ACTA ARITHMETICA
147.4 (2011)

A structure theory for small sum subsets

by

Yahya Ould Hamidoune (Paris)

1. Introduction. Let A, B be finite subsets of $\mathbb{Z}/n\mathbb{Z}$ such that $|A|, |B| \geq 2 + 2s$ and $|A + B| = |A| + |B| - 1 + s \leq n - 2 - 2s$. For n prime and $s = 0$, Vosper's Theorem [17] states that A and B are r-progressions for some step r. For n prime and $s = 1$, the authors of [9] proved that there is an r such that each of the sets A and B is obtained by deleting one element from an r-progression. Some applications of the last result may be found in the literature. In particular, it is used recently by Nazarewicz, O'Brien, O'Neill and Staples in the characterization of equality cases in Pollard's Theorem [14]. The authors of [10] obtained a description of the sets A, B if $s = 1$, $0 \in B$ and if every element of $B \setminus \{0\}$ generates $\mathbb{Z}/n\mathbb{Z}$.

Kemperman's structure Theorem [11] is a deep classical result, giving a recursive reconstruction of subsets A, B of an abelian group with $|A + B| = |A| + |B| - 1$. A dual equivalent reconstruction is given by Lev [13]. Recently Grynkiewicz [2] obtained a recursive reconstruction for the subsets A, B of an abelian group with $|A + B| = |A| + |B|$.

Using hyper-atoms and the strong isoperimetric property, the author obtained in [8] a description of the subgroups appearing in the reconstructions of Kemperman and Lev. In the present work, we investigate a more complicated hyper-atom structure. The above mentioned results follow as corollaries, in a relatively short space, from one of our main theorems. Most of the ingredients of our approach works in the non-abelian case. We need some terminology in order to present our results:

Let S be a generating subset of an abelian group G with $0 \in S$. For a subset $X \subset G$, we put $\partial_S(X) = (X + S) \setminus X$ and $X^S = G \setminus (X + S)$.

We say that S is *k-separable* if there is an X such that $|X| \geq k$ and $|X^S| \geq k$.

2010 *Mathematics Subject Classification*: Primary 11P70.
Key words and phrases: Minkowski sum, inverse theorems, approximate groups.

DOI: 10.4064/aa147-4-1

Suppose that $|G| \geq 2k-1$. The *kth connectivity* of S is defined as

$$\kappa_k(S) = \min\{|\partial(X)| : \infty > |X| \geq k \text{ and } |X^S| \geq k\},$$

where $\min \emptyset = |G| - 2k + 1$.

A finite subset X of G such that $|X| \geq k$, $|X^S| \geq k$ and $|\partial(X)| = \kappa_k(S)$ is called a *k-fragment* of S. A k-fragment with minimal cardinality is called a *k-atom*. We shall say that a subset S is *degenerate* if there is a subgroup which is a 2-fragment of S. A maximal subgroup which is a 2-fragment of a degenerate subset S will be called a *hyper-atom* of S.

The basic facts concerning the isoperimetric method may be found in [7].

A subset of a group G of cardinality one will be considered as a d-progression for every $d \in G$. A set S will be called an *$(r,-j)$-progression* if it can be obtained from an arithmetic progression with difference r by deleting j elements. Notice that an arithmetic progression P of difference r is also an $(r,-j)$-progression if r has an order $\geq |P| + j$. An $(r,-1)$-progression will sometimes be called a *near-r-progression*.

Let H be a subgroup of an abelian group G and let $d \in G/H$. Recall that a set S is said to be *H-periodic* if $S + H = S$. A set is said to be *$(H,-j)$-periodic* if it is obtained by deleting j elements from an H-periodic set. A partition $A = \bigcup_{i\in I} A_i$ will be called an *H-decomposition* of A if for every i, A_i is the nonempty intersection of some H-coset with A. An H-decomposition $X = \bigcup_{0\leq i\leq u} X_i$ such that $X_i + H + d = X_{i+1} + H$ for $1 \leq i \leq u-1$ will be called an *H-progression* with difference d.

For a nonempty subset X of G, we shall denote by X^* an arbitrary translated copy of X containing 0.

The pair $\{S,T\}$ will be called an *H-essential pair* if $S = \bigcup_{0\leq i\leq u} S_i$ and $T = \bigcup_{0\leq i\leq t} T_i$ are H-progressions with the same difference such that $|S+H| - |S| = |T+H| - |T| = |H|$ and one of the following holds:

(i) $|H| - 1 = |S_0| = |S_u| = |T_0| = |T_t| = 1$.
(ii) $|S_u| = |T_t| = 1$, $|S_{u-1}| = |T_{t-1}| = |H| - 1$, $T_{t-1} + S_u = T_t + S_{u-1}$.
(iii) There are two subgroups K_0, K_1 of order 2 such that $H = K_0 \oplus K_1$, $S_0^* = T_0^* = K_0$ and $S_u^* = T_t^* = K_1$.

An essential pair of type (iii) will be called a *Klein pair*.

Our first goal is to prove the next two results:

THEOREM 1.1. *Let $\mu \in \{0,1\}$. Let S be a degenerate generating subset of an abelian group G with $0 \in S$ and let H be a hyper-atom of S. Let T be a finite subset of G such that $3 - \mu \leq |S| \leq \max(4-2\mu, |S|) \leq |T|$, $S+T$ is aperiodic and $|S| + |T| - \mu = |S+T| \leq (2|G| + 2\mu)/3$. Then one of the following holds:*

(i) *$\mu = 0$ and $|G| = 3|S| = 3|T| = 4\kappa_2(T^*) = 12$.*
(ii) *$\mu = 0$ and $\{S,T\}$ is an H-essential pair.*

(iii) *There are H-progressions $S = \bigcup_{0\le i\le u} S_i$ and $T = \bigcup_{0\le i\le t} T_i$ with the same difference such that one of the sets $S \setminus S_u$, $T \setminus T_t$ is H-periodic and the other is $(H, -\nu)$-periodic, and $|T_t + S_u| = |T_t| + |S_u| - \nu - \mu$, where $0 \le \nu \le 1-\mu$. Moreover $|T+H|-|T| \le |H|-\mu$.*

THEOREM 1.2. *Let $\mu \in \{0,1\}$. Let S be a finite generating subset of an abelian group G such that $0 \in S$ and $3 \le |S| \le (|G| + 5\mu - 4)/2$. Assume moreover that $\kappa_{3-\mu}(S) \le |S| - \mu$, and that $\kappa_4(S) \le |S|$ if $|S| = 3 = \mu + 3$. If S is nondegenerate, then S is an $(r, \mu - 1)$-progression for some r.*

The case $\mu = 1$ of the last result was obtained in [4]. Another proof of this result is included in [7].

The organization of the paper is the following:

Section 2 presents our tools. Let S and T be finite subsets of an abelian group G such that $3 - \mu \le |S| \le \max(4 - 2\mu, |S|) \le |T|$, $S + T$ is aperiodic and $|S| + |T| - \mu = |S + T|$, where $\mu \in \{0, 1\}$. In Section 3, assuming that S is degenerate with a hyper-atom H and that $|S + T| \le (2|G| + 2\mu)/3$, we obtain a $2n/3$-modular result asserting that for $|G| \ne 12$, $\phi(S)$ and $\phi(T)$ are progressions with the same difference, where $\phi : G \to G/H$ denotes the canonical morphism. In Section 4, we prove Theorem 1.1. In Section 5, we show that a subset S with $\kappa_{3-\mu}(S) \le |S| - \mu$ and $4 \le |S| \le (|G| + 5\mu - 4)/2$ is either degenerate or a near-progression. Section 5 also contains the proof of Theorem 1.2. In Section 6, we obtain a modular structure theorem encoding efficiently all the situations with $|S + T| \le |G| - 4$. We apply the last result in Section 7 to give the structure of S and T allowing $|S| = |T| = 3$ and $|S+T| = |G|-3$. We show how to recover the structure results of Kemperman [11] and Grynkiewicz [2].

In the present work, we apply Kneser's Theorem (proved in less than two pages in [16]), Lemma 2.4 (proved in few lines in [10]). We also apply Theorem 2.9, Theorem 2.13 and Proposition 2.17 (these three results are proved in around two pages in [7]). We include short proofs for other needed lemmas, making the work nearly self-contained.

We omit the easy case where $S+T$ is periodic (cf. [8, 2]), the trivial case $|S| = 2$ and the easy case $|S + T| \le |G| - 2$.

2. Some tools

2.1. Preliminaries. Let A, B be finite subsets of an abelian group G. We write $A + B = \{x + y \ : \ x \in A \text{ and } y \in B\}$. The subgroup generated by A will be denoted by $\langle A\rangle$. Recall the following results:

LEMMA 2.1 (folklore). *If A and B are subsets of a finite group G such that $|A| + |B| \ge |G| + 1$, then $A + B = G$.*

THEOREM 2.2 (Scherk's Theorem [15]). *Let A and B be finite subsets of an abelian group G. If there is an element c of G such that $|A\cap(c-B)|=1$, then $|A+B|\geq|A|+|B|-1$.*

THEOREM 2.3 (Kneser's Theorem [12]). *Let A,B be finite subsets of an abelian group. If $A+B$ is aperiodic, then $|A+B|\geq|A|+|B|-1$.*

LEMMA 2.4 ([10]). *Let A be an $(r,-1)$-progression with $0\in A$ and let $B\subset\langle A\rangle$ be such that $\min(|B|,|A|)\geq 3$ and $|B+A|\leq|A|+|B|\leq|\langle A\rangle|-4$. If $A+B$ is aperiodic, then B is an $(r,-1)$-progression.*

LEMMA 2.5 ([1]). *Let X be a finite subset of an abelian group G. Then $X\subset(X^S)^{-S}$ and $(X^S)^{-S}+S=X+S$.*

Proof. Clearly $X\subset(X^S)^{-S}$. Take $x=y+s$ with $y\in(X^S)^{-S}$ and $s\in S$. We have $x\in X+S$, otherwise $x-s\in X^S-S$ and hence $y=x-s\notin(X^S)^{-S}$, a contradiction. ∎

We can use Kneser's Theorem to get some isoperimetric duality:

LEMMA 2.6. *Let X be a subset of a finite abelian group G such that $X+S$ is aperiodic and $|X+S|=|X|+|S|-\mu$, where $\mu\geq 0$. Then X^S-S is aperiodic. There is $0\leq\zeta\leq 1$ such that $|X^S-S|=|X^S|+|S|-\zeta$. Moreover $|(X^S)^{-S}|=|X|+\zeta-\mu$.*

Proof. By Lemma 2.5, X^S-S is aperiodic. By Kneser's Theorem, $\zeta\leq 1$. Clearly $X^S-S\subset G\setminus X$, and hence

$$\begin{aligned}|X^S|+|S|-\zeta+|(X^S)^{-S}|&=|X^S-S|+|(X^S)^{-S}|=|G|\\&=|X+S|+|X^S|=|X^S|+|X|+|S|-\mu.\end{aligned}$$

Thus $|(X^S)^{-S}|=|X|+\zeta-\mu$. ∎

The following lemma is a very special case of the main result of [2]:

LEMMA 2.7 ([2]). *Let S,T be subsets of an abelian group G such that $|S|=|T|=3$, $S+T$ is aperiodic and $|T+S|=6-\mu$, where $0\leq\mu\leq 1$. Then there exist $r,a\in G$ such that one of the following holds:*

(i) *One of the sets S and T is an r-progression.*
(ii) *$T=a+S$.*

Proof. Without loss of generality, we may assume $0\in T\cap S$. Suppose that neither S nor T is a progression.

Assume first that there is an $a\in S\setminus\{0\}$ with $2a=0$. Put $H=\{0,a\}$ and $S=\{0,a,b\}$. We have $|T+H|=2|H|$, otherwise $T+S$ would contain a periodic subset of size 6. By translating T suitably, we may take $T=\{0,a,c\}$. Now $T+S\supset H\cup(b+H)\cup(c+H)$. We must have $b+H=c+H$, and hence $c=b+r$ for some $r\in H$. Thus $T=r+S$ and (ii) holds. So we may assume that $2x\neq 0$ for every $x\in(S\cup T)\setminus\{0\}$.

Now for every $x \in T \setminus \{0\}$, we have $|(x+S) \cap X| \leq 1$, otherwise S would be an x-progression, a contradiction. Observe that $|(S+x) \cap (S+y)| = 1$ for any distinct $x, y \in T$, since otherwise putting $T = \{x, y, z\}$, we have $|(S+z) \cap (S+x)| \geq 2$ or $|(S+z) \cap (S+y)| \geq 2$, a contradiction.

Notice that the last observation is still valid if S and T are permuted.

Put $T = \{0, u, v\}$. Since $|S \cap (S+u)| = 1$, there is an a such that $S - a = S_0 = \{0, u, w\}$. Since $|S_0 \cap (S_0 + v)| = 1$, we have $w \in \{u+v, u-v, v, -v\}$. Up to a translation by $-u$, we have $w = v$ or $w = -v$. Assuming $w = -v$, we have $S + T = \{0, u, v, 2u, v+u, -v, u-v\}$. It follows that $u - v \in \{0, u, v, 2u, v+u, -v, u-v\}$. All possible cases imply that one of the sets S and T is a progression, a contradiction. Thus $w = v$, and hence (ii) holds. ∎

2.2. Isoperimetric tools. Let S be a finite subset of an abelian group. A k-fragment of S^* will be called a *k-fragment* of S. This notion is independent of the choice of S^* [4]. A k-fragment of $-S$ will be called a *negative* k-fragment of S.

Lemma 2.8 ([7]). *Let S be a generating subset of an abelian group G with $0 \in S$. Let X be a k-fragment of S and let A be a k-atom of S. Then $-X$ is a negative k-fragment of S. Moreover X^S is a negative k-fragment of S if G is finite. In particular, $|X^S| \geq |A|$.*

A fragment X of S such that $|X| \leq |X^S|$ will be called a *proper* fragment. The following result will be a fundamental tool in this paper:

Theorem 2.9 ([7]). *Let S be a generating subset of an abelian group G with $0 \in S$. If X and Y are two k-fragments of S such that $|X \cap Y| \geq k$ and $|(X \cup Y) + S| \leq |G| - k$, then $X \cap Y$ and $X \cup Y$ are k-fragments of S. In particular, $X \cap Y$ is a k-fragment if $|X| \leq |Y^S|$ or if X and Y are proper k-fragments.*

The basic intersection theorem is the following:

Theorem 2.10 ([5, 8]). *Let S be a generating subset of an abelian group G with $0 \in S$. Let A be a k-atom of S and let F be a k-fragment of S with $|A \cap F| \geq k$. Then $A \subset F$. In particular, $A = F$ if F is a k-atom.*

Proof. By Lemma 2.8, $|A^S| \geq |F|$. By Theorem 2.9, $A \cap F$ is a k-fragment and hence $A \cap F = A$. ∎

The structure of 1-atoms obtained in [3] using an old terminology is the following:

Proposition 2.11 ([3]). *Let S be a finite generating subset of an abelian group G with $0 \in S$. Let H be a 1-atom of S with $0 \in H$ and let F be a 1-fragment of S. Then H is a subgroup and $F + H = F$. Moreover $\kappa_1(S) \geq |S|/2$.*

Proof. Take an element $x \in H$. Since $(x+H) \cap H \neq \emptyset$, Theorem 2.10 yields $x+H = H$. Since H is finite, it is a subgroup. Take an element $y \in F$; the same argument shows that $y+H \subset F$, and hence $F+H = F$. Note that $H \neq G$, $0 \in S$ and that S generates G. In particular, $|H+S| \geq 2|H|$. Thus, $|H+S| - |H| \geq |S+H|/2$. By the definition of κ_1, we have

$$\kappa_1(S) = |H+S| - |H| \geq |S+H|/2 \geq |S|/2. \blacksquare$$

We need the following consequence of the above result:

PROPOSITION 2.12. *Let Y be a finite subset of an abelian group G with $0 \in Y$. Put $K = \langle Y \rangle$ and let $Z \subset K$. Let X be an aperiodic subset of G such that $|X+Y| \leq |X| + r|Y|$ and let $X = X_0 \cup \cdots \cup X_t$ be a K-decomposition. Set $W = \{i \in [0,t] : |X_i + Y| < |K|\}$ and $P = \{i \in [0,t] : |X_i| = |K|\}$. Then*

(i) *$|X+Y| \geq |X| + |W|\,|Y|/2$ and $|W| \leq 2r$. If $|Y| \geq 3$, then $|W| \leq 2r-1$.*

(ii) *If $|W| = 2r$, then $|X+Y| = |X| + r|Y|$ and $|P| = t+1-2r$. Moreover X_i and Y are progressions with the same difference for every $i \in W$.*

(iii) *If $|W| = 2$ and $r = 1$, then $|(\bigcup_{i\in W} X_i) + Z| \geq |\bigcup_{i\in W} X_i| + |W|$.*

(iv) *If $X+Y$ is aperiodic, $r = 1$ and $W = \{w\}$, then $X \setminus X_w$ is $(K,-1)$-periodic.*

Proof. Let H be a 1-atom of Y with $0 \in H$. By Proposition 2.11, we have

$$\begin{aligned} |X| + r|Y| \geq |X+Y| &\geq \sum_{i\in W} |X_i + Y| + \sum_{i\notin W} |X_i + Y| \\ &\geq \sum_{i\in W} (|X_i^*| + \kappa_1(Y)) + \sum_{i\notin W} |K| \\ &\geq \sum_{i\in W} (|X_i| + |Y|/2) + \sum_{i\notin W} |X_i| \geq |X| + |W|\,|Y|/2. \end{aligned}$$

Hence $|W| \leq 2r$. Assume now that $|W| = 2r$. Then the last chain consists of equalities and therefore $P = [0,t] \setminus W$ and $\kappa_1(Y) = |Y|/2$. By Proposition 2.11, $X_i + H = X_i$ for all $i \in W$. In particular, $X + H = X$. Since X is aperiodic, we have $|H| = 1$. Therefore $|Y| - 1 = |H+Y| - |H| = \kappa_1(Y) = |Y|/2$. Hence $|Y| = 2$. Put $Y = \{0, d\}$. Since $|X_i + Y| = |X_i| + 1$, X_i is a progression with difference d for all $i \in W$. Thus

$$\Big|\bigcup_{i\in W} (X_i + Z)\Big| \geq \sum_{i\in W} |Z + X_i^*| \geq \sum_{i\in W} (|X_i| + 1) = \sum_{i\in W} |X_i| + |W|,$$

since d generates K and $|X_i| < |K|$ for all $i \in W$.

Suppose that $X+Y$ is aperiodic, $r = 1$ and $W = \{w\}$. By Kneser's Theorem, $|X+Y| \geq t|K| + |X_w + Y| \geq t|K| + |X_w| + |Y| - 1$, and (iv) holds. $\blacksquare$

We need the following description of 2-atoms proved in [6]:

THEOREM 2.13 ([6]). *Let S be a finite generating subset of an abelian group G with $0 \in S$ and $\kappa_2(S) \le |S|$. Also assume that $|S| \ne |G| - 6$ if $\kappa_2(S) = |S|$. Let H be a 2-atom of S with $0 \in H$. Then either H is a subgroup or $|H| = 2$.*

A simplified proof of Theorem 2.13 is given in [7]. A generalization to the case $\kappa_2(S) \le |S| + 4$ is obtained in [10].

2.3. Vosper subsets. Let S be a subset of an abelian group G with $0 \in S$. We shall say that S is a *Vosper subset* if for all $X \subset G$ with $|X| \ge 2$, we have

$$|X + S| \ge \min(|G| - 1, |X| + |S|).$$

We need the following lemma:

LEMMA 2.14 ([8]). *Let S be a finite generating subset of an abelian group G with $0 \in S$. Let $X \subset G$ be such that $|X + S| = |X| + |S| - 1$ and $|X| \ge |S|$. Assume moreover that S is either a Vosper subset or a progression. Then $|X + (S \setminus \{y\})| \ge |X| + |S| - 2$ for every $y \in S$.*

Proof. Notice that $\kappa_2(S \setminus x) \ge |S| - 2$ if S is an arithmetic progression. Assume that S is a Vosper subset. By definition, we have $|X + S| \ge |G| - 1$. There are two possibilities:

CASE 1: $|X + S| = |G| - 1$. Suppose that $|X + (S \setminus \{y\})| \le |X| + |S| - 3$ and take $z \in (X + S) \setminus (X + (S \setminus \{y\}))$. We have $z - y \in X$. Also $(X \setminus \{z - y\}) + S \subset ((X + S) \setminus \{z\})$. By the definition of a Vosper subset, we have $|(X \setminus \{z - y\}) + S| \ge \min(|G| - 1, |X| - 1 + |S|) = |X| + |S| - 1$. Clearly $X + S \supset ((X \setminus \{z - y\}) + S) \cup \{z\}$. Hence $|X + S| \ge |X| + |S|$, a contradiction.

CASE 2: $|X + S| = |G|$. Suppose that $|X + (S \setminus \{y\})| \le |X| + |S| - 3$ and take a 2-subset T of $(X + S) \setminus (X + (S \setminus \{y\}))$. We have $T - y \subset X$. Also $(X \setminus (T - y)) + S \subset (X + S) \setminus T$. By the definition of a Vosper subset, $|(X \setminus (T - y)) + S| \ge \min(|G| - 1, |X| - 2 + |S|)$. We have $|X| = 1$. Otherwise and since $X + S \supset ((X \setminus (T - y)) + S) \cup T$, we have $|X + S| \ge |X| + |S|$, a contradiction. Then $|X| = |S| = 3$, and hence $|G| = 5$. Now by the Cauchy–Davenport Theorem, $|X + (S \setminus \{y\})| \ge |X| + |S| - 2$, a contradiction. ∎

We need the following lemma which is a consequence of Theorem 2.13:

PROPOSITION 2.15 ([4, 8]). *Let S be a finite generating subset of an abelian group G such that $0 \in S$, $|S| \le (|G| + 1)/2$ and $\kappa_2(S) \le |S| - 1$. If S is not a progression, then S is degenerate.*

COROLLARY 2.16. *Let S be a finite degenerate generating subset of an abelian group G such that $0 \in S$ and $\kappa_2(S) \le |S| < |G|/2$, and let H be*

a hyper-atom of S. Then $\phi(S)$ is either a progression or a Vosper subset, where ϕ is the canonical morphism from G onto G/H.

Proof. Assume that $\phi(S)$ is neither a Vosper subset nor a progression. Then $\kappa_2(\phi(S)) \le |\phi(S)| - 1$. We have $|S+H| \le |S| + |H| < |G|/2 + |H|$. Therefore $2|S+H| < |G| + 2|H|$ and hence $2|\phi(S)| \le |G|/|H| + 1$. By Proposition 2.15, $\phi(S)$ has a 2-fragment K which is a subgroup.

We have $|\phi^{-1}(K)+S| \le (|K|+|\phi(S)|-1)|H| = |\phi^{-1}(K)|+|H+S|-|H| = |\phi^{-1}(K)| + \kappa_2(S)$. Since $K + \phi(S) \ne G/H$, we have $\phi^{-1}(K) + S \ne G$. In particular, $\phi^{-1}(K)$ is a 2-fragment which is a subgroup, a contradiction. ∎

2.4. The strong isoperimetric property. Let $S = \bigcup_{0\le i\le u} S_i$ and $T = \bigcup_{0\le i\le t} T_i$ be H-decompositions. A (T,S,H)-*matching* is a family $\{n_i : i \in J\}$, where $J \subset [0,t]$ such that $G \setminus (T+H) \supset \bigcup_{i\in J} T_i + S_{n_i}$ is an H-decomposition. We shall call $|J|$ the *size* of the matching.

We call the property in the next result the *strong isoperimetric property.*

Proposition 2.17 ([7]). *Let G be an abelian group and let S be a finite subset of G with $0 \in S$. Let H be a subgroup of G which is a 2-fragment and let $S = S_0 \cup \cdots \cup S_u$ and $T = T_0 \cup \cdots \cup T_t$ be H-decompositions. If $t \ge u$ and $|G| \ge (t+u+1)|H|$, then there is a (T,S,H)-matching of size u.*

Notice that the obvious necessary condition $t \ge u$ was omitted in [7]. The proof requires no change.

3. Modular progressions

Theorem 3.1. *Let $\mu \in \{0,1\}$. Let S be a degenerate generating subset of an abelian group G with $0 \in S$ and let H be a hyper-atom of S. Let $\phi : G \to G/H$ denote the canonical morphism. Let T be a finite subset of G such that $3 - \mu \le |S| \le \max(4-2\mu, |S|) \le |T|$, $S+T$ is aperiodic and $|S+T| = |S|+|T|-\mu \le (2|G|+2\mu)/3$. Then one of the following conditions holds:*

(i) *$\mu = 0$ and $|G| = 3|S| = 3|T| = 4\kappa_2(T^*) = 12$.*
(ii) *$|\phi(S+T)| = |\phi(S)| + |\phi(T)| - 1$ and moreover $\phi(S)$ and $\phi(T)$ are progressions with the same difference.*

Proof. Set $|G| = n$, $h = |H|$, $|\phi(S)| = u+1$, $|\phi(T)| = t+1$, $|\phi(S+T)| = k+1$ and $q = n/h$. Take H-decompositions $T = \bigcup_{0\le i\le t} T_i$ and $S = \bigcup_{0\le i\le u} S_i$ such that $|S_0| \ge \cdots \ge |S_u|$. For $0 \le i \le u$, put $K_i = \langle S_i^* \rangle$. We shall also assume (by a suitable reordering) that $|K_0| \ge |K_u|$ in the case where $|S_0| = |S_u|$. We have $|G| > |S+H| \ge 2|H|$, and hence $|G| \ge 6$. Therefore $|T^S| \ge (|G| - 2\mu)/3 > 1$. Since $|S+T| \le |G| - 2$, we have

$$uh = |H+S| - h = \kappa_2(S) \le |S| - \mu. \tag{3.1}$$

It follows that for all $u \geq j \geq 0$,

$$(j+1)|S_{u-j}| \geq |S_{u-j}| + \cdots + |S_u| \geq jh + \mu. \tag{3.2}$$

Hence for $u \geq 2$,

$$|S_0| + |S_{u-1}| \geq \frac{2(|S_0| + |S_{u-1}| + |S_u|)}{3} \geq \frac{2|H| + \mu}{3}. \tag{3.3}$$

Without loss of generality, we may assume that $0 \in S_0$.

Since T is aperiodic, we have $(t+1)h > |T| \geq |S| \geq \kappa_2(S) = uh$, and hence

$$t \geq u. \tag{3.4}$$

Choose a (possibly empty) (T, S, H)-matching $\{n_i : i \in J\}$, where $J \subset [0, t]$. Put $|J| = r$. Take an H-decomposition $S + T = \bigcup_{0 \leq i \leq k} E_i$ such that

(1) $T_i + S_0 \subset E_i$ for all $0 \leq i \leq t$,
(2) $\bigcup_{i \in J}(T_i + S_{n_i}) \subset \bigcup_{1 \leq i \leq r} E_{t+i}$.

We also assume that $|E_{t+r+1}| \leq \cdots \leq |E_k|$ if $k \geq t + r + 1$. We shall choose the H-decomposition and J so as to maximize $(r, |E_k|)$ lexicographically.

We put $P = \{i \in [0, k] : |E_i| = h\}$ and $W = \{i \in [0, t] : |E_i| < h\}$.

Suppose that $k \geq t + r + 1$ and take an s with $T_s + S_{\alpha_s} \subset E_k$. Then $T_s + S_{n_s} \subset E_j$ for some $t + 1 \leq j \leq t + r$, otherwise $J \cup \{s\}$ would give a matching of size $r + 1$. Since $1 \leq \min(n_s, \alpha_s)$ and $n_s \neq \alpha_s$, we have $u \geq 2$. Now we can choose $\alpha_s \geq u - 1$, otherwise $(J \setminus \{j\}) \cup \{k\}$ gives a matching contradicting our choice. In particular,

$$|E_k| \geq |S_{u-1}| \quad \text{and} \quad u \geq 2, \quad \text{if } k \geq t + r + 1. \tag{3.5}$$

Case 1: $\phi(T) = G/H$. Thus $t + 1 = q$. Let us show that

$$u = 1.$$

Suppose $u \geq 2$. By (3.2),

$$|S_0| \geq \frac{uh + \mu}{u + 1} \geq \frac{2h + \mu}{3}.$$

On the other hand,

$$|T + S| \geq \sum_{i \in [0,t]} |T_i + S_0| \geq q|S_0| \geq q\frac{2h + \mu}{3} \geq \frac{2n + 3\mu}{3}.$$

It also follows that $\mu = 0$ and $|T_i + S_0| = |S_0| = 2h/3$ for all i. Also $u = 2$ and $|S_2| = |S_1| = |S_0|$. The same thing applies to S_1 and S_2, and hence $T_i^* + S_s = S_s$ for all i, s. Since S is aperiodic we must have $|T_i| = 1$ for all i. Since $T + S = T + S_0 = T + S_1$, there are distinct r, s with $T_r + S_0 = T_s + S_1$. It follows that $S_1 = S_0 + w$, where $\{w\} = T_r - T_s$. Now we have $T + S = T + S_1 = T + S_0 + w = T + S + w$, a contradiction.

Assuming $K_0 \neq H$, by (3.2) we have $h \geq 2|S_0| \geq |S_0| + |S_1| \geq h$. Thus

$$h/2 = |S_0| \geq |K_0| \geq |K_1| \geq |S_1| = h/2.$$

Thus we must have $S_0 = K_0$ and $S_1 = K_1 + b$ for some b. Since S is aperiodic, we have $K_0 \cap K_1 = \{0\}$ and hence $h^2/4 \leq h$. In particular, $|K_0| = |K_1| = 2$ and H is isomorphic to $K_0 \oplus K_1$. Since $t + 1 = q$, we have $S + T = (T + K_0) \cup (T + K_1 + b)$. Then $E_i \supset (K_0 + T_i) \cup (K_1 + c)$ for some c, and hence $|E_i| \geq 3$ for all i. Therefore $|S + T| \geq 3q = 3n/4 > (2n + 2)/3$, since $n \geq 3h = 12$, a contradiction. Thus

$$K_0 = H.$$

Put $\rho = \max\{|H| - |T_i| : i \in P\}$. Since $|T_i + S_0| < h$ for every $i \in W$, Proposition 2.11 yields

$$|T + S| \geq \sum_{i \in P} |E_i| + \sum_{i \in W} |T_i^* + S_0| \geq |P|\,|H| + \sum_{i \in W} |T_i| + |W|\frac{|S_0|}{2} \tag{3.6}$$

$$\geq |T| + \rho + |W|\frac{|S_0|}{2}. \tag{3.7}$$

Since $u = 1$, $\phi(S_1)$ generates G/H. By a suitable translation of T, we may assume the following:

1. $0 \in T_0$, and $|T_0| \geq \max\{|T_1|, \ldots, |T_t|\}$.
2. $\phi(T_i + S_1) = \phi(T_{i+1})$ for all $0 \leq i \leq t - 1$.

Suppose that $|W| \leq 2$. By (3.6) and (3.2) we have

$$|T + S| \geq |P|h + \sum_{i \in W} |T_i + S_0| \geq (q - |W|)h + |W|\frac{h + \mu}{2}$$

$$\geq (q - 2)h + 2\frac{h + \mu}{2} \geq \frac{2n}{3} + \mu.$$

Hence $q = 3$, $\mu = 0$ and $|S_0| = h/2$. It follows that $|S_1| = h/2$. Also we have $|E_i| = |T_i + S_0| = |S_0|$ for all $i \in W$. It follows that $T_i^* + S_0 = S_0$ for all $i \in W$. Hence $|T_i| = 1$ for all $i \in W$, since $T + S$ is aperiodic. Since $q = 3$ and $|T| \geq 4$, we have $|T_0| \geq 2$. Thus $P = \{0\}$. Therefore $|T_0 + S_1| = |E_1| = |S_0| = |S_1|$ and S_1 is periodic. Now $T + S \supset E_0 \cup (T_0 + S_1) \cup (T_1 + S_1)$, which is a periodic subset of cardinality $2n/3$, a contradiction, proving that

$$|W| \geq 3.$$

Suppose that $q \neq 3$. We must have $|P| = 0$, since otherwise there are $p \in P$ and $s \in W$ with $T_p + S_1 \subset E_s$. But $h > |E_s| \geq |T_p + S_1|$. By Lemma 2.1, $|T_p| + |S_1| \leq h$, and hence $\rho \geq |S_1|$. By (3.7), $|T + S| \geq |T| + |S_1| + 3|S_0|/2 > |T| + |S|$, a contradiction.

By (3.7), $q = |W| = 4$. Since $|T + S_0| \leq |T + S| \leq |T| + 2|S_0|$, by Proposition 2.12 we have $|S_0| = 2$ and $|T + S_1| = |T| + 4$. Therefore $T + S_1 =$

$T+S=T+S_0$. Thus S_0 and S_1 are aperiodic. Since $2 \geq |S_0| \geq h/2$, we have $3 \leq h \leq 4$. Since $|H| \leq 4$, it follows that $S_0 = S_1 + e$ for some e. Now $T+S = T+S_0 = T+S_1+e = T+S+e$, a contradiction. Therefore

$$q = 3.$$

We have $n/3 = h \leq |S+H|-|H| = \kappa_2|S| \leq |S|-\mu \leq n/3-5\mu/6$. Hence

$$\mu = 0 \quad \text{and} \quad |S| = |T| = h = n/3.$$

The next step is to show that $n = 12$. Since $7 \leq 2n/3$, we have $n \geq 12$. Suppose that $n > 12$ and hence $h \geq 5$. Put $L_i = \langle T_i^* \rangle$ for $0 \leq i \leq 2$.

Assume first that there is a j with $L_j = H$. By Theorem 2.9 and since $h = |T^S|$, the set $T_j = (w+H) \cap T$ (for some w) is a 2-fragment. In particular $|T_j^* + S| = |T_j^*| + |S|$.

Since S is aperiodic and by Proposition 2.12 applied with $Y = T_j^*$, S_0 and S_1 are progressions with the same difference. It follows, since $|S_0| \geq h/2 > 2$, that

$$|T+S| \geq |T+S_0| = \sum_{i \leq 3} |T_i + S_0| \geq |T| + 3|S_0| - 3 \geq |T| + 2|S_0|,$$

and hence $|S_0| = |S_1| = 3$. Since S_0, S_1 are progressions with the same difference and the same cardinality, we have $S_1 = S_0 + b$ for some $b \neq 0$. Also $|T+S_1| \geq |T| + 3|S_1| - 3 = |T+S|$. Now we have $T+S = T+S_1 = T+S_0+b = T+S+b$, a contradiction.

So we may assume that $L_j \neq H$ for all j. Since S_0 generates H, we have

$$2|T| \geq |T+S| \geq |T+S_0| = \sum_{0 \leq i \leq 2} |T_i + S_0| \geq \sum_{0 \leq i \leq 2} 2|T_i| = 2|T|. \tag{3.8}$$

Hence all the above inequalities are in fact equalities. In particular, $2|T_0| = |T_0 + S_0| < h$, since $0 \in W$. We also have $T+S = T+S_0$.

Take an L_i-decomposition $S_0 = S_{i0} \cup S_{i1}$. Without loss of generality we may assume $0 \in S_{i0}$ and $|S_{i0}| \geq |S_{i1}|$. From the above inequalities, we have $T_i + S_{i0} = T_i$. Since $|S_{i0}| \geq |S_0|/2 \geq h/4$ and $|T_i + S_0| = 2|T_i|$, we see that T_i is a single coset with cardinality in $\{h/4, h/3\}$. Since $|T_0| + |T_1| + |T_2| = h$, we have necessarily $|T_0| = |T_1| = |T_2| = h/3$. At least two of the subgroups T_0, T_1^*, T_2^* have a nonzero intersection (otherwise $h^3 \leq 27h$ and we get a contradiction), say $|T_0 \cap T_1^*| \geq 2$ (the other cases being similar).

Observe that $|S_0| \leq 2h/3 - 1$, otherwise $S_0 + T_0 = S_0$, and hence $T+S = T+S_0$ would be periodic, a contradiction. In particular, $|S_1| > h/3$.

Now $T+S \supset (T_0+S_0) \cup (T_0+S_1) \cup (T_1+S_1)$, which is a periodic subset of cardinality $2h = |S+T|$, a contradiction. So

$$n = 12.$$

Thus $|T_0| = |T_1| + 1 = |T_2| + 1 = 2$. Clearly $T+S \supset (T_0+S_0) \cup (T_0+S_1) \cup (T_1+S_1) \cup (T_2+S_0)$. Since $|S+T| = 8$, we necessarily have

$T_1 + S_1 = T_2 + S_0$. Thus $S_1 = S_0 + z$, where $\{z\} = T_2 - T_1$. So we may write $S = S_0 + \{0, z\}$. Since $T + \{0, z\}$ involves three H-cosets and since $P = \emptyset$, we have $|T + S| = |T + \{0, z\} + S_0| \geq |T + \{0, z\}| + 3$, forcing that $|T + \{0, z\}| = |T| + 1$. Hence $\kappa_2(T^*) \leq |T| - 1$ (observe that T^* generates G). We must have $\kappa_2(T^*) = 3 = |T| - 1$, otherwise T would be periodic by Proposition 2.11.

Case 2: $\phi(T) \neq G/H$, i.e. $t + 1 < q$.

Claim 1. *If $u \geq 2$, then $|P \cap [0, t]| \geq 2$.*

Suppose that $u \geq 2$ and there is a $j \in [0, t]$ such that $P \cap [0, t] \subset \{j\}$ and put $\delta = \max\{|E_i| : t + 1 \leq i \leq k\}$.

For all $i \neq j$, we have $|T_i| \leq h/3$, since otherwise by (3.2) and Lemma 2.1, $|S_0 + T_i| = h$, a contradiction. We have

$$|S| + |T| \geq |S + T| \geq \sum_{i \in [0,t] \setminus \{j\}} |T_i + S_0| + |T_j + S_0| + \sum_{i \in [t+1,k]} |E_i| \geq 2|T| - |T_j| + \delta + (k - t - 1)|S_u|. \tag{3.9}$$

Assume $|T_j| > |S_u|$. By Lemma 2.1, $|S_i + T_j| = h$ for all $0 \leq i \leq u$. Since $P \cap [0, t] \subset \{j\}$, $\delta = h$ and $k \geq t + 2$. By (3.9), we have $|S| + |T| \geq |S + T| \geq 2|T| - |T_j| + h + |S_u| > 2|T|$, a contradiction, proving that

$$|T_j| \leq |S_u|.$$

Therefore and by (3.9), we have $|S| + |T| \geq |S + T| \geq 2|T| - |T_j| + |S_u|$. It follows that this is a chain of equalities and hence $T_j + S_0 = T_j$ and therefore $|T_j| = h = |S_u|$. In particular, S is periodic, a contradiction.

Take a 2-subset $R \subset [0, t] \cap P$. Put $\gamma = \min\{|E_i| : t < i < k\}$. Then

$$|S + T| \geq \sum_{i \in R} |E_i| + \sum_{i \in [0,t] \setminus R} |T_i + S_0| + \sum_{i \in [t+1,k-1]} |E_i| + |E_k| \geq 2h + (t - 1)|S_0| + (k - t - 1)\gamma + |S_u|. \tag{3.10}$$

Claim 2. $q \geq u + t + 1$.

Suppose the contrary. Then $u \geq 2$. By Lemma 2.1, $\phi(T + (S \setminus S_u)) = G/H$. Hence $k + 1 = q$ and $|E_i| \geq |S_{u-1}|$ for all $t + 1 \leq i \leq k$. By (3.2) and (3.3),

$$\begin{aligned} |S + T| &\geq 2h + (t - 1)|S_0| + (q - t - 1)|S_{u-1}| \\ &= 2h + (2t - q)|S_0| + (q - t - 1)(|S_0| + |S_{u-1}|) \\ &\geq 2h + (2t - q)\frac{2h}{3} + \frac{4h(q - t - 1)}{3} = \frac{2n + 2h}{3}, \end{aligned}$$

because $q \leq t + u \leq 2t$, a contradiction.

Claim 3. $|\phi(S + T)| = |\phi(S)| + |\phi(T)| - 1$.

Put $\beta = 1$ if $k > r + t$ and $\beta = 0$ otherwise. We have

$$
\begin{aligned}
(3.11)\quad |S| + |T| \geq |S + T| &= \sum_{0 \leq i \leq k} |E_i| \\
&\geq \sum_{i \in [0,t] \setminus J} |T_i + S_0| + \sum_{i \in J} |T_i + S_{n_i}| + \sum_{i \in J} |T_i + S_0| + \beta |E_k| \\
&\geq |T| + r|S_0| + \beta |S_{u-1}|.
\end{aligned}
$$

By Claim 2 and Proposition 2.17, $r \geq u$. Suppose that $u < r$. By (3.11), $|S| = (u+1)|S_0|$. We also have $T_i + S_0 = T_i$, and hence $|T_i| = h$, for all $i \in [0,t] \setminus J$. Also $T_i + S_{n_i} = T_i$ for all $i \in J$.

Since T is aperiodic, by (3.2) we have $h/2 \leq |S_0| = |S_u| \leq h/2$ and $u = 1$. Take $l \in J$. It follows that $T_l + S_1 = T_l$ and $S_0 = S_0 + T_l = S_0 + T_l + S_1$, a contradiction since a generating set of size $< h$ cannot have a period of size $h/2$. So $r = u$. Let us show that $k = t + u$. Suppose the contrary. By (3.5), $|E_k| \geq |S_{u-1}|$ and $u \geq 2$. By (3.11), $|S| = u|S_0| + |S_{u-1}|$. By (3.2), $2h/3 \leq |S_0| = |S_u|$. In particular $|K_i| = h$ for all i. By (3.11), we also have $T_i + S_0 = T_i$, and hence $|T_i| = h$, for all $i \in [0,t] \setminus J$, $T_i + S_{n_i} = T_i$ and hence $|T_i| = h$, for all $i \in J$, a contradiction since T is aperiodic. Thus $k = t + u$.

Claim 4. *If $u \geq 2$, then $k \leq q - 3$.*

Since $|\phi(T + S)| = k + 1 = t + 1 + u$, by Lemma 2.14 we have $|\phi(T + (S \setminus S_u)| \geq t + u$, and hence $\gamma \geq |S_{u-1}|$.

Suppose that $t + u = k \geq q - 2$. Then $2t + 1 \geq t + 1 + u = k + 1 \geq q - 1$. By (3.10), (3.2) and (3.3) we have

$$
\begin{aligned}
|S+T| &= \sum_{i \in R} |E_i| + \sum_{i \in [0,t] \setminus R} |E_i| + \sum_{i \in [t+1, k-1]} |E_i| + |E_k| \\
&\geq 2h + (t-1)|S_0| + (k-t-1)|S_{u-1}| + |S_u| \\
&= 2h + |S_0| + |S_u| + |S_{u-1}| + (2t-k)|S_0| + (k-t-2)(|S_{u-1}| + |S_0|) \\
&\geq 4h + \mu + (2t-k)|S_0| + (k-t-2)\frac{4h}{3} \\
&= \frac{2h(k+2)}{3} + \mu \geq \mu + \frac{2n}{3},
\end{aligned}
$$

because $k = t + u \leq 2t$. It follows that $\mu = 0$ and that the last chain consists of equalities. In particular $|S_0| + |S_{u-1}| = 4h/3$ and $|S_0| + |S_{u-1}| + |S_u| = 2h$. Hence $|S_0| = |S_{u-1}| = |S_u| = 2h/3$. It also follows that $|E_i| = 2h/3$ for all $i \in [0,k] \setminus R$. Hence for all i, $|T_i| \leq h/3$, since otherwise by Lemma 2.1, $|S_0 + T_i| = |S_1 + T_i| = |S_2 + T_i| = h$, a contradiction. Thus

$$
|S| + |T| \geq |S + T| \geq \sum_{i \in [0,t]} |T_i + S_0| + |E_k| \geq 2|T| + |S_u|,
$$

a contradiction.

Assume that $u \geq 2$. By Claim 4, $q-2 \geq |\phi(S+T)|$, and hence by Claim 3, $\phi(S)$ is not a Vosper subset. By Corollary 2.16, $\phi(S)$ is a progression for $u \geq 2$. But $\phi(S)$ is obviously a progression for $u = 1$.

By Claim 3, $\phi(T)$ is a progression with the same difference as $\phi(S)$ if $t+1+u = |\phi(S+T)| \leq q-1$. Assume that $q = t+1+u$. By Claim 4, $u = 1$ and $|\phi(T)| = q-1$. Thus $\phi(T)$ is a progression with arbitrary difference. ∎

4. The $2n/3$-theorem. We start with a lemma converting modular structure into subset structure.

LEMMA 4.1. *Let $\mu \in \{0,1\}$. Let S be a generating subset of an abelian group G with $0 \in S$ and let H be a subgroup such that $|S+H|-|H| \leq |S|-\mu$. Let $\phi : G \to G/H$ denote the canonical morphism. Let T be a finite subset of G such that $3-\mu \leq |S| \leq \max(4-2\mu, |S|) \leq |T|$, $S+T$ is aperiodic and $|S|+|T|-\mu = |S+T| \leq |G|-4+2\mu$. If $\phi(S)$ and $\phi(T)$ are progressions with the same difference and $|\phi(G)| \geq |\phi(S)|+|\phi(T)|-1$, then there are H-progressions $S = \bigcup_{0\leq i\leq u} S_i$ and $T = \bigcup_{0\leq i\leq t} T_i$ with the same difference such that one of the following conditions holds:*

(i) *$\mu = 0$ and $\{S,T\}$ is an H-essential pair.*
(ii) *One of the sets $S \setminus S_u$ and $T \setminus T_t$ is H-periodic and the other is $(H,-\nu)$-periodic. Moreover $|T_t+S_u| = |T_t|+|S_u|-\nu-\mu$, where $0 \leq \nu \leq 1-\mu$.*

If G is finite, then $|\phi(T^S)|+|\phi(S)| \leq |\phi(G)|+1$. Moreover if $|T^S-S| \leq |T^S|+|S|-1$, then $\phi(R)$ and $\phi(S)$ are progressions with the same difference for every subset $R \subset T^S$ with $|R| \geq |T^S|-1$.

Proof. Take H-progressions $S = \bigcup_{0\leq i\leq u} S_i$ and $T = \bigcup_{0\leq i\leq t} T_i$ with the same difference d_0. Set $K_i = \langle S_i^* \rangle$ for $0 \leq i \leq u$. By a suitable translation and choice of d_0, we may assume that $0 \in S_0$, $|S_0| \geq |S_u|$ and that $|K_0| \geq |K_u|$ if $|S_0| = |S_u|$. For $U \subset [0,u]$, we have $|U|\,|H| - \sum_{i\in U} |S_i| \leq |S+H|-|S| \leq |H|-\mu$. Thus

$$\sum_{i\in U} |S_i| \geq (|U|-1)|H|+\mu. \tag{4.1}$$

Take an H-decomposition $S+T = \bigcup_{0\leq i\leq k} E_i$ such that

(1) $T_i + S_0 \subset E_i$ for all $0 \leq i \leq t$,
(2) $T_t + S_i \subset E_{t+i}$ for all $1 \leq i \leq u$.

Set $P = \{i : |E_i| = |H|\}$ and $W = [0,t] \setminus P$. Put $h = |H|$ and $n = |G| = qh$.

CASE 1: $K_0 \neq H$. By (4.1), we have $\mu = 0$, $|K_0| = |K_u| = h/2$ and

$$|S_i| = h \quad \text{for all } i \in [1, u-1]. \tag{4.2}$$

Since S is aperiodic, we have $K_0 \cap K_u = \{0\}$, and hence $h \in \{2,4\}$.

SUBCASE 1.1: $h = 2$. We have $|E_i| \geq \max\{|S_1|, \dots, |S_{u-1}|\} = h$ for all $1 \leq i \leq t+u-1$. Hence

$$\begin{aligned}|T| + |S| &= |T_0 + S_0| + (t+u-1)h + |T_t + S_u| \\ &= |S| + |T_0| + (t-1)h + |T_t|.\end{aligned}$$

Up to replacing d_0 by $-d_0$, we may assume that $|T_0| \geq |T_t|$. Since T is aperiodic we must have $|T_t| = 1$. If $|T_0| = 1$, then $\{S, T\}$ is an H-essential pair. If $|T_0| = 2$, then (ii) holds with $\nu = 1$.

SUBCASE 1.2: $h = 4$. Since S is aperiodic, we have $K_0 \cap K_u = \{0\}$, and hence $H = K_0 \oplus K_u$. It follows that $|S_i| = h$ for all $i \in [1, u-1]$. One may check as in Subcase 1.1 that $|T_i| = h$ for all $i \in [1, t-1]$, $T_0^* = K_0$ and $T_t^* = K_1$. Thus $\{S, T\}$ is an H-essential pair (a Klein pair).

CASE 2: S_0 generates H. Observe that $|T+S| \geq |T+S_0| + \sum_{1 \leq i \leq u} |E_{t+i}| \geq |T+S_0| + |S| - |S_0|$. Therefore $|T+S_0| \leq |T| + |S_0|$. Assume that $|W| \geq 2$. By Proposition 2.12, $\mu = 0$, $|T+S_0| = |T| + |S_0|$, $|S_0| = 2$, $|W| = 2$ and $|T_i| = h$ for all $i \notin W$. Moreover T_i is a progression with the same difference as S_0 for every $i \in W$. Observe that for every $i \in W \setminus \{0\}$, we have $i-1 \in W$, otherwise $|H| = |T_{i-1}|$ and $|H| = |T_{i-1} + S_1| \leq |E_i|$, a contradiction. So $W = \{0, 1\}$. We must have $t = 1$, otherwise $|E_i| \geq \min(|T_i|, |T_t|) = h$ for all $i \geq 2$. It follows that $|S+T| \geq (t+u-1)h + |T_0+S_0| + |T_1+S_0| \geq |T| + 2 + uh$ and hence $|S_u| = h$, a contradiction. Since T_0 and T_1 are progressions with the same difference as S_0, we have

$$\begin{aligned}|S+T| &\geq |T_0+S_0| + |T_1+S_0| + |T_1+S_1| \\ &\geq |T_0| + |S_0| - 1 + |T_1| + |S_0| - 1 + |S_1| + |T_1| - 1 \\ &\geq |T| + |S| + |T_1| - 1.\end{aligned}$$

Therefore $|T_1| = 1$. Since $|S_0| \geq h/2$, we have $3 \leq h \leq 4$. Since $|T_0 + S_0| < h$, we have $|T_0| \leq 2$. Therefore $|T| \leq 3$, a contradiction. Thus $|W| \leq 1$.

Take an $r \in [0, t]$ such that $W \subset \{r\}$. We have

$$\begin{aligned}|S| + |T| &= |E_r| + \sum_{i \in [0,t] \setminus \{r\}} |E_i| + \sum_{1 \leq i \leq u} |E_{t+i}| \\ &\geq |T_r + S_0| + th + \sum_{1 \leq i \leq u} |S_i + T_t| \geq |S_0| + th + \sum_{1 \leq i \leq u} |S_i|.\end{aligned}$$

Hence for some $\epsilon \geq 0$, we have

$$|T + H| - |H| \geq |T| + \epsilon. \tag{4.3}$$

SUBCASE 2.1: $\epsilon = 0$. Then the last chain consists of equalities. In particular $E_r = S_0 + T_r^* = S_0$ and $|E_{t+i}| = |S_i + T_t| = |S_i|$ for all $1 \leq i \leq u$. Let us show that

$$S_0 + T_t^* = S_0. \tag{4.4}$$

Assuming the contrary, we have necessarily $r \neq t$ and $|S_0| < h$. Since S_0 generates H, the period of S_0 has order $< h/2$. In particular $|T_r| < h/2$. By (4.3), $|T_t| > h/2$, and hence $K_t = H$. Since $S_u + T_t = S_u$, we have $|S_0| \geq |S_u| = h$, a contradiction.

It follows that $S + T_t = S$ and hence $|T_t| = 1$. By (4.3), $|T_i| \geq h - 1$, and hence $|E_i| \geq |T_i + S_0| \geq h$ for $i \neq t$. Thus $r = t$ if $W \neq \emptyset$.

Assume first that $W \neq \emptyset$. Thus $W = \{t\}$. We must have $|S_1| = 1$, otherwise $|E_t| \geq |S_1 + T_{t-1}| \geq h$ by Lemma 2.1, a contradiction. We have $u = 1$, otherwise $|S_0| + |S_1| + |S_u| \geq 2h$. Thus $|S_0| + |S_1| \geq 2|H| - 1$. Since $|S_0| \geq |S_u|$, we have $|S_0| = |H|$ and hence $|E_t| = h$, a contradiction. Hence $\{S, T\}$ is an essential pair.

Assume now that $W = \emptyset$. We must have $|S_u| = 1$, otherwise $|E_i| \geq h$ for all $0 \leq i \leq t + u - 1$ and hence $|S + T| \geq (t + u)h + |S_u| > |S| + |T|$, since $\epsilon = \mu = 0$. We must have $|T_{t-1}| = h - 1$, otherwise $|E_i| \geq h$ for all $t + 1 \leq i \leq t + u - 1$ and hence $|S + T| \geq (t + u)h + |S_u| > |S| + |T|$, since $\epsilon = \mu = 0$. Similarly $|S_{u-1}| = h - 1$. Since $\epsilon = \mu = 0$, we have $|S_i| = h$ for all $0 \leq i \leq u - 2$, and $|T_i| = h$ for all $0 \leq i \leq t - 2$. Therefore $\{S, T\}$ is an essential pair.

Subcase 2.2: $\epsilon \geq 1$. By (4.3) for all $v < w$,

$$|T_v| + |T_w| \geq |H| + \epsilon \geq |H| + 1. \tag{4.5}$$

Take $1 \leq r \leq u - 1$. Clearly $E_{t+r} \supset (T_t + S_r) \cup (T_{t-1} + S_{r+1})$. By (4.1) and (4.5), we have $|T_t| + |S_r| + |T_{t-1}| + |S_{r-1}| \geq 2h + 1$. Then either $|T_t| + |S_r| > h$ or $|T_{t-1}| + |S_{r+1}| > h$. By Lemma 2.1, $|E_{t+r}| = h$. Therefore $[0, t + u - 1] \subset P$.

Put $\nu = (u + t)h - |S \setminus S_u| - |T \setminus T_t|$. We now have

$$\begin{aligned} |S| + |T| - \mu = |S + T| &= \sum_{0 \leq i \leq t+u} |E_i| + |T_t + S_u| \\ &= (t + u)h + |T_t + S_u| = |S \setminus S_u| + |T \setminus T_t| + \nu + |S_t + T_u|. \end{aligned}$$

Therefore $|T_t + S_u| = |T_t| + |S_u| - \mu - \nu$. Since $[0, t + u - 1] \subset P$, $S_t + T_u$ is aperiodic. By Kneser's Theorem $\mu + \nu \leq 1$.

Suppose now that G is finite. Since $T + S$ involves full cosets except for the extremities, $\phi(T^S)$ is a progression with the same difference as $\phi(S)$. By Lemma 4.1, $S \setminus S_u$ and $T \setminus T_t$ are $(\mu - 1)$-periodic.

Assume that $|\phi(T^S)| + |\phi(S)| \geq q + 2$. Clearly there is a v such that $S \setminus (S_u \cup S_v)$ is periodic and $|S_v| \geq |H| - 2$. Thus $|\phi(T^S)| + |\phi(S \setminus (S_u \cup S_v))| \geq q - 1$. Thus $|G| - |T| \geq |T^S - S| \geq |T^S - (S \setminus (S_u \cup S_v))| + |S_v| \geq (q - 1)|H| + |H| - 2 = |G| - 2$, a contradiction. Suppose that $|T^S - S| \leq |T^S| + |S| - 1$. It follows that $\kappa_2(S) \leq |S| - 1$ and hence $|H + S| - |S| < |H|$. Therefore $\{S, T\}$

is not an elementary pair. Thus (ii) holds. In particular $(S+T)\setminus(S_u+T_u)$ is periodic. Hence $\phi(R)$ is a progression with the same difference as $\phi(S)$. ∎

Proof of Theorem 1.1. Suppose that (i) does not hold. By Theorem 3.1, $\phi(S), \phi(T)$ are progressions with the same difference and $|\phi(S+T)| = |\phi(S)| + |\phi(T)| - 1$. Take H-progressions $S = \bigcup_{0\le i\le u} S_i$ and $T = \bigcup_{0\le i\le t} T_i$ with the same difference. Since S is degenerate, $|G| > 2|H|$ and hence $|G| \ge 6$. Therefore $|S+T| \le (2|G|+2)/3 < |G| - 1$, and thus $u|H| = |H+S| - |H| = \kappa_2(S) \le |S| - \mu$. By Lemma 4.1, (ii) or (iii) holds. ∎

5. The nondegenerate case

5.1. Some lemmas. Suppose that $0 \in S$ and $G = \langle S\rangle$. Then clearly $1 \le \kappa_1(S) \le \cdots \le \kappa_k(S)$. If $\kappa_k(S) = \kappa_{k-1}(S)$, then every k-fragment is a $(k-1)$-fragment. Also every $(k-1)$-fragment F with $k \le |F|$ and $k \le |F^S|$ is a k-fragment.

The above trivial observation will be used extensively in this section.

Our strategy consists in replacing a set with its 3-atom or 4-atom. We need to show that nondegeneracy is preserved by this operation.

LEMMA 5.1. *Let S be a finite generating nondegenerate subset of an abelian group G such that $0 \in S$ and $\kappa_2(S) = |S| \le (|G|-4)/2$. Let F be a 2-fragment of S with $0 \in F$, $|F| \ge 3$ and $|F^S| \ge 4$. Then*

(i) *A proper 2-fragment of S contains no nonzero coset.*
(ii) *$F+S$ is aperiodic and F generates G.*
(iii) *Assume that $|F| \le 4$ and that $|F| + |S| > 6$. Then F is nondegenerate.*
(iv) *If A is a 3-atom of S with $|A| \ge 4$, then $|A| = 4$ and $\kappa_2(A) = |A|$.*

Proof. Suppose that (i) is false and take a minimal proper 2-fragment X containing a nonzero subgroup Q. Take a $y \in Q$. We have $|(X+y)\cap X| \ge |Q| \ge 2$. By Theorem 2.9, $(X+y)\cap X$ is a 2-fragment (clearly a proper one). By the minimality of X, we have $X = X + y$. Therefore $X + Q = X$. Since X is not a subgroup, there is an x with $x + X \ne X$. Observe that $X \cap (x+X)$ is Q-periodic. We have $|(X+x)\cap X| \ge |Q+x| \ge 2$. By Theorem 2.9, $(X+x)\cap X$ is a 2-fragment. By the minimality of X, we have $(X+x)\cap X = X$, and hence $X + x = X$, a contradiction. This proves (i).

Let us show that $F+S$ is aperiodic. Suppose that $F+S+Q = F+S$ for some nonzero subgroup Q. By the definition of κ_2, we have

$$|F| + |S| = |F+Q+S| \ge |F+Q| + \kappa_2(S) = |F+Q| + |S|.$$

It follows that $F = F + Q$ is periodic. By (i), $|F| > |F^S|$. By Lemma 2.8, $-F^S = G \setminus (F+S)$ is a proper periodic 2-fragment, a contradiction.

Put $N = \langle F\rangle$ and $s|N| = |S+N|$. Assume that $s > 1$. By Proposition 2.12(iv), $|G|/2 > |S| \geq (s-1)|N|$. It follows that $S + N \neq G$ and that $|N+S| - |N| \leq |S| = \kappa_2(S)$. Thus N is a 2-fragment of S, a contradiction.

Suppose that (iii) is false. Since $|G| \geq |F| + |S| + 4 \geq 11$ and $|G|$ is composite, we have $|F+S| \leq (|G|-4)/2 + 4 \leq 2|G|/3$.

By Theorem 1.1, $|S+H| - |H| \leq |S|$. Thus H is a 2-fragment of S, a contradiction.

Clearly, we may assume that $0 \in A$. By (ii), A is aperiodic and generates G. Since $|A+S| \leq |A| + |S|$, we have $\kappa_2(A) \leq |A|$. Let H be a 2-atom of A.

Suppose that $|A| \geq 5$. Assume first that $|H| > 2$ and take a 3-subset $\{0, z, z'\}$ of H. By Theorem 2.10, $|A \cap (A+x)| \leq 2$ for every $x \neq 0$. Thus

$$\begin{aligned}\kappa_2(A) + |A| &\geq |H| + |A| \geq 2 + \kappa_2(A)\\ &= |A + \{0, z, z'\}| \geq |A| + |A| - 2 + |A| - 4 = 3|A| - 6,\end{aligned}$$

and hence

$$2|A| \leq \kappa_2(A) + 6.$$

Suppose that $\kappa_2(A) \leq |A| - 1$. By Proposition 2.11, $|H| \leq \kappa_2(A) \leq |A| - 1 \leq 4$. By Theorem 2.13, H is a subgroup. Take an H-decomposition $A = \bigcup_{0\leq i\leq t} A_i$. Since $|H| \leq 4$ and by (i), $|A_i| \leq 2$ for every i. Hence $u \geq 2$ and thus $6 \leq u|H| = \kappa_2(A)$, a contradiction, proving that $\kappa_2(A) = |A|$. It follows that S is a 2-fragment of A. Since S is nondegenerate, there is an r such that $\{0, r\}$ is a 2-atom of S. Take a minimal 2-fragment $R \subset S$ of A such that $|\{0,r\}+R| = |R|+2$ and $|R| \geq 3$ (note that S is such a fragment). Clearly $|R \cup (r+R)| \leq |G| - 2$. By Theorem 2.9, $R \cap (r+R)$ is a 2-fragment of A such that $|R \cap (r+R)| = |R| - 2$. It follows that $|R| \leq 4$. Thus $|A| > |R|$, a contradiction proving that $|A| \leq 4$.

Thus $|H| = 2$, say $H = \{0, z\}$ for some z. Since A is aperiodic, by Theorem 2.10 we have $|A \cap (A+z)| \leq 2$. Hence

$$2 + |A| \geq 2 + \kappa_2(A) = |A + \{0, z\}| \geq |A| + |A| - 2 = 2|A| - 2,$$

and so $|A| \leq 4$, a contradiction.

By (iii), A is nondegenerate. Assume that $\kappa_2(A) \leq |A| - 1$. There is an r such that A is an r-progression by Proposition 2.15, and hence $|A \cap (A+r)| = 3$, contradicting Theorem 2.10. ∎

We recall that the arcs of Cayley graphs defined on a group G by a subset S are usually colored by the elements of $S \setminus \{0\}$. It will be helpful to have this image in mind. However we assume no knowledge of Cayley graphs.

Put $E = \{(x, y) \in A \times A : x - y \in S \setminus \{0\}\}$. The family $\{x - y : x - y \in S \setminus \{0\}\}$ will be called the *family of colors* present in A.

LEMMA 5.2. *Let S be a finite subset of an abelian group G such that $0 \in S$ and $\kappa_3(S) = |S|$. Let F be a k-fragment with $|F| \geq k+1$ and let $a \in F+S$ be such that $|(a-S)\cap F| = 1$, say $(a-S)\cap F = \{b\}$. Then $F \setminus \{b\}$ is a k-fragment.*

Let A be a k-atom of S with $0 \in A$ and $|A| \geq k+1$. Put $S^* = S \setminus \{0\}$ and $E = \{(x,y) \in A \times A : x - y \in S^*\}$. Then

(1) *For every $x \in A+S$, $|(x-S)\cap A| \geq 2$.*
(2) $|A| \leq |E| = \sum_{x\in A} |(x-S^*)\cap A| \leq (|S|-1)|A| - 2\kappa_k(S)$.
(3) *There is a nonempty subset $R \subset E$ such that $\sum_{(x,y)\in R}(x-y) = 0$.*

Proof. We have $(F \setminus \{b\}) + S \subset ((F+S)\setminus\{a\}) \cup \{b\}$, and hence $F \setminus \{b\}$ is a k-fragment.

Bounding the total number of arcs inside A or reaching $\partial(A)$ from A by the number of arcs leaving A, we have, using (1),

$$|A|\,|S^*| \geq \sum_{a\in\partial(A)} |(a-S^*)\cap A| + \sum_{a\in A} |(a-S^*)\cap A| \geq 2\kappa_k(S) + |A|,$$

and (2) follows.

In the graph induced by A, every vertex receives an arc colored by an element of S^*, by (1). Since A is finite, A must contain a directed cycle, $R = \{(a_1,a_2),(a_2,a_3),\dots,(a_j,a_{j+1})\}$ with $a_{j+1} = a_1$. We have

$$\sum_{(x,y)\in R}(x-y) = \sum_{1\leq i\leq j}(a_{i+1}-a_i) = a_{j+1} - a_1 = 0. \ \blacksquare$$

Now we prove the optimality of the 4-atom of a subset of size 3.

LEMMA 5.3. *Let S be a finite generating nondegenerate subset of an abelian group G such that $0 \in S$, $|S| = 3$ and $\kappa_4(S) = \kappa_2(S) = |S|$. Let A be a 4-atom of S with $0 \in A$. Then A is nondegenerate and $|A| = 4$.*

Proof. We shall assume that $S = \{0,u,v\}$ is translated in order to maximize the order of $u-v$. Suppose to the contrary that $|A| \geq 5$. By Lemma 5.2(1), every element of $\partial(A)$ has the colors u and v. Thus $(\partial(A)+\{u,v\})\cap\partial(A) = \emptyset$. Also $\partial(A) \subset (A+u)\cap(A+v)$. By Theorem 2.9, $3 \geq |(A+u)\cap(A+v)| \geq |\partial(A)|$, and hence $\partial(A) = (A+u)\cap(A+v)$. By Theorem 2.9, $\partial(A)$ is a 2-fragment of S. It follows that $\partial(A)+u = \partial(A)+v = \partial(\partial(A))$. Thus $u-v$ has order 3. By considering $S-u$ and $S-v$ and the minimality of the order of $u-v$, we see that the orders of u and v are at most 3. Since S generates G, we have $|G| \leq 9$, contradicting the 4-separability of S. ∎

5.2. Proof of Theorem 1.2. The case $\kappa_2(S) \leq |S|-1$ follows by Proposition 2.15. So we may assume $\kappa_2(S) = |S|$, and hence $\mu = 0$.

CLAIM 1. *If $|S| = 4$, then S is a near-progression.*

Put $A_0 = S$. Let A_1 denote a 3-atom of S and let A_2 denote a 4-atom of A_1 such that $0 \in A_1 \cap A_2$. Suppose that $\min(|A_1|, |A_2|) \geq 4$. By Lemma 5.1, A_1 and A_2 are nondegenerate generating subsets with $|A_1| = |A_2| = 4$, and $\kappa_2(A_1) = \kappa_2(A_2) = 4$. It follows that A_0 is a 3-atom of A_1 (inducing a symmetry between A_0 and A_1). By Theorem 2.13, there is an r such that $\{0, r\}$ is a 2-atom of A_1 and hence $|A_1 + \{0, r\}| = |A_1| + 2$. Therefore there is a u such that $\{0, u\} + \{0, r\} \subset A_1 - a$ for some $a \in A_1$. By suitably translating A_1, we may assume that $u \neq -r$ (otherwise we replace A by $A + r$) and that $a = 0$. By the definition of κ_2, for every $x \in \{u, r\}$ we have $|A_2 + \{0, x\}| \geq |A_2| + 2$. We must have $x = r$, since otherwise A_0 contains two r-arcs and two u-arcs. But the total number of arcs colored by elements of $A_1 \setminus \{0\}$ is 4, by Lemma 5.2. Thus the sequence $\{r, r, u, u\}$ represents the family of colors inside A_0. By Lemma 5.2, there is a nonempty subfamily R summing to 0. We have $|R| \neq 2$, since $2r \neq 0$ and $2u \neq 0$ by Lemma 5.1. We have $|R| \neq 4$, since otherwise $2(u + a) = 2u + 2a = 0$, and S would contain the coset $\{0, a + b\}$, contradicting Lemma 5.1. It follows that $|R| = 3$. Without loss of generality we may assume $R = \{r, r, u\}$. Therefore $2r + u = 0$. Thus $A = \{0, u, -2u, -u\}$, and hence $A' = \{0, u, 2u\}$ is a 3-atom of A, a contradiction. Thus

$$\{0, r, 2r\} \subset A_1.$$

Let us show that $|A_0 + \{0, r\}| = |A_0| + 2$. Assuming the contrary, we have $|A_0 + \{0, r\} + \{0, r\}| \leq |A_0 + \{0, r\}| + 1$. In particular $A_0 + A_1$ is the union of full r-cosets and an r-progression. Thus

$$|A_0 + A_1| + 1 \geq |A_0 + A_1 + \{0, r\}| = |A_0 + \{0, r\}| + |A_1| \geq |A_0| + |A_1| + 2,$$

a contradiction. Thus $\{0, v\} + \{0, r\} \subset A_0 - b$ for some $b \in A_0$ and some v. As for A_1, we see that we may take $b = 0$ and $v = r$. It follows that $(2r - A_0) \cap A_1 \supset \{0, r, 2r\}$. By Lemma 5.2(1)&(2),

$$5 \leq \sum_{x \in A_1} |(x - A_0^*) \cap A_1| \leq 3|A_1| - 2\kappa_2(A_0) = 4,$$

a contradiction. Thus there is an $i \in \{0, 1\}$ such that A_i has a 3-atom M with $|M| = 3$. Put $A_i = T$. By Lemma 5.1, M is nondegenerate and $\langle M^* \rangle = G$.

Note that M is not a near-progression, otherwise by successive applications of Lemma 2.4, we see that S is a near-progression and the Claim holds. By Proposition 2.15, $\kappa_2(T) \geq |T|$. It follows that T is a 2-fragment of M.

Clearly $\sum_{x \in T+M} |(x - M) \cap T| \leq |T|\,|M| = 12$. Thus there is a $c \in M + T$ such that $|(c - M) \cap T| = 1$. By Lemma 5.2, T contains a 2-fragment F of M with $|F| = 3$. Observe that F is not a progression, otherwise M would be a near-progression.

By Lemma 2.7, $M = F + z$ for some z. By translating M suitably, we may assume that $M \subset T$. Now $8 \leq |T + T| \leq |T + M| + 1 \leq 2|T| = 8$.

By Theorem 2.13, there is an r such that $\{0,r\}$ is a 2-atom of T and hence $|T+\{0,r\}| = |T|+2$. Therefore there is a u such that $\{0,u\}+\{0,r\} \subset T-a'$ for some $a' \in T$. Without loss of generality, we may assume that $a' = 0$ and $u \neq -r$ (otherwise we replace T by $T+u$).

Case 1: $u = r$. Put $T = \{0,r,2r,w\}$. We have $T+T = \{0,r,2r,3r,4r\} \cup \{w, w+r, w+2r\} \cup \{2w\}$. We cannot have $2w \in \{w, w+r, w+2r\}$. Thus $2w \in \{0,r,2r,3r,4r\}$. We cannot have $2w \in \{0,2r,4r\}$, otherwise T would contain a nonzero coset contradicting Lemma 5.1. Thus $2w \in \{r,3r\}$. If $2w = r$, then $T = \{0,w,2w,4w\}$ a contradiction. So we must have $2w = 3r$, and hence $T-r = \{-r,0,r,w-r\} = \{-2(w-r),0,2(w-r),w-r\}$. Therefore T is a $(w-r,-1)$-progression, a contradiction.

Case 2: $u \neq r$ and hence $T = R \cup \{0\}$, where $R = \{u,v,u+v\}$. One may see easily using Lemma 5.1 that $R \cap (-T) = \emptyset$. It follows that $|R \cap (R+R)| \geq 2$. Without loss of generality we may take $u \in R+R = (u+R) \cup (u+v+R) \cup (u+v+\{0,v\}) \cup \{2v\}$. Using Lemma 5.1, we see that T is a near-progression, a contradiction.

We shall now prove the theorem:

Assume first that $|S| \geq 4$ and let A be a 3-atom of S. If $|A| = 4$, then by Lemma 5.1, $\kappa_3(A) = |A|$. By Claim 1, A is a near-progression. By Lemma 2.4, S is a near-progression. Suppose that $|A| \neq 4$. By Lemma 5.1, $|A| = 3$. Clearly $|G| \geq |A+S|+4 \geq 12$. Let A' denote a 4-atom of A. By Lemmas 5.1 and 5.3, A' is nondegenerate and $|A'| = 4$. By Claim 1, A' is a near-progression. By Lemma 2.4 applied twice, A and S are near-progressions.

Assume $|S| = 3$. Let A' denote a 4-atom of S. By Lemmas 5.1 and 5.3, A' is nondegenerate and $|A'| = 4$. By Claim 1, A' is a near-progression. By Lemma 2.4, S is a near-progression. ∎

6. The $(n-4)$-modular theorem. We shall now describe the structure if $|S+T| \leq |G|-4$.

Let S be a finite subset of an abelian group G. A subgroup H is said to be a *super-atom* of S if either $H = \langle S^* \rangle$ or H is a hyper-atom of $\langle S^* \rangle$.

Theorem 6.1. *Let $\mu \in \{0,1\}$. Let S and T be finite subsets of an abelian group G generated by $S^* \cup T^*$. Also assume that $3-\mu \leq |S| \leq \max(4-2\mu, |S|) \leq |T|$, $S+T$ is aperiodic and $|S+T| = |S|+|T|-\mu \leq |G|-4+2\mu$. Then one of the following conditions holds:*

(i) *S and T are $(r,\mu-1)$-progressions for some r.*

(ii) *There is a subgroup H such that $|\phi(S+T)| = |\phi(S)|+|\phi(T)|-1$ and moreover $\phi(S)$ and $\phi(T)$ are progressions with the same difference if $\min\{|\phi(S)|, |\phi(T)|, |\phi(G)|-|\phi(S+T)|\} \geq 2$, where $\phi : G \to G/H$ is the canonical map. Moreover H is a super-atom of S or T^S if $|G| \neq 12$.*

Proof. Without loss of generality we may take $T = T^*$ and $S = S^*$. Assume first that S generates a proper subgroup K (not necessarily containing T) and let $T = \bigcup_{0\le i\le t} T_i$ be a K-decomposition. Put $W = \{i : |T_i + S| < |K|\}$.

By Proposition 2.12, $W = \{v\}$ for some v. Put $\nu = t|K| - |T \setminus T_v|$. We have

$$|T| + |S| - \mu = |T + S| = t|K| + |T_t + S| = |T \setminus T_t| + \nu + |T_t + S|.$$

Thus $|T_t + S| = |T_t| + |S| - \mu - \nu$. Since $T + S$ is aperiodic, $T_t + S$ is aperiodic. By Kneser's Theorem, $\mu + \nu \le 1$. Hence (ii) holds with $H = K$.

Assume now that S generates G. If S is a near-progression, the result holds by Lemma 2.4. So we may assume that S is not a near-progression. Put $X = T^S$ and $Y = (T^S)^{-S} = G \setminus (X - S)$. By Lemma 2.6, $X - S$ is aperiodic and there is $0 \le \zeta \le 1$ with $|X - S| = |X| + |S| - \zeta$.

Case 1: $|S| \le |T^S|$. We have

$$|S| \le \frac{|T| + |S|}{2} \le \frac{|T + S| + \mu}{2} \le \frac{|G| + \mu - 4}{2}.$$

By Theorem 1.2, S is degenerate. Let H be a hyper-atom of S and put $q|H| = |G|$.

Subcase 1.1: $|T| \le |T^S|$. Hence $|S| + |T| \le (2|G| + 2\mu)/3$. The result holds by Theorem 3.1 unless $|G| = 3|T| = 12 = 4\kappa_2(T)$. By Proposition 2.15, T is degenerate. The result holds by Theorem 3.1 with H denoting a hyper-atom of T.

Subcase 1.2: $|S| \le |T^S| < |T|$ and hence $|S| + |T^S| \le (2|G| + 2\mu)/3$. In particular $|G| > 12$, if $|S| = 4$. By Lemma 2.6, $X - S$ is aperiodic and $|X - S| = |X| + |S| - \zeta$. By Theorem 3.1, $\phi(S)$ and $\phi(X^{-S})$ are progressions with the same difference. By Lemma 4.1, $|\phi(S)| + |\phi(X^{-S})| \le q + 1$. The result holds if $T = X^S$. Suppose that $T \ne X^S$. By Lemma 2.6, $\zeta = 1$. Then $|T| = |X^{-S}| - 1$. By Lemma 4.1, $\phi(T), \phi(S)$ are progressions with the same difference.

Case 2: $|T^S| < |S|$. Assume first that X^* generates a proper subgroup Q and put $|G| = q'|Q|$. Take Q-decompositions $T = \bigcup_{0\le i\le t} T_i$ and $S = \bigcup_{0\le i\le u} S_i$. Since X is contained in a single coset, say $X \subset T_t + S_u$, the other Q-cosets are all contained in $T + S$. By Theorem 2.2, we have $t + u + 1 \le q'$. Hence $|T| + |S| - \mu = |T + S| \ge (t + u)|Q| + |T_t| + |S_u| - 1$. In this case (i) or (ii) holds.

Assume now that X generates G. Since $|X - S| \le |X| + |S|$, X cannot be a near-progression by Lemma 2.4. By Theorem 1.2, X is degenerate. Let N be a hyper-atom of X and let $\psi : G \to G/N$ be the canonical morphism. By Theorem 3.1, $\psi(S)$ and $\psi(X^{-S})$ are progressions with the same difference.

Also $|\psi(S)+\psi(X^{-S})| \le q'+1$. The result holds if $T = X^{-S}$. Suppose that $T \ne X^{-S}$. By Lemma 2.6, $\zeta = 1$. Then $|T| = |X^{-S}| - 1$. By Lemma 4.1, $\psi(T), \psi(S)$ are arithmetic progressions with the same difference. ∎

7. The $(n-3)$-structure theorem

THEOREM 7.1. *Let S and T be finite subsets of an abelian group G generated by $S^* \cup T^*$. Assume moreover that $3-\mu \le |S| \le |T|$, $S+T$ is aperiodic and $|S+T| = |S|+|T|-\mu \le |G|-3-\mu$, where $0 \le \mu \le 1$. Then one of the following conditions holds:*

(i) *$\mu = 0, |S| = 3$ and there is an a such that either $T = a+S$ or $T = G \setminus (-a-2S)$.*
(ii) *S and T are $(r, \mu-1)$-progressions for some r.*
(iii) *$\mu = 0$ and $\{S,T\}$ is an H-essential pair.*
(iv) *There exist a subgroup H and two H-decompositions $S = \bigcup_{0\le i\le u} S_i$ and $T = \bigcup_{0\le i\le t} T_i$ (H-progressions with the same difference if*

$$\min\{|\phi(S)|, |\phi(T)|, |\phi(G)| - |\phi(S+T)|\} \ge 2)$$

such that one of the sets $S \setminus S_u$, $T \setminus T_t$ is H-periodic and the other is $(H, -\nu)$-periodic, and $|T_t + S_u| = |T_t| + |S_u| - \nu - \mu$, where $0 \le \nu \le 1-\mu$. Moreover $|\phi(S+T)| = |\phi(S)| + |\phi(T)| - 1$, where $\phi : G \to G/H$ is the canonical map and H is a super-atom of S or of T^S if $|G| \ne 12$.

Proof. The result holds by Theorem 6.1 and Lemma 4.1 if $\mu = 1$. Assume that $\mu = 0$. The result holds by Theorem 6.1 and Lemma 4.1 if $|T| \ge 4$ and $|S+T| \le |G| - 4$. Assume first $|T| = 3$. By Lemma 2.7, either (ii) holds or $T = a+S$ for some a. Assume now that $|T| \ge 4$ and that $|T^S| = 3$. By Lemma 2.6, $|T^S - S| = |T^S| + |S| - \zeta$ for some $0 \le \zeta \le 1$.

Suppose that one of the sets T^S and S is an r-progression (and therefore the other is a near-r-progression). Thus $R - S$ is an r-progression and the result holds. Otherwise by Lemma 2.7, there is an a such that $R = -a - S$. Hence $T = G \setminus (R-S) = R = G \setminus (-a-2S)$. ∎

A partition $A = A_1 \cup A_0$ is said to be *quasi-H-periodic* if $A_0 + H = A_0$ and A_1 is contained in some H-coset.

COROLLARY 7.2 (Kemperman structure theorem [2]). *Let A and B be finite subsets of an abelian group G such that $|A+B| = |A|+|B|-1 \le |G|-2$ and $A+B$ is aperiodic. Then there are a subgroup H and quasi-H-periodic partitions $A = A_0 \cup A_1$ and $B = B_0 \cup B_1$ such that $|B_1+A_1| = |A_1|+|B_1|-1$. Moreover $|\phi(A+B)| = |\phi(A)|+|\phi(B)|-1$ and $|\phi(A_1+B_1-A)\cap\phi(B)| = 1$, where $\phi : G \to G/H$ is the canonical map.*

COROLLARY 7.3 (Grynkiewicz structure theorem [2]). *Let A and B be finite subsets of an abelian group G such that $|A+B| = |A|+|B| \leq |G|-3$, $A+B$ is aperiodic and $3 \leq |A| \leq |B|$. Then one of the following holds:*

(1) $|A| = 3$ *and there is an a such that either $B = a + A$ or $T = G \setminus (-a - 2A)$.*
(2) *There exist $a, b \in G$ such that $|(A \cup \{a\}) + (B \cup \{b\})| = |A \cup \{a\}| + |B \cup \{b\}| - 1$.*
(3) *There is a subgroup H and quasi-H-periodic partitions $A = A_0 \cup A_1$ and $B = B_0 \cup B_1$ such that $|B_1 + A_1| = |A_1| + |B_1| - 1$. Moreover $|\phi(A+B)| = |\phi(A)| + |\phi(B)| - 1$ and $|\phi(A_1 + B_1 - A) \cap \phi(B)| = 1$, where $\phi : G \to G/H$ is the canonical map.*
(4) *$\{A, B\}$ is a Klein pair.*

The result follows easily from Theorem 7.1 after two observations:

- Near-progressions and essential non-Klein pairs satisfy (1).
- If Theorem 7.1(iv) holds with $\nu = 1$, then (1) holds.

Without loss of generality we may take $\langle A^* \cup B^* \rangle = G$. Thus Theorem 7.1 implies the last two results and shows moreover that $\phi(A)$, $\phi(B)$ are progressions with the same difference if $\min\{|\phi(A)|, |\phi(B)|, |G|-|\phi(A+B)|\} \geq 2$. This information is crucial in order to obtain Lev's result [13] and Lev's type reconstructions for $|A+B| = |A|+|B|$. Another reconstruction follows directly from Theorem 7.1.

Acknowledgements. The author would like to thank an anonymous referee for helpful comments.

References

[1] E. Balandraud, *Une variante de la méthode isopérimétrique de Hamidoune, appliquée au théorème de Kneser*, Ann. Inst. Fourier (Grenoble) 58 (2008), 915–943.
[2] D. Grynkiewicz, *A step beyond Kemperman's structure theorem*, Mathematika 55 (2009), no. 1-2, 67–114.
[3] Y. O. Hamidoune, *On the connectivity of Cayley digraphs*, Eur. J. Combin. 5 (1984), 309–312.
[4] —, *Subsets with small sums in abelian groups I: The Vosper property*, ibid. 18 (1997), 541–556.
[5] —, *An isoperimetric method in additive theory*, J. Algebra 179 (1996), 622–630.
[6] —, *Some results in additive number theory I: The critical pair theory*, Acta Arith. 96 (2000), 97–119.
[7] —, *Some additive applications of the isoperimetric approach*, Ann. Inst. Fourier (Grenoble) 58 (2008), 2007–2036.
[8] —, *Hyper-atoms and the critical pair theory*, Combinatorica, to appear; arXiv:0805.3522v1.
[9] Y. O. Hamidoune and Ø. J. Rødseth, *An inverse theorem mod p*, Acta Arith. 92 (2000), 251–262.

[10] Y. O. Hamidoune, O. Serra and G. Zémor, *On the critical pair theory in Abelian groups: Beyond Chowla's Theorem*, Combinatorica 28 (2008), 441–467.
[11] J. H. B. Kemperman, *On small sumsets in Abelian groups*, Acta Math. 103 (1960), 66–88.
[12] M. Kneser, *Summenmengen in lokalkompakten abelschen Gruppen*, Math. Z. 66 (1956), 88–110.
[13] V. F. Lev, *Critical pairs in abelian groups and Kemperman's structure theorem*, Int. J. Number Theory 2 (2006), 379–396.
[14] E. Nazarewicz, M. O'Brien, M. O'Neill and C. Staples, *Equality in Pollard's theorem on set addition of congruence classes*, Acta Arith. 127 (2007), 1–15.
[15] P. Scherk and L. Moser, *Advanced Problems and Solutions: Solution 4466*, Amer. Math. Monthly 62 (1955), 46–47.
[16] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge Stud. Adv. Math. 105, Cambridge Univ. Press, 2006.
[17] G. Vosper, *The critical pairs of subsets of a group of prime order*, J. London Math. Soc. 31 (1956), 200–205.

Yahya Ould Hamidoune
E. Combinatoire
UPMC Univ. Paris 06
Case 189
4 Place Jussieu
75005 Paris, France
E-mail: hamidoune@math.jussieu.fr

Received on 17.11.2008
and in revised form on 1.11.2010 (5864)