LEV F. VSEVOLOD

On small sumsets in abelian groups

Astérisque, tome 258 (1999), p. 317-321
<http://www.numdam.org/item?id=AST_1999__258__317_0>

Astérisque **258**, 1999, p. 317–321

ON SMALL SUMSETS IN ABELIAN GROUPS

by

Vsevolod F. Lev

Abstract. — In this paper we investigate the structure of those pairs of finite subsets of an abelian group whose sums have relatively few elements: $|A + B| < |A| + |B|$. In 1960, J. H. B. Kemperman gave an exhaustive but rather sophisticated description of recursive nature. Using intermediate results of Kemperman, we obtain below a description of another type. Though not (generally speaking) sufficient, our description is intuitive and transparent and can be easily used in applications.

1. Introduction

By G we denote an abelian group. A finite non-empty subset $S \subseteq G$ is said to be *an arithmetic progression with difference* d if S is of the form

$$S = \{a + id\colon i = 1, \dots, |S|\} \quad (a, d \in G).$$

If, in addition, the order of the group element d satisfies ord $d \geq |S| + 2$, then we say that S is a *true* arithmetic progression.

Let A and B be finite subsets of G. We write

$$A + B = \{a + b\colon a \in A,\ b \in B\},$$

and consider the following condition:

$$|A + B| \leq |A| + |B| - 1. \tag{$*$}$$

The aim of this paper is to prove the following

Main Theorem. — *Let A and B satisfy $(*)$, and suppose that* $\max\{|A|, |B|\} > 1$. *Then there exist a finite subgroup $H \subseteq G$ and two finite subsets $S_1, S_2 \subseteq G$ such that $A \subseteq S_1 + H$, $B \subseteq S_2 + H$, and one of the following holds:*

i) $|S_1| = |S_2| = 1$, *and* $|A + B| \geq \frac{1}{2}|H| + 1$;

ii) $|S_1| = 1$, $|S_2| > 1$, *and* $|A + B| \geq (|S_2| - 1)|H| + 1$;

iii) $|S_1| > 1$, $|S_2| = 1$, *and* $|A + B| \geq (|S_1| - 1)|H| + 1$;

1991 ***Mathematics Subject Classification.*** — 11P99, 11B75.
Key words and phrases. — Sumsets, small doubling.

iv) $\min\{|S_1|, |S_2|\} > 1$, *and* $|A+B| \geq (|S_1| + |S_2| - 2)|H| + 1$; *moreover,* S_1 *and* S_2 *are true arithmetic progressions with common difference* d *of order at least* $\operatorname{ord} d \geq |S_1| + |S_2| + 1$.

It can be easily verified that the conclusion of Main Theorem implies

$$|A + B + H| - |A + B| \leq |H| - 1$$

in cases ii)–iv), and

$$|A + B + H| - |A + B| \leq \frac{1}{2}|H| - 1$$

in case i): just observe that

$$|A + B + H| \leq |S_1 + S_2 + H| \leq |S_1 + S_2||H|.$$

Thus, $A + B$ "almost" fills in a system of H-cosets, while both $(A + H)/H$ and $(B + H)/H$ are in arithmetic progressions — unless some of them consists of just one element.

The Main Theorem will be proved in Section 3. Now, we give two definitions.

We say that the subgroup $H \subseteq G$, $|H| \geq 2$ is *a period* of the finite subset $C \subseteq G$ if C is a union of one or more H-cosets, that is if $C + H = C$. In this case C is called *periodic* and we write $H = P(C)$.

We say that the subgroup $H \subseteq G$, $|H| \geq 2$ is a *quasi-period* of the finite subset $C \subseteq G$, if C is a union of one or more H-cosets and possibly a subset of yet another H-coset. In this case C is called *quasi-periodic* and we write $H = Q(C)$.

If $H = P(C)$, we also say that H is a *true* period of C, as opposed to $H = Q(C)$, when C is a *quasi*-period. Obviously, if $H = P(C)$ or $H = Q(C)$ then $|H| < \infty$. Notice that according to the above definitions each periodic set is also quasi-periodic.

2. Auxiliary results

The following deep result due to Kemperman (see **[1]**) plays the central role in our proof.

***Theorem 1* (Kemperman).** — *Let* A *and* B *be finite subsets of* G *such that* $(*)$ *holds and* $\min\{|A|, |B|\} > 1$. *Then either* $A + B$ *is an arithmetic progression or* $A + B$ *is quasi-periodic.*

Corollary 1. — *Under the assumptions of Theorem 1, one of the following holds:*

i) $A + B$ *is in true arithmetic progression;*

ii) $A + B = c + H \setminus \{0\}$ *where* $H \subseteq G$ *is a subgroup, and* $c \in G$ *— an element of* G;

iii) $A + B$ *is quasi-periodic.*

The next lemma also originates in **[1]**.

***Lemma 1* (Kemperman).** — *Suppose that* $(*)$ *holds and that* $A + B$ *is in true arithmetic progression of difference* d. *Then also* A *and* B *are in true arithmetic progressions with the same difference* d. *Moreover, in* $(*)$ *equality holds, and therefore* $\operatorname{ord} d \geq |A| + |B| + 1$.

We need three more lemmas.

***Lemma* 2.** — *Let A and B be finite non-empty subsets of G, and let $H \subseteq G$ be a finite non-zero subgroup of G, satisfying*

$$(|A+H|-|A|)+(|B+H|-|B|)<|H|.$$

Then $H = P(A+B)$.

Proof. — We choose $c = a + b \in A + B$ and $h \in H$ and we prove that $c + h \in A + B$. We have:

$$|(a+H)\cap \overline{A}|+|(b+H)\cap \overline{B}| \le |(A+H)\cap \overline{A}|+|(B+H)\cap \overline{B}|<|H|,$$

hence

$$|(a+H)\cap A|+|(b+H)\cap B|>|H|,$$
$$|H\cap (A-a)|+|h-H\cap (B-b)|>|H|,$$

and therefore there exist $h_a, h_b \in H$ such that

$$h_a = h-h_b,\ h_a = a'-a,\ h_b = b'-b \quad (a'\in A,\ b'\in B).$$

But then $c + h = a + b + h_a + h_b = a' + b' \in A + B$ which was to be proved. □

***Lemma* 3.** — *Let $A, B \subseteq G$ satisfy $(*)$. Suppose that $A + B$ is quasi-periodic, and write $H = Q(A + B)$. Denote by σ the canonical homomorphism $\sigma\colon G \to G/H$, and set $A_1 = \sigma A$, $B_1 = \sigma B$. Then*

i) $|A_1 + B_1| \le |A_1| + |B_1| - 1$;
ii) $|A_1 + B_1| < |A + B|$;
iii) $|A + B| - 1 \ge (|A_1 + B_1| - 1)|H|$.

Proof. — i) Suppose first that $H = P(A + B)$. Obviously, $|A + B| \le |A + H| + |B + H| - 1$. But the left-hand side, as well as $|A + H|$ and $|B + H|$, divides by $|H|$, so we also have $|A + B| \le |A + H| + |B + H| - |H|$. Eventually, $|A + H| = |A_1||H|$, $|B + H| = |B_1||H|$ and $|A + B| = |A_1 + B_1||H|$.

Now consider the situation, when H is a quasi-period, but not a *true* period of $A + B$. Then by Lemma 2,

$$|A+B|+1 \le |A|+|B| \le |A+H|+|B+H|-|H|,$$

hence (since the right-hand side divides by $|H|$) we also have $|A + B + H| \le |A + H| + |B + H| - |H|$, and the proof finishes as in the case $H = P(A + B)$.

ii) Follows from iii).

iii) If $H = P(A + B)$, then

$$|A+B|-1 = |A_1+B_1||H|-1 > (|A_1+B_1|-1)|H|.$$

If H is not a true period of $A + B$, then $A + B$ contains $|A_1 + B_1| - 1$ full H-cosets, and at least one element in yet another H-coset, therefore $|A + B| \ge (|A_1 + B_1| - 1)|H| + 1$.

□

Lemma 4. — *Let* $A+B=c+H\setminus\{0\}$ *and suppose that* $\min\{|A|,|B|\}\ge 2$*, where* $A,B\subseteq G$ *are subsets,* $H\subseteq G$ *a subgroup, and* $c\in G$ *an element of* G*. Then* $|H|\ge 4$*.*

Proof. — We have: $|H|-1=|A+B|\ge|A|\ge 2$, hence $|H|\ge 3$. Suppose $|H|=3$, and so $|A|=|B|=|A+B|=2$. Let $A=a+\{0,d_1\},\ B=b+\{0,d_2\}$. Then $A+B=a+b+\{0,d_1,d_2,d_1+d_2\}$, hence $d_2=d_1,\ d_1+d_2=0$, and $H=\{0\}\cup\{a+b-c,a+b+d-c\}$, where $d=d_1=d_2,\ 2d=0$. Therefore $d=(a+b+d-c)-(a+b-c)\in H$, which contradicts to $|H|=3,\ 2d=0$. □

3. Proof of the Main Theorem

Denote $G_0=G,\ A_0=A,\ B_0=B$ and consider the following conditions:

1) $|A|=|B|=1$;
2) $|A|=1,\ |B|>1$;
3) $|A|>1,\ |B|=1$;
4) $A+B=c+\widetilde{H}\setminus\{0\}$, where $\widetilde{H}$ is a subgroup, and $c\in G$ — an element of G;
5) $A+B$ is in true arithmetic progression.

If all these conditions fail, then by Corollary 1 the sum A_0+B_0 is quasi-periodic, and we put $H_1=Q(A_0+B_0)$, $G_1=G_0/H_1$, denote by σ_1 the canonical homomorphism $\sigma_1\colon G_0\to G_1$ and set $A_1=\sigma_1A_0,\ B_1=\sigma_1B_0$, so that A_1,B_1 satisfy $(*)$ by Lemma 3, i). Now check, whether some of the conditions 1)–5) is met with G_1,A_1,B_1 substituted for G,A,B. If not, we continue the process by defining

$$H_2=Q(A_1+B_1),\ G_2=G_1/H_2,$$
$$\sigma_2\colon G_1\to G_2,\ A_2=\sigma_2A_1,\ B_2=\sigma_2B_1$$

and so on. At each step we obtain a pair of subsets $A_i,B_i\subseteq G_i$, satisfying $(*)$ and also $|A_i+B_i|<|A_{i-1}+B_{i-1}|$ (by Lemma 3, ii)). Eventually we obtain a pair $A_k,B_k\subseteq G_k$ $(k\ge 0)$, which meets at least one of the conditions 1)–5). We write $\sigma=\sigma_k\cdots\sigma_1\colon G\to G_k$ (or $\sigma=\mathrm{id}_G$ in the case $k=0$) so that $A_k=\sigma A,\ B_k=\sigma B$, and we write $H=\sigma^{-1}\widetilde{H}$ if the first condition met is 4), or $H=\ker\sigma$ otherwise. We distinguish 5 cases according to the first condition satisfied.

1) Here $k>0$ and $A_{k-1}+B_{k-1}=c+H_k$, where $c\in G_{k-1}$ (since H_k is a quasi-period of $A_{k-1}+B_{k-1}$), therefore $A_{k-1}\subseteq a+H_k,\ B_{k-1}\subseteq b+H_k$ $(a,b\in G_{k-1})$, whence $A\subseteq a'+H,\ B\subseteq b'+H$ $(a',b'\in G)$. We choose now $S_1=\{a'\},\ S_2=\{b'\}$ and observe, that by Lemma 3, iii)

$$\begin{aligned}|A+B|-1 &\ge (|A_1+B_1|-1)|H_1|\ge\cdots\ge\\ &\ge (|A_{k-1}+B_{k-1}|-1)|H_{k-1}|\cdots|H_1|=\\ &= (|H_k|-1)|H_{k-1}|\cdots|H_1|\ge\\ &\ge \frac{1}{2}|H_k||H_{k-1}|\cdots|H_1|=\frac{1}{2}|H|.\end{aligned}$$

2) Also here we may assume $k>0$, since otherwise the result is trivial if we choose $S_1=A,\ S_2=B,\ H=\{0\}$. Furthermore, as in 1) we have $A\subseteq a+H$. We choose $S_1=\{a\}$, and for S_2 we choose the system of arbitrary representatives of all

H-cosets, containing at least one element of B, so that $A \subseteq S_1 + H$, $B \subseteq S_2 + H$ and $|S_2| = |B_k|$. Then

$$|A+B| - 1 \geq \cdots \geq (|A_k + B_k| - 1)|H_k| \cdots |H_1| = (|S_2| - 1)|H|.$$

3) This case is analogous to the previous one in view of the symmetry between A and B.

4) In this case there exist $a, b \in G$ such that $A \subseteq a + H$, $B \subseteq b + H$ and we choose $S_1 = \{a\}$, $S_2 = \{b\}$. Then

$$\begin{aligned} |A+B| - 1 &\geq \cdots \geq (|A_k + B_k| - 1)|H_k| \cdots |H_1| = \\ &= (|\widetilde{H}| - 2)|H_k| \cdots |H_1| \geq \frac{1}{2}|\widetilde{H}||H_k| \cdots |H_1| = \frac{1}{2}|H| \end{aligned}$$

(since $|\widetilde{H}| \geq 4$ by Lemma 4).

5) In this case, by Lemma 1, A_k and B_k are in true arithmetic progressions with common difference d of order $\operatorname{ord} d \geq |A_k| + |B_k| + 1$, and $|A_k + B_k| = |A_k| + |B_k| - 1$. It is easily seen that we can choose two true arithmetic progressions $S_1, S_2 \subseteq G$ with a common difference d' in such a way, that $A_k = \sigma S_1$, $B_k = \sigma S_2$ and $|S_1| = |A_k|$, $|S_2| = |B_k|$, $\operatorname{ord} d' \geq \operatorname{ord} d$. Then

$$A \subseteq S_1 + H, \ B \subseteq S_2 + H, \ \operatorname{ord} d' \geq |S_1| + |S_2| + 1$$

and

$$|A+B| - 1 \geq \cdots \geq (|A_k + B_k| - 1)|H_k| \cdots |H_1| = (|S_1| + |S_2| - 2)|H|.$$

This completes the proof. □

References

[1] Kemperman J.H.B., *On small sumsets in an abelian group*, Acta Math., **103**, 1960, 63–88.

V.F. Lev, Inst. of Mathematics, Hebrew University, Jerusalem, Israel 91904
E-mail : seva@math.huji.ac.il • *Url :* http://www.ma.huji.ac.il/~seva/