and

$$|A \cdot \tilde{A}^{-1} \cdot \tilde{A} \cdot A^{-1}| \leq 4\frac{|A \cdot B|^4 |A^{-1} \cdot A|}{|A|^4}.$$

Compare this against Exercise 2.7.11. Hint: if $x := a_1 a_2^{-1} a_3 a_4^{-1}$ be a typical element of $A \cdot \tilde{A}^{-1} \cdot \tilde{A} \cdot A^{-1}$, obtain at least $(\frac{|A||B|^2}{2|A \cdot B|})^2$ representations of the form

$$x = [a_1 b_2](b'_2)^{-1}[(a'_2)^{-1} a'_3] b'_3 [a_4 b_2]^{-1}$$

where $a_1 b_2, a_4 b_2 \in A \cdot B$, $b'_2, b'_3 \in B$, and $(a'_2)^{-1} a'_3 \in A^{-1} \cdot A$.

2.7.13 Prove Theorem 2.48.

2.8 Elementary sum-product estimates

We now discuss some results concerning the sum set and product set of a subset A of a commutative ring Z, thus combining both the additive and multiplicative theory of the preceding sections (but keeping the multiplication commutative, for simplicity). The question here is to analyze the extent to which a set A can be approximately closed under addition and multiplication simultaneously. Of course, one way that this can happen is if A is a subring of Z; it appears that up to trivial changes (such as removing some elements, adding a small number of new elements, or dilating the set), this is essentially the only such example, although we currently only have a satisfactory and complete formalization of this principle when Z is a field (Theorem 2.55). In some ways the theory here is in fact easier than the sum set theory, because one can exploit two rather different structures arising from the smallness of $A + A$ and the smallness of $A \cdot A$ to obtain a conclusion. As in the rest of this chapter, our discussion is for general fields, with a particular emphasis on the finite field $\mathbf{Z}_p$. We remark that for the field $\mathbf{R}$ much better results are known, see Sections 8.3, 8.5.

In this section Z will always denote a commutative ring, and Z^* will denote the elements of Z which are not zero-divisors; these form a multiplicative cancellative commutative monoid in Z. The situation is significantly better understood in the case that Z is a field (see in particular Theorem 2.55 below); in such cases we shall emphasize this by writing the field as F instead of Z, and $F^\times$ instead of $F^* = F \backslash \{0\}$ to emphasize that $F^\times$ is now a multiplicative group. A fundamental concept in the field setting is that of a *quotient set*, which is the arithmetic equivalent of the concept of a quotient field of a division ring.

Definition 2.49 (Quotient set) Let A be a finite subset of a field F such that $|A| \geq 2$. Then the *quotient set* $Q[A]$ of A is defined to be

$$Q[A] := \frac{A-A}{(A-A)\backslash 0} := \left\{ \frac{a-b}{c-d} : a,b,c,d \in A; c \neq d \right\}.$$

We also set $Q[A]^\times := Q[A]\backslash 0$ to be the invertible elements in $Q[A]$.

Observe that $Q[A]$ contains both 0 and 1, and is symmetric under both additive and multiplicative inversion, thus $Q[A] = -Q[A]$ and $Q[A]^\times = (Q[A]^\times)^{-1}$. It is also invariant under translations and dilations of A, thus $Q[A] = Q[A+x] = Q[\lambda \cdot A]$ for all $x \in F$ and $\lambda \in F^\times$. Geometrically, $Q[A]$ can be viewed as the set of slopes of lines connecting points in $A \times A$.

The relevance of the quotient set to sum-product estimates lies in the trivial but fundamental observation:

Lemma 2.50 *Let A be a finite subset of a field F such that $|A| \geq 2$, and let $x \in F$. Then $|A + x \cdot A| = |A|^2$ if and only if $x \notin Q[A]$.*

Proof We have $|A + x \cdot A| = |A|^2$ if and only if the map $(a,b) \mapsto a + xb$ is injective on $A \times A$, which is true if and only if $a + xb \neq c + xd$ for all distinct $(a,b), (c,d) \in A \times A$, which after some algebra is equivalent to asserting that $x \notin Q[A]$. □

This has an immediate corollary:

Corollary 2.51 *If A is a subset of a finite field F such that $|A| > |F|^{1/2}$, then $Q[A] = F$.*

Note that the condition $|A| > |F|^{1/2}$ is absolutely sharp, as can be seen by considering the case when A is a subfield of F of index 2.

Lemma 2.50 has another important consequence: it gives a criterion under which $Q[A]$ is a subfield of F.

Corollary 2.52 *Let A be a finite subfield of a field F such that $|A| \geq 2$ and*

$$|A + Q[A] \cdot Q[A] \cdot A|, |A + (Q[A] + Q[A]) \cdot A| < |A|^2.$$

Then $Q[A]$ is a subfield of F.

This corollary may be compared with Exercise 2.6.5.

Proof From Lemma 2.50 and the hypotheses we see that $Q[A] \cdot Q[A] \subseteq Q[A]$ and $Q[A] + Q[A] \subseteq Q[A]$. In particular $Q[A]^\times \cdot Q[A]^\times = Q[A]^\times$. Since $Q[A]$ is finite and contains 0, 1, we see from Proposition 2.7 that $Q[A]$ is an additive group, and similarly from the multiplicative version of this Proposition we see that $Q[A]^\times$ is a multiplicative group. The claim follows. □

In order to use this corollary, one needs to control rational expressions of A such as $A + Q[A] \cdot Q[A] \cdot A$. In analogy with sum set estimates such as Corollary 2.23, one might first expect that once $|A + A| \leq K|A|$ and $|A \cdot A| \leq K|A|$, then all polynomial or rational expressions of A are controlled in cardinality by $CK^C|A|$. This however is not the case, even if one normalizes A to contain 0 and 1. To see this, consider $A = G \cup \{x\}$ where G is a subfield of F and $x \notin G$. Then one easily verifies $|A + A|, |A \cdot A| < 2|A|$ but $|A \cdot A + A \cdot A| \geq (|A| - 1)^2$, since $A \cdot A + A \cdot A$ contains $G + x \cdot G$, which has size $|G|^2$ by Lemma 2.50. This example is similar to one appearing in the preceding section, and it is resolved in a similar way, namely by passing from A to a subset of A.

Lemma 2.53 (Katz–Tao lemma) *[199], [41] Let Z be a commutative ring, and let $A \subseteq Z^*$ be a finite non-empty subset such that $|A + A| \leq K|A|$ and $|A \cdot A| \leq K|A|$ for some $K \geq 1$. Then there exists a subset A' of A such that $|A'| \geq |A|/2K - 1$ and $|A' \cdot A' - A' \cdot A'| = O(K^{O(1)}|A'|)$.*

Note that this lemma works in arbitrary commutative rings, not just in fields. The requirement that none of the elements of A be zero-divisors is not serious in the case of a field, since one can simply remove the origin 0 from A if necessary, but is a non-trivial requirement in other commutative rings.

Proof We use an argument from [41]. We may assume that $A > 10K$ (for instance) since the claim is trivial otherwise. Consider the dilates $\{a \cdot A : a \in A\}$ of A. Since $a \in Z^*$, $a \cdot A$ has the same cardinality as A. In particular we have

$$\sum_{x \in A \cdot A} \sum_{a \in A} 1_{a \cdot A}(x) = |A|^2.$$

Since $|A \cdot A| \leq K|A|$, we may apply Cauchy–Schwarz and conclude

$$\sum_{x \in A \cdot A} \left(\sum_{a \in A} 1_{a \cdot A}(x) \right)^2 \geq |A|^3/K.$$

We rearrange this as

$$\sum_{a,b \in A} |(a \cdot A) \cap (b \cdot A)| \geq |A|^3/K.$$

By the pigeonhole principle we can thus find a $b \in A$ such that

$$\sum_{a \in A} |(a \cdot A) \cap (b \cdot A)| \geq |A|^2/K.$$

Fix this b. Setting A' to be the set of all $a \in A$ such that

$$|(a \cdot A) \cap (b \cdot A)| \geq |A|/2K$$

we conclude that

$$\sum_{a\in A'} |(a\cdot A)\cap(b\cdot A)| \geq |A|^2/2K$$

and hence $|A'| \geq |A|/2K$. By shrinking A' by one if necessary we may assume $b \notin A'$. Now recall the Ruzsa distance $d(A,B) := \log \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$, and observe that $d(a\cdot A, a\cdot B) = d(A,B)$ whenever a is not a zero-divisor. Then $d(A,A) \leq 2d(A,-A) = 2\log K$, and hence

$$d(a\cdot A, a\cdot A) = d(b\cdot A, b\cdot A) = d(A,A) \leq 2\log K \text{ for all } a \in A'.$$

Since $(a\cdot A)\cap(b\cdot A)$ is a large subset of $a\cdot A$ and $b\cdot A$, one can compute

$$d(a\cdot A, a\cdot A\cap b\cdot A), d(b\cdot A, a\cdot A\cap b\cdot A) = O(1+\log K)$$

and hence by the Ruzsa triangle inequality

$$d(a\cdot A, b\cdot A) = O(1+\log K) \text{ for all } a \in A'. \tag{2.41}$$

Dilating this, we obtain

$$d(a_1a_2\cdot A, ba_2\cdot A), d(ba_2\cdot A, b^2\cdot A) = O(1+\log K) \text{ for all } a_1,a_2 \in A'$$

and hence by the Ruzsa triangle inequality

$$d(a_1a_2\cdot A, b^2\cdot A) = O(1+\log K) \text{ for all } a_1,a_2 \in A'. \tag{2.42}$$

To proceed further we need to "invert" elements in A. For any $a \in A$ let $\hat{a} := \prod_{a'\in A\setminus\{a\}} a' \in Z^*$. By dilating (2.41) (with a replaced by a_3) by $a_1a_2\prod_{a'\in A\setminus\{a_3,b\}} a'$ for $a_1,a_2,a_3 \in A'$, we obtain

$$d(a_1a_2\hat{b}\cdot A, a_1a_2\hat{a}_3\cdot A) = O(1+\log K) \text{ for all } a_1,a_2,a_3 \in A'.$$

Meanwhile, from dilating (2.42) we have

$$d(a_1a_2\hat{b}\cdot A, b^2\hat{b}\cdot A) = O(1+\log K) \text{ for all } a_1,a_2,a_3 \in A'.$$

Applying the Ruzsa triangle inequality, we thus have

$$d(a_1a_2\hat{a}_3\cdot A, a_1'a_2'\hat{a}_3'\cdot A) = O(1+\log K) \text{ for all } a_1,a_2,a_3,a_1',a_2',a_3' \in A'$$

and hence

$$|a_1a_2\hat{a}_3\cdot A - a_1'a_2'\hat{a}_3'\cdot A| = O(K^{O(1)})|A|.$$

Therefore we have

$$\sum_{x,y\in A'\cdot A'\cdot\hat{A}'} |x\cdot A - y\cdot A| = O(K^{O(1)})|A||A'\cdot A'\cdot\hat{A}'|^2,$$

where $\hat{A}' := \{\hat{a} : a \in A'\}$. But since $|A \cdot A| \leq K|A|$ and $|A'| \geq |A|/2K - 1$, we see from the multiplicative version of sum set estimates (working in the formal multiplicative group generated by the cancellative commutative monoid Z^*) that $|A' \cdot A' \cdot \hat{A}'| = O(K^{O(1)}|A|)$. We thus have

$$\sum_{x,y \in A' \cdot A' \cdot \hat{A}'} |x \cdot A - y \cdot A| \leq O(K^{O(1)}|A'|^3).$$

We rewrite the left-hand side as

$$\sum_{z \in Z} |\{(x, y) : \exists\, a, b \in A' \text{ such that } z = xa - yb\}|.$$

Write $\omega := \prod_{a \in A} a$, and observe that whenever $a_1, a_2, a_3, a_4 \in A'$, the number $\omega(a_1a_2 - a_3a_4)$ has at least $|A'|^2$ representations of the form $xa - yb$ with $x, y \in A' \cdot A' \cdot \hat{A}'$ and $a, b \in A'$, with (x, y) distinct, thanks to the identity

$$\omega(a_1a_2 - a_3a_4) = (a_1a_2\hat{a})a - (a_3a_4\hat{b})b.$$

Thus

$$|\omega \cdot (A' \cdot A' - A' \cdot A')| = O(K^{O(1)}|A'|)$$

and the claim follows since $\omega \in Z^*$. □

A modification of the above argument also gives the following statement, which can be viewed as a variant of Corollary 2.23 for the sum-product setting; we leave the proof to Exercise 2.8.1.

Lemma 2.54 *[43] Let Z be a commutative ring, and let $A \subseteq Z^*$ be a finite non-empty set such that $|A \cdot A - A \cdot A| \leq K|A|$. Then we have $|A^k - A^k| \leq K^{O(k)}|A|$ for all $k \geq 1$, where $A^k = A \cdot \ldots \cdot A$ is the k-fold product set of A.*

We can now classify those finite subsets of fields with small additive doubling and multiplicative doubling constant, up to polynomial losses:

Theorem 2.55 (Freiman theorem for sum-products) *Let A be a finite non-empty subset of a field F, and let $K \geq 1$. Then the following statements are equivalent up to constants, in the sense that if the j*th *property holds for some absolute constant C_j, then the k*th *property will also hold for some absolute constant C_k depending on C_j:*

(i) $|A + A| \leq C_1K^{C_1}|A|$ *and* $|A \cdot A| \leq C_1K^{C_1}|A|$*;*
(ii) either $|A| \leq C_2K^{C_2}$*, or else there exists a subfield G of F, a non-zero element $x \in F$, and a set X in F such that* $|G| \leq C_2K^{C_2}|A|$, $|X| \leq C_2K^{C_2}$, *and* $A \subseteq x \cdot G \cup X$.

This is a slight strengthening of a result in [43], [44].

Proof We shall only show the forward implication, leaving the easy backward implication to Exercise 2.8.2. By relabeling $C_1 K^{C_1}$ as K, we may thus assume that $|A+A| \leq K|A|$ and $|A \cdot A| \leq K|A|$. We may assume that $|A| \geq C_0 K^{C_0}$ for some large absolute constant C_0, since the claim is trivial otherwise. We may also remove 0 from A without any difficulty, thus we may assume $A \subseteq F^*$. Applying Lemma 2.53 and Lemma 2.54, we may find a subset A' of A with $|A'| = \Omega(K^{-O(1)}|A|)$ and $|(A')^k - (A')^k| = O(K)^{O(k)}|A'|$ for all $k \geq 1$. By Corollary 2.23 this implies that

$$|n(A')^k - m(A')^k| \leq O(K)^{O_{k,n,m}(1)}|A'| \text{ for all } n, k, m \geq 1. \tag{2.43}$$

Dilating A with a non-zero factor if necessary, we may assume $1 \in A'$ (noting that the hypothesis and conclusion of the theorem are invariant under such dilations). We may now add 0 back to A' and A without affecting (2.43).

Now we apply Corollary 2.52. Let $D := (A'-A')\backslash\{0\}$ and $G := Q[A'] = (A'-A')/D$. Using lowest common denominators, we observe that

$$A' + G \cdot G \cdot A' \subseteq \frac{(A' \cdot D \cdot D - (A'-A') \cdot (A'-A') \cdot A')}{D^2} \subseteq \frac{(4(A')^3 - 4(A')^3)}{D^2}.$$

on the other hand, from (2.43) we have

$$|(4(A')^3 - 4(A')^3) \cdot D^2| = O(K^{O(1)}|A'|),$$

so by the multiplicative version of Corollary 2.12 we see that

$$|A' + G \cdot G \cdot A'| = O(K^{O(1)}|A'|) < |A'|^2$$

if C_0 is sufficiently large. A similar argument gives $|A' + (G+G) \cdot A'| = O(K^{O(1)}|A'|) < |A'|^2$. Applying Corollary 2.52 we see that G is in fact a field.

Now let x be a non-zero element of A', and let y be an element of A'. Then $(a-y)/x \in Q[A'] = G$ for all $a \in A'$, thus

$$A' \subseteq x \cdot G + y.$$

Thus

$$x \cdot G + y = A' + x \cdot G \subseteq A' + A' \cdot Q[A']$$

and hence

$$(x \cdot G + y)^2 \subseteq (A' + A' \cdot Q[A'])^2.$$

But an argument using (2.43) and Corollary 2.12 as before gives $|(A' + A' \cdot Q[A'])^2| = O(K^{O(1)}|A'|) \leq O(K^{O(1)}|G|)$. Direct computation shows that $|(x \cdot G + y)^2| \geq |G|^2$ unless $y \in x \cdot G$. Thus (if C_0 is sufficiently large) we can take $y \in x \cdot G$. Because A' contains 1, we thus have $A' \subseteq G$.

Since $|A + A'| \leq K|A| = O(K^{O(1)}|A'|)$, we may apply Ruzsa's covering lemma (Lemma 2.14) and cover A by $O(K^{O(1)})$ translates of $A' - A'$, and hence by $O(K^{O(1)})$ translates of G. A similar argument using the multiplicative version of this lemma (and temporarily removing the non-invertible 0 element from A if necessary) covers A by $O(K^C)$ dilates of G. On the other hand, we have $|(G \cdot x) \cap (G + y)| \leq 1$ whenever $x \neq 1$. Thus we have $|A \backslash G| = O(K^{O(1)})$, and the claim follows. □

This theorem implies that at least one of $A + A$ or $A \cdot A$ is large if A does not intersect with a subfield of F:

Corollary 2.56 (Sum-product estimate) *[43],[44] Let A be a finite non-empty subset of a field F, and suppose that $K \geq 1$ is such that there is no finite subfield G of F of cardinality $|G| \leq K|A|$ and no $x \in F$ such that $|A \backslash (x \cdot G)| \leq K$. Then we have either $|A| = O(K^{O(1)})$ or $|A + A| + |A \cdot A| = \Omega(K^c|A|)$ for some absolute constant $c > 0$.*

Remark 2.57 In the particular case when F has no finite subfields we thus obtain $|A + A| + |A \cdot A| = \Omega(|A|^{1+\varepsilon})$ for some absolute constant $\varepsilon > 0$; this result was first obtained (when $F = \mathbf{R}$) by Erdős and Szemerédi [91]. In the setting of the real line it is was in fact conjectured in [91] that one can take ε arbitrarily close to 1 in the above estimate. For the most recent value of ε, see Theorem 8.15.

In the particular case of the field $F = F_p$ of prime order, which has no subfields other than $\{1\}$ and F_p, one obtains

Corollary 2.58 (Sum-product estimate for F_p) *[43],[44] Let A be a non-empty subset of F_p. Then*

$$|A + A| + |A \cdot A| = \Omega(\min(|A|, |F_p|/|A|)^c|A|)$$

for some absolute constant $c > 0$.

If H is any non-empty subset of F_p, then we have $kH^k + kH^k$, $kH^k \cdot kH^k \subset k^2H^{k^2}$ for all $k \geq 2$. Thus we have

$$|k^2H^{k^2}| = \Omega(\min(|kH^k|, p/|kH^k|)^c|kH^k|)$$

for some absolute constant $c > 0$. We can iterate this estimate (starting with $k = 2$ and squaring repeatedly) to establish

Corollary 2.59 *Let H be any non-empty subset of F_p, and let $A, \delta > 0$. Then there exists an integer $k = k(A, \delta) \geq 1$ such that*

$$|kH^k| = \Omega_{A,\delta}(\min(|H|^A, p^{1-\delta})).$$

We leave the proof of this corollary as an exercise. By using Lemma 4.10 from Chapter 4 one can in fact set $\delta = 0$ here, though we will not need this fact here.

In the special case when H is a multiplicative subgroup of F_p, we have $H^k = H$, and hence Corollary 2.59 gives

$$|kH| = \Omega_{A,\delta}(\min(|H|^A, p^{1-\delta})).$$

Thus multiplicative subgroups have rather rapid additive expansion. It turns out that one can do something similar for approximate groups:

Theorem 2.60 *[40] Let H be a non-empty subset of F_p such that $|H^2| \leq K|H|$, and let $A, \delta > 0$. Then there exists an integer $k = k(A, \delta) \geq 1$ such that*

$$|kH| = \Omega_{A,\delta}(K^{-O_{A,\delta}(1)} \min(|H|^A, p^{1-\delta})).$$

This result can be deduced from Corollary 2.59 and the following proposition; we leave the precise deduction as an exercise.

Proposition 2.61 *Let F be an arbitrary field, and let $H \subset F^\times$ be a finite non-empty subset of invertible field elements such that $|H^2| \leq K|H|$ for some $K \geq 1$. Let $k \geq 1$ and $L \geq 1$ be such that kH obeys the following "additive non-expansion" property: we have $|2kH| \leq L|kH''|$ for any subset H'' of H of cardinality $|H''| \geq \frac{1}{2K}|H|$. Then there exists a subset H' of H of cardinality $|H'| \geq \frac{1}{2K}|H|$ such that*

$$|j(H')^j| = O_j((1 + \log|H|)^{j^2} K^{O(j^2)} L^{O(j^2)} |kH|)$$

for all $j \geq 1$.

Proof From the multiplicative version of Exercise 2.3.24 we can find $H' \subset H$ with $|H'| \geq \frac{1}{2K}|H|$ and $h_0 \in H'$ such that $|(h \cdot H) \cap (h_0 \cdot H)| \geq \frac{1}{2K}|H|$ for all $h \in H'$. By dilation we may normalize $h_0 = 1$. From the additive non-expansion property we conclude that

$$|2kH| \leq L|k((h \cdot H) \cap H)| \leq L|A_h| \text{ for all } h \in H',$$

where $A_h := k(h \cdot H) \cap kH$. Since

$$|kH + A_h| \leq |2kH|; \quad |k(h \cdot H) + A_h| \leq |2k(h \cdot H)| = |2kH|$$

we thus obtain the Ruzsa distance estimates

$$d(kH, -A_h), d(k(h \cdot H), -A_h) \leq \log L$$

and hence by the triangle inequality

$$d(kH, k(h \cdot H)) \leq 2 \log L. \tag{2.44}$$

Now we turn to controlling $j(H')^j$ for some j. We first observe that

$$|(H')^2| \leq |H^2| \leq K|H| \leq 2K^2|H'|$$

and thus by the multiplicative analog of Exercise 2.3.10 we have

$$|(H')^2 \cdot (H')^{-1}| = O\big(K^{O(1)}|H'|\big).$$

We can then apply the multiplicative version of Exercise 1.1.8 to obtain a set $X \subset (H')^2 \cdot (H')^{-1}$ of cardinality $|X| = O(K^{O(1)}(1 + \log |H|))$ such that $(H')^2 \subset X \cdot H'$, and thus $(H')^j \subset X^{j-1} \cdot H'$. Thus by the pigeonhole principle we can bound

$$|j(H')^j| \leq |j(X^{j-1}H')| \leq |X|^{j(j-1)}|x_1 \cdot H' + \cdots + x_j \cdot H'|$$

for some $x_1, \ldots, x_j \in X^{j-1}$; it thus suffices to show that

$$|x_1 \cdot H' + \cdots + x_j \cdot H'| = O_j\big(L^{O(j^2)}|kH|\big).$$

Since xH' is contained in a translate of $k(xH')$, we have the somewhat crude estimate

$$|x_1 \cdot H' + \cdots + x_j \cdot H'| \leq |jB|$$

where $B := k(x_1 \cdot H) \cup \cdots \cup k(x_j \cdot H)$. But the x_i are all products of $O(j)$ elements from H' and $(H')^{-1}$. From repeated application of (2.44) and the triangle inequality we conclude that

$$d(k(x_i \cdot H), k(x_{i'} \cdot H)) \leq O(j \log L) \text{ for all } 1 \leq i, i' \leq j$$

and hence

$$d(B, B) \leq O(j \log L) + O(\log j).$$

From Exercise 2.3.10 we conclude that $|jB| = O_j(L^{O(j^2)}|B|)$, and the claim follows. □

By combining Corollary 2.60 with the asymmetric Balog–Szemerédi–Gowers theorem, we can show that multiplicative subgroups of F_p cannot have high additive energy:

Corollary 2.62 *Let H be a multiplicative subgroup of F_p such that $|H| \geq p^\delta$ for some $0 < \delta \leq 1$. Then there exists an $\varepsilon = \varepsilon(\delta) > 0$, depending only on δ, such that $E(A, H) \leq p^{-\varepsilon}|A||H|^2$ for all $A \subseteq F_p$ with $1 \leq |A| \leq p^{1-\delta}$, if p is sufficiently large and depending on δ.*

Proof Let $\varepsilon' = \varepsilon'(\delta) > 0$ be a small number to be chosen later, and let $\varepsilon = \varepsilon(\varepsilon', \delta') > 0$ be an even smaller number to be chosen later. Suppose for contradiction that there existed a set A such that $E(A, H) \geq p^{-\varepsilon}|A||H|^2$. Applying Corollary 2.36 (with $L := p$ and ε replaced by ε') we can find (if ε is sufficiently small and depending on ε') a subset H' of H with cardinality

$$|H'| = \Omega_{\varepsilon'}\big(p^{-\varepsilon'/2}|H|\big)$$

such that

$$|kH'| \leq |A + kH'| = O_{\varepsilon',k}\big(p^{k\varepsilon'/2}|A|\big)$$

for all k. Since H is a multiplicative subgroup, we see that

$$|H' \cdot H'| \leq |H^2| = |H| = O_{\varepsilon'}\big(p^{\varepsilon'/2}|H'|\big).$$

Since $|H| \geq p^{\delta}$, we also see (if ε' is sufficiently small depending on δ) that $|H|^A \geq p^{1-\delta/2}$ for some A depending only on δ. We can thus apply Corollary 2.60 (with δ replaced by $\delta/2$) and conclude that for a sufficiently large k depending on δ we have

$$|kH'| = \Omega_{\varepsilon',\delta}\big(p^{1-\delta/2-O_\delta(\varepsilon')}\big).$$

This gives a contradiction if ε' is sufficiently small and depending on δ, and p is sufficiently large. □

We shall apply this to exponential sums over multiplicative subgroups; see Theorem 4.41. For a variant of this estimate, see Lemma 9.44.

It seems of interest to obtain estimates of this type for more general commutative rings, and possibly even to non-commutative rings by combining these arguments with those in the preceding section. In this direction, Bourgain has established

Theorem 2.63 *[41] Let p be a large prime, and let A be a subset of the commutative ring $F_p \times F_p$ (endowed with the product structure $(a, b) \cdot (c, d) = (ac, bd)$) be such that $|A| \geq p^{\delta}$ and $|A + A|$, $|A \cdot A| \leq p^{\varepsilon}|A|$ for some $\delta, \varepsilon > 0$. Then there exists a set G of $F_p \times F_p$ such that $|G| \leq p^{O_\delta(\varepsilon)}|A|$ and $|A \cap G| \geq p^{-O_\delta(\varepsilon)}|A|$, where G is one of the following objects:*

- *the whole space $G = F_p \times F_p$;*
- *a horizontal line $G = F_p \times \{a\}$ for some $a \in F_p$;*
- *a vertical line $G = \{a\} \times F_p$ for some $a \in F_p$;*
- *a line $G = \{(x, ax) : x \in F_p\}$ for some $a \in F_p^\times$.*

We sketch a proof of this proposition in the exercises. This is not as complete a characterization of sets with small sum-product as Theorem 2.55 – in particular, it does not address the case of very small A – but is already sufficient to control

a number of exponential sums of importance in number theory and cryptography. See [41], [40].

The problem of obtaining good sum-product estimates when the ambient commutative ring is the integers $\mathbf{Z} = Z$ has attracted a lot of interest. In this case it has been conjectured by Erdős and Szemerédi [91] that

$$|kA| + |A^k| = \Omega_{k,\varepsilon}(|A|^{k-\varepsilon}) \tag{2.45}$$

for all $\varepsilon > 0$, all $k \geq 2$ and all additive sets $A \subset \mathbf{Z}$. Even the $k = 2$ case is open (and considered very difficult); this $k = 2$ case has currently been verified for all $\varepsilon > \frac{8}{11}$, see Theorem 8.15. In another direction towards (2.45), a recent result of Bourgain and Chang [42] has shown that for every $m > 1$ there exists an integer $k = k(m) \geq 1$ such that

$$|kA| + |A^k| = \Omega_m(|A|^m) \tag{2.46}$$

for all additive sets $A \subset \mathbf{Z}$. This last result is rather deep, in particular using an intricate "induction on scales" argument, coupled with some quantitative Freiman-type theorems.

Exercises

2.8.1 [41] Modify the proof of Lemma 2.53 to prove Lemma 2.54. (Hint: first use multiple applications of the triangle inequality to obtain control on $|x \cdot A - y \cdot A|$ for all $x, y \in A^k \cdot \hat{A}$.)

2.8.2 Prove the remaining implication in Theorem 2.55.

2.8.3 Deduce Corollary 2.56 and Corollary 2.58 from Theorem 2.55.

2.8.4 [44], [43] Let A, A', B be non-empty subsets of a field F such that $0 \notin B$. Using the first moment method, show that there exists $\xi \in B$ such that

$$E(A, \xi \cdot A') \leq \frac{|A|^2|A'|^2}{|B|} + |A||A'|$$

and conclude from (2.8) that

$$|A + \xi \cdot A'| \geq \frac{|A||A'||B|}{|A||A'| + |B|}.$$

2.8.5 [44] Let A be a subset of a finite field F such that $|A| > |F|^{1/2}$. Show that $|(A - A) \cdot A + (A - A) \cdot A| \geq \sup_{x \in F} |A + x \cdot A| \geq \frac{|F|}{2}$ and then conclude that

$$F = (A - A) \cdot A + (A - A) \cdot A + (A - A) \cdot A + (A - A) \cdot A.$$

(Hints: the first inequality follows easily from Corollary 2.51. For the second inequality, use Exercise 2.8.4.)

2.8.6 (Croot, personal communication) Let A be a subset of a finite field F such that $|A| > |F|^{1/k}$ for some integer $k \geq 2$. Show that $|Q[A]| \geq |F|^{1/(k-1)}$; this clearly generalizes Corollary 2.51. (Hint: exploit the fact that the maps $(a_1, \ldots, a_k) \mapsto x_1 a_1 + \cdots + x_k a_k$ fail to be injective for *arbitrary* $x_1, \ldots, x_k \in F$.)

2.8.7 [43] Let A be a subset of a field F such that $|A| \geq |F|^{\varepsilon}$ for some $\varepsilon > 0$. Show that there exists an integer $k = k(\varepsilon) > 1$ depending only on ε such that $k(A^k) - k(A^k) = G$ for some subfield G of F. (Use Exercise 2.8.5 or Lemma 4.10.)

2.8.8 [41] Let F_p be a field of prime order p and $Z = F_p \times F_p$. Let $A \subseteq Z$ be such that $|A \cap (\{a\} \times F_p)| \geq p^{\delta}$ and $|A \cap (\{b\} \times F_p)| \geq p^{\delta}$ for some $0 < \delta < 1$ and $a, b \in F_p$. Show that for some $k = k(\delta) > 0$ we have $k(A^k) - k(A^k) = Z$. (Hint: use Exercise 2.8.7.)

2.8.9 [41] Let F_p, Z, be as in Exercise 2.8.8, and let $\pi_1 : Z \to F_p$, $\pi_2 : Z \to F_p$ be the coordinate projections. Suppose that $A \subseteq Z$ is such that $|\pi_1(A)|, |\pi_2(A)| \geq p^{\delta}$ for some $0 < \delta < 1$ and such that at least one of π_1, π_2 is not injective. Show that for some $k = k(\delta) > 0$ we have $k(A^k) - k(A^k) = Z$. (Hint: by Exercise 2.8.8 it suffices to find some k' such that $k'(A^{k'}) - k'(A^{k'})$ contains a large intersection with either a horizontal line or a vertical line.)

2.8.10 [41] Let F_p, Z, π_1, π_2 be as in Exercises 2.8.8, 2.8.9. Suppose that $A \subseteq Z$ is such that $|\pi_1(A)|, |\pi_2(A)| \geq p^{\delta}$ for some $0 < \delta < 1$. Show that either A is contained in a line $\{(x, ax) : x \in F_p\}$ for some $a \in F_p^{\times}$, or else $k(A^k) - k(A^k) = Z$ for some $k = k(\delta) > 0$. (Hint: by Exercise 2.8.7 one can reduce to the case where $\pi_1(A) = \pi_2(A) = F_p$. Now divide into two cases depending on whether π_1 or π_2 is injective on $2A - 2A$ or not.)

2.8.11 [41] Use Exercise 2.8.10 and Lemmas 2.53, 2.54 to deduce Theorem 2.63. (You will have to take a small amount of care concerning the zero-divisors $\{0\} \times F_p \cup F_p \times \{0\}$.)

2.8.12 Let Z be a commutative ring, and A_1, A_2, A_3, A_4 be subsets of $Z^{\times}$ such that $|A_1| = |A_2| = |A_3| = |A_4| = N$ and $|A_1 \cdot A_2 - A_3 \cdot A_4| \leq KN$. Show that $|A_j \cdot A_j - A_j \cdot A_j| \leq K^{O(1)} N$ for all $j = 1, 2, 3, 4$. This lemma allows one to extend several of the above results to the setting where the single set A is replaced by a number of sets of comparable cardinality.

2.8.13 Prove Corollary 2.59.

2.8.14 Use Corollary 2.59 and Proposition 2.61 to prove Theorem 2.60. (Hint: start with k equal to a large power of 2, and set L equal to a small power of $|H|$. If the hypotheses of Proposition 2.61 are satisfied, then one can lower bound $|kH|$ by $|j(H')^j|$, which can be controlled using

Corollary 2.59. If not, we can lower bound $|2kH|$ by $L|kH'|$ for some large subset H' of H; now replace k by $k/2$ and H by H' and argue as before. Continuing this process, one eventually obtains a good lower bound on $|kH|$ or $|2kH|$, either by combining Proposition 2.61 with Corollary 2.59, or by accumulating enough powers of L.)

2.8.15 [40] Prove the following variant of Corollary 2.62: for any $\delta > 0$ there exists $\varepsilon > 0$ such that whenever H, A are subsets of F_p with $|H| \geq p^\delta$, $|H \cdot H| \leq p^\varepsilon |H|$, and $1 < |A| < p^{1-\delta}$, then $E(A, H) = O_\delta(p^{-\varepsilon}|A||H|^2)$. In particular we have $|A + H| = \Omega_\delta(p^\varepsilon |H|)$.

2.8.16 [18] Let A be an additive set in F_p such that $|A| < p^{1-\delta}$ for some $\delta > 0$. Show that there exists an $\varepsilon > 0$ depending on δ such that $|\{(a, b, c, d, e, f) \in A^6 : ab + c = de + f\}| = O_{\varepsilon,\delta}(|A|^{5-\varepsilon})$. (Hint: use the Balog–Szemerédi–Gowers theorem in both the additive and multiplicative forms, together with Corollary 2.58.) This estimate is used in [18] to show that iterations of the map $X \mapsto X_1 \cdot X_2 + X_3$ on random variables in F_p (where X_1, X_2, X_3 are independent trials of X) converge in a certain sense to the uniform distribution, which has applications to random number generation.