Cauchy-Davenport theorem in group extensions

L'Enseignement Mathématique, t. 51 (2005), p. 239–254

CAUCHY-DAVENPORT THEOREM IN GROUP EXTENSIONS

by Gyula KÁROLYI *)

ABSTRACT. Let A and B be nonempty subsets of a finite group G in which the order of the smallest nonzero subgroup is not smaller than $d = |A| + |B| - 1$. Then at least d different elements of G have a representation in the form ab, where $a \in A$ and $b \in B$. This extends a classical theorem of Cauchy and Davenport to noncommutative groups. We also generalize Vosper's inverse theorem in the same spirit, giving a complete description of critical pairs A, B for which exactly d group elements can be written in the form ab. The proofs depend on the structure of group extensions.

1. INTRODUCTION

Let $G \neq 1$ be any group. Denote by $p(G)$ the order of the smallest nontrivial subgroup of G. If G is finite, then $p(G)$ equals the smallest prime divisor of the order of G. On the other hand, $p(G) = \infty$ if and only if G is torsion free. For any prime number p, we will denote by $\mathbf{Z}_p$ the group of p elements. Somewhat unconventionally, throughout this paper we will use multiplicative notation even in the case of Abelian groups.

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

$$AB = \{ab \mid a \in A, b \in B\}.$$

According to the Cauchy-Davenport theorem ([2], [4]), $|AB| \geq k + \ell - 1$ holds if $G \cong \mathbf{Z}_p$, where p is a prime number such that $p \geq k + \ell - 1$. This result has been generalized in several ways, see e.g. [3, 23, 24, 25, 27].

In particular, the following improvement can easily be obtained from Kneser's theorem ([19], [21]) or can be proved directly with a short combinatorial argument, see [16].

---

*) On leave from Eötvös University, Budapest. Research partially supported by Hungarian Scientific Research Grants OTKA T043623 and T043631.

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

Kneser's theorem cannot be extended to noncommutative groups in a natural way ([22], [28]), and the simple combinatorial proof does not work either. Denote by $\mu_G(k, \ell)$ the minimum size of the product set AB where A and B range over all subsets of G of cardinality k and ℓ, respectively. For finite Abelian groups G, the function μ_G has been exactly determined by Eliahou, Kervaire and Plagne [7]. Some partial results in the non-Abelian case were found recently by Eliahou and Kervaire ([5], [6]). In particular, they proved the inequality $\mu_G(k, \ell) \leq k + \ell - 1$ for all possible values of k and ℓ when G is a finite solvable group. That equality holds here for $k + \ell - 1 \leq p(G)$, a case in which the upper bound is folklore, is contained in the following result that we found extending some of the ideas developed in [14, 15, 17].

THEOREM 2. *If A and B are nonempty subsets of a finite group G such that $p(G) \geq |A| + |B| - 1$, then $|AB| \geq |A| + |B| - 1$.*

Based on the theory of group extensions, the proof of this result is surprisingly simple. Most of this paper is devoted to the study of critical pairs A, B for which equality is attained in the above theorem.

According to Vosper's inverse theorem [26], if A, B are nonempty subsets of $\mathbf{Z}_p$ such that $|AB| = |A| + |B| - 1$, then either $|A| + |B| - 1 = p$ (that is, $AB = \mathbf{Z}_p$), or one of the sets A and B contains only one element, or $|AB| = p - 1$ and with the notation $\{c\} = \mathbf{Z}_p \setminus AB$, B is the complement of the set cA^{-1} in $\mathbf{Z}_p$, or both A and B are (geometric) progressions with the same common quotient. Hamidoune and Rødseth [12] go one step further; they characterize all pairs A, B with $|AB| = |A| + |B|$. An extension of Vosper's theorem to arbitrary Abelian groups is due to Kemperman [18]. For a related result, see Lev [20].

Vosper's theorem has been extended to torsion free groups by Brailovsky and Freiman [1]. A generalization to arbitrary noncommutative groups has been obtained by Hamidoune [10]. To state it, we first have to recall the following notion. Let B be a finite subset of a group G such that $1 \in B$. B is called a *Cauchy-subset* of G if, for every finite nonempty subset A of G,

$$|AB| \geq \min\{|G|, |A| + |B| - 1\}.$$

If the group G is finite, then a subset S that contains the unit element is known to be a Cauchy subset if and only if for every subgroup H of G,

$$\min\{|SH|,\ |HS|\} \geq \min\{|G|,\ |H| + |S| - 1\},$$

see Corollary 3.4 in [10]. Now Theorem 6.6 in the same paper can be stated as follows. (Here $\langle q\rangle$ denotes the subgroup generated by the element q.)

THEOREM 3. *Let G be a finite group and let B be a Cauchy subset of G such that $|G|$ is coprime to $|B|-1$. Assume that $|AB| = |A|+|B|-1 \leq |G|-1$ holds for some subset A of G. Then either $|A| = 1$, or $A = G \setminus aB^{-1}$ for some $a \in G$, or there are elements $a, b, q \in G$ and natural numbers k, l such that*

$$A = \{a, aq, aq^2, \ldots, aq^{k-1}\} \quad \text{and} \quad B = (G \setminus \langle q\rangle b) \cup \{b, qb, q^2b, \ldots, q^{l-1}b\}.$$

Since without any loss of generality we may assume in Vosper's theorem that $1 \in B$, and any such B with $|B| \geq 2$ is a Cauchy subset of $\mathbf{Z}_p$, Vosper's theorem follows immediately from the above result of Hamidoune. Note that if G is not a cyclic group of prime order, then a subset B of G with $2 \leq |B| \leq p(G)$ is not a Cauchy subset in general. Thus the following result gives a different kind of generalization of Vosper's inverse theorem, more in the spirit of Theorem 2.

THEOREM 4. *Let A, B be subsets of a finite group G such that $|A| = k$, $|B| = \ell$ and $k + \ell - 1 \leq p(G) - 1$. Then $|AB| = k + \ell - 1$ if and only if one of the following conditions holds:*

(i) $k = 1$ *or* $\ell = 1$;

(ii) *there exist* $a, b, q \in G$ *such that*

$$A = \{a, aq, aq^2, \ldots, aq^{k-1}\} \quad \text{and} \quad B = \{b, qb, q^2b, \ldots, q^{l-1}b\};$$

(iii) $k + \ell - 1 = p(G) - 1$ *and there exist a subgroup* F *of* G *of order* $p(G)$ *and elements* $u, v \in G$, $z \in F$ *such that*

$$A \subset uF, \quad B \subset Fv \quad \text{and} \quad A = u(F \setminus zvB^{-1}).$$

Note that the assertions of both Theorems 2 and 4 are obvious if $p(G) = 2$. Thus in view of the Feit–Thompson theorem [8], it is enough to prove the assertions for solvable groups. Given that the results hold for cyclic groups of prime order, the natural approach is then to transfer the results to group extensions. In the case of Theorem 2 this is relatively simple, and depends only mildly on the structure of the extension, see Lemma 7. We prove this result in the next section. The proof of Theorem 4 is more delicate; in this case we cannot directly transfer the result to group extensions. In Section 3 we study how much the general approach of the previous section can contribute towards the characterization of critical pairs if we also assume that the group H in Lemma 7 is a cyclic group of prime order, meaning that we can also take advantage of Vosper's inverse theorem. We complete the proof of Theorem 4 in the last section, where we finally take into account the specific structure of cyclic extensions. The proof also relies on Hamidoune's result Theorem 3.

Finally we note that the following alternative proof of Theorem 2 has been suggested by Hamidoune [11]. Let A and S denote nonempty finite subsets of an arbitrary group G. Denote by $\langle S\rangle$ the subgroup generated by S and by $\nu(S)$ the mininum order of an element in S. According to a result of Hamidoune [9], if $A\cup AS\neq A\langle S\rangle$, then

$$|A\cup AS|\geq |A|+\min\{|S|,\,\nu|S|\}\,.$$

Now let A and B be arbitrary nonempty finite subsets of G satisfying $|A|+|B|-1\leq p(G)$. If $|B|=1$, then obviously $AB|=|A|+|B|-1$. Otherwise, replacing A by Ab and B by $b^{-1}B$ for some element $b\in B$, we may assume that $1\in B$. Let $S=B\setminus\{1\}$, then $\nu(S)\geq p(G)$ and $|\langle S\rangle|\geq p(G)$. Moreover, $A\cup AS=AB$. Thus either $AB=A\langle S\rangle$, in which case

$$|AB|\geq|\langle S\rangle|\geq p(G)\geq|A|+|B|-1\,,$$

or the above theorem implies that

$$|AB|=|A\cup AS|\geq|A|+\min\{|S|,\,\nu(S)\}=|A|+|S|=|A|+|B|-1\,.$$

Even though this argument extends Theorem 2 to infinite groups, we feel that our direct approach is more transparent. We also depend on our proof in order to derive Theorem 4.

2. PROOF OF THEOREM 2

For simplicity, we say that the group G possesses the Cauchy-Davenport property if for any pair of nonempty subsets A,B of G with $p(G)\geq|A|+|B|-1$, we have $|AB|\geq|A|+|B|-1$. In view of our previous remarks, Theorem 2 can be reduced to the following

THEOREM 5. *Every finite solvable group G possesses the Cauchy-Davenport property.*

Let $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$ be a composition series of G. Here every composition factor G_i/G_{i+1} is a cyclic group of prime order, and the length of the series $r = r(G)$, being equal to the total number of prime divisors of the order of G, does not depend on the particular choice of the composition series. If $G/N = H$ for some proper normal subgroup N of G, then $|G| = |N| \cdot |H|$ and thus $p(G) = \min\{p(N), p(H)\}$. We just remark that even if the group G is not finite, the inequality $p(G) \geq \min\{p(N), p(H)\}$ is not difficult to verify. Since every cyclic group of prime order has the Cauchy-Davenport property, Theorem 5 follows easily by induction on r from the following lemma.

LEMMA 6. *Let G be an arbitrary group with a proper normal subgroup N. Assume that $p(G) = \min\{p(N), p(G/N)\}$. If both N and G/N possess the Cauchy-Davenport property, then so does G.*

Before we indicate how this lemma follows from a more general statement, we briefly recall the structure of general group extensions, following the terminology of [13]. Namely, if $H = G/N$, then the group G can be reconstructed from N and H as follows. There exist a map $f\colon H \times H \to N$ and for every $h \in H$ an automorphism $\vartheta_h \in \mathrm{Aut}(N)$ such that the following conditions hold for every $n \in N$ and $h_1, h_2, h_3 \in H$:

(i) $f(1, h_1) = f(h_1, 1) = 1$;

(ii) $f(h_1, h_2)f(h_1h_2, h_3) = \vartheta_{h_1}\big(f(h_2, h_3)\big)f(h_1, h_2h_3)$;

(iii) $\vartheta_{h_1}\vartheta_{h_2}(n) = f(h_1, h_2)\vartheta_{h_1h_2}(n)f(h_1, h_2)^{-1}$;

(iv) ϑ_1 is the unit element of $\mathrm{Aut}(N)$.

Then G is isomorphic to the group we obtain if we equip the set of ordered pairs $\{(n, h) \mid n \in N, h \in H\}$ with the multiplication

$$(n_1, h_1)(n_2, h_2) =: \big(n_1\vartheta_{h_1}(n_2)f(h_1, h_2), h_1h_2\big)\,.$$

The behavior in the second coordinate is just as in the case of direct product, thus the properties of H can be exploited in a natural way. Note also that for every $h_1, h_2 \in H$, the mapping

$$n \to \vartheta_{h_1}(n)f(h_1, h_2)$$

is an $N \to N$ bijection. This is the key fact that allows us to exploit also the properties of N. Now it is clear that Lemma 6 is a special case of the following statement.

LEMMA 7. *Let N and H be arbitrary groups that possess the Cauchy-Davenport property. Assume that bijections $\varphi_{h_1,h_2}, \psi_{h_1,h_2} : N \to N$ are given for every $h_1, h_2 \in H$. Define a binary operation on the set of ordered pairs $G = \{(n,h) \mid n \in N, h \in H\}$ as follows:*

$$(n_1,h_1)(n_2,h_2) =: \left(\varphi_{h_1,h_2}(n_1)\psi_{h_1,h_2}(n_2), h_1h_2\right).$$

Then $|AB| \geq |A| + |B| - 1$ holds for arbitrary subsets A, B of G which satisfy

$$|A| + |B| - 1 \leq \min\{p(N), p(H)\}.$$

Proof. The assertion is obvious if one of the sets A and B is infinite. Thus we assume that A, B are finite subsets of G such that $|A| + |B| - 1 \leq \min\{p(N), p(H)\}$. Write $k = |A|$, $\ell = |B|$ and let $A = C_1 \cup \cdots \cup C_s$ and $B = D_1 \cup \cdots \cup D_t$, where $C_i = \{(a_{ij}, c_i) \quad 1 \leq i \leq k_i\}$ and $D_i = \{(b_{ij}, d_i) \mid 1 \leq i \leq \ell_i\}$. We assume that $C = \{c_1, \ldots, c_s\}$ and $D = \{d_1, \ldots, d_t\}$ are subsets of H of cardinality s and t, respectively. We will also assume that $k_1 \leq \cdots \leq k_s$ and $\ell_1 \leq \cdots \leq \ell_t$. Thus, $s \leq k$, $t \leq \ell$ and $\sum_{i=1}^{s} k_i = k$, $\sum_{i=1}^{t} \ell_i = \ell$. Introduce also $A_i = \{a_{ij} \mid 1 \leq j \leq k_i\}$ and $B_i = \{b_{ij} \mid 1 \leq j \leq \ell_i\}$; they are subsets of N. In C_iD_j, the second coordinate of each element is c_id_j, whereas the first coordinates form the set $\varphi_{c_i,d_j}(A_i)\psi_{c_i,d_j}(B_j)$. Since φ_{c_i,d_j} and ψ_{c_i,d_j} are $N \to N$ bijections and

$$k_i + \ell_j - 1 \leq k + \ell - 1 \leq \min\{p(N), p(H)\} \leq p(N),$$

our hypothesis on the group N implies that

$$|C_iD_j| = |\varphi_{c_i,d_j}(A_i)\psi_{c_i,d_j}(B_j)| \geq k_i + \ell_j - 1 \geq 1$$

holds for every $1 \leq i \leq s$ and $1 \leq j \leq t$. Due to the symmetry of the multiplication introduced on G, we may assume without any loss of generality that $s \geq t$. Consider the numbers $c_1d_t, c_2d_t, \ldots, c_sd_t \in H$; they are s different elements of the set product CD. Since $s + t - 1 \leq k + \ell - 1 \leq p(H)$, our hypothesis on the group H implies that $|CD| \geq s + t - 1$. Therefore there exists a set I of $t - 1$ pairs (γ, δ) such that the numbers

$$c_i d_t \quad (1 \le i \le s), \qquad c_\gamma d_\delta \quad \big((\gamma,\delta) \in I\big)$$

are all different. Since the sets

$$C_i D_t \quad (1 \le i \le s), \qquad C_\gamma D_\delta \quad \big((\gamma,\delta) \in I\big)$$

are pairwise disjoint subsets of AB, it follows that

$$
\begin{aligned}
&(1) \qquad & |AB| &\ge \sum_{i=1}^{s} |C_i D_t| + \sum_{(\gamma,\delta)\in I} |C_\gamma D_\delta| \\
&(2) \qquad & &\ge \sum_{i=1}^{s} (k_i + \ell_t - 1) + (t-1) \\
&(3) \qquad & &= k + t\ell_t + (s-t)\ell_t - s + t - 1 \\
&(4) \qquad & &= k + t\ell_t + (s-t)(\ell_t - 1) - 1 \\
&(5) \qquad & &\ge k + \ell - 1\,,
\end{aligned}
$$

as was to be proved.

3. AN INTERMEDIATE STEP

Now we take a closer look at the proof of Lemma 7. For the rest of this section we assume that the finite sets A, B satisfy

$$|AB| = |A| + |B| - 1 \le \min\{p(N), p(H)\} - 1\,.$$

Then we must have equality in (5), which means that $\ell_1 = \ell_2 = \cdots = \ell_t$ and also that either $s = t$ or $\ell_t = 1$ must hold. Note that we have assumed $s \ge t$. In the case $t \ge s$ a similar argument yields that $k_1 = k_2 = \cdots = k_s$ and, in addition, either $s = t$ or $k_s = 1$. Thus, if $s > t = 1$, then $\ell = \ell_1 = 1$, and similarly, if $t > s = 1$, then $k = 1$.

Assume now that $s, t \ge 2$. If H is a cyclic group of order p for some prime number p, then H clearly possesses the Cauchy-Davenport property. In (1) we also must have equality, which means that

$$|CD| = s + t - 1 \le k + \ell - 1 \le \min\{p(N), p(H)\} - 1 \le p - 1\,.$$

Vosper's inverse theorem applied to H leaves us two possibilities, one being that $C = H \setminus hD^{-1}$ for some $h \in H$, but this only can occur if $s = k$, $\ell = t$ and $k + \ell = p \le p(N)$. The other possibility is that $C = \{c'_1, \ldots, c'_s\}$

and $D = \{d'_1, \dots, d'_t\}$, where $c'_i = cq^{i-1}$ and $d'_i = dq^{i-1}$ for suitable elements $c, d, q \in H$. There is an index $1 \le \alpha \le s$ such that $c_s = c'_\alpha$. Clearly,

$$\begin{aligned} CD &= \{cd, cdq, cdq^2, \dots, cdq^{s+t-2}\} \\ &= \{c'_1 d'_1, c'_2 d'_1, \dots, c'_\alpha d'_1, c'_\alpha d'_2, \dots, c'_\alpha d'_t, c'_{\alpha+1} d'_t, \dots, c'_s d'_t\}. \end{aligned}$$

Writing $C'_i = C_j$, $k'_i = k_j$ if $c'_i = c_j$ and $D'_i = D_j$, $\ell'_i = \ell_j$ if $d'_i = d_j$, and noticing that the sets

$$C'_1 D'_1, C'_2 D'_1, \dots, C'_\alpha D'_1, C'_\alpha D'_2, \dots, C'_\alpha D'_t, C'_{\alpha+1} D'_t, \dots, C'_s D'_t$$

are pairwise disjoint subsets of G that satisfy

$$|C'_i D'_j| \ge k'_i + \ell'_i - 1 \ge k'_i,$$

we may argue that

$$\begin{aligned} |AB| &\ge \sum_{i=1}^{\alpha-1} |C'_i D'_1| + \sum_{i=1}^{t} |C'_\alpha D'_i| + \sum_{i=\alpha+1}^{s} |C'_i D'_t| \\ &\ge \sum_{i=1}^{t} (k_s + \ell_i - 1) + \sum_{i=1}^{s-1} k_i \\ &= \sum_{i=1}^{s} k_i + \sum_{i=1}^{t} \ell_i + (t-1)k_s - t \\ &= k + \ell - 1 + (t-1)(k_s - 1) \\ &\ge k + \ell - 1. \end{aligned}$$

From the conditions $|AB| = |A| + |B| - 1$ and $t \ge 2$ it follows that $k_s = 1$, that is, $s = k$. A similar argument also yields $t = \ell$.

We summarize these observations in the following lemma.

LEMMA 8. *Let N be an arbitrary group that possesses the Cauchy-Davenport property, and let $H = \mathbf{Z}_p$ for some prime number p. Assume that bijections $\varphi_{h_1,h_2}, \psi_{h_1,h_2} : N \to N$ are given for every $h_1, h_2 \in H$. Define a binary operation on the set of ordered pairs $G = \{(n, h) \mid n \in N, h \in H\}$ as follows:*

$$(n_1, h_1)(n_2, h_2) =: \left(\varphi_{h_1,h_2}(n_1)\psi_{h_1,h_2}(n_2), h_1 h_2\right).$$

If A, B are subsets of G which satisfy

$$|AB| = |A| + |B| - 1 \le \min\{p(N), p\} - 1,$$

then (using the notations introduced in the proof of Lemma 7) one of the following conditions holds:

(a) $k = 1$ *or* $\ell = 1$;

(b) $k, \ell \geq 2$ *and* $s = t = 1$;

(c) $s = k \geq 2$, $t = \ell \geq 2$ *and* C, D *are progressions in* H *with the same common quotient;*

(d) $s = k \geq 2$, $t = \ell \geq 2$, $k + \ell = p \leq p(N)$ *and* $C = H \setminus hD^{-1}$ *for a suitable element* $h \in H$.

4. Proof of Theorem 4

The 'if' part is quite simple. First, if $k = 1$ then $|AB| = |B| = \ell$, and if $\ell = 1$ then $|AB| = |A| = k$. Next, if the second condition holds, then again

$$|AB| = |\{aq^i b \mid 0 \leq i \leq k + \ell - 2\}| = k + \ell - 1,$$

because the order of q is at least $k + \ell$. Finally, in the third case we also have

$$|AB| = |uFv \setminus \{uzv\}| = |F| - 1 = k + \ell - 1.$$

To prove the necessity of the conditions, we may assume that the group G is solvable. We proceed by induction on the length of the composition series of G. If $r(G) = 1$ then G is a cyclic group of prime order and the result is contained in Vosper's theorem. So we assume that $r(G) \geq 2$ and that the theorem has been already verified for every finite solvable group G' with $r(G') < r(G)$. Choose a normal subgroup $N \lhd G$ such that $H = G/N \cong \mathbf{Z}_p$ for a prime number p. Then G is a cyclic extension of N by H, and can be reconstructed from N and $H = \langle h \rangle$ as follows. There is an element $n_0 \in N$ and an automorphism $\vartheta \in \mathrm{Aut}(N)$ such that $\vartheta(n_0) = n_0$, $\vartheta^p(n) = n_0 n n_0^{-1}$ for every $n \in N$ and the multiplication on the set of ordered pairs

$$G_0 = \{(n, h^i) \mid n \in N, 0 \leq i \leq p - 1\}$$

introduced as

$$(n_1, h^i)(n_2, h^j) = \left(n_1 \vartheta^i(n_2) f(h^i, h^j), h^{i+j}\right),$$

where

$$f(h^i, h^j) = \begin{cases} 1 & \text{if } i + j < p \\ n_0 & \text{if } i + j \geq p \end{cases}$$

makes G_0 a group isomorphic to G, which we may as well identify with G.

In particular, the function $f\colon H \times H \to N$ satisfies among others the relations

$$f(h^u, 1) = f(1, h^v) \tag{6}$$

and

$$\vartheta^i\big(f(h^u, h^v)\big) = f(h^u, h^v) \tag{7}$$

for every integer i and $0 \le u, v \le p-1$.

According to Theorem 2, N possesses the Cauchy-Davenport property. We also have

$$|A| + |B| - 1 \le p(G) - 1 = \min\{p(N), p\} - 1 .$$

Thus we may apply Lemma 8 with

$$\varphi_{h^i,h^j} \equiv \mathrm{id} \qquad \text{and} \qquad \psi_{h^i,h^j}(n) = \vartheta^i(n) f(h^i, h^j) .$$

Accordingly, we distinguish four cases.

(a) If $k = 1$ or $\ell = 1$, then condition (i) holds.

(b) If $k, \ell \ge 2$ and $s = t = 1$, then $|A_1| = k_1 = k$ and $|B_1| = \ell_1 = \ell$. Thus,

$$A = \{(a_i, h^\alpha) \mid 1 \le i \le k\} \qquad \text{and} \qquad B = \{(b_j, h^\beta) \mid 1 \le j \le \ell\}$$

with suitable integers $0 \le \alpha, \beta \le p-1$. Therefore

$$AB = \big\{\big(a_i \vartheta^\alpha(b_j) f(h^\alpha, h^\beta), h^{\alpha+\beta}\big) \mid 1 \le i \le k, 1 \le j \le \ell\big\} .$$

Put $B_1' = \{\vartheta^\alpha(b_j) \mid 1 \le j \le \ell\}$. Then A_1, B_1' are subsets of N of cardinality k and ℓ, respectively. Since every element of AB has the same second coordinate $h^{\alpha+\beta}$ and multiplication by $f(h^\alpha, h^\beta)$ is an $N \to N$ bijection, these sets satisfy

$$|A_1 B_1'| = |AB| = k + \ell - 1 \le p(N) - 1 .$$

N is a finite solvable group with $r(N) = r(G) - 1$, thus our induction hypothesis implies that either (b1) there exist elements $a, b, q \in N$ such that $A_1 = \{a, aq, \dots, aq^{k-1}\}$ and $B_1' = \{b, qb, \dots, q^{\ell-1}b\}$, or (b2) $k + \ell - 1 = p(N) - 1 = p(G) - 1$ and there exist a subgroup F of N of order $p(N)$ and elements $u, v \in N$, $z \in F$ such that $A_1 \subset uF$, $B_1' \subset Fv$ and $A_1 = u\big(F \setminus zv(B_1')^{-1}\big)$.

We elaborate on these two subcases separately.

(b1) We prove that in this case condition (ii) holds. More precisely, we prove that

$$A = \{a_0, a_0q_0, \dots, a_0q_0^{k-1}\} \qquad \text{and} \qquad B = \{b_0, q_0b_0, \dots, q_0^{\ell-1}b_0\}, \tag{8}$$

where $a_0 = (a, h^\alpha)$, $b_0 = \big(\vartheta^{-\alpha}(b), h^\beta\big)$ and $q_0 = \big(\vartheta^{-\alpha}(q), 1\big)$.

We may assume that $a_{i+1} = aq^i$ and $b_{j+1} = \vartheta^{-\alpha}(q^jb)$ holds for $0 \le i \le k-1$ and $0 \le j \le \ell - 1$. Thus $(a_1, h^\alpha) = a_0$ and $(b_1, h^\beta) = b_0$. We proceed by induction as follows. Assume first that we have already verified that $(a_i, h^\alpha) = a_0q_0^{i-1}$ holds for some $1 \le i \le k-1$. Then

$$\begin{aligned} a_0q_0^i &= (a_i, h^\alpha)q_0 = (aq^{i-1}, h^\alpha)(\vartheta^{-\alpha}(q), 1) \\ &= (aq^{i-1}\vartheta^\alpha(\vartheta^{-\alpha}(q))f(h^\alpha, 1), h^\alpha) = (aq^i, h^\alpha) = (a_{i+1}, h^\alpha). \end{aligned}$$

On the other hand, if we have $(b_j, h^\beta) = q_0^{j-1}b_0$ for some $1 \le j \le \ell-1$, then

$$\begin{aligned} q_0^jb_0 &= q_0(b_j, h^\beta) = (\vartheta^{-\alpha}(q), 1)(\vartheta^{-\alpha}(q^{j-1}b), h^\beta) \\ &= (\vartheta^{-\alpha}(q)\vartheta^0(\vartheta^{-\alpha}(q^{j-1}b))f(1, h^\beta), h^\beta) = (\vartheta^{-\alpha}(q^jb), h^\beta) = (b_{j+1}, h^\beta), \end{aligned}$$

since ϑ, and thus also $\vartheta^{-\alpha}$ is an automorphism of N. This verifies (8).

(b2) In this case we can write

$$A_1 = \{u\dot{a}_1, u\dot{a}_2, \dots, u\dot{a}_k\} \qquad \text{and} \qquad B_1' = \{\dot{b}_1v, \dot{b}_2v, \dots, \dot{b}_\ell v\},$$

where $a_i = u\dot{a}_i$, $\vartheta^\alpha(b_j) = \dot{b}_jv$ and

$$\{\dot{a}_1, \dot{a}_2, \dots, \dot{a}_k\} = F \setminus z\{\dot{b}_1^{-1}, \dot{b}_2^{-1}, \dots, \dot{b}_\ell^{-1}\}. \tag{9}$$

Let $F_0 = \{(\vartheta^{-\alpha}(f), 1) \mid f \in F\}$; then $|F_0| = |F| = p(N) = p(G)$, and clearly F_0 is a subgroup of G isomorphic to F. Introduce also $u_0 = (u, h^\alpha)$ and $v_0 = (\vartheta^{-\alpha}(v), h^\beta)$, and consider the sets $A_0, B_0 \subset F_0$ defined as follows:

$$A_0 = \{(\vartheta^{-\alpha}(\dot{a}_i), 1) \mid 1 \le i \le k\} \qquad \text{and} \qquad B_0 = \{(\vartheta^{-\alpha}(\dot{b}_j), 1) \mid 1 \le j \le k\}.$$

Then $A = u_0A_0 \subset u_0F_0$, because for any $1 \le i \le k$,

$$\begin{aligned} u_0(\vartheta^{-\alpha}(\dot{a}_i), 1) &= (u, h^\alpha)(\vartheta^{-\alpha}(\dot{a}_i), 1) \\ &= (u\vartheta^\alpha(\vartheta^{-\alpha}(\dot{a}_i))f(h^\alpha, 1), h^\alpha) = (u\dot{a}_i, h^\alpha) = (a_i, h^\alpha) \end{aligned}$$

holds. Similarly, for every $1 \le j \le \ell$ we have

$$\begin{aligned} (\vartheta^{-\alpha}(\dot{b}_j), 1)v_0 &= (\vartheta^{-\alpha}(\dot{b}_j), 1)(\vartheta^{-\alpha}(v), h^\beta) \\ &= (\vartheta^{-\alpha}(\dot{b}_j)\vartheta^0(\vartheta^{-\alpha}(v))f(1, h^\beta), h^\beta) \\ &= (\vartheta^{-\alpha}(\dot{b}_jv), h^\beta) = (b_j, h^\beta), \end{aligned}$$

implying that $B = B_0 v_0 \subset F_0 v_0$. Finally, applying $\vartheta^{-\alpha}$ to Equation (9) and observing that the map $\varphi\colon N \to G$ defined as $\varphi(x) = (x, 1)$ induces a group isomorphism from $\vartheta^{-\alpha}(F)$ onto F_0, we find that $A_0 = F_0 \setminus z_0 B_0^{-1}$, where $z_0 = (\vartheta^{-\alpha}(z), 1) \in F_0$. Consequently,

$$A = u_0 A_0 = u_0(F_0 \setminus z_0(Bv_0^{-1})^{-1}) = u_0(F_0 \setminus z_0 v_0 B^{-1}),$$

justifying that condition (iii) holds in this case.

(c) $s = k \geq 2$, $t = \ell \geq 2$ and C, D are progressions in H with the same common quotient. In this case we may write

$$A = \{(a_i, c_i) \mid 1 \leq i \leq k\} \qquad \text{and} \qquad B = \{(b_j, d_j) \mid 1 \leq j \leq \ell\},$$

where $c_i = h^{\alpha+(i-1)\gamma}$ and $d_j = h^{\beta+(j-1)\gamma}$ with suitable integers $0 \leq \alpha, \beta, \gamma \leq p-1$, $\gamma \neq 0$. Let $a_0 = (a_1, c_1) = (a_1, h^\alpha)$, $b_0 = (b_1, d_1) = (b_1, h^\beta)$ and $q_0 = (x, h^\gamma)$ where

$$x = \vartheta^{-\alpha}(a_1^{-1} a_2 (f(h^\alpha, h^\gamma))^{-1}).$$

This implies that

$$a_0 q_0 = (a_1, h^\alpha)(x, h^\gamma) = (a_1 \vartheta^\alpha(x) f(h^\alpha, h^\gamma), h^{\alpha+\gamma}) = (a_2, h^{\alpha+\gamma}) = (a_2, c_2).$$

We claim that in general,

$$(a_i, c_i) = a_0 q_0^{i-1} \qquad \text{and} \qquad (b_j, d_j) = q_0^{j-1} b_0$$

holds for every $1 \leq i \leq k$ and $1 \leq j \leq \ell$, indicating that condition (ii) is satisfied in this case.

Let $1 \leq i \leq k$, $1 \leq j \leq \ell$ and $m = i + j - 2$. Then

$$(a_i, c_i)(b_j, d_j) = (a_i \vartheta^{\alpha+(i-1)\gamma}(b_j) f(h^{\alpha+(i-1)\gamma}, h^{\beta+(j-1)\gamma}), h^{\alpha+\beta+m\gamma}).$$

Thus, for each $0 \leq m \leq k+\ell-2$, there is an element x_m of AB whose second coordinate is $h^{\alpha+\beta+m\gamma}$. Moreover, the facts that p is a prime, $1 \leq \gamma \leq p-1$ and $k + \ell - 1 \leq p$ imply that the numbers $h^{\alpha+\beta+m\gamma}$ $(0 \leq m \leq k + \ell - 2)$ are $k + \ell - 1$ different elements of H, thus the element $x_m \in AB$ must be unique. It follows that

$$(a_i, c_i)(b_j, d_j) = (a_{i'}, c_{i'})(b_{j'}, d_{j'})$$

holds whenever $i+j = i'+j'$. We know that $(a_2, c_2) = (a_1, c_1) q_0$. For arbitrary $1 \leq j \leq \ell - 1$ we have

$$(a_2, c_2)(b_j, d_j) = (a_1, c_1)(b_{j+1}, d_{j+1}),$$

which then implies $q_0(b_j, d_j) = (b_{j+1}, d_{j+1})$. Thus, $(b_j, d_j) = q_0^{j-1} b_0$ follows by induction on j. In particular, $(b_2, d_2) = q_0(b_1, d_1)$. Thus the relation

$$(a_{i+1}, c_{i+1})(b_1, d_1) = (a_i, c_i)(b_2, d_2)$$

implies $(a_{i+1}, c_{i+1}) = (a_i, c_i)q_0$ for every $1 \le i \le k-1$, and we also obtain $(a_i, c_i) = a_0 q_0^{i-1}$ by induction on i.

(d) $s = k \ge 2$, $t = \ell \ge 2$, $k + \ell = p \le p(N)$ and $C = H \setminus hD^{-1}$ for a suitable element $h \in H$. Let us note first, that we may assume $\ell \ge k$. This is because $A = u(F \setminus zvB^{-1})$ is equivalent to $B = (F \setminus A^{-1}uz)v$ and therefore, by reversing the multiplication on G (that is, introducing $a * b = ba$) we may exchange the roles of A and B without changing the statement of Theorem 4. Once again, we may write

$$A = \{(a_i, c_i) \mid 1 \le i \le k\} \qquad \text{and} \qquad B = \{(b_j, d_j) \mid 1 \le j \le \ell\}.$$

Introduce $\dot{A} = (a_1, c_1)^{-1}A$ and $\dot{B} = B(b_1, d_1)^{-1}$, then we can write

$$\dot{A} = \{(\dot{a}_i, \dot{c}_i) \mid 1 \le i \le k\} \qquad \text{and} \qquad \dot{B} = \{(\dot{b}_j, \dot{d}_j) \mid 1 \le j \le \ell\},$$

where $(\dot{a}_1, \dot{c}_1) = (\dot{b}_1, \dot{d}_1) = (1, 1) \in \dot{A} \cap \dot{B}$, and writing $\dot{C} = \{\dot{c}_i \mid 1 \le i \le k\}$ and $\dot{D} = \{\dot{d}_j \mid 1 \le j \le \ell\}$, we have $|\dot{A}| = |\dot{C}| = k$, $|\dot{B}| = |\dot{D}| = \ell$, and $\dot{C} = H \setminus \dot{h}\dot{D}^{-1}$ holds with $\dot{h} = c_1^{-1} h d_1^{-1}$. In addition, clearly $|\dot{A}\dot{B}| = |AB| = |\dot{A}| + |\dot{B}| - 1$. We distinguish two cases.

(d1) $G_0 = \langle \dot{B} \rangle \ne G$. Now we claim that $\dot{A} \subset G_0$. Indeed, if $a \in \dot{A} \setminus G_0$ then $(1, 1)\dot{B}$ and $a\dot{B}$ are disjoint subsets of $\dot{A}\dot{B}$, yielding

$$|\dot{A}\dot{B}| \ge 2|\dot{B}| = 2\ell > p > |\dot{A}| + |\dot{B}| - 1,$$

a contradiction. Note that G_0 is a proper subgroup of G, hence solvable with $r(G_0) < r(G)$ and $p(G_0) \ge p(G)$. Thus we may apply our induction hypothesis to conclude that either there exist $\dot{a}, \dot{b}, q_0 \in G_0$ such that

$$\dot{A} = \{\dot{a}, \dot{a}q_0, \dot{a}q_0^2, \ldots, \dot{a}q_0^{k-1}\} \qquad \text{and} \qquad \dot{B} = \{\dot{b}, q_0\dot{b}, q_0^2\dot{b}, \ldots, q_0^{\ell-1}\dot{b}\},$$

or $p(G_0) = p(G)$ and there exist a subgroup F of $G_0 < G$ of order $p(G)$ and elements $u, v \in G_0$, $z \in F$ such that

$$\dot{A} \subset uF, \dot{B} \subset Fv \qquad \text{and} \qquad \dot{A} = u(F \setminus zv\dot{B}^{-1}).$$

In the first case we have

$$A = \{a_0, a_0q_0, a_0q_0^2, \ldots, a_0q_0^{k-1}\} \qquad \text{and} \qquad B = \{b_0, q_0b_0, q_0^2b_0, \ldots, q_0^{\ell-1}b_0\}$$

with $a_0 = (a_1, c_1)\dot{a}$ and $b_0 = \dot{b}(b_1, d_1)$, and thus condition (ii) holds. In the other case, since $(1, 1) \in \dot{A} \cap \dot{B}$, we may assume $u = v = 1$, and writing $u_0 = (a_1, c_1)$, $v_0 = (b_1, d_1)$ we may conclude that

$$A \subset u_0F, B \subset Fv_0 \qquad \text{and} \qquad A = u_0(F \setminus zv_0B^{-1}),$$

implying condition (iii).

(d2) $G_0 = \langle \dot{B} \rangle = G$. In this case we show that $\dot{B}$ is a Cauchy-subset of G. To see that, let H_0 be any subgroup of G. If $H_0 = G$, then clearly

$$\min\{|\dot{B}H_0|,\ |H_0\dot{B}|\} = |G| \geq \min\{|G|,\ |H_0| + |\dot{B}| - 1\}.$$

If $H_0 = \{(1,1)\}$, then

$$\min\{|\dot{B}H_0|,\ |H_0\dot{B}|\} = |\dot{B}| = \min\{|G|,\ |H_0| + |\dot{B}| - 1\}.$$

Otherwise $\dot{B} \not\subseteq H_0$, $|H_0| \geq p(G) > |\dot{B}|$, and thus

$$\min\{|\dot{B}H_0|,\ |H_0\dot{B}|\} \geq 2|H_0| \geq |H_0| + |\dot{B}| - 1 = \min\{|G|,\ |H_0| + |\dot{B}| - 1\}.$$

Therefore we can apply Theorem 3. Since $|\dot{A}| \neq 1$ and $|\dot{A}| + |\dot{B}| < |G|$, it follows that there are elements $a, b, q \in G$ and a natural number l such that

$$\dot{A} = \{a, aq, aq^2, \dots, aq^{k-1}\} \quad \text{and} \quad \dot{B} = (G \setminus \langle q \rangle b) \cup \{b, qb, q^2b, \dots, q^{l-1}b\}.$$

If we had $\langle q \rangle \neq G$, we would have $|G| \geq p(G)\,|\langle q \rangle b|$, and thus it would follow that

$$\ell = |\dot{B}| \geq \frac{p(G)-1}{p(G)}|G| \geq \frac{p(G)-1}{p(G)}(p(G))^2 \geq p(G) > \ell,$$

a contradiction. Consequently, $\langle q \rangle = G$, $l = \ell$,

$$\dot{A} = \{a, aq, aq^2, \dots, aq^{k-1}\} \quad \text{and} \quad \dot{B} = \{b, qb, q^2b, \dots, q^{\ell-1}b\},$$

and with the notation $a_0 = (a_1, c_1)a$, $b_0 = b(b_1, d_1)$ we see that

$$A = \{a_0, a_0q, a_0q^2, \dots, a_0q^{k-1}\} \quad \text{and} \quad B = \{b_0, qb_0, q^2b_0, \dots, q^{\ell-1}b_0\},$$

implying that condition (ii) must hold.

This concludes the induction step, and the proof of Theorem 4 is complete.

ACKNOWLEDGEMENTS. I am grateful to Shalom Eliahou and Yahya Ould Hamidoune who provided me with helpful suggestions. I am also grateful for the hospitality of I.H.É.S., where part of this work was completed thanks to the support of the European Commission through its 6th Framework Programme "Structuring the European Research Area" and the contract Nr. RITA-CT-2004-505493 for the provision of Transnational Access implemented as Specific Support Action.

REFERENCES

[1] BRAILOVSKY, L. V. and G. A. FREIMAN. On a product of finite subsets in a torsion-free group. *J. Algebra 130* (1990), 462–476.

[2] CAUCHY, A. L. Recherches sur les nombres. *J. École Polytech. 9* (1813), 99–116.

[3] CHOWLA, I. A theorem on the addition of residue classes: Application to the number $\Gamma(k)$ in Waring's problem. *Proc. Indian Acad. Sci. A 2* (1935), 242–243.

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

[5] ELIAHOU, S. and M. KERVAIRE. The small sumsets property for solvable finite groups. To appear in *European J. Combin.* (2005).

[6] ELIAHOU, S. and M. KERVAIRE. Sumsets in dihedral groups. To appear in *European J. Combin.* (2005).

[7] ELIAHOU, S., M. KERVAIRE, and A. PLAGNE. Optimally small sumsets in finite abelian groups. *J. Number Theory 101* (2003), 338–348.

[8] FEIT, W. and J. G. THOMPSON. Solvability of groups of odd order. *Pacific J. Math. 13* (1963), 775–1029.

[9] HAMIDOUNE, Y. O. A generalization of an addition theorem of Shatrowsky. *European J. Combin. 13* (1992), 249–255.

[10] —— On small subset product in a group. *Astérisque 258* (1999), 281–308.

[11] —— Personal communication (2005).

[12] HAMIDOUNE, Y. O. and Ø. J. RØDSETH. An inverse theorem mod p. *Acta Arith. 92* (2000), 251–262.

[13] HUMPHREYS, J. F. *A Course in Group Theory.* Oxford University Press, 1996.

[14] KÁROLYI, GY. On restricted set addition in Abelian groups. *Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 46* (2003), 47–54.

[15] —— The Erdős–Heilbronn problem in Abelian groups. *Israel J. Math. 139* (2004), 349–359.

[16] —— A compactness argument in the additive theory and the polynomial method. *Discrete Math. 302* (2005), 124–144.

[17] —— An inverse theorem for the restricted set addition in Abelian groups. *J. Algebra 290* (2005), 557–593.

[18] KEMPERMAN, J. H. B. On small sumsets in an abelian group. *Acta Math. 103* (1960), 63–88.

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

[20] LEV, V. F. On small sumsets in abelian groups. *Astérisque 258* (1999), 317–321.

[21] NATHANSON, M. B. *Additive Number Theory. Inverse Problems and the Geometry of Sumsets.* Graduate Texts in Mathematics *165*. Springer, 1996.

[22] OLSON, J. E. On the symmetric difference of two sets in a group. *European J. Combin. 7* (1986), 43–54.

[23] PILLAI, S. S. Generalization of a theorem of Davenport on the addition of residue classes. *Proc. Indian Acad. Sci. A 6* (1938), 179–180.

[24] POLLARD, J. M. A generalisation of the theorem of Cauchy and Davenport. *J. London Math. Soc. (2) 8* (1974), 460–462.

[25] SHATROWSKY, L. A new generalization of Davenport's-Pillai's theorem on the addition of residue classes. *C. R. (Doklady) Akad. Sci. USSR, N. S. 45* (1944), 315–317.

[26] VOSPER, A. G. The critical pairs of subsets of a group of prime order. *J. London Math. Soc. 31* (1956), 200–205. Addendum, 280–282.

[27] YUZVINSKY, S. Orthogonal pairings of Euclidean spaces. *Michigan Math. J. 28* (1981), 131–145.

[28] ZEMOR, G. A generalisation to noncommutative groups of a theorem of Mann. *Discrete Math. 126* (1994), 365–372.

(Reçu le 18 juillet 2005)

G. Károlyi

Institute of Theoretical Computer Science
ETH Zentrum
CH-8092 Zurich
Switzerland
e-mail: karolyi@cs.elte.hu