SUM-PRODUCT ESTIMATES

BEN GREEN

Abstract. Notes on the sum-product estimates of Bourgain-Katz-Tao and Bourgain-Konyagin.

1. introduction

The aim of these notes is to give a self-contained proof of the sum-product estimates of Bourgain, Katz, Tao and Konyagin. Specifically we will establish:

Theorem 1.1. *Suppose that p is a prime, and that $A \subseteq \mathbb{F}_p \setminus \{0\}$ is a set with $|A| \leqslant p^{1-\delta}$. Then there is an absolute constant $c = c(\delta) > 0$ such that we have the estimate*

$$|A + A| + |A \cdot A| \geqslant c|A|^{1+c}.$$

2. The Balog-Szemerédi-Gowers theorem

The first three sections are devoted to proving Proposition 4.4. This proposition shows that if $|A + A|$ and $|A \cdot A|$ are both small then, after passing to a largeish subset of A, we may control more complicated algebraic expressions too.

Let A be a subset of an abelian group, written additively. We write $M^+(A)$ for the number of *additive quadruples* in A, that is to say quadruples $(a_1, a_2, a_3, a_4) \in A^4$ such that $a_1 - a_2 = a_3 - a_4$. If A is a subset of some abelian group written multiplicatively, then we write $M^\times(A)$ for the number of solutions to $a_1/a_2 = a_3/a_4$. A very simple application of the Cauchy-Schwarz inequality serves to establish that if A has small doubling, then $M^+(A)$ is large.

Lemma 2.1. *Suppose that A is a subset of an abelian group with $|A| = N$, and that $|A+A| \leqslant K|A|$. Then $M^+(A) \geqslant K^{-1}N^3$. Similarly, suppose that $|A\cdot A| \leqslant K|A|$. Then $M^\times(A) \geqslant K^{-1}N^3$.*

Proof. We have

$$M^+(A) = \sum_x 1_A * 1_A(x)^2 \geqslant |A + A|^{-1}\Big(\sum_x 1_A * 1_A(x)\Big)^2 = \frac{N^4}{|A + A|}. \qquad \square$$

The converse inequality does not hold: there are sets with large $M^+(A)$ which also have very large doubling (take A to be the union of an arithmetic progression of length $N/2$ and $N/2$ random points, for example). There is, however, a very useful result of Balog and Szemerédi which *does* provide a converse, so long as one is prepared to pass to a subset of A.

The author is a Clay Research Fellow, and is pleased to acknowledge the support of the Clay Mathematics Institute. These are lecture notes for a course taught at MIT in Autumn 2005.

Lemma 2.2 (Gowers)**.** *Suppose that $|A| = N$ and that $M^+(A) = \alpha N^3$. Then there is a set $A' \subseteq A$, $|A'| \geqslant \alpha N/8$, such that for all $a_1', a_2' \in A'$ there are at least $2^{-29}\alpha^{11}N^7$ solutions to the equation*

$$a_1' - a_2' = x_1 - x_2 + x_3 - x_4 + x_5 - x_6 + x_7 - x_8$$

with $x_i \in A$.

Proof. (following Gowers [4], with variation due to Chang [3]). We construct a graph $\Gamma = (V, E)$, the *popular difference graph* of A, as follows. We set $V := A$ and join a_1 to a_2 if the number of solutions to $a_1 - a_2 = a_3 - a_4$ with $a_3, a_4 \in A$ is at least $\alpha N/2$. Now we have

$$\alpha N^3 = M^+(A) = \sum_{a_1,a_2} 1_A * 1_{-A}(a_1 - a_2) \leqslant N|E(\Gamma)| + \frac{1}{2}\alpha N^3,$$

and so

$$|E(\Gamma)| \geqslant \alpha N^2/2. \tag{2.1}$$

We will be interested in the neighbourhoods of vertices in Γ. Thus for $x \in V$ define

$$N(x) := \{y \in V : xy \in E(\Gamma)\}.$$

Set $\delta := 2^{-11}\alpha^3$. We say that a pair $(a_1, a_2) \in A^2$ is *unfriendly* if

$$|N(a_1) \cap N(a_2)| \leqslant \delta N.$$

Claim. There is some $a^* \in A$ such that $|N(a^*)| \geqslant \alpha N/4$, and such that at least 95 percent of the pairs $(x_1, x_2) \in N(a^*)^2$ are friendly.

Proof. Fix an unfriendly pair $(a_1, a_2) \in A^2$. The number of t for which $a_1, a_2 \in N(t)$ is then precisely $|N(a_1) \cap N(a_2)|$, which by definition is at most δN. Thus if $t \in A$ is selected at random, the probability that $(a_1, a_2) \in N(t)^2$ is δ. Writing $f(t)$ for the number of unfriendly pairs in $N(t)^2$, we therefore have

$$\mathbb{E}_{t\in A} f(t) \leqslant \delta N^2.$$

Now we also have

$$\mathbb{E}_{t\in A}|N(t)| = N^{-1}|E(\Gamma)| \geqslant \alpha N/2.$$

Therefore, in view of the choice of δ, we have

$$\mathbb{E}_{t\in A}\big(|N(t)| - \frac{320}{\alpha^2 N} f(t)\big) \geqslant \alpha N/4.$$

Choose a particular value of a^* for which

$$|N(a^*)| - \frac{320}{\alpha^2 N} f(a^*) \geqslant \alpha N/4.$$

Certainly, then, we have

$$|N(a^*)| \geqslant \alpha N/4;$$

furthermore, we have

$$f(a^*) \leqslant \alpha^2 N^2/320 \leqslant \frac{1}{20}|N(a^*)|^2.$$

This proves the claim. □

Now it is easy to see that for at least 1/2 of all $a \in N(a^*)$, at least 90 percent of $x \in N(a^*)$ are such that (a, x) is friendly. Define A' to be the set of such a, and suppose

that $a_1', a_2' \in A'$. Then for at least 80 percent of $w \in N(a^*)$, both of the pairs (a_1', w) and (a_2', w) are friendly. This means, by definition, that

$$|N(a_1') \cap N(w)| \geqslant \delta N$$

and

$$|N(a_2') \cap N(w)| \geqslant \delta N.$$

There are, therefore, at least $\alpha\delta^2 N^3/8$ choices of a triple (w, b_1, b_2) such that all of $a_1'b_1$, b_1w, wb_2 and b_2a_2' lie in Γ. For each such triple there are (by definition of Γ) at least $(\alpha N/2)^4$ solutions to the system of equations

$$\begin{aligned} a_1' - b_1 &= x_1 - x_2 \\ b_1 - w &= x_3 - x_4 \\ w - b_2 &= x_5 - x_6 \\ b_2 - a_2' &= x_7 - x_8. \end{aligned}$$

Summing these equations, we obtain

$$a_1' - a_2' = x_1 - x_2 + x_3 - x_4 + x_5 - x_6 + x_7 - x_8$$

in at least $2^{-29}\alpha^{11}N^7$ ways. □

Chang [3] in fact obtains slightly better bounds by refining the notion of "popular difference", working on dyadic ranges where $1_A * 1_{-A}$ is roughly constant.

Corollary 2.3 (Balog-Szemerédi-Gowers)**.** *Suppose that A is a subset of an abelian group with $|A| = N$, and that $M^+(A) = \alpha N^3$. Then there is a set $A' \subseteq A$, $|A'| \geqslant \alpha N/8$, such that $|A' - A'| \leqslant 2^{32}\alpha^{-12}|A'|$.*

Proof. Simply take the set A' constructed above. To each element $x = a_1' - a_2' \in A' - A'$ is associated at least $2^{-29}\alpha^{11}N^7$ octuples $(x_1, \dots, x_8) \in A^8$ such that $a_1' - a_2' = x_1 - \cdots - x_8$. Clearly, then, $|A' - A'| \leqslant 2^{29}\alpha^{-11}N$. □

3. Bounding the algebra generated by A

In this section and the next we work in an arbitrary field k. Only in the final section will the specific properties of $\mathbb{F}_p$ come to the fore. Now the knowledge that $|A+A|, |A \cdot A| \leqslant K|A|$ is not in itself enough to prove Theorem 1.1. In this section we use the Balog-Szemerédi-Gowers theorem to show that after passing to a subset $A'' \subseteq A$ we may assume that more complicated algebraic expressions are also small.

Proposition 3.1. *Suppose that $A \subseteq k$ and that $|A + A|, |A \cdot A| \leqslant K|A|$. Then there is some $A'' \subseteq A$ with $|A''| \gg K^{-C}|A|$ such that $|A'' \cdot A'' - A'' \cdot A''| \ll K^C|A|$.*

Proof. Write $N := |A|$. We may assume (after adjusting constants slightly) that $0 \notin A$. From Lemmas 2.1 and 2.2, we may find a subset $A' \subseteq A$ with $|A'| \gg N/K$ such that for each pair $(a_1', a_2') \in A'^2$ there are $\gg K^{-11}N^7$ solutions to the equation

$$a_1' - a_2' = a_1 - a_2 + a_3 - a_4 + a_5 - a_6 + a_7 - a_8.$$

Multiplying though by an arbitrary element of $A \cdot A \cdot A \cdot A \cdot A / A \cdot A \cdot A \cdot A$, we see that if

$$x \in X := \frac{(A' - A')A \cdot A \cdot A \cdot A \cdot A}{A \cdot A \cdot A \cdot A}$$

then there are $\gg K^{-11}N^7$ solutions to the equation

$$x = b_1 - b_2 + b_3 - b_4 + b_5 - b_6 + b_7 - b_8$$

with

$$b_i \in B := \frac{A \cdot A \cdot A \cdot A \cdot A \cdot A}{A \cdot A \cdot A \cdot A}.$$

Note that from the multiplicative form of the Plünnecke-Ruzsa inequalities we have

$$|B| \leqslant K^{10}N.$$

It follows, then, that

$$|X| \ll K^{91}N. \tag{3.1}$$

We now refine A' multiplicatively. Noting that

$$|A' \cdot A'| \leqslant |A \cdot A| \leqslant KN \leqslant 8K^2|A'|,$$

we may apply the multiplicative form of Lemmas 2.1 and 2.2 to obtain a further refinement $A'' \subseteq A'$, $|A''| \gg K^{-3}N$, such that for any pair $(a_1'', a_2'') \in A''$ there are $\gg K^{-22}N^7$ solutions to the equation

$$\frac{a_1''}{a_2''} = \frac{a_1'a_2'a_3'a_4'}{a_5'a_6'a_7'a_8'} \tag{3.2}$$

with $a_i' \in A'$.

Pick an arbitrary further pair of elements a_3'', a_4''. Then we have

$$a_1''a_4'' - a_2''a_3'' = \frac{a_1'a_2'a_3'a_4'a_2''a_4'' - a_3''a_2''a_5'a_6'a_7'a_8'}{a_5'a_6'a_7'a_8'}.$$

This may be written as

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6,$$

where

$$\begin{aligned}
a_5'a_6'a_7'a_8'x_1 &= a_1'a_2'a_3'a_4'a_2''(a_4'' - a_8'),\\
a_5'a_6'a_7'a_8'x_2 &= a_1'a_2'a_3'a_4'(a_2'' - a_7')a_8',\\
a_5'a_6'a_7'a_8'x_3 &= a_1'a_2'a_3'(a_4' - a_6')a_7'a_8',\\
a_5'a_6'a_7'a_8'x_4 &= a_1'a_2'(a_3' - a_5')a_6'a_7'a_8',\\
a_5'a_6'a_7'a_8'x_5 &= a_1'(a_2' - a_3'')a_5'a_6'a_7'a_8'
\end{aligned}$$

and

$$a_5'a_6'a_7'a_8'x_6 = (a_1' - a_2'')a_3''a_5'a_6'a_7'a_8'.$$

Observe that each x_i lies in the set X which we defined earlier, and whose cardinality is bounded by (3.1). Regarding the a_i'' as fixed, one may use (3.2) and simple algebra to recover, in turn, the six quantities $a_8', a_7', a_6'/a_4', a_5'/a_3', a_2'$ and a_1' from a knowledge of the x_i. Thus the map

$$(a_1', a_2', a_3', a_4', a_5', a_6', a_7', a_8') \to (x_1, x_2, x_3, x_4, x_5, x_6)$$

is at most N^2-to-one, which means that there are $\gg K^{-22}N^5$ sextuples $(x_1, \dots, x_6) \in X^6$ so that

$$a_1''a_4'' - a_2''a_3'' = x_1 + x_2 + x_3 + x_4 + x_5 + x_6.$$

It follows from (3.1) that

$$|A'' \cdot A'' - A'' \cdot A''| \ll K^{568}N,$$

as required. □

4. The algebra generated by A

In this section we show (quoting almost verbatim from [1]) that if k is a field and if $A \subseteq k$ is a set with $|A \cdot A - A \cdot A| \leqslant K|A|$, then in fact A is almost closed under much more complicated algebraic operations too.

Proposition 4.1. *Suppose that k is a field and that $A \subseteq k$ is a set with $|A \cdot A - A \cdot A| \leqslant K|A|$. Let P be any multivariable polynomial with integer coefficients. Then there is some constant $C(P)$ such that*

$$|P(A, A, \dots, A)| \ll_P K^{C(P)}|A|.$$

Let A, B be two sets in k. Then we write $A \Subset B$ if there is an absolute constant C together with a set $X \subseteq k$, $|X| \leqslant CK^C$, such that $A \subseteq X + B$. The following lemma[1], known as Ruzsa's Covering Lemma, gives a supply of situations like this.

Lemma 4.2. *Let A and B be subsets of k such that either $|A + B| \leqslant CK^C|A|$ or $|A - B| \leqslant CK^C|A|$. Then $B \Subset A - A$.*

Proof. By symmetry we may assume that $|A + B| \leqslant CK^C|A|$. Let X be a maximal subset of B with the property that the sets $\{x + A : x \in X\}$ are all disjoint. Since these sets $x+A$ all have cardinality $|A|$ and are all contained in $A+B$ we have $|X||A| \leqslant |A+B|$, and hence $|X| \leqslant CK^C$. Since the set X is maximal, we see that for every $b \in B$, the set $b + A$ must intersect $x + A$ for some $x \in X$. Thus $b \in x + A - A$, and hence $B \subseteq X + A - A$ as desired. □

We say that an element $x \in k$ *good* if we have $x \cdot A \Subset A - A$.

Proposition 4.3. *Every element of A is good. If x and y are good then $x + y$, $x - y$ and xy are all good.*

Remark. Note that the definition of "good" involves an absolute constant C. That constant may (and will, in fact) be larger for $x + y$ (or $x - y$, xy) than it is for x and y.

Proof. Let us first show that every element of A is good. Since $1 \in A$, we have

$$|A \cdot A - A| \leqslant |A \cdot A - A \cdot A| \leqslant K|A|$$

and hence by Lemma 4.2

$$A \cdot A \Subset A - A \tag{4.1}$$

and so indeed

$$a \cdot A \Subset A - A$$

for each $a \in A$.

Now suppose that x and y are good, so that $x \cdot A \Subset A - A$ and $y \cdot A \Subset A - A$. Then

$$(x + y) \cdot A \subseteq x \cdot A + y \cdot A \Subset A - A + A - A.$$

On the other hand, since $|A - A| \leqslant |A.A - A.A| \leqslant K|A|$, the Plünnecke-Ruzsa inequalities imply that

$$|A - A + A - A + A| \leqslant K^5|A|$$

and hence by Lemma 4.2

$$A - A + A - A \Subset A - A. \tag{4.2}$$

[1]We saw essentially this lemma when we proved Freiman's theorem in $\mathbb{F}_2^n$.

Since $\Subset$ is clearly a transitive relation, we have $(x+y)\cdot A \Subset A-A$ and hence $x+y$ is good. A very similar argument shows that $x-y$ is good.

It remains to show that xy is good. Since $x\cdot A \Subset A-A$ we have

$$xy\cdot A \Subset y\cdot A - y\cdot A.$$

But since $y\cdot A \Subset A-A$, we have

$$xy\cdot A \Subset A-A-A+A.$$

By (4.2) we conclude that xy is good. □

Proof of Proposition 4.1. Write A^m for the product of m copies of A. We now prove inductively that $A^m \Subset A-A$ for all $m=0,1,2,3,\dots$. The cases $m=0,1$ are trivial, and the case $m=2$ has already been proved in (4.1). Suppose then that $m\geqslant 3$, and that we have already proven that $A^{m-1}\Subset A-A$. Thus

$$A^{m-1}\subseteq X+A-A$$

for some set X with $|X|\leqslant CK^C$. Clearly we may assume that $X\subseteq A^{m-1}-(A-A)$, since if $x\notin A^{m-1}-(A-A)$ then $A^{m-1}\cap(x+A-A)=\emptyset$. In particular every element of X is good. We now multiply through by A to obtain

$$A^m\subseteq X\cdot A+A\cdot A-A\cdot A.$$

Since every element of X is good, and $|X|\leqslant CK^C$, we see that $X\cdot A\Subset A-A$. By (4.1) we thus have

$$A^m\Subset A-A+A-A-(A-A).$$

But by arguing as in the proof of (4.2) we have

$$A-A+A-A-(A-A)\Subset A-A.$$

Thus we have indeed proved inductively that $A^m\Subset A-A$ for all m. To conclude the proof of Proposition 4.1, simply note that from (4.2) and the transitivity of $\Subset$ we have $P(A,\dots,A)\Subset A-A$ for every multivariable polynomial P with integer coefficients. The required bound on $|P(A,\dots,A)|$ is immediate. □

We conclude this section with a corollary. This corollary will be the only result that we carry through to the final section of the paper, where Theorem 1.1 will be proved. If $A\subseteq k$ is a set then we define

$$J(A):=\big\{a_5\big(\frac{a_1a_2-a_3a_4}{a_3-a_1}+a_6\big):a_1,\dots,a_6\in A, a_1\neq a_3\big\}.$$

Proposition 4.4. *Suppose that $A\subseteq k$ satisfies $|A+A|\leqslant K|A|$ and $|A\cdot A|\leqslant K|A|$. Then there is a set $A''\subseteq A$ with $|A''|\gg K^{-C}|A|$ and $|J(A'')|\ll K^C|A|$.*

Proof. By Proposition 3.1 there is $A''\subseteq A$ with $|A''|\gg K^{-C}|A|$ and such that $|A''\cdot A''-A''\cdot A''|\ll K^C|A''|$. Note that

$$J(A'')\subseteq\frac{P(A'',\dots,A'')}{(A''-A'')\setminus\{0\}},$$

where

$$P(x_1,x_2,x_3,x_4,x_5,x_6):=x_5(x_1x_2-x_3x_4+x_3x_6-x_1x_6).$$

Note that $P(A'', \dots, A'')$ contains a homothetic copy of $A'' - A''$, since

$$x^2(a_1 - a_2) = x(xa_1 - xa_2 + xx - xx)$$

for any $x \in A''$. Thus we have

$$|J(A'')| \leqslant |X/\widetilde{X}|,$$

where

$$X := P(A'', \dots, A'')$$

and $\widetilde{X} := X \setminus \{0\}$. Now an application of Proposition 4.1 confirms that

$$|X \cdot X| \ll K^C|A''| \ll K^C|X|,$$

and so

$$|\widetilde{X} \cdot \widetilde{X}| \ll K^C|\widetilde{X}|.$$

Applying the Plünnecke-Ruzsa inequalities in $k^\times$, it follows that

$$|J(A'')| \leqslant |X/\widetilde{X}| \leqslant |\widetilde{X}/\widetilde{X}| + 1 \ll K^C|X| \ll K^C|A|,$$

as required. □

5. A lower bound for the algebra generated by A

Finally, we specialize to the case $k = \mathbb{F}_p$. Let $A \subseteq \mathbb{F}_p$; our aim in this section is to prove a lower bound for $|J(A)|$. Combined with the results of the previous section, this will easily lead to a proof of Theorem 1.1.

Proposition 5.1. *Suppose that $A \subseteq \mathbb{F}_p$. Then*

(i) *If $|A| > \sqrt{p}$ we have $|J(A)| \geqslant p/2$;*
(ii) *If $|A| \leqslant \sqrt{p}$ we have $|J(A)| \geqslant |A|^3/2|A - A|$.*

To get lower bounds for $|J(A)|$ we will use the following simple lemma. This together with later lemmas somehow encode the notion that it is not possible to find a "basis" for $\mathbb{F}_p^\times$ over A.

Lemma 5.2. *Suppose that $A \subseteq \mathbb{F}_p^\times$, and that $\xi \in \mathbb{F}_p$ is such that $|A \cdot (A + \xi)| < |A|^2$. Then*

$$A \cdot (A + \xi) \subseteq J(A).$$

Proof. Since $|A \cdot (A + \xi)| < |A|^2$ there are two pairs $(a_1, a_2) \neq (a_3, a_4)$ such that $a_1(a_2 + \xi) = a_3(a_4 + \xi)$. Clearly $a_1 \neq a_3$ and $a_2 \neq a_4$, and thus

$$\xi = \frac{a_1a_2 - a_3a_4}{a_3 - a_1}.$$

It follows immediately that for any $a_5, a_6 \in A$ we have

$$a_5(a_6 + \xi) = \frac{a_5(a_3a_6 - a_1a_6 + a_1a_2 - a_3a_4)}{a_3 - a_1} \in J(A).$$

The result follows. □

We must turn, then, to the rather strange task of finding values of ξ for which $|A \cdot (A + \xi)|$ is large, but not actually equal to $|A|^2$. The following lemma handles the "large" part of that endeavour:

Lemma 5.3. *Suppose that $A \subseteq \mathbb{F}_p^\times$. Then there is some $\xi \in \mathbb{F}_p$ such that*

$$|A \cdot (A+\xi)| \geqslant \frac{|A|^2 p}{|A|^2 + p}.$$

Proof. Write $f_\xi(s)$ for the number of representations of s as $a_1(a_2+\xi)$ with $a_1, a_2 \in A$. Note that

$$\sum_{\xi \in \mathbb{F}_p} \sum_{s \in \mathbb{F}_p} f_\xi(s)^2 = |\{(a_1,a_2,a_3,a_4,\xi) : a_1(a_2+\xi) = a_3(a_4+\xi)\}|.$$

We distinguish two types of such quintuples: those with $a_1 = a_3$ and $a_2 = a_4$, of which there are $|A|^2 p$, and those where this is not the case, of which there are at most $|A|^4$ since ξ is uniquely determined by $a_1, \dots, a_4$. Thus

$$\sum_{\xi \in \mathbb{F}_p} \sum_{s \in \mathbb{F}_p} f_\xi(s)^2 \leqslant |A|^2 p + |A|^4,$$

and so there is some $\xi \in \mathbb{F}_p$ such that

$$\sum_{s \in \mathbb{F}_p} f_\xi(s)^2 \leqslant |A|^2 + \frac{|A|^4}{p}.$$

Noting that $f_\xi(s)$ is supported on $A \cdot (A+\xi)$, the result now follows immediately from the Cauchy-Schwarz inequality:

$$|A|^2 + \frac{|A|^4}{p} \geqslant \sum_{s \in \mathbb{F}_p} f_\xi(s)^2 \geqslant \frac{1}{|A \cdot (A+\xi)|} \Big(\sum_{s \in \mathbb{F}_p} f_\xi(s) \Big)^2 = \frac{|A|^4}{|A \cdot (A+\xi)|}. \qquad \square$$

Now we say that some $\xi \in \mathbb{F}_p$ is *involved* with A if $|A \cdot (A+\xi)| < |A|^2$. Write $K := |A-A|/|A|$. As we stated, our aim is to find a ξ which is involved with A but *not very involved*, which for us will mean that $|A \cdot (A+\xi)| \geqslant |A|^2/2K$.

Lemma 5.4. *Suppose that $A \subseteq \mathbb{F}_p$ satisfies $|A| \leqslant \sqrt{p}$ and $|A-A| \leqslant K|A|$. Then there is some $\xi \in \mathbb{F}_p$ such that ξ is involved with A but not very involved, that is to say we have*

$$\frac{|A|^2}{2K} \leqslant |A \cdot (A+\xi)| < |A|^2.$$

Proof. Suppose, as a hypothesis for contradiction, that this is not the case. It is easy to see from Lemma 5.3 that there is at least one ξ which is not very involved with A, and hence by our assumption it must be not involved with A at all, i.e. $|A \cdot (A+\xi)| = |A|^2$. This means, of course, that all $|A|^2$ of the quantities $a_1(a_2+\xi)$ are distinct. Since $|A-A| \leqslant K|A|$ we see that there is some $d \neq 0$ which has at least $(|A|-1)/K > |A|/2K$ representations as $a - a'$ with $a, a' \in A$. For any a' such that $a'+d \in A$ and for any $a'' \in A$, we clearly have $a''(a'+\xi+d) \in A \cdot (A+\xi)$. It follows that

$$|A \cdot (A+\xi+d)| \geqslant |A|^2/2K,$$

and so $\xi + d$ is not very involved with A. By our assumption it cannot be involved with A at all, and so we have shown that the set

$$\Lambda = \{\xi \in \mathbb{F}_p : \xi \text{ is not involved with } A\}$$

satisfies $\Lambda = \Lambda + d$. Since $\Lambda \neq 0$, it immediately follows that $\Lambda = \mathbb{F}_p$. Clearly, however, 0 is involved with A because

$$|A \cdot A| = |A|(|A|+1)/2 < |A|^2.$$

This contradiction proves the lemma. □

Proof of Proposition 5.1. Suppose first that we are in case (i), that is $|A| > \sqrt{p}$. Then clearly *every* value of ξ is involved with A, and so in view of Lemma 5.3 there is some ξ such that

$$p/2 \leqslant |A \cdot (A+\xi)| < |A|^2.$$

The proposition follows immediately from this Lemma 5.2. For case (ii), in which $|A| \leqslant \sqrt{p}$, we may instead apply Lemma 5.4 and, of course, Lemma 5.2. □

To finish, we supply the proof of Theorem 1.1. Suppose that $A \subseteq \mathbb{F}_p$ is such that $|A+A|, |A \cdot A| \leqslant K|A|$. Then, by Proposition 4.4, there is a set $A'' \subseteq A$ with $|A''| \gg K^{-C}|A|$ and

$$|J(A'')| \ll K^C|A|.$$

Since $|A''-A''| \ll K^C|A|$, we know from Proposition 5.1 that

$$|J(A'')| \gg \min(p, K^{-C}|A|^2).$$

The result follows immediately upon comparing these two bounds. □

6. Bibliographical remarks.

Theorem 1.1 was proved in [1] for $|A| > p^\delta$. This condition was removed in [2]. Their method imported some rather algebraic tools (Stepanov's method). I observed in writing these notes that by switching the rôle of addition and multiplication in [2], or rather in an old preprint of Konyagin available on the ArXiV, the proof becomes much more elementary. That modification is presented here. The observation that Stepanov's method is not necessary to prove Theorem 1.1 was made earlier in [5], where a closely related elementary proof is given. In that book one may also find an account of the original method of [2].

7. acknowledgement

I would like to thank Vicky Neale for carefully reading these notes and for drawing my attention to a number of typographical errors.

References

[1] J. Bourgain, N. H. Katz and T. C. Tao, *A sum-product estimate in finite fields, and applications,* Geom. Funct. Anal. **14** (2004), no. 1, 27–57.
[2] J. Bourgain and S. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order,* C.R. Acad. Sci. Paris, Ser. I **337** (2003), 75–80.
[3] M.-C. Chang, *On problems of Erdős and Rudin,* J. Funct. Anal. **207** (2004), no. 2, 444–460.
[4] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four,* Geom. Funct. Anal. **8** (1998), no. 3, 529–551.
[5] T. C. Tao and V. H. Vu, *Additive combinatorics,* book in preparation.

Department of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, England
E-mail address: b.j.green@bristol.ac.uk