

4. $|A \cdot A - A \cdot A|$ SMALL IMPLIES $|P(A, \dots, A)|$ SMALL

Recall that our goal is to prove the BKT theorem, which roughly says that no finite field F of prime order has approximate subrings. The first half of the proof was to find a polynomial $P \in \mathbb{Z}[X_1, \dots, X_n]$ such that $P(A, \dots, A) = F$ for all such fields F and any reasonably sized subset $A \subseteq F$. Last week, we proved the sumset estimates, Theorem 3.3, which will help us today to control the size of $|nA - mA|$ given a good understanding of the size of $|A - A|$. This will show up again next week when we show that if F has an approximate subring A , then $|A \cdot A - A \cdot A|$ is small, too. Given this and the following Theorem, we can deduce the BKT theorem, which we shall do shortly:

Theorem 4.1. *Suppose that $A \subseteq F$ is nonempty and contains $1 \in F$. Furthermore suppose that $|A \cdot A - A \cdot A| \leq K|A|$ for some $K \geq 1$. Then*

$$|P(A, \dots, A)| \leq CK^C|A|$$

for all polynomials P and some constant C (depending only on P).

Before we begin the proof of the theorem, we need to set up some notation and prove a few preliminary results. We will say that A is **essentially contained** in B (denoted $A \Subset B$) if there is a subset $X \subseteq F$ such that $|X| \leq DK^D$ for some constant D (independent of A , B , and F) and $A \subseteq X + B$. Note that this is a transitive property: if $A \Subset B$ and $B \Subset C$, then there are X_A and X_B with $|X_A| \leq D_A K^{D_A}$ and $A \subseteq X_A + B$ (and similarly for X_B). Thus

$$A \subseteq X_A + B \subseteq X_A + X_B + C$$

but $|X_A + X_B| \leq (D_A K^{D_A})(D_B K^{D_B}) \leq D_C K^{D_C}$ for some D_C independent of A, B, C and F , so $A \Subset C$ as claimed.⁴

Now we prove another useful lemma by Ruzsa, which has a similar flavor to Lemma 1.3 and Exercise 1.2:

Lemma 4.2. *Let $A, B \subseteq F$ such that $|A + B| \leq CK^C|A|$. Then $B \Subset A - A$.*

Proof. Let $X \subseteq B$ be maximal with respect to the property that the $x + A$ are disjoint for $x \in X$. Then

$$|X||A| = \sum |x + A| = \left| \bigcup (x + A) \right| \leq |A + B|$$

by translation invariance and the fact that $X \subseteq B$. Thus X has the desired cardinality, so it remains to show that $B \subseteq X + A - A$. But the maximality of X ensures that for all $b \in B$, the sets $b + A$ and $x + A$ intersect for some $x \in X$. That is, for every b , there are $a_1, a_2 \in A$ and $x \in X$ such that $b + a_1 = x + a_2$, or $b = x + a_2 - a_1$, which is in $X + A - A$. \square

We will make another convenient definition so we don't need to keep track of pesky constants. We will say that an element $x \in F$ is **good** if $x \cdot A \Subset A - A$. Now we use Lemma 4.2 to find some good elements in F :

Proposition 4.3. *Assuming the hypotheses of Theorem 4.1:*

- (1) *All elements of A are good*
- (2) *$x, y \in F$ good $\Rightarrow x + y$ good*

⁴In order to improve readability of this text, we will suppress such detailed arguments involving constants implied by this notation. See the appendix for more details.

(3) $x, y \in F$ good $\Rightarrow xy$ good

Proof of 1. For all $a_1, a_2, a_3 \in A$, we certainly have

$$a_1 a_2 - a_3 = a_1 a_2 - a_3 \cdot 1 \in A \cdot A - A \cdot A$$

by the assumption on A . Therefore

$$|A \cdot A - A| \leq |A \cdot A - A \cdot A| \leq K|A|$$

So applying Lemma 4.2 with $B = A \cdot A$, we find that $A \cdot A \subseteq A - A$, which implies that all elements of A are good. \square

Proof of 2. Suppose that $x \cdot A \subseteq A - A$ and $y \cdot A \subseteq A - A$. Then

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

But by the hypothesis on A , we know $A \subseteq A \cdot A$, so

$$|A - A| \leq |A \cdot A - A \cdot A| \leq K|A|$$

Therefore $|A - A + A - A + A| \leq K^C|A|$ by sumset estimates (Theorem 3.3) where C is some absolute constant.⁵ Therefore, by applying Lemma 4.2 with $B = A - A + A - A$, we see that

$$(12) \quad A - A + A - A \subseteq A - A$$

Therefore, since \subseteq is transitive, $(x + y) \cdot A \subseteq A - A$ as needed. \square

Exercise 4.1. Prove part 3 of Proposition 4.3.

Exercise 4.2. Use Proposition 4.3 to show that for any polynomial $P \in \mathbb{Z}[X_1, \dots, X_n]$, all elements $x \in P(A, \dots, A)$ are good.

Now we may prove the Theorem.

Proof of Theorem 4.1. We will temporarily use the notation $A^1 := A, A^k := A^{k-1} \cdot A$. The result follows from this:

claim: $A^k \subseteq A - A$ for all $k \geq 1$.

Indeed, if this were true, then applying a similar argument to that in Exercise 4.2 yields

$$P(A, \dots, A) \subseteq A - A,$$

which says that there is a set $X \subseteq F$ with $|X| \leq CK^C$ for some constant C and

$$\begin{aligned} P(A, \dots, A) &\subseteq X + A - A \\ \Rightarrow |P(A, \dots, A)| &\leq |X||A - A| \\ &\leq CK^C|A \cdot A - A \cdot A| \leq (C + 1)K^{(C+1)}|A| \end{aligned}$$

So, it remains to prove the claim, which we will do by induction. The case when $k = 1$ is trivial, and the case $k = 2$ was dealt with in the proof of part 1 of Proposition 4.3. Now we assume that $k > 2$ and that the claim has been proven for A^{k-1} . Thus there is a subset $X \subseteq F$ such that $A^{k-1} \subseteq X + A - A$ and $|X| \leq CK^C$ for some constant C independent of A . That is, for every $a_{k-1} \in A^{k-1}$, there exists an $x \in X$ and $a, a' \in A$ such that

$$a_{k-1} = x + a - a' \Rightarrow x = a_{k-1} - a + a'$$

⁵Indeed, by exercise 3.2, we may take $C = 5$.

so we may ensure that $X \subseteq A^{k-1} - A + A$ by removing superfluous elements from X . But then by Exercise 4.2, we notice that all elements of X are good since $A^{k-1} - A + A$ is certainly a polynomial expression in A . Now we multiply by A to get

$$A^k \subseteq X \cdot A + A \cdot A - A \cdot A$$

But for each $x \in X$, there is a small Y_x such that

$$x \cdot A \subseteq Y_x + A - A$$

since x is good, so

$$X \cdot A \subseteq \bigcup (Y_x + A - A) \subseteq \bigcup (Y_x) + A - A$$

But $Y = \cup Y_x$ is small, and $A^k \subseteq (Y + A - A) + A \cdot A + A \cdot A$, so

$$A^k \subseteq A - A + A - A + A - A$$

Now we apply sumset estimates and Ruzsa's lemma again—as in the proof of the second part of the proposition—to finish the proof of the claim. \square

Proof of Theorem 0.1. Let $\delta > 0$ be given. Recall that Lemmas 2.1 and 2.2 combine to give us a polynomial P depending only on δ such that $P(A, \dots, A) = F := \mathbb{Z}/p\mathbb{Z}$ for any prime p and all $A \subset F$ with $p^\delta < |A| < p^{1-\delta}$. First we note that BKT is automatically true for small p depending only on δ since, given any such bound on p , there are only finitely many such F and A , so it is easy to find c and ε that satisfy the conclusion of the theorem for those p . (We will later put a constraint on p based only on δ .) If the conclusion were false, then there would be an $A \subseteq F$ such that $|A + A|$ and $|A \cdot A|$ are both $\leq K|A|^{1+\varepsilon} = K|A|^\varepsilon|A|$ for all $\varepsilon > 0$ and some K depending on ε . From next week's results, we know that this implies

$$|A \cdot A - A \cdot A| \leq CK^C|A|^{1+C\varepsilon}$$

for some constant C , and then by today's main result (Theorem 4.1), $|P(A, \dots, A)| \leq DK^D|A|^{1+D\varepsilon}$ for a constant D (since P is fixed). Now we choose $\varepsilon > 0$ so that $\delta + D\varepsilon(\delta - 1) > 0$. Notice that ε depends only on δ and D , but D is a universal constant, so we may demand that p satisfies

$$p^{\delta + D\varepsilon(\delta - 1)} > DK^D$$

by the above discussion. Putting this all together, along with the bounds on $|A|$ in the hypotheses, we get

$$p > DK^D|A|^{1+D\varepsilon} \geq |P(A, \dots, A)| = p$$

which is a contradiction, proving the theorem. \square

We will fill the gap of the proof next week when we present Gowers' version of the Balog-Szemerédi theorem in order to show that an approximate subring A also has small $A \cdot A - A \cdot A$.