ON SMALL SUMSETS IN AN ABELIAN GROUP

BY

J. H. B. KEMPERMAN

Purdue University, Lafayette, Indiana, U.S.A. [1]

1. Introduction

Let G be an abelian group, A, B and C subsets of G. By $A+B$ we denote the set of all the elements $g \in G$ having at least one representation as a sum $g=a+b$ of an element $a \in A$ and an element $b \in B$. For each $g \in G$, the number of such representations is denoted as $\nu_g(A, B)$. Further, $H(C)$ will denote the subgroup of G consisting of all the elements $g \in G$ for which $C+g=C$, thus, $C+H(C)=C$. If $H(C) \neq \{0\}$ then C is said to be *periodic*, otherwise, *aperiodic*. Finally, $[C]$ denotes the number of elements in C.

In this paper, we shall determine the structure of those pairs (A, B) of non-empty finite subsets of G for which

$$[A+B] < [A]+[B]. \tag{1}$$

In view of Theorem 3.1 due to Kneser [4], [5] it suffices to consider the case that $A+B$ is aperiodic and

$$[A+B]=[A]+[B]-1, \tag{2}$$

cf. Theorem 3.4. If (2) holds, $2 \leqslant [A] < \infty$, $2 \leqslant [B] < \infty$, then (Theorem 2.1) either $A+B$ is in arithmetic progression or $A+B$ is the union of a non-empty periodic set C' and a subset C'' of some $H(C')$-coset. On the basis of such information on $A+B$, one can study the structure of the pair (A, B) itself, see section 4. The final result is Theorem 5.1; here besides (2) it is assumed that $\nu_c(A, B)=1$ has a solution c in case $A+B$ is periodic. Theorem 5.1 completely determines the (rather complicated) structure of the pairs (A, B) satisfying (1), cf. the discussion at the end of section 5.

[1] This work was supported by the National Science Foundation, research grants NSF–G 1979, NSF–G 5226.

For the special case that G is cyclic of prime order, this structure was already established by Vosper [8] (see also the Corollary to Lemma 4.3).

In view of a result due to Kneser [6], p. 89 (namely, a generalization of his Theorem 3.1 to abelian locally compact groups), the Structure Theorem 5.1 also solves the problem of determining the structure of those pairs (A, B) of non-empty measurable subsets of an abelian locally compact group G for which

$$\mu_*(A+B)<\mu(A)+\mu(B);$$

here, μ denotes a fixed Haar measure on G, μ_* the inner measure induced by μ.

The Structure Theorem 5.1 is also a useful tool in investigating the function $\nu_c(A, B)$, (A and B fixed). As an illustration, we shall derive in the final section 6 some curious results of the following type. Let A, B be finite non-empty subsets of an abelian group G such that

$$[A]+[B]-[A+B]=\varrho\geqslant 1.$$

It was shown by Scherk [7] that $\nu_c(A, B)\geqslant\varrho$ holds for each element $c\in A+B$ (see also section 3); let n denote the number of elements c for which $\nu_c(A, B)=\varrho$. Assertion: for each element c, we have $\nu_c(A, B)\geqslant n$ as soon as $\nu_c(A, B)>\varrho$.

2. Small sumsets in a discrete group

In this paper, all groups considered are discrete abelian groups. Let G be such a group.

Definition. A subset C of G is said to be *quasi-periodic* if there exists a subgroup F of G of order $[F]\geqslant 2$ (a so-called *quasi-period* of C), such that C is the disjoint union of a *non-empty* set C' consisting of F-cosets (that is $C'+F=C'$), and a residual set C'' contained in a remaining F-coset (that is $C''\subset c+F$ if $c\in C''$).

Observe that $[2]\leqslant[F]\leqslant[C]$ for each quasi-period F of C, hence, if each element $g\neq 0$ in G is of order $>[C]$ then C cannot possibly be quasi-periodic. Further, each periodic set is also quasi-periodic.

Definition. A subset C of G is said to be in *arithmetic progression* if C is of the form $C=\{c_0+jd;\ j=0, 1, \ldots, [C]-1\}$. If so, d is called a *difference* of C; note that d is necessarily of order $\geqslant[C]$.

It is important to find the precise structure of the pairs A, B of finite subsets of G satisfying

$$[A+B]=[A]+[B]-1, \tag{1}$$

cf. Theorem 3.4. As a first step in determining this structure, we shall prove:

THEOREM 2.1. *Let A, B be finite subsets of G such that* (1) *holds and* $[A]\geqslant 2$, $[B]\geqslant 2$. *Then either $A+B$ is in arithmetic progression or $A+B$ is quasi-periodic.*

The proof of Theorem 2.1 makes use of the second assertion of the following Lemma 2.2. The proof of Lemma 2.2 is a refinement of Kneser's [4, 467] proof of the first assertion (3).

LEMMA 2.2. *Suppose that the finite subset C of G is the union of the proper non-empty subsets $C_0, \ldots, C_n$ $(n\geqslant 1)$ in such a way that*

$$[C]<[C_i]+[H(C_i)], \qquad (i=0, 1, \ldots, n). \tag{2}$$

Then

$$[C]+[H(C)]\geqslant [C_i]+[H(C_i)] \tag{3}$$

holds for at least one $i=0, \ldots, n$. Moreover, either C is quasi-periodic or, for some $c\in C$, we have $C-c=H_1\cup H_2$, where H_1, H_2 denote finite subgroups of G of equal order with $H_1\cap H_2=\{0\}$.

COROLLARY (Kneser). *Let $C_0, \ldots, C_n$ be finite non-empty sets with*

$$[C_i]+[H(C_i)]\geqslant \alpha, \qquad (i=0, \ldots, n).$$

Then $C=C_0\cup\cdots\cup C_n$ satisfies $[C]+[H(C)]\geqslant\alpha$.

Proof of Lemma 2.2. Let I_k denote the statement that Lemma 2.2 holds true for $n=k$. Let n denote a fixed integer, $n\geqslant 2$, and suppose that I_k holds for $k=1, \ldots, n-1$. Consequently, in proving I_n, it may be assumed that C is not equal to the union of less than $n+1$ among the sets $C_0, \ldots, C_n$. Put $C_1'=C_1\cup\cdots\cup C_n$. Then $C_1, \ldots, C_n$ are proper subsets of C_1' while C_0, C_1' are proper subsets of C. From (2) and I_{n-1}, we have $[C_1']+[H(C_1')]\geqslant [C_i]+[H(C_i)]>[C]$ for at least one index $i=1, \ldots, n$. Hence, in view of $C_0\cup C_1'=C$, $[C_0]+[H(C_0)]>[C]$, I_1 implies the stated assertion I_n. It remains to prove I_1.

We now assume $n=1$. Thus,

$$C=C_0\cup C_1, \quad C_0\neq C, \quad C_1\neq C. \tag{4}$$

Let $H(C_i)=H_i$, thus, from the definition of $H(C_i)$,

$$C_i+H_i=C_i, \qquad (i=0, 1). \tag{5}$$

Further, put $H_0+H_1=H^*$, $H_0\cap H_1=H$, $[H]=h$ and let m_i denote the index of H_i in the group H^*, thus,

$$[H^*]=m_0m_1h, \ [H_0]=m_1h, \ [H_1]=m_0h.$$

From (5), $\bar{C}_i \cap C_j$ is the union of H-cosets ($\bar{C}_i$ denoting the complement of C_i in G), hence, from (2) and (4),

$$0 < [\bar{C}_i \cap C_j] \leqslant (m_j - 1)\, h; \tag{6}$$

here, and in the sequel, $i = 0, 1$, while $j = 1 - i$. From (4) and (5), $C + x = C$ for $x \in H$, thus, $[H(C)] \geqslant h$, consequently, in proving (3), it suffices to show that

$$[\bar{C}_i \cap C_j] = (m_j - 1)\, h. \tag{7}$$

Interchanging the indices, if necessary, we may assume $[H_0] \geqslant [H_1]$, thus, $m_0 \leqslant m_1$. From (6), there exists an element $c_0 \in \bar{C}_1 \cap C_0$. Let c_0 be fixed. Then

$$D = c_0 + H^* \textit{ satisfies } [\bar{C}_1 \cap C_0 \cap D] > 0. \tag{8}$$

Note that the intersection of an H_0-coset in D and an H_1-coset in D is precisely an H-coset. From (5), $C_i \cap D$ is the union of (say) u_i cosets of H_i, $0 \leqslant u_i \leqslant m_i$, thus, $\bar{C}_i \cap D$ is the union of $m_i - u_i$ cosets of H_i. Consequently,

$$[\bar{C}_0 \cap C_1 \cap D] = (m_0 - u_0)\, u_1 h, \tag{9}$$

and

$$0 < [\bar{C}_1 \cap C_0 \cap D] = (m_1 - u_1)\, u_0 h \leqslant (m_0 - 1)\, h \leqslant (m_1 - 1)\, h, \tag{10}$$

in view of (6), (8), $m_0 \leqslant m_1$. From (10),

$$1 \leqslant u_0 \leqslant m_0 - 1, \qquad 1 \leqslant u_1 \leqslant m_1 - 1. \tag{11}$$

We now have, from (9), (10) and (11),

$$-\sum_{i=0}^{1} \{(m_j - 1)\, h - [\bar{C}_i \cap C_j]\} - \sum_{i=0}^{1} [\bar{C}_i \cap C_j \cap \bar{D}]$$
$$= \sum_{i=0}^{1} \{[\bar{C}_i \cap C_j \cap D] - (m_j - 1)\, h\} = (m_0 - u_0 - 1)(u_1 - 1) + (m_1 - u_1 - 1)(u_0 - 1) \geqslant 0.$$

It follows from (6) that: (i) (7) and, thus, (3) holds; (ii) Either $u_1 = 1$ or $u_0 = m_0 - 1$; moreover, either $u_0 = 1$ or $u_1 = m_1 - 1$; (iii) Finally, $[\bar{C}_i \cap C_j \cap \bar{D}] = 0$, $(i = 0, 1)$.

Let $C' = C \cap \bar{D}$. From (iii) and (4), $C' = C_0 \cap \bar{D} = C_1 \cap \bar{D}$. From (5) and (8), $C' + H^* = C'$. Note that, from (6), $m_j \geqslant 2$, thus, $[H_i] \geqslant 2$. If C' is non-empty then H^* is a quasi-period of C. If $h \geqslant 2$ then, from $C + H = C$, H is a quasi-period of C. If $u_0 = m_0 - 1$ then H_0 is a quasi-period of C, similarly, if $u_1 = m_1 - 1$. Consequently, if C is not quasi-periodic then C' is empty, $H_0 \cap H_1 = H = \{0\}$ and $u_0 = u_1 = 1$, hence, C is the union of an H_0-coset in D and an H_1-coset in D. Moreover, from (7) and (9), $m_1 - 1 = m_0 - 1$, thus, $[H_0] = [H_1]$. This proves Lemma 2.2.

Proof of Theorem 2.1. For brevity, put $A+B=C$. Assume first that to each element $b_i \in B$ there corresponds a set C_i such that $C_i \neq C$ and

$$A+b_i \subset C_i \subset C; \qquad [C_i]+[H(C_i)]>[C]. \tag{12}$$

Especially, $C=A+B$ is the union of the *proper* subsets C_i. Suppose that C is not quasi-periodic. Then, from (12) and Lemma 2.2, there exists an element $c_0=a_0+b_0$ ($a_0 \in A$, $b_0 \in B$) in $C=A+B$ and finite subgroups H_1, H_2 of equal order such that $H_1 \cap H_2=\{0\}$ and $A+B-c_0=H_1 \cup H_2$. Hence, $A'=-a_0+A$ and $B'=B-b_0$ satisfy $A'+B'=H_1 \cup H_2$, $A' \subset H_1 \cup H_2$, $B' \subset H_1 \cup H_2$, $[A'] \geqslant 2$, $[B'] \geqslant 2$.

Let $a \in A'$, $a \neq 0$, $a \in H_1$ (say), thus, $a \notin H_2$. Then $b \in B' \cap H_2$ implies $a+b \in H_1 \cup H_2$, hence, $b=0$, consequently, $B' \subset H_1$. Taking $b \in B'$, $b \neq 0$, we have in a similar fashion that $A' \subset H_1$, hence, $H_1 \cup H_2=A'+B' \subset H_1$ which is impossible.

Next, suppose that there exists an element $b_i \in B$ such that (12) always implies $C_i=C$. Replacing B by the set $B-b_i$, we may assume $b_i=0 \in B$, thus,

$$A \subset C_0 \subset C, \ [C_0]+[H(C_0)]>[C] \ \textit{imply} \ C_0=C. \tag{13}$$

Now, consider a pair A_0, B_0 of finite subsets of G such that:

(i) $A \subset A_0$, $0 \in B_0$, $A_0+B_0 \subset C$ (thus, $A_0 \subset C$), $[B_0] \geqslant 2$ and

$$[A_0]+[B_0]=[C]+1; \tag{14}$$

(from (1) and $[B] \geqslant 2$, these relations hold for $A_0=A$, $B_0=B$);

(ii) Subject to (i), $[A_0]$ is maximal.

Suppose first that $A_0+B_0=A_0$, thus, $[H(A_0)] \geqslant [B_0]$. From $A \subset A_0=A_0+B_0 \subset C$, (14) and (13), we have $A_0=C$, hence, from (14), $[B_0]=1$, a contradiction.

Therefore, the set D_1 (say) of elements $a \in A_0$ with $a+B_0' \not\subset A_0$ is non-empty. Here, B_0' shall denote the non-empty set obtained from B_0 by deleting the element 0. Thus, from (14),

$$[B_0']=[B_0]-1=[D_0], \ \textit{where} \ D_0=C \cap \bar{A}_0 \tag{15}$$

($\bar{A}_0$ denoting the complement of A_0 in G).

Let $a \in D_1$. It is easily seen that the pair of sets

$$A_1=A_0 \cup (a+B_0'), \qquad B_1=B_0 \cap (-a+A_0)$$

satisfies

$$A \subset A_1, \ 0 \in B_1, \ A_1+B_1 \subset A_0+B_0 \subset C, \ [A_1]+[B_1]=[A_0]+[B_0]=[C]+1 \ \textit{and} \ [A_1]>[A_0].$$

Consequently, from the maximal character of $[A_0]$, we have $[B_1]=1$, hence, $[A_1]=[C]$. It follows from $A_1\subset A_1+B_1\subset A_0+B_0\subset C$ that $C=A_1$, thus,

$$D_0=C\cap \bar{A}_0=A_1\cap \bar{A}_0\subset a+B_0',$$

hence, from (15),

$$a\in D_1 \textit{ implies } a+B_0'=D_0. \tag{16}$$

Generalizing the definition of D_1, let $D_m\,(m\geqslant 1)$ denote the set of all those elements $a\in A_0$ such that m is equal to the *smallest* number of elements $b_1, \dots, b_m$ in B_0' for which $a+b_1+\cdots+b_m\notin A_0$. Let k denote the largest integer m for which D_m is non-empty. Finally, let D_∞ denote the set of all elements $a\in A_0$ satisfying

$$a+b_1+\cdots+b_n\in A_0$$

for each choice of the elements $b_1, \dots, b_n$ in B_0'. Here, the D_j are disjoint, while (from $A_0\subset C$, $D_0=C\cap\bar{A}_0$)

$$A_0=D_\infty\cup D_k\cup\cdots\cup D_1; \qquad C=D_\infty\cup D_k\cup\cdots\cup D_1\cup D_0. \tag{17}$$

Clearly, $D_\infty+B_0'=D_\infty$. We assert that, moreover,

$$a\in D_m \textit{ implies } a+B_0'=D_{m-1} \qquad (m=1, \dots, k). \tag{18}$$

From (16), (18) holds for $m=1$. Let $m\geqslant 2$, $a\in D_m$ and $b'\in B_0'$. From the definition of D_m, $a+b'\in D_j$ for some $j\geqslant m-1$, while there exist elements $b_1, \dots, b_{m-1}$ in B_0' with $a_1=a+b_1+\cdots+b_{m-1}\in D_1$, thus, $(a+b')+b_1+\cdots+b_{m-1}=a_1+b'\notin A_0$, from (16), showing that $a+b'\in D_j$ for some $j\leqslant m-1$, consequently, $a+b'\in D_{m-1}$. This proves

$$a\in D_m \textit{ implies } a+B_0'\subset D_{m-1} \qquad (m=1, \dots, k). \tag{19}$$

Especially, $D_m+B_0'\subset D_{m-1}$, hence, $[D_m]\leqslant[D_{m-1}]$ $(m=1, \dots, k)$, thus,

$$[B_0']=[a+B_0']\leqslant[D_{m-1}]\leqslant[D_0]=[B_0']$$

and (19) implies (18).

For $1\leqslant m\leqslant k$, let F_m denote the group generated by all the differences a_1-a_2 of elements a_1, a_2 in D_m, thus, D_m is contained in an F_m-coset, $[F_m]\geqslant 2$ if and only if $[D_m]\geqslant 2$. From (18), $a_1+B_0'=a_2+B_0'$ if $a_1, a_2\in D_m$, hence, $B_0'+F_m=B_0'$, thus, F_m is finite while, from (18) and $D_\infty+B_0'=D_\infty$,

$$D_j+F_m=D_j \textit{ if } j=0, 1, \dots, k-1 \textit{ or } j=\infty. \tag{20}$$

From (17) and (20), F_k is a quasi-period of C provided that $[D_k]\geqslant 2$, thus, assume $[D_k]=1$, that is, D_k consists of a single element c_k. But then, from (17) and (20),

F_m is a quasi-period of C provided that $[D_m]\geqslant 2$, thus, assume $[D_m]=1$ $(m=1, \ldots, k)$. Finally, if D_∞ is non-empty then, from $D_\infty+B_0'=D_\infty$, (17) and (18), the group generated by B_0 is a quasi-period of C, thus, assume that D_∞ is empty.

If $k=1$ then, from (17), $[A_0]=[D_1]=1$, contradicting $[A_0]\geqslant[A]\geqslant 2$. Applying (18) for $m=2$, we have $[B_0']=[D_1]=1$, hence, B_0' consists of a single element $d\neq 0$. From (18), D_{k-m} consists of the single element c_k+md $(m=0, 1, \ldots, k)$. The D_j being disjoint, these $k+1$ elements are distinct, thus, from (17), C is an arithmetic progression of difference d. This completes the proof of Theorem 2.1.

3. Auxiliary results

In the subsequent sections, we shall frequently need the following result due to Kneser [5], [6]. For the benefit of the reader, Kneser's proof is given below.

THEOREM 3.1. *Let A, B be finite non-empty subsets of the (abelian) group G satisfying*

$$[A+B]\leqslant[A]+[B]-1. \tag{1}$$

Then $H=H(A+B)$ satisfies

$$[A+B]+[H]=[A+H]+[B+H]. \tag{2}$$

Hence, $A+B$ is periodic if

$$[A+B]\leqslant[A]+[B]-2.$$

Proof. Let b_i denote a fixed element in B. Consider a pair A_i, B_i of finite subsets of G such that:

(i) $A\subset A_i$, $b_i\in B_i$, $A_i+B_i\subset A+B$ and

$$[A_i]+[B_i]=[A+H]+[B+H]; \tag{3}$$

(from $A+B+H=A+B$, $A_i=A+H$, $B_i=B+H$ is such a pair);

(ii) Subject to (i), $[A_i]$ is maximal.

Let $C_i=A_i+B_i$, thus,

$$A+b_i\subset C_i\subset A+B. \tag{4}$$

Let $a\in A_i$. It is easily seen that the pair

$$A_i'=A_i\cup(a+B_i-b_i), \quad B_i'=B_i\cap(-a+A_i+b_i)$$

satisfies (i) and $A_i\subset A_i'$, thus, $A_i'=A_i$. Consequently, $a+B_i-b_i\subset A_i$, for each $a\in A_i$, hence, $A_i=A_i+B_i-b_i=C-b_i$ and $H(C_i)=H(A_i)\supset B_i-b_i$, thus, from (3),

$$[C_i] + [H(C_i)] \geqslant [A+H] + [B+H]. \tag{5}$$

From (4), $A+B$ is the union of the sets C_i $(b_i \in B)$, hence,

$$[A+B] + [H] \geqslant [A+H] + [B+H], \tag{6}$$

from $H = H(A+B)$ and the Corollary to Lemma 2.2. If (2) were false then, all terms in (6) being multiples of $[H]$, we would have $[A+B] \geqslant [A+H] + [B+H]$, contradicting (1). This proves Theorem 3.1.

For the moment, let G denote an additively written semigroup (commutative or not) in which the left and right cancellation laws hold. If A, B are subsets of G and $g \in G$ then $\nu_g(A, B)$ shall denote the number of different representations of g as a sum $g = a + b$ $(a \in A,\ b \in B)$. The following result will be needed for the special case only that G is an abelian group.

THEOREM 3.2. *Let A, B be finite subsets of G. Then, for each element $c \in A+B$,*

$$\nu_c(A, B) \geqslant [A] + [B] - [A+B]. \tag{7}$$

That $c \in A+B$ implies (7) was shown in [3] under the condition that c possesses an inverse in an apropriate extension in G. But by a recent result of Liapin (cf. [2], no. 21), each element of G has this property.

Now, assume again that G is an abelian group. For this case, Theorem 3.2 was first proved by Scherk [7]. It can be strengthened as follows.

LEMMA 3.3. *Let G be an abelian group, A and B finite non-empty subsets of G. Put $H(A+B) = H$ and*

$$[A] + [B] - [A+B] = \varrho, \tag{8}$$

thus (from Theorem 3.1), H is a finite group of order $\geqslant \varrho$. Let $a_0 \in A$, $b_0 \in B$ be fixed, $c_0 = a_0 + b_0$. Then each element $c \in c_0 + H$ has at least ϱ representations of the form

$$c = a + b \text{ with } a \in A \cap (a_0 + H), \quad b \in B \cap (b_0 + H).$$

Proof. We may assume $\varrho \geqslant 1$, otherwise, the assertion is trivial. From Theorem 3.1 and (8),

$$[(A+H) \cap \bar{A}] + [(B+H) \cap \bar{B}] = [H] - \varrho,$$

hence,
$$[(a_0+H) \cap \bar{A})] + [(b_0+H) \cap \bar{B}] \leqslant [H] - \varrho,$$

thus,
$$[(a_0+H) \cap A] + [(b_0+H) \cap B] \geqslant [H] + \varrho,$$

showing that, for each $h \in H$, the subsets $(a_0+H) \cap A$ and $(a_0 + b_0 + h) - ((b_0+H) \cap B)$ of $a_0 + H$ have at least ϱ elements in common.

The following result shows that, in characterizing the pairs of finite sets satisfying (9), it would suffice to consider the case that $A+B$ is aperiodic (in which case (9) holds with the equality sign). We shall however also be interested in the case that $A+B$ is periodic, while $\nu_c(A, B)=1$ holds for at least one element c (cf. Theorem 5.1).

THEOREM 3.4. *Let G be an abelian group. The following construction yields precisely all the pairs A, B of non-empty finite subsets of G satisfying*

$$[A+B] \leqslant [A]+[B]-1. \tag{9}$$

Construction: *Choose a finite subgroup H of G and, further, a pair of non-empty finite subsets A^*, B^* of G/H such that A^*+B^* is aperiodic and*

$$[A^*+B^*]=[A^*]+[B^*]-1. \tag{10}$$

Finally, let A be any subset of $\sigma^{-1}A^*$, B any subset of $\sigma^{-1}B^*$ such that

$$[\sigma^{-1}A^* \cap \bar{A}]+[\sigma^{-1}B^* \cap \bar{B}]<[H]; \tag{11}$$

here, σ denotes the quotient mapping $G \to G/H$.

Proof. (i) The above construction yields a pair A, B satisfying (9). For, using (11) and (10),

$$\begin{aligned}[A]+[B] &> [\sigma^{-1}A^*]+[\sigma^{-1}B^*]-[H]=([A^*]+[B^*]-1)[H]\\ &=[A^*+B^*][H]=[\sigma^{-1}(A^*+B^*)] \geqslant [A+B],\end{aligned}$$

in view of $\sigma(A+B)=\sigma A+\sigma B \subset A^*+B^*$.

(ii) Suppose that (9) holds. Let $H=H(A+B)$, thus, H is a finite group satisfying $A+B+H=A+B$ and (2), from Theorem 3.1. Let σ denote the quotient mapping $G \to G/H$ and put $A^*=\sigma A$, $B^*=\sigma B$. From $A+B+H=A+B$, (2) implies (10). From $\sigma^{-1}A^*=A+H$ and $\sigma^{-1}B^*=B+H$, (9) and (2) imply (11). Finally, if $A^*+B^*+x=A^*+B^*$ then, for $g \in \sigma^{-1}x$, we have $A+B+g=A+B$, hence, $g \in H$, thus, $x=0$.

4. From sum to components

Again, G shall denote an abelian group, A and B finite non-empty subsets of G. If

$$[A+B] \leqslant [A]+[B]-1, \tag{1}$$

$[A] \geqslant 2$, $[B] \geqslant 2$, then, from Theorem 2.1 and Theorem 3.1, either $A+B$ is in arithmetic progression or $A+B$ is quasi-periodic. Problem: given such information on

$A+B$, what can be said about the pair A, B itself? Let us first consider the simple case that $A+B$ is either a coset or a coset with one element deleted.

LEMMA 4.1. *Let H denote a finite subgroup of G. In order that* (1) *holds and $A+B$ coincide with an H-coset, it is necessary and sufficient that each of A, B is a subset of some H-coset in such a way that $[A]+[B]>[H]$.*

Proof. Obvious.

LEMMA 4.2. *Let H denote a finite subgroup of G. In order that* (1) *holds and that $A+B$ is obtained from an H-coset by deleting one element c_0, it is necessary and sufficient that A is an aperiodic subset of some H-coset, while B is of the form $B=c_0-\bar{A}\cap(a+H)$ $(a\in A)$. If so,* (1) *holds with the equality sign.*

Proof. Necessity. Clearly, $A+B$ is aperiodic, hence, A is an aperiodic subset of the coset $a+H$ $(a\in A)$. Moreover, from (1), $[B]\geqslant[H]-[A]=[B']$, where $B'=c_0-$ $-\bar{A}\cap(a+H)$. It is easily seen that $B\subset B'$, hence, $B=B'$ and (1) holds with the equality sign.

Sufficiency. Put $A+B=C$. Clearly, $C\in c_0+H$, $c_0\notin C$, $[C]<[H]=[A]+[B]$. Suppose that $[C]\leqslant[H]-2$. Then, from Theorem 3.1, $[F]\geqslant 2$ where $F=H(C)$. Thus, A being aperiodic, $[A+F]>[A]$, hence, $[A+F]+[B]>[H]$. But then $C=(A+F)+B$ would occupy the full coset c_0+H, contradicting $c_0\notin C$. This proves Lemma 4.2.

Now, let us consider the case that (1) holds with $A+B$ as an arithmetic progression of difference $d\neq 0$. The following lemma shows that also A and B are in arithmetic progression provided that $[A+B]\leqslant[H]-2$, where H denotes the cyclic group generated by d. On the other hand, the sufficient conditions of Lemma 4.1 and Lemma 4.2 show that this is no longer true if $[A+B]=[H]$ or $[A+B]=[H]-1$.

LEMMA 4.3. *Suppose that* (1) *holds and that $A+B$ is in arithmetic progression of difference $d\neq 0$. Suppose further that $[A+B]\leqslant n-2$, where n denotes the order of the element d. Then also A and B are in arithmetic progression of difference d. Moreover, in* (1) *the equality sign holds.*

Proof. Let H denote the cyclic subgroup of G generated by d, $[H]=n\leqslant\infty$. Replacing A by $-a_0+A$ $(a_0\in A)$ and B by $B-b_0$ $(b_0\in B)$, we may assume $0\in A$, $0\in B$, thus, $0\in A+B\subset H$, $A\subset H$, $B\subset H$. In this proof, all sets considered are subsets of H, thus, $\bar{D}$ will denote the complement of D in H. Further, a set D is said to be in arithmetic progression iff it is of the form $\{jd;\ j=j_0,\ \dots,\ j_0+[D]-1\}$. The case $n=\infty$ being rather trivial ($A+B$ filling the entire interval between the sum of the smallest and the sum of the largest elements in A and B), we shall assume $n<\infty$. Further, we shall need the following lemma.

If P, Q are non-empty sets, $[P+Q]<n$, $P+Q$ in arithmetic progression then

$$[P+Q] \geqslant [P]+[Q]-1.$$

For, it is easily seen that $P+Q$ cannot possibly be periodic, thus, the assertion follows from Theorem 3.1. Actually, we need this lemma only for the special case that also P is in arithmetic progression. For this case, we have the following elementary proof.

Shifting P and Q,

let $$P=\{jd;\ j=0,\ 1,\ \ldots,\ k-1\}$$

and $$P+Q=\{jd;\ j=0,\ 1,\ \ldots,\ m-1\},$$

where $$k \leqslant m<n,\ md \notin P+Q.$$

Now, $P+qd=\{jd;\ j=q,\ \ldots,\ q+k-1\} \subset P+Q$ implies that q is one of the integers $0,\ 1,\ \ldots,\ m-k$, hence, $[Q] \leqslant m-k+1=[P+Q]-[P]+1$.

Let us proceed with the proof of Lemma 4.3. Put $A+B=C$, thus, $\bar{C}-B \subset \bar{A}$, hence, from (1),

$$[\bar{C}-B] \leqslant [\bar{A}] \leqslant [\bar{C}]+[B]-1. \tag{2}$$

Moreover, C being in arithmetic progression, also $\bar{C}$ is in arithmetic progression, $[\bar{C}] \geqslant 2$. It suffices to prove that $\bar{C}-B$ is in arithmetic progression. For then, from $[\bar{C}-B] \leqslant [\bar{A}]<n$ and the above lemma, $[\bar{C}-B] \geqslant [\bar{C}]+[B]-1$. Hence, in (2) and (1] the equality signs hold, thus, $\bar{A}=\bar{C}-B$ is in arithmetic progression, consequently, A and (similarly) B is in arithmetic progression.

On the contrary, suppose that $\bar{C}-B$ is the union of the arithmetic progressions $\bar{A}_1, \ldots, \bar{A}_k$, where k is minimal, $k \geqslant 2$. Let $b \in B$, $1 \leqslant i<j \leqslant k$; because $\bar{C}-b$ is in arithmetic progression and k is minimal, $\bar{C}-b$ cannot have elements in common with both $\bar{A}_i$ and $\bar{A}_j$. Consequently, putting

$$B_i=\{b: b \in B,\ \bar{A}_i \cap (\bar{C}-b) \neq \phi\},$$

the sets $B_1, \ldots, B_k$ are non-empty disjoint sets with union B. Moreover, $\bar{C}-B_i=\bar{A}_i$, hence, from the above lemma,

$$[\bar{C}]+[B_i]-1 \leqslant [\bar{A}_i], \quad (i=1,\ \ldots,\ k).$$

Adding these relations, we find

$$k\,([\bar{C}]-1)+[B] \leqslant [\bar{C}-B] \leqslant [\bar{C}]-1+[B],$$

from (2). But $[\bar{C}]-1 \geqslant 1$, hence, $k \leqslant 1$, a contradiction.

COROLLARY. *Suppose that* $[A] \geqslant 2$, $[B] \geqslant 2$, $[A+B] \leqslant [A]+[B]-1$. *Suppose further that each element* $g \neq 0$ *in* G *is of order* $\geqslant [A+B]+2$. *Then* A, B *and* $A+B$ *are in arithmetic progression with a common difference* d.

REMARK. For the special case that G is a cyclic group of prime order, this result is due to Vosper [8] and was rediscovered by Chowla and Straus [1]. In [9] Vosper gave a simplified proof which can easily be modified so as to yield the above corollary.

Proof. G has no subgroups F with $2 \leqslant [F] \leqslant [A+B]$, hence, $A+B$ cannot be quasi-periodic, thus, from Theorem 2.1 and Theorem 3.1, $A+B$ is in arithmetic progression. Now, apply Lemma 4.3.

The following is concerned with the case that $A+B$ is quasi-periodic.

DEFINITION. Let A, B be finite non-empty subsets of G. Then $P(A, B)$ shall denote the (possibly empty) collection of pairs (F, C'') such that:

(i) F is a finite subgroup of G of order $[F] \geqslant 2$;

(ii) C'' is a proper non-empty subset of $A+B$ and is contained in some F-coset; moreover, the complement C' of C'' in $A+B$ is the union of one or more F-cosets.

(iii) If $A+B$ is periodic then C'' itself in an F-coset, while $\nu_c(A, B) = 1$ holds for at least one element $c \in C''$.

Further, for $(F, C'') \in P(A, B)$, let $\varrho(F, C'') \geqslant 1$ denote the number of representations of $\sigma\, C''$ as a sum $\bar{a}+\bar{b}$ with $\bar{a} \in \sigma A$, $\bar{b} \in \sigma B$, (σ denoting the quotient mapping $G \to G/F$). Finally, let $P_1(A, B)$ denote the collection of all the pairs (F, C'') in $P(A, B)$ for which $\varrho(F, C'') = 1$.

Note that $P(A, B)$ is non-empty if and only if either $A+B$ is quasi-periodic but not periodic or if $A+B$ is periodic (but not the coset of a cyclic group of prime order), while $\nu_c(A, B) = 1$ holds for at least one element c. Hence, from the Theorems 3.1 and 3.2, if $P(A, B)$ is non-empty then $[A+B] \geqslant [A]+[B]-1$.

LEMMA 4.4. *Consider a pair* A, B *of non-empty finite subsets of* G *satisfying*

$$[A+B] = [A]+[B]-1 \tag{3}$$

and suppose that $P(A, B)$ *is non-empty. Let* (F, C'') *be a fixed pair in* $P(A, B)$, *put* $\varrho(F, C'') = \varrho$, *and let* $\sigma C'' = \bar{a}_i + \bar{b}_i$ $(i = 1, \dots, \varrho)$ *be the* ϱ *different representations of* $\sigma C''$ *with* $\bar{a}_i \in \sigma A$, $\bar{b}_i \in \sigma B$ (σ *denoting the quotient mapping* $G \to G/F$). *Finally, let* $A_i = A \cap (\sigma^{-1}\bar{a}_i)$, $B_i = B \cap (\sigma^{-1}\bar{b}_i)$, $i = 1, \dots, \varrho$. Assertions:

(i) *Clearly, each of* $A_1, \dots, A_\varrho$ *is contained in an* F*-coset, such that different* A_i *are contained in different* F*-cosets. Moreover, the complement* A' *of* $A_1 \cup \dots \cup A_\varrho$ *in* A *satisfies* $A' + F = A'$. *Analogous results hold for* $B_1, \dots, B_\varrho$.

(ii) *Clearly,* C'' *is the union of the non-empty sets* $A_i + B_i$ $(i = 1, \dots, \varrho)$. *Moreover, permuting the indices if necessary,*

$$[A_1] + [B_1] = [C''] + 1, \tag{4}$$

and

$$[A_i] + [B_i] = [F] \qquad (i = 2, \dots, \varrho), \tag{5}$$

(*thus,* $[A_i] < [F]$, $[B_i] < [F]$, $i = 2, \dots, \varrho$). *Further, if* $A + B$ *is periodic then, for some* $c_0 \in C''$, $\nu_{c_0}(A_1, B_1) = \nu_{c_0}(A, B) = 1$.

(iii) *Finally,*

$$[\sigma A + \sigma B] = [\sigma A] + [\sigma B] - \varrho. \tag{6}$$

Proof. Suppose that $A' + F \neq A'$, thus, $[A^*] > [A]$, where $A^* = A \cup (A' + F)$. But

$$(A' + F) + B \subset C' + F = C' \subset A + B,$$

thus, $A^* + B = A + B$ and $\nu_c(A^*, B) = \nu_c(A, B)$ for each $c \in C''$. From (3), $[A^* + B] < [A^*] + [B] - 1$, hence, from the Theorems 3.1 and 3.2, $A^* + B = A + B$ is periodic while $\nu_c(A^*, B) \geqslant 2$ for each $c \in A + B$. But if $A + B$ is periodic we have $\nu_c(A^*, B) = \nu_c(A, B) = 1$ for at least one $c \in C''$, a contradiction. This proves $A' + F = A'$.

We now assert that, after a proper permutation of the indices,

$$[A_1] + [B_1] \leqslant [C''] + 1, \tag{7}$$

and

$$[A_i] + [B_i] \leqslant [F] \qquad (i = 2, \dots, \varrho). \tag{8}$$

Suppose first that $C'' = (A_1 + B_1) \cup \dots \cup (A_\varrho + B_\varrho)$ contains an element c with $\nu_c(A, B) = 1$. Then c is contained in only one of the sets $A_i + B_i$ (say) in $A_1 + B_1$, such that $\nu_c(A_1, B_1) = 1$. Now, (7) follows from Theorem 3.2 and (8) from Lemma 4.1 and $c \notin A_i + B_i$ $(i = 2, \dots, \varrho)$.

On the contrary, if such an element c does not exist then $A + B$ and, hence, C'' is aperiodic. For the moment, suppose that

$$[A_i] + [B_i] \geqslant [C''] + 2 \qquad (i = 1, \dots, \varrho). \tag{9}$$

Then, from Theorem 3.1, $C_i = A_i + B_i$ would satisfy

$$[C_i] + [H(C_i)] \geqslant [C''] + 2 \qquad (i = 1, \dots, \varrho).$$

But C'' is the union of $C_1, \dots, C_\varrho$, hence, from the Corollary to Lemma 2.2, $[C''] + [H(C'')] \geqslant [C''] + 2$ and C'' would be periodic, a contradiction.

Therefore, (9) is false and (7) holds after a proper permutation of the indices. Finally, C'' being aperiodic, C'' and, thus, A_i+B_i is a proper subset of $C''+F$ ($[F]\geqslant 2$) and Lemma 4.1 implies (8). This completes the proof of (7) and (8).

From the definition of A_i, B_i, A' and B',

$$\sum_{i=1}^{\varrho}([A_i]+[B_i])=[A]-[A']+[B]-[B']. \tag{10}$$

Further, A' is the union of $[\sigma A]-\varrho$ cosets of F, B' is the union of $[\sigma B]-\varrho$ cosets of F, while $A+B=C$ (say) is the disjoint union of C' and C'', C' being the union of $[\sigma C]-1$ cosets of F. Hence, from (10) and (3),

$$\sum_{i=1}^{\varrho}([A_i]+[B_i])=(\varrho-1)[F]+[C'']+1+\lambda[F], \tag{11}$$

where
$$\lambda=\varrho+[\sigma C]-[\sigma A]-[\sigma B]. \tag{12}$$

It follows from (7), (8) and (11) that $\lambda\leqslant 0$. On the other hand, $\bar{c}=\sigma C''$ satisfies $\nu_{\bar{c}}(\sigma A,\sigma B)=\varrho$, hence, from Theorem 3.2, $\lambda\geqslant 0$. Consequently, $\lambda=0$, proving (6). Finally, (7), (8) and (11) imply (4) and (5). This completes the proof of Lemma 4.4.

LEMMA 4.5. *Suppose that* (3) *holds and that* $P(A, B)$ *is non-empty. Then either* $A+B$ *is a coset of a finite group, or* $A+B$ *is obtained from a coset of a finite group by deleting one element or* $P_1(A, B)$ *is non-empty.*

Proof. Consider a pair $(F, C'')\in P(A, B)$ with $[F]$ *maximal*. Observe that the complement D (say) of $A+B$ in $A+B+F$ is given by

$$D=\bar{C}''\cap(c+F) \qquad (c\in C''),$$

thus, D is contained in an F-coset. Further, D is empty if and only if $A+B$ is periodic.

If $\varrho(F, C'')=1$ we are ready, thus, suppose that $\varrho(F, C'')\geqslant 2$. It follows from (6) and Theorem 3.1 that the set $\sigma(A+B)$ is periodic, σ denoting the quotient mapping $G\rightarrow G/F$. In other words, there exists a finite subgroup H of G/F of order $[H]\geqslant 2$, such that $\sigma(A+B)$ is the union of (say) $m\geqslant 1$ cosets of H. Consequently, $A+B+F$ is the union of m cosets of the group $\sigma^{-1}H=K$ (say). Here, $[K]=[H][F]>[F]$, thus, K contains F as a proper subgroup. Finally, the complement D of $A+B$ in $A+B+F$ is properly contained in some K-coset. It follows from the maximal character of $[F]$ that $m=1$. Hence, $A+B$ is obtained from a certain coset $g+K$ of K by deleting a subset D of a certain F-coset contained in $g+K$.

If $[D]\leqslant 1$ we are ready, thus, assume $[D]\geqslant 2$, hence, $A+B$ is aperiodic. Now consider a *minimal* group F_1 having the following properties: (i) $F_1\subset F\subset K$; (ii) D is contained in some F_1-coset. Thus, $[F_1]\geqslant[D]\geqslant 2$. Let C_1'' denote the part of $A+B$ in the coset $D+F_1$, thus,

$$C_1''=(A+B)\cap(d+F_1)=\bar{D}\cap(d+F_1),$$

$(d\in D)$. Each F_1-coset different from $D+F_1$ and contained in $g+K$ is also contained in $A+B$. Finally, $A+B$ being aperiodic, C_1'' is non-empty, consequently,

$$(F_1,\ C_1'')\in P(A,\ B).$$

Let $\varrho(F,\ C_1'')=\varrho_1$. It suffices to prove that $\varrho_1=1$.

On the contrary, suppose that $\varrho_1\geqslant 2$. From Lemma 4.4, applied to the pair $(F_1,\ C_1'')$, there exist non-empty sets A_2, B_2 with $[A_2]+[B_2]=[F_1]$ and such that $A_2+B_2=C_2$ (say) is contained in C_1''. Now, consider the group $H(C_2)$, satisfying $C_2+H(C_2)=C_2$. We have $C_2\subset C_1''$ while C_1'' in turn is a proper subset of $d+F_1$ $(d\in D)$, consequently, $H(C_2)$ is a proper subgroup of F_1. On the other hand, from Theorem 3.1,

$$[C_2+H(C_2)]+[H(C_2)]\geqslant[A_2]+[B_2]=[F_1]=[d+F_1],$$

showing that $C_2=C_2+H(C_2)$ and, hence, C_1'' contains all but at most one of the $H(C_2)$-cosets contained in $d+F_1$, $d\in D$. Consequently, the complement D of C_1'' in $d+F_1$ $(d\in D)$ is contained in an $H(C_2)$-coset, a contradiction, in view of the minimal character of F_1. This proves Lemma 4.5.

Remark. Suppose that (3) holds and that $A+\mathrm{B}$ is periodic but not the coset of a finite group. If $\nu_c(A,\ B)=1$ has a solution c (that is if $P(A,\ B)$ is non-empty), then Lemma 3.3 easily implies $(H,\ c+H)\in P_1(A,\ B)$, where $H=H(A+\mathrm{B})$. This yields a second proof of Lemma 4.5 for the (easiest) case that $A+B$ is periodic.

Lemma 4.6. *Let A, B be finite non-empty subsets of G satisfying* (3) *and $\nu_{c_0}(A,\ B)=1$ for some $c_0\in A+B$. Let K denote a finite subgroup of G and suppose that either* (i) *$A+B=c_0+K$, while $\nu_{c_1}(A,\ B)=1$ for some $c_1\neq c_0$; or* (ii) *$A+B$ is obtained from c_0+K by deleting one element c_1.*

Then either both A and B are in arithmetic progression of difference $d=c_1-c_0$ or $P_1(A,B)$ is non-empty.

Proof. Suppose that (i) holds and let $c_1=a_1+b_1$ $(a_1\in A,\ b_1\in B)$. Then $a\in A$, $a\neq a_1$ imply $-a+c_1\in\bar{B}\cap(B+K)$. But $[A]-1=[K]-[B]=[\bar{B}\cap(B+K)]$, hence, (*) each element in $\bar{B}\cap(B+K)$ can be written as $-a'+c_1$ with $a'\in A$. Now, suppose that (ii) holds. From $c_1 \notin A+B$ we have $-A+c_1 \subset \bar{B} \cap (B+K)$. But $[A]=[K]-[B]=$ $=[\bar{B} \cap (B+K)]$, hence (*) holds also in this case.

Let $c_0=a_0+b_0$ ($a_0 \in A$, $b_0 \in B$). Then $a \in A$, $a \neq a_0$ imply $-a+c_0 \in \bar{B} \cap (B+K)$, hence, from (*), $(c_1-c_0)+a \in A$. Letting F denote the cyclic subgroup of K generated by $d=c_1-c_0 \neq 0$, $[F] \geqslant 2$, it follows that the subset A of a_0+K, (similarly, the subset B of b_0+K), is the union of a number of F-cosets and an arithmetic progression of difference d contained in a_0+F (or b_0+F, respectively).

It remains to consider the case that F is a proper subgroup of K, thus, $(F, C'') \in P(A, B)$, where $C''=(A+B) \cap (c_0+F)$. Suppose that $\varrho(F, C'') \geqslant 2$ and let σ denote the quotient mapping $G \rightarrow G/F$. Then, there exist elements $\bar{a} \in \sigma A$, $\bar{b} \in \sigma B$ such that $\sigma c_0=\bar{a}+\bar{b}$, $\bar{a} \neq \sigma a_0$, $\bar{b} \neq \sigma b_0$. But then the F-cosets $A'=\sigma^{-1}\bar{a}$, $B'=\sigma^{-1}\bar{b}$ are contained in A and B, respectively, while $c_0 \in A'+B'$, thus, $\nu_{c_0}(A, B) \geqslant \nu_{c_0}(A', B')=$ $=[F] \geqslant 2$, a contradiction. This proves Lemma 4.6.

5. The main structure theorem

Definition. The pair (A_1, B_1) of non-empty finite subsets of the group G is said to be an *elementary pair* if at least one of the following conditions (I)–(IV) holds true.

(I) Either $[A_1]=1$ or $[B_1]=1$.

(II) A_1 and B_1 are in arithmetic progression with a common difference d, where d is of order $\geqslant [A_1]+[B_1]-1$; (hence, A_1+B_1 is an arithmetic progression of difference d while $\nu_c(A_1, B_1)=1$ holds for at least one $c \in A_1+B_1$).

(III) For some finite group H, each of A_1, B_1 is contained in an H-coset while $[A_1]+[B_1]=[H]+1$; (hence, A_1+B_1 is an H-coset). Moreover, *precisely one* element c satisfies $\nu_c(A_1, B_1)=1$.

(IV) A_1 is aperiodic. Further, for some finite subgroup H of G, A_1 is contained in an H-coset while B_1 is of the form $B_1=g_0-\bar{A}_1 \cap (a+H)$ ($a \in A_1$); (hence, from Lemma 4.2, A_1+B_1 is obtained from g_0+H by deleting the element g_0). Moreover, *no* element c satisfies $\nu_c(A_1, B_1)=1$.

Observe that each of the conditions (I)–(IV) implies

$$[A_1+B_1]=[A_1]+[B_1]-1.$$

Theorem 5.1. *Let G be an abelian group, $[G] \geqslant 2$, and let A, B denote finite non-empty subsets of G. Then a necessary and sufficient condition, in order that*

$$[A+B]=[A]+[B]-1 \tag{1}$$

and, moreover,

(2) *if $A+B$ is periodic then $\nu_c(A, B)=1$ for at least one c,*

is the existence of a non-empty subset A_1 of A, a non-empty subset B_1 of B and a subgroup F of G order $[F]\geqslant 2$, such that:

(i) *The pair (A_1, B_1) is elementary, each of A_1, B_1 is contained in an F-coset.*

(ii) *The element $\bar{c}=\sigma(A_1+B_1)$ has $\bar{c}=\sigma A_1+\sigma B_1$ as its only representation of the form $\bar{c}=\bar{a}+\bar{b}$, $\bar{a}\in\sigma A$, $\bar{b}\in\sigma B$. Here, σ denotes the quotient mapping $G\to G/F$.*

(iii) *The complement A' of A_1 in A satisfies $A'+F=A'$, similarly, the complement B' of B_1 in B satisfies $B'+F=B'$ (hence, from* (ii)*, the complement C' of A_1+B_1 in $A+B$ satisfies $C'+F=C'$).*

(iv) *Finally,* $$[\sigma A+\sigma B]=[\sigma A]+[\sigma B]-1.$$

This theorem will be obtained by combining Lemma 4.4 and:

LEMMA 5.2. *Lct A, B be finite non-empty subsets of G satisfying* (1) *and* (2). *Then either the pair (A, B) is elementary or $P_1(A, B)$ is non-empty.*

Proof. We may assume $[A]\geqslant 2$, $[B]\geqslant 2$ (thus, $[A+B]\geqslant 2$), otherwise, (A, B) is elementary of type (I). Let us first consider a number of special cases.

(i) Suppose that $A+B$ is a coset of some finite group H. Then $A+B$ is periodic, thus, from (2), there exists an element c_0 with $\nu_{c_0}(A, B)=1$. If no other such element exists (A, B) is elementary of type (III). Otherwise, from Lemma 4.6, either (A, B) is elementary of type (II) or $P_1(A, B)$ is non-empty.

(ii) Next, consider the case that $A+B$ is obtained from a coset of a finite group H by deleting one element g_0. If no element c_0 exists with $\nu_{c_0}(A, B)=1$ then, from Lemma 4.2, (A, B) is elementary of type (IV). Otherwise, from Lemma 4.6, either (A, B) is elementary of type (II) or $P_1(A, B)$ is non-empty.

Let us now treat the general case. From $[A]\geqslant 2$, $[B]\geqslant 2$, (1) and Theorem 2.1, either $A+B$ is in arithmetic progression or $A+B$ is quasi-periodic. Suppose that none of the above cases (i), (ii) occurs. If $A+B$ is in arithmetic progression then, from Lemma 4.3, (A, B) is elementary of type (II). If $A+B$ is quasi-periodic then $P(A, B)$ is non-empty, hence, from Lemma 4.5, $P_1(A, B)$ is non-empty. This proves Lemma 5.2.

Proof of Theorem 5.1. The stated conditions are sufficient. For, from (iii), we have
$$[A+B]=[A_1+B_1]+(\sigma[A+B]-1)[F],$$
similar formulae holding for A and B. But, (A_1, B_1) being an elementary pair,

$[A_1+B_1]=[A_1]+[B_1]-1$, hence, (iv) implies (1). Moreover, (2) holds. For, suppose that $A+B$ is periodic, thus, (A_1, B_1) cannot be elementary of type (IV), hence, in view of (ii), $\nu_c(A, B)=\nu_c(A_1, B_1)=1$ for at least one element $c \in A_1+B_1$.

Thus, suppose that the non-empty finite sets A, B satisfy (1) and (2). If (A, B) itself is an elementary pair then the assertions of Theorem 5.1 trivially hold with $A_1=A$, $B_1=B$, $F=G$. Hence, in view of Lemma 5.2, we may assume that $P_1(A, B)$ is non-empty. Now, consider a pair $(F, C'') \in P_1(A, B)$ with $[F]$ *minimal* and let σ denote the quotient mapping $G \to G/F$. From $\varrho(F, C'')=1$, $\sigma C''$ has a unique representation as $\sigma C''=\bar{a}+\bar{b}$ with $\bar{a} \in \sigma A$, $\bar{b} \in \sigma B$. Consider the non-empty sets $A_1=A \cap (\sigma^{-1}\bar{a})$ and $B_1=B \cap (\sigma^{-1}\bar{b})$, thus, $A_1+B_1=C''$ and each of A_1, B_1 is contained in an F-coset. We assert that F, A_1, B_1 satisfy the assertions of Theorem 5.1.

Here, (ii) is obvious while (iii) and (iv) follow from Lemma 4.4. It remains to prove that the pair (A_1, B_1) is elementary. For this, it suffices to verify that

$$P_1(A_1, B_1) \subset P_1(A, B). \tag{3}$$

For, each $(F_1, C_1'') \in P_1(A_1, B_1)$ satisfies $[F_1]<[A_1+B_1] \leqslant [F]$, thus, $[F]$ being minimal, (3) implies that $P_1(A_1, B_1)$ is *empty*. Moreover, from Lemma 4.4,

$$[A_1+B_1]=[A_1]+[B_1]-1.$$

Finally, if $A_1+B_1=C''$ is periodic then $A+B$ is periodic and C'' contains an element c with $\nu_c(A, B)=\nu_c(A_1, B_1)=1$. It now follows from Lemma 5.2 that (A_1, B_1) is an elementary pair.

Consider a fixed pair $(F_1, C_1'') \in P_1(A_1, B_1)$. We must show that $(F_1, C_1'') \in P_1(A, B)$. In the first place, C_1'' is a proper non-empty subset of A_1+B_1 and, hence, of $A+B$. Further, the complement of C_1'' in A_1+B_1 is the union of one or more F_1-cosets. But A_1+B_1 is contained in an F-coset, thus, F_1 is a subgroup of F. Moreover, the complement of A_1+B_1 in $A+B$ is a union of F-cosets, consequently, the complement of C_1'' in $A+B$ is a union of F_1-cosets. Further, if $A+B$ is periodic then A_1+B_1 is periodic, hence, C_1'' contains an element c with

$$\nu_c(A_1, B_1)=\nu_c(A, B)=1.$$

Finally, we must show that

$$C_1''+F_1=(a+F_1)+(b+F_1), \tag{4}$$

$a \in A$, $b \in B$, uniquely determine the cosets $a+F_1$ and $b+F_1$. From $C_1'' \subset A_1+B_1=C''$, (4) implies $C''+F=(a+F)+(b+F)$, hence, from (ii), $a \in A_1$ and $b \in B_1$. But, from

$(F_1, C_1'') \in P_1(A_1, B_1)$, the relation (4) with $a \in A_1$ and $b \in B_1$ does indeed uniquely determine the cosets $a+F_1$ and $b+F_1$. This completes the proof of Theorem 5.1.

For G as an abelian group, let $\prod_G(N)$ denote the class of pairs (A, B) of non-empty finite subsets of G satisfying

$$[A+B] \leqslant [A]+[B]-1, \qquad [A+B] \leqslant N.$$

For each $N>0$, this class $\Pi_G(N)$ can be constructed by applying Theorem 3.4 at most once and Theorem 5.1 at most $\log_2 N$ times. More precisely:

(i) Theorem 3.4 shows how to obtain all the pairs (A, B) in $\Pi_G(N)$ for which $A+B$ is periodic, provided that, for each finite subgroup F of G of order $[F] \geqslant 2$, one already knows the class of all the pairs (A, B) in $\Pi_{G/F}(N/[F])$ for which $A+B$ is aperiodic.

(ii) Theorem 5.1 shows how to obtain the pairs (A, B) in $\Pi_G(N)$ for which $A+B$ is either aperiodic or contains an element c with $\nu_c(A, B)=1$, provided that, for each finite subgroup F of G of order $[F] \geqslant 2$, one already knows the class of pairs (A, B) in $\Pi_{G/F}(\{N/[F]\})$ for which $A+B$ contains an element c with $\nu_c(A, B)=1$; (here, $\{\alpha\}$ denotes the smallest integer $\geqslant \alpha$).

In fact, the following more explicit construction yields all the pairs (A, B) of non-empty finite subsets of G for which (1) and (2) hold. This is an easy consequence of Theorem 5.1; observe that the pair (A_1, B_1) in the formulation of Theorem 5.1 is elementary of type (IV) if (and only if) $\nu_c(A, B) \neq 1$ for each $c \in G$.

Construction: choose $r \geqslant 1$ groups $G_1, \ldots, G_r$ such that $G_1 = G$ and $G_{j+1} = G_j/F_j$ where F_j denotes a finite non-trivial $(2 \leqslant [F_j] < [G_j])$ subgroup of G_j, $(j=1, \ldots, r-1)$. In the following manner, one now constructs, for $i=r, r-1, \ldots, 1$, a pair of non-empty finite subsets P_i, Q_i of G_i. If $r=1$ one chooses $P_1 = P_1''$, $Q_1 = Q_1''$ as an arbitrary elementary pair of subsets of $G_1 = G$, thus, assume $r \geqslant 2$. Then one first chooses the subsets P_r, Q_r of G_r such that (P_r, Q_r) is elementary of type (I), (II) or (III), $[P_r+Q_r] \geqslant 2$.

Let $1 \leqslant j \leqslant r-1$ and suppose that, for $i=j+1, \ldots, r$, the subsets P_i, Q_i of G_i have already been chosen in such a manner that $\nu_c(P_i, Q_i)=1$ holds for at least one $c \in P_i+Q_i$. Now, select any element c from $P_{j+1}+Q_{j+1}$ having only one representation as $c=p+q$ with $p \in P_{j+1}$, $q \in Q_{j+1}$. Further, (σ denoting the quotient mapping $G_j \to G_j/F_j = G_{j+1}$), choose a subset P_j'' of $\sigma^{-1}p$ and a subset Q_j'' of $\sigma^{-1}q$ in such a manner that the pair (P_j'', Q_j'') is elementary if $j=1$, elementary of type (I), (II) or (III) if $j>1$. Now, let $P_j = P_j'' \cup \sigma^{-1}P_{j+1}^*$ and $Q_j = Q_j'' \cup \sigma^{-1}Q_{j+1}^*$ where P_{j+1}^*, Q_{j+1}^*

denote the sets obtained from P_{j+1}, Q_{j+1} by deleting p or q, respectively. This completes the construction. Finally, let $A = P_1$, $B = Q_1$.

Here, $\nu_c(A, B) = 1$ holds for at least one element $c \in A + B$ if and only if (P_1'', Q_1''), is not elementary of type (IV). Further, $A + B$ is aperiodic if and only if $P_1'' + Q_1''$ is aperiodic.

The above results leave one seemingly important question unanswered, namely: what is the precise structure of the elementary pairs of type (III) and (IV)? But note that *Theorem* 5.1 *remains valid* of one modifies the definition of "elementary pair" by replacing in (III) "precisely one" by "at least one" and omitting in (IV) the condition that no element c satisfies $\nu_c(A, B) = 1$; (one needs only to verify that the conditions (i)–(iv) of Theorem 5.1 are still sufficient for (1) and (2)). Further, adopting this modified definition. the above construction again yields the full class of pairs (A, B) satisfying (1) and (2). From this point of view, there remains only the problem to determine the structure of the pairs (A, B) of subsets of a finite group H such that $[A] + [B] = [H] + 1$ while $\nu_c(A, B) = 1$ holds for at least one element $c \in H$. But it is easily seen that the following construction yields precisely all such pairs: choose B as an arbitrary non-empty subset of H and let $A = (c - \bar{B}) \cup \{a\}$ with $c \in H$, $a \in H$ arbitrary.

6. Elements having few or many representations

Let A, B be non-empty finite subsets of an abelian group G such that

$$\varrho = [A] + [B] - [A + B] \geqslant 1.$$

Let n_r denote the number of elements $g \in G$ having precisely r representations of the form $g = a + b$ $(a \in A,\ b \in B)$. From Theorem 3.2, we have $n_r = 0$ if $0 < r < \varrho$. In this section, we shall prove the curious fact that also $n_r = 0$ if $\varrho < r < n_\varrho$ (which is non-trivial only if $n_\varrho > \varrho + 1$).

As an illustration, let G be of finite even order, let F be a subgroup of G of index 2 and let $F_1 = x + F$ $(x \in G,\ x \notin F)$. Take A as the union of F and the elements $a_1, \ldots, a_\sigma$ in F_1 and take B as the union of F and the elements $b_{\sigma+1}, \ldots, b_\varrho$ in F_1 $(0 \leqslant \sigma \leqslant \varrho < [F])$. Then $A + B = F \cup F_1$, further, $\nu_g(A, B) = \varrho$ iff $g \in F_1$, thus, $n_\varrho = [F]$, finally, $\nu_g(A, B) \geqslant [F] = n_\varrho$ for each element g in the complement F of F_1 in $A + B$. Note that each element c with $\nu_c(A, B) = \varrho$ is such that, in each of its representations $c = a + b$ $(a \in A,\ b \in B)$, either $a \in \{a_1, \ldots, a_\sigma\}$ or $b \in \{b_{\sigma+1}, \ldots, b_\varrho\}$. This phenomenon always occurs when $n_\varrho > 2\varrho$, cf. Theorem 6.2.

We shall first consider the case $\varrho = 1$.

THEOREM 6.1. *Let A, B be a pair of finite non-empty subsets of an abelian group G, such that*

$$[A+B]=[A]+[B]-1. \tag{1}$$

Let $c_1, \ldots, c_n$ $(n \geqslant 0)$ denote all the different elements in $A+B$ having only one representation as $c_j = a_j + b_j$ $(a_j \in A,\ b_j \in B)$. Assertion:

(α) *If $n=0$ the set $A+B$ is either periodic or can be made periodic by adding one element.*

(β) *If $n=1$ the set $A+B$ is either periodic or can be made periodic by deleting one element.*

(γ) *If $n \geqslant 3$ then either $a_1 = \cdots = a_n$ or $b_1 = \cdots = b_n$. Moreover, $\nu_c(A, B) \geqslant n$ for each $c \in A+B$ with $c \neq c_j$ $(j=1, \ldots, n)$.*

Proof. One may assume that either $A+B$ is aperiodic or $n \geqslant 1$, thus, (5.2) holds. From Theorem 5.1, there exist non-empty sets $A_1 \subset A$, $B_1 \subset B$ and a subgroup F of G, $[F] \geqslant 2$, satisfying the assertions (i)–(iv) of Theorem 5.1. From (ii),

$$\nu_c(A, B) = \nu_c(A_1, B_1) \quad \textit{if } c \in A_1 + B_1, \tag{2}$$

hence, $n \geqslant m$, where m denotes the number of elements $c \in A_1 + B_1$ with $\nu_c(A_1, B_1) = 1$. Moreover, (for $1 \leqslant p \leqslant n$),

$$c_p = a_p + b_p \notin A_1 + B_1 \quad \textit{implies that } A_1 = \{a_p\} \textit{ or } B_1 = \{b_p\}; \tag{3}$$

(such an element c_p exists iff $n > m$). For, if $c_p \notin A_1 + B_1$ then either $a_p \notin A_1$ or $b_p \notin B_1$, (say) $a_p \notin A_1$. From (iii), $a_p + F \subset A$, hence, $1 = \nu_{c_p}(A, B) \geqslant [(b_p + F) \cap B]$, thus,

$$(b_p + F) \cap B = \{b_p\},$$

hence, from (iii), $B_1 = \{b_p\}$. This proves (3).

Suppose first that $n=0$; then $m=0$ and (A_1, B_1) must be elementary of type (IV). This proves (α) in view of (iii). Next, suppose that $A+B$ is aperiodic and $n=1$. If $m=0$ then, from (3), $[A_1]=1$ or $[B_1]=1$, hence, $m \geqslant 1$, a contradiction. Thus, $m=1$, while $A_1 + B_1$ is aperiodic, consequently, (A_1, B_1) is elementary either of type (I) or of type (II), in fact, $[A_1] = [B_1] = 1$, that is, $A_1 + B_1$ consists of a single element. This proves (β) in view of (iii).

Finally, suppose that $n \geqslant 3$. We assert that (*) there exist two elements $c_p \neq c_q$ $(1 \leqslant p, q \leqslant n)$, such that either $a_p = a_q$ or $b_p = b_q$. First, if $m < n$ there exists an element $c_p = a_p + b_p \notin A_1 + B_1$, hence, from (3), $B_1 = \{b_p\}$ (say), thus, from (2), not only c_p but also each element c_q in $A_1 + B_1$ is among the elements $c_j = a_j + b_j$ with $b_j = b_p$.

On the other hand, if $m = n \geqslant 3$ then (A_1, B_1) is necessarily elementary of type (I), (say) B_1 consists of a single element b, hence, from (2), each of the $m \geqslant 3$ elements in $A_1 + B_1$ is an element $c_j = a_j + b_j$ with $b_j = b$. This proves (*).

For definiteness, suppose that $c_p \neq c_q$ are such that $b_p = b_q$, thus, $[C''] \geqslant 2$, where C'' denotes the set of those elements c_j $(j = 1, \ldots, n)$ for which $b_j = b_p$. If B' denotes the set obtained from B by deleting b_p, the set $A + B'$ is precisely the complement of C'' in $A + B$. Thus, from (1) and Theorem 3.2,

$$2 \leqslant [C''] = [A] + [B'] - [A + B'] \leqslant \nu_c(A, B') \leqslant \nu_c(A, B),$$

for each element $c \in A + B'$. It follows that, for $j = 1, \ldots, n$, $c_j \notin A + B'$, thus, $c_j \in C''$, that is, $b_j = b_p$. Finally, $\nu_c(A, B) \geqslant [C''] = n$ for each element c in the complement $A + B'$ of $C'' = \{c_1, \ldots, c_n\}$ in $A + B$. This proves Theorem 6.1.

THEOREM 6.2. *Let A, B be a pair of finite non-empty subsets of an abelian group G, such that*

$$[A + B] = [A] + [B] - \varrho \quad \textit{with } \varrho \geqslant 1. \tag{4}$$

Let $c_1, \ldots, c_n$ $(n \geqslant 0)$ denote the different elements in $A + B$ satisfying $\nu_g(A, B) = \varrho$. Assertion:

(i) *We have $\nu_c(A, B) \geqslant n$ for each element $c \in A + B$ with $c \neq c_j$ $(j = 1, \ldots, n)$.*

(ii) *If $n > 2\varrho$ there exist different elements $a_1, \ldots, a_\sigma$ in A and different elements $b_{\sigma+1}, \ldots, b_\varrho$ in B $(0 \leqslant \sigma \leqslant \varrho)$, such that, for each $j = 1, \ldots, n$, the ϱ representations $c_j = a + b$ of c_j are of the form*

$$c_j = a_\nu + b_\nu^{(j)} \; (\nu = 1, \ldots, \sigma), \; c_j = a_\mu^{(j)} + b_\mu \; (\mu = \sigma + 1, \ldots, \varrho),$$

where $\quad a_\mu^{(j)} \in A, \; b_\nu^{(j)} \in B, \; a_\mu^{(j)} \neq a_\nu, \; b_\nu^{(j)} \neq b_\mu \; (1 \leqslant \nu \leqslant \sigma, \; \sigma + 1 \leqslant \mu \leqslant \varrho).$

We shall first prove a special case.

LEMMA 6.3. *Let H denote a finite subgroup of the abelian group G, A and B subsets of some H-coset, such that*

$$[A] + [B] = [H] + \varrho \quad \textit{with } \varrho \geqslant 1, \tag{5}$$

thus, $A + B$ is an H-coset. Finally, let $c_1, \ldots, c_n$ denote all the different elements satisfying $\nu_g(A, B) = \varrho$. Then the assertions (i) *and* (ii) *of Theorem* 6.2 *hold. Hence, from* (i), *$[A] \geqslant n$, $[B] \geqslant n$ if $n < [H]$. Moreover, $[A] = [H]$ or $[B] = [H]$ if $n = [H]$.*

Proof. Without loss of generality, we may assume that both A and B are contained in H, thus, $A+B=H$. Let $\bar{A}$, $\bar{B}$ denote the complements of A, B in H. Then, for each $g \in H$,

$$\nu_g(A, B)+\nu_g(A, \bar{B})=\nu_g(A, H)=[A],$$

$$\nu_g(\bar{A}, \bar{B})+\nu_g(A, \bar{B})=[\bar{B}]=[H]-[B],$$

hence, from (5),

$$\nu_g(A, B)=\varrho+\nu_g(\bar{A}, \bar{B})\geqslant\varrho. \tag{6}$$

Consequently, $\nu_g(A, B)=\varrho$ iff $\nu_g(\bar{A}, \bar{B})=0$ iff $g\notin\bar{A}+\bar{B}$, thus, $\bar{A}+\bar{B}$ is precisely the complement of $\{c_1, \ldots, c_n\}$ in H, hence,

$$[\bar{A}+\bar{B}]=[H]-n. \tag{7}$$

If $n=[H]$ then either $\bar{A}$ is empty, thus, $A=H$, or $\bar{B}$ is empty, thus, $B=H$. Lemma 6.3 being obvious in these cases, we may assume that $\bar{A}$ and $\bar{B}$ are non-empty. From (5),

$$[\bar{A}]+[\bar{B}]=[H]-\varrho, \tag{8}$$

hence, from (7),

$$[\bar{A}+\bar{B}]=[\bar{A}]+[\bar{B}]-(n-\varrho). \tag{9}$$

From (6), (9) and Theorem 3.2,

$$\nu_g(A, B)=\varrho+\nu_g(\bar{A}, \bar{B})\geqslant\varrho+(n-\varrho)=n$$

for each element g in the complement $\bar{A}+\bar{B}$ of $\{c_1, \ldots, c_n\}$ in $A+B=H$, proving assertion (i).

Now, assume $n>2\varrho$. From (9) and Theorem 3.1, there exists a subgroup F of H of order $[F]\geqslant n-\varrho>\varrho$, such that

$$[\bar{A}+\bar{B}]+[F]=[\bar{A}+F]+[\bar{B}+F],$$

hence, from (7) and (8),

$$[H]+[F]>[\bar{A}+F]+[\bar{B}+F]\geqslant[H]-\varrho>[H]-[F],$$

consequently,

$$[\bar{A}+F]+[\bar{B}+F]=[H]. \tag{10}$$

Further, let $a_1, \ldots, a_\sigma$ denote the different elements of $A\cap(\bar{A}+F)$ and let $b_{\sigma+1}, \ldots, b_\tau$ denote the different elements of $B\cap(\bar{B}+F)$, hence,

$$[\bar{A}+F]=[\bar{A}]+\sigma,\ [\bar{B}+F]=[\bar{B}]+(\tau-\sigma),$$

thus, from (8) and (10), $\tau=\varrho$.

Let $c=c_j$ be such that $\nu_c(A, B)=\varrho$; let $c=a+b$ with $a \in A$, $b \in B$. If $a+F \subset A$, $b+F \subset B$ then $\nu_c(A, B) \geqslant [F] > \varrho$, a contradiction. Hence, either $a \in \bar{A}+F$ or $b \in \bar{B}+F$, that is, either a coincides with one of the elements $a_1, \ldots, a_\sigma$ or b coincides with one of the elements $b_{\sigma+1}, \ldots, b_\varrho$, but not both, otherwise, $\nu_c(A, B) < \varrho$. This proves assertion (ii).

Proof of Theorem 6.2. Without loss of generality, we may assume $n \geqslant 1$. Let $H(A+B)=H$, thus, $A+B$ is a union of H-cosets, and let τ denote the quotient mapping $G \rightarrow G/H$. Applying Theorem 3.1, we have

$$[\tau A+\tau B]=[\tau A]+[\tau B]-1 \tag{11}$$

and

$$[(A+H) \cap \bar{A}]+[(B+H) \cap \bar{B}]=[H]-\varrho. \tag{12}$$

Let us first consider the case $[H]=\varrho$. From (12), both A and B are unions of H-cosets, hence, for each $g \in G$, we have $\nu_g(A, B)=\varrho \cdot \nu_{\tau g}(\tau A, \tau B)$. Thus,

$$n=n_1[H]=n_1\varrho,$$

where n_1 denotes the number of elements $c \in \tau A+\tau B$ satisfying $\nu_c(\tau A, \tau B)=1$. In view of (11), applying assertion (γ) of Theorem 6.1 to the pair of subsets τA, τB of G/H, the assertions (i) and (ii) easily follow.

It remains to consider the case $[H] \neq \varrho$, thus, $[H] > \varrho$, from (12). Let j be fixed $(1 \leqslant j \leqslant n)$, thus, $\nu_{c_j}(A, B)=\varrho$. From Lemma 3.3, the element τc_j has only one representation as $\tau c_j=\bar{a}_j+\bar{b}_j$ with $\bar{a}_j \in \tau A$, $\bar{b}_j \in \tau B$. In other words, introducing the non-empty sets

$$A_j=A \cap \tau^{-1}\bar{a}_j, \qquad B_j=B \cap \tau^{-1}\bar{b}_j,$$

(each contained in an H-coset), we have

$$c \in c_j+H,\ c=a+b\ (a \in A,\ b \in B)\ \textit{implies}\ a \in A_j,\ b \in B_j. \tag{13}$$

Moreover, from (12), cf. the proof of Lemma 3.3,

$$[A_j]+[B_j]=[H]+\varrho, \tag{14}$$

$A_j+B_j=c_j+H$, while the complement A_j' of A_j in A is a union of H-cosets, similarly, the complement B_j' of B_j in B.

Suppose first that $[B_j]=[H]>\varrho$, thus, from (14), A_j consists of ϱ elements $a_1, \ldots, a_\varrho$ (say). Let C'' denote the complement of $A_j'+B$ in $A+B$, thus, C'' is precisely the set of those elements c_k $(k=1, \ldots, n)$ which have all their ϱ representations of the form $c_k = a_i + b_i^{(k)}$, $(b_i^{(k)} \in B,\ i = 1, \dots, \varrho)$. From (13), $[C''] \geqslant [H] > \varrho$, while, from (4),

$$[A_j' + B] = [A + B] - [C''] = [A_j'] + [B] - [C''].$$

Hence, from Theorem 3.2,

$$\nu_c(A, B) \geqslant \nu_c(A_j', B) \geqslant [C''] > \varrho \qquad \textit{if } c \in A_j' + B.$$

It follows that none of $c_1, \dots, c_n$ is in $A_j' + B$, thus, $C'' = \{c_1, \dots, c_n\}$, proving assertion (ii). Moreover, $\nu_c(A, B) \geqslant [C''] = n$ for each element in the complement $A_j' + B$ of C'' in $A + B$, proving assertion (i).

A similar reasoning applies when $[A_j] = [H]$. Thus, it remains to consider the case that $[A_j] < [H]$, $[B_j] < [H]$ $(j = 1, \dots, n)$. But the complement of each $A_j = A \cap \tau^{-1} \bar{a}_j$ in A is a union of H-cosets, hence, A_j does not depend on j, similarly, B_j does not depend on j. It follows that $c_k \in c_k + H = A_k + B_k = A_j + B_j$ $(k = 1, \dots, n)$, hence, from (13), $c_1, \dots, c_n$ are precisely all the elements satisfying $\nu_g(A_j, B_j) = \varrho$. In view of (14), applying Lemma 6.3 to the pair A_j, B_j, one immediately obtains assertion (ii) and further, $\nu_c(A, B) = \nu_c(A_j, B_j) \geqslant n$ for each $c \in A_j + B_j$ with $c \neq c_j$ $(j = 1, \dots, n)$. Moreover, $[A_j] < [H]$, $[B_j] < [H]$ and Lemma 6.3 imply $[A_j] \geqslant n$, $[B_j] \geqslant n$. Hence, if

$$c = a + b \notin A_j + B_j \qquad (a \in A,\ b \in B),$$

then either $a + H \subset A$, $[(b + H) \cap B] \geqslant n$ or vice versa, thus, $\nu_c(A, B) \geqslant n$, proving assertion (i). This completes the proof of Theorem 6.2.

Consider a pair of non-empty finite subsets A, B of an abelian group G. Note that $\nu_g(A, B) \leqslant [B]$ for each $g \in G$. Let m_i $(i = 0, 1, \dots)$ denote the number of elements $g \in G$ satisfying $\nu_g(A, B) = [B] - i$.

THEOREM 6.4. *Suppose that* $\lambda > 0$, *where*

$$\lambda = m_0 - [A] + [B]. \tag{15}$$

Then $m_i = 0$ *if either* $0 < i < \lambda$ *or* $\lambda < i < m_\lambda$.

Proof. We shall first assume that the group G is finite. Let $\bar{A}$ denote the (finite) complement of A in G. One may assume that $\bar{A}$ is non-empty, otherwise, $A = G$ and $m_i = 0$ for each $i > 0$. Obviously, $\nu_g(A, B) + \nu_g(\bar{A}, B) = [B]$, hence, m_i is also equal to the number of elements g with $\nu_g(\bar{A}, B) = i$. Especially, m_0 equals the number of elements not in $\bar{A} + B$, thus, from (15),

$$[\bar{A} + B] = [\bar{A}] + [B] - \lambda.$$

It follows from Theorem 3.2 that $m_i = 0$ if $0 < i < \lambda$. Moreover, if $\lambda > 0$ then, from assertion (i) of Theorem 6.2, $\nu_c(\bar{A}, B) > \lambda$ implies $\nu_c(\bar{A}, B) \geqslant m_\lambda$, hence, $m_i = 0$ if $\lambda < i < m_\lambda$.

The case $[G] = \infty$ can be reduced to the previous case by applying the following lemma with D as any finite subset of G containing A, B and $A + B$.

LEMMA 6.5. *Let G be an abelian group, D a finite subset of G. Then there exists a finite group G_1 and a homomorphic mapping T of the group G_0 generated by D unto G_1, such that T maps D unto $T(D)$ in a $1 : 1$ fashion.*

Proof. Let D' denote the set of all non-zero differences $d_1 - d_2$ of elements d_1, d_2 in D. By Zorn's lemma, there exists a maximal subgroup H of G_0 disjoint from D'. Let $G_1 = G_0/H$ and let T denote the quotient mapping of G_0 unto G_1. For d_1, d_2 in D, $d_1 \neq d_2$, we have $d_1 \notin d_2 + H$, thus, $T(d_1) \neq T(d_2)$, showing that T is $1 : 1$ on D.

Further, G_1 is generated by the finite set $T(D)$, hence, G_1 is of finite order if each element in G_1 is of finite order. Suppose that $g \in G_1$ is of infinite order. Because $T(D')$ is finite, we have $\pm ng \notin T(D')$ for $n \geqslant n_0$, n_0 sufficiently large. But then $H' = T^{-1}\{jn_0 g;\ j = 0, \pm 1, \ldots\}$ would be a subgroup of G disjoint from D' and containing H as a proper subgroup. This is impossible, H being maximal.

References

[1]. S. CHOWLA & E. G. STRAUS, On the lower bound in the Cauchy-Davenport theorem. Abstract, *Bull. Amer. Math. Soc.*, 63 (1957), 280.

[2]. P. DUBREIL, & C. PISOT, *Algèbre et théorie des nombres. Séminaire* 1955–56, Paris (1956).

[3]. J. H. B. KEMPERMAN, On complexes in a semigroup, *Indag. Math.*, 18 (1956), 247–254.

[4]. M. KNESER, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.*, 58 (1953), 459–484.

[5]. ——, Ein Satz über abelschen Gruppen mit Anwendungen auf die Geometrie der Zahlen, *Math. Z.*, 61 (1955), 429–434.

[6]. ——, Summenmengen in lokalkompakten abelschen Gruppen. *Math. Z.*, 66 (1956), 88–110.

[7]. P. SCHERK, Distinct elements in a set of sums. *Amer. Math. Monthly*, 62 (1955), 46.

[8]. G. VOSPER, The critical pairs of subsets of a group of prime order, *J. London Math. Soc.*, 31 (1956), 200–205.

[9]. ——, Addendum to "The critical pairs of subsets of a group of prime order", *Ibid.*, 280–282.

Received April 28, 1959.