STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM
AFDELING ZUIVERE WISKUNDE

ZW 1969 - 007

A Combinatorial problem on finite Abelian Groups II

by

P. van Emde Boas.

June 1969

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

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) and the Central Organization for Applied Scientific Research in the Netherlands (T.N.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

§ 0. Introduction.

This report studies the following combinatorial problem on finite Abelian groups:

Let G be a finite Abelian group of order $\omega(G)$. We ask for a minimal positive integer n such that any sequence $a_1, \ldots, a_n$ of elements from g contains a non empty subsequence with sum zero. This minimal n is a constant of the group g which we denote by $\mu(G)$.

The problem is to express $\mu(G)$ by means of other constants of the group. Let $G = C_{d_1} \oplus C_{d_2} \oplus \ldots\ldots \oplus C_{d_k}$ where $d_1 \mid d_2, d_2 \mid d_3, \ldots - \ldots, d_{k-1} \mid d_k$ and where C_{d_i} denotes the cyclic group of order d_i. (It is well known that any finite Abelian group has a unique representation of this form). Then we can define the following constant of G:

$$M(G) = d_1 + d_2 + \ldots\ldots + d_k - k + 1.$$

It was conjectured in 1965 by P.C. BAAYEN that for all groups G we have equality $\mu(G) = M(G)$. This general conjecture however had to be rejected when he proved in May 1969 that for $G = C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_6$ we have $\mu(G) > M(G)$.

The equality $\mu(G) = M(G)$ holds for a impressive collection of groups. We mention the following cases:

I G is an Abelian p-group (i.e. the integers d_j are powers of some fixed prime)

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

V $G = C_2 \oplus C_{2nm_1} \oplus C_{2nm_2}$ with $n = 2^{k_1}.3^{k_2}.5^{k_3}.7^{k_y}$ and either $m_1 = 1$, m_2 arbitrary or $m_1 = p^r$ and $m_2 = p^s$.

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

The problem together with some elementary results was first published in 1967 [8] . At the same time the results I and II were proved independently by J.E. OLSON [19] and D. KRUYSWIJK [1]. The results III, IV and V were proved in spring 1968 by P.C. BAAYEN, J.H. VAN LINT and the author. [1], [2] [12] [13]. Finally the series VI and the first counter-example was found by P.C. BAAYEN May 1969 [3] [4] [5].

An upper estimate for $\mu(G)$ was given by J.E. OLSON [19]. He gives

$$\mu(G) \leq \omega(H) + \omega(K) - 1 \qquad \text{when } G = H \oplus K$$

$$\text{and } \omega(H) \mid \omega(K).$$

Recently D. KRUYSWIJK proved the following upper estimate (to be published in a forth coming report [5]):

$$\mu(G) \leq \omega(C) \{1 + \log \omega(H)\}$$

where $G = H \oplus C$ and C is isomorphic with a maximal cyclic subgroup of G.

This result implies, in our notation:

$$\mu(G) = d_k + \sigma \log \frac{\omega(G)}{d_k}$$

with $$\frac{d_1 - 1}{\log d_1} \leq \sigma \leq d_k$$

hence it gives a reasonable result for "homogeneous" groups (where $d_1 = d_2 = \ldots = d_k$).

For the special case $G = C_p \oplus C_p$ equality $\mu(G) = M(G)$ was conjectured earlier by P. ERDÖS. In 1961 P. ERDÖS , A. GINSBURG and A. ZIV published the following result: [10].

Let G be the group $C_n \oplus C_n$ and let H be some cyclic subgroup of order n. Then any sequence of length $2n - 1$ consisting of elements <u>from a fixed coset of H</u> contains a subsequence with sum zero.
The same result was proved by N.G. DE BRUIJN.

Another special case results when the elements a_n are supposed to be distinct. In 1967 H.B. MANN and J.E. OLSON published the following result [15] :

Let $G = C_p + C_p$ then any sequence of distinct elements with length $\geq 2p - 2$ contains a subsequence with sum zero.

For related problems see [14] [17] [18].

The constant μ has some connection with problems in Algebraic number theory as has been stated by H. DAVENPORT [7]. Let G be the class-group of an Algebraic number field F, then $\mu(G)$ is the maximal number of prime ideals (counting multiplicity) in the decomposition of an irreducible integer in F. See Section 6.

J.E. OLSON [19] has given the following application in theory of Vector spaces over finite fields:

Let V be an k-dimensional vector space over $\mathbb{F}_{p^l}$ and let $x_1, \ldots, x_k$ be a base for V. Define the unit polytope V to be the collection of all elements $x = \varepsilon_1 x_1 + \ldots\ldots + \varepsilon_k x_k$ with $\varepsilon_j = 0$ or 1. Let A be an arbitrary k - n dimensional subspace of V. Then the intersection $V \cap A$ contains at least

$$\max \{ 1 , 2^{k - n.l.(p-1)} \} \quad \text{points.}$$

Part of this application was also given in [8].

For the proofs of the cases II, III, IV and V we use some other properties which are shared by some but not all Abelian groups.

(A) Let $G = C_{d_1} + \ldots + C_{d_k}$, $d_1 \mid d_2 \mid \ldots\ldots \mid d_k$ then any sequence of length $\geq M(G) + d_k - 1$ contains a non empty subsequence with sum zero of length $\leq d_k$.

Property (A) is shared by all p-groups such that $2 d_k \geq M(G) + 1$ and by all groups with $k \leq 2$, but for example not by $G = (C_2)^3$.

A sequence S of length $\mu(G) - 1$ which contains no subsequences with sum zero has the property that any element of G exept zero turns up as the sum of some subsequence of S. For sequences of length $\mu(G) - 2$ without zero-subsequences there may exist "holes". Property (B) now states:

(B) Any sequence of length $M(G) - 2$ which contains no subsequences with sum zero has all its "holes" contained in some fixed proper coset of an subgroup $H \subset G$.

Property B) is actually stronger then the equality $\mu(G) = M(G)$. It is shared by all p-groups and by all groups $C_{d_1} \oplus C_{d_2}$ with $d_1 = n\, m_1 \quad d_2 = n\, m_2$, provided that:

(1) either $m_1 = p^{l_1} \quad m_2 = p^{l_2}$ or $m_1 = 1$ and m_2 arbitrary

(2) all prime factors of n have the following property (C)

(C) Each sequence of length $3p - 3$ of elements from $C_p \oplus C_p$ which contains no zero-subsequences of length $\leq p$ and which contains no two disjoint zero-subsequences consists of three distinct elements each taken $p - 1$ times.

This property has been verified by calculation (for $p = 7$ by means of the X - 8 computer at the Mathematical Centre [9]) for the primes $p = 2, 3, 5$ and 7.

Author conjectures (C) to hold for all primes.

Property (B) is not shared by groups for which $M(G) < \mu(G)$. It is an open problem wether (B) holds for all groups G with $M(G) = \mu(G)$ or wether (B') holds for all groups if (B') is derived from (B) by writing "$\mu(G) - 2$" instead of "$M(G) - 2$".

In this report we give proofs of the results I, II, III, IV and V. Further we give proofs of J.E. OLSONS's upper estimate and the stated applications.
For the other results the litterature is given in the references.

§ 1 Definitions and elementary results.

Let A be an arbitrary set. An A-sequence S is a finite sequence of elements of A. (the possibility of repetitions is not excluded). The sequence may be empty, in which case we write $S = \emptyset$.

Let $S = (a_1, \ldots, a_k)$. The integer k is called the length of S - notation $l(S)$.
We put $l(\emptyset) = 0$.
A subsequence T of S - notation $T \leq S$ is an A-sequence

$$T = (a_{i_1}, \ldots, a_{i_s}) \quad \text{with } 1 \leq i_1 < \ldots < i_s \leq k$$

For each subset of the set of integers $\{1, \ldots, k\}$ there exist a corresponding subsequence of S. This makes it possible to define the set theoretical notions "union" , "intersection" , "difference" and "disjoint" for the collection of all subsequences of S by means of this correspondence.

From now on we suppose A to be some subset of a finite Abelian group $G = \{G, +, 0\}$. of order $\omega(G)$.
The value of an A-sequence S - notation $|S|$ is the group element

$$|S| = a_1 + \ldots + a_k \quad \text{when } S = (a_1, \ldots, a_k)$$

$[S]$ denotes the subset of G consisting of the value's of non empty subsequences of S:

$[S] := \{|T| \mid T \leq S \text{ and } T \neq \emptyset\}$

We put $[S]^* := [S] \cup \{0\} = \{|T| \mid T \leq S\}$.

Remark that we have for disjoint S_1 and $S_2 \leq S$:

$$[S_1 \cup S_2] = ([S_1]^* + [S_2]) \cup ([S_1] + [S_2]^*)$$

$$= [S_1] \cup [S_2] \cup ([S_1] + [S_2])$$

A subsequence T with $|T| = 0$ is called a zero-subsequence.

An A-sequence S is called primitive iff $0 \notin [S]$. If S is primitive and is not contained in some primitive A-sequence T with $l(T) > l(S)$ is called A-maximal. With maximal we mean G-maximal. S is called irreducible iff $|S| = 0$ and each proper subsequence of S is primitive. An hole of S is an element $g \in G$ which is not contained in $[S]^*$

We put $[S]_m = \{|T| \mid T \leq S \text{ and } 0 < l(T) \leq m\}$

and $[S]_m^* = [S]_m \cup \{0\}$.

Let $G = C_{d_1} \oplus C_{d_2} \oplus \dots \oplus C_{d_k}$ where

$1 < d_1 \mid d_2 \mid \dots \mid d_k$ and where C_{d_i} denotes the cyclic group of order d_i.

It is well known that the integers d_i and the number k are constants of the group G. This follows from the main theorem on finite Abelian groups. We call the numbers d_i the chain-invariants of G; k is called the dimension of G.

Some times it is permitted that $d_1 = 1$. The representation of G is not unique in this case but the following two constants stay uniquely determined:

$\Lambda(G) := d_1 + d_2 + \dots + d_k - k$

$M(G) := \Lambda(G) + 1 = d_1 + d_2 + \dots + d_k - k + 1$.

We are interested in upper bounds of the length of irreducible or primitive G-sequences. That such upper bounds exist follows from the following proposition:

(1.1) proposition If S is an irreducible or primitive G-sequence then $l(S) \leq \omega(G)$

proof: Suppose $l(S) \geq \omega(G) + 1$. We consider the elements:

a_1, $a_1 + a_2$, $a_1 + a_2 + a_3$, ..., $a_1 + a_2 + \dots + a_{l(S)}$

These are $> \omega(G)$ elements in a group of order $\omega(G)$ hence at least two of them are equal. Let

$a_1 + a_2 + \dots + a_i = a_1 + a_2 + \dots + a_{i+j}$ then

$a_{i+1} + \dots + a_{i+j} = 0$ and therefore S is neither primitive nor irreducible.

proposition (1.1) justifies the following definitions:

$\lambda(G,A)$ is the maximal length of a primitive A-sequence. We put $\lambda(G) := \lambda(G,G)$.
Analogeous we denote by $\mu(G,A)$ the maximal length of an irreducible A-sequence and again we put $\mu(G) = \mu(G,G)$.

The relations between $\lambda(G,A)$ and $\mu(G,A)$, $\lambda(G)$ and $\mu(G)$ given by:

(1.2) <u>proposition</u> $\mu(G) = \lambda(G) + 1$

<u>proof</u>: Let S be primitive then the sequence $S \cup \{-|S|\}$ is irreducible. Conversily let T be an irreducible sequence then each subsequence of length $l(T) - 1$ is primitive.
Hence we have $\mu(G) \geq \lambda(G) + 1$ and
$\lambda(G) \geq \mu(G) - 1$
which proves the proposition.

<u>remark</u>: from (1,2) it follows that $\mu(G)$ can also be defined as the least integer k with the property that each G-sequence of length $\geq k$ contains a zero-subsequence.

<u>remark</u>: the inequality $\lambda(G,A) \geq \mu(G,A) - 1$ is proved analogeous as (1,2). However the inequality $\mu(G,A) \geq \lambda(G,A) + 1$ is not generaly true. See after (1.15)

(1.3) <u>proposition</u> $\lambda(G,A) \leq \lambda(G)$

(1.4) <u>propositon</u> $\mu(G,A) \leq \mu(G)$

These propositions follow trivially by considering A-sequences to be G-sequences; remark however that an A-maximal sequence is not necessary also maximal

(1.5) <u>corollary</u> $\lambda(G) \leq \omega(G) - 1$, $\mu(G) \leq \omega(G)$

That these upper estimates sometimes are the best possible follows from the next proposition:

(1.6) <u>proposition</u> $\mu(C_m) \geq \omega(C_m) = m$

<u>proof</u>: The sequence $\underbrace{(a, a, \ldots\ldots, a)}_{mx}$

where a is a generator of C_m is irreducible.

Hence (by (1.5)) $\mu(C_m) = m = M(C_m)$ and

$$\lambda(C_m) = m-1 = \Lambda(C_m).$$

The converse of (1.6) holds also:

(1.7) <u>proposition</u>: If $\mu(G) = \lambda(G)$ then G is a cyclic group

<u>proof</u> Let $S = (a_1, a_2, \ldots, a_m)$ be an irreducible G-sequence with $m = \omega(G)$. We prove all elements to be equal. The unique element $a = a_i$ is clearly an element of order $m = \omega(G)$ and therefore G is cyclic. Suppose therefore that S contains two different elements. Without loss of generality we may assume $a_1 \neq a_2$.

Now consider the two collections of elements:

$$B_1 = \{a_1, a_1+a_3, a_1+a_3+a_4, \ldots\ldots, a_1+a_3+a_4+ \ldots\ldots + a_m\}$$
$$B_2 = \{a_2, a_2+a_3, a_2+a_3+a_4, \ldots\ldots, a_2+a_3+a_4+ \ldots\ldots + a_m\}.$$

By the irreducibillity of S it follows that both sets B_1 and B_2 consist of the $\omega(G) - 1$ non-zero elements of G. Thus B_1 contains the element $a_1 - a_2 \neq 0$. As $a_1 - a_2 \neq a_1$ we have $a_1 - a_2 = a_1 + a_3 + a_4 + \ldots\ldots + a_i$ for some $i \geq 3$. But then we derive $a_2 + a_3 + a_4 + \ldots\ldots + a_i = 0$ which contradicts the irreducibillity of S.

(1.8) <u>corollary</u>: $\mu(G) = \omega(G)$ iff G is a cyclic group.

Another case where the equality $\mu(G) = M(G)$ is almost trivial is the case $G = (C_2)^k$. We may assume G to be the additive group from the k-dimensional vector space over $\mathbb{F}_2$.

The only scalars in F_2 are 0 and 1. From this it follows that a sequence $(a_1, \ldots\ldots, a_m)$ is primitive iff its elements are linear independent over $\mathbb{F}_2$. Thus follows

(1.9) <u>proposition</u> $\lambda((C_2)^k) = \Lambda((C_2)^k)$

<u>proof</u>: we have $\lambda((C_2)^k) = \dim (\mathbb{F}_2\ )^k = k = k(2-1) = \Lambda((C_2)^k)$.

In the sequal we will represent the elements of the group $G = C_{d_1} \oplus C_{d_2} \oplus \ldots\ldots \oplus C_{d_k}$, $d_i > 1$ by a "vectorlike" notation:

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} \qquad \text{with } 0 \leq x_j < d_j$$

Addition is performed coordinate-wise:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_k \end{pmatrix} \qquad \text{where } z_i \equiv x_i + y_i \pmod{d_i}$$

We denote the "base"-elements by $e_1, \ldots, e_k$ and the "diagonal"-element by e_0 :

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ \ldots\ldots, \ e_k = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}, \quad e_0 = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

The following propositions give some value's of $\lambda(G,A)$ and $\mu(G,A)$ for special choices of A. Let A_1 be the set of "base"-elements : $A_1 = \{e_1, \ldots, e_k\}$ and let A_2 be the set of base elements together with the diagonal element : $A_2 = \{e_0, e_1, \ldots, e_k\}$ then we have the following relations:

(1.10) <u>proposition</u> $\lambda(G,A_1) = \Lambda(G)$

(1.11) <u>proposition</u> $\mu(G,A_1) = d_k$

(1.12) <u>proposition</u> $\mu(G,A_2) = M(G)$

(1.13) <u>proposition</u> $\lambda(G,A_2) = \Lambda(G)$

<u>proof</u>: An A_1-sequence is primitive iff it contains each element e_j at most $(d_j - 1)$ times. This proves (1.10). An A_1-sequence is irreducible iff it contains a fixed element e_j exactly d_j times and (1.11) follows.

The sequence S defined by

$$S = (e_0, \underbrace{e_1 \ldots\ldots e_1}_{(d_1-1)x}, \underbrace{e_2 \ldots\ldots e_2}_{(d_2-1)x}, \ldots\ldots, \underbrace{e_k \ldots\ldots e_k}_{(d_k-1)x})$$

is an example of an irreducible A_2-sequence of length M(g) all other irreducible A_2-sequneces that are not A_1-sequences are of the form:

$$S_t = (\underbrace{e_0 \ldots\ldots e_0}_{tx}, \underbrace{e_1 \ldots\ldots e_1}_{f_1 x}, \ldots\ldots, \underbrace{e_k \ldots\ldots e_k}_{f_k x})$$

where the t, f_i are determined by

$0 \leq t \leq d_k$, $f_k = d_k - t$, and

$f_j + t \equiv 0 \pmod{d_j}$, $0 \leq f_j < d_j$ for $1 \leq j < k$

Thus $f_1 + \ldots\ldots + f_k + t \leq (d_1-1) + (d_2-1) + \ldots\ldots + (d_{k-1}-1) + d_k = M(G)$

As $\mu(G,A_1) = d_k \leq M(G)$ this proves (1.12).

The proof of (1.13) is less trivial. We put

$$d_1 = d_2 = \ldots = d_{j_1} < d_{j_1+1} = \ldots\ldots = d_{j_2} < d_{j_2+1} = \ldots < \ldots < \ldots = d_{j_s} = d_k$$

Suppose S is a primitive A_2-sequence :

$$S = (\underbrace{e_0 \,\ldots\ldots\, e_0}_{t\,x}, \underbrace{e_1 \,\ldots\ldots\, e_1}_{f_1\,x}, \ldots\ldots, \underbrace{e_k \,\ldots\ldots\, e_k}_{f_k\,x})$$

Without loss of generality we may assume that for each i $0 \leq i \leq s-1$ we have:

$$f_{j_i+1} \geq f_{j_i+2} \geq \ldots\ldots \geq f_{j_{i+1}} = g_i$$

This implies:

$$l(S) = f_1 + \ldots + f_{j_1} + f_{j_1+1} + \ldots + f_{j_2} + \ldots\ldots + f_{j_{s-1}} + f_{j_{s-1}+1} + \ldots$$

$$+ \ldots + f_{j_s} + t \leq$$

$$\leq (d_{j_1}-1) + \ldots + (d_{j_1}-1) + g_1 + (d_{j_2}-1) + \ldots + g_2 + \ldots\ldots + g_{s-1} + (d_k-1) +$$

$$+ \ldots + g_s + t =$$

$$= \Lambda(G) - ((d_{j_1}-1) + (d_{j_2}-1) + \ldots + (d_{j_s}-1) - (g_1 + g_2 + \ldots\ldots g_s + t))$$

We see that (1.13) is a consequence of the following lemma:

(1.14) <u>Lemma</u> Suppose $t + g_1 + g_2 + \ldots\ldots + g_s > d_{j_1} + d_{j_2} + \ldots + d_{j_s} - s$ then S is not primitive.

For assuming lemma (1.14) we see that "S is primitive" implies $t + g_1 + \ldots\ldots + g_s \leq d_{j_1} + \ldots\ldots + d_{j_s} - s$ thus

$$l(S) \leq \Lambda(G) + (t + g_1 + \ldots + g_s - (d_{j_1} + \ldots + d_{j_s} - s)) \leq$$
$$\leq \Lambda(G)$$

which had to be proved.

<u>Proof of lemma (1.14)</u>: We put $v = t + g_1 + \ldots + g_s - (d_j + \ldots + d_{j_s} - s)$.

(A_s) Suppose now $v > 0$

As we have $g_i \leq d_{j_i} - 1$ we derive

$$v_1 := t + g_s - (d_{j_s} - 1) \geq v > 0$$

Now consider the following subsequences of S

$$S_t^{(0)} = (\underbrace{e_0 \ldots e_0}_{tx}, \underbrace{(e_k, e_{k-1}, \ldots, e_{j_{s-1}+1}), (e_k, e_{k-1}, \ldots, e_{j_{s-1}+1}), \ldots, (e_k, e_{k-1}, \ldots, e_{j_{s-1}+1})}_{(d_{j_s} - t)x})$$

$$\vdots$$

$$S_{t-v_1+1}^{(0)} = (\underbrace{e_0 \ldots e_0}_{(t-v_1+1)x}, \underbrace{(e_k, \ldots, e_{j_{s-1}+1}), (e_k, \ldots, e_{j_{s-1}+1}), \ldots, (e_k, \ldots, e_{j_{s-1}+1})}_{g_s\, x})$$

These subsequences have the property that their values

$$|S_{t-\nu}^{(0)}| = \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \qquad \text{with} \qquad \begin{array}{l} x_j = 0 \text{ for } j_{s-1}+1 \leq j \leq k \text{ and} \\ x_j \equiv t-\nu \pmod{d_j} \text{ for } 1 \leq j \leq j_{s-2} \end{array}$$

There are two possibilities:

(B_{s-1}) One of the integers $t, t-1, \ldots, t-\nu_1+1$ say $t-\nu$ is congruent zero mod $d_{j_{s-1}}$

In this case $S_{t-\nu}^{(0)}$ is a zero-subsequence and S is not primitive (G)

(A_{s-1}) Each of the integers $t, t-1, \ldots, t-v_1+1$ is incongruent zero (mod $d_{j_{s-1}}$)

Now we put $t_1 \equiv t \pmod{d_{j_{s-1}}}$ $\quad 0 < t_1 < d_{j_{s-1}}$ and we conclude $t_1 \geq v_1$

Therefore we may define:

$$v_2 := \min (v_1, t_1 + g_{s-1} - (d_{j_{s-1}} - 1)) \geq v > 0$$

We consider again the following subsequences of S:

$$S_t^{(1)} = S_t^{(0)} \cup ((\underbrace{(e_{j_{s-1}}, \ldots\ldots, e_{j_{s-2}+1}), \ldots\ldots, (e_{j_{s-1}}, \ldots\ldots, e_{j_{s-2}+1})}_{(d_{j_{s-1}} - t_1)x})$$

$$\vdots$$

$$S_{t-v_2+1}^{(1)} = S_{t-v_2+1}^{(0)} \quad (\underbrace{(e_{j_{s-1}}, \ldots, e_{j_{s-2}+1}), \ldots\ldots, (e_{j_{s-1}}, \ldots, e_{j_{s-2}+1})}_{(d_{j_{s-1}} - t_1 + v_2 - 1)x})$$

These sequences have the property:

$$|S_{t-\nu}^{(1)}| = \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \quad \text{with} \quad \begin{array}{l} x_j = 0 \quad \text{for } j_{s-2} + 1 \leq j \leq k \\ \text{and } x_j \equiv t-\nu \pmod{d_j})| \text{ for } 1 \leq j \leq j_{s-2} \end{array}$$

Again there are two possibillities:

(B_{s-2}) One of the integers $t, t-1, \ldots, t-v_2+1$ say $t-\nu$ is congruent zero (mod $d_{j_{s-2}}$).

(A_{s-2}) Else.

In the case (B_{s-2}) we see that $|S_{t-\nu}^{(1)}| = 0$ (G).
In the case (A_{s-2}) we proceed as before:

Put $t_2 \equiv t \pmod{d_{j_{s-2}}}$ and $0 < t_2 < d_{j_{s-2}}$; again we have $t_2 \geq v_2$ and therefore

$v_3 := \min (v_2, t_2 + g_{s-2} - (d_{j_{s-2}} - 1)) \geq v > 0$ and we consider again subsequences $S_{t-\nu}^{(2)}$ etc.....

Proceeding as indicated either we succeed in constructing a zero-subsequence of S or we go on until we have performed s steps. Then we are ready also because each sequence $S^{(s-1)}_{t-\nu}$ is a zero-subsequence. Hence S is not primitive.

remark : The logical scheme of the proof is indicated by the following diagram:

$$\begin{tikzcd}
(A_s) \arrow[r] \arrow[dr, "\text{or}"'] & (A_{s-1}) \arrow[r] \arrow[dr, "\text{or}"'] & (A_{s-2}) \arrow[r] \arrow[dr, "\text{or}"'] & \cdots \arrow[r] & (A_1) \arrow[r] & (G) \\
 & (B_{s-1}) \arrow[dr] & (B_{s-2}) \arrow[dr] & (B_{s-3}) \arrow[dr] & & \\
 & & (G) & (G) & (G) &
\end{tikzcd}$$

(1.15) corollary: For any group G $\Lambda(G) \leq \lambda(G)$ and $M(G) \leq \mu(G)$

proof: follows directly from (1.10) and (1.12) by (1.3) and (1.4).

remark: (1.10) and (1.11) give a general example where $\lambda(G,A) + 1 > \mu(G,A)$

We have the following generalisation of (1.10).

(1.16) proposition: Let $G = H \oplus K$ then $\lambda(G) \geq \lambda(H) + \lambda(K)$

proof: Let $S_1 = (x_1, \ldots, x_{\lambda(H)})$ be a primitive H-sequence and let $S_2 = (y_1, \ldots, y_{\lambda(K)})$ be a primitive K-sequence then also the following sequence S of length $\lambda(H) + \lambda(K)$ is primitive:

$$S = \left(\begin{pmatrix} x_1 \\ 0 \end{pmatrix} \begin{pmatrix} x_2 \\ 0 \end{pmatrix} \cdots \begin{pmatrix} x_{\lambda(H)} \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ y_1 \end{pmatrix} \cdots\cdots \begin{pmatrix} 0 \\ y_{\lambda(K)} \end{pmatrix} \right)$$

remark: (1.15) can be derived directly from (1.16)

remark: it is generally not true that $\Lambda(H \oplus K) = \Lambda(H) + \Lambda(K)$ even not when we suppose $\omega(H) \mid \omega(K)$.

Take for example $K = C_{50} \oplus C_2$ and $H = C_{10} \oplus C_5$

Then we have $H \oplus K = C_{50} \oplus C_{10} \oplus C_{10}$ while

$$50 + 13 = \Lambda(H) \oplus \Lambda(K) < \Lambda(H \oplus K) = 67$$

It is however true that $\Lambda((G)^n) = n \Lambda(G)$ for any group G.

An upper estimate $\mu(G \oplus H) \leq \mu(G) . \mu(H)$ is derived in section 3.

From (1.2) we derive that for any primitive G-sequence S of length $\lambda(G)$ we have $[S]^* = G$. In section 4 and 5 we shall consider primitive sequences of length $\lambda(G) - 1$. It has been conjectured by P.C. BAAYEN that for any primitive G-sequence of length $\Lambda(G) - 1$ the holes of S are contained in a proper coset of some subgroup $N \subsetneq G$.

We define a new constant $\nu(G)$:

$\nu(G)$ is the minimal integer k such that any G-sequence S of length $\geq k$ either is not primitive or has all its holes in a proper coset of some subgroup N of G (which may depend on S)

(A proper coset of a subgroup N is a set $a + N$ for some $a \notin N$)

It is clear that $\nu(G) \leq \lambda(G)$.
Taking A_1 as before it is also easy to find a A_1-sequence of length $\Lambda(G) - 2$ which is primitive and such that not all its holes are contained in some proper coset.
Thus $\nu(G) \geq \Lambda(G) - 1$. This last fact can also be derived from proposition (1.17).

(1.17) <u>proposition</u>: $\nu(G) \geq \lambda(G) - 1$

<u>proof</u>: Consider a primitive G-sequence of length $\nu(G)$. Suppose S is not maximal.

Then all holes of S are contained in some proper coset $a + N$, $a \notin N \subseteq G$. Let $S \cup \{x\}$ be a primitive G-sequence extending S then it follows that $x \equiv -a \pmod N$ and therefore $x \not\equiv 0 \pmod N$. Therefore $(a-x) + N \subset [S]^*$ thus $[S \cup \{x\}] \supset a + N$. This implies $[S \cup \{x\}]^* = G$.

It follows that any primitive g-sequence of length $\nu(G) + 1$ is maximal. Hence $\lambda(G) \leq \nu(G) + 1$.

(1.18) <u>corollary</u>: For all groups G with $\nu(G) = \Lambda(G) - 1$ we have $\lambda(G) = \Lambda(G)$.

<u>proof</u>: $\lambda(G) \geq \Lambda(G)$ by (1.16) while $\lambda(G) \leq \nu(G) + 1 = \Lambda(G)$ by (1.17).

(1.18) shows that the conjecture $\nu(G) = \Lambda(G) - 1$ is actually stronger then the conjecture $\lambda(G) = \Lambda(G)$.
It is therefore not generally true.

(1.19) <u>proposition</u>: For any cyclic group G we have $\nu(G) = \Lambda(G) - 1$

<u>proof</u>: Let S be a primitive C_m sequence of length $m - 2$. Suppose S is not maximal, then there exist an element $a \in G$ $a \not\equiv 0$ such that $-a \notin [S]^*$ and therefore $S \cup \{a\}$ is primitive also. It follows that $S' = S \cup \{a\} \cup \{-|S \cup \{a\}|\}$ is an irreducible sequence of length m . As shown in (1.7) S' contains a fixed generator of C_m m times thus S contains m-2 times the element a. From this we deduce that the unique hole of S is the element $-a$ which forms the proper coset $-a + \{0\}$.

(1.20) <u>proposition</u>: For $G = (C_2)^k$ we have $\nu(G) = \Lambda(G) - 1$

<u>proof</u>: Let S be a primitive $(\mathbb{F}_2)^k$ - sequence of length k - 1 then the elements of S are linear independent and their linear closure is a subspace A of dimension k-1. Thus all holes of S are contained in the proper coset $(\mathbb{F}_2)^k \setminus A = A + x$ for some $x \notin A$.

§ 2 p-groups.

The main result considered in this section is the theorem:

(2.1) Theorem [J.E. OLSON] For any Abelian p-group G the equality $\lambda(G) = \Lambda(G)$ is true.

This result was obtained independently by D. KRUYSWIJK and J.E. OLSON using essentially the same methods. The same procedure was used to prove the equality $\nu(G)\ G\Lambda(G) - 1$ for p-groups which was needed for the proof of case IV.

For an "homogeneous" p-group $G = C_p \oplus \ldots\ldots \oplus C_p$ another proof was suggested by H. DAVENPORT . The method is based on the following theorem of C. CHEVALLEY (See [6] and also [11]).

(2.2) Theorem [C. CHEVALLEY] Let $f_1, \ldots\ldots, f_m$ be polynomials from $\mathbb{F}_{p^k}[X_1, \ldots\ldots, X_n]$ of degrees $d_1, \ldots\ldots, d_m$ such that $f_1(0,0,\ldots,0) = f_2(0,0,\ldots,0) = \ldots\ldots = f_m(0,0,\ldots\ldots,0) = 0$ and $d_1 + d_2 + \ldots\ldots + d_m < n$.
Then there exist a non-zero solution of the equations

$$f_i(x_1, \ldots\ldots, x_n) = 0 \qquad 1 \leq i \leq m \qquad \text{(a)}$$

proof: We consider the following function

$$\psi = \mathbb{N} \longrightarrow \mathbb{F}_{p^k}$$

$$\psi(n) := \sum_{x \in \mathbb{F}_{p^k}} x^n$$

It follows that $\psi(i) = 0$ iff $p^k - 1 \nmid i$

and $\psi(i) = -1$ iff $p^k - 1 \mid i$

We put $\psi(0) = 0 = \sum_{x \in \mathbb{F}_{p^k}} 1$

By straightforward calculation one sees:

$$\sum_{(x_1,\ldots,x_n) \in (\mathbb{F}_{p^k})^n} x_1^{m_1} \cdot x_2^{m_2} \cdot \ldots\ldots \cdot x_n^{m_n} = \psi(m_1) \cdot \psi(m_2) \cdot \ldots \cdot \psi(m_n)$$

This sum therefore is zero whenever $m_1 + m_2 + \dots +_n < n(p^k-1)$

Next we consider the polynomial:

$$G(X_1, \dots, X_n) := \prod_{i=1}^{n} (1 - (f_i(X_1, \dots, X_n))^{p^k-1}$$

We have $\deg(g) = (p^k-1)(d_1 + d_2 + \dots + d_m) < n(p^k-1)$

As $(f_i(x_1, \dots, x_n))^{p^k-1} = 0$ or 1 depending on whether $(x_1, \dots, x_n)$ is a root of f_i or not. It follows that $G(x_1, \dots, x_n) = 1$ when $(x_1, \dots, x_n)$ is a solution of the equations (a); else $G(x_1, \dots, x_n)=0$. Therefore we may use G to count the solutions of the equations (a) modulo p.

Suppose $(0, 0, \dots, 0)$ is the only solution of (a) then we have:

$$\sum_{(x_1, \dots, x_n) \in (\mathbb{F}_{p^k})^n} G(x_1, \dots, x_n) = 1.$$

However we have also

$$\sum_{(x_1, \dots, x_n) \in (\mathbb{F}_{p^k})^n} G(x_1, \dots, x_n) =$$

$$= \sum_{(x_1, \dots, x_n) \in (\mathbb{F}_{p^k})^n} \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} x_1^{i_1} \cdot \dots \cdot x_n^{i_n} .$$

$$= \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} \sum_{(x_1, \dots, x_n) \in (\mathbb{F}_{p^k})^n} x_1^{i_1} \cdot \dots \cdot x_n^{i_n} =$$

$$= \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} \cdot \psi(i_1) \cdot \dots \cdot \psi(i_n)$$

$$= \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} \cdot 0 = 0$$

For $i_1 + \dots + i_n \leq \deg(G) < n(p^k-1)$

This gives a contradiction.

(2.3) <u>Theorem</u>: for $G = C_p \oplus C_p \oplus \ldots\ldots \oplus C_p$ we have $\lambda(G) = \Lambda(G)$

<u>proof</u>: It is sufficient to show $\lambda(G) \leq k(p-1)$.
Suppose we have a $(C_p)^k$-sequence of length
$n > k(p-1)$. $S = (a_1,\ldots,a_n)$ where $a_i = \begin{pmatrix} a_{i1} \\ \vdots \\ a_{ik} \end{pmatrix}$

Consider the following equations (a) over $(\mathbb{F}_p)^n$

$$\begin{aligned} a_{11} \; X_1^{p-1} + \ldots \quad & + a_{n1} X_n^{p-1} = 0 \\ \vdots \qquad\qquad & \qquad\qquad\qquad\qquad (a) \\ a_{1k} \; X_1^{p-1} + \quad & + a_{nk} X_n^{p-1} = 0 \end{aligned}$$

The total degree of (a) is equal $k(p-1) < n$, and $(0,0,\ldots,0)$ is a solution. From the theorem of CHEVALLEY we derive that there exist a non-zero solution $(y_1,\ldots, y_n)$ of (a). Now we have $(y_i)^{p-1} = 0$ or 1 depending on whether $y_i = 0$ or $y_i \neq 0$.

It follows that $y_1^{p-1}\, a_1 + \ldots\ldots + y_n^{p-1}\, a_n = 0$ in $(C_p)^k$.

Hence S is not primitive. This completes the proof.

<u>remark</u>: It is useless to apply (2.2) for the additive group of $(\mathbb{F}_{p^k})^n$ with $k > 1$ as it is isomorphic to $(C_p)^{k.n}$. The result would be

$$\lambda(((C_p)^k)^m) \leq m(p^k-1)$$

which in fact is weaker then the result we proved already.

To prove (2.1) we consider the group Algebra $\mathbb{F}_p(G)$. We assume G to be $G = C_{p^{n_1}} \oplus \ldots \oplus C_{p^{n_k}}$ with $0 < n_1 \leq n_2 \leq \ldots\ldots \leq n_k$.

It is convenient to consider a multiplicative copy $\overline{G}$ of G :

$$\overline{G} = \{a_1^{g_1} \cdot a_2^{g_2} \cdot \ldots \cdot a_k^{g_k} \mid \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} \in G\}$$

where $a_i^{p^{n_i}} = 1$ and $a_i\, a_j = a_j\, a_i$

are the generating relations of $\overline{G}$.

We denote $A^g = a_1^{g_1} \cdot a_2^{g_2} \cdot \ldots \cdot a_k^{g_k}$ when $g = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}$

This defines a canonical is omorphism from G on to $\overline{G}$.

We also consider the polynomial ring $\mathbb{F}_p[X_1,\ldots\ldots,X_k]$ and a surjection Φ from $\mathbb{F}_p[X_1,\ldots,X_k]$ on to $\mathbb{F}_p(\overline{G})$ defined by

$$\Phi(X_1^{g_1} \cdot \ldots \cdot X_k^{g_k}) = a_1^{g_1} \cdot \ldots \cdot a_k^{g_k}$$

We denote $X^g = X_1^{g_1} \cdot \ldots \cdot X_k^{g_k}$ when $g = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}$

(2.4) Lemma : For any $g \in G$ there exist polynomials $P_{g,i} \in F_p[X_1,\ldots, X_k]$ such that

$$1 - X^g = P_{g,1}\,(1 - X_1) + \ldots + P_{g,k}\,(1 - X_k)$$

proof: $(1 - X^g)\,(1, \ldots, 1) = 0$ hence $1 - X^g$ is contained in the ideal $(1 - X_1, \ldots, 1 - X_n)$

(2.5) Lemma: The following equations hold in $\mathbb{F}_p(\overline{G})$

1) $(1 - a)^{p^n} = 0$ when $a^{p^n} = 1 \in \overline{G}$

2) $(1 - a)^{p^n - 1} = \sum_{\nu=0}^{p^n-1} a^{\nu}$

3) $(1 - a)^{p^n - 2} = \sum_{\nu=0}^{p^n-2} \nu \; a^{\nu-1}$

proof: In $\mathbb{F}_p[X]$ we have $(1 - X)^{p^n} = 1 - X^{p^n}$.

By dividing by $(1 - X)$ we derive

$$(1 - X)^{p^n - 1} = \sum_{\nu=0}^{p^n - 1} X^\nu$$

From this we conclude by formal differentiation

$$(1 - X)^{p^n - 2} = \sum_{\nu=0}^{p^n - 1} \nu \, X^{\nu - 1}$$

The lemma follows by application of an homomorphism mapping X on a.

(2.6) Lemma: Let $S = (g_1, \ldots, g_m)$ be a G-sequence and put $N(S,g) := N_{\text{even}} - N_{\text{odd}}$ where $N_{\text{even (odd)}}$ is the number of solutions of the equation:

$$e_1 g_1 + e_2 g_2 + \ldots + e_m g_m = 1 \qquad e_i = 0,1$$

with $\sum_{i=1}^{m} e_i$ even (odd).

Then we have in $\mathbb{F}_p(\overline{G})$

$$\prod_{j=1}^{m} (1 - A^{g_j}) = \sum_{g \in \overline{G}} N(S,g) \, A^g$$

Proof: The lemma follows by the combinatorial meaning of the $N(S,g)$. (We consider $N(S,g)$ to be an element of $\mathbb{F}_p$).

proof of Theorem (2.1): Let S be a G-sequence of length

$$m > \Lambda(G) = p^{n_1} + \ldots + p^{n_k} - k.$$

Then $\sum_{j=1}^{m} (1 - X^{g_j}) = \prod_{j=1}^{m} \sum_{i=1}^{k} P_{g_j,i} \cdot (1 - X_i) =$

$$= \sum_{i=1}^{k} Q_i \cdot (1 - X_i)^{p^{n_i}}$$

for some fixed $Q_i \in \mathbb{F}_p[X_1, \ldots, X_k]$,

as $((1 - X_1), \ldots, (1 - X_k))^m \subset ((1 - X_1)^{p^{n_1}}, \ldots, (1 - X_k)^{p^{n_k}})$

By application of Φ we conclude

$$\prod_{j=1}^{m} (1 - A^{g_j}) = \sum_{i=1}^{k} Q_i.(1 - a_i)^{p^{n_i}} = 0.$$

It follows that $N(S,0) = 0$. For primitive S we have $N(S,0) = 1$ hence S is not primitive.

<u>remark</u>: This proof is due to J.E. OLSON [19]. By considering sequences of length $\Lambda(G)$ and $\Lambda(G) - 1$ we obtain more information.

(2.7) <u>proposition</u>: Let G be a p-group, then for any sequence S of length $\Lambda(G)$ there exist a $c \in \mathbb{F}_p$ such that

$N(S,g) \equiv c \pmod p$ for every $g \in G$.

<u>proof</u>: We have $\prod_{j=1}^{\Lambda(G)} (1 - X^{g_j}) = c. \prod_{i=1}^{k} (1 - X_i)^{p^{n_i}-1} + Q$

for some $Q \in ((1 - X_1)^{p^{n_1}}, \ldots.., (1 - X_k)^{p^{n_k}})$ and

$c \in \mathbb{F}_p$.

from this we derive:

$$\prod_{j=1}^{\Lambda(G)} (1 - X^{g_j}) = c \prod_{i=1}^{k} \sum_{j=0}^{(p^{n_i}-1)} a^j = c \sum_{g \in G} A^g.$$

Thus $\mu(S,g) \equiv c \pmod p$

<u>remark</u>: By (2.7) any primitive sequence S of length $\Lambda(G)$ satisfies $N(S, g) \equiv 1 \pmod p$. and is therefore maximal. This again proves (2.1) (See [1])

(2.8) <u>Theorem</u>: for any p-group G we have $\nu(G) = \Lambda(G) - 1$.

<u>proof</u>: Again we form the product $\prod_{j=1}^{\Lambda(G)-1} (1 - A^{g_j})$.

Now we have:

$$\prod_{j=1}^{\Lambda(G)-1} (1 - X^{g}) \equiv \sum_{i=1}^{k} c_i \prod_{j=1}^{k} (1 - X_j)^{p^{n_i - 1 - \delta_{ij}}} +$$

$$c_0 \prod_{j=1}^{k} (1 - X_j)^{p^{n_i} - 1}$$

$$(\mathrm{mod}\ ((1 - X_1)^{p^{n_1}}, \ldots, (1 - X_k)^{p^{n_k}}))$$

(δ_{ij} denotes the Kronecker symbol).

By application of Φ and (2.5) we conclude:

$$\prod_{j=1}^{\Lambda(G)-1} (1 - A^{g_j}) = c_0 \prod_{i=1}^{k} \Big(\sum_{j=0}^{p^{n_i}-1} a_i^j \Big) + \sum_{i=1}^{k} c_i . \Big(\sum_{\nu=0}^{p^{n_i}-1} \nu . a_i^{\nu-1} \Big) \prod_{\substack{j=1 \\ j \neq i}}^{k} \Big(\sum_{\nu=0}^{p^{n_j}-1} a_j^{\nu} \Big)$$

$$= \sum_{g \in G} (c_0 + c_1(g_1+1) + \ldots + c_k(g_k+1)) \ A^{g}.$$

Hence $N(S,g) = \sum_{i=1}^{k} c_i g_i + \sum_{i=0}^{k} c_i$

Now suppose that S is primitive then

$$N(S,0) = 1 = \sum_{i=0}^{k} c_i .$$

It follows that all holes of S satisfy the equation:

$$\sum_{i=1}^{k} c_i g_i = -1.$$

which equation defines a proper coset in g exept for the case $c_1 = c_2 = \ldots = c_k = 0$.

In this case however S is maximal.

§ 3 Induction methods.

In this section we study groups G which appear in a short exact sequence:

$$0 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 0$$

(i.e. i and π are homomorphisms such that i is injective, π is surjective and the image of N in G is equal the kernel of π).

Consider a G-sequence S. By applying π we form a H-sequence of the same length which we denote by $\pi\, S$. Suppose $\pi\, S$ contains some disjoint zero-subsequences, say $\pi\, S_1, \ldots, \pi\, S_\nu$. Then we can form a N-sequence of length ν:

$$(i^{-1}\ |S_1|, \ldots., i^{-1}\ |S_\nu|) \ .$$

Suppose now that this N-sequence contains a zero-subsequence. Then $|S_1 \cup S_2 \cup \ldots.. \cup S_\nu| = 0$ and it follows that S is not primitive. This argument makes it possible to express $\mu(G)$ in terms of $\mu(H)$ and $\mu(K)$. The resulting estimate is however to general and can be strengthened by a deeper analysis of long H-sequences.

(3.1) <u>proposition</u>: If $0 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 0$ is a short exact sequence then we have

$$\mu(G) \leq \mu(H) \ . \ \mu(N)$$

<u>proof</u>: Suppose S is a zero-sequence of length $\geq \mu(H) \ . \ \mu(N) + 1$. From the definition of $\mu(H)$ it follows that $\pi\, S$ is the union of at least $\mu(N) + 1$ disjoint zero-subsequences say $\pi\, S_1, \ldots, \pi\, S_\nu$.

Considering the N-sequence

$$(i^{-1}\ |S_1|, \ldots., i^{-1}\ |S_\nu|),$$

We see this is a zero-sequence of length $> \mu(N)$ hence it is not irreducible , so it contains a proper zero-subsequence $(i^{-1}\ |S_{j_1}|\ , \ldots., i^{-1}\ |S_{j_t}|)$. Then $S_{j_1} \cup \ldots. \cup S_{j_t}$ is a proper zero-subsequence of S thus

S is not irreducible.

(3.2) <u>corollary</u>: Let G have the following decomposition in p-groups $G = G_{p_1} \oplus \ldots. \oplus G_{p_r}$. then

$$\mu(G) \leq \mu(G_{p_1}) \cdot \ldots\ldots \cdot \mu(G_{p_r})$$

<u>proof</u>: by induction on r.

For "homogeneous" groups $(C_n)^k$ this gives

$$\mu(C_n)^k \leq n.k^r \quad \text{whenever } n = p_1^{j_1} \cdot \ldots. \cdot p_r^{j_r} .$$

This estimate is sufficient to prove $\lambda(G) = \Lambda(G)$ only when g is cyclic in which case the equality already was proved.

<u>definition</u>: 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 is a G-sequence S_1 with $|S_1| = 0$ and $l(S_1) \leq d_k$.

It is clear that any G-sequence that is sufficiently large contains short zero-subsequences. The integer d_k is the largest order in the group. Any G-sequence S of length $\geq (d_k-1)\,\omega(G) + 1$ contains at least d_k times some fixed element a and $(\underbrace{a, \ldots, a}_{d_k \text{ x}})$ is a short zero-sequence.

We denote by $\mu_B(G,A)$ the least integer k such that any A-sequence contains a short zero-subsequence. Again we put $\mu_B(G) = \mu_B(G,G)$. It is clear that $\mu_B(G,A) \geq \mu(G,A)$. We have for any A-sequence S:

$$l(S) \geq \mu_B(G,A) \quad \Longrightarrow \quad 0 \in [S]_{d_k}$$

By induction on t this can be generalised:

(3.3) <u>proposition:</u> Any A-sequence of length $\geq \mu_B(G,A) + t.d_k$ contains at least $t + 1$ disjoint short zero-subsequences.

We denote by $\mathcal{B}$ the collection of all finite Abelian groups for which we have:

$$\mu_B(G) \leq \mu(G) - 1 + d_k.$$

(3.4) <u>proposition</u>: All cyclic groups are contained in $\mathcal{B}$.

<u>proof</u>: For a cyclic group all irreducible zero-sequences are short zero-sequences by (1.1). Thus

$$\mu_B(G) = \mu(G) = \omega(G) \leq 2.\omega(G) - 1 = \mu(G) - 1 + d_k.$$

(3.5) <u>proposition</u>: All p-groups $G = C_{p^{n_1}} \oplus C_{p^{n_2}} \oplus \ldots \oplus C_{p^{n_k}}$ with

$$p^{n_k} > p^{n_{k-1}} + \ldots + p^{n_1} - k + 2 \qquad n_1 \leq n_2 \leq \ldots \leq n_k$$

are contained in $\mathcal{B}$.

<u>proof:</u> We know already that

$\mu(G) = p^{n_k} + p^{n_{k-1}} + \ldots + p^{n_1} - k + 1$ and

$\mu(G \oplus C_{p^k}) = p^{n_k} + p^{n_k} + p^{n_{k-1}} + \ldots + p^{n_2} - k$ thus

$\mu(G \oplus C_{p^k}) = \mu(G) + p^{n_k} - 1 \quad < \quad 3\,p^{n_k}.$ and

$\mu(G) \quad < \quad 2\,p^{n_k}$.

Now consider a G-sequence S of length $\mu(G) + p^{n_k} - 1$.

We construct a $(G \oplus C_{p^k})$-sequence S' as follows:

If $S = (a_1, \ldots, a_m)$ then $S' = \left(\begin{pmatrix} a_1 \\ 1 \end{pmatrix}, \ldots\ldots, \begin{pmatrix} a_m \\ 1 \end{pmatrix}\right)$

Because $l(S') = \mu(G \oplus C_{p^{n_k}})$ S' not primitive.

This implies that S contains a zero-subsequence T of length $t.p^{n_k}$ with t = 1 or 2. In the case t = 1 T already is a short zero-sequence. However if t = 2 then $l(T) > \mu(G)$ thus T is not irreducible, and T is the union of two disjoint zero-subsequences one of which is short.

The proof can be adapted to give the next generalisation (for which we have no useful application)

(3.5') <u>generalistation</u>: Suppose $\mu(G) \leq m$, $\mu(G \oplus C_m) = \mu(G) + m - 1$ and $\mu(G \oplus C_m \oplus C_m) = \mu(G) + 2m - 2$ then $G \oplus C_m \in \mathcal{B}$.

From (3.5) we see that all p-groups of dimension 2 are contained in $\mathcal{B}$.

Not all groups are contained in $\mathcal{B}$ for example.

(3.6) <u>proposition:</u> $\mu_B((C_2)^k) = 2^k$.

<u>proof</u>: A short $(C_2)^k$ zero-sequence either has the form (0) or (a, a) for some $a \in (C_2)^k$. Hence $\mu_B((C_2)^k) \leq 2^k$ as any sequence of length $2^k = \omega((C_2)^k)$ contains either the element 0 or a pair of equal elements. But $\mu_B((C_2)^k) > 2^k - 1$ for the sequence consisting of the non zero elements of $(C_2)^k$ each taken only once contains no short zero-subsequences.

For $k \geq 3$ we have $2^k = \mu_B((C_2)^k) > \mu((C_2)^k) + 2 - 1 =$

$$= k + 2.$$

The described induction method is based on the presence in πS of sufficient disjoint short zero-subsequences, and is always possible when H is contained in $\mathcal{B}$

If $H = (C_2)^3 \notin \mathcal{B}$ some adapted procedure can be applied (see section 4). For $H = (C_2)^4$ we have no general induction method and for $H = (C_2)^5$ such a general procedure cannot be expected to exist as the group $G = C_2^5 \oplus C_3$ is an example where the equality $\lambda(G) = \Lambda(G)$ is false.

(3.7) Theorem: Suppose $G_1 = C_{d_1} \oplus \ldots\ldots \oplus C_{d_k}$, $G_2 = C_{e_1} \oplus \ldots\ldots \oplus C_{e_k}$ and $G_3 = C_{d_1e_1} \oplus \ldots\ldots \oplus C_{d_ke_k}$ while

$d_1 \mid \ldots\ldots \mid d_k \quad e_1 \mid \ldots\ldots \mid e_k$. (At this place the possibility $d_i = 1$ or $e_i = 1$ is not excluded!)

Suppose $\mu(G_1) = M(G_1) \quad \mu(G_2) = M(G_2)$.

Finally suppose that there exist a integer $j \quad 1 \leq j \leq k$ such that $d_1 = d_2 = \ldots = d_{j-1} = 1$ and $e_j = e_{j+1} = \ldots = e_k$.

Then we have:

a) when both G_1 and G_2 are contained in $\mathcal{B}$ then also G_3 is contained in $\mathcal{B}$ and $\mu(G_3) = M(G_3)$

b) when only G_2 is in $\mathcal{B}$ we have $\mu(G_3) = M(G_3)$

proof: There existsan exact sequence $0 \longrightarrow G_1 \xrightarrow{i} G_3 \xrightarrow{\pi} G_2 \longrightarrow 0$

Let S be a G_3-sequence of length $M(G_3)$. We have

$$M(G_3) = d_k e_k + \ldots\ldots + d_1 e_1 - k + 1 =$$

$$(d_k + d_{k-1} + \ldots\ldots + d_j - k + j - 1)e_k + e_k + e_{k-1} + \ldots + e_1 - k + 1 =$$

$$(d_k + d_{k-1} + \ldots\ldots + d_1 - k)e_k + e_k + e_{k-1} + \ldots\ldots + e_1 - k + 1 =$$

$$\Lambda(G_1) \; e_k + M(G_2).$$

If $G_2 \in \mathcal{B}$ this implies that πS contains at least $\Lambda(G_1)$ disjoint short zero-subsequences while the remaining $\geq M(G_2)$ elements contain another zero-sequence.

Hence there are at least $M(G_1) = \mu(G_1)$ disjoint zero-subsequences in πS, and we prove like in (3.1) that S is not primitive. It follows that $\mu(G_3) \leq M(G_3)$

Next suppose that G_1 and G_2 are both contained in $\mathcal{B}$ and let S be a G_3 - sequence of length $M(G_3) + d_k e_k - 1$. We have:

$$M(G_3) + d_k e_k - 1 = (\Lambda(G_1) + d_k)e_k + M(G_2) - 1$$

Hence πS contains at least $\Lambda(G_1) + d_k$ disjoint short zero-subsequences say $\pi S_1, \ldots, \pi S_m$.
The G_1-sequence $(i^{-1}|S_1| , \ldots, i^{-1}|S_m|)$ however contains a short zero-subsequence as $m \geq \mu_B(G_1)$, say $(i^{-1}|S_{\nu_1}| , \ldots, i^{-1}|S_{\nu_n}|)$ $(n \leq d_k)$.
Now $S'' = S_{\nu_1} \cup \ldots \cup S_{\nu_n}$ is a G_3-zero-sequence of length $\leq n\, e_k \leq d_k\, e_k$. It follows that $\mu_B(G_3) \leq M(G_3) + d_k e_k - 1$. which completes the proof.

(3.8) <u>Theorem</u>: $\mu(G) = M(G)$ and $G \in \mathcal{B}$ for all G of dimension ≤ 2. (i.e. $G = C_{d_1} \oplus C_{d_2}$)

<u>proof</u>: By induction on the number t of prime factors of d_1. For $t = 0$ we have $G = C_1 \oplus C_m$ and the theorem holds by (1.7) and (3.4).
Suppose that the theorem is proved for all G for which d_1 contains less then t prime factors and let $G_3 = C_{d_1} + C_{d_2}$ where d_1 contains exactly t prime factors. Let $d_1 = p^k.m$ $(m, p) = 1$. Put $G_1 = C_{d_1/p^k} \oplus C_{d_2/p^k}$ and

$G_2 = C_{p^k} + C_{p^k}$.
It follows that all conditions in (3.7) a) are satisfied by G_1, G_2, and G_3 hence $\mu(G_3) = M(G_3)$ and $G_3 \in \mathcal{B}$.

(3.9) <u>Theorem</u>: Let G be a p-group and suppose $p^n > \Lambda(G)$ then for any $m \in \mathbb{N}$ we have:
$\mu(G \oplus C_{m\, p^n}) = M(G \oplus C_{m\, p^n})$ and $G \oplus C_{m\, p^n} \in \mathcal{B}$.

<u>proof</u>: Put $G_1 = \underbrace{C_1 \oplus C_1 \oplus \ldots\ldots \oplus C_1}_{\dim(G)\text{ terms}} \oplus C_m$ and

$$G_2 = G \oplus C_{p^n} \quad , \quad G_3 = G \oplus C_{p^n m} \; .$$

Then all conditions in (3.7) a) are satisfied for G_1, G_2 and G_3 and the theorem follows.

(3.8) and (3.9) prove the equality $\lambda = \Lambda$ in the cases II and III from the introduction.

The next two applications are due to J.E. OLSON [19].

(3.10) <u>Theorem</u>: Let $G = H \oplus K$ where $\omega(H) \mid \omega(K)$ then $\mu(G) \leq \omega(H) + \omega(K) - 1$.

<u>proof</u>: By induction on the number of prime factors (counting multiplicity) of $\omega(H)$. If $\omega(H) = 1$ the theorem follows by (1.5). Suppose the theorem is proven for all groups $G = H \oplus K$ where $\omega(H)$ contains less then t prime factors and let $G_3 = H_3 \oplus K_3$ where $\omega(H_3)$ contains exactly t prime factors. Let $p \mid \omega(H_3)$. We take subgroups $H_1 \leq H_3$ and $K_1 \leq K_3$ such that $\mathrm{ind}[H_1 : H_3] = \mathrm{ind}[K_1 : K_3] = p$. consider the exact sequence.

$$0 \longrightarrow H_1 \oplus K_1 \xrightarrow{i_1 \oplus i_2} H_3 \oplus K_3 \xrightarrow{\pi_1 \oplus \pi_2} C_p \oplus C_p \longrightarrow 0.$$

It follows that for any G-sequence S of length $\geq \omega(H_3) + \omega(K_3) - 1 = (\omega(H_1) + \omega(K_1) - 2)p + (2p - 1)$ sequence π S contains at least $\omega(H_1) + \omega(K_1) - 1$ disjoint zero-sequences. As $\mu(H_1 + K_1) \leq \omega(H_1) + \omega(K_1) - 1$ by induction hypothesis it follows like in (3.1) that S is not primitive.

(3.11) corollary: Let G be a finite Abelian group and let $k \mid \omega(G)$ then any G-sequence S of length $\geq \omega(G) + k - 1$ contains a zero-subsequence of length divisible by k.

proof: Let $H = C_k \oplus G$, then we have $\mu(H) \leq \omega(G) + k - 1$. The corollary follows by considering the H-sequence.

$$S' = (\binom{1}{a_1}, \ldots, \binom{1}{a_m}) \quad \text{when } S = (a_1, \ldots, a_m)$$

This corollary generalises the result of P. ERODÖS , A. GINSBURG, A. ZIV [10] and N.G. DE BRUYN we mentioned in the introduction.

§ 4 Groups of the form $C_{2n_1} \oplus C_{2n_2} \oplus C_{2n_3}$.

For a group $G = C_{2n_1} \oplus C_{2n_2} \oplus C_{2n_3}$ there exists an exact sequence:

$$0 \longrightarrow C_{n_1} \oplus C_{n_2} \oplus C_{n_3} \xrightarrow{i} G \xrightarrow{\pi} C_2 \oplus C_2 \oplus C_2 \longrightarrow 0$$

As was stated in section 3 we have $\mu_B((C_2)^3) = 8$ hence $(C_2)^3 \notin \mathcal{B}$.
However we have the next lemma:

(4.1) Lemma: Any $C_2 \oplus C_2 \oplus C_2$-sequence S of length 2k + 8 contains either k + 3 disjoint zero-subsequences or it contains k + 1 disjoint short zero-subsequences while the remaining elements are at least six distinct elements $\neq 0$.

proof: As $\mu_B((C_2)^k) = 8$ we have by (3.3) that S contains at least k + 1 disjoint short zero-subsequences. Consider the remaining ≥ 6 elements:

$a_1 \ a_2 \ \dots \ a_m \qquad\qquad m \geq 6$.

There are three possibillities:

1) for some j $a_j = 0$. Then the remaining ≥ 5 elements contain another zero-sequence and S contains k + 3 disjoint zero-sequences.
2) for some $i \neq j$ we have $a_i = a_j$. Now the remaining ≥ 4 elements contain another zero-sequence and again S contains k + 3 disjoint zero-sequence.
3) If neither 1) nor 2) holds $a_1 \dots a_m$ are distinct and unequal zero. As $m \geq 6$ this proves the lemma.

(4.2) Theorem [P.C. BAAYEN - J.H. VAN LINT] : Let $G_1 = C_{n_1} \oplus C_{n_2} \oplus C_{n_3}$

$n_1 \mid n_2 \mid n_3$ be a group for which $\nu(G_1) = \Lambda(G_1) - 1$ then for $G_2 = C_{2n_1} \oplus C_{2n_2} \oplus C_{2n_3}$ we have $\mu(G_2) = M(G_2)$

<u>proof</u>: Let S be a G_2-sequence of length $M(G_2)$. Consider the exact sequence:

$$0 \longrightarrow G_1 \xrightarrow{i} G_2 \xrightarrow{\pi} C_2 + C_2 + C_2 \longrightarrow 0$$

We have $M(G_2) = (n_1 + n_2 + n_3)2 - 2 = (n_1 + n_2 + n_3 - 5)2 + 8$.
By (4.1) we know that either π S contains $n_1 + n_2 + n_3 - 5 + 3 = \mu(G_1)$ disjoint zero-subsequences or π S contains $\nu(G_1) = n_1 + n_2 + n_3 - 4$ disjoint short zero-sequences and at least six other distinct non zero-elements.

In the first case it follows that S is not primitive like in section 3. In the last case we consider the $\nu(G_1)$ disjoint short zero-sequences: $\pi S_1, \ldots, \pi S_m$ $m = \nu(G_1)$ and we form the G_1-sequence:
$T = (i^{-1}|S_1|, \ldots, i^{-1}|S_m|)$.
If T is not primitive then S is not primitive either. Else we see (as $m = \nu(G_1)$) that all holes of T are contained in some proper coset $y + N$ $y \notin N$.
Let $\pi a_1, \ldots, \pi a_6$ be six of the remaining distinct non zero elements of π S. By a suitable choice of a base in $(C_2)^3$ we may assume that $(\pi a_1, \ldots, \pi a_6) =$

$$= \left(\begin{pmatrix}1\\0\\0\end{pmatrix}\begin{pmatrix}0\\1\\0\end{pmatrix}\begin{pmatrix}0\\0\\1\end{pmatrix}\begin{pmatrix}1\\1\\0\end{pmatrix}\begin{pmatrix}1\\0\\1\end{pmatrix}\begin{pmatrix}0\\1\\1\end{pmatrix}\right)$$

This means that the sequence $(a_1, \ldots a_6)$ contains the following subsequences $V_1, \ldots, V_7$ with values $i(G_1)$:

$V_1 = (a_1, a_2, a_4)$, $V_2 = (a_1, a_2, a_5, a_6)$
$V_3 = (a_1, a_3, a_5)$, $V_4 = (a_1, a_3, a_4, a_6)$
$V_5 = (a_2, a_3, a_6)$, $V_6 = (a_2, a_3, a_4, a_5)$
$V_7 = (a_4, a_5, a_6)$

Put $t_i = i^{-1} |V_i|$ $i = 1, \ldots, 7$

Suppose that for some i $1 \leq i \leq 7$ we have $t_i \not\equiv -y \bmod N$. Then $T \cup \{t_i\}$ is not primitive hence S is not primitive also. However if $t_i \equiv -y \pmod N$ then we have
$|V_1| + |V_3| + |V_5| + |V_7| = |V_2| + |V_4| + |V_6|$ thus
$t_1 + t_3 + t_5 + t_7 = t_2 + t_4 + t_6$
which implies $-4y \equiv -3y \pmod N$ and therefore $y \in N$ which gives a contradiction

(4.3) <u>corollary</u>: For any prime p and for all integers $n_1 \leq n_2 \leq n_3$ we have

$$\mu(C_{2p^{n_1}} \oplus C_{2p^{n_2}} \oplus C_{2p^{n_3}}) = M(C_{2p^{n_1}} \oplus C_{2p^{n_2}} \oplus C_{2p^{n_3}})$$

<u>proof</u>: By (2.8) we have $\nu(C_{p^{n_1}} \oplus C_{p^{n_2}} \oplus C_{p^{n_3}}) =$

$= \Lambda(C_{p^{n_1}} \oplus C_{p^{n_2}} \oplus C_{p^{n_3}}) - 1$, and we may apply (4.2)

(4.4) <u>corollary</u>: for any $m \in N$ we have:

$$M(C_{2m} \oplus C_2 \oplus C_2) = \mu(C_{2m} \oplus C_2 \oplus C_2)$$

<u>proof</u>: by (4.2) and (1.19).

(4.5) <u>corollary</u>: Suppose $\nu(C_{nm_1} \oplus C_{nm_2}) = \Lambda(C_{nm_1} \oplus C_{nm_2}) - 1$. Then

$$M(C_2 \oplus C_{2nm_1} \oplus C_{2nm_2}) = \mu(C_2 \oplus C_{2nm_1} \oplus C_{2nm_2})$$

<u>proof</u>: by (4.2)

(4.3) proves the equality $\lambda = \Lambda$ for case IV. (4.5) reduces the proof of case V to the problem of proving $\nu(C_{nm_2} \oplus C_{nm_2}) = \Lambda(C_{nm_1} \oplus C_{nm_2}) - 1$ for the n, m_1 and m_2 mentioned in the formulation of case V. See section 5.

§ 5 Induction methods for the equality $\nu = \Lambda - 1$.

In this section we prove a theorem stating:

$\nu(C_{d_1} \oplus C_{d_2}) = \Lambda(C_{d_1} \oplus C_{d_2}) - 1$ implies

$\nu(C_{d_1p} \oplus C_{d_2p}) = \Lambda(C_{d_1p} \oplus C_{d_2p}) - 1$ provided that the prime p

satisfies the extra condition (C). We need the extra condition (C) for the following reason: our argument is based on the same methods used in section 3. However somewhere within the proof we meet a $C_p \oplus C_p$-sequence T of length $3p - 3 = \mu_B(C_p \oplus C_p) - 1$ which has the following two properties:

I) T contains no short zero-sequences
II) Each zero-subsequence of T is irreducible.

Such sequences are possible; for example the sequence

$$T = (\underbrace{\begin{pmatrix}1\\0\end{pmatrix} \cdots\cdots \begin{pmatrix}1\\0\end{pmatrix}}_{(p-1)x} \underbrace{\begin{pmatrix}0\\1\end{pmatrix} \cdots\cdots \begin{pmatrix}0\\1\end{pmatrix}}_{(p-1)x} \underbrace{\begin{pmatrix}1\\a\end{pmatrix} \cdots\cdots \begin{pmatrix}1\\a\end{pmatrix}}_{(p-1)x}),\ 1 \leq a \leq p-1$$ has properties

I and II.

Condition (C) gives us the extra information we need; it says that the given example is (modulo some base-transformation) the only sequence T which has both properties I and II:

<u>Definition</u>: A prime p has property (C) iff any $(C_p \oplus C_p)$-sequence of length 3p - 3 having properties I and II consists of three distinct elements each with multiplicity p - 1.

Property (C) is shared by 2, 3, 5 and 7. For all other primes it is unknown whether they have property (C).

By chosing a suitable base for $C_p \oplus C_p$ we may then assume two of these elements to be equal $\binom{1}{0}$ resp. $\binom{0}{1}$. It proves then that the third element is one of the elements $\binom{a}{b}$ with a = 1 and $1 \leq b \leq p-1$, b = 1 and $1 \leq a \leq p-1$ or a + b = p and $1 \leq a, b \leq p-1$. This follows from the following theorems proved by P. NOORDZIJ [16]:

(5.1) <u>Theorem</u>: Let $k \in \mathbb{N}$ and let $1 \leq a, b \leq k$ with the following property: "Whenever $1 \leq n \leq k-1$ and whenever $t_a k < n.a \leq (t_a+1)k$ and $t_b.k < n.b \leq (t_b+1)k$ then

$$n(a+b-1) < k(t_a + t_b + 1) \qquad (1) \quad "$$

then $a = 1$ or $b = 1$ or $a+b = k$.

(5.2) <u>Theorem</u>: Let $k \in \mathbb{N}$ and let $1 \leq a, b \leq k$ with the following property: " Whenever $1 \leq n \leq k-1$ and whenever $t_a.k < n.a \leq (t_a+1)k$ and $t_b.k < n.b \leq (t_b+1)k$ then

$$n(a+b-1) \leq k(t_a + t_b + 1) \qquad (2) \quad "$$

Then $a = 1$ or $b = 1$ or $a+b = k$ or $a+b = k+1$ or we have one of the (exeptional) situations:

i) $k = 4m$, $a = 2$, $b = 2m-1$,

ii) $k = 9$, $a = 2$, $b = 5$ or

iii) $k = 14$, $a = 3$, $b = 5$.

The proof of the main result of this section however is independent of the results (5.1) and (5.2) which we mantion only for the extra information they give.

(5.3) <u>Lemma</u>: Let Q be a finite Abelian group and let G_1 be the group $C_p \oplus C_p \oplus Q$. Let π_1 and π_2 be the natural projections on $C_p \oplus C_p$ and on Q. Let S be a G_1-sequence of length $3p-3$ with the following properties:

i) $\pi_1 S$ contains three distinct non zero-elements each with multiplicity $p-1$.

ii) $\pi_1 S$ contains no short zero-subsequence

iii) For some fixed $t \neq 0$ in Q we have $\pi_2|T| = t$ whenever $\pi_2|T| = t$ whenever $\pi_1 T$ is a zero-subsequence of $\pi_1 S$.

Then there exists a proper coset $c + N \subset C_p \oplus C_p$, $x \notin N$ such that for any $y \in C_p \oplus C_p$ $y \neq 0$ and $y \notin x + N$ there are at least two subsequences T_1 and $T_2 \leq S$ such that $\pi_1|T_1| = \pi_1|T_2|$ and $\pi_2|T_1| \neq \pi_2|T_2|$

<u>proof</u>: After a suitable choice of a base for $C_p \oplus C_p$ we may assume

$$\pi_1 S = (\underbrace{\binom{1}{0} \ldots\ldots \binom{1}{0}}_{\substack{p-1\\ \text{times}}} \underbrace{\binom{0}{1} \ldots\ldots \binom{0}{1}}_{\substack{p-1\\ \text{times}}} \underbrace{\binom{a}{b} \ldots\ldots \binom{a}{b}}_{\substack{p-1\\ \text{times}}})$$

in order that π_1 S does not contain a short zero-subsequence we have $p-a + p-b + 1 > p$ thus $a+b < p+1$, for

$$V_1 = (\underbrace{\binom{1}{0} \ldots\ldots \binom{1}{0}}_{(p-a)x}, \underbrace{\binom{0}{1} \ldots\ldots \binom{0}{1}}_{(p-b)x}, \binom{a}{b})$$ is a zero-sequence

We may write $S = \left(\begin{pmatrix}1\\0\\x_1\end{pmatrix} \ldots\ldots \begin{pmatrix}1\\0\\x_{p-1}\end{pmatrix}\begin{pmatrix}0\\1\\y_1\end{pmatrix} \ldots\ldots \begin{pmatrix}0\\1\\y_{p-1}\end{pmatrix}\begin{pmatrix}a\\b\\z_1\end{pmatrix} \ldots \begin{pmatrix}a\\b\\z_{p-1}\end{pmatrix}\right)$

by iii,it follows that for any subsequence T with $\pi_1 T = V_1$ we have $\pi_2|T| = t$. This implies $z_1 = z_2 = \ldots z_{p-1} = z$. By reasons of symmetry it follows that $x_1 = \ldots = x_{p-1} = x$ and $y_1 = \ldots = y_{p-1} = y$. Thus S contains three distinct elements each $(p-1)$ times.

Because $a+b \leq p$ we may assume $a \leq p/2$. Next we consider the sequence

$$V_2 = (\underbrace{\binom{1}{0} \ldots\ldots \binom{1}{0}}_{(p-2a)x} \underbrace{\binom{0}{1} \ldots\ldots \binom{0}{1}}_{(p-2b+\delta p)x} \binom{a}{b} \binom{a}{b})$$

with $\delta = 0$ if $2b < p$ and $\delta = 1$ else. By iii) we have for any sequence T with $\pi_1 T = V_2$ $\pi_2|T| = t$. This implies:

$$(p-a)x + (p-b)y + z = t = (p-2a)x + (p-2b+\delta p)y + 2z .$$

Thus $z = ax + by - \delta py$ and $t = p(x+y) - \delta py$. If $\delta = 0$ we have $t = p(x+y) \neq 0$ thus $px \neq 0$ or $py \neq 0$; else we have $t = px \neq 0$.

Now we consider three possible cases:

<u>case 1</u>: $a = b = 1$. Then $\delta = 0$. We may assume $px \neq 0$.

Put $K = \{\binom{u}{v} \in C_p \oplus C_p \;:\; u = p-1\}$

Then K is a proper coset in $C_p + C_p$. For any $\binom{h}{k} \in C_p$ with $0 \neq \binom{h}{k}$ and $\binom{h}{k} \notin K$ we put $n_1 = h+1$ $n_3 = p-1$ and $n_2 = \begin{cases} 0 & \text{whenever } k = p-1 \\ k+1 & \text{whenever } k < p-1 \end{cases}$

Then $T_1 = \left(\underbrace{\begin{pmatrix}1\\0\\x\end{pmatrix} \cdots \begin{pmatrix}1\\0\\x\end{pmatrix}}_{hx} \underbrace{\begin{pmatrix}0\\1\\y\end{pmatrix} \cdots\cdots \begin{pmatrix}0\\1\\y\end{pmatrix}}_{kx}\right)$ and

$$T_2 = \left(\underbrace{\begin{pmatrix}1\\0\\x\end{pmatrix} \cdots \begin{pmatrix}1\\0\\x\end{pmatrix}}_{n_1x} \underbrace{\begin{pmatrix}0\\1\\y\end{pmatrix} \cdots\cdots \begin{pmatrix}0\\1\\y\end{pmatrix}}_{n_2x} \underbrace{\begin{pmatrix}1\\1\\z\end{pmatrix} \cdots\cdots \begin{pmatrix}1\\1\\z\end{pmatrix}}_{n_3x}\right)$$

are subsequences of S with $\pi_1|T_1| = \pi_1|T_2| = \binom{h}{k}$ and $\pi_2|T_2| - \pi_2|T_1| = (h+1)x + n_2 y + (p-1)z - (hx + ky) =$

$$= \begin{cases} t \neq 0 & \text{when } n_2 = k+1 \\ px \neq 0 & \text{when } n_2 = 0 \end{cases}$$

which completes the proof for <u>case</u> 1

<u>case 2</u> $a = 1$, $b > 1$.

If $b \geq p/2$ we choose a new base $f_1 = \binom{1}{b}$, $f_2 = \binom{0}{1}$. Then $\binom{1}{0} = f_1 + (p-b) f_2$ and $(p-b) \leq p/2$. Therefore we may assume $b \leq p/2$. This implies $\delta = 0$ and $z = x + by$ $t = p(x-y)$ let $m \in \mathbb{N}$ be determined by:

$$mb < p \leq (m+1)\, b$$

then $m \leq p-2$ because $1 < b \leq p/2$.

Considering the sequences

$$V_m = \left(\underbrace{\begin{pmatrix}1\\0\\x\end{pmatrix} \cdots \begin{pmatrix}1\\0\\x\end{pmatrix}}_{(p-m)x} \underbrace{\begin{pmatrix}0\\1\\y\end{pmatrix} \cdots \begin{pmatrix}0\\1\\y\end{pmatrix}}_{(p-mb)x} \underbrace{\begin{pmatrix}1\\b\\z\end{pmatrix} \cdots \begin{pmatrix}1\\b\\z\end{pmatrix}}_{mx} \right) \quad \text{and}$$

$$V_{m+1} = \left(\underbrace{\begin{pmatrix}1\\0\\x\end{pmatrix} \cdots \begin{pmatrix}1\\0\\x\end{pmatrix}}_{(p-m+1)x} \underbrace{\begin{pmatrix}0\\1\\y\end{pmatrix} \cdots \begin{pmatrix}0\\1\\y\end{pmatrix}}_{(2p-(m+1)b)x} \underbrace{\begin{pmatrix}1\\b\\z\end{pmatrix} \cdots \begin{pmatrix}1\\b\\z\end{pmatrix}}_{(m+1)x} \right)$$

We derive $(p-m)x + (p-mb)y + mz = t =$

$$= (p-(m+1))x + (2p-(m+1)b)y + (m+1)z$$

thus $-x + (p-b)y + z = 0$

As $z = x + by$ we conclude $py = 0$. Take K as in the case 1 . If $0 \neq \binom{h}{k} \notin K$ we see:

$$h.\begin{pmatrix}1\\0\\x\end{pmatrix} + k\begin{pmatrix}0\\1\\y\end{pmatrix} = \begin{pmatrix}h\\k\\hx+ky\end{pmatrix} \in [S]$$

and also

$$(h+1)\begin{pmatrix}1\\0\\x\end{pmatrix} + n_2.\begin{pmatrix}0\\1\\y\end{pmatrix} + (p-1)\begin{pmatrix}1\\b\\z\end{pmatrix} \in [S]$$

where $n_2 \equiv k + b \pmod p$ and $0 \leq n_2 \leq p-1$

But $hx + ky - (h+1)x - n_2 y - (p-1)z =$
$-x - by - (p-1)(x + by) = -p(x + by) = -px = -t \neq 0$

which completes the proof for case 2

<u>case 3</u> $a \neq 1$ and $b \neq 1$

We derive that i) ii) and iii) imply $a + b = p$. Then we take a new base $f_1 = \binom{a}{b}$ $f_2 = \binom{0}{1}$ and then we have $\binom{1}{0} = c\, f_1 + f_2$ with $c\, a \equiv 1 \pmod p$ thus reducing <u>case 3</u> to <u>case 2</u> . (using (5.1) this reduction can be performed directly)

for $k = 1, \ldots, p-2$ we put $\delta_k = 1$ whenever $ka \leq sp < (k+1)a$ for some s and $\delta_k = 0$ else. We also put $\varepsilon_k = 1$ if $kb \leq tp < (k+1)b$ and $\varepsilon_k = 0$ else. It follows that $\varepsilon_1 = \delta$.
Considering sequences V_k and V_{k+1} with $\pi_1|V_k| = \pi_1|V_{k+1}| = 0$ and V_k resp. V_{k+1} containing k resp. $k+1$ times the element $\begin{pmatrix} a \\ b \\ z \end{pmatrix}$ we derive the equations:

$$(p.([\tfrac{ka}{p}] + 1) - ka)x + (p.([\tfrac{kb}{p}] + 1) - kb)\,y + kz = t$$

and $$(p.([\tfrac{ka}{p}] + 1 + \delta_k) - (k+1)a)x + (p.([\tfrac{kb}{p}] + 1 + \varepsilon_k) - (k+1)b)y + (k+1)z = t.$$

Thus $(\delta_k.p - a)x + (\varepsilon_k.p - b)y + z = 0$

for $k = 1$ we have $\delta_1 = 0$

hence $ax + (b - \varepsilon_1 p)y = z$ (1)

we have also $t = p(x+y) - \varepsilon_1 py$ (2)

Suppose we have for some $1 < \nu \leq p-2$

(X.1) $\delta_\nu = \varepsilon_\nu = 0$ then we derive

$$ax + by = z \qquad (3)$$

with (1) and (2) this gives $\varepsilon_1\, py = 0$ and $t = p(x+y)$ (4)

(X.2) Similarly $\delta_\nu = 1$ $\varepsilon_\nu = 0$ gives

$$ax + by - px = z \qquad (5)$$

Thus $px = \varepsilon_1\, py$ and $t = px$ (6)

(X.3) Analogously $\delta_\nu = 0$ $\varepsilon_\nu = 1$ gives

$$ax + by - py = z \qquad (7)$$

Thus $py = \varepsilon_1\, py$ and $t = py$ (8)

(X.4) Finally $\delta_\nu = \varepsilon_\nu = 1$ gives

$$ax + by - p(x+y) = z \tag{9}$$

thus $\quad p(x+y) = \varepsilon_1\, py$ and $t = 0$ (10)

We therefore may exclude X.4

We have $\quad (a-1)p < (p-1)a < ap$ and
$(b-1)p < (p-1)b < bp$.

Therefore we conclude $\sum\limits_{\nu=1}^{p-2} \delta_\nu = a-1$ and $\sum\limits_{\nu=1}^{p-2} \varepsilon_\nu = b-1$

As $a > 1$ and $b > 1$ we deduce that both the cases (X.2) and (X.3) are realised for some ν. Suppose (X.1) is realised also for some ν then we have

$$t = px = py = p(x+y)$$

which means $t = px = py = 0$. This gives a contradiction. Therefore we also must exclude (X.1) This implies that we have

$$\sum_{\nu=1}^{p-2} (\delta_\nu + \varepsilon_\nu) = \sum_{\nu=1}^{p-2} 1 = p-2 = a+b-2.$$

and therefore $a+b = p$ which completes the proof.

Now we can formulate and proof the main theorem of this section:

(5.4) <u>Theorem</u>: Let $G_1 = C_{d_1} \oplus C_{d_2}$ and suppose $\nu(G_1) = \Lambda(G_1) - 1$
Let p be a prime satisfying condition (C) then we have
for $G_2 = C_{d_1 p} \oplus C_{d_2 p}$, $\nu(G_2) = \Lambda(G_2) - 1$

<u>proof</u>: We consider an exact sequence:

$$0 \longrightarrow G_1 \xrightarrow{i} G_2 \xrightarrow{\pi} C_p \oplus C_p \longrightarrow 0.$$

Let S be a primitive G_2-sequence of length $\Lambda(G_2) - 1 =$
$d_1 p + d_2 p - 3 = (d_1 + d_2 - 3)p + 3p - 3.$

Now there are three possibilities:

a) π S contains at least $d_1 + d_2 - 1$ disjoint zero-subsequences. Then we derive that S is not primitive by the argument from section 3.

b) a) is not true and π S contains exactly $d_1 + d_2 - 2$ disjoint short zero-subsequences say $\pi S_1, \ldots, \pi S_{\Lambda(G_1)}$

Put $T_1 = (i^{-1}|S_1|, \ldots, i^{-1}|S_{\Lambda(G_1)}|)$ then either T_1 (and also S) is not primitive or else T_1 is maximal. Let T_2 be the G_2-sequence of the remaining elements say $(a_1, \ldots, a_m)$. It follows that $2p - 3 \leq m \leq 2p - 2$.

πT_2 is primitive else we should have case a) Therefore all holes of πT_2 are contained in some proper coset $x + N \subset C_p \oplus C_p$ $x \notin N$ as $\nu(C_p \oplus C_p) = 2p - 3$. Now we have:

$$\boxed{S} \supset (i\boxed{T_1}^{*} + \boxed{T_2}^{*}) \setminus \{0\}$$

$$(i(G_1) + \boxed{T_2}^{*}) \setminus \{0\}.$$

as $\pi\boxed{T_2}^{*} = C_p \oplus C_p \setminus (x + N)$ we conclude that all cosets of G_1 exept some of those that are mapped by π in $x + N$ contain some element of $\boxed{T_2}^{*}$. This implies

$$\boxed{S} \supset G_2 \setminus \{0\} \setminus (x' + \pi^{-1}(N))$$

where $x' \in \pi^{-1}(x)$ thus $x' \notin \pi^{-1}(N)$. It follows that all holes of S are contained in the proper coset $x' + \pi^{-1}(N)$

c) Neither a) nor b) are true. We derive that π S contains exactly $d_1 + d_2 - 3$ disjoint zero-subsequences of length p and that the remaining $3p-3$ elements of π S say π T form a sequence with properties I and II.

By the assumption that p satisfies (C) we conclude that π T consists of three elements each with multiplicity (p-1).

Let the $d_1 + d_2 - 3$ disjoint short zero-subsequences of S be named $S_1, \ldots\ldots, S_{\nu(G_1)}$.

Then all holes of $T_1 = (i^{-1}|S_1|, \ldots, i^{-1}|S_{\nu(G_1)}|)$ are contained in some proper coset $t_1 + M \subset G_1$. We put $Q := G_2 / _{i(M)}$ and $t := -(it_1 + i(M))$

Let $T = (x_1, \ldots, x_{3p-3})$. Now we apply lemma (5.3) on the sequence $\left(\begin{pmatrix}\pi x_1 \\ x_1 + i M\end{pmatrix} \cdots \begin{pmatrix}\pi x_{3p-3} \\ x_{3p-3} + i M\end{pmatrix}\right) = V$

i) and ii) follow by assumptions. Suppose iii) is not true. Then T contains a subsequence U with $\pi|U| = 0$ and $|U| + i M \neq t$ and we conclude that $T_1 \cup \{i^{-1}|U|\}$ is not primitive (and S is not primitive either). Therefore we may assume that iii) also holds.

Then there exists a proper coset $x + N \subset C_p \oplus C_p$ $x \notin N$ such that for any $y \in C_p \oplus C_p$ $y \neq 0$ and $y \notin x + N$ there are at least two subsequences V_1 and $V_2 \leq V$ such that $\pi_1|V_1| = \pi_1|V_2| = y$ and $\pi_2|V_1| \neq \pi_2|V_2|$ (where π_1 are the projections from $C_p \oplus C_p \oplus Q$ on $C_p \oplus C_p$ resp. on Q).

We now prove $[S] \supset G_2 \setminus \{0\} \setminus \pi^{-1}(x + N)$.

First we consider the coset $i(G_1)$. Let $U \subset T$ be a subsequence with $\pi|U| = 0$ then $|U| + i(M) = t$ and therefore $T_1 \cup \{i^{-1}|U|\}$ is a G_1-sequence of length $\Lambda(G_1)$ thus a maximal G_1-sequence.
Thus $i(G_1) \setminus \{0\} \subset [S]$.

Next we consider a coset $y + i(G_1)$ with $\pi y \notin x + N$.

Then we have sequences V_1 and $V_2 \leq T$ with
$\pi|V_1| = \pi|V_2| = \pi(y)$ and $\pi_2|V_1| \neq \pi_2|V_2|$
As $\pi(|V_2| - |V_1|) = 0$ we have $\nu = (|V_2| - |V_1|) \in i(G_1)$

with $\nu \notin i(M)$.

Now $(y + i(G_1)) \cap [S] \supset (|V_1| + i[T_1]^*) \cup (|V_2| + i[T_1]^*)$

$= (i[T_1]^* + |V_1|) + \{0,v\} =$

$|V_1| + (i[T_1]^* + \{0,v\}) =$

$|V_1| + ((i(G_1) \setminus i(t_1 + M)) + \{0,v\})$

as $v \notin i(M)$ we have

$i(t_1 + M) \subset v + (i(G_1) \setminus i(t + M))$ thus

$(y + i(G_1)) \cap [S] \supset |V_1| + i(G_1) = y + i(G_1)$

which proves $y + i(G_1) \subset [S]$. This completes the proof.

The question remains which prime numbers p satisfy condition (C). As the only $(C_2 + C_2)$ - sequence of length 3 satisfying I and II is equal $(\binom{1}{0}, \binom{0}{1}, \binom{1}{1})$ it is clear that 2 satisfies (C). For 3 (C) is also easily verified and verification "by hand" is also possible for p = 5. Finaly for p = 7 the verification has been performed by the ELECTROLOGICA X-8 computer of the Mathematical Centre. The program is based on the "forbidden region" algorithm which was described in [8, § 12] . (See [9]).

For primes > 7 it is unknown whether condition (C) is satisfied or not.

Using either $C_1 \oplus C_m$ or $C_{p^{q_1}} \oplus C_{p^{q_2}}$, p prime $p > 7$ and $q_1 \leq q_2$ as base for induction by (5.4) we derive the following proposition:

(5.5) <u>proposition</u>: Let $n = 2^{k_1} 3^{k_2} 5^{k_3} 7^{k_4}$ and let either $m_1 = 1$ $m_2 = m$ arbitrary or $m_1 = p^{q_1}$ $m_2 = p^{q_2}$ with p prime $p > 7$ and $q_1 \leq q_2$ then we have:

$$\nu(C_{nm_1} \oplus C_{nm_2}) = \Lambda(C_{nm_1} \oplus C_{nm_2}) - 1$$

(5.6) <u>corollary</u>: Let n and m_1, m_2 be as in (5.5) then

$$\lambda(C_2 \oplus C_{2nm_1} \oplus C_{2nm_2}) = \Lambda(C_2 \oplus C_{2nm_1} \oplus C_{2nm_2})$$

<u>proof</u>: By (5.5) and (4.5)

We now have proved the cases I,..., V from the introduction for case VI see [4].

§ 6 Application in Algebraic number theory

Let $\mathcal{Z} = \mathbb{Z}^{(\mathbb{N})}$ be a countable (restricted) direct sum of infinite cyclic groups, i.e. $\mathcal{Z}$ is the group of all sequences $\{k_i\}_{i \in \mathbb{N}}$ with $k_i \in \mathbb{Z}$ and $k_i = 0$ for all but finitely many indices i where addition is performed coordinate-wise. We define $|x| = \sum_{k=1}^{\infty} x_k$ when $x = \{x_i\}_{i \in \mathbb{N}}$.

Let $\mathcal{R}$ be a subgroup of finite index in $\mathcal{Z}$. The natural projection from $\mathcal{Z}$ on to $G = \mathcal{Z}/\mathcal{R}$ is denoted by π. The set of the images in G of the base elements $e_j = \{\delta_{ij}\}_{i \in \mathbb{N}}$ is denoted by $A(\mathcal{R})$

Example I: Let G be a finite Abelian group and let $\{g_i\}_{i \in \mathbb{N}}$ be an infinite G-sequence. We define a homomorphism $\pi : \mathcal{Z} \to G$ as follows: First we put $p(e_j) = g_j$, then P can be extended uniquely to a homomorphism π. Let $\mathcal{R} = \ker \pi$ then $\mathcal{Z}/\mathcal{R} \cong \pi(\mathcal{Z}) = \langle g_1, g_2, \ldots \rangle \subset G$. thus $\mathcal{Z}/\mathcal{R}$ is finite. $A(\mathcal{R})$ is the subset of G consisting of all elements contained in $\{g_i\}_{i \in \mathbb{N}}$.

Example II: Let $\mathcal{Z}$ be the group of fractional ideals (the group of all divisors) of an algebraic number field F. Let $\mathcal{R}$ be the subgroup of principal ideals (principal divisors).

It is a known theorem that $\mathcal{Z}/\mathcal{R} = G$, the class group of the algebraic number field is finite. Its order H is called the class-number of F. See for example [20].

It is also known that the prime ideals (prime divisors) are equidistributed over the H ideal classes of F. See for example [21]. As these prime ideals form the base elements e_j in $\mathcal{Z}$ this implies $A(\mathcal{R}) = G$.

Let $\mathcal{N}$ be the subcollection of all positive element of $\mathcal{Z}$ i.e. $\mathcal{N}$ consist of all sequences $\{k_i\}_{i \in \mathbb{N}}$ with $k_i \geq 0$ all i.

In example II $\mathcal{N}$ is the collection of all integral ideals (positive divisors) in F. We write $a \leq b$ whenever $b - a \in \mathcal{N}$ $(a,b \in \mathcal{Z})$. Now we have the following definitions:

An element $x \in \mathcal{N}$ is called <u>primitive</u> iff $x \geq y$ and $y \in \mathcal{N} \cap \mathcal{R}$ implies $y = 0$.

An element $x \in \mathcal{N} \cap \mathcal{R}$ is called <u>irreducible</u> whenever $x = y+z$, $y,z \in \mathcal{N} \cap \mathcal{R}$ implies $y = 0$ or $z = 0$.

Let a be an element of $\mathcal{N}$. Then we define the A($\mathcal{R}$)-sequence S_a to be the sequence

$$S_a := (\underbrace{\pi(e_1) \ldots \pi(e_1)}_{a_1 x},\ \underbrace{\pi(e_2) \ldots \pi(e_2)}_{a_2 x},\ \ldots\ldots,\ \underbrace{\pi(e_k) \ldots \pi(e_k)}_{a_k x}\ )$$

where $a_i = 0$ for $i > k$.

The sequence S_0 is equal $\emptyset$.

The following propositions are easily verified:

(6.1): <u>proposition</u>: For every $x \in \mathcal{N}$ we have $\pi(x) = |S_x|$. x is primitive iff S_x is primitive and $x \in \mathcal{N} \cap \mathcal{R}$ is irreducible iff S_x is irreducible. Finally we have $|x| = l(S_x)$

We now define the following two constants:

$\overline{\lambda}(G, \mathcal{R}) = \sup \{ \ |x| \ | \ x \in \mathcal{N},\ x \text{ primitive } \}$

$\overline{\mu}(G, \mathcal{R}) = \sup \{ \ |x| \ | \ x \in \mathcal{N} \cap \mathcal{R},\ x \text{ irreducible } \}$

These constants are related to the constants defined in section I by the following theorem:

(6.2) <u>Theorem:</u> $\bar{\lambda}(G, \mathcal{R}) = \lambda(G, A(\mathcal{R}))$

$\bar{\mu}(G, \mathcal{R}) = \mu(G, A(\mathcal{R}))$.

<u>proof</u>: Let S be a primitive (irreducible) $A(\mathcal{R})$-sequence
As $A(\mathcal{R}) = \pi(\{e_j \mid j \in \mathbb{N}\})$ we may choose for each element $\mathfrak{s} \in S$ an base element $e_{j_\mathfrak{s}}$ such that $\mathfrak{s} = \pi(e_{j_\mathfrak{s}})$. Let $x = \sum_{\mathfrak{s} \in S} e_{j_\mathfrak{s}}$ then it follows that $S_x = S$.
By (6.1) we conclude $|S| = \pi(x)$, $l(S) = |x|$, and x is primitive (irreducible). Hence

$\bar{\lambda}(G, \mathcal{R}) \geq \lambda(G, A(\mathcal{R}))$ and

$\bar{\mu}(G, \mathcal{R}) \geq \mu(G, A(\mathcal{R}))$.

Conversely let x be a primitive (irreducible) element from $\mathcal{N}$ ($\mathcal{N} \cap \mathcal{R}$). Then S_x is also primitive irreducible) and $l(S_x) = |x|$. Hence

$\lambda(G, A(\mathcal{R})) \geq \bar{\lambda}(G, \mathcal{R})$ and

$\mu(G, A(\mathcal{R})) \geq \bar{\mu}(G, \mathcal{R})$.

This completes the proof.

In Example II there exists a 1 - 1 homomorphism ζ from the semigroup $\mathcal{N} \cap \mathcal{R}$ on to the multiplicative semigroup $(\mathcal{O} \setminus \{0\})/\mathcal{U}$ where $\mathcal{O}$ is the ring of integers in F and $\mathcal{U}$ is the group of units in $\mathcal{O}$. This homomorfism maps the irreducible elements x of $\mathcal{N} \cap \mathcal{R}$ on to the conjugation classes of irreducible integers in $\mathcal{O}$. The number $|x|$ denotes now the number of prime ideals (counting multiplicity) in the decomposition of the integers in $\zeta(x)$.

From this we derive the next theorem which proves the statement of H. DAVENPORT [7] mentioned in the introduction.

(6.3) <u>Theorem:</u> The maximal number of prime ideals (counting multiplicity) in the decomposition of an irreducible integer in an Algebraic number field F with classgroup G is equal $\mu(G)$.

<u>proof</u>: This number is equal $\sup \{|x| \mid x \in \mathcal{N} \cap \mathcal{R},\ x \text{ irreducible}\} =$

$$= \bar{\mu}(G, \mathcal{R}) = \mu(G, A(\mathcal{R})) = \mu(G, G) = \mu(G).$$

§ 7 Application in the theory of finite dimensional vectorspaces over $\mathbb{F}_{p^k}$; application in graph theory.

Let V be a vectorspace over $\mathbb{F}_{p^k}$ and let $e_1, \ldots, e_m$ be a base for V. The unit-cell U (with respect to $e_1, \ldots, e_m$) is the collection
$U := \{x \in V \mid x = \lambda_1 e_1 + \ldots + \lambda_m e_m \quad \text{with } \lambda_i = 0,1 \text{ for } i = 1\ldots m\}$.

Let A be a (m-1)-dimensional subspace of V. One might ask whether $U \cap A$ contains some non zero element . We have the following theorem:

(7.1) Theorem: Let V be a m-dimensional vectorspace over $\mathbb{F}_{p^k}$ and let A be some (m-1)-dimensional subspace of V. Let U be the Unit-cell with respect to some base of V. Then $A \cap U$ contains a non-zero element provided that $m \geq (p-1).k.1 + 1 =$

proof: consider the Vector space $V/_A$ and the canonical projection $\pi : V \to V/_A$. The additive group of $V/_A$ is isomorphic to $(\mathbb{F}^+_{p^k})^1 \cong C_p^{k.1}$

We form the $V/_A$ - sequence $S = (\pi e_1, \ldots, \pi e_m)$.
Suppose $m \geq (p-1)\, k\, 1 + 1 = \mu(C_p^{k1})$. Then S is not primitive. Thus there exists some non empty zero-subsequence $T = (\pi e_{i_1}, \ldots, \pi e_{i_\nu})$.
This means that $e_{i_1} + \ldots + e_{i_\nu} \in U \cap A$ which completes the proof.

remark: Theorem (7.1) is in fact as strong as the theorem which states that $\lambda(G) = \Lambda(G)$ for any homogeneous p-group of the form $G = (C_p)^m$. For let $(a_1, \ldots, a_N)$ be a G-sequence and let A be the subspace of $\mathbb{F}_p^N$ consisting of all N-tupples $(\lambda_1, \ldots, \lambda_N)$ such that $\lambda_1 a_1 + \ldots + \lambda_N a_N = 0$ in G then A is a subspace of dimension $\geq N - m$.

It is clear that $(a_1, \ldots, a_N)$ is not primitive iff $A \cap U$ contains a non zero element where U is the unit cell with respect to the canonical base of F_p^N .
By (7.1) then it follows that $\mu(G) \leq m.1(p-1) + 1$.
See also [8].
J.W. OLSON has given an estimate of the number of elements in $A \cap U$. See [19].

(7.2) Lemma: Let $S = (g_1, \ldots, g_m)$ be some G sequence. Then the number of solutions $\lambda_1, \ldots, \lambda_m$ with $\lambda_i = 0,1$ to the equation

$$\lambda_1 g_1 + \ldots + \lambda_m g_m = 0 \qquad (1)$$

is at least $2^{\max\{m - \lambda(G), 0\}}$

proof: By complete induction. The lemma is true for $m \leq \lambda(G)$ or $m = \lambda(G) + 1$. Suppose the lemma has been proved for $m = \lambda(G) + k$ $k \geq 1$ and let in (1) $m = \lambda(G) + k + 1$.
We may assume without less of generality that for some $t \leq \lambda(G) + 1$ we have $g_1 + g_2 + \ldots + g_t = 0$
by induction hypothesis there are at least 2^k solutions to the equation:

$$\lambda_2'(-g_2) + \ldots\ldots + \lambda_t'(-g_t) + \lambda_{t+1} g_t + \ldots\ldots + \lambda_m' g_m = 0$$

For each of these solutions we conclude:

$$g_1 + (1-\lambda_2')g_2 + \ldots + (1-\lambda_t')g_t + \lambda_{t+1}' g_t + \ldots + \lambda_m' g_m = 0$$

which gives us a solution of (2) with $\lambda_1 = 1$. Hence we have at least 2^k solutions with $\lambda_1 = 1$.

By induction we have also at least 2^k solutions of

$$\lambda_2' g_2 + \ldots + \lambda_t' g_t + \lambda_{t+1}' g_{t+1} + \ldots\ldots + \lambda_m' g_m = 0$$

which gives us $\geq 2^k$ solutions of (1) with $\lambda_1 = 0$.

Taking all the solutions together we see that there are at least $2^k + 2^k = 2^{k+1}$ solutions to (1).

(7.3) <u>theorem</u>: [J.E. OLSON]: Let V be a m-dimensional Vectorspace over $\mathbb{F}_{p^k}$ and let A be some m-1 dimensional subspace of V. Let U be the unit-cell with respect to some base of V. Then $A \cap U$ contains at least 2^N elements where $N = \max\{0, k.l.(p-1)\}$.

<u>proof</u>: This theorem follows by lemma (7.2) by the same construction as in (7.1) There is a 1-1 correspondence between elements of $A \cap U$ and solutions of the equation:

$$\lambda_1 \pi(e_1) + \dots + \lambda_m \pi(e_m) = 0$$

with

$$\lambda_i = 0,1 \qquad 1 \leq i \leq m.$$

The notion of the unit-cell appears also in the following proposition:

(7.4) <u>proposition</u>: Let $V = (\mathbb{F}_p)^m$ and let $e_1, \dots, e_m$ be some base for V and let U be the unit-cell with respect to this base. Then any V-sequence S of length $\geq m(p-2) + 1$ contains a subsequence T with $|T| \in U$.

<u>proof</u>: We extend S to the sequence

$S' = S \cup \{(p-1)e_1, \dots, (p-1)e_m\}$. As $l(S') \geq m(p-1)+1$ $= \mu(V^+)$ there exist a subsequence $T' \leq S'$ with value zero.

Let $T' = T \cup \{(p-1)e_{i_1}, \dots (p-1)e_{i_\nu}\}$ where $T \leq S$ then $|T| = e_{i_1} + \dots + e_{i_\nu} \in U$.

<u>remark</u>: proposition (7.4) again is as strong as the theorem which states that $\lambda(((\mathbb{F}_p)^k)^+) = k(p-1)$. Let S be a $((\mathbb{F}_p)^k)^+$-sequence of length $\geq k(p-1) + 1$. There are two possibillities:

a) S contains no subsequence of k linear independent vectors in $(F_p)^k$. Then the linear closure of S is contained in some lower-dimensional subspace of $(\mathbb{F}_p)^k$, say $A \cong (\mathbb{F}_p)^{k_o}$ with $k_o < k$.
From now on we consider S to be an A-sequence which reduces the problem to case b).

b) S contains k linear independent elements say $a_1, \ldots, a_k$. Consider the unit-cell U with respect to the base $-a_1, \ldots, -a_k$. After taking the elements $a_1, \ldots, a_k$ from S the remaining elements form a $((F_p)^k)^+$ - sequence S' of length $\geq k(p-2) + 1$. By (7.4) there is a subsequence $T' \leq S'$ with $|T| \in U$. Then we can extend T to a zero-subsequence by adjoining some of the elements $a_1, \ldots, a_k$.

(7.4) can be generalised to the following proposition.

(7.5) <u>proposition</u>: Let $V = (F_p)^m$ and let $e_1, \ldots, e_m$ be a base for V. Let U_s be the collection of all elements of the form $\lambda_1 e_1 + \ldots + \lambda_m e_m$ with $\lambda_i = 0, 1, \ldots, s$. Then any V^+-sequence S of length $\geq m(p-s-1) + 1$ contains a subsequence with value in U_s .

<u>proof</u>: By extending S by th elements:

$$\underbrace{-e_1, \ldots, -e_1}_{s\ x}, \underbrace{-e_2, \ldots, -e_2}_{s\ x}, \ldots, \underbrace{-e_m, \ldots, -e_m}_{s\ x}$$

Finaly we give an application in graph-theory.

Let A be a undirected with n vertices $X_1, \ldots, X_n$ and m edges $a_1, \ldots, a_m$ (Loops and multiple connections are permitted). If a_j is a vertex from X_{s_j} to X_{t_j} ($s_j = t_j$ when a_j is a loop) we put:

$$g_j = \begin{pmatrix} \delta_{1s_j} + \delta_{1t_j} \\ \vdots \\ \delta_{ns_j} + \delta_{nt_j} \end{pmatrix} \quad (C_q)^n . \quad (\delta_{ij} \text{ is the Kronecker symbol})$$

Hence g_j is a vector with one coordinate = 2 when g_j is a loop or two coordinates = 1 when g_j is a proper edge and the remaining coordinates equal 0. This way we construct for every graph A with n vertices a $(C_q)^n$ sequence $S_A = (g_1, \ldots, g_m)$.

The subsequences of S_A correspond to subgraphs of A derived from A by deleting some edges from A.
It is clear that the sum of the i-th coordinates of the vectors g_j from S_A is equal to the local order of the graph A at the vertex X_i.
Now we formulate our next proposition:

(7.6) <u>proposition:</u> Let A be an undirected graph with n vertices and m edges and let q be some prime-power $q = p^k$. Suppose $m \geq n(q-1) + 1$. Then A contains some non empty subgraph A' such that the local order of A' at each vertex of A is divisible by q.

<u>proof</u>: Consider the sequence S_A. As

$$l(S_A) = m \geq n(q-1) + 1 = \mu((C_q)^n) \quad \text{we}$$

derive that S_A contains some non empty zero-subsequence S'. The corresponding subgraph A' has the desired property.

For q = 2 (7.6) is trivial as any graph consisting of more edges then vertices contains at least one cycle.

§ 8 Counter-example to the conjecture $\Lambda(G) = \lambda(G)$, unsolved problems.

(8.1) Theorem [P.C. BAAYEN]. For $G = (C_2)^{4k} \oplus C_{4k+2}$ $k \geq 1$ we have $\lambda(G) \geq M(G) = \Lambda(G) + 1$.

proof: We write $G = (C_2)^{4k+1} \oplus C_{2k+1}$. Let π_1 and π_2 the canonical projections on $(C_2)^{4k+1}$ resp. C_{2k+1}. We construct a primitive G-sequence of length $M(G) = 4k + 4k + 2 = 8k + 2$. Let $e_1, \ldots, e_{4k+1}$ be a base for $(C_2)^{4k+1}$ and put $d = e_1 + \ldots + e_{4k+1}$. A <u>nearly - diagonal element</u> is an element $f_j = d + e_j = d - e_j$.

Now consider the sequence

$$S = \begin{pmatrix} e_1 \\ 1 \end{pmatrix}, \begin{pmatrix} e_2 \\ 1 \end{pmatrix}, \ldots\ldots, \begin{pmatrix} e_{4k+1} \\ 1 \end{pmatrix}, \begin{pmatrix} f_1 \\ 1 \end{pmatrix}, \ldots\ldots, \begin{pmatrix} f_{4k+1} \\ 1 \end{pmatrix}.$$

Then $l(S) = M(G) = 2(4k + 1)$. We show that S is primitive. It is sufficient to show that each zero-sequence of $\pi_1 S$ has a length which is not divisible by $2k + 1$.

From the symmetry of S with respect to permutations of the base elements $e_j \in (C_2)^{4k+1}$ it follows that the length of a zero-sequence of πS is completely determined by the number of nearly-diagonal elements contained in it.

Consider a som of t nearly-diagonal elements. This is a vector with exactly t coordinates = 1 whenever t is even and $4k + 1 - t$ coordinates = 1 when t is odd. To complete such a sequence to form a zero-sequence we need t respectively $4k + 1 - t$ base elements e_j.

Thus the length of a zero-subsequence of $\pi_1 S$ is equal $2t$ when t is even and $4k + 1$ when t is odd.

Now we have $\quad 1 \leq t \leq 4k + 1$.

As $(2k + 1, 4k + 1) = 1$ no zero-subsequence of $\pi_1 S$ with an odd number of nearly-diagonal elements has length divisible by $2k + 1$. However when this number is even we have $t = 2s$ with $1 \leq s \leq 2k$ and therefore the length of such a zero-subsequence of $\pi_1 S$ is equal $4s$ $1 \leq s \leq 2k$ which number is not divisible by $2k + 1$. as $(4, 2k + 1) = 1$. This completes the proof.

The smallest example of this series is the group $(C_2)^4 \oplus C_6$ There the sequence S is given by:

$$S = \begin{array}{|ccccc|ccccc|l}
\hline
1&0&0&0&0&0&1&1&1&1& \\
0&1&0&0&0&1&0&1&1&1& (C_2)^5 \\
0&0&1&0&0&1&1&0&1&1& \\
0&0&0&1&0&1&1&1&0&1& \\
0&0&0&0&1&1&1&1&1&0& \\
\hline
1&1&1&1&1&1&1&1&1&1& C_3 \\
\hline
\end{array}$$

(8.2) <u>corollary</u>: For any integer N there exist a finite Abelian group G for which $\lambda(G) - \Lambda(G) \geq N$.

<u>proof</u>: We have $\lambda(G) \geq \Lambda(G) + 1$ for $G = (C)^4_2 \oplus C_6$ by (1.16) we therefore conclude

$$\lambda(G^N) \geq N.\lambda(G) \geq N.\Lambda(G) + N = \Lambda(G^N) + N.$$

<u>Unsolved problems</u>:

I) The classes I,II, III, IV, V, and VI contain all groups G with $\omega(G) \leq 100$ except the two groups $(C_2)^4 \oplus C_6$ for which $\lambda(G) \geq \Lambda(G) + 1$ and $(C_3)^2 \oplus C_6$ for which it is unknown whether $\lambda(G) = \Lambda(G)$. Determine $\lambda(G)$ for these two groups.

II) Is condition (C) satisfied for all primes p?

III) Does there exist any counter-example for $\lambda = \Lambda$ of dimension ≤ 4?

IV) How "large" becomes the "excess" $\lambda(G) - \Lambda(G)$ compared to the order of G; for example is the relation

$$\limsup_{\omega(G)\to\infty} \frac{\lambda(G) - \Lambda(G)}{\omega(G)} = 0 \qquad \text{true?}$$

V) Is the equality $\nu(G) = \lambda(G) - 1$ generally true? .

References.

[1] P.C. BAAYEN. Een combinatorisch probleem voor eindige Abelse groepen. MC Syllabus 5. Colloquium Discrete Wiskunde Caput 3. (1968). Mathematical Centre Amsterdam.

[2] P.C. BAAYEN. Een geval van een structuurprobleem voor Abelse groepen . WN 24. Mathematical Centre Amsterdam (1968).

[3] P.C. BAAYEN. Een combinatorisch vermoeden bevestigd voor $C_2 \oplus C_2 \oplus C_2 \oplus C_6$. WN 25. Mathematical Centre Amsterdam (1968).

[4] P.C. BAAYEN. $(C_2 \oplus C_2 \oplus C_2 \oplus C_{2n})!$ is true for odd n. Report ZW-1969-006. Mathematical Centre Amsterdam. (to appear).

[5] P.C. BAAYEN. P. VAN EMDE BOAS, D. KRUYSWIJK. A combinatorial problem on Finite Abelian groups III. Report ZW-1969-008 Mathematical Centre Amsterdam (to appear).

[6] C. CHEVALLEY. Démonstration d'une hypothèse de M. ARTIN. Abh. Math. Sem. Univ. Hamburg 11 (1936), 73-75.

[7] H. DAVENPORT. Proceedings of the Midwestern Conference on Group theory and Number theory. Ohio State University, April 1966.

[8] P. VAN EMDE BOAS, D. KRUYSWIJK. A combinatorial problem on finite Abelian groups. Report ZW-1967-009. Mathematical Centre Amsterdam (1967).

[9] P. VAN EMDE BOAS. Some ALGOL 60 Algorithms for the verification of combinatorial conjectures on finite Abelian groups. Report ZW-1968-014 (to appear).

[10] P. ERDÖS, A. GINSBURG, A. ZIV. Theorem in the additive number theory. Bulletin of the research counsil of Israel. 10 F (1961) 41-43.

[11] S. LANG. Algebra. Caput V, Exercise 6. Addison-Wesley publishing company Inc. Reading Massachusetts.

[12] J.H. VAN LINT. $(C_2 \oplus C_2 \oplus C_6)$! is true. Note 26 onderafdeling der wiskunde. T.H. Eindhoven. (1968).

[13] J.H. VAN LINT. $(C_2 \oplus C_2 \oplus C_{2p})$! is true. Note 27 onderafdeling der wiskunde. T.H. Eindhoven (1968).

[14] H.B. MANN. Two addition theorems. Journal of combinatorial theory 3 (1967) 233-235.

[15] H.B. MANN, J.E. OLSON. Sums of Sets in the elementary Abelian groups of type (p,p). Journal of combinatorial theory 2 (1967) , 275-284.

[16] P. NOORDZIJ. Rapport nr. 4 Wiskundig Seminarium der Vrije Universiteit.

[17] J.E. OLSON . An addition theorem for the Elementary Abelian group. Journal of Combinatorial theory 5 (1968), 53-58.

[18] J.E. OLSON. An addition theorem modulo p. Journal of combinatorial theory 5 (1968), 45-52.

[19] J.E. OLSON. A combinatorial problem on finite Abelian groups. I & II. I Journal of Number theory 1 (1969) (8-11).
II Journal of Number theory (to appear).

[20] E. WEISS. Algebraic Number theory. Mc. Graw-Hill Book company Inc. (1963).

[21] H. WEYL. Algebraic theory of Numbers. Annals of Math. Studies I. Princeton (1940).