ACTA ARITHMETICA
* (200*)

The Erdős–Heilbronn problem for finite groups

by

Paul Balister (Memphis, TN) and
Jeffrey Paul Wheeler (Pittsburgh, PA)

1. Background. Additive number theory can be best described as the study of sums of sets of integers. A simple example is, given two subsets A and B of a set of integers, what facts can we determine about $A+B$ where $A+B := \{a+b \mid a \in A \text{ and } b \in B\}$? We will state a result regarding this example shortly. We note that a very familiar problem in number theory, namely Lagrange's Theorem that every nonnegative integer can be written as the sum of four squares, can be expressed in terms of sumsets. In particular, if we let $\mathbb{N}_0$ be the set of nonnegative integers and if we let S be the set of all integers that are perfect squares, then Lagrange's Theorem has the form

$$\mathbb{N}_0 = S + S + S + S.$$

As well the binary version of Goldbach's Conjecture can be restated in terms of sumsets. In particular, let $\mathbb{E} = \{2x \mid x \in \mathbb{Z},\ x \geq 2\}$ and let $\mathbb{P} = \{p \in \mathbb{Z} \mid p \text{ is prime}\}$. Then

$$\mathbb{E} \subseteq \mathbb{P} + \mathbb{P}.$$

A classical problem in additive number theory was the conjecture of Paul Erdős and Hans Heilbronn [9] which stood as an open problem for over 30 years until proved in 1994. We seek to extend this result. This conjecture has its roots in a theorem proved by Cauchy [4] in 1813 and independently by Davenport [6] in 1935 (Davenport discovered in 1947 [7] that Cauchy had previously proved the theorem). The theorem in its original form is

Theorem 1.1 (Original Cauchy–Davenport). *If A and B are nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$ with p prime, then $|A+B| \geq \min\{p, |A|+|B|-1\}$, where $A+B := \{a+b \mid a \in A \text{ and } b \in B\}$.*

2010 *Mathematics Subject Classification*: 05, 11, 20.
Key words and phrases: Cauchy–Davenport theorem, Erdős–Heilbronn problem, additive number theory, sumsets, polynomial method, solvable groups, finite groups.

We note that in 1935 Inder Chowla [5] extended the result to composite moduli m when $0 \in B$ and the other members of B are relatively prime to m.

The structures over which the Cauchy–Davenport Theorem holds have been extended beyond $\mathbb{Z}/p\mathbb{Z}$. Before stating the extended versions, the following definition is needed.

DEFINITION 1.2 (Minimal torsion element). Let G be a group. We define $p(G)$ to be the smallest positive integer p for which there exists a nonzero element g of G with $pg = 0$ (or, if multiplicative notation is used, $g^p = 1$). If no such p exists, we write $p(G) = \infty$.

Before we continue, an observation:

REMARK 1.3. If G is finite, then $p(G)$ is the smallest prime factor of $|G|$.

Equipped with this we can state that the Cauchy–Davenport Theorem has been extended to abelian groups by Károlyi [14], [15] and then to all finite groups by Károlyi [16] and Balister and Wheeler [3], namely:

THEOREM 1.4 (Cauchy–Davenport Theorem for finite groups). *If A and B are nonempty subsets of a finite group G, then $|A \cdot B| \geq \min\{p(G), |A| + |B| - 1\}$, where $A \cdot B := \{a \cdot b \mid a \in A \text{ and } b \in B\}$.*

Naturally, induction further gives us

THEOREM 1.5. *Let $h \geq 2$. Then for $A_1, \ldots, A_h$ nonempty subsets of a finite group G,*

$$|A_1 \cdots A_h| \geq \min\Big\{p(G), \sum_{i=1}^{h} |A_i| - h + 1\Big\}.$$

Over 40 years ago, Paul Erdős and Hans Heilbronn conjectured that if the addition in the Cauchy–Davenport Theorem is restricted to distinct elements, the lower bound changes only slightly. Erdős stated this conjecture in 1963 during a number theory conference at the University of Colorado [9]. Interestingly, Erdős and Heilbronn did not mention the conjecture in their 1964 paper on sums of sets of congruence classes [12] though Erdős mentioned it often in his lectures (see [19, page 106]). Eventually the conjecture was formally stated in Erdős' contribution to a 1971 text [10] as well as in a book by Erdős and Graham in 1980 [11]. In particular,

THEOREM 1.6 (Erdős–Heilbronn Problem). *If A and B are nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$ with p prime, then $|A \dot{+} B| \geq \min\{p, |A| + |B| - 3\}$, where $A \dot{+} B := \{a + b \bmod p \mid a \in A,\ b \in B \text{ and } a \neq b\}$.*

The conjecture was first proved for the case $A = B$ by Dias da Silva and Hamidounne in 1994 [8] with the more general case established by Alon, Nathanson, and Ruzsa using the polynomial method in 1995 [1]. Károlyi

extended this result to abelian groups for the case $A = B$ in 2004 [15] and to cyclic groups of prime power order in 2005 [17].

Our aim is to establish this result for all finite groups. We in fact prove a more general result, for which it will be useful to introduce the following notation.

DEFINITION 1.7. For a group G let $\mathrm{Aut}(G)$ be the group of automorphisms of G. Suppose $\theta \in \mathrm{Aut}(G)$ and $A, B \subseteq G$. Write

$$A \overset{\theta}{\cdot} B := \{a \cdot \theta(b) \mid a \in A,\, b \in B, \text{ and } a \neq b\}.$$

Given this definition, we can clearly state our objective, namely to extend the theorem to finite groups; in particular we seek to prove

THEOREM 1.8 (Generalized Erdős–Heilbronn for finite groups). *If A and B are nonempty subsets of a finite group G, and $\theta \in \mathrm{Aut}(G)$, then*

$$|A \overset{\theta}{\cdot} B| \geq \min\{p(G) - \delta, |A| + |B| - 3\},$$

where $\delta = 0$ if θ has odd order in $\mathrm{Aut}(G)$ and $\delta = 1$ otherwise.

As well we can state

COROLLARY 1.9. *If A and B are nonempty subsets of a finite group G, and $\theta \in \mathrm{Aut}(G)$, then*

$$|\{ab \mid a \neq \theta(b),\, a \in A,\, b \in B\}| \geq \min\{p(G) - \delta, |A| + |B| - 3\},$$

where $\delta = 0$ if θ has odd order in $\mathrm{Aut}(G)$ and $\delta = 1$ otherwise.

Proof. We have

$$\begin{aligned}\{ab \mid a \neq \theta(b),\, a \in A,\, b \in B\} &= \{a\theta^{-1}(u) \mid a \neq u,\, a \in A,\, u \in \theta(B)\} \\ &= A \overset{\theta^{-1}}{\cdot} \theta(B).\end{aligned}$$

We then use Theorem 1.8 noting that $\theta^{-1} \in \mathrm{Aut}(G)$ has the same order as θ and that $|\theta(B)| = |B|$. ∎

We note that Lev [18] has shown that the results of Theorem 1.8 and Corollary 1.9 are not true for an arbitrary bijection θ.

An additional outcome is

THEOREM 1.10 (Erdős–Heilbronn Conjecture for finite groups). *If A and B are nonempty subsets of a finite group G, then*

$$|\{ab \mid a \in A,\, b \in B,\, a \neq b\}| \geq \min\{p(G), |A| + |B| - 3\}.$$

Proof. Follows from Theorem 1.8 by putting $\theta = 1$. ∎

2. A structure theorem for finite solvable groups. Our approach to establishing the Erdős–Heilbronn Problem in the case of finite groups will involve solvable groups. We begin by reminding the reader of some basic definitions.

DEFINITION 2.1. Let G be a group. The *commutator* of x and y in G is defined to be $[x, y] = xyx^{-1}y^{-1}$. The *commutator* of two subgroups H and K of G is $[H, K] = \langle [h, k] \mid h \in H,\ k \in K \rangle$. We define inductively

$$G^{(0)} = G, \quad G^{(1)} = [G, G],\ \ldots,\ G^{(i+1)} = [G^{(i)}, G^{(i)}] \text{ for } i \geq 1.$$

And though several equivalent definitions exist, we choose the following definition for solvable group: G is *solvable* if there exists an $n \geq 0$ such that $G^{(n)} = \{1\}$.

Given these definitions we state some useful facts.

1. $G^{(1)} \trianglelefteq G$.
2. $G/G^{(1)}$ is abelian.
3. If $G \neq \{1\}$ is solvable then $G \neq G^{(1)}$.
4. Subgroups of solvable groups are solvable.

We are now ready to establish the following important theorem.

THEOREM 2.2 (The associated field structure theorem). *Let G be a non-trivial finite solvable group and let $\theta \in \mathrm{Aut}(G)$. Then there exists a $K \trianglelefteq G$, $K \neq G$, such that*

(1) $\theta(K) = K$,
(2) $G/K \cong (\mathbb{F}_{p^n}, +)$ *for some prime p and $n \geq 1$,*
(3) $\overline{\theta}(x) = \gamma x$ *where $\gamma \in \mathbb{F}_{p^n}^{\times}$, $x \in G/K$, and $\overline{\theta}$ is the map induced by θ on G/K which we identify with $\mathbb{F}_{p^n}$ by* (2).

Proof. Easy matters first. Suppose $\theta \in \mathrm{Aut}(G)$ and $K \trianglelefteq G$ with $\theta(K) = K$. The map $\overline{\theta}$ is defined by $\overline{\theta}(gK) = \theta(g)K$; this is well defined since if $g_1K = g_2K$, then

$$\theta({g_2}^{-1}g_1) \in \theta(K) = K,$$

so $\theta(g_1) \in \theta(g_2)K$ and thus $\theta(g_1)K = \theta(g_2)K$.

With well-definedness established, we continue by noting that there is at least one proper normal subgroup with an abelian quotient, namely $G^{(1)}$. Note that $\theta(xyx^{-1}y^{-1}) = \theta(x)\theta(y)\theta(x)^{-1}\theta(y)^{-1}$ and thus $G^{(1)}$ is fixed by θ. Thus if $K = G^{(1)}$ we have the following:

1. K is a proper normal subgroup of G.
2. $\theta(K) = K$.
3. G/K is abelian.

Of all subgroups meeting these three conditions, choose a subgroup K which is maximal in the sense that there is no K' meeting each of the three conditions and $K \subsetneq K'$. We claim that this is the desired subgroup; i.e., that G/K can be given a field structure and $\overline{\theta}(gK) = \theta(g)K$ is multiplication by a nonzero element from G/K.

Before proceeding with the proof, a helpful observation:

OBSERVATION 2.3. *G/K has no proper, nontrivial $\overline{\theta}$-invariant subgroup.*

Proof of observation. Suppose that G/K has a proper, nontrivial $\overline{\theta}$-invariant subgroup, in other words there exists a subgroup H with $K \leq H \leq G$ such that $\{1\} \lneq H/K \lneq G/K$ and $\overline{\theta}(H/K) \subseteq H/K$. But G/K is abelian, so $\{1\} \lhd H/K \lhd G/K$, thus $K \lhd H \lhd G$ and $\theta(H) \subseteq H$. But $|\theta(H)| = |H|$, so $\theta(H) = H$. Also $G/H \cong (G/K)/(K/H)$ is abelian. These contradict the maximality of K. Hence G/K has no proper, nontrivial $\overline{\theta}$-invariant subgroup. ∎

Now we continue with the proof of Theorem 2.2.

Since G/K is abelian, $G/K \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$, a product of cyclic groups. Let p be a prime factor of d_1. Put $P = \{x \mid x^p = 1\}$, the set of all elements in G/K of order dividing p. Since G/K is abelian, P is a subgroup of G/K. Also, since $x^p = 1$ we have $\overline{\theta}(x)^p = 1$, thus $\overline{\theta}(P) \subseteq P$ and so P is $\overline{\theta}$-invariant. But $P \neq \{1\}$, so $P = G/K$. Hence $d_i = p$ for $1 \leq i \leq r$, i.e., $G/K \cong (\mathbb{Z}/p\mathbb{Z})^n \cong (\mathbb{F}_p)^n$. We must be careful in that this isomorphism is an additive group isomorphism; there is work yet to do to establish a field structure.

Given this, we now show that G/K meets the remaining conditions of the lemma, namely that G/K can be given the structure of a finite field and that $\overline{\theta}(x) = \gamma x$ for $\gamma \in \mathbb{F}_{p^n}^{\times}$ where $x = gK$, $g \in G$.

First, since $G/K \cong (\mathbb{F}_p)^n$, G/K is a $\mathbb{F}_p$-vector space. Moreover, since $\overline{\theta}$ is an additive group homomorphism, for any scalar $k \in \{0, 1, \ldots, p-1\} = \mathbb{F}_p$,

$$\overline{\theta}(kx) = \overline{\theta}(\underbrace{x + \cdots + x}_{k \text{ terms}}) = \underbrace{\overline{\theta}(x) + \cdots + \overline{\theta}(x)}_{k \text{ terms}} = k\overline{\theta}(x),$$

i.e., $\overline{\theta}$ is an $\mathbb{F}_p$-linear map. Now we pick a nonzero $e_1 \in G/K$ and define a map $\chi\colon \mathbb{F}_p[x] \to G/K$ by

$$\chi\Big(\sum a_i x^i\Big) = \sum a_i \overline{\theta}^{\,i}(e_1) \quad (G/K \text{ written additively}).$$

This map is $\mathbb{F}_p$-linear. Also, if $f(x) = \sum a_i x^i$ then

$$\begin{aligned} \chi(xf(x)) &= \chi\Big(\sum a_i x^{i+1}\Big) = \sum a_i \overline{\theta}^{\,i+1}(e_1) \\ &= \overline{\theta}\Big(\sum a_i \overline{\theta}^{\,i}(e_1)\Big) \quad \text{(by linearity)} \\ &= \overline{\theta}(\chi(f(x))). \end{aligned} \tag{1}$$

The image $V \subseteq G/K$ of χ is a linear subspace of G/K, and hence a subgroup of G/K, and by (1), $\overline{\theta}(V) \subseteq V$. But $\overline{\theta}$ has no nontrivial proper invariant subgroup. As $0 \neq e_1 \in V$, we must have $V = G/K$, and so χ is surjective. Thus, by the First Isomorphism Theorem (for groups),

$$\mathbb{F}_p[x]/\ker(\chi) \cong G/K \quad \text{(as groups)}. \tag{2}$$

CLAIM. $\ker(\chi)$ *is a maximal ideal of the ring* $\mathbb{F}_p[x]$.

Proof of claim. Suppose $f(x) \in \ker(\chi)$, so that $\chi(f(x)) = 0$. Then $\chi(xf(x)) = \overline{\theta}(\chi(f(x))) = 0$. Therefore an induction argument implies that $\chi(g(x)f(x)) = 0$ for any $g(x) \in \mathbb{F}_p[x]$. Since $\ker(\chi)$ is a subgroup under $+$, we have shown that $\ker(\chi)$ is an ideal.

Suppose that there exists an ideal I of $\mathbb{F}_p[x]$ such that

$$\ker(\chi) \subsetneq I \subsetneq \mathbb{F}_p[x].$$

Considering the image of each of these under χ, we get

$$(0) \subsetneq \chi(I) \subsetneq G/K.$$

The inclusions here are strict since we know that χ induces the isomorphism (2). But since I is an ideal of $\mathbb{F}_p[x]$, we have $xI \subseteq I$, and so by (1), $\overline{\theta}(\chi(I)) = \chi(xI) \subseteq \chi(I)$, i.e., $\chi(I)$ is $\overline{\theta}$-invariant. This is a contradiction, hence $\ker(\chi)$ is maximal. ∎

As a result, $\mathbb{F}_p[x]/\ker(\chi)$ is a field, in particular

$$\mathbb{F}_p[x]/\ker(\chi) \cong \mathbb{F}_{p^n} \quad \text{(as rings)}$$

for some $n \geq 1$.

Hence we have condition (2) of the theorem (namely, the field structure). But again, we have more. We have shown in (1) that $\overline{\theta}$ acting on G/K is the same in $\mathbb{F}_p[x]/\ker(\chi)$ as multiplication by x, which is the same in $\mathbb{F}_{p^n}$ as multiplication by a nonzero element, i.e., we have met condition (3) of the theorem. ∎

3. The Erdős–Heilbronn problem for finite solvable groups. Let G be a finite solvable group. By Theorem 2.2, for any $\theta \in \mathrm{Aut}(G)$ there is some $K \trianglelefteq G$ such that

1. $\theta(K) = K$,
2. $G/K \cong (\mathbb{F}_{p^n}, +)$,
3. $\overline{\theta}(x) = \gamma x$ where $\gamma \in \mathbb{F}_{p^n}^{\times}$ and $\overline{\theta}$ is the map induced by θ on G/K.

For each $h \in (\mathbb{F}_{p^n}, +) \cong G/K$ pick a representative $\tilde{h} \in G$ of h, in particular choose $\tilde{0} = 1$. Define $\psi\colon K \times (\mathbb{F}_{p^n}, +) \to G$ by $\psi(k, h) = k\tilde{h}$. Then ψ is a bijection and

$$\begin{aligned}(3)\qquad \psi(k_1, h_1) \cdot \psi(k_2, h_2) &= k_1\tilde{h}_1 \cdot k_2\tilde{h}_2 = k_1\phi_{h_1}(k_2)\tilde{h}_1\tilde{h}_2 \\ &= (k_1\phi_{h_1}(k_2)\eta_{h_1,h_2})(\widetilde{h_1 + h_2}) \\ &= \psi(k_1\phi_{h_1}(k_2)\eta_{h_1,h_2}, h_1 + h_2)\end{aligned}$$

where $\phi_h(k) = \tilde{h}k\tilde{h}^{-1}$ (so in particular $\phi_h \in \mathrm{Aut}(K)$) and $\eta_{h_i,h_j} = \tilde{h}_i \cdot \tilde{h}_j \cdot (\widetilde{h_i + h_j})^{-1} \in K$ with $\tilde{h}$ the coset representative of h in G. Hence ψ can be

considered an isomorphism if we put the following nonstandard multiplication on $K \times (\mathbb{F}_{p^n}, +)$:

$$(k_1, h_1) \star (k_2, h_2) = (k_1 \phi_{h_1}(k_2) \eta_{h_1,h_2}, h_1 + h_2).$$

In summary, for $A \subseteq G$, we can consider $A \subseteq K \times (\mathbb{F}_{p^n}, +)$, in particular, $A = \{(k_1, h_1), \ldots, (k_t, h_t)\}$ for some $k_1, \ldots, k_t \in K$ and $h_1, \ldots, h_t \in (\mathbb{F}_{p^n}, +)$.

REMARK 3.1. Let (k_1, h_1) and (k_2, h_2) be elements in G, let $\theta \in \mathrm{Aut}(G)$, and let $\gamma \in \mathbb{F}_{p^n}^{\times}$ be as in condition (3) of Theorem 2.2. Then

$$\begin{aligned} \theta(k_2, h_2) &= \theta((k_2, 0) \star (1, h_2)) = \theta(k_2, 0) \star \theta(1, h_2) \\ &= (\theta(k_2), 0) \star (c_{h_2}, \overline{\theta}(h_2)) = (\theta(k_2) c_{h_2}, \gamma h_2) \end{aligned} \tag{4}$$

where $c_{h_2} \in K$ depends only on h_2. Thus

$$\begin{aligned} (k_1, h_1) \star \theta(k_2, h_2) &= (k_1, h_1) \star (\theta(k_2) c_{h_2}, \gamma h_2) \\ &= (k_1 \cdot \phi_{h_1}[\theta(k_2) c_{h_2}] \eta_{h_1,h_2}, h_1 + \gamma h_2) \\ &= (k_1 \cdot \phi_{h_1}[\theta(k_2)] \cdot \phi_{h_1}[c_{h_2}] \cdot \eta_{h_1,h_2}, h_1 + \gamma h_2) \\ &= (k_1 \cdot \theta'(k_2) \cdot f_{h_1,h_2}, h_1 + \gamma h_2) \end{aligned} \tag{5}$$

where $\theta' := \phi_{h_1} \circ \theta \in \mathrm{Aut}(K)$, and f_{h_1,h_2} depends only on h_1, h_2.

DEFINITION 3.2. For any $A \subseteq G$, consider A as a subset of $K \times \mathbb{F}_{p^n}$. Define

$$A^1 := \{k \in K \mid \text{there exists } h \in \mathbb{F}_{p^n} \text{ such that } (k, h) \in A\},$$
$$A^2 := \{h \in \mathbb{F}_{p^n} \mid \text{there exists } k \in K \text{ such that } (k, h) \in A\}.$$

In other words, A^1 is the collection of first coordinates of A and A^2 is the collection of second coordinates of A when A is written as a subset of $K \times \mathbb{F}_{p^n}$.

DEFINITION 3.3. Put $a = |A|$ and $b = |B|$. Let $A^2 = \{h_1, \ldots, h_\alpha\}$ and $B^2 = \{h'_1, \ldots, h'_\beta\}$. Then define $A_i = \{(k, h) \in A \mid h = h_i\}$, $1 \le i \le \alpha$, and write $a_i = |A_i|$. Order the h_i's so that $a_1 \ge \cdots \ge a_\alpha$. Construct $B_1, \ldots, B_\beta$ in a similar manner so that $B_j = \{(k, h) \in B \mid h = h'_j\}$, $b_j = |B_j|$, and $b_1 \ge \cdots \ge b_\beta$.

Note that $A = A_1 \cup \cdots \cup A_\alpha$ and $B = B_1 \cup \cdots \cup B_\beta$, hence $|A| = a = a_1 + \cdots + a_\alpha$ and $|B| = b = b_1 + \cdots + b_\beta$.

The following lemmas and remarks will be the last pieces in equipping us to establish the desired theorem.

LEMMA 3.4. *If* $h_i \neq h'_j$, *then*

$$|A_i \overset{\theta}{\cdot} B_j| = |(A_i)^1 \cdot \theta'((B_j)^1)|.$$

If $h_i = h'_j$, *then*

$$|A_i \overset{\theta}{\cdot} B_j| = |(A_i)^1 \overset{\theta'}{\cdot} (B_j)^1|,$$

where $\theta' = \phi_{h_i} \circ \theta$.

Proof. Regarding the first equality, by Definition 1.7, Remark 3.1, and noting that $h_i \neq h'_j$, we have

$$\begin{aligned}|A_i \overset{\theta}{\cdot} B_j| &= |\{a_i \cdot \theta(b_j) \mid a_i \in A_i,\, b_j \in B_j,\, a_i \neq b_j\}| \\ &= |\{(k_i, h_i) \star \theta(k_j, h'_j) \mid k_i \in A_i^1,\, k_j \in B_j^1\}| \\ &= |\{k_i \cdot \theta'(k_j) \cdot f_{h_i,h'_j}, h_i + \gamma h'_j\}|.\end{aligned}$$

Since h_i and h'_j are fixed elements, $f_{h_i,h_j} \in K$ is fixed. But multiplication by an element of K is a bijection on K. Likewise, since ϕ_{h_i} is conjugation by h_i, $\theta' = \phi_{h_i} \circ \theta$ is a fixed automorphism of K. Hence

$$|A_i \overset{\theta}{\cdot} B_j| = |\{k_i \cdot \theta'(k_j) \mid k_i \in A_i^1,\, k_j \in B_j^1\}| = |(A_i)^1 \cdot \theta'(B_j^1)|.$$

As for the second equality, again by Definition 1.7, Remark 3.1, and our observation regarding θ' we have

$$\begin{aligned}|A_i \overset{\theta}{\cdot} B_j| &= |\{a_i \cdot \theta(b_j) \mid a_i \in A_i,\, b_j \in B_j,\, a_i \neq b_j\}| \\ &= |\{(k_i, h_i) \star \theta(k_j, h_i) \mid k_i \in A_i^1,\, k_j \in B_j^1,\, k_i \neq k_j\}| \\ &= |\{(k_i \cdot \theta'(k_j) \cdot f_{h_i,h_i}, h_i + \gamma h_i) \mid k_i \neq k_j\}| \\ &= |\{k_i \cdot \theta'(k_j) \mid k_i \neq k_j\}| = |A_i^1 \overset{\theta'}{\cdot} B_j^1|. \ \blacksquare\end{aligned}$$

Since we have introduced $\theta' = \phi_h \circ \theta$ we address the following:

Lemma 3.5. *For G a group of odd order, if θ has odd order in* $\mathrm{Aut}(G)$ *then θ' has odd order in* $\mathrm{Aut}(K)$.

Proof. We first establish that $\theta' \in \mathrm{Aut}(K)$. By Theorem 2.2, $\theta(K) = K$ and θ is an isomorphism, therefore $\theta \in \mathrm{Aut}(K)$. Moreover it is well known that for K a normal subgroup of G, conjugation by any $h \in G$ is an automorphism of K, i.e., $\phi_h \in \mathrm{Aut}(K)$. Thus $\theta' = \phi_h \circ \theta \in \mathrm{Aut}(K)$. As well we establish that since $\mathrm{Inn}(G) := \{\phi_h \mid h \in G\} \cong G/Z(G)$ and since $|G|$ is odd, $|\mathrm{Inn}(G)|$ must be odd.

Suppose $\theta^r = 1$ in $\mathrm{Aut}(G)$ where r is odd. Then $\theta^r = 1$ in $\mathrm{Aut}(G)/\mathrm{Inn}(G)$. But θ and θ' give rise to the same element of $\mathrm{Aut}(G)/\mathrm{Inn}(G)$, so $\theta'^r = 1$ in $\mathrm{Aut}(G)/\mathrm{Inn}(G)$. Thus $\theta'^r \in \mathrm{Inn}(G)$ and so by Lagrange's Theorem, $\theta'^{rs} = 1$ in $\mathrm{Aut}(G)$ where $s = |\mathrm{Inn}(G)|$. But then $\theta'^{rs} = 1$ as an element of $\mathrm{Aut}(K)$ and rs is odd, so θ' has odd order in $\mathrm{Aut}(K)$. $\blacksquare$

We also require the following generalization of the polynomial method [2] due to Hao Pan and Zhi-Wei Sun [20].

Lemma 3.6 (The polynomial method). *Suppose A and B are nonempty subsets of $\mathbb{F}_{p^n}$. Fix $\gamma \in \mathbb{F}_{p^n}^\times$. Then $|A \overset{\gamma}{+} B| \geq \min\{p - \delta, |A| + |B| - 3\}$, where $A \overset{\gamma}{+} B := \{a + \gamma b \mid a \in A,\, b \in B,\, a \neq b\}$ and where $\delta = 1$ if $\gamma = -1$ and $\delta = 0$ otherwise.*

REMARK 3.7. Assume $p - \delta_\gamma \geq \alpha + \beta - 3$ where $\delta_\gamma = 1$ if $\gamma = -1$ and $\delta_\gamma = 0$ otherwise.

CASE 1: Suppose that there does not exist an j such that $h'_j = h_1$, i.e., the second coordinates of the B_j's will be distinct from A_1^2.

The set $\{h_1 + \gamma h'_j \mid 1 \leq j \leq \beta\}$ will have β elements. But $A^2, B^2 \subseteq \mathbb{F}_{p^n}$, hence by Lemma 3.6 and Theorem 2.2, $|A^2 \overset{\gamma}{+} B^2| \geq \alpha + \beta - 3$. Thus there are at least $\alpha - 3$ elements of the form $h_i + \gamma h'_j$, $h_i \neq \gamma h'_j$, that are not in the set $\{h_1 + \gamma h'_j \mid 1 \leq j \leq \beta\}$.

CASE 2: Now suppose that there does exist an r such that $h'_r = h_1$, i.e., some second coordinate of the B_j's will be the same as A_1^2.

Hence the set $\{h_1 + \gamma h'_j \mid h_1 \neq h'_j\}$ will have $\beta - 1$ elements. But $A^2, B^2 \subseteq \mathbb{F}_{p^n}$, hence by Lemma 3.6 and Theorem 2.2, $|A^2 \overset{\gamma}{+} B^2| \geq \alpha + \beta - 3$. Thus, since $\alpha + \beta - 3 = (\beta - 1) + (\alpha - 2)$, there are at least $\alpha - 2$ elements of the form $h_i + \gamma h'_j$, $h_i \neq h'_j$ not in the set $\{h_1 + \gamma h'_j \mid h_1 \neq h'_j\}$.

REMARK 3.8. Assume that $p - \delta_\gamma \geq \alpha + \beta - 1$ where $\delta_\gamma = 1$ if $\gamma = -1$ and $\delta_\gamma = 0$ otherwise. The set $\{(A_1 \cdot \theta(B_j))^2 \mid 1 \leq j \leq \beta\} = \{h_1 + \gamma h_j \mid 1 \leq j \leq \beta\}$ will have β elements. But $A^2, B^2 \subseteq \mathbb{F}_{p^n}$, hence by Theorem 1.4 $|A^2 + \gamma B^2| \geq \alpha + \beta - 1$. Thus, since $\alpha + \beta - 1 = \beta + (\alpha - 1)$, there are at least $\alpha - 1$ elements $h_i + \gamma h'_j$ that are not in the set $\{h_1 + \gamma h'_j \mid 1 \leq j \leq \beta\}$.

And lastly,

REMARK 3.9. For G a finite solvable group with a normal subgroup K we have $p(K) \geq p(G)$ and $p \geq p(G)$ where the p is the characteristic of the field in Theorem 2.2.

Proof. By Remark 1.3, $p(G)$ is the smallest prime factor of $|G|$. Since $K \leq G$, by Lagrange's Theorem, $|K| \,|\, |G|$, thus $p(K) \geq p(G)$. Likewise, G/K is of order p^n, thus $p \geq p(G)$. ∎

Before continuing, we define the following generalizations of the δ_γ from the polynomial method.

DEFINITION 3.10. For $\theta \in \mathrm{Aut}(G)$, put

$$\delta_\theta = \begin{cases} 1 & \text{if } \theta \text{ has even order in } \mathrm{Aut}(G), \\ 0 & \text{if } \theta \text{ has odd order in } \mathrm{Aut}(G). \end{cases}$$

Likewise, put

$$\delta_{\theta'} = \begin{cases} 1 & \text{if } \theta' \text{ has even order in } \mathrm{Aut}(K), \\ 0 & \text{if } \theta' \text{ has odd order in } \mathrm{Aut}(K), \end{cases}$$

where $\theta' = \phi_{h_i} \circ \theta$ with ϕ_{h_i} representing conjugation by h_i.

Hence by Lemma 3.5, $\delta_{\theta'} \leq \delta_\theta$, we have

Corollary 3.11.

$$p(G) - \delta_\theta \leq p(K) - \delta_{\theta'}. \ \blacksquare$$

Now we may state and prove the main result of this section.

Theorem 3.12 (Solvable Erdős–Heilbronn). *Suppose $A, B \subseteq G$, G solvable of order n, with $|A| = a$, $|B| = b$, $a, b > 0$, and $\theta \in \mathrm{Aut}(G)$. Then $|A \overset{\theta}{\cdot} B| \geq \min\{p(G) - \delta_\theta, a + b - 3\}$ where $\delta_\theta = 1$ if θ is of even order in $\mathrm{Aut}(G)$ and $\delta_\theta = 0$ otherwise.*

Proof. We will proceed by induction on n, namely we will assume the theorem holds for solvable groups of order less than n (note that the base case is trivial in that if $|G| = 1$, then $A = B = G$ and thus $a + b - 3 < 0$ whereas $A \overset{\theta}{\cdot} B$ is empty). We know that there exists a $K \trianglelefteq G$ such that $G/K \cong \mathbb{F}_{p^n}$. We may assume that $p - \delta_\theta \geq a + b - 3$, otherwise we may replace A and B by an $A^* \subseteq A$ and a $B^* \subseteq B$ such that this holds. We will express A and B as in Definition 3.3 and since $|A \overset{\theta}{\cdot} B| = |B^{-1} \overset{\theta^{-1}}{\cdot} A^{-1}|$ and θ and θ^{-1} give rise to the same K and δ_θ, without loss of generality we choose A and B such that $\beta \geq \alpha$.

We further note that $\delta_\gamma = 1$ implies that $\delta_\theta = 1$ (if $\overline{\theta}$ is multiplication by $\gamma = -1$, then $\overline{\theta}$ has order 2, so θ has even order). Hence $\alpha + \beta - 3 \leq |A| + |B| - 3 \leq p(G) - \delta_\theta \leq p - \delta_\gamma$ where the last inequality follows from Remark 3.9.

Case 1: There does not exist a j, $1 \leq j \leq \beta$, such that $A_1^2 = B_j^2$, i.e., the second coordinates of the B_j's are distinct from the second coordinate of A_1.

Together with Remark 3.7 we get (since there are at least $\alpha - 3$ nonempty disjoint sets $A_i \overset{\theta}{\cdot} B_j$, $1 < i \leq \alpha$, $1 \leq j \leq \beta$, disjoint from all $A_1 \overset{\theta}{\cdot} B_j$, i.e., there are $\alpha - 3$ second coordinates that come from these sets)

$$|A \overset{\theta}{\cdot} B| \geq |A_1 \overset{\theta}{\cdot} B_1| + |A_1 \overset{\theta}{\cdot} B_2| + \cdots + |A_1 \overset{\theta}{\cdot} B_\beta| + \alpha - 3.$$

By Case 1 of Lemma 3.4, we have

$$|A \overset{\theta}{\cdot} B| \geq |A_1^1 \cdot \theta'(B_1^1)| + |A_1^1 \cdot \theta'(B_2^1)| + \cdots + |A_1^1 \cdot \theta'(B_\beta^1)| + \alpha - 3.$$

Thus by Theorem 1.4,

$$\begin{aligned} |A \overset{\theta}{\cdot} B| &\geq (a_1 + b_1 - 1) + (a_1 + b_2 - 1) + \cdots + (a_1 + b_\beta - 1) + \alpha - 3 \\ &\geq \beta a_1 + b_1 + b_2 + \cdots + b_\beta - \beta + \alpha - 3 \\ &= \alpha a_1 + b + (\beta - \alpha)(a_1 - 1) - 3 \\ &\geq a + b - 3, \end{aligned}$$

since $\alpha a_1 = a_1 + \cdots + a_1 \geq a_1 + a_2 + \cdots + a_\alpha = a$, $\beta \geq \alpha$, and $a_1 \geq 1$.

Note that the above holds as long as each $a_1 + b_i - 1 \leq p(K) - \delta_{\theta'}$. If this is not true for some i, then

$$\begin{aligned} |A \overset{\theta}{\cdot} B| \geq |A_1 \overset{\theta}{\cdot} B_i| &\geq p(K) - \delta_{\theta'} \\ &\geq p(G) - \delta_\theta \quad \text{(by Corollary 3.11)} \\ &\geq a + b - 3 \quad \text{(by assumption).} \end{aligned}$$

Case 2: There exists a j, $1 \leq j \leq \beta$, such that $A_1^2 = B_j^2$, i.e., some B_j has a second coordinate that agrees with the second coordinate of A_1.

First we note that by Remark 3.8 there exists a set I of pairs (i, m) with $h_i + \gamma h'_m$ distinct and not equal to any $h_1 + \gamma h'_j$. Note that if $\alpha + \beta - 1 \leq p - \delta_\gamma$ then $|I| = \alpha - 1$. Hence

Subcase A: $a_1 > 1$. Then

$$|A \overset{\theta}{\cdot} B| \geq |A_1 \overset{\theta}{\cdot} B_1| + \cdots + |A_1 \overset{\theta}{\cdot} B_j| + \cdots + |A_1 \overset{\theta}{\cdot} B_\beta| + \sum_{(i,m)\in I} |A_i \overset{\theta}{\cdot} B_m|.$$

By Lemma 3.4, we have

$$\begin{aligned} |A \overset{\theta}{\cdot} B| \geq |A_1^1 \cdot \theta'(B_1^1)| + \cdots + |A_1^1 \overset{\theta'}{\cdot} B_j^1| + \cdots + |A_1^1 \cdot \theta'(B_\beta^1)| \\ + (|I| - |\{A_i \overset{\theta}{\cdot} B_m = \emptyset \mid (i,m) \in I\}|). \end{aligned}$$

But $A_i \overset{\theta}{\cdot} B_m = \emptyset$ if and only if $A_i = B_m = \{(k, h)\}$, i.e., each is a singleton. In particular, for each i this can only occur with at most one value of m. Thus if $r = |\{|A_i| = 1\}|$, then $|\{A_i \overset{\theta}{\cdot} B_m = \emptyset\}| \leq r$. Recall that if $\alpha + \beta - 1 \leq p - \delta_\gamma$ then $|I| = \alpha - 1$. Hence by the induction hypothesis on K, which is solvable and of order less than n, we get

$$\begin{aligned} |A \overset{\theta}{\cdot} B| &\geq (a_1 + b_1 - 1) + \cdots + (a_1 + b_j - 3) + \cdots + (a_1 + b_\beta - 1) \\ &\quad + (\alpha - 1 - r) \\ &\geq \beta a_1 + b_1 + \cdots + b_\beta - \beta + \alpha - 3 - r \\ &= \alpha a_1 + b + (\beta - \alpha)(a_1 - 1) - 3 - r. \end{aligned}$$

Since $\beta \geq \alpha$, $a_1 \geq 2$, and $\alpha a_1 - a = \sum_{i=1}^{\alpha} (a_1 - a_i) \geq r$, we have

$$|A \overset{\theta}{\cdot} B| \geq a + r + b - 3 - r = a + b - 3.$$

Now by assumption $a + b - 3 \leq p(G) - \delta_\theta \leq p - \delta_\gamma$, so if $\alpha + \beta - 1 > p - \delta_\gamma$, we must have $a_1 = 2$ and $a_i = 1$ for all $i > 1$, and also each $b_j = 1$. In particular, this means that

$$|A_1^1 \overset{\theta'}{\cdot} B_j^1| \geq 1 = a_1 + b_j - 2$$

and $|I| = \alpha - 2$. Hence, following the same work as above we still have that

$$|A \overset{\theta}{\cdot} B| \geq a + b - 3.$$

SUBCASE B: $a_1 = \cdots = a_\alpha = 1$ and no $A_i = B_m$. Then
$$|A \overset{\theta}{\cdot} B| \geq |A_1 \overset{\theta}{\cdot} B_1| + \cdots + |A_1 \overset{\theta}{\cdot} B_j| + \cdots + |A_1 \overset{\theta}{\cdot} B_\beta| + \sum_{(i,m)\in I} |A_i \overset{\theta}{\cdot} B_m|.$$

By Lemma 3.4, we have

$$|A \overset{\theta}{\cdot} B| \geq |A_1^1 \cdot \theta'(B_1^1)| + \cdots + |A_1^1 \overset{\theta'}{\cdot} B_j^1| + \cdots + |A_1^1 \cdot \theta'(B_\beta^1)| + |I| - |\{A_i = B_m\}| = (*). \tag{6}$$

Since $|A_1| = 1$,

$$(*) = b_1 + \cdots + (b_j - 1) + \cdots + b_\beta + |I| = b + |I| - 1. \tag{7}$$

We may have $\alpha + \beta - 1 \geq |A| + |B| - 3$. Unfortunately, this means that we have three further subcases.

SUBCASE B.1: $\alpha + \beta - 1 \leq |A| + |B| - 3$. From our observation in Subcase A, we have $|I| = \alpha - 1$. But $a = \sum_{i=1}^{\alpha} a_i = \alpha$, so
$$|A \overset{\theta}{\cdot} B| \geq b + |I| - 1 = a + b - 2.$$

SUBCASE B.2: $\alpha + \beta - 1 = |A| + |B| - 2$. Here $|I| \geq \alpha - 2 = a - 2$. Hence
$$|A \overset{\theta}{\cdot} B| \geq b + |I| - 1 \geq a + b - 3.$$

SUBCASE B.3: $\alpha + \beta - 1 = |A| + |B| - 1$. In this situation $b_j = 1$ for every j. Also $|I| \geq \alpha - 3 = a - 3$. Moreover, $|A_1^1 \overset{\theta'}{\cdot} B_j^1| \geq 1 = b_j$ since $A_i^1 \neq B_j^1$. Hence continuing (6) we obtain
$$|A \overset{\theta}{\cdot} B| \geq b_1 + \cdots + b_j + \cdots + b_\beta + |I| \geq a + b - 3.$$

SUBCASE C: $a_1 = \cdots = a_\alpha = 1$ and there exist i and m such that $A_i = B_m$. Without loss of generality, let A_1 be one such A_i, namely $A_1 = B_s$. As well we note that by Remark 3.7, Case 2, we have a set J of pairs (i, m) with $h_i + \gamma h'_m$ distinct, $h_i \neq h'_m$ and $h_i + \gamma h'_m$ not equal to any $h_1 + \gamma h'_s$ and $|J| = \alpha - 2$. Hence

$$|A \overset{\theta}{\cdot} B| \geq |A_1 \overset{\theta}{\cdot} B_1| + \cdots + |A_1 \overset{\theta}{\cdot} B_{s-1}| + |A_1 \overset{\theta}{\cdot} B_{s+1}| + \cdots + |A_1 \overset{\theta}{\cdot} B_\beta| + \sum_{(i,m)\in J} |A_i \overset{\theta}{\cdot} B_m|.$$

By Remark 3.7, Case 2,

$$|A \overset{\theta}{\cdot} B| \geq b_1 + \cdots + b_{s-1} + b_{s+1} + \cdots + b_\beta + \alpha - 2 = b - 1 + \alpha - 2 = a + b - 3. \ \blacksquare$$

4. The Erdős–Heilbronn conjecture for finite groups. We now extend Theorem 3.12 to all finite groups. Before we continue, we recall

THEOREM 4.1 (Feit–Thompson [13]). *Every group of odd order is solvable.*

THEOREM 4.2 (Generalized Erdős–Heilbronn for finite groups). *Let G be a finite group, $\theta \in \mathrm{Aut}(G)$, and let $A, B \subseteq G$ with $|A| = a$ and $|B| = b$, $a, b > 0$. Then $|A \overset{\theta}{\cdot} B| \geq \min\{p(G) - \delta, a + b - 3\}$ where $\delta = 1$ if θ is of even order in $\mathrm{Aut}(G)$ and $\delta = 0$ otherwise.*

Proof. We first consider the case when G is of even order, hence $p(G) = 2$. If $a = 1$ or 2, then $|A \overset{\theta}{\cdot} B| \geq |B| - 1 > a + b - 3$. For $a \geq 3$, $|A \overset{\theta}{\cdot} B| \geq |A| - 1 \geq 2 = p(G)$. Lastly, if G is of odd order, then by Theorem 4.1, G is solvable. The result then follows from Theorem 3.12. ∎

5. Closing remarks. Of course, Alon, Nathanson, and Ruzsa's work [1] established the Erdős–Heilbronn problem for elementary abelian groups. As noted earlier, Gyula Károlyi used different techniques to extend the Erdős–Heilbronn problem to abelian groups for the case $A = B$ in 2004 [15] and to cyclic groups of prime power order in 2005 [17]. Our result completes these results in establishing the general case of the Erdős–Heilbronn problem for any finite abelian group. Moreover, we note the extent of the comprehensiveness of the result; in particular, establishing this theorem required using the techniques of Károlyi together with the polynomial method of Alon, Nathanson, and Ruzsa.

Acknowledgements. The authors wish to thank Gyula Károlyi for introducing us to this problem. As well we wish to thank Zhi-Wei Sun for alerting us to a significant oversight in the original version of one of our proofs. We especially wish to thank the referee for a helpful recommendation which shortened a proof, for providing us with a list of inaccuracies, and, in particular, for a very careful reading of our paper.

References

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

[2] —, —, —, *The polynomial method and restricted sums of congruence classes*, J. Number Theory 56 (1996), 404–417.

[3] P. Balister and J. P. Wheeler, *The Cauchy–Davenport theorem for finite groups*, preprint, http://jeffreypaulwheeler.com/, 2006.

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

[5] I. Chowla, *A theorem on the addition of residue classes: application to the number $\Gamma(k)$ in Waring's problem*, Proc. Indian Acad. Sci. Sect. A 1 (1935), 242–243.

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

[7] —, *A historical note*, ibid. 22 (1947), 100–101.

[8] J. A. Dias da Silva and Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. London Math. Soc. 26 (1994), 140–146.
[9] P. Erdős, *On the addition of residue classes mod p*, in: Proc. 1963 Number Theory Conference at the Univ. of Colorado, Univ. of Colorado Press, 1963, 16–17.
[10] —, *Some problems in number theory*, in: Computers in Number Theory, A. O. L. Atkin and B. J. Birch (eds.), Academic Press, 1971, 405–414.
[11] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Monogr. Enseign. Math. 28, Univ. de Genève, 1980.
[12] P. Erdős and H. Heilbronn, *On the addition of residue classes mod p*, Acta Arith. 9 (1964), 149–159.
[13] W. Feit and J. Thompson, *Solvability of groups of odd order*, Pacific J. Math. 13 (1963), 775–1029.
[14] G. Károlyi, *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] —, *The Cauchy–Davenport theorem in group extensions*, Enseign. Math. 51 (2005), 239–254.
[17] —, *A compactness argument in the additive theory and the polynomial method*, Discrete Math. 302 (2005), 124–144.
[18] V. F. Lev, *Restricted set addition in groups II. A generalization of the Erdős–Heilbronn conjecture*, Electron. J. Combin. 7 (2000), Research paper R4, 10 pp.
[19] M. B. Nathanson, *Additive Number Theory*, *Inverse Problems and the Geometry of Subsets*, Springer, 1996.
[20] H. Pan and Z.-W. Sun, *A lower bound for* $|\{a+b : a \in A, b \in B, P(a,b) \neq 0\}|$, J. Combin. Theory Ser. A 100 (2002), 387–393.

Department of Mathematical Sciences
University of Memphis
Memphis, TN 38152, U.S.A.
E-mail: pbalistr@memphis.edu

Department of Mathematics
University of Pittsburgh
Pittsburgh, PA 15260, U.S.A.
E-mail: jpw41@pitt.edu

Received on 9.11.2006
and in revised form on 12.6.2009 (5318)