SUMS OF LENGTH t IN ABELIAN GROUPS

BY

GEORGE T. DIDERRICH

ABSTRACT

Let G be an Abelian group written additively, B a finite subset of G, and let t be a positive integer. For $t \leqq |B|$, let B_t denote the set of sums of t *distinct* elements over B. Furthermore, let K be a subgroup of G and let σ denote the canonical homomorphism $\sigma : G \to G/K$. Write $B_t \pmod{B_t}$ for $B_t\sigma$ and write $B_t \pmod{K}$ for $B\sigma$. The following addition theorem in groups is proved. Let G be an Abelian group with no 2-torsion and let B a be finite subset of G. If t is a positive integer such that $t < |B|$ then $|B_t \pmod{K}| \geqq |B \pmod{K}|$ for any finite subgroup K of G.

0. Introduction

Let G be an Abelian group written additively, B a finite nonempty subset of G, and t a positive integer. For $1 \leqq t \leqq |B|$ we denote by B_t the set of sums of t *distinct* elements over B. Thus if $B = \{b_1, \cdots, b_k\}$, then $B_t = \{b_{i_1} + \cdots + b_{i_t} | 1 \leqq i_1 < \cdots < i_t \leqq k\}$. Also, for clarity we will sometimes write $(B)_t$ instead of B_t to avoid confusion with sets having a subscript.

We are concerned with the following problem. What is the relation between $|B|$ and $|B_t|$? More generally, let K be a subgroup of G and let σ denote the canonical homomorphism $\sigma: G \to G/K$. What is the relation between $|B\sigma|$ and $|B_t\sigma|$? To exhibit the role of K we shall write $B_t \pmod{K}$ for $B_t\sigma$ and $B \pmod{K}$ for $B\sigma$ in G/K. H. B. Mann and J. E. Olson (cf. Lemma 4 in [5]) proved in $G = Z_p$ that $|B_t| \geqq |B|$ if $t < |B|$. The author (cf. [1], Th. 2.7 and also [3]) proved that if $|B| > 2$, then $|B_2| \geqq |B|$ iff $B \neq x + N$ where $x \in G$ and N is an elementary Abelian 2-group. The study of sums of length t was motivated by the problem of estimating the size of sums of sets in arithmetic progression.

Received August 15, 1972

The reader should consult [2], [3], and [5] to see how knowledge of $|B_t|$ results in the best possible estimates or nearly best possible estimates of certain sums of sets in arithmetic progression.

Our purpose is to prove:

THEOREM 1. *Let G be an Abelian group with no 2-torsion and let B be a finite subset of G. If t is a positive integer such that $t < |B|$, then $|B_t(\mathrm{mod}\, K)| \geqq |B(\mathrm{mod}\, K)|$ for any finite subgroup K of G.*

The proof of Theorem 1 is carried out by employing the fundamental addition theorems in groups: Kneser's theorem (cf. [6], Th. 1.5) which is a generalization of the Cauchy-Davenport theorem (cf. [6], Corollary 1.2.3), and Kemperman's structure theorem (cf. [4], Th. 5.1) which is a generalization of Vosper's theorem (cf. [6], Th. 1.3). Through the course of the paper we refer to these theorems by their name only. Also, we follow the notation and terminology in Mann's book [6] and Kemperman's paper [4].

Before we enter into the details of the proof of Theorem 1, we define two further concepts. A finite subset C of G is said to be *periodic*, if there exists a nontrivial subgroup F of G such that $C + F = C$, i.e., C is a union of F-cosets. Otherwise we say C is *aperiodic*. A finite set A in G (possibly not Abelian) of size $|A| \geqq 2$ is in *arithmetic progression* on the right with difference d ($d \neq 0$) provided that A is in the form $A = \{a_0, a_0 + d, \cdots, a_0 + sd\}$ where s is a positive integer and $|A| \leqq |\langle d \rangle|$ where $\langle d \rangle$ is the cyclic group generated by d. A similar definition can be dualized for the left. Note, a set with exactly two elements can always be regarded as being in arithmetic progression on the right or the left.

1. Some preliminary lemmas

We require the following lemmas. Lemma 1.1, Lemma 1.2, and Lemma 1.3 are essentially due to Mann and Olson [5].

LEMMA 1.1. *Let G be a group (possibly not Abelian) with no 2-torsion and let B be a finite subset of G with $|B| \geqq 6$. Then B contains a subset R of size $|R| = 3$ which is not in arithmetic progression on the right.*

PROOF. For $x \in G$, $x + B$ is in arithmetic progression on the right if and only if B is in progression on the right. Thus, without loss of generality we may assume

$0 \in B$ since we may replace B by $-b+B$ where $b \in B$. Let $B' = \{0, b_2, \cdots, b_6\}$ be a subset of B. We shall select three elements r_1, r_2 and r_3 from B' to form $R = \{r_1, r_2, r_3\}$ so that R is not in progression. We choose $r_1 = 0$, $r_2 = b_2$, and pick r_3 distinct so that the following conditions hold:

i) $r_3 \neq -r_2$

ii) $r_3 \neq 2r_2$

iii) $2r_3 \neq r_2$.

The above selection of r_3 can be accomplished because if B' contains (say) $b_3 = -r_2$ and $b_4 = 2r_2$, we may choose r_3 which differs from b_3 and b_4, since b_5 and b_6 remain. Thus, conditions (i) and (ii) are satisfied if $r_3 = b_5$ or $r_3 = b_6$. Furthermore, either $r_3 = b_5$ or $r_3 = b_6$ must satisfy (iii) because if both fail to satisfy (iii), then $2b_5 = 2b_6$ hence $b_5 = b_6$ (since G has no 2-torsion) which is a contradiction. Hence, without loss of generality we may select $r_3 = b_5$. Thus $R = \{r_1, r_2, r_3\}$ is not in arithmetic progression on the right. This completes the proof.

LEMMA 1.2. *Let G be a group (possibly not Abelian) with no 2-torsion. Let t be a positive integer and let G_t be the set of sums of t distinct elements of G. If $t < |G|$, then $G_t = G$.*

PROOF. Let $g_1 \neq 0$ be an arbitrary element of G. Since no element of G is its own inverse, the elements of G may be listed as follows:

$$0,\ g_1,\ -g_1,\ g_2,\ -g_2, \cdots$$

If $= 2s+1$, then

$$g_1 = g_1 + (g_2 - g_2) + \cdots + (g_s - g_s).$$

Consequently, g_1 is a sum of t distinct elements of G, and similarly

$$0 = 0 + (g_2 - g_2) + \cdots + (g_s - g_s).$$

If $t = 2s$, then

$$g_1 = g_1 + 0 + (g_2 - g_2) + \cdots + (g_s - g_s)$$

and

$$0 = (g_1 - g_1) + \cdots + (g_s - g_s)$$

Therefore, $G_t = G$.

REMARK. Lemma 1.2 is false for G with 2-torsion. For example, if G is the elementary Abelian 2-group of order 2^n, then $|G_2| < |G|$. However, as noted in the introduction, the author proved $|B_2| \geqq |B|$ iff $B \neq x + N$ where N is the elementary Abelian 2-group.

LEMMA 1.3. *Let G be either a torsion-free Abelian group or a cyclic group of prime order p. Let B a finite subset of G and let t be a positive integer $1 \leqq t < |B|$. Then $|B_t| \geqq |B|$.*

PROOF. Since B is a finite subset of G, we may assume that G is finitely generated. We proceed by induction on t. For $t = 1$ the statement is true. Assume $t > 1$ and that the statement is true for all $t' < t$. Set $|B| = k$ and let $B = \{b_1, \cdots, b_k\}$. By Lemma 1.2, we may assume that B is aperiodic. We shall prove that the statement is true for $t = 2$.

If G is cyclic of prime order, we may take $b_1 = 0$, $b_2 = 1$ and $0 < 1 < b_3 < \cdots < b_k$ using the ordering inherited from Z (the integers). Then $0 + 1, \cdots, 0 + b_k$ are distinct, and $1 + b_k$ is distinct from $1, \cdots, b_k$ because either $1 + b_k = 0$ or $b_k < 1 + b_k$. Hence $|B_2| \geqq |B|$.

If G is free, we use a similar argument using the lexiographical ordering inherited from Z, since G is a direct sum of copies of Z.

Therefore, we may assume $t \geqq 3$. Now $|B_{k-t}| = |B_t|$ because $b_1 + \cdots + b_k - B_t \subseteq B_{k-t}$ and $b_1 + \cdots + b_k - B_{(k-t)} \subseteq B_t$. Hence, if $k + t < t$ we are done by induction. Thus we may assume $k \geqq 2t$, so $k \geqq 6$, and by Lemma 1.1 we can find a subset R of three elements of B which is not arithmetic progression. Let $B^* = B \setminus R$, then $|B^*| = k-3$. Now $t - 1 < k - 3$, so by induction

$$|B^*_{t-1}| \geqq |B^*| = k-3.$$

If $B^*_{t-1} + R$ is periodic, we are done; hence, we may assume that $B_{t-1} + R$ is aperiodic. Note that if $|B^*_{t-1} + R| = p-1$ (for $G = Z_p$) we are again done because we may assume that $|B| < p$ by Lemma 1.2. Thus by Kneser's theorem:

$$|B^*_{t-1} + R| \geqq |B^*_{t-1}| + |R| - 1.$$

If equality holds, then by Kemperman's structure theorem (B^*_{t-1}, R) must be an elementary pair because (i) for G torsion free, G contains no nontrivial finit

subgroups, and (ii) for $G = Z_p$ and the previous discussion, we may assume that $|B^*_{t-1} + R| \leqq p-2$. But $|B^*_{t-1}| > 1$, $|R| > 1$, and R is *not* arithmetic progression. This is a contradiction, i.e., (B^*_{t-1}, R) cannot be an elementary pair, therefore, we must have

$$|B^*_{t-1} + R| > |B^*_{t-1}| + |R| - 1$$

$$\geqq (k-3) + 3 = k.$$

Since $B^*_{t-1} + R \subseteq B_t$, we have proved $|B_t| \geqq |B|$.

2. Preliminaries for the Proof of Theorem 1

We introduce the following notation. Let G be an Abelian group with no 2-torsion and let H be a finite nontrivial subgroup of G. Let B be a finite subset of G of size $k = |B|$. Let $\sigma: G \to G/H$ denote the canonical homomorphism from G to the factor group G/H. We write $B(\mathrm{mod}\, H)$ to denote $B\sigma$; moreover, we put $X = B(\mathrm{mod}\, H)$ where $X = \{x_1, \cdots, x_m\}$, and thus $|X| = m$. Next, we define the following sets:

$$A_i = B \cap (x_i + H), \quad 1 \leqq i \leqq m$$

and we put $k_i = |A_i|$.

We arrange the notation so that

$$k_1 \geqq k_2 \geqq \cdots \geqq k_m \geqq 1.$$

Note that $\sum k_i = k$.

Without loss of generality we may assume that G is *finitely* generated because for K a finite subgroup of G, we may consider $G^* = \langle B, K \rangle$ the group generated by $B \cup K$. Hence $G = F \oplus T$ where F is the free part and T is the torsion part. Note that T is finite.

In the proof of Propositions 1.4, 1.5, 1.6, and Theorem 1, we proceed by double induction on t and the order of T. For $t = 1$, Theorem 1 is true, and for $T = \{0\}$ the theorem is true by Lemma 1.3. Consequently, we may assume that $t > 1$ and $|T| > 2$, and we make the inductive assumption that:

i) Theorem 1 is true for all orders $|T'| \leqq |T|$ when $t' < t$ and

ii) Theorem 1 is true for all orders $|T'| < |T|$ when $t' = t$.

PROPOSITION 1.4. *Let H be a nontrivial finite subgroup of G. Then*

$$\left|B_t(\mathrm{mod}\, H)\right| \geqq \left|B(\mathrm{mod}\, H)\right|.$$

PROOF. *Case* I. $k_1 = k_2 = \cdots = k_m = 1$.

In this case each element of B is in one and only one H-coset, therefore $|X| = |B| = k = m$ and $X_t = B_t(\mathrm{mod}\, H)$. However, by the inductive assumption on T, Theorem 1 holds in G/H, consequently $|X_t| \geqq |X|$, and thus $\left|B_t(\mathrm{mod}\, H)\right| \geqq \left|B(\mathrm{mod}\, H)\right|$.

Case II. $k_1 \geqq 2$.

Choose an element r from $A_1 = (x_1 + H) \cap B$ and consider the set $B' = B \setminus \{r\}$. Since $k > t$, we have $k - 1 > t - 1$. Furthermore, by the inductive assumption on t

$$\left|B'_{t-1}(\mathrm{mod}\, H)\right| \geqq \left|B'(\mathrm{mod}\, H)\right|.$$

But $\left|B'(\mathrm{mod}\, H)\right| = \left|B(\mathrm{mod}\, H)\right|$ and $r + B'_{t-1} \subseteq B_t$ so $(r + B'_{t-1})(\mathrm{mod}\, H) \subseteq B_t(\mathrm{mod}\, H)$. Thus $\left|B_t(\mathrm{mod}\, H)\right| \geqq \left|B'_{t-1}(\mathrm{mod}\, H)\right| \geqq \left|B(\mathrm{mod}\, H)\right|$.

This completes the proof.

PROPOSITION 1.5. *Let H be a cyclic subgroup of G of order p (p prime and $p > 2$). Recall that $m = |X|$ where $X = B(\mathrm{mod}\, H)$. If $t < m$, then $|B_t| \geqq |B|$.*

PROOF. We consider sums of t elements over distinct elements of X in G/H, then by the inductive assumption on the order of T, we have $|X_t| \geqq |X| = m$. Define the set $X' = X \setminus \{x_1\}$ then $t - 1 < m - 1$, and by induction $|X'_{t-1}| \geqq |X'| = m - 1$. Since $x_1 + X'_{t-1} \subseteq X_t$, it follows that at least $m - 1$ sums in X_t must contain x_1. Therefore, the corresponding set in G

$$S = \bigcup_{x_{i_1} + \cdots + x_{i_t} \in X_t} (A_{i_1} + \cdots + A_{i_t})$$

is a subset of B_t which contains at least $(m-1)k_1 + k_j$ ($j \geqq 1$) elements. Thus $|S| \geqq (m-1)k_1 + k_j$, but $(m-1)k_1 + k_j \geqq \sum k_i = k$ because $k_1 \geqq k_2 \geqq \cdots \geqq k_m \geqq 1$. Thus $|B_t| \geqq |B.|$

PROPOSITION 1.6. *Let H and m be defined as in Proposition 1.5. Assume $k_1 \geqq 3$, $m \geqq 2$, and $k - m \geqq t$. Then $|B_t| \geqq |B|$.*

PROOF. Let n be the largest index i, $1 \leqq i \leqq m$, such that $k_i \geqq 2$. Thus

$k_1 \geqq k_2 \geqq \cdots \geqq k_n \geqq 2$ and $k_{n+1} = \cdots = k_m = 1$. Now one can easily verify that the conditions $k_1 \geqq 3$, $m \geqq 2$, and $k - m \geqq t$ imply that there exist positive integers $t_1, \cdots, t_n$ satisfying the conditions:

i) $t_1 + \cdots + t_n = t - 1$

ii) $1 \leqq t_1 < k_1 - 1$

iii) $1 \leqq t_j < k_j$ for $2 \leqq j \leqq n$, if $n \geqq 2$.

Assume $n > 1$ and consider the set $X' = t_1 x_1 + \cdots + t_n x_n + X$ in the factor group G/H. Note that $|X'| = |X| = m$. Define the following sets S_j for $1 \leqq j \leqq m$ by:

$$S_j = (A_1)_{t_1} + \cdots + (A_j)_{t_j+1} + \cdots + (A_n)_{t_n}, \text{ for } 1 \leqq j \leqq n.$$

$$S_j = (A_1)_{t_1} + \cdots + (A_j)_{t_j} + \cdots + (A_n)_{t_n} + A_j, \quad \text{for } n < j \leqq m.$$

Thus $S_j \subseteq t_1 x_1 + \cdots + t_n x_n + x_j + H$ for $1 \leqq j \leqq m$; furthermore, since $t_1 < t - 1$ (because $n > 1$) we have by the induction assumption $|(A_1)_{t_1}| \geqq |A_1| = k_1$. Therefore $\{S_j\}$ is a collection of m disjoint sets, each a subset of B_t and each containing at least k_1 elements, so $|US_j| \geqq mk_1$, hence $|B_t| \geqq |B|$.

If $n = 1$, then $t_1 = t-1$ and $k_2 = \cdots = k_m = 1$. For $m \geqq 3$, we consider $((A_1)_{t-1} + A_2) \cup \cdots \cup ((A_1)_{t-1} + A_m)$ which consists of $k_1(m-1)$ elements, but $k_1(m-1) \geqq k_1 + (m-1)$. Therefore $|B_t| \geqq |B|$. For $m = 2$, we observe that $|(A_1)_t| \geqq k_1$ by Lemma 1.3. Thus $((A_1)_{t-1} + A_2) \cup (A_1)_t$ consists of $2k_1$ elements, so $|B_t| \geqq |B|$. This concludes the proof.

3. Proof of Theorem 1

We carry out the induction on t and T as explained before. We know that T contains a cyclic subgroup H of order p (p a prime). We first show $|B_t| \geqq |B|$.

Since $|B_{k-t}| = |B_t|$ (cf. proof of Lemma 1.3) we may assume that $k \geqq 2t$. Recall our notation $X = \{x_1, \cdots, x_m\}$. If $m = 1$, then Lemma 1.3 implies that $|B_t| \geqq |B|$, so we may assume that $m \geqq 2$. By Proposition 1.5 we may assume that $t \geqq m$. However, $k \geqq 2t$ and $t \geqq m$ imply that $k - m \geqq t$. If $k_1 \geqq 3$, then Proposition 1.6 gives $|B_t| \geqq |B|$. Therefore we may assume that $m \geqq 2$, $t \geqq m$, $k - m \geqq t$, $k \geqq 2t$, and $k_1 = 2$. These conditions imply that $m > 2$, $k_1 = k_2 = \cdots = k_m = 2$, and $t = m$. For $m \geqq 3$ define the sets S_j ($1 \leqq j \leqq m$) by

$$S_1 = A_1 + \cdots + A_m$$
$$S_2 = (A_1)_2 + A_3 + \cdots + A_m, \ (A_2 \text{ not included})$$
$$\vdots$$
$$S_j = (A_1)_2 + A_2 + \cdots + A_m, \ (A_j \text{ not included})$$
$$\vdots$$
$$S_m = (A_1)_2 + A_2 + \cdots + A_{m-1}, \ (A_m \text{ not included}).$$

Then each $S_j \subseteq x_1 + x_2 + \cdots + x_m + x_1 - x_j + H$, so $\{S_j\}$ is a collection of m disjoint sets each a subset of B_t and each consisting of at least two elements. So $|US_j| \geqq 2m$, and thus $|B_t| \geqq |B|$.

For $m = 2$ we have $|(A_1 + A_2) \cup (A_1)_2| \geqq 4$, so $|B_t| \geqq |B|$.

Next let K be any subgroup of T. Then Proposition 1.4 implies that $|B_t(\text{mod } K)| \geqq |B(\text{mod } K)|$. This completes the induction and proves the theorem for the case that G is finitely generated.

For the general case, let B be a finite subset of G, let K be a finite subgroup of G, and let $G^* = \langle B, K\rangle$ denote the group generated by $B \cup K$. Since G^* is *finitely* generated, we have

$$|B_t(\text{mod } K)| \geqq |B(\text{mod } K)|.$$

This completes the proof of the theorem.

COROLLARY. *Assuming that the hypothesis of Theorem* 1 *is true,* $|B_t| \geqq |B|$.

PROOF. Take $K = \{0\}$ in the theorem.

COROLLARY. *Let G be an Abelian group with no 2-torsion, let B be a finite subset of G, let K be a subgroup of G such that G/K has no 2-torsion, and let t be a positive integer such that $t < |B|$. Then,*

$$|B_t(\text{mod } K)| \geqq |B(\text{mod } K)|.$$

PROOF. The proof follows by induction on t, Theorem 1, and the same proof given in Proposition 1.4.

REMARK. The problem for G with 2-torsion is a bit more involved; however, we expect a solution can be worked out using the methods developed in the theorem and a greater dependence on Kemperman's structure theorem.

ACKNOWLEDGEMENT

We would like to express our gratitude to H. B. Mann for pointing out several important simplifications in the proof of Theorem 1.

REFERENCES

1. G. T. Diderrich, *On some addition theorems in groups*, Ph. D. Thesis, University of Wisconsin-Madison, 1972.

2. G. T. Diderrich, *An addition theorem for Abelian groups of order pq*, to appear in J. Number Theory.

3. G. T. Diderrich and H. B. Mann, *Combinatorial problems in finite Abelian groups*, to appear in Proc. Amer. Math. Soc.

4. J. H. B. Kemperman, *On small sumsets in an Abelian group*, Acta Math. **103** (1960), 63–88.

5. H. B. Mann and J. E. Olson, *Sums of sets in the elementary Abelian group of type* (p, p), J. Combinatorial Theory **5** (1968), 45–52.

6. H. B. Mann. *Addition Theorems*, John Wiley and Sons, 1965.

2973 N. CRAMER ST.,
MILWAUKEE, WISCONSIN,
U. S. A. 53211.