases equality must apply as a consequence of (7.3) for special small groups. Next, let us try to find $\tau(27, 3)$. The algorithm gives here $\tau \leq 8$ and we know, by applying a certain group, that here $\tau \geq 7$. A sufficient condition

for $\tau \leq 7$ would be $\tau(8,3) \leq 4$. But recently E. LIEUWENS has studied the matrix

a a a b b c c c
p p q r r p q q
v w x v w x v w
s t v t s v s t

and has found that it is non-tractable. Hence we do not know whether $\tau(27,3) = 7$ or 8. An efficient computer algorithm for this track-function has been looked for, but not yet found.

§ 10 Proof of Theorem (7,2).

Cases $m = 1$; $l = m$; $l = m+1$ are dealt with by (15) and (16) . Hence we may assume $m \geq 2$. Furthermore we may assume that the assertion of the theorem is true for all l with

$$m \leq l \leq L-1 \qquad (m \text{ fixed}),$$

where L is some number $\geq m+2$. Under this assumption we proceed to prove it for $l = L$. We choose L^* according to lemma (8,1) and find by (17): $m \leq L^* \leq L-1$; hence assertion (7,2) is true for $l = L^*$

Denoting $m(1 + \log lm^{-1})$ by $f(l)$, we have:

$$f(L) - f(L^*) = m \log \frac{L}{L^*}$$

and hence, by (17):

$$f(L) - f(L^*) \geq m \log \frac{m}{m-1} = -m \log(1 - \frac{1}{m}) =$$

$$= 1 + \frac{1}{2m} + \frac{1}{3m^2} + \ldots\ldots > 1$$

Starting from (18) we find at last:

$$\tau(L,m) \leq \tau(L^*,m) + 1 \leq f(L^*) + 1 < f(L),$$

which completes the proof.

§ 11 Proof of Theorem (7,3).

The proof depends on basic properties of the group-characters of G into a projection field F. For F we may take the complex domain, as is habitual in textbooks. But our argument remains valid if we take for F a finite field of order $\equiv 1$ modulo m(G). Hence the proof does not range outside elementary combinatorics. See § 13 for comment, if needed.
We take G in the multiplicative version, so that we can use a group-algebra FG, where F is a field of the above description. We are interested in products of the form

$$(19) \qquad (g_1-z_1)\,(g_2-z_2)\,\ldots\,(g_h-z_h),\ (g_i \in G,\ z_i \in F),$$

the interest being due to the fact that $g_1, g_2, \ldots, g_h$ will have a subsequence with product-value 1 in all cases where (18) presents the zero in FG. The latter assertion is proved as follows (cf. OLSON [5]): If all the z_i are zero, the product (19) cannot be the zero of the algebra. Hence, if the product is zero, at least one of the z_i is $\neq 0$. We restrict our attention to those factors, where $z_i \neq 0$. There will be no loss of generality, and probably no confusion , if we denote their product again by (19), where now we may syppose that all $z_i \neq 0$.

Clearly, the product is equal to

$$\zeta_1 \bar{g}_1 + \zeta_2 \bar{g}_2 + \ldots + \zeta_n \bar{g}_n \pm z_1 z_2 \cdots z_h \ ,$$

where $n = 2^h-1$, the ζ_i are constants in F, and the $\bar{g}_i$ are subsequence products of $g_1, g_2, \ldots, g_h$. The final term is $\neq 0$ and it follows easily, that the whole form cannot be zero, unless at least one of the $\bar{g}_i$ is the unit-element of G, which is 1.
We give an example.

Take $G = \{1, g, g^2, g^3, g^4, g^5\}$ with $g^6 = 1$ and let F be the residue-system modulo 13.

Then we have:

$$g(g-1)(g+1)(g^2-3)(g^2+4) = 0 \text{ in } FG.$$

Indeed, the sequence g, g, g, g^2, g^2 has three subsequences with product value 1.

How do we find a sufficient condition for (19) to be 0 in FG? By a well-known principle of character theory (see § 13 if needed) we have the following criterium:

The product (19) presents the zero in FG if and only if the product

(20) $$(\chi(g_1) - z_1)(\chi(g_2) - z_2) \ldots. (\chi(g_h) - z_h)$$

vanishes in F for every group-character χ which maps G into $F \setminus \{0\}$.

How do we find a sufficient condition for (20) to be zero in F for any choice of χ? This is a question of factors 0, which will caper through (20) when the sequence $z_1, \ldots, z_h$ is chosen in a special way.

Let $\{\chi_1, \chi_2, \ldots., \chi_\Omega\}$ be the collection of all characters and let $g_1, g_2, \ldots, g_h$ be an arbitrary element-sequence over G. We consider the matrix

$$\begin{matrix} \chi_1(g_1) & \chi_2(g_1) & \ldots & \chi_\Omega(g_1) \\ \chi_1(g_2) & \chi_2(g_2) & \ldots & \chi_\Omega(g_2) \\ \vdots & & & \\ \chi_1(g_h) & \chi_2(g_h) & \ldots & \chi_\Omega(g_h). \end{matrix}$$

and we look back at § 8. Suppose that (21) has a track T, as defined in that section. Then we define a sequence $z_1, z_2, \ldots, z_h$ as follows:

If T does not intersect the α-th row of the matrix, put $z_\alpha = 0$.
If T does intersect the α-th row, put $z_\alpha = \chi^*$, where χ^* is the value of the elements in the intersection.

This sequence z_α, alloted to the given sequence g_α, makes (20) vanish uniformly as to the choice of χ. Hence the existence of a track T in (21) is sufficient for the existence of a sequence z_α, such that (19) presents the zero in the algebra FG. (As may be pointed out, it is necessary as well).

Of course, this criterium is conclusive for our problem. We have known from the beginning (but not used sofar) that all character-values lie in the root-group of the equation $z^m = 1$. It follows that (21) is a matrix of type (Ω, h, m). Hence if $h \geq \tau(\Omega,m)$, the matrix is tractable for whatever choice of the sequence $g_1, \ldots, g_h$; and (19) with proper $z_1, \ldots, z_h$ will be zero in FG.
This amounts to (7,3).

§ 12 Discussion of the upper estimate.

For cyclic groups we have $\mu(G) = m$. For non-cyclic groups, theorem (7,1) and subsequent remark give:

$$\frac{\mu(G) - m}{\log \Omega - \log m} < m. \tag{22}$$

On the other hand we have here:

$$\frac{p-1}{\log p} \leq \frac{\mu(G) - m}{\log \Omega - \log m}, \tag{23}$$

where p is the least non-trivial cycle-order in G. This is proved as follows:

Let $G \cong C_{d_1} \oplus \ldots\ldots \oplus C_{d_k}$ with $2 \leq d_1 \mid d_2 \ldots \mid d_k$,

then $k \geq 2$, $p \leq d_1$ and $d_k = m$.

Further $\mu(G) \geq M(G)$, where

$$M(G) = m + \sum_{i=1}^{k-1} (d_i - 1). \qquad \text{(see [2])}.$$

We note the fact that the function $\frac{x-1}{\log x}$ increases from its closure-value 1 to ∞ for $1 \leq x < \infty$ (put $x = e^u$), and find henceforth:

$$\mu(G) - m \geq M(G) - m \geq \frac{d_1 - 1}{\log d_1} \sum_{i=1}^{k-1} \log d_i \geq \frac{p-1}{\log p} \log \frac{\Omega}{m},$$

which proves (23)

A final remark as to the strength of (22). For any $\varepsilon > 0$ we can find a collection of groups G such that $m \to \infty$ and

$$\frac{\mu(G) - m}{\log \Omega - \log m} > (\tfrac{1}{2} - \varepsilon) \frac{m}{\log m},$$

while moreover all the G are excessive in the sense of § 5. The proof is left to the reader.

Now take groups G of type

$$C_m \oplus C_m \oplus \ldots\ldots \oplus C_m,$$

then we have $$\frac{\mu(G) - m}{\log \Omega - \log m} \geq \frac{m-1}{\log m},$$

with equality if m is a prime-power. There is a weak suggestion, just like in §§ 5, 6 that equality might hold here in all cases.

§ 13 Some remarks on group-characters.

The following approach to group-characters (added on request) is none too elegant, but it may suffice for readers who want to verify § 11 in a direct way.

Let G and R be multiplicative groups and let $\longleftrightarrow$ and $\longleftrightarrow\!\!\bullet\!\!\longrightarrow$ be isomorphisms, such that

$$G \longleftrightarrow C_{a_1} \oplus C_{a_2} \oplus \ldots\ldots \oplus C_{a_k} ,$$

$$R \longleftrightarrow\!\!\bullet\!\!\longrightarrow \{\frac{0}{m}, \frac{1}{m}, \ldots\ldots, \frac{m-1}{m}\}^{+} \text{ modulo } 1,$$

where m is the least common multiple of the a_i, hence $m = m(G)$. We consider a duality mapping χ of the lexicon G,G into R, where χ is defined as follows:

$$\chi(x,y) \longleftrightarrow\!\!\bullet\!\!\longrightarrow \frac{\xi_1\eta_1}{a_1} + \frac{\xi_2\eta_2}{a_2} + \ldots\ldots + \frac{\xi_k\eta_k}{a_k}$$

with $x \longleftrightarrow (\xi_1, \ldots\ldots, \xi_k)$ and $y \longleftrightarrow (\eta_1, \ldots\ldots, \eta_k)$.

By straightforward reasoning one will find that any homomorphism of G into R must be of type $\chi(x_0, y)$ for some fixed $x_0 \in G$. Moreover, if $x_0 \neq x_1$, the mappings $\chi(x_0, y)$ and $\chi(x_1, y)$ are not identical. It follows that there are precisely Ω homomorphic mappings. If $G = \{x_1, x_2, \ldots, x_\Omega\}$ then

$$\{(\chi(x_0,y) , \chi(x_1,y) \ldots\ldots\ldots \chi(x_\Omega,y)\}$$

is the collection of all homomorphisms of G into R.

Next, let F be either the complex domain, or a finite field of order $\equiv 1$ modulo m. Then the equation $Z^m = 1$ has m roots in F and the roots' group is cyclic. Let us denote this group by R. Under isomorphism $\longleftrightarrow\!\!\bullet\!\!\longrightarrow$ we find Ω group-characters (= homomorphisms) of G into R, and they are at once all the characters of G into the multiplication group of F.

Now the sum-formula of finite geometric sequences leads up to:

$$\sum_{y \in G} \chi(x,y) \quad \begin{cases} = \Omega & \text{if } x = 1 \longleftrightarrow (0, 0, \ldots, 0) \\ = 0 & \text{if } x \neq 1 \end{cases}$$

These are fundamental relations. The fact should be marked that $\Omega \neq 0$ in F. If F is finite, this is by no means trivial, but it follows from the fact that any prime divisor of Ω is a prime-divisor of m. If the characteristic prime of F were a divisor of Ω, it would divide m and this is not possible.

The fundamental relations imply the truth of the following statement:

$$\text{If} \quad \sum_{x \in G} f(x)\, \chi(x,y) = 0 \text{ for all } y, \quad (f : G \to F)$$

$$\text{then } f(x) = 0 \text{ for all } x \in G.$$

(The proof proceeds by orthogonal inversion: multiply the sum $\sum$ by a factor $\chi(x_0^{-1},y)$; next take a summation over all y and divide by Ω).

This character-proposition is all we need for the establishing of (20). Any element of the algebra FG has a linear presentation of the form

$$\sum_{x \in G} \zeta_x\, x \qquad (\zeta_x \in F).$$

The calculus of homomorphic substitution will do the rest.

References

1. P.C. Baayen. $C_2 \oplus C_2 \oplus C_2 \oplus C_{2m}$!
ZW-1969-006.

2. P. van Emde Boas. A Combinatorial problem on finite Abelian Groups II, Math. Centre Report ZW-1969-007.

3. P. van Emde Boas , E. Wattel. Een structuurprobleem opgelost voor $C_3 \oplus C_3 \oplus C_6$. WN 26.

4. P. van Emde Boas. Some Combinatorial properties of the group $C_3 \oplus C_3 \oplus C_3$.
ZW-1969-010.

5. J.E. Olson. A combinatorial problem on finite Abelian groups. Journal of Number theory 1 (1969) 8-11.