2.6.8 Let A be an additive set. Refine (2.21) slightly to

$$|\mathrm{Sym}_\alpha(A)| \leq 1 + \frac{|A|(|A|-1)}{\alpha} \text{ for all } \alpha > 0.$$

2.6.9 [350] Let A, B be additive sets in $\mathbf{Z}$, such that B consists entirely of positive numbers. Show that there exists $b \in B$ such that

$$|A \cap (A+b)| < \frac{|A|-1}{|B|}\frac{|A|}{2}.$$

(Hint: use Exercise 2.6.8, and exploit the fact that only half of the elements of $\mathrm{Sym}_\alpha(A)\backslash\{0\}$ are positive.)

2.6.10 [44] Let A be an additive set such that $|A+A| \leq K|A|$ for some $K \geq 1$. Let G be the group generated by $\mathrm{Sym}_{\frac{2}{9K}}(A)$. Show that there exists a coset $x+G$ of G such that $|A \cap (x+G)| \geq |A|/3$. (Hint: suppose for contradiction that $|A \cap (x+G)| < |A|/3$ for all x. Use the greedy algorithm to partition $A = A' \cup A''$ where $|A|/3 \leq |A'|, |A''| \leq 2|A|/3$ and such that $A' - A''$ is disjoint from G (and thus disjoint from $\mathrm{Sym}_{\frac{2}{9K}}(A)$). Use this to obtain an upper bound on $E(A', A'')$ and use (2.8) to obtain a contradiction.)

2.7 Non-commutative analogues

Many of the above arguments carry over to the non-commutative setting, though one of course now needs to take care with the ordering of multiplication. We sketch some of the main points here and leave the details as exercises. For further details see [362].

Definition 2.37 A *multiplicative group* is any group G (not necessarily abelian) with group operation $\cdot$, with inversion operation $x \mapsto x^{-1}$, and identity element 1. An *multiplicative set* is a pair (A, G), where G is a multiplicative group, and A is a finite non-empty subset of G. We often abbreviate a multiplicative set (A, G) simply as A, and refer to G as the *ambient group*.

If A and B are multiplicative sets with common ambient group G, we define their product set

$$A \cdot B := \{ab : a \in A, b \in B\}$$

and the inverse set

$$A^{-1} := \{a^{-1} : a \in A\}.$$

We also define right translates $A \cdot x$ and left translates $x \cdot A$ for $x \in G$ in the usual manner. Note that $x \cdot A \neq A \cdot x$ and $A \cdot B \neq B \cdot A$ in general, although we do have $|A| = |x \cdot A| = |A \cdot x| = |A^{-1}|$. We also define iterated product sets $A^{\cdot n} := A \cdot \ldots \cdot A$ for $n \geq 1$, with the conventions that $A^{\cdot 0} := \{1\}$ and $A^{\cdot -n} := (A^{\cdot n})^{-1} = (A^{-1})^{\cdot n}$.

We remark that $A \cdot B$ and $B \cdot A$ may have widely different cardinalities; for instance if H is a finite subgroup of G and x is an element of G that does not lie in the normalizer $N(H) := \{x \in G : xH = Hx\}$ of H, then $H \cdot (x \cdot H)$ and $(x \cdot H) \cdot H$ can have very different cardinalities. However, we still have the analogue of (2.1):

$$\max(|A|, |B|) \leq |A \cdot B|, |B \cdot A| \leq |A||B|;$$

see exercises.

We define the *(left-invariant) Ruzsa distance* $d(A, B)$ between two multiplicative sets:

$$d(A, B) := \log \frac{|A \cdot B^{-1}|}{|A|^{1/2}|B|^{1/2}}.$$

This distance still obeys the Ruzsa triangle inequality, mainly thanks to the identity $(ab^{-1})(bc^{-1}) = ac^{-1}$. It is left-invariant in each variable, thus $d(x \cdot A, B) = d(A, x \cdot B) = d(A, B)$, and is jointly right-invariant, $d(A \cdot x, B \cdot x) = d(A, B)$, but is not separately right-invariant in each variable. Also it is not reflection invariant; the metric $d^*(A, B) := d(A^{-1}, B^{-1})$ is the *right-invariant Ruzsa distance*, which we will not use here.

Define a *multiplicative K-approximate group* to be any multiplicative set H which is symmetric (so $H = H^{-1}$), contains the identity, and is such that there exists a set X of cardinality $|X| \leq K$ such that we have the inclusions

$$H \cdot H \subseteq X \cdot H \subseteq H \cdot X \cdot X; \qquad H \cdot H \subseteq H \cdot X \subseteq X \cdot X \cdot H.$$

We can characterize when $d(A, B)$ is zero:

Proposition 2.38 *Let A, B be multiplicative sets in an ambient group G. Then $d(A, B) = 0$ if and only if A and B are both left cosets of the same finite subgroup H, thus $A = x \cdot H$ and $B = y \cdot H$ for some $x, y \in G$.*

We leave the proof as an exercise. Observe that $d(A, B) = 0$ does not necessarily imply that A or B has small doubling; if x or y lie outside the normalizer of H then A^2 or B^2 can be significantly larger than A or B. Similarly we see that $d(A, B) = 0$ does not imply that $d(A, B^{-1}) = 0$. So there does not appear to be an analogue of Corollary 2.12. However, with some care and a few new arguments, we can still obtain the analogues of the results from Sections 2.4 and 2.5. Let us start by the analogue of Ruzsa's covering lemma, which can be proved by the same argument.

Lemma 2.39 *Let A, B be multiplicative sets in an ambient group G such that $|A \cdot B| \leq K|A|$. Then there exists a finite set X in B of cardinality at most K such that $B \subset A^{-1} \cdot A \cdot X$.*

From Section 2.4, we know that if A is a subset of a commutative group G and $|A + A| \leq K|A|$, then $|nA - mA| \leq O(K^{O(m+n)}|A|)$ for any n, m. This no longer holds in a non-commutative setting. Consider for instance $A := H \cup \{x\}$ where H is a subgroup of G and x lies outside the normalizer $N(H)$ of H. Then $A \cdot A = H \cup (x \cdot H) \cup (H \cdot x) \cup \{x^2\}$, so $|A \cdot A| \leq 3|A| - 2$; but $A \cdot A \cdot A$ contains $H \cdot x \cdot H$ which can be as large as $|H|^2 = (|A| - 1)^2$. Interestingly, it turns out that if we assume that $|A \cdot A \cdot A|$ is small, then the problem disappears and we can otain the following analogue of Proposition 2.26.

Proposition 2.40 *Let A be a multiplicative set in a group G, 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 positive absolute constant C_j, then the k*th *property will also hold for some absolute constant C_k depending on C_j:*

(i) $|A \cdot A \cdot A| \leq K^{C_1}|A|$;
(ii) We have $|A^{\epsilon_1} \cdots A^{\epsilon_n}| \leq K^{C_2 n}|A|$ *for all* $n \geq 1$ *and all signs* $\epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}$;
(iii) there exists a K^{C_3}*-approximate group H containing A where* $|H| \leq K^{C_3}|A|$.

Proof First we show that (i) implies (ii). Assuming (i), we have $|A \cdot A| \leq |A \cdot A \cdot A| \leq K^{C_1}|A|$. It follows that $d(A, A^{-1})$ (which equals $d(A^{-1}, A)$) and $d(A \cdot A, A^{-1})$ are $O(\log K)$. By the triangle inequality $d(A \cdot A, A) = O(\log K)$, which implies $|A \cdot A \cdot A^{-1}| \leq K^{O(1)}|A|$ and $d(A, A \cdot A^{-1}) = O(\log K)$. Again by the triangle inequality, we have $d(A \cdot A^{-1}, A^{-1}) = O(\log K)$, which implies $|A \cdot A^{-1} \cdot A| \leq K^{O(1)}|A|$. By a similar argument, we can show that $|A^{-1} \cdot A \cdot A| \leq K^{O(1)}|A|$. With these bounds (and taking inverse) we obtain the statment of (ii) for $n = 3$. From here, it is easy to finish the proof by induction on n, with $n = 3$ being the base case. (For $n = 2$, the statement in (ii) is trivial.)

Next, we prove that (ii) implies (iii). Set $H' = A \cup \{1\} \cup A^{-1}$ and $H = H' \cdot H' \cdot H'$. Clearly H is symmetric and contains A. By (ii), $|H| \leq K^{O(1)}|A|$. It thus remains to show that H is a $K^{O(1)}$- approximate group. Notice that $|H' \cdot H \cdot H| \leq K^{O(1)}|A|$. By the covering lemma, we have a set Y of cardinality $K^{O(1)}$ in $H \cdot H$ such that

$$H \cdot H \subset H'^{-1} \cdot H' \cdot Y.$$

Notice that the right-hand side is a subset of $H \cdot Y$. Now set $X = Y \cup Y^{-1}$. Since both H and X are symmetric $H \cdot H$ is contained in both $H \cdot X$ and $X \cdot H$.

Moreover, as $X \subset H \cdot H$,

$$H \cdot X \subset H \cdot H \cdot H \subset X \cdot H \cdot H \subset X \cdot X \cdot H$$

completing the proof.

The remaining implications are straightforward and left as an exercise. □

Now we are going to prove we can still obtain (iii) under the assumption that $d(A, B) = O(\log K)$ for some set B. We will need the following variant of Lemma 2.13, whose proof we leave as an exercise.

Lemma 2.41 *Let A be a multiplicative set. Then there exists a symmetric set $S \subset A^{-1} \cdot A$ such that $|S| \geq |A|/2$ and*

$$|A \cdot S^{\cdot n} \cdot A^{-1}| \leq \frac{2^n |A \cdot A^{-1}|^{n+1} |A^{-1} \cdot A|^n}{|A|^{2n}}$$

for all integers $n \geq 0$.

As $d(A, A) \leq 2d(A, B)$, this implies

Corollary 2.42 *Let A be a multiplicative set such that $d(A, B) \leq \log K$ for some $K \geq 1$. Then there exists a symmetric set S such that $|S| \geq \Omega(K^{-O(1)}|A|)$ and*

$$|A \cdot S^{\cdot n} \cdot A^{-1}| \leq O(K)^{O(1+n)}|A|$$

for all integers $n \geq 0$.

Proposition 2.43 *Let A, B be multiplicative sets in a group G, 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) $d(A, B) \leq C_1(1 + \log K)$;
(ii) there exists a $C_2 K^{C_2}$-approximate group H such that $|H| \leq C_2 K^{C_2}|A|$, $A \subset X \cdot H$ and $B \subset Y \cdot H$ for some multiplicative sets X, Y of cardinality at most $C_2 K^{C_2}$.

Proof We only need to prove that (i) implies (ii), as the reverse implication is trivial. Notice that (i) implies $d(A, A) = O(\log K)$. Thus, we have a symmetric set S of cardinality $K^{O(1)}|A|$ such that

$$|A \cdot S^{\cdot 3} \cdot A^{-1}| \leq K^{O(1)}|A|.$$

This implies that $|A \cdot S| \leq K^{O(1)}|A|$ and thus $d(A, S) = O(\log K)$. Furthermore, $|S^3| \leq K^{O(1)}|S|$ so we can find a $O(K^{O(1)})$-approximate group H of size $K^{O(1)}|A|$ containing S. This, in particular, implies that $d(S, H^{-1}) = O(\log K)$. By the triangle inequality, $d(A, H^{-1}) = O(\log K)$, which yields $|A \cdot H| \leq K^{O(1)}|A|$. By the

covering lemma, there is a set Y of cardinality $K^{O(1)}$ such that $A \subset Y \cdot H \cdot H^{-1}$. But as H is an approximate group, $H^{-1} = H$ and $H \cdot H \subset Z \cdot H$ for some set Z of size $K^{O(1)}$. Thus, $A \subset (Y \cdot Z) \cdot H$, where $|Y \cdot Z| \leq |Y||Z| = K^{O(1)}$. The conclusion for B can be proved similarly. □

Let us now consider the non-commutative verstion of Balog–Szemerédi–Gowers theorem. Theorem 2.29 still holds when the ambient group Z is non-commutative. The proof of this theorem is purely graph-theoretical (see Section 6.4) and has little to do with the commutativity of the group.

Theorem 2.44 (Balog–Szemerédi–Gowers theorem, non-commutative version) *Let A, B be multiplicative sets in an ambient group Z, and let $G \subseteq A \times B$ be such that*

$$|G| \geq |A||B|/K \text{ and } |A \overset{G}{\cdot} B| \leq K'|A|^{1/2}|B|^{1/2}$$

for some $K \geq 1$ and $K' > 0$. Then there exists subsets $A' \subseteq A$, $B' \subseteq B$ such that

$$|A'| \geq \frac{|A|}{4\sqrt{2}K} \tag{2.37}$$

$$|B'| \geq \frac{|B|}{4K} \tag{2.38}$$

$$|A' \cdot B'| \leq 2^{12}K^4(K')^3|A|^{1/2}|B|^{1/2}. \tag{2.39}$$

In particular we have

$$d(A', B'^{-1}) \leq 5\log K + 3\log K' + O(1).$$

Define the *multiplicative energy* $E(A, B)$ between two multiplicative sets A, B with common ambient group to be

$$E(A, B) := |\{(a, a', b, b') \in A \times A \times B \times B : ab = a'b'\}|. \tag{2.40}$$

A significant difficulty here is that $E(A, B)$ obeys far fewer symmetries in the non-commutative case than in the commutative case; indeed, the only symmetry available is that $E(A, B) = E(B^{-1}, A^{-1})$. However in the case when $B = A^{-1}$ we have a crucial additional identity $E(A, A^{-1}) = E(A^{-1}, A)$ (see exercises), which can be thought of as a very weak, restricted form of commutativity.

The following variant of Lemma 2.30 holds, with basically the same proof.

Lemma 2.45 *Let A, B be multiplicative sets in an ambient group Z, and let G be a non-empty subset of $A \times B$. Then*

$$E(A, B) \geq \frac{|G|^2}{|A \overset{G}{\cdot} B|}.$$

Conversely, if $E(A,B) \geq |A|^{3/2}|B|^{3/2}/K$ *for some* $K \geq 1$*, then there exists* $G \subseteq A \times B$ *such that*

$$|G| \geq |A||B|/2K; \quad |A \overset{G}{\cdot} B| \leq 2K|A|^{1/2}|B|^{1/2}.$$

Finally, notice that by the triangle inequality

$$d(A', A') \leq d(A', B'^{-1}) + d(B'^{-1}, A') = 2d(A', B'^{-1}),$$

which means that if $d(A', B'^{-1})$ is small, then $d(A', A')$ is also small. From here, we can use the same arguments for the commutative case to deduce

Corollary 2.46 *Let* A, B *be multiplicative sets in an ambient group* Z *such that* $E(A,B) \geq |A|^{3/2}|B|^{3/2}/K$ *for some* $K > 1$*. Then there exists a subset* $A' \subset A$ *such that* $|A'| = \Omega(K^{-O(1)}|A|)$ *and* $|A' \cdot (A')^{-1}| = O(K^{O(1)}|A|)$ *for some absolute constant* C*.*

Combining this with the identity $E(A, A^{-1}) = E(A^{-1}, A)$ we obtain the following weak commutativity property between A and A^{-1}:

Corollary 2.47 *Let* A *be a multiplicative set such that* $|A \cdot A| \leq K|A|$ *for some* $K \geq 1$*. Then there exists a subset* $A' \subset A$ *such that* $|A'| = \Omega(K^{-O(1)}|A|)$ *and* $|A' \cdot (A')^{-1}| = O(K^{O(1)}|A|)$*.*

It is now not too hard to obtain the following theorem.

Theorem 2.48 *Let* A, B *be multiplicative sets in a group* G*, and let* $K \geq 1$*. Then the following statements are equivalent up to constants, in the sense that if the* jth *property holds for some absolute constant* C_j*, then the* kth *property will also hold for some absolute constant* C_k *depending on* C_j*:*

(i) $E(A,B) \geq C_1^{-1}K^{-C_1}|A|^{3/2}|B|^{3/2}$*;*
(ii) there exists a subset $G \subset A \cdot B$ *with* $|G| \geq C_2^{-1}K^{-C_2}|A||B|$ *such that* $|A \overset{G}{\cdot} B| \leq C_2K^{C_2}|A|^{1/2}|B|^{1/2}$*;*
(iii) there exists a $C_3K^{C_3}$*-approximate group* H *and* $x, y \in G$ *such that* $|H| \leq C_3K^{C_3}|A|^{1/2}|B|^{1/2}$ *and*

$$|A \cap (x \cdot H)|, |B \cap (H \cdot y)| \geq C_3^{-1}K^{-C_3}|H|.$$

We leave the proofs of these statements to the exercises. Despite these characterizations, there is much left to be done in the study of product sets in non-commutative groups. For instance we do not currently have a satisfactory version of Freiman's theorem in general. However there has been some progress in the case of very small doubling [172] and also in certain special groups such as $SL_2(\mathbf{Z})$ or free groups; see for instance [78], [182].

Exercises

2.7.1 Prove a multiplicative version of Lemma 2.1.

2.7.2 Prove a multiplicative version of Lemma 2.6.

2.7.3 Prove Proposition 2.38.

2.7.4 Let (A, G) be a multiplicative set. Prove that $|A \cdot A| = |A|$ if and only if A is a normal coset of H, i.e. $A = x \cdot H = H \cdot x$ for some $x \in N(H)$.

2.7.5 Let A be a symmetric multiplicative set, so $A = A^{-1}$, and let $\sigma_n[A]$ denote the n-fold doubling numbers $|A^n|/|A|$. Using the Ruzsa triangle inequality, show that $\sigma_{m+n-2}[A] \leq \sigma_m[A]\sigma_n[A]$ for all $m, n \geq 2$.

2.7.6 Let A and B be multiplicative sets. Establish the identities $E(A, B) = E(B^{-1}, A^{-1})$ and $E(A, A^{-1}) = E(A^{-1}, A)$, and the inequality $E(A, B) \geq \frac{|A|^2|B|^2}{|A \cdot B|}$.

2.7.7 Let A, B, C be additive sets in an ambient group Z, let $0 < \varepsilon < 1/4$, and let $G \subset A \times B^{-1}$, $H \subset B \times C^{-1}$ be such that $|G| \geq (1-\varepsilon)|A||B|$ and $|H| \geq (1-\varepsilon)|B||C|$. By modifying the solution of Exercise 2.5.4, show that there exists subsets $A' \subseteq A$ and $C' \subseteq C$ with $|A'| \geq (1-\varepsilon^{1/2})|A|$ and $|C'| \geq (1-\varepsilon^{1/2})|C|$ such that $|A' \cdot (C')^{-1}| \leq \frac{|A \cdot^G B^{-1}||B \cdot^H C^{-1}|}{(1-2\varepsilon^{1/2})|B|}$.

2.7.8 Let A be a multiplicative set such that $|A \cdot A^{-1}| \leq K|A|$ and $|A^{-1} \cdot A| \leq K|A|$. Show that there exists a subset $\tilde{A}$ of A such that $|\tilde{A}| \geq |A|/2K$ and

$$|\tilde{A} \cdot \tilde{A}^{-1} \cdot \ldots \cdot \tilde{A}^{(-1)^{n+1}}| \leq 2^{n-2}K^{2n-3}|A|$$

for all $n \geq 2$, where the product consists of n factors alternating between $\tilde{A}$ and $\tilde{A}^{-1}$.

2.7.9 If A and B are multiplicative sets in a group G, show that there exist sets $X_1, X_2 \subseteq A$ such that $|X_1| \leq \frac{|A \cdot B|}{|B|}$, $|X_2| \leq \frac{|B \cdot A|}{|B|}$, and $A \subseteq X_1 \cdot B \cdot B^{-1}$ and $A \subseteq B^{-1} \cdot B \cdot X_2$, by modifying the proof of Lemma 2.14.

2.7.10 Prove Lemma 2.41.

2.7.11 Show that the direct analogue of Proposition 2.18 fails in the non-commutative case, even when $A = B = A^{-1}$.

2.7.12 Let A, B be multiplicative sets in an ambient group G, and let $\tilde{A}$ be the set

$$\tilde{A} := \left\{ a \in A : |\{(a', b, b') \in A \times B \times B : a = a'b'b^{-1}\}| \geq \frac{|A||B|^2}{2|A \cdot B|} \right\}.$$

Establish the bounds

$$|\tilde{A}| \geq \frac{|A|^2}{2|A \cdot B|}$$