ON RESTRICTED SET ADDITION IN ABELIAN GROUPS

GYULA KÁROLYI[1] Department of Algebra and Number Theory, Eötvös University, Pázmány P. sétány 1/C, Budapest, H–1117 Hungary

Abstract. Let A be a set of k elements of an Abelian group G in which the order of the smallest nonzero subgroup is at least $2k-3$. Then the number of different elements of G that can be written in the form $a+a'$, where $a, a' \in A$, $a \neq a'$, is at least $2k-3$, as it has been shown in [12]. Here we give yet another proof of this result.

1. Introduction

Let $G \neq 0$ denote any Abelian group. Define $p(G)$ as the smallest positive integer p for which there exists a nonzero element g of G with $pg = 0$. If no such integer exists, we write $p(G) = \infty$. Thus, $p(G) = \infty$ if and only if G is torsion free, otherwise it is a prime number that equals the order of the smallest nontrivial subgroup of G. In particular, if G is finite, then $p(G)$ is the smallest prime divisor of $|G|$.

For nonempty subsets $A, B \subseteq G$ with $|A| = k$ and $|B| = \ell$, define

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

[1]Visiting the Rényi Institute of the Hungarian Academy of Sciences. Research partially supported by Hungarian Scientific Research Grants OTKA T043623 and T043631.

and

$$A\dot{+}B = \{a + b \mid a \in A, b \in B, a \neq b\}.$$

If G is torsion free, that is, G is an ordered Abelian group, then the elements of A and B can be enumerated as $a_1 < a_2 < \ldots < a_k$ and $b_1 < b_2 < \ldots < b_\ell$ such that

$$a_1 + b_1 < a_2 + b_1 < \ldots < a_k + b_1 < a_k + b_2 < \ldots < a_k + b_\ell.$$

Thus we can conclude that $|A + B| \geq k + \ell - 1$ and $|A\dot{+}B| \geq k + \ell - 3$. In particular, $|A + A| \geq 2k - 1$ and $|A\dot{+}A| \geq 2k - 3$.

According to the Cauchy–Davenport theorem [3], if p is a prime number and $p \geq k + \ell - 1$, then $|A + B| \geq k + \ell - 1$ holds for any $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|A| = k, |B| = \ell$. This result has been generalized in several ways. In particular, the following improvement can be obtained easily from Kneser's theorem [13, 16] or can be proved directly with a combinatorial argument, see [11].

Theorem 1. *If A and B are nonempty subsets of an Abelian group G such that $p(G) \geq |A| + |B| - 1$, then $|A + B| \geq |A| + |B| - 1$.*

The case of restricted addition is apparently more difficult. In 1994 Dias da Silva and Hamidoune [4] proved the following analogue of the Cauchy–Davenport theorem, thus settling a problem of Erdős and Heilbronn (see [8]).

Theorem 2. *If A is a k-element subset of the p-element group $\mathbb{Z}/p\mathbb{Z}$, p a prime, then*

$$|A\dot{+}A| \geq \min\{p, 2k - 3\}.$$

Later Alon, Nathanson and Ruzsa [1, 2] applying the so-called 'polynomial method' gave a simpler proof that also yields

$$|A\dot{+}B| \geq \min\{p, |A| + |B| - 2\}$$

if $|A| \neq |B|$. Some lower estimates on the cardinality of $A\dot{+}B$ in arbitrary Abelian groups were obtained recently by Lev [14, 15], and also by Hamidoune, Lladó and Serra [10] in the case $A = B$. Moreover, some more refined results in elementary Abelian groups have been proved by Eliahou and Kervaire, see [5, 6, 7].

In [12] we obtained the following extension of the Dias da Silva–Hamidoune theorem.

Theorem 3. *If A is a k-element subset of an Abelian group G, then*

$$|A\dot{+}A| \geq \min\{p(G), 2k-3\}.$$

The aim of the present note is to give a short alternative proof of this result.

2. The Key Idea of the Proof

The case $p(G) = 2$ being fairly obvious, we will assume that $p(G) \geq 3$ in order to avoid some minor technicalities. In this case Theorem 3 is clearly equivalent to the following.

Theorem 4. *If A is a k-element subset of an Abelian group G with $p(G) \geq 2k-3$, then*

$$|A\dot{+}A| \geq 2k-3.$$

Indeed, if $2k-3 > p(G)$, then one can apply Theorem 4 for any subset A' of A with $p(G) = 2|A'| - 3$ to obtain the result; one only has to note that $A'\dot{+}A' \subseteq A\dot{+}A$.

Since A is contained in a finitely generated subgroup H of G, and obviously $p(H) \geq p(G)$, it is enough to prove Theorem 4 in the case when G is finitely generated. In this case we can write

$$G = G^1 \oplus G^2 \oplus \ldots \oplus G^m,$$

where each group G^i is isomorphic either to the infinite cyclic group $\mathbb{Z}$ or to a cyclic group $\mathbb{Z}/p^\alpha\mathbb{Z}$ with some prime number $p \geq p(G)$ and positive integer α. We have seen that the theorem is true if $G \cong \mathbb{Z}$, and Theorem 2 claims the same if $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime number p. In view of all this, to prove Theorem 4 it is enough to verify the following two statements.

Statement 5. *If Theorem 4 is valid for the Abelian groups G^1 and G^2, then it also holds for their direct sum $G^1 \oplus G^2$.*

Statement 6. *Let $p \geq 3$ be a prime number and let α be a positive integer. If Theorem 4 is valid for the group $\mathbb{Z}/p^\alpha\mathbb{Z}$, then it also holds for the group $\mathbb{Z}/p^{\alpha+1}\mathbb{Z}$.*

The key observation is that we can verify both statements using the same argument, based on the following notion. Let G^1 and G^2 be two Abelian groups for which we have already verified Theorem 4 for all possible values of k, and let $\varphi : G^1 \times G^1 \to G^2$ be any map. On the set of all ordered pairs (g^1, g^2) $(g^1 \in G^1, g^2 \in G^2)$, define an additive structure G_φ by introducing an operation $+_\varphi$ as follows:

$$(g^1, g^2) +_\varphi (h^1, h^2) =: (g^1 + h^1, g^2 + h^2 + \varphi(g^1, h^1)).$$

Note that if the map φ is symmetrical, then the operation $+_\varphi$ is commutative. Now Statements 5 and 6 can be easily derived from the following lemma.

Lemma 7. *Let A be a k-element subset of G_φ such that*

$$2k - 3 \le \min\{p(G^1), p(G^2)\}.$$

Then the set

$$A\dot{+}A =: \{a +_\varphi b \mid a, b \in A, a \ne b\}$$

has at least $2k - 3$ different elements.

Indeed, letting $\varphi \equiv 0$ we get back the notion of direct sum: $G_\varphi \cong G^1 \oplus G^2$. Since $p(G^1 \oplus G^2) = \min\{p(G^1), p(G^2)\}$, Statement 5 follows immediately. On the other hand, if we choose $G^1 = \mathbb{Z}/p\mathbb{Z}$, $G^2 = \mathbb{Z}/p^\alpha\mathbb{Z}$, and we define

$$\varphi(x + p\mathbb{Z}, y + p\mathbb{Z}) = \begin{cases} 0 & \text{if } x + y < p \\ 1 & \text{otherwise} \end{cases}$$

for $x, y \in \{0, 1, \dots, p-1\}$, then $G_\varphi \cong \mathbb{Z}/p^{\alpha+1}\mathbb{Z}$. Since

$$p(\mathbb{Z}/p^{\alpha+1}\mathbb{Z}) = p(\mathbb{Z}/p^\alpha\mathbb{Z}) = p(\mathbb{Z}/p\mathbb{Z}) = p,$$

Lemma 7, coupled with Theorem 2 implies Statement 6 as well.

It only remains to prove Lemma 7.

3. Preliminary Lemmas

For a set $X \subseteq G_\varphi$ write

$$X^1 = \{g^1 \in G^1 \mid \text{there exists } g^2 \in G^2 \text{ with } (g^1, g^2) \in X\}.$$

We define X^2 in a similar way. For $A, B \subseteq G_\varphi$ we also introduce

$$A + B =: \{a +_\varphi b \mid a \in A, b \in B\}.$$

An immediate consequence of these definitions is the following statement.

Proposition 8. *For arbitrary $X, Y \subseteq G_\varphi$ we have $(X \setminus Y)^1 \supseteq X^1 \setminus Y^1$ and $X^1 \dot{+} X^1 \subseteq (X \dot{+} X)^1 \subseteq X^1 + X^1$.*

The careful reader may observe that the second part of the statement does not remain valid in general if, instead of the projection to the first coordinate, one considers the projection to the second one.

We have to prove that $|A \dot{+} A| \geq 2k - 3$ for the k-element set $A \subseteq G_\varphi$. Note that

$$2|A^i| - 3 \leq 2k - 3 \leq p(G^i)$$

for $i = 1, 2$. Write $A = A_0 \cup C$, where $C = C_1 \cup \ldots \cup C_t$,

$$A_0 = \{(a_i, b_i) \ | 1 \leq i \leq s\}, \ C_i = \{(c_i, d_{ij}) \ | 1 \leq j \leq k_i\}$$

for $1 \leq i \leq t$ such that $2 \leq k_1 \leq k_2 \leq \ldots \leq k_t$, and $a_1, \ldots, a_s, c_1, \ldots, c_t$ are pairwise different elements of G^1. In particular, $k = s + k_1 + \ldots + k_t$ and $|A^1| = s + t$. The following easy lemma will be used frequently throughout the proof.

Lemma 9. *For $1 \leq \alpha, \beta \leq t$, $\alpha \neq \beta$ we have*

$$|C_\alpha \dot{+} C_\alpha| \geq 2k_\alpha - 3$$

and

$$|C_\alpha \dot{+} C_\beta| \geq k_\alpha + k_\beta - 1.$$

Proof. Adding $\varphi(c_\alpha, c_\alpha)$ to each element of $C_\alpha^2 \dot{+} C_\alpha^2$, we obtain the set $(C_\alpha \dot{+} C_\alpha)^2$. Consequently, $|C_\alpha \dot{+} C_\alpha| = |(C_\alpha \dot{+} C_\alpha)^2| = |C_\alpha^2 \dot{+} C_\alpha^2|$. Since

$$2|C_\alpha^2| - 3 = 2k_\alpha - 3 \leq 2k - 3 \leq p(G^2),$$

the first estimate follows directly from our hypothesis on G^2. Similarly, $(C_\alpha \dot{+} C_\beta)^2$ is obtained translating the set $C_\alpha^2 + C_\beta^2$ by $\varphi(c_\alpha, c_\beta)$. In this case we have

$$|C_\alpha^2| + |C_\beta^2| - 1 = k_\alpha + k_\beta - 1 \leq 2k - 5 < p(G^2),$$

and thus Theorem 1, applied to G^2, immediately implies

$$|C_\alpha \dot{+} C_\beta| = |(C_\alpha \dot{+} C_\beta)^2| = |C_\alpha^2 + C_\beta^2| \geq k_\alpha + k_\beta - 1.$$

□

4. Proof of Lemma 7

Assume first that $s = 0$, in which case $A = C = C_1 \cup \ldots \cup C_t$, $k = k_1 + \ldots + k_t$. The numbers $c_i + c_t$ $(1 \le i \le t)$ are t distinct elements of $C^1 + C^1$. It follows from Theorem 1 that $|C^1 + C^1| \ge 2t - 1$, and thus there is a set I of $t - 1$ pairs (γ, δ) such that the numbers

$$c_i + c_t \ (1 \le i \le t),\ c_\gamma + c_\delta \ ((\gamma, \delta) \in I)$$

are all different. Lemma 9 implies $|C_\gamma \dot{+} C_\delta| \ge 1$ for these pairs (γ, δ). It follows that the sets

$$C_i \dot{+} C_t \ (1 \le i \le t),\ C_\gamma \dot{+} C_\delta \ ((\gamma, \delta) \in I)$$

are pairwise disjoint subsets of $A \dot{+} A$. Based on Lemma 9 and the inequalities $k_i \le k_t$ for $1 \le i \le t$, we then indeed obtain

$$\begin{aligned} |A \dot{+} A| &\ge \sum_{(\gamma,\delta)\in I} |C_\gamma \dot{+} C_\delta| + \sum_{i=1}^{t-1} |C_i \dot{+} C_t| + |C_t \dot{+} C_t| \\ &\ge (t-1) + \sum_{i=1}^{t-1} (k_i + k_t - 1) + (2k_t - 3) \\ &\ge t - 1 + 2\sum_{i=1}^{t} k_i - (t-1) - 3 = 2k - 3. \end{aligned}$$

In the sequel we may assume that $s \ge 1$. If $t = 0$, that is, $|A_0^1| = s = k$, then we have

$$|A \dot{+} A| \ge |A_0^1 \dot{+} A_0^1| \ge 2k - 3$$

according to our assumption on the group G^1. Next, if $t = 1$ then we have $3 \le s + 2 \le (k + 2) - 2$. Note that in this case $(A \setminus C) \dot{+} C = A_0 \dot{+} C$ and $C \dot{+} C$ are disjoint, since $(g^1, g^2) \in C \dot{+} C$ implies $g^1 = c_1 + c_1$, while $g^1 = a_i + c_1$ for some $1 \le i \le s$ if $(g^1, g^2) \in A_0 \dot{+} C$. Moreover, the elements $(a_i + c_1, b_i + d_{1j})$ are pairwise different for $1 \le i \le s$, $1 \le j \le k_1$, thus we obtain the estimate

$$\begin{aligned} |A \dot{+} A| &\ge |A \dot{+} C| = |A_0 \dot{+} C| + |C \dot{+} C| \\ &\ge sk_1 + (2k_1 - 3) = s(k - s) + 2(k - s) - 3 \\ &= ((k + 2) - (s + 2))(s + 2) - 3 \ge 2k - 3, \end{aligned}$$

as it was to be proved.

Finally, turning to the general case $s \geq 1, t \geq 2$, we can argue as follows. First we claim that there is an index $1 \leq j \leq t-1$ such that

$$a_1 + c_j \notin \{c_1 + c_t, c_2 + c_t, \ldots, c_{t-1} + c_t\}.$$

Indeed, were

$$\{a_1 + c_j \mid 1 \leq j \leq t-1\} = \{c_i + c_t \mid 1 \leq i \leq t-1\},$$

we would get $D + \{d\} = D$ with $D = \{c_1, c_2, \ldots, c_{t-1}\}$ and $d = a_1 - c_t \neq 0$. This would in turn imply that the pairwise different numbers

$$c_1, c_1 + d, c_1 + 2d, \ldots, c_1 + (p(G^1) - 1)d$$

all belong to D, which is absurd, since

$$|D| = t - 1 < 2t - 2 \leq k - 3 < 2k - 3 \leq p(G^1).$$

This way we specified $t + 1$ pairwise different elements,

$$a_1 + c_j, a_1 + c_t, c_1 + c_t, c_2 + c_t, \ldots, c_{t-1} + c_t$$

of the set $A^1 \dot{+} A^1$ whose cardinality is at least $2(s+t)-3$, based on our assumption on G^1. From Proposition 8 it follows that $A \dot{+} A$ contains at least

$$2(s + t) - 3 - (t + 1) = 2s + t - 4$$

elements (g^1, g^2) such that

$$g^1 \notin \{a_1 + c_j, a_1 + c_t, c_1 + c_t, \ldots, c_{t-1} + c_t\}.$$

Denote the set of these elements by E. Introducing $F_\alpha = \{(a_1, b_1)\} \dot{+} C_\alpha$ for $\alpha = j, t$ we find that E, F_j, F_t and $C_i \dot{+} C_t$ $(1 \leq i \leq t-1)$ are pairwise disjoint subsets of $A \dot{+} A$. Obviously $|F_j| = k_j \geq k_1$ and $|F_t| = k_t$, hence Lemma 9 implies that

$$\begin{aligned} |A \dot{+} A| &\geq |E| + |F_j| + |F_t| + \sum_{i=1}^{t-1} |C_i \dot{+} C_t| \\ &\geq (2s + t - 4) + k_1 + k_t + \sum_{i=1}^{t-1} (k_i + k_t - 1) \\ &\geq 2s + t - 4 + 2\sum_{i=1}^{t} k_i - (t - 1) = 2k - 3. \end{aligned}$$

This completes the proof of Lemma 7. □

References

[1] N. Alon, M.B. Nathanson, and I.Z. Ruzsa, Adding distinct congruence classes modulo a prime, *Amer. Math. Monthly* **102** (1995) 250–255

[2] N. Alon, M.B. Nathanson, and I.Z. Ruzsa, The polynomial method and restricted sums of congruence classes, *J. Number Th.* **56** (1996) 404–417

[3] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* **10** (1935) 30–32

[4] J.A. Dias da Silva and Y.O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* **26** (1994) 140–146

[5] S. Eliahou and M. Kervaire, Sumsets in vector spaces over finite fields, *J. Number Th.* **71** (1998) 12–39

[6] S. Eliahou and M. Kervaire, Restricted sums of sets of cardinality $1 + p$ in a vector space over F_p, *Discrete Math.* **235** (2001) 199–213

[7] S. Eliahou and M. Kervaire, Restricted sumsets in finite vector spaces: the case $p = 3$, *Integers* **1** (2001), Research paper A2, 19 pages (electronic)

[8] P. Erdős and R.L. Graham, Old and New Problems and Results in Combinatorial Number Theory, *L'Enseignement Mathématique*, Geneva, 1980

[9] G.A. Freiman, Foundations of a Structural Theory of Set Addition, *Translations of Mathematical Monographs* **37** AMS, 1973

[10] Y.O. Hamidoune, A.S. Lladó, and O. Serra, On restricted sums, *Combin. Prob. Comput.* **9** (2000) 513–518

[11] Gy. Károlyi, A compactness argument in the additive theory and the polynomial method, to appear in *Discrete Math.* (2003)

[12] Gy. Károlyi, The Erdős–Heilbronn problem in Abelian groups, to appear in *Israel J. Math.* (2003)

[13] M. Kneser, Abschätzungen der asymptotischen Dichte von Summenmengen, *Math. Z.* **58** (1953) 459–484

[14] V.F. Lev, Restricted set addition in groups. I: The classical setting, *J. London. Math. Soc. (2)* **62** (2000) 27–40

[15] V.F. Lev, Restricted set addition in groups. II: A generalization of the Erdős-Heilbronn conjecture, *Electron. J. Combin.* **7** (2000), Research paper R4, 10 pages (electronic)

[16] M.B. Nathanson, Additive Number Theory. Inverse Problems and the Geometry of Sumsets, *GTM* **165**, Springer, 1996

E-mail address: karolyi@cs.elte.hu