Sums of various dilates

Thesis by
Jeck Lim

In Partial Fulfillment of the Requirements for the
Degree of
Doctor of Philosophy

CALIFORNIA INSTITUTE OF TECHNOLOGY
Pasadena, California

2025
Defended May 29, 2025

Jeck Lim
ORCID: 0009-0002-0369-8523

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to my advisor, David Conlon, for his guidance and support throughout my time at Caltech. His mentorship has been instrumental in shaping my mathematical interests and has continually inspired me to pursue work of the highest caliber. His positivity and assurance have also helped strengthen my self-esteem and confidence, for which I am especially thankful.

I am also grateful to the Caltech mathematics department for providing such a welcoming and intellectually stimulating environment. I thank Tom Hutchcroft, Huy Tuan Pham, and Vesselin Dimitrov for serving on my thesis committee and for their valuable time and feedback.

I would like to thank my friends at Caltech—Trung, Dylan, Bjarne, Yuxin, and Deepesh—for their camaraderie and for making life here so much more enjoyable. I will fondly remember our intellectual discussions, board game nights, and weekly food adventures, especially our many visits to Borneo Eatery.

Finally, I am deeply thankful to my family in Singapore for their constant love and support. Our weekly Zoom calls brought warmth and comfort, helping me feel at home even while being so far away.

ABSTRACT

Given a finite subset A of an ambient abelian group and a dilate λ, how large must the sum of dilate $A + \lambda \cdot A$ be in terms of A? In this thesis, we study this problem in various settings and generalizations, proving tight bounds in many cases. Our five main results are as follows.

1. In the setting of a d-dimensional subset A of $\mathbb{R}^d$, we prove an exact lower bound on the size of the difference set $A - A$.

2. In the case when $\lambda \in \mathbb{C}$ is a transcendental number, we show that there is an absolute constant $c > 0$ such that $|A + \lambda \cdot A| \geq \exp(c\sqrt{\log |A|})|A|$ for any finite subset A of $\mathbb{C}$. This is best possible up to the constant c.

3. In the algebraic case, given algebraic numbers $\lambda_1, \ldots, \lambda_k$, we prove tight lower bounds for the sum of dilates $A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A$. As an important ingredient, we also prove a Freiman-type structure theorem for sets with small sums of dilates.

4. In the setting of sums of linear transformations, we prove tight bounds for the sum of two linear transformations and tight bounds for the sum of multiple pre-commuting linear transformations.

5. In the setting of groups of prime order, we prove near-optimal lower and upper bounds for the sum of dilate $A + \lambda \cdot A$ for A of a given density and large λ.

PUBLISHED CONTENT AND CONTRIBUTIONS

[1] D. Conlon and J. Lim, Difference sets in $\mathbb{R}^d$, *to appear in Israel Journal of Mathematics* (2025), DOI: 10.1007/s11856-025-2717-2.

[2] D. Conlon and J. Lim, Sums of dilates over groups of prime order, *to appear in American Mathematical Monthly* (2025), arXiv:2409.17112.

[3] D. Conlon and J. Lim, Sums of linear transformations, *to appear in Transactions of the American Mathematical Society* (2025), arXiv:2203.09827, DOI: 10.1090/tran/9433.

[4] D. Conlon and J. Lim, Sums of transcendental dilates, *Bulletin of the London Mathematical Society* **55** (2023), no. 5, 2400–2406, DOI: 10.1112/blms.12870.

In each of the papers listed above, all authors contributed equally.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

1.1 Sumsets

Given two subsets A, B of an abelian group, the *sumset* $A + B$ is defined by

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

and the difference set $A - B$ is defined similarly. Sumsets play a central role in additive combinatorics. One of the most classical problems involving sumsets is the study of their cardinalities and structural characteristics when A and B satisfy particular constraints. For instance, if A and B are subsets of the integers, then with no additional constraints, $|A + B| \geq |A| + |B| - 1$ is best possible, as witnessed by arithmetic progressions of the same common difference.

If A is a subset of a ring R (or more generally an R-module) and λ is an element of R, the *dilate* $\lambda \cdot A$ is defined by

$$\lambda \cdot A := \{\lambda a : a \in A\}.$$

The sum of dilates can then be written as

$$A + \lambda \cdot A = \{a + \lambda \cdot a' : a, a' \in A\},$$

or more generally with multiple dilates

$$\lambda_1 \cdot A + \cdots + \lambda_k \cdot A = \{\lambda_1 a_1 + \cdots + \lambda_k a_k : a_1, \ldots, a_k \in A\}.$$

Such sums of dilates have attracted considerable attention in recent years, with the basic problem asking for an estimate on the minimum size of $|\lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$ given $|A|$. Formally, the general problem is as follows.

Problem 1.1.1. *Let R be a ring and M an R-module. Given $\lambda_1, \ldots, \lambda_k \in R$ and a positive integer n, determine the smallest possible value of $|\lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$ across all $A \subseteq M$ with $|A| = n$.*

We are interested in the asymptotics of $|\lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$ as $n \to \infty$, with $\lambda_1, \ldots, \lambda_k$ fixed. In this thesis, we study this general problem in various settings.

1.2 High-dimensional difference sets

Our first setting regards the difference set $A-A$, for $A \subset \mathbb{Z}^d$. Without any restrictions on A, the simple bound $|A - A| \geq 2|A| - 1$ is best possible, with equality when A is an arithmetic progression. However, an arithmetic progression is one-dimensional and does not make full use of the ambient $\mathbb{Z}^d$, so a natural restriction is that A must be a d-dimensional set, that is, A is not contained in an affine hyperplane.

The motivation for this problem originated from Freiman's structure theorem, one of the most fundamental results in additive combinatorics. It says that any finite set of integers A with small doubling, that is, with $|A + A| \leq K|A|$ for some fixed constant K, is contained in a generalized arithmetic progression of small size and dimension.

The first step in Freiman's original proof [17] of this theorem is a simple lemma showing that if A is a finite d-dimensional subset of $\mathbb{R}^d$, then

$$|A + A| \geq (d + 1)|A| - d(d + 1)/2,$$

where we say that a subset A of $\mathbb{R}^d$ is *k-dimensional* and write $\dim(A) = k$ if the dimension of the affine subspace spanned by A is k. Freiman's result is tight, as may be seen by considering the union of d parallel arithmetic progressions with the same common difference.

Surprisingly, the analogous problem of estimating $|A - A|$ for d-dimensional subsets A of $\mathbb{R}^d$ has remained open, despite first being raised by Uhrin [49] in 1980 because of connections to the geometry of numbers and then reiterated many times (see, for example, [13, 18, 37, 44, 45]). The best known construction is due to Stanchescu [45], who showed there exist arbitrarily large sets d-dimensional subsets $A \subset \mathbb{R}^d$ satisfying

$$|A - A| = \left(2d - 2 + \frac{1}{d-1}\right)|A| - (2d^2 - 4d + 3).$$

Supplanting an earlier conjecture of Ruzsa [37], Stanchescu proposed that this is best possible.

Conjecture 1.2.1 (Stanchescu [45])**.** *Suppose $d \geq 2$ and $A \subset \mathbb{R}^d$ is a finite set such that* $\dim(A) = d$*. Then*

$$|A - A| \geq \left(2d - 2 + \frac{1}{d-1}\right)|A| - (2d^2 - 4d + 3).$$

This conjecture was only known to be true for $d = 2, 3$. In Chapter 2, we prove Conjecture 1.2.1 in full provided only that $|A|$ is sufficiently large in terms of d, essentially resolving the problem of minimising the value of $|A - A|$ over all d-dimensional sets A of a given size. Our method builds on work of Mudgal [31] and earlier work of Stanchescu [44, 46].

Theorem 1.2.2. *Suppose $d \geq 2$ and $A \subset \mathbb{R}^d$ is a finite set such that $\dim(A) = d$. Then, provided $|A|$ is sufficiently large in terms of d,*

$$|A - A| \geq \left(2d - 2 + \frac{1}{d-1}\right)|A| - (2d^2 - 4d + 3).$$

1.3 Sums of linear transformations

We look again at Problem 1.1.1. Over the integers ($R = M = \mathbb{Z}$), this problem was essentially solved by Bukh [8].

Theorem 1.3.1 (Bukh [8])**.** *If $\lambda_1, \dots, \lambda_k$ are coprime integers, then, for any finite set of integers A,*

$$|\lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \geq (|\lambda_1| + \cdots + |\lambda_k|)|A| - o(|A|),$$

which is best possible up to the lower-order term.

This result was later tightened by Balog and Shakan [2] when $k = 2$ and then Shakan [42] in the general case, improving the $o(|A|)$ term to a constant depending only on $\lambda_1, \dots, \lambda_k$ (see also [11, 12, 15, 23, 30] for some earlier work on specific cases).

In this thesis, we will be concerned with generalizations of these results to higher dimensions, for example, when $M = \mathbb{Z}^d$. One possible direction is to again look at sums of dilates with the restriction that A is d-dimensional (see, for example, [3, 25, 31–33]). Another direction is to allow more kinds of dilates by setting $R = \mathrm{Mat}_d(\mathbb{Z})$, the ring of $d \times d$ integer matrices. This is encapsulated in the following conjecture of Bukh. This conjecture first appeared on Bukh's webpage, but has since been reiterated by several other authors [28, 33, 42].

Conjecture 1.3.2. *Suppose that $\mathcal{L}_1, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ have no common non-trivial invariant subspace and $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d = \mathbb{Z}^d$. Then, for any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_1 A + \cdots + \mathcal{L}_k A| \geq (|\det(\mathcal{L}_1)|^{1/d} + \cdots + |\det(\mathcal{L}_k)|^{1/d})^d |A| - o(|A|).$$

The intuition behind this conjecture comes from the Brunn–Minkowski inequality, the statement that for bodies $A, B \subset \mathbb{R}^d$, the measure of their sumset is $\mu(A+B) \geq (\mu(A)^{1/d} + \mu(B)^{1/d})^d$, where μ is the Lebesgue measure on $\mathbb{R}^d$. The conjecture is then the statement that, under appropriate technical conditions, a discrete analogue of the Brunn–Minkowski inequality should hold, possibly with some correction term to deal with boundary effects.

It turns out that Bukh's conjecture is not quite correct and both conditions, that $\mathcal{L}_1, \dots, \mathcal{L}_k$ have no common non-trivial invariant subspace and that $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d = \mathbb{Z}^d$, need modification. The correct conditions are *irreducibility* and *coprimality*, which we define in Chapter 3. This gives the following modified version of Bukh's conjecture.

Conjecture 1.3.3. *Suppose that $\mathcal{L}_1, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Then, for any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_1 A + \cdots + \mathcal{L}_k A| \geq \left(|\det(\mathcal{L}_1)|^{1/d} + \cdots + |\det(\mathcal{L}_k)|^{1/d}\right)^d |A| - o(|A|).$$

In Chapter 3, we prove this modified conjecture for $k = 2$ and any d in the following strong form. We note that this result is best possible up to the lower-order term in certain cases, for instance, when $d = 2$, $\mathcal{L}_1$ is the identity and $\mathcal{L}_2 \in \mathrm{Mat}_2(\mathbb{Z})$ is a dilate of a rotation about the origin through an angle which is not an integer multiple of π.

Theorem 1.3.4. *Suppose that $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Then there are constants D, $\sigma > 0$ such that, for any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq \left(|\det(\mathcal{L}_1)|^{1/d} + |\det(\mathcal{L}_2)|^{1/d}\right)^d |A| - D|A|^{1-\sigma}.$$

Despite the Brunn–Minkowski inequality being tight, the bound in Conjecture 1.3.3 is not tight in many cases. Indeed, one expects tightness from Brunn–Minkowski only if there exists a convex set $A \subset \mathbb{R}^d$ such that $\mathcal{L}_1 A, \dots, \mathcal{L}_k A$ are all homothetic, which does not hold in general. This motivates the following problem.

Problem 1.3.5. *Given $\mathcal{L}_1, \mathcal{L}_2, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ which are irreducible and coprime, determine the largest possible constant $H = H(\mathcal{L}_1, \dots, \mathcal{L}_k)$ such that the following holds. For any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_1 A + \mathcal{L}_2 A + \cdots + \mathcal{L}_k A| \geq H|A| - o(|A|).$$

Bukh's conjecture then says that

$$H(\mathcal{L}_1, \dots, \mathcal{L}_k) \geq (|\det(\mathcal{L}_1)|^{1/d} + \cdots + |\det(\mathcal{L}_k)|^{1/d})^d,$$

although we do not expect equality in general.

We will revisit this problem again in Chapter 7. Using the results from previous chapters, we determine the exact value of $H(\mathcal{L}_1, \dots, \mathcal{L}_k)$ for *pre-commuting matrices*. In particular, this resolves Problem 1.3.5 for $k = 2$ and any d, because, as we will see, any pair $\mathcal{L}_1, \mathcal{L}_2$ of irreducible and coprime matrices are non-singular and hence pre-commuting.

1.4 Sums of real and complex dilates

We again look at Problem 1.1.1. This time, consider the setting where $M = R = \mathbb{R}$ or $\mathbb{C}$. As mentioned before, if $\lambda_1, \dots, \lambda_k \in \mathbb{Z}$ and $A \subset \mathbb{Z}$, then this is completely solved by Bukh in Theorem 1.3.1. Consider now the general case when the λ_i are allowed to be any real (or complex) number, and A a finite subset of the real (or complex) numbers. By scaling the λ_i, we may assume without loss of generality that one of the λ_i is 1. With this in mind, we have the following problem.

Problem 1.4.1. *Given $\lambda_1, \dots, \lambda_k \in \mathbb{C}$, determine the smallest possible value of $|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$ in terms of $|A|$.*

For instance, when the λ_i are rational, by "clearing denominators," we may write $\lambda_i = p_i/q$ with $p_1, \dots, p_k, q$ coprime. Then, the result of Bukh (Theorem 1.3.1), which easily extends to all $A \subset \mathbb{R}$, implies that

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \geq q(1 + |\lambda_1| + \cdots + |\lambda_k|)|A| - o(|A|),$$

which is best possible up to the lower-order term.

Transcendental dilates

Let us consider the case $k = 1$, where we are estimating the size of the simpler $|A + \lambda \cdot A|$. For transcendental λ, it turns out that $|A + \lambda \cdot A|$ grows superlinearly in $|A|$, that is, for any constant $C > 0$, $|A + \lambda \cdot A| \geq C|A|$ for $|A|$ large enough. Can we get a more precise growth rate of $|A + \lambda \cdot A|$ in terms of $|A|$?

Konyagin and Łaba [27] showed that there exists an absolute constant $c > 0$ such that

$$|A + \lambda \cdot A| \geq c \frac{\log |A|}{\log \log |A|} |A|.$$

This result was subsequently improved by Sanders [39], by Schoen [41] and again by Sanders [40] using successive quantitative refinements of Freiman's theorem [17] on sets of small doubling, with Sanders' second bound saying that there exists an absolute constant $c > 0$ such that, for $|A|$ sufficiently large,

$$|A + \lambda \cdot A| \geq e^{\log^c |A|}|A|.$$

This already comes quite close to matching the best known upper bound, due to Konyagin and Łaba [27], which says that there exists $c' > 0$ and, for any fixed transcendental number λ, arbitrarily large finite subsets A of $\mathbb{R}$ such that

$$|A + \lambda \cdot A| \leq e^{c'\sqrt{\log |A|}}|A|.$$

In Chapter 4, we show that this upper bound is in fact best possible up to the constant c'.

Theorem 1.4.2. *There is an absolute constant $c > 0$ such that*

$$|A + \lambda \cdot A| \geq e^{c\sqrt{\log |A|}}|A|$$

for any finite subset A of $\mathbb{C}$ and any transcendental number $\lambda \in \mathbb{C}$.

Algebraic dilates

For algebraic $\lambda_1, \ldots, \lambda_k$, the minimum size of $A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A$ only grows linearly in $|A|$. Thus, in the algebraic case, we are interested in this linear rate.

Problem 1.4.3. *Given algebraic $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$, determine the largest possible constant $H = H(\lambda_1, \ldots, \lambda_k)$ such that the following holds. For any finite subset $A \subset \mathbb{C}$, we have $|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \geq H|A| - o(|A|)$.*

Let us first consider this problem for the case $k = 1$. There is a general result due to Chen and Fang [10], itself improving an earlier result of Breuillard and Green [7], saying that, for any fixed $\lambda \geq 1$, $|A + \lambda \cdot A| \geq (1 + \lambda - o(1))|A|$ holds for all finite subsets A of $\mathbb{R}$. This is best possible when λ is an integer, but can be quite slack in other cases, for instance, when $\lambda = p/q$ with p and q coprime and $p, q > 1$ as seen in Theorem 1.3.1.

In their paper, Krachun and Petrov [28] studied the case where $\lambda = \sqrt{2}$, showing that

$$|A + \sqrt{2} \cdot A| \geq (1 + \sqrt{2})^2|A| - o(|A|),$$

which is best possible up to the lower-order term, as may be seen by considering the set $A = \{x + y\sqrt{2} : 0 \le x < M, 0 \le y < N\}$ with the ratio M/N approaching $\sqrt{2}$. They also formulated a conjecture for a general real algebraic λ. Indeed, if $f(x) \in \mathbb{Z}[x]$ is the minimal polynomial of λ, assumed to have coprime coefficients, and $f(x) = \prod_{i=1}^{d}(a_i x + b_i)$ is a full complex factorization of f, let $H(\lambda) = \prod_{i=1}^{d}(|a_i| + |b_i|)$. For example, if $\lambda = (p/q)^{1/d}$ is in its simplest form, then $H(\lambda) = (p^{1/d} + q^{1/d})^d$.

Krachun and Petrov proved that there exists $A \subset \mathbb{R}$ of arbitrarily large size with $|A + \lambda \cdot A| = H(\lambda)|A| - o(|A|)$. They conjectured that this value $H(\lambda)$ is best possible.

Conjecture 1.4.4 (Krachun–Petrov [28])**.** *For any real algebraic number λ, and finite subset $A \subset \mathbb{R}$,*

$$|A + \lambda \cdot A| \ge H(\lambda)|A| - o(|A|).$$

In Chapter 6, we determine $H(\lambda_1, \dots, \lambda_k)$, completely solving Problem 1.4.3, which includes Conjecture 1.4.4 as a special case.

Theorem 1.4.5. *Let $\lambda_1, \dots, \lambda_k$ be algebraic numbers. Then for any subset A of $\mathbb{C}$,*

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \ge H(\lambda_1, \dots, \lambda_k)|A| - o(|A|),$$

where $H(\lambda_1, \dots, \lambda_k)$ is an explicit constant that is best possible.

A crucial ingredient of this result is a Freiman-type structure theorem for sets with small sums of dilates, stated below.

Theorem 1.4.6. *Let $C, p > 0$. Then there are constants $n = n(C, p)$ and $F = F(C, p)$ such that for any $A \subset \mathcal{O}_K$ satisfying*

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \le C|A|,$$

there exists a p-proper $\mathcal{O}_K$-GAP $P \subset \mathcal{O}_K$ containing A of dimension at most n and size at most $F|A|$.

The definition of an $\mathcal{O}_K$-GAP, and the proof of this result, are quite technical, so we dedicate the entirety of Chapter 5 to them.

Problems 1.4.3 and 1.3.5 are very closely related. To see this connection, first consider the case $k = 1$ and let $K = \mathbb{Q}(\lambda)$, the number field generated by an

algebraic number λ. This is a finite field extension of $\mathbb{Q}$, say of degree d. Then, $\mathbb{Q}(\lambda) \cong \mathbb{Q}^d$ as a $\mathbb{Q}$-vector space, and multiplication by λ is equivalent to a linear map $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Q})$ under this isomorphism. Thus, the problem of estimating $|A + \lambda \cdot A|$ for $A \subset \mathbb{R}$ is equivalent to the problem of estimating $|A' + \mathcal{L}A'|$ for $A' \subset \mathbb{Q}^d$.

In Chapter 7, we make this equivalence precise. In particular, we show that the problem of estimating $|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$ for λ_i algebraic is equivalent to estimating $|\mathcal{L}_0 A + \mathcal{L}_1 \cdot A + \cdots + \mathcal{L}_k \cdot A|$ for pre-commuting matrices $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$. We will define pre-commuting matrices and classify them in Chapter 7. Using this equivalence, we can deduce results about algebraic dilates from linear transformations, and vice versa. As an example, we show that Theorem 1.3.4 can be translated to prove Conjecture 1.4.4 for λ of the form $(p/q)^{1/d}$. In the other direction, we show that Theorem 1.4.5 can be translated to solve Problem 1.3.5 for pre-commuting matrices.

1.5 Sums of dilates mod p

Let us return to the following simple case of Problem 1.1.1 – estimating the minimum size of $|A+\lambda \cdot A|$ in terms of $|A|$. In all the previous sections, we considered A living in an ambient space M without torsion, such as $\mathbb{Z}^d$ or $\mathbb{C}$. This time, we consider $M = \mathbb{Z}/p\mathbb{Z}$, the group of large prime order p, and λ an integer.

Over $\mathbb{Z}$, it is a simple exercise to show that $|A + B| \geq |A| + |B| - 1$. Over $\mathbb{Z}/p\mathbb{Z}$, the corresponding inequality, known as the Cauchy–Davenport theorem [9, 14], says that

$$|A + B| \geq \min\{|A| + |B| - 1, p\},$$

since one must account for the possibility that the sumset contains all the elements of $\mathbb{Z}/p\mathbb{Z}$. Several proofs of this inequality are known (see, for example, [1]), but, unlike the integer case, none of them is particularly simple.

The problem of estimating the minimum size of $|A + \lambda \cdot A|$ over $\mathbb{Z}/p\mathbb{Z}$ with p prime was first studied in detail by Plagne [35] and by Fiz Pontiveros [16]. The latter showed that for every $\lambda \in \mathbb{Z}$ there exists $\alpha > 0$ such that

$$|A + \lambda \cdot A| \geq (|\lambda| + 1)|A| - C_\lambda$$

for all $|A| \leq \alpha p$. On the other hand, he showed that for every $\lambda \in \mathbb{Z}$ and $\epsilon > 0$ there exists $\delta > 0$ such that, for every sufficiently large prime p, there is a set $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|A| \geq (\frac{1}{2} - \epsilon)p$ such that $|A + \lambda \cdot A| \leq (1 - \delta)p$. That is, as $|A|$ approaches

$p/2$, one cannot do much better than the Cauchy–Davenport theorem, which tells us that $|A + \lambda \cdot A| \geq 2|A| - 1$.

For our purposes, it will be convenient to introduce some terminology. For p prime, $\lambda \in \mathbb{Z}$ and $\alpha \in (0, 1)$, we let

$$\mathrm{ex}(\mathbb{Z}/p\mathbb{Z}, \lambda, \alpha) = \min \{|A + \lambda \cdot A|/p : A \subseteq \mathbb{Z}/p\mathbb{Z}, \, |A| \geq \alpha p\}$$

and then define $\mathrm{ex}(\lambda, \alpha) = \limsup_p \mathrm{ex}(\mathbb{Z}/p\mathbb{Z}, \lambda, \alpha)$. The problem of asymptotically estimating the minimum size of sums of dilates over $\mathbb{Z}/p\mathbb{Z}$ may then be rephrased as the problem of determining $\mathrm{ex}(\lambda, \alpha)$. This seems very difficult in full generality, though the results of Fiz Pontiveros described above imply that

- $\mathrm{ex}(\lambda, \alpha) = (|\lambda| + 1)\alpha$ for λ fixed and α sufficiently small in terms of λ and
- $\mathrm{ex}(\lambda, \alpha) < 1$ for $\alpha < \frac{1}{2}$.

We look at the case where α is fixed and λ is allowed to grow. In rough terms, we wish to understand how small the sum of dilates $A + \lambda \cdot A$ can be if we fix the density α of A and let λ tend to infinity. More precisely, we set $\mathrm{ex}(\alpha) = \limsup_{\lambda \to \infty} \mathrm{ex}(\lambda, \alpha)$ and investigate the behavior of $\mathrm{ex}(\alpha)$.

By Cauchy–Davenport, if $\alpha \geq \frac{1}{2}$, then $\mathrm{ex}(\alpha) = 1$. Moreover, if $\alpha \leq \frac{1}{2}$, then, again by Cauchy–Davenport, $|A + \lambda \cdot A| \geq 2|A| - 1$, so $\mathrm{ex}(\alpha) \geq 2\alpha$. On the other hand, since $|A + \lambda \cdot A| \leq p$, we always have the trivial upper bound $\mathrm{ex}(\alpha) \leq 1$.

In Chapter 8, we improve these simple bounds significantly, giving a reasonably complete picture of the behavior of $\mathrm{ex}(\alpha)$.

Theorem 1.5.1. *There exist constants $C, C', c > 0$ such that*

$$e^{C' \log^c(1/\alpha)}\alpha \leq \mathrm{ex}(\alpha) \leq e^{C\sqrt{\log(1/\alpha)}}\alpha$$

for all $\alpha \in (0, \frac{1}{2})$. Moreover, $\mathrm{ex}(\alpha) < 1$ for all $\alpha \in (0, \frac{1}{2})$.

1.6 Notation and preliminaries

For functions $f, g : \mathbb{N} \to \mathbb{R}$, we use the following "Big-O" and Vinogradov notations.

1. We write $f = O(g)$ to mean there exists a constant $C > 0$ such that $|f(n)| \leq Cg(n)$ for all sufficiently large n. We also write $f \ll g$ to mean the same thing.

2. We write $f = o(g)$ to mean $\lim_{n\to\infty} f(n)/g(n) = 0$.

3. We write $f = \Omega(g)$ to mean $g = O(f)$.

4. We write $f = \Theta(g)$ to mean $f = O(g)$ and $g = O(f)$. We also write $f \sim g$ to mean the same thing.

Next, we state some standard results from additive combinatorics which we will be using repeatedly. We have the following sum and difference version of the Ruzsa triangle inequality.

Lemma 1.6.1 (Ruzsa [38])**.** *For any finite subset X, Y, Z of an abelian group, the following holds.*

1. $|X||Y + Z| \leq |X + Y||X + Z|$.

2. $|X||Y - Z| \leq |X - Y||X - Z|$.

For a positive integer m and a set A, denote by mA the m-fold sumset $A + A + \cdots + A$. This is not to be confused with the dilate $m \cdot A$.

Lemma 1.6.2 (Plünnecke–Ruzsa [36])**.** *If A and B are finite subsets of an abelian group and $K > 0$ is a constant so that $|A + B| \leq K|A|$, then for all nonnegative integers m, n, $|mB - nB| \leq K^{m+n}|A|$.*

A fundamental result in additive combinatorics is Freiman's structure theorem. A *generalized arithmetic progression* (or *GAP* for short) is a set P of the form

$$P = \{v_0 + a_1 v_1 + \cdots + a_d v_d : 0 \leq a_i < L_1 \text{ for all } i\}, \tag{1.1}$$

for some integers $v_0, v_1, \ldots, v_d, L_1, \ldots, L_d$, where d is the dimension of the GAP P. We say that P is *proper* if the terms in (1.1) are distinct. Freiman's theorem can then be stated as:

Theorem 1.6.3 (Freiman [17])**.** *Let $K > 0$. Then there exist $d, F > 0$ depending only on K such that the following holds. If $A \subset \mathbb{Z}$ satisfies $|A + A| \leq K|A|$, then A is contained in a proper GAP of dimension at most d and size at most $F|A|$.*

Chapter 2

DIFFERENCE SETS IN $\mathbb{R}^d$

Parts of this chapter are based on the author's publications. The materials have been adapted for inclusion in this thesis.

[1] D. Conlon and J. Lim, Difference sets in $\mathbb{R}^d$, *to appear in Israel Journal of Mathematics* (2025), DOI: 10.1007/s11856-025-2717-2.

Recall from the introduction that a subset A of $\mathbb{R}^d$ is *k-dimensional*, written $\dim(A) = k$, if the dimension of the affine subspace spanned by A is k. In other words, A is contained in an affine subspace of dimension k, but not in an affine subspace of dimension $k-1$. In this chapter, we are interested in the minimum size of $|A-A|$ in terms of $|A|$, where $A \subset \mathbb{R}^d$ is d-dimensional.

For small d, the problem is well understood. Indeed, for $d = 1$, it is an elementary observation that $|A-A| \geq 2|A| - 1$, which is tight for arithmetic progressions, while, for $d = 2$, the bound $|A-A| \geq 3|A| - 3$, tight for the union of two parallel arithmetic progressions with the same length and common difference, was proven by Freiman, Heppes and Uhrin [18]. More generally, they showed that if A is a finite d-dimensional subset of $\mathbb{R}^d$, then

$$|A-A| \geq (d+1)|A| - d(d+1)/2,$$

in analogy with Freiman's result on $|A+A|$. This estimate was later generalized by Ruzsa [37], who showed that if $A, B \subset \mathbb{R}^d$ are finite sets such that $|A| \geq |B|$ and $\dim(A+B) = d$, then

$$|A+B| \geq |A| + d|B| - d(d+1)/2. \tag{2.1}$$

Finally, for $d = 3$, Stanchescu [44], making use of this inequality of Ruzsa, proved that $|A-A| \geq 4.5|A| - 9$ for any finite 3-dimensional subset A of $\mathbb{R}^3$. This is again tight, with the example now being a parallelogram of four parallel arithmetic progressions with the same length and common difference.

In general, the best known construction is due to Stanchescu [45] and comes from a collection of $2d-2$ carefully placed parallel arithmetic progressions with the

same length and common difference. More precisely, set $T = \{e_0, e_1, \dots, e_{d-2}\}$, where e_0 is the origin and $\{e_1, \dots, e_d\}$ is the standard basis for $\mathbb{R}^d$, and, for any natural number k, let $A_k = (T \cup (a_k - T)) + P_k$, where $a_k = e_d - ke_{d-1}$ and $P_k = \{e_0, e_{d-1}, 2e_{d-1}, \dots, (k-1)e_{d-1}\}$. Worked out carefully, this construction satisfies

$$|A_k - A_k| = \left(2d - 2 + \frac{1}{d-1}\right)|A_k| - (2d^2 - 4d + 3).$$

Supplanting an earlier conjecture of Ruzsa [37], Stanchescu proposed that this is best possible.

Conjecture 2.0.1 (Stanchescu [45])**.** *Suppose $d \geq 2$ and $A \subset \mathbb{R}^d$ is a finite set such that* $\dim(A) = d$*. Then*

$$|A - A| \geq \left(2d - 2 + \frac{1}{d-1}\right)|A| - (2d^2 - 4d + 3).$$

Until very recently, little was known about this conjecture for $d \geq 4$ besides the result of Freiman, Heppes and Uhrin [18]. However, the situation was considerably improved by Mudgal [31], who showed that

$$|A - A| \geq (2d-2)|A| - o(|A|)$$

for any finite d-dimensional subset A of $\mathbb{R}^d$. In this chapter, we build on both Mudgal's work and earlier work of Stanchescu [44, 46] to prove Conjecture 2.0.1 in full provided only that $|A|$ is sufficiently large in terms of d, essentially resolving the problem of minimising the value of $|A - A|$ over all d-dimensional sets A of a given size.

Theorem 2.0.2. *Suppose $d \geq 2$ and $A \subset \mathbb{R}^d$ is a finite set such that* $\dim(A) = d$*. Then, provided $|A|$ is sufficiently large in terms of d,*

$$|A - A| \geq \left(2d - 2 + \frac{1}{d-1}\right)|A| - (2d^2 - 4d + 3).$$

We begin our proof of Theorem 2.0.2 in the next section with a result that we believe to be of independent interest, an extension of a result of Stanchescu [46] about the structure of d-dimensional subsets A of $\mathbb{R}^d$ with doubling constant smaller than $d + 4/3$ to asymmetric sums $A + B$.

Remark. *Shortly after completing this paper, we learned from Akshat Mudgal that he had independently proved an asymptotic version of Conjecture 2.0.1. We refer the reader to his paper [32] for further details.*

2.1 An asymmetric version of a theorem of Stanchescu

Our starting point is with the following theorem of Stanchescu [46] (see also [47] for the $d = 3$ case).

Theorem 2.1.1 (Stanchescu [46])**.** *Suppose $d \geq 2$ and $A \subset \mathbb{R}^d$ is a finite set with $\dim(A) = d$. If $|A| > 3 \cdot 4^d$ and $|A + A| < (d + 4/3)|A| - \frac{1}{6}(3d^2 + 5d + 8)$, then A can be covered by d parallel lines.*

By considering the set $A = A_0 \cup \{e_3, \ldots, e_d\}$ with $A_0 = \{ie_1 + je_2 : 0 \leq i < n, 0 \leq j \leq 2\}$ for some natural number n, which satisfies $|A + A| = (d + 4/3)|A| - \frac{1}{6}(3d^2 + 5d + 8)$ and yet cannot be covered by d parallel lines, we see that Theorem 2.1.1 is tight. The main result of this section is an extension of Theorem 2.1.1 to asymmetric sums $A + B$. We begin with the two-dimensional case, whose proof relies in a critical way on the following result of Grynkiewicz and Serra [22, Theorem 1.3].

Lemma 2.1.2 (Grynkiewicz–Serra [22])**.** *Let $A, B \subset \mathbb{R}^2$ be finite sets, let l be a line, let r_1 be the number of lines parallel to l which intersect A and let r_2 be the number of lines parallel to l that intersect B. Then*

$$|A + B| \geq \left(\frac{|A|}{r_1} + \frac{|B|}{r_2} - 1 \right) (r_1 + r_2 - 1).$$

In particular, we note that, since $|B| \geq r_2$ and $r_1 \geq 1$,

$$|A + B| \geq \frac{r_2}{r_1} |A|.$$

Lemma 2.1.3. *Let $A, B \subset \mathbb{R}^2$ be finite sets and l be a fixed line. Let r_1 be the number of lines parallel to l which intersect A. If $|A| \geq |B|$ and $|A+B| < |A|+7|B|/3-5\sqrt{|A|}$, then either $r_1 \leq 2$ or $r_1 > |A|/4$.*

Proof. Notice that if A is at most 1 dimensional, then either $r_1 = 1$ or $r_1 = |A|$, so we may assume that $\dim(A) = 2$. Let r_2 be the number of lines parallel to l which intersect B. We consider 2 cases, depending on whether r_1 is at most $\sqrt{|A|}$ or not.

Case 1: $r_1 \leq \sqrt{|A|}$

We have $10|A|/3 \geq |A+B| \geq |A|r_2/r_1$, so $r_2 \leq 10r_1/3 \leq 4\sqrt{|A|}$. Thus, by Lemma 2.1.2 and the fact that $|A| \geq |B|$,

$$\begin{aligned}|A+B| &\geq \left(\frac{|A|}{r_1} + \frac{|B|}{r_2} - 1\right)(r_1 + r_2 - 1)\\ &= |A| + \frac{r_2-1}{r_1}|A| + \left(1 + \frac{r_1-1}{r_2}\right)|B| - r_1 - r_2 + 1\\ &\geq |A| + \left(1 + \frac{r_2-1}{r_1} + \frac{r_1-1}{r_2}\right)|B| - 5\sqrt{|A|}.\end{aligned}$$

If $r_2 = 1$ and $r_1 \geq 3$, then this last expression is $|A| + r_1|B| - 5\sqrt{|A|} \geq |A| + 3|B| - 5\sqrt{|A|}$. If $r_2 = 2$ and $r_1 \geq 3$, then it is

$$|A| + \left(\frac{1}{2} + \frac{1}{r_1} + \frac{r_1}{2}\right)|B| - 5\sqrt{|A|} \geq |A| + \frac{7}{3}|B| - 5\sqrt{|A|}.$$

If $r_2 \geq 3$ and $r_1 \geq 3$, then it is at least

$$|A| + \left(3 - \frac{1}{r_1} - \frac{1}{r_2}\right)|B| - 5\sqrt{|A|} \geq |A| + \frac{7}{3}|B| - 5\sqrt{|A|}.$$

In each case, we contradict our assumption that $|A+B| < |A| + 7|B|/3 - 5\sqrt{|A|}$, so we must have $r_1 \leq 2$.

Case 2: $r_1 \geq \sqrt{|A|}$

Let $r_1' = |A|/r_1$ and $r_2' = |B|/r_2$, so that $r_1' \leq \sqrt{|A|}$ and

$$|A+B| \geq \left(\frac{|A|}{r_1'} + \frac{|B|}{r_2'} - 1\right)(r_1' + r_2' - 1),$$

which is the same expression as in the previous case, but now r_1', r_2' may not be integers. Nevertheless, we still have $1 \leq r_1' \leq |A|$ and $1 \leq r_2' \leq |B|$, so that $|A+B| \geq \frac{r_2'}{r_1'}|A|$ and, therefore, $r_2' \leq 4\sqrt{|A|}$ holds similarly. Expanding the equation above and using $|A| \geq |B|$, we have

$$\begin{aligned}|A+B| &\geq |A| + \left(1 + \frac{r_2'}{r_1'} + \frac{r_1'-1}{r_2'} - \frac{1}{r_1'}\right)|B| - 5\sqrt{|A|}\\ &\geq |A| + \left(1 + 2\sqrt{\frac{r_1'-1}{r_1'}} - \frac{1}{r_1'}\right)|B| - 5\sqrt{|A|}.\end{aligned}$$

Setting $c = \sqrt{\frac{r_1'-1}{r_1'}}$, we see that if $r_1 \leq |A|/4$ or, equivalently, $r_1' \geq 4$, then $c \geq \frac{\sqrt{3}}{2}$ and the expression above is $|A| + (2c + c^2)|B| - 5\sqrt{|A|} \geq |A| + 7|B|/3 - 5\sqrt{|A|}$. But this again contradicts our assumption, so we must have $r_1 > |A|/4$. □

For higher dimensions, we will use an induction scheme based on taking a series of compressions. Let us first say what a compression is in this context.

Definition 2.1.4. Let H be a hyperplane in $\mathbb{R}^d$ and $v \in \mathbb{R}^d$ a vector not parallel to H. For a finite set $A \subset \mathbb{R}^d$, the *compression of A onto H with respect to v*, denoted by $P(A) = P_{H,v}(A)$, is formed by replacing the points on any line l parallel to v which intersects A at $s \geq 1$ points with the points $u + jv$, $j = 0, 1, \ldots, s-1$, where u is the intersection of l with H.

By preserving the ordering of the points on each line, we may view the compression P as a pointwise map $A \to P(A)$, so we may talk about points of A being fixed by P. Note that it is clearly the case that $|P(A)| = |A|$. Moreover, sumsets cannot increase in size after applying this compression operation. That this is the case is our next result.

Lemma 2.1.5. *For finite sets $A, B \subset \mathbb{R}^d$ and a compression P,*

$$|P(A) + P(B)| \leq |A + B|.$$

Proof. Without loss of generality, we may assume that H passes through the origin. Let $p : \mathbb{R}^d \to H$ be the projection onto H along v. For $u \in p(A)$, let l_u be the line through u parallel to v and define $X_u = X \cap l_u$ for any set $X \subset \mathbb{R}^d$. Note that $p(P(A)) = p(A)$ and so $p(P(A) + P(B)) = p(A + B)$. It therefore suffices to show that $|(P(A) + P(B))_u| \leq |(A + B)_u|$ for each $u \in p(A + B) = p(A) + p(B)$. Since $P(A)_x$ is a set of the form $\{x + jv : j = 0, \ldots, s-1\}$, we have

$$\begin{aligned}
|(P(A) + P(B))_u| &= \max\left\{|P(A)_x + P(B)_y| : x \in p(A), y \in p(B), x + y = u\right\} \\
&= \max\left\{|P(A)_x| + |P(B)_y| - 1 : x \in p(A), y \in p(B), x + y = u\right\} \\
&= \max\left\{|A_x| + |B_y| - 1 : x \in p(A), y \in p(B), x + y = u\right\} \\
&\leq |(A + B)_u|.
\end{aligned}$$

□

Our main compression lemma, which draws on ideas in the work of Stanchescu [46, 47], is now as follows.

Lemma 2.1.6. *Let $A, B \subset \mathbb{R}^d$ be finite sets such that $\dim(A) = d \geq 3$ and l be a fixed line. Suppose that there are exactly $s < |A|$ lines parallel to l which intersect A. Then there are sets $A', B' \subset \mathbb{R}^d$ satisfying the following properties:*

1. $|A'| = |A|$, $|B'| = |B|$;

2. $|A' + B'| \leq |A + B|$;

3. *there are exactly* s *lines* $l'_1, \ldots, l'_s$ *parallel to* l *intersecting* A';

4. $\dim(A') = d$;

5. $l'_1, \ldots, l'_{s-1}$ *lie on a hyperplane;*

6. l'_s *intersects* A' *at a single point.*

Proof. The sets A', B' will be obtained by taking a series of compressions, so 1 and 2 will automatically be satisfied by Lemma 2.1.5. Let $e_1, \ldots, e_d$ be the standard basis of $\mathbb{R}^d$. By applying an affine transformation if necessary, we may assume that l is the line $\mathbb{R}e_d$ and that A contains the set $S = \{0, e_1, \ldots, e_d\}$ (this is possible since at least one line parallel to l intersects A in at least 2 points). For each i, let H_i be the hyperplane through 0 perpendicular to e_i. Let $P_i = P_{H_i, e_i}$ be the compression onto H_i with respect to e_i. Let $A_1 = P_d(A)$, noting that this set satisfies 3 and $s = |A_1 \cap H_d|$. Furthermore, for any compression P_i, $i < d$, $|P_i(A_1) \cap H_d| = s$, so $P_i(A_1)$ also satisfies 3. Now set $A_2 = P_1(P_2(\cdots P_{d-1}(A_1)\cdots))$. Then $A_2 \subset \mathbb{N}_0^d$ again satisfies 3 and, since $S \subseteq A_2$, $\dim(A_2) = d$ and it also satisfies 4. Moreover, A_2 has the property that if $(x_1, \ldots, x_d) \in A_2$, then, for any $y_1, \ldots, y_d \in \mathbb{N}_0$ with $y_i \leq x_i$ for all i, $(y_1, \ldots, y_d) \in A_2$.

We now show that a finite number of further compressions will give us a set additionally satisfying 5 and 6. Suppose A_2 can be covered by n hyperplanes parallel to H_{d-1}, i.e., the $(d-1)$th coordinate of all the points of A_2 is the set $\{0, 1, \ldots, n-1\}$. Let $w = (w_1, \ldots, w_{d-2}, 0, 0) \in A_2$ be such that $w_1 + \cdots + w_{d-2}$ is maximal. Then, whenever $tw + u \in A_2 \cap H_{d-1} \cap H_d$ for some $u \in \mathbb{N}_0^d$ and $t \geq 1$, we must have $u = 0$ and $t = 1$. Let P be the compression onto H_{d-1} with respect to $f = e_{d-1} - w$. Set $A_3 = P(A_2)$. Since f is parallel to H_d, $|A_3 \cap H_d| = |A_2 \cap H_d| = s$. The number of lines through A_3 parallel to l is $|A_3 \cap H_d| = s$, so 3 is still satisfied. Moreover, since $w \in A_2$, e_{d-1} is fixed by P, so $S \subseteq A_3$ and 4 is still satisfied. We now consider two cases:

Case 1: $n = 2$

We claim that A_3 is covered by H_{d-1} and the single line $e_{d-1} + \mathbb{R}e_d$, so that 5 is satisfied with $l'_s = e_{d-1} + \mathbb{R}e_d$. Indeed, by the maximality of $\|w\|_1$, the points of A_2 on any vertical line $u + \mathbb{R}e_d$ with $u \in H_d \setminus \{e_{d-1}\}$ are mapped by P into a vertical

line contained in H_{d-1}. To see this, suppose $e_{d-1}+re_d+v \in A_2$ with $v \in H_{d-1} \cap H_d$ and $r \in \mathbb{N}_0$. Then $e_{d-1} + re_d + v$ is fixed by P iff $v + re_d + w \in A_2$. If $v \neq 0$, then $v + w \notin A_2$ by the maximality of w, so $v + re_d + w \notin A_2$ and $e_{d-1} + re_d + v$ is not fixed by the compression, being moved instead to $v + re_d + w$.

Case 2: $n > 2$

Suppose $(n-1)e_{d-1} + v \in A_2$ with $v \in H_{d-1}$. Then, since $(n-1)w + v \notin A_2$ as in Case 1, $(n-1)e_{d-1} + v$ is not fixed by the compression. Thus, A_3 is contained in fewer than n hyperplanes parallel to H_{d-1}. By repeatedly applying compressions of this type, we will eventually reach the previous case. Abusing notation very slightly, we shall still call the set obtained after these repeated compressions A_3.

Thus, A_3 is covered by H_{d-1} and the line $e_{d-1} + \mathbb{R}e_d$. Suppose now that $r > 0$ is the largest integer such that $re_d \in A_3$. Let P' be the compression with respect to $g = e_{d-1} - re_d$ and set $A_4 = P'(A_3)$. Then all points of A_3 in H_{d-1} and e_{d-1} are fixed by P', but $e_{d-1} + te_d$ is mapped to $(r + t)e_d$ for each $t > 0$. Thus, $A_4 \cap (e_{d-1} + H_{d-1}) = \{e_{d-1}\}$, so that A_4 satisfies 3-6. We may therefore set $A' = A_4$. Finally, to obtain B', we simply apply the same series of compressions to B that we applied to A. □

We are now in a position to prove the main result of this section, the promised asymmetric version of Theorem 2.1.1.

Theorem 2.1.7. *Let $d \geq 2$, $A, B \subset \mathbb{R}^d$ be finite sets and l be a line. Let r be the number of lines parallel to l which intersect A. Suppose that A is d-dimensional, $|A| \geq |B|$ and $|A+B| < |A|+(d+1/3)|B|-2^{d+1}\sqrt{|A|}-E_d$, where $E_d = (d+2)^{2^d-2}$. Then $r = d$ or $r > |A|/4$.*

Proof. Notice that since $\dim(A) = d$, we must have $r \geq d$. We shall induct on d. The case $d = 2$ was dealt with in Lemma 2.1.3. We may therefore assume that $d \geq 3$. E_d is chosen to satisfy the following inequalities:

1. $E_d \geq 2(E_{d-1} + 1)$,
2. $E_d \geq (d + 2)(2^d + E_{d-1} + 1)^2$.

If $|A| \le (2^d + E_{d-1} + 1)^2$, then $|A| + (d + 1/3)|B| \le (d + 2)|A| \le E_d$, so it is not possible that $|A + B| < |A| + (d + 1/3)|B| - 2^{d+1}\sqrt{|A|} - E_d$. We may therefore assume that $|A| > (2^d + E_{d-1} + 1)^2$ and, thus, that $|A| - 2^d\sqrt{|A|} - E_{d-1} - 1 \ge 0$.

Suppose that $d < r \le |A|/4$. By Lemma 2.1.6, replacing A with A', we can assume that $A = A_1 \cup \{e_d\}$, where A_1 lies on the hyperplane H defined by $x_d = 0$. Let $H_1, \dots, H_s$ be the hyperplanes parallel to H that intersect B and let $B_i = B \cap H_i$.

If $s = 1$, then $|A + B| = |A_1 + B| + |B|$. Moreover, A_1 is $(d - 1)$-dimensional and is covered by $r - 1 \le |A_1|/4$ lines parallel to l. Thus, if $|B| \le |A_1|$, our induction hypothesis implies that $|A_1+B| \ge |A_1|+(d-1+1/3)|B|-2^d\sqrt{|A_1|}-E_{d-1}$. If instead $|B| > |A_1|$, then $|B| = |A_1| + 1$, so, letting B' be B with an element removed, our induction hypothesis implies that $|A_1 + B| \ge |A_1 + B'| \ge |A_1| + (d - 1 + 1/3)(|B| - 1) - 2^d\sqrt{|A_1|} - E_{d-1}$. In either case, we have

$$\begin{aligned} |A + B| &\ge |A_1| + (d + 1/3)(|B| - 1) - 2^d\sqrt{|A_1|} - E_{d-1} \\ &\ge |A| + (d + 1/3)|B| - 2^{d+1}\sqrt{|A|} - E_d. \end{aligned}$$

If $s \ge 2$, then $|A + B| \ge |A_1 + B| = |A_1 + B_1| + \cdots + |A_1 + B_s|$. By our induction hypothesis, $|A_1 + B_i| \ge |A_1| + (d - 1 + 1/3)|B_i| - 2^d\sqrt{|A_1|} - E_{d-1}$ for each i and so

$$\begin{aligned} |A + B| &\ge s|A_1| + (d - 1 + 1/3)|B| - 2^d s\sqrt{|A_1|} - sE_{d-1} \\ &\ge 2|A| + (s - 2)|A| - s + (d - 1 + 1/3)|B| \\ &\qquad - 2^{d+1}\sqrt{|A|} - 2^d(s - 2)\sqrt{|A|} - sE_{d-1} \\ &\ge |A| + (d + 1/3)|B| - 2^{d+1}\sqrt{|A|} - 2(E_{d-1} + 1) \\ &\qquad + (s - 2)(|A| - 2^d\sqrt{|A|} - E_{d-1} - 1) \\ &\ge |A| + (d + 1/3)|B| - 2^{d+1}\sqrt{|A|} - E_d. \end{aligned}$$

□

2.2 Special cases of Theorem 2.0.2

In this section, we show that the conclusion of Theorem 2.0.2 holds if we make some additional assumptions about the structure of A. We begin with a simple example of such a result.

Lemma 2.2.1. *Let $A \subset \mathbb{R}^d$ be a finite set with $\dim(A) = d$ that can be covered by d parallel lines. Then*

$$|A - A| \ge \left(2d - 2 + \frac{2}{d}\right)|A| - (d^2 - d + 1).$$

Proof. Suppose $A = A_1 \cup \cdots \cup A_d$ where each A_i lies on a line parallel to some fixed line l. Let $a_i = |A_i|$ and assume, without loss of generality, that $a_1 \geq a_2 \geq \cdots \geq a_d$. Since A is d-dimensional, the d lines covering A are in general position, i.e., no k of them lie on a $(k-1)$-dimensional affine subspace for each $1 \leq k \leq d$. Thus, for $i \neq j$, the sets $A_i - A_j$ are pairwise disjoint and also disjoint from $A_1 - A_1$. Hence, we have

$$\begin{aligned} |A - A| &\geq |A_1 - A_1| + \sum_{i \neq j} |A_i - A_j| \\ &\geq 2a_1 - 1 + \sum_{i \neq j} (a_i + a_j - 1) \\ &\geq 2a_1 - 1 + 2(d-1) \sum_i a_i - d(d-1) \\ &\geq \left(2d - 2 + \frac{2}{d}\right) |A| - (d^2 - d + 1). \end{aligned}$$

□

We will use a common framework for the next two lemmas, with the following definition playing a key role.

Definition 2.2.2. Let $A \subset \mathbb{R}^d$ be a finite set with $\dim(A) = d$ and l be a fixed line. A hyperplane H is said to be a *supporting hyperplane* of A if all points of A either lie on H or on one side of H. A supporting hyperplane H of A is said to be a *major hyperplane of A (with respect to l)* if H is parallel to l and $|H \cap A|$ is maximal.

Suppose now that $A \subset \mathbb{R}^d$ is d-dimensional and l is a fixed line. Let H be a major hyperplane with respect to l and $H_1 = H, H_2, \ldots, H_r$ be the hyperplanes parallel to H that intersect A, arranged in the natural order. Let $A_i = A \cap H_i$ for $i = 1, \ldots, r$. Since $|A_1|$ is maximal, $|A_1| \geq |A_r|$. Let π be the projection along l onto a hyperplane perpendicular to l. Then $\dim(\pi(A)) = d - 1$ and $\pi(H)$ is a maximal face of the convex hull of $\pi(A)$ (since $|H \cap A|$ is maximal), so $\dim(\pi(A_1)) = d - 2$, which implies that there are at least $d - 1$ lines parallel to l intersecting A_1. If any such line intersects A_1 in at least 2 points, then $\dim(A_1) = d - 1$. Assuming this setup, the next lemma explores the situation where A is covered by two parallel hyperplanes.

Lemma 2.2.3. *Suppose that* $r = 2$, $\dim(A_1) = d - 1$ *and there are* s *lines parallel to* l *intersecting* A_1.

1. *If $s = d - 1$, then*

$$|A - A| \geq (2d-2)\,|A| + \frac{2}{d-1}|A_1| - (2d^2 - 4d + 3)$$
$$\geq \left(2d - 2 + \frac{1}{d-1}\right)|A| - (2d^2 - 4d + 3).$$

2. *If $d \leq s \leq |A_1|/4$ and*

$$|A_1 - A_1| \geq \left(2d - 4 + \frac{1}{d-2}\right)|A_1| - (2d^2 - 8d + 9),$$

then, given $0 < \epsilon < \min(\frac{2}{3}, \frac{1}{d-2}) - \frac{1}{d-1}$, there is some n_0 such that for $|A| \geq n_0$,

$$|A - A| \geq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|A|.$$

Proof. For 1, note, by Lemma 2.2.1, that

$$|A_1 - A_1| \geq \left(2d - 4 + \frac{2}{d-1}\right)|A_1| - (d^2 - 3d + 3).$$

By Ruzsa's inequality (2.1), $|A_1 - A_2| \geq |A_1| + (d-1)|A_2| - d(d-1)/2$ and so

$$\begin{aligned}
|A - A| &\geq |A_1 - A_1| + 2|A_1 - A_2| \\
&\geq \left(2d - 2 + \frac{2}{d-1}\right)|A_1| + (2d-2)|A_2| - d(d-1) - (d^2 - 3d + 3) \\
&\geq (2d-2)|A| + \frac{2}{d-1}|A_1| - (2d^2 - 4d + 3) \\
&\geq \left(2d - 2 + \frac{1}{d-1}\right)|A| - (2d^2 - 4d + 3).
\end{aligned}$$

For 2, A_1 is $(d-1)$-dimensional and cannot be covered by $d-1$ lines, so this case only exists for $d \geq 3$. Since $|A_1| \geq |A_2|$, Theorem 2.1.7 implies that

$$|A_1 - A_2| \geq |A_1| + (d - 2/3)|A_2| - 2^d\sqrt{|A_1|} - E_{d-1}.$$

But then, since $|A_1| \geq |A|/2$ can be taken sufficiently large,

$$\begin{aligned}
|A - A| &\geq |A_1 - A_1| + 2|A_1 - A_2| \\
&\geq \left(2d - 4 + \frac{1}{d-2}\right)|A_1| - (2d^2 - 8d + 9) \\
&\qquad + 2|A_1| + 2(d - 2/3)|A_2| - 2^{d+1}\sqrt{|A_1|} - 2E_{d-1} \\
&\geq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|A| + \left(\frac{1}{(d-1)(d-2)} - \epsilon\right)|A_1| \\
&\qquad - (2d^2 - 8d + 9) - 2^{d+1}\sqrt{|A_1|} - 2E_{d-1} \\
&\geq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|A|,
\end{aligned}$$

as required. □

We now consider the situation where every line parallel to l meets A in a reasonable number of points.

Lemma 2.2.4. *Let $0 < \epsilon < 1/(4d+1)(d-1)$. Suppose that every line parallel to l intersecting A intersects A in at least $4d$ points. Then there is a constant C_d such that either*

1. $$|A - A| \geq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|A| - C_d$$

   or

2. $r = 2$ *and*

$$|A - A| \geq (2d-2)|A| + \frac{2}{d-1}|H \cap A| - (2d^2 - 4d + 3).$$

In particular,

$$|A - A| \geq \left(2d - 2 + \frac{1}{d-1}\right)|A| - (2d^2 - 4d + 3)$$

for $|A|$ sufficiently large.

Proof. We shall induct on d and $|A|$. Let n_0 be chosen sufficiently large that the following conditions hold:

1. Lemma 2.2.3 holds with this n_0.
2. Whenever $B \subset \mathbb{R}^d$ has $\dim(B) = d - 1 > 1$, each line parallel to l intersecting B intersects it in at least $4(d-1)$ points and $|B| \geq n_0/2$, then

$$|B - B| \geq \left(2d - 4 + \frac{1}{d-2}\right)|B| - (2d^2 - 8d + 9).$$

   This is possible by induction since C_{d-1} is already determined.

3. $\epsilon n_0 \geq d(d-1)$.

Then $C_d \geq 2d^2 - 4d + 3$ is chosen sufficiently large that the first option in the lemma trivially holds for $|A| \leq n_0$.

The base case $d = 2$ and the inductive step will be handled together. If $|A| \leq n_0$, the lemma holds, so we may assume that $|A| > n_0$. Since $\dim(A_1) = d - 1$, there are at least $d - 1$ lines parallel to l intersecting A_1. Each such line intersects A_1 in at least $4d$ points, so we have $|A_1| \geq 4d(d-1)$.

First suppose $r = 2$. If A_1 is covered by s lines parallel to l, then, as above, $s \geq d - 1$. If $s = d - 1$, then, by Lemma 2.2.3,

$$|A - A| \geq (2d-2)|A| + \frac{2}{d-1}|A_1| - (2d^2 - 4d + 3).$$

If $s > d - 1$, then we must have $d > 2$, since, for $d = 2$, $\dim(A_1) = 1$ and A_1 is covered by a single line. Since $\dim(A_1) = d - 1 > 1$ and $|A_1| \geq |A|/2 \geq n_0/2$, condition 2 implies that

$$|A_1 - A_1| \geq \left(2d - 4 + \frac{1}{d-2}\right)|A_1| - (2d^2 - 8d + 9).$$

Each line parallel to l passes through at least 4 points of A_1, so $s \leq |A_1|/4$. Thus, by Lemma 2.2.3 and condition 1,

$$|A - A| \geq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|A|.$$

Now suppose $r > 2$. Let $B = A \setminus H_r$ and note that $\dim(B) = d$ and $|B| \geq |A|/2$. By our induction hypothesis,

$$|B - B| \geq \left(2d - 2 + \frac{1}{d-1}\right)|B| - C_d.$$

Let H' be a major hyperplane of B with respect to l (which is not necessarily a major hyperplane of A!), so that $|B \cap H'| \geq |A_1|$. If $|A_1| \geq 2\epsilon|A|$, then, using Ruzsa's inequality (2.1) and condition 3,

$$\begin{aligned}
|A - A| &\geq |B - B| + 2|A_1 - A_r| \\
&\geq \left(2d - 2 + \frac{1}{d-1}\right)|B| - C_d + 2|A_1| + (2d-2)|A_r| - d(d-1) \\
&\geq \left(2d - 2 + \frac{1}{d-1}\right)|A| + \left(2 - \frac{1}{d-1}\right)|A_1| - C_d - d(d-1) \\
&\geq \left(2d - 2 + \frac{1}{d-1} + 2\epsilon\right)|A| - C_d - d(d-1) \\
&\geq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|A| - C_d.
\end{aligned}$$

We may therefore assume that $|A_1| < 2\epsilon|A|$.

If B cannot be covered by two translates of H', then, by our induction hypothesis,

$$|B - B| \geq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|B| - C_d.$$

Thus, again using Ruzsa's inequality (2.1),

$$\begin{aligned}
|A - A| &\geq |B - B| + 2|A_1 - A_r| \\
&\geq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|B| + 2|A_1| + (2d-2)|A_r| - d(d-1) - C_d \\
&\geq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|A| + \left(2 - \frac{1}{d-1} - \epsilon\right)|A_1| - d(d-1) - C_d \\
&\geq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|A| - C_d,
\end{aligned}$$

since $|A_1| \geq 4d(d-1)$.

We may therefore assume that B is covered by two translates of H', say H' and H''. If $A_r \subseteq H' \cup H''$, then $A \subseteq H' \cup H''$, so one of $|A \cap H'|, |A \cap H''|$ is at least $|A|/2$, say $|A \cap H'| \geq |A|/2$. But H is a major hyperplane of A, so $|A_1| = |A \cap H| \geq |A \cap H'| \geq |A|/2$, contradicting our assumption that $|A_1| < 2\epsilon|A|$. Hence, $A_r \nsubseteq H' \cup H''$.

If

$$|B - B| \geq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|B| - C_d,$$

then the above argument holds similarly. Thus, by our induction hypothesis, we must have that

$$|B - B| \geq (2d-2)|B| + \frac{2}{d-1}|H' \cap B| - (2d^2 - 4d + 3).$$

Let $B_1 = B \cap H'$, $B_2 = B \cap H''$, noting that $|B_1| \geq |B_2|$. Fix also a point $x \in A_r$ that does not lie on $H' \cup H''$. If x lies between H' and H'', then $x - B_1, B_1 - x, B - B$ are pairwise disjoint. If H' lies between x and H'', then $x - B_2, B_2 - x, B - B$ are pairwise disjoint. If H'' lies between x and H', then $x - B_1, B_1 - x, B - B$ are pairwise disjoint. In any case, there is some $i \in \{1, 2\}$ such that $x - B_i, B_i - x, B - B$ are pairwise disjoint. Since $|B_1| \geq |B_2|$,

$$\begin{aligned}|A-A| &\geq |B-B| + 2|B_2| \\ &\geq (2d-2)\,|B| + \frac{2}{d-1}|B_1| - (2d^2-4d+3) + 2|B_2| \\ &\geq \left(2d-2+\frac{2}{d-1}\right)|B| - (2d^2-4d+3) \\ &= \left(2d-2+\frac{2}{d-1}\right)(|A|-|A_r|) - (2d^2-4d+3) \\ &\geq \left(2d-2+\frac{1}{d-1}+\epsilon\right)|A| - C_d,\end{aligned}$$

where the last inequality follows from $|A_r| \leq |A_1| \leq 2\epsilon|A|$ and $\epsilon < 1/(4d+1)(d-1)$. □

2.3 Proof of Theorem 2.0.2

The final ingredient in our proof is the following structure theorem due to Mudgal [33, Lemma 3.2], saying that sets with small doubling in $\mathbb{R}^d$ can be almost completely covered by a reasonably small collection of parallel lines.

Lemma 2.3.1 (Mudgal [33])**.** *For any $c > 0$, there exist constants $0 < \sigma \leq 1/2$ and $C > 0$ such that if $A \subset \mathbb{R}^d$ is a finite set with $|A| = n$ and $|A+A| \leq cn$, then there exist parallel lines $l_1, l_2, \ldots, l_r$ with*

$$|A \cap l_1| \geq \cdots \geq |A \cap l_r| \geq |A \cap l_1|^{1/2} \geq C^{-1}n^{\sigma}$$

and

$$|A \setminus (l_1 \cup l_2 \cup \cdots \cup l_r)| < Ccn^{1-\sigma}.$$

We are now ready to prove Theorem 2.0.2, which, we recall, states that if $d \geq 2$ and $A \subset \mathbb{R}^d$ is a finite set such that $\dim(A) = d$, then, provided $|A|$ is sufficiently large,

$$|A-A| \geq \left(2d-2+\frac{1}{d-1}\right)|A| - (2d^2-4d+3).$$

Proof of Theorem 2.0.2. We shall proceed by induction on d, starting from the known case $d = 2$ [18]. We will suppose throughout that n_0 is large enough for our arguments to hold. Our aim is to show that, for all $A \subset \mathbb{R}^d$ with $\dim(A) = d$,

$$|A-A| \geq \left(2d-2+\frac{1}{d-1}\right)|A| - \max(2d^2-4d+3, D-|A|/3),$$

where $D \geq 2d^2 - 4d + 3$ is chosen so that the above inequality trivially holds for $|A| \leq n_0$. The result then clearly follows for $|A|$ sufficiently large. We will proceed by induction on $|A|$, where the base case $|A| \leq n_0$ trivially holds.

We may clearly assume that $|A - A| \leq (2d-1)|A|$, since otherwise we already have the required conclusion. By the Plünnecke–Ruzsa inequality (Lemma 1.6.2), we then have $|A + A| \leq (2d-1)^2|A|$. Applying Lemma 2.3.1 with $c = (2d-1)^2$, we get parallel lines $l_1, \ldots, l_r$ and constants $0 < \sigma \leq 1/2$ and $C > 0$ such that

$$|A \cap l_1| \geq \cdots \geq |A \cap l_r| \geq |A \cap l_1|^{1/2} \geq C^{-1}n^{\sigma}$$

and

$$|A \setminus (l_1 \cup l_2 \cup \cdots \cup l_r)| < Ccn^{1-\sigma},$$

where $n = |A|$. Since $|A \cap l_i| \geq C^{-1}n^{\sigma}$ for each i, we have $n = |A| \geq rC^{-1}n^{\sigma}$ or $r \leq Cn^{1-\sigma}$. Let $A' = A \cap (l_1 \cup \cdots \cup l_r)$ and $S = A \setminus A'$, so that $|S| < Ccn^{1-\sigma}$. If $\dim(A') = d_1 < d$, then, by our induction hypothesis, for $|A|$ sufficiently large,

$$|A' - A'| \geq \left(2d_1 - 2 + \frac{1}{d_1 - 1}\right)|A'| - (2d_1^2 - 4d_1 + 3).$$

There are $a_1, \ldots, a_{d-d_1} \in S$ such that $\dim(A' \cup \{a_1, \ldots, a_{d-d_1}\}) = d$. This implies that $a_1, \ldots, a_{d-d_1}$ lie outside the affine span of A', so the sets

$$A' - A', A' - a_1, \ldots, A' - a_{d-d_1}, a_1 - A', \ldots, a_{d-d_1} - A'$$

are pairwise disjoint. Thus,

$$\begin{aligned}
|A - A| &\geq |A' - A'| + \sum_{i=1}^{d-d_1} (|A' - a_i| + |a_i - A'|) \\
&\geq \left(2d_1 - 2 + \frac{1}{d_1 - 1}\right)|A'| - (2d_1^2 - 4d_1 + 3) + 2(d - d_1)|A'| \\
&\geq \left(2d - 2 + \frac{1}{d_1 - 1}\right)(|A| - |S|) - (2d_1^2 - 4d_1 + 3) \\
&\geq \left(2d - 2 + \frac{1}{d - 1}\right)|A|
\end{aligned}$$

for $|A| \geq n_0$ sufficiently large. Thus, we may assume that $\dim(A') = d$.

For n_0 sufficiently large, we may assume that each line l_i intersects A' in at least $4d$ points. Let H be a major hyperplane of A' with respect to l_1 and let $H_1 =$

$H, H_2, \ldots, H_r$ be the translates of H covering A' in the natural order. Fix $0 < \epsilon < 1/(4d+1)(d-1)$. If we are in the case of Lemma 2.2.4 where

$$|A' - A'| \geq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|A'| - C_d,$$

then, since $|S| = O(|A|^{1-\sigma})$ is sublinear, for $|A|$ sufficiently large,

$$\begin{aligned}|A - A| &\geq |A' - A'| \\ &\geq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|A'| - C_d \\ &\geq \left(2d - 2 + \frac{1}{d-1}\right)|A|.\end{aligned}$$

Thus, we may assume that $r = 2$ and

$$|A' - A'| \geq (2d-2)|A'| + \frac{2}{d-1}|A_1'| - (2d^2 - 4d + 3).$$

Let $A_1' = A' \cap H_1$ and $A_2' = A' \cap H_2$. If $S \not\subseteq H_1 \cup H_2$, then there is a point $x \in S$ not lying on the hyperplanes H_1, H_2. But then $x - A_i', A_i' - x, A' - A'$ are pairwise disjoint for some $i \in \{1, 2\}$ and so, since $|A_1'| \geq |A_2'|$,

$$\begin{aligned}|A - A| &\geq |A' - A'| + 2|A_2'| \\ &\geq (2d-2)|A'| + \frac{2}{d-1}|A_1'| - (2d^2 - 4d + 3) + 2|A_2'| \\ &\geq \left(2d - 2 + \frac{2}{d-1}\right)|A'| - (2d^2 - 4d + 3) \\ &\geq \left(2d - 2 + \frac{1}{d-1}\right)|A|.\end{aligned}$$

We may therefore assume that $S \subseteq H_1 \cup H_2$.

Let $A_1 = A \cap H_1$ and $A_2 = A \cap H_2$. Let H' be a major hyperplane of A with respect to l_1 (possibly equal to H) and $H_1' = H', H_2', \ldots, H_s'$ be the translates of H' covering A, ordered naturally. Let $B_i = A \cap H_i'$ for $i = 1, \ldots, s$. Since H_1, H_2 are both supporting hyperplanes of A, we must have $|B_1| \geq \max(|A_1|, |A_2|) \geq |A|/2 > |S|$, so B_1 must contain at least one point of A'. Hence, B_1 contains one of the lines $l_i \cap A$, each of which has at least 2 points, and so $\dim(B_1) = d - 1$.

Suppose $s = 2$. The number of lines parallel to l_1 intersecting B_1 is at most $r + |S| = O(|A|^{1-\sigma})$, which is smaller than $|B_1|/4$. Thus, for n_0 sufficiently large, by both cases of Lemma 2.2.3,

$$|A - A| \geq \left(2d - 2 + \frac{1}{d-1}\right)|A| - (2d^2 - 4d + 3).$$

We may therefore assume that $s > 2$. Let $B = A \setminus B_s$, noting that $|B| \geq |A|/2$ and $\dim(B) = d$. By our induction hypothesis,

$$|B - B| \geq \left(2d - 2 + \frac{1}{d-1}\right)|B| - D.$$

Thus, again using Ruzsa's inequality (2.1),

$$\begin{aligned}
|A - A| &\geq |B - B| + 2|B_1 - B_s| \\
&\geq \left(2d - 2 + \frac{1}{d-1}\right)|B| - D + 2|B_1| + (2d-2)|B_s| - d(d-1) \\
&\geq \left(2d - 2 + \frac{1}{d-1}\right)|A| + \left(2 - \frac{1}{d-1}\right)|B_1| - d(d-1) - D \\
&\geq \left(2d - 2 + \frac{1}{d-1}\right)|A| + \left(1 - \frac{1}{2(d-1)}\right)|A| - d(d-1) - D \\
&\geq \left(2d - 2 + \frac{1}{d-1}\right)|A| - D + |A|/3,
\end{aligned}$$

where the last inequality holds if $|A|/6 \geq n_0/6 \geq d(d-1)$. □

2.4 Concluding remarks

By carefully analysing our proof of Theorem 2.0.2, it is possible to deduce some structural properties of large sets $A \subset \mathbb{R}^d$ with $\dim(A) = d$ and

$$|A - A| \leq \left(2d - 2 + \frac{1}{d-1}\right)|A| + o(|A|).$$

In particular, such sets can be covered by two parallel hyperplanes H_1 and H_2, where, writing $A_1 = A \cap H_1$ and $A_2 = A \cap H_2$, we can assume that A_1 and A_2 have roughly the same size, differing by $o(|A|)$. We can also assume that $\dim(A_1) = d - 1$ and that A_1 can be covered by $d - 1$ parallel lines $l_1, \ldots, l_{d-1}$, where the sets $A_1 \cap l_i$ all have approximately equal size, again up to $o(|A|)$.

In practice, H_1 will be a major hyperplane of A with respect to l_1, which, we recall, means that it is parallel to l_1, it is supporting, in the sense that all points of A lie either on or on one side of it, and $|H_1 \cap A|$ is as large as possible. Knowing this allows us to also deduce that $\dim(A_2) = d - 1$. Indeed, it must be the case that the affine span of A_2 is parallel to l_1, since otherwise $|A_1 - A_2|$ would be too large. But then, if $\dim(A_2) < d - 1$, there is a supporting hyperplane through A_2 and one of the $A_1 \cap l_i$ which contains more points than H_1, contradicting the fact that H_1 is a major hyperplane. Since $|A_1|$ and $|A_2|$ differ by $o(|A|)$, this then allows us to argue that A_2 is also covered by $d - 1$ lines parallel to l_1 of approximately equal size.

In fact, we can deduce the very same structural properties for large sets $A \subset \mathbb{R}^d$ with $\dim(A) = d$ and

$$|A - A| \leq \left(2d - 2 + \frac{1}{d-1} + \epsilon\right)|A| + o(|A|)$$

for some $\epsilon > 0$, giving a difference version of Stanchescu's result about the structure of d-dimensional subsets of $\mathbb{R}^d$ with doubling constant smaller than $d + 4/3$, which we stated as Theorem 2.1.1. It would be interesting to determine the maximum value of ϵ for which this continues to hold.

Unfortunately, our methods tell us very little about how A_1 and A_2 are related, though we suspect that A_2 should be close to a translate of $-A_1$. Proving this, which will likely require a better understanding of when Ruzsa's inequality (2.1) is tight, may then lead to a determination of the exact structure of d-dimensional subsets A of $\mathbb{R}^d$ with $|A - A|$ as small as possible in terms of $|A|$, a problem that was already solved for $d = 2$ and 3 by Stanchescu [44].

Chapter 3

SUMS OF LINEAR TRANSFORMATIONS

Parts of this chapter are based on the author's publications. The materials have been adapted for inclusion in this thesis.

[1] D. Conlon and J. Lim, Sums of linear transformations, *to appear in Transactions of the American Mathematical Society* (2025), arXiv:2203.09827, DOI: 10.1090/tran/9433.

In this chapter, we look into the following conjecture of Bukh mentioned in the introduction.

Conjecture 3.0.1. *Suppose that* $\mathcal{L}_1, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ *have no common non-trivial invariant subspace and* $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d = \mathbb{Z}^d$. *Then, for any finite subset* A *of* $\mathbb{Z}^d$,

$$|\mathcal{L}_1 A + \cdots + \mathcal{L}_k A| \geq (|\det(\mathcal{L}_1)|^{1/d} + \cdots + |\det(\mathcal{L}_k)|^{1/d})^d |A| - o(|A|).$$

For $d = 1$, this is the problem on integer dilates, which was solved by Bukh [8]. For larger d, the intuition behind this conjecture comes from the Brunn–Minkowski inequality (see, for example, [19]). This classic inequality states that if A and B are two non-empty compact subsets of $\mathbb{R}^d$, then

$$\mu(A+B)^{1/d} \geq \mu(A)^{1/d} + \mu(B)^{1/d},$$

where μ is the Lebesgue measure on $\mathbb{R}^d$. Since $\mu(\mathcal{L}A) = |\det(\mathcal{L})|\mu(A)$ for any $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{R})$ and any measurable subset A of $\mathbb{R}^d$, we may conclude that, for any $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{R})$,

$$\begin{aligned}\mu(\mathcal{L}_1 A + \mathcal{L}_2 A) &\geq (\mu(\mathcal{L}_1 A)^{1/d} + \mu(\mathcal{L}_2 A)^{1/d})^d \\ &\geq (|\det(\mathcal{L}_1)|^{1/d} + |\det(\mathcal{L}_2)|^{1/d})^d \mu(A).\end{aligned}$$

Moreover, the analogous statement holds for the sum of more transformations by a simple induction. Conjecture 3.0.1 is then the statement that, under appropriate technical conditions, a discrete analogue of this result should hold, possibly with some correction term to deal with boundary effects.

The first result towards this conjecture was given by Mudgal [33], who showed that if $\mathcal{L} \in GL_2(\mathbb{R})$ has no real eigenvalues, then $|A + \mathcal{L}A| \geq 4|A| - o(|A|)$ for any finite subset A of $\mathbb{R}^2$. In particular, this confirms Conjecture 3.0.1 when $k = d = 2$, $\mathcal{L}_1$ is the identity and $|\det(\mathcal{L}_2)| = 1$.[1] Surprisingly, despite this success, it turns out that Bukh's conjecture is not quite correct and both conditions, that $\mathcal{L}_1, \dots, \mathcal{L}_k$ have no common non-trivial invariant subspace and that $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d = \mathbb{Z}^d$, need modification.

The first condition, that $\mathcal{L}_1, \dots, \mathcal{L}_k$ have no common non-trivial invariant subspace is clearly necessary, since otherwise, for subsets A of such a common invariant subspace, the problem reduces to one of lower dimension. However, this is not the only case where the problem can reduce to one of lower dimension. For instance, a simple concrete example where this can happen is when $d = k = 2$ and both $\mathcal{L}_1$ and $\mathcal{L}_2$ are anti-clockwise rotations about the origin by $\pi/2$. Indeed, even though $|\det(\mathcal{L}_1)| = |\det(\mathcal{L}_2)| = 1$, so that the conjecture predicts that $|\mathcal{L}_1A + \mathcal{L}_2A| \geq 4|A| - o(|A|)$, we only have $|\mathcal{L}_1A + \mathcal{L}_2A| = 2|A| - 1$ when $A = \{(0, x) : x \in [n]\}$. In order to rule out such examples, we update Bukh's condition as follows.

Definition 3.0.2. We say that $\mathcal{L}_1, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are *irreducible* if there are no non-trivial subspaces U, V of $\mathbb{Q}^d$ of the same dimension such that $\mathcal{L}_iU \subseteq V$ for all i.

To reiterate the point, this condition is clearly necessary, since otherwise we may restrict A and the $\mathcal{L}_i$ to U, again reducing the problem to one of lower dimension.

Consider now the transformations

$$\mathcal{L}_1 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathcal{L}_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 2 & 0 \end{pmatrix}.$$

It is easily checked that $\mathcal{L}_1$ and $\mathcal{L}_2$ are irreducible and that $\mathcal{L}_1\mathbb{Z}^2 + \mathcal{L}_2\mathbb{Z}^2 = \mathbb{Z}^2$. However, the set $A = \{(x, 2y) : x, y \in [n]\}$ has $|A| = n^2$ and $|\mathcal{L}_1A + \mathcal{L}_2A| = (2n-1)^2 \sim 4|A|$, giving another counterexample to Conjecture 3.0.1, which predicts that $|\mathcal{L}_1A + \mathcal{L}_2A| \geq 8|A| - o(|A|)$.

The issue here is that $\mathcal{L}_1$ and $\mathcal{L}_2$ have a "common right factor" with determinant of absolute value > 1. On the other hand, Bukh's condition that $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d = \mathbb{Z}^d$

[1] There is a caveat here, which is that Mudgal's result, which applies to arbitrary subsets of $\mathbb{R}^2$, requires that $\mathcal{L}$ have no non-trivial invariant subspace over $\mathbb{R}$. Our interpretation of Bukh's conjecture, which concerns subsets of $\mathbb{Z}^d$ (or $\mathbb{Q}^d$), is that there is instead no non-trivial invariant subspace over $\mathbb{Q}$.

is equivalent to $\mathcal{L}_1, \dots, \mathcal{L}_k$ not having a "common left factor" with determinant of absolute value > 1. Indeed, if $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d = L \subsetneq \mathbb{Z}^d$, then there is some $\mathcal{P} \in \mathrm{Mat}_d(\mathbb{Z})$ with determinant of absolute value > 1 such that $\mathcal{P}\mathbb{Z}^d \supseteq L$, which implies that $\mathcal{P}^{-1}\mathcal{L}_i\mathbb{Z}^d \subseteq \mathbb{Z}^d$ and so $\mathcal{P}^{-1}\mathcal{L}_i \in \mathrm{Mat}_d(\mathbb{Z})$ for all i. Conversely, if there is some $\mathcal{P} \in \mathrm{Mat}_d(\mathbb{Z})$ with determinant of absolute value > 1 such that $\mathcal{P}^{-1}\mathcal{L}_i \in \mathrm{Mat}_d(\mathbb{Z})$ for all i, then $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d \subseteq \mathcal{P}\mathbb{Z}^d \subsetneq \mathbb{Z}^d$. Our second condition incorporates and generalizes both of these possibilities.

Definition 3.0.3. We say that $\mathcal{L}_1, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are *coprime* if there are no $\mathcal{P}, \mathcal{Q} \in \mathrm{GL}_d(\mathbb{Q})$ with $0 < |\det(\mathcal{P})\det(\mathcal{Q})| < 1$ such that

$$\mathcal{P}\mathcal{L}_1\mathcal{Q}, \mathcal{P}\mathcal{L}_2\mathcal{Q}, \dots, \mathcal{P}\mathcal{L}_k\mathcal{Q} \in \mathrm{Mat}_d(\mathbb{Z}).$$

In particular, $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d = \mathbb{Z}^d$.

To see that this condition is also necessary, observe that, for any $A \subset \mathbb{Q}^d$, if we let $A' = \mathcal{Q}^{-1}A$, then $|A'| = |A|$ and $|\mathcal{L}_1A + \cdots + \mathcal{L}_kA| = |\mathcal{P}\mathcal{L}_1\mathcal{Q}A' + \cdots + \mathcal{P}\mathcal{L}_k\mathcal{Q}A'|$. But the transformations $\mathcal{P}\mathcal{L}_i\mathcal{Q}$ have smaller determinants, suggesting that the lower bound should instead be phrased in terms of these determinants.

Taking all these observations into account, we arrive at the following modified version of Bukh's conjecture.

Conjecture 3.0.4. *Suppose that $\mathcal{L}_1, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Then, for any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_1A + \cdots + \mathcal{L}_kA| \geq \left(|\det(\mathcal{L}_1)|^{1/d} + \cdots + |\det(\mathcal{L}_k)|^{1/d}\right)^d |A| - o(|A|).$$

Our main result is a proof of this modified conjecture for $k = 2$ and any d in the following strong form. We note that this result is best possible up to the lower-order term in certain cases, for instance, when $d = 2$, $\mathcal{L}_1$ is the identity and $\mathcal{L}_2 \in \mathrm{Mat}_2(\mathbb{Z})$ is a dilate of a rotation about the origin through an angle which is not an integer multiple of π.

Theorem 3.0.5. *Suppose that $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Then there are constants D, $\sigma > 0$ such that, for any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_1A + \mathcal{L}_2A| \geq \left(|\det(\mathcal{L}_1)|^{1/d} + |\det(\mathcal{L}_2)|^{1/d}\right)^d |A| - D|A|^{1-\sigma}.$$

The proof of this result has two main steps. First, in Section 3.1, we use compression methods to prove a certain discrete version of the Brunn–Minkowski inequality. The core of the proof is then a bootstrapping argument that starts with a trivial bound and repeatedly improves it using our Brunn–Minkowski inequality, ultimately approaching the estimate stated in Theorem 3.0.5. Because the details of this second step are rather easier to digest when $\mathcal{L}_1$ is the identity map, we will, in Section 3.2, first prove Theorem 3.0.5 in this special case. We then prove the full result in Section 3.3.

Remark. *We note that the results in this chapter are nearly superseded by those in Chapters 6 and 7. In particular, in Chapter 7, we prove a near-strengthening of Theorem 3.0.5, establishing that* $|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq H(\mathcal{L}_1, \mathcal{L}_2)|A| - o(|A|)$ *for an explicit constant* $H(\mathcal{L}_1, \mathcal{L}_2)$ *that is best possible. This result is not strictly stronger, as the error term* $o(|A|)$ *is weaker than the* $D|A|^{1-\sigma}$ *error appearing in Theorem 3.0.5. Nevertheless, the approaches are different, and the ideas presented in this chapter remain of independent interest.*

3.1 A discrete Brunn–Minkowski inequality

In this section, we begin our proof of Theorem 3.0.5 by using compression arguments to establish the following discrete analogue of the Brunn–Minkowski theorem. We refer the reader to [6, 20, 21] for a selection of results in a similar vein.

Lemma 3.1.1. *Fix a basis* $\{b_1, \dots, b_d\}$ *of* $\mathbb{R}^d$*. For each* $I \subseteq [d]$*, let* $p_I : \mathbb{R}^d \to \mathbb{R}^I$ *be the projection onto the span of* $\{b_i\}_{i \in I}$ *along the given basis. Then, for any finite subsets* A, B *of* $\mathbb{R}^d$*,*

$$|A + B| \geq (|A|^{1/d} + |B|^{1/d})^d - \sum_{I \subsetneq [d]} |p_I(A + B)|.$$

Proof. By applying a suitable linear transformation, we may assume that the basis is the standard one. Let $p_i = p_{[d]\setminus\{i\}} : \mathbb{R}^d \to \mathbb{R}^{d-1}$ be the linear map that removes the ith coordinate.

We define i-compressions for $i = 1, \dots, d$ as follows. For a set $A \subset \mathbb{R}^d$ and a point $x \in p_i(A)$, let $A_x = p_i^{-1}(x)$. Define the i-compression of A to be the set A' such that $p_i(A') = p_i(A)$ and, for each $x \in p_i(A)$, the ith coordinates of A'_x are $0, 1, \dots, |A_x| - 1$. Note that $|A'| = |A|$, so an i-compression does not alter the size of the set.

Suppose that A' and B' are the i-compressions of A and B. We will now show that $|A' + B'| \leq |A + B|$ and, more generally, that $|p_S(A' + B')| \leq |p_S(A + B)|$ for any $S \subseteq [d]$. If $i \notin S$, then $p_S(A' + B') = p_S(A + B)$. We may therefore assume that $i \in S$. Let $T = S \setminus \{i\}$. For a set C and $x \in p_T(C)$, denote by $(p_S(C))_x$ the set $\{y \in p_S(C) : p_T(y) = x\}$. Then, for any $z \in p_T(A' + B') = p_T(A') + p_T(B')$, there is some $x \in p_T(A') = p_T(A)$ and $y \in p_T(B') = p_T(B)$ such that $x + y = z$ and $|(p_S(A' + B'))_z| = |(p_S(A'))_x| + |(p_S(B'))_y| - 1$. Hence,

$$\begin{aligned}|(p_S(A + B))_z| &\geq |(p_S(A))_x| + |(p_S(B))_y| - 1 = |(p_S(A'))_x| + |(p_S(B'))_y| - 1 \\ &= |(p_S(A' + B'))_z|.\end{aligned}$$

Taking the sum over all z, we have $|p_S(A' + B')| \leq |p_S(A + B)|$, as claimed. We therefore see that if the required inequality holds for the i-compressions of A and B, then it also holds for the original sets.

By repeatedly taking i-compressions for $i = 1, \dots, d$, we may assume that $A, B \subset \mathbb{Z}^d_{\geq 0}$. We will say that A is i-compressed if the i-compression of A is A itself and A is compressed if it is i-compressed for all i. Now, by considering the sum of the coordinates of all the points of A or B, we see that taking the i-compression strictly decreases these sums unless they are already i-compressed. Therefore, by repeatedly taking i-compressions for each i, we may assume that A and B are compressed. This means that for any points $(x_1, \dots, x_d) \in A$ and $(y_1, \dots, y_d)$ such that $0 \leq y_i \leq x_i$ for all i, $(y_1, \dots, y_d) \in A$ and similarly for B.

For a point $x = (x_1, \dots, x_d) \in \mathbb{Z}^d$, let C_x be the closed cube $\prod_{i=1}^d [x_i - 1, x_i]$. Define $A^* = \bigcup_{x \in A} C_x$, a compact set with $\mu(A^*) = |A|$, and define B^* similarly. Then, by the Brunn–Minkowski inequality, we have

$$\mu(A^* + B^*) \geq (|A|^{1/d} + |B|^{1/d})^d.$$

We can write $A^* + B^*$ as the union of closed cubes

$$A^* + B^* = \bigcup_{x \in A + B + \{0,-1\}^d} C_x.$$

Since A and B are compressed, so is $A + B$. Using this fact, we can rewrite $A^* + B^*$ as a union of closed sets with disjoint interiors in the following way. For $S \subseteq [d]$, let P_S be the set of points in $\mathbb{Z}^d$ such that $p_S(P_S) = p_S(A + B)$ and the coordinates outside of S are all -1. Notice that the P_S are pairwise disjoint for each $S \subseteq [d]$

and $P_S \subseteq A + B + \{0,-1\}^d$. Furthermore, for each $x \in A + B + \{0,-1\}^d$, let S be the set of coordinates of x which are not -1. Then $x \in P_S$, so that

$$A^* + B^* = \bigcup_{S \subseteq [d]} \bigcup_{x \in P_S} C_x.$$

In particular, $\mu(A^* + B^*) = \sum_{S \subseteq [d]} |P_S| = \sum_{S \subseteq [d]} |p_S(A + B)|$. Hence, since $p_{[d]}(A + B) = A + B$, we have

$$\mu(A^* + B^*) = |A + B| + \sum_{I \subsetneq [d]} |p_I(A + B)|$$

and the lemma follows. □

Our aim now is to apply this discrete Brunn–Minkowski inequality to prove an estimate that will play an important role in the bootstrap arguments of the next two sections. For this, we will need several additional ingredients, beginning with the following classical theorem of Freiman [17] (see also [5]) on subsets of small doubling in torsion-free abelian groups. Given such a group G, a proper progression P of dimension s and size L is a set of the form

$$P = \{v_0 + u_1 v_1 + \cdots + u_s v_s : 0 \leq u_i < L_i \text{ for } 1 \leq i \leq s\},$$

where $L_1 L_2 \cdots L_s = L$, $v_0, v_1, \ldots, v_s$ are elements of G and all of the sums arising in the definition of P are distinct.

Theorem 3.1.2. *For any $K > 0$, there exist constants C_1 and C_2 such that if A is a subset of a torsion-free abelian group G with $|A + A| \leq K|A|$, then A is contained in a proper progression of dimension $s \leq C_1$ and size $L \leq C_2|A|$.*

We also need the following result of Plünnecke–Ruzsa type [28, Lemma 3.1].

Lemma 3.1.3. *Let G be an abelian group. If sets $A, B \subseteq G$ with $|A| = |B|$ are such that $C := A + B$ satisfies $|C| \leq K|A|$ for some $K > 0$, then $|C + C| \leq K^6|C|$.*

Finally, we need the following technical lemma, saying that if $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Q})$ has no non-trivial invariant subspace over $\mathbb{Q}$ and A is a finite subset of $\mathbb{Z}^d$ with $|A + \mathcal{L}A| \leq K|A|$, then A cannot be concentrated on an affine subspace.

Lemma 3.1.4. *Let $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Q})$ with no non-trivial invariant subspace over $\mathbb{Q}$ and let $A \subset \mathbb{Z}^d$ be such that $|A| = n$ and $|A + \mathcal{L}A| \leq Kn$ for some $K > 0$. If U is a vector subspace of $\mathbb{Q}^d$ of dimension $k < d$, then every translate of U contains at most $(Kn)^{1-2^{-k}}$ points of A.*

Proof. The fact that $\mathcal{L}$ has no non-trivial invariant subspace implies that $\mathcal{L}$ is invertible (over $\mathbb{Q}$). We prove the lemma by induction on k. For $k = 1$, let U_1 be a 1-dimensional subspace. Then, since $\mathcal{L}$ is invertible, $\mathcal{L}U_1$ is a line. Furthermore, the line $\mathcal{L}U_1$ is not parallel to U_1, since U_1 is not an invariant subspace of $\mathcal{L}$. Thus, for any translate U_1+u of U_1, $|(U_1+u)\cap A|^2 = |((U_1+u)\cap A)+\mathcal{L}((U_1+u)\cap A)| \leq Kn$, so $|(U_1+u)\cap A| \leq (Kn)^{1/2}$. This proves the base case of our induction.

For $1 < k < d$, let U_k be a subspace of dimension k. Then $\mathcal{L}U_k \neq U_k$ since $\mathcal{L}$ has no non-trivial invariant subspace, so $V = \mathcal{L}U_k \cap U_k$ is a subspace of dimension strictly smaller than k. Let $U_k + u$ be a translate of U_k with $|(U_k+u)\cap A| = m$. Suppose r translates of V are required to cover $(U_k+u)\cap A$. Note that for any collection of translates V' of V, the affine subspaces $V' + \mathcal{L}(U_k+u)$ are translates of $\mathcal{L}U_k$ and are disjoint. Thus, $Kn \geq |((U_k+u)\cap A)+\mathcal{L}((U_k+u)\cap A)| \geq mr$. On the other hand, each translate of V intersects A in at most $(Kn)^{1-2^{1-k}}$ points by the induction hypothesis. Thus, $m \leq r(Kn)^{1-2^{1-k}}$. Using $mr \leq Kn$, it follows that $m^2 \leq (Kn)^{2-2^{1-k}}$, so $m \leq (Kn)^{1-2^{-k}}$, as desired. □

We now come to our application of Lemma 3.1.1.

Lemma 3.1.5. *Let $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Q})$ with no non-trivial invariant subspace over $\mathbb{Q}$ and let $A \subset \mathbb{Z}^d$ be such that $|A+\mathcal{L}A| \leq K|A|$ for some $K > 0$. Then there are constants $D, \sigma > 0$ depending only on d and K such that, for any $B_1 \subseteq A$, $B_2 \subseteq \mathcal{L}A$,*

$$|B_1 + B_2| \geq \left(|B_1|^{1/d} + |B_2|^{1/d}\right)^d - D|A|^{1-\sigma}.$$

Proof. Let $n = |A|$. By Lemma 3.1.3, $|A+\mathcal{L}A+A+\mathcal{L}A| \leq K^6|A+\mathcal{L}A| \leq K_1 n$, where $K_1 = K^7$. We also claim that

$$|A+\mathcal{L}A+\mathcal{L}(A+\mathcal{L}A)| \leq K_2 n,$$

where $K_2 = K_1^2$. To see this, first note that $|A+\mathcal{L}A+\mathcal{L}A| \leq |A+\mathcal{L}A+A+\mathcal{L}A| \leq K_1 n$ and $|\mathcal{L}A+\mathcal{L}A+\mathcal{L}^2A| = |A+A+\mathcal{L}A| \leq |A+\mathcal{L}A+A+\mathcal{L}A| \leq K_1 n$. By applying the sum version of Ruzsa's triangle inequality (Lemma 1.6.1) with $X = \mathcal{L}A, Y = A+\mathcal{L}A, Z = \mathcal{L}A+\mathcal{L}^2A$, we have

$$n|A+\mathcal{L}A+\mathcal{L}A+\mathcal{L}^2A| \leq |A+\mathcal{L}A+\mathcal{L}A||\mathcal{L}A+\mathcal{L}A+\mathcal{L}^2A| \leq K_1^2 n^2.$$

Thus, $|A+\mathcal{L}A+\mathcal{L}(A+\mathcal{L}A)| \leq K_1^2 n$, as claimed.

Since $|A + \mathcal{L}A + A + \mathcal{L}A| \leq K_1 n$, we can apply Theorem 3.1.2 to conclude that $A + \mathcal{L}A$ is contained in a proper progression

$$P = \{v_0 + u_1 v_1 + \cdots + u_s v_s : 0 \leq u_i < L_i \text{ for } 1 \leq i \leq s\},$$

where $s \leq K_3$, $L_1 \geq L_2 \geq \cdots \geq L_s$ and $L_1 L_2 \cdots L_s \leq K_4 n$ for some K_3, K_4 depending only on K. Note that P cannot be contained in a hyperplane, since otherwise it would contradict Lemma 3.1.4.

Let $i_1 = 1$ and, for $j = 2, \ldots, d$, set i_j to be the smallest number such that v_{i_j} does not lie in the span of $v_{i_1}, \ldots, v_{i_{j-1}}$. Then $v_{i_1}, \ldots, v_{i_d}$ forms a basis of $\mathbb{R}^d$. By applying Lemma 3.1.1 with this basis, we get that

$$\begin{aligned}|B_1 + B_2| &\geq \left(|B_1|^{1/d} + |B_2|^{1/d}\right)^d - \sum_{I \subsetneq [d]} |p_I(B_1 + B_2)| \\ &\geq \left(|B_1|^{1/d} + |B_2|^{1/d}\right)^d - 2^d(|p_1(B_1 + B_2)| + \cdots + |p_d(B_1 + B_2)|),\end{aligned}$$

where $p_j = p_{[d]\setminus\{j\}}$, the projection along the basis element v_{i_j}. Hence, it suffices to show that there is some $\sigma > 0$ such that $|p_j(A + \mathcal{L}A)| = O(n^{1-\sigma})$ for all j.

Note that $|p_j(A + \mathcal{L}A)| \leq L_1 \cdots L_s / L_{i_j} \leq K_4 n / L_{i_j}$. Let H be the span of $v_1, v_2, \ldots, v_{i_j - 1}$, which is a proper subspace. Using the claim that $|A + \mathcal{L}A + \mathcal{L}(A + \mathcal{L}A)| \leq K_2 n$, we can apply Lemma 3.1.4 with A replaced by $A + \mathcal{L}A$ to conclude that each translate of H contains at most $(K_2 n)^{1-2^{1-d}}$ points of $A + \mathcal{L}A$. But P is covered by $L_{i_j} L_{i_j+1} \cdots L_s$ translates of H. Hence,

$$L_{i_j} L_{i_j+1} \cdots L_s \geq n/(K_2 n)^{1-2^{1-d}} = K_5 n^{2^{1-d}},$$

where $K_5 = K_2^{2^{1-d}-1}$. Since $L_{i_j} \geq L_{i_j+1} \geq \cdots \geq L_s$, we have

$$L_{i_j} \geq K_5^{1/s} n^{2^{1-d}/s} \geq K_6 n^{2^{1-d}/K_3},$$

where $K_6 = K_5^{1/K_3}$. Thus,

$$|p_j(A + \mathcal{L}A)| \leq K_4 n / L_{i_j} \leq \frac{K_4}{K_6} n^{1-2^{1-d}/K_3}.$$

The result therefore follows by taking $\sigma = 2^{1-d}/K_3$ and $D = 2^d d K_4 / K_6$. □

3.2 Bounding $A + \mathcal{L}A$

As promised, we will first prove our main result in the special case where one of the transformations is the identity. Like the general case, we will do this by

proving a bootstrapping lemma which allows us to successively obtain better and better bounds, approaching the optimal one. We start with a weaker version of this bootstrapping lemma.

Both here and in what follows, we will make extensive use of the fact that if $\mathcal{L}$ is not singular, then $\mathcal{L}\mathbb{Z}^d$ has index $k = |\det \mathcal{L}|$ in $\mathbb{Z}^d$. Indeed, this can be seen by considering the Smith normal form $\mathcal{L} = SDT$, where $S, T \in \mathrm{Mat}_d(\mathbb{Z})$ are invertible over $\mathbb{Z}$ and $D \in \mathrm{Mat}_d(\mathbb{Z})$ is diagonal. Then the index satisfies

$$[\mathbb{Z}^d : \mathcal{L}\mathbb{Z}^d] = [S^{-1}\mathbb{Z}^d : DT\mathbb{Z}^d] = [\mathbb{Z}^d : D\mathbb{Z}^d] = |\det D| = |\det \mathcal{L}|.$$

Lemma 3.2.1. *Let $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Z})$ have no non-trivial invariant subspace over $\mathbb{Q}$ and $k = |\det \mathcal{L}|$. Then there are constants $\sigma_1 > 0$ and $D > 0$ depending only on d and k such that the following holds. Suppose that there are $0 < \alpha < (1 + k^{1/d})^d$ and $D_1 > 0$ such that*

$$|A + \mathcal{L}A| \geq ((1 + k^{1/d})^d - \alpha)|A| - D_1|A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$. Let $I_1, \ldots, I_k$ be the cosets of $\mathcal{L}\mathbb{Z}^d$ in $\mathbb{Z}^d$ and let $A_i = A \cap I_i$ for $i = 1, \ldots, k$. If there is some j for which $0 < |A_j| \leq |A|/k$, then

$$|A + \mathcal{L}A| \geq \left((1 + k^{1/d})^d - \max\left(\alpha - 1, \frac{k-1}{k}\alpha\right)\right)|A| - (D + (k-1)D_1)|A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$.

Proof. Assume that $|A + \mathcal{L}A| \leq (1 + k^{1/d})^d|A|$. Let D and $\sigma_1 = \sigma$ be the constants obtained from applying Lemma 3.1.5 with $K = (1 + k^{1/d})^d$. Then, for each i, we have

$$|A_i + \mathcal{L}A| \geq \left(|A_i|^{1/d} + |A|^{1/d}\right)^d - D|A|^{1-\sigma_1}.$$

Since $\mathcal{L}A \subset \mathcal{L}\mathbb{Z}^d$, we have $(A + \mathcal{L}A) \cap I_i = A_i + \mathcal{L}A$. Hence, we can write $A + \mathcal{L}A$ as the disjoint union

$$A + \mathcal{L}A = (A_1 + \mathcal{L}A) \cup \cdots \cup (A_k + \mathcal{L}A).$$

Suppose, without loss of generality, that $0 < |A_1| \leq |A|/k$. We shall bound $|A_1 + \mathcal{L}A|$ by the estimate above and the rest by

$$\begin{aligned} |A_i + \mathcal{L}A| &\geq |A_i + \mathcal{L}A_i| \geq ((1 + k^{1/d})^d - \alpha)|A_i| - D_1|A_i|^{1-\sigma_1} \\ &\geq ((1 + k^{1/d})^d - \alpha)|A_i| - D_1|A|^{1-\sigma_1} \end{aligned}$$

for $i = 2, \dots, k$. Combining these estimates, we have

$$\begin{aligned}
|A + \mathcal{L}A| &\geq |A_1 + \mathcal{L}A| + |A_2 + \mathcal{L}A| + \cdots + |A_k + \mathcal{L}A| \\
&\geq \left(|A_1|^{1/d} + |A|^{1/d}\right)^d + ((1 + k^{1/d})^d - \alpha) \sum_{i=2}^{k} |A_i| \\
&\quad - (D + (k-1)D_1)|A|^{1-\sigma_1} \\
&= \left(|A_1|^{1/d} + |A|^{1/d}\right)^d + ((1 + k^{1/d})^d - \alpha)(|A| - |A_1|) \\
&\quad - (D + (k-1)D_1)|A|^{1-\sigma_1}.
\end{aligned}$$

This last expression is concave in terms of $|A_1|$, which can be seen by expanding the binomial term and noting that each term in the binomial sum is concave. Hence, it is minimized when $|A_1| = 0$ or $|A_1| = |A|/k$.

In the first case, where the minimum is when $|A_1| = 0$, we have

$$|A + \mathcal{L}A| \geq ((1 + k^{1/d})^d - (\alpha - 1))|A| - (D + (k-1)D_1)|A|^{1-\sigma_1}.$$

In the second case, where the minimum is when $|A_1| = |A|/k$, we have

$$|A + \mathcal{L}A| \geq \left((1 + k^{1/d})^d - \frac{k-1}{k}\alpha\right)|A| - (D + (k-1)D_1)|A|^{1-\sigma_1}.$$

In either case, we have

$$|A + \mathcal{L}A| \geq \left((1 + k^{1/d})^d - \max\left(\alpha - 1, \frac{k-1}{k}\alpha\right)\right)|A| - (D + (k-1)D_1)|A|^{1-\sigma_1},$$

as required. □

This lemma shows that bootstrapping works if each of the k cosets A_i of A are non-empty. To show that a similar result holds in general, we split each of the cosets A_i into smaller cosets A_{ij}. There are then three cases: if A is contained in some smaller sublattice, then we can rescale A, which will contradict a certain minimality assumption; if $A + \mathcal{L}A$ contains cosets that are distinct from all the $A_{ij} + \mathcal{L}A_{ij}$, then this additional coset boosts the bound; and, finally, if any of the A_i splits into k non-empty cosets, we can again apply the lemma above. The following lemma will allow us to show that one of these three cases must hold.

Lemma 3.2.2. *Let $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Z})$ be a linear transformation that is invertible over $\mathbb{Q}$. Let X be a subset of the finite abelian group $G = \mathbb{Z}^d/\mathcal{L}^2\mathbb{Z}^d$ containing 0 and let H be the subgroup $\mathcal{L}\mathbb{Z}^d/\mathcal{L}^2\mathbb{Z}^d$ of G. Notice that $\mathcal{L}$ naturally induces a map $G \to G$. Then at least one of the following holds:*

1. *$X + H$ does not generate G;*

2. *$X + \mathcal{L}X \supsetneq X$ (note that $X + \mathcal{L}X \supseteq X$ always holds);*

3. *$H \subseteq X$.*

Proof. Suppose all 3 do not hold. Let $L = \{v \in G : \mathcal{L}v \in X\}$. Since $0 \in X$, we have $H \subseteq L$. For any $v \in L$ and $a \in X$, we have $\mathcal{L}v + \mathcal{L}a \in X + \mathcal{L}X = X$, so $v + a \in L$. Since $H + X$ generates G, for any $b \in G$, there are $h \in H$ and $a_1, \dots, a_k \in X$ for some k such that $b = h + a_1 + \cdots + a_k$. If $h + a_1 + \cdots + a_i \in L$ for some i, then $(h + a_1 + \cdots + a_i) + a_{i+1} \in L$, so, by the fact that $h \in L$ and a simple induction, we have that $b = h + a_1 + \cdots + a_k \in L$. Thus, $L = G$, which implies that $H \subseteq X$, a contradiction. □

We are now ready for our main bootstrapping lemma.

Lemma 3.2.3. *Let d and k be positive integers. Then there are constants $\sigma_1 > 0$ and $D > 0$ depending only on d and k such that the following holds. Suppose that there are $0 < \alpha < (1 + k^{1/d})^d$ and $D_1 > 0$ such that*

$$|A + \mathcal{L}A| \geq ((1 + k^{1/d})^d - \alpha)|A| - D_1|A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$ and all $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Z})$ with no non-trivial invariant subspace over $\mathbb{Q}$ and $k = |\det \mathcal{L}|$. Then

$$|A + \mathcal{L}A| \geq \left((1 + k^{1/d})^d - \max\left(\alpha - \frac{1}{k^2}, \frac{k^2 - 1}{k^2}\alpha\right)\right)|A| - (D + k^2 D_1)|A|^{1-\sigma_1}$$

holds for all such A and $\mathcal{L}$.

Proof. Take σ_1, D as in Lemma 3.2.1. By translating A, we may assume that $0 \in A$. We may also assume that $|A + \mathcal{L}A| \leq (1 + k^{1/d})^d |A|$, so that, by Lemma 3.1.4, A does not lie on a hyperplane. Let $\langle A \rangle$ denote the $\mathbb{Z}$-span of A, which is a d-dimensional sublattice of $\mathbb{Z}^d$. Suppose the lemma does not hold and pick a counterexample $(A, \mathcal{L})$ such that $\langle A \rangle$ has minimum index in $\mathbb{Z}^d$.

Let $v_1 = 0, v_2, \dots, v_k$ be coset representatives of $\mathcal{L}\mathbb{Z}^d$ over $\mathbb{Z}^d$. For $i, j = 1, \dots, k$, let $A_i = A \cap (v_i + \mathcal{L}\mathbb{Z}^d)$ and $A_{ij} = A \cap (v_i + \mathcal{L}v_j + \mathcal{L}^2\mathbb{Z}^d)$. Then the A_{ij} partition A_i and the A_i partition A. If there is some i for which $0 < |A_i| \leq |A|/k$, then we are done by Lemma 3.2.1. Hence, we may assume that either $A_i = \emptyset$ or $|A_i| > |A|/k$ for every i.

If there is some i, j such that $A_i \neq \emptyset$ and $0 < |A_{ij}| \leq |A_i|/k$, then let $A' = \mathcal{L}^{-1}(A_i - v_i) = \mathcal{L}^{-1}(A - v_i) \cap \mathbb{Z}^d \subseteq \mathbb{Z}^d$. For each $l = 1, \ldots, k$, let $A'_l = \mathcal{L}^{-1}(A_{il} - v_i) = \mathcal{L}^{-1}(A - v_i) \cap (v_l + \mathcal{L}\mathbb{Z}^d)$. Thus, $A'_l = A' \cap (v_l + \mathcal{L}\mathbb{Z}^d)$. Hence, applying Lemma 3.2.1 with A and A_j replaced by A' and A'_j, we have

$$\begin{aligned}|A_i + \mathcal{L}A_i| &= |A' + \mathcal{L}A'| \\ &\geq \left((1 + k^{1/d})^d - \max\left(\alpha - 1, \frac{k-1}{k}\alpha\right)\right)|A_i| - (D + (k-1)D_1)|A_i|^{1-\sigma_1}.\end{aligned}$$

Using the fact that $|A + \mathcal{L}A| \geq \sum_{l=1}^{k} |A_l + \mathcal{L}A_l|$ and $|A_i| \geq |A|/k$, we have

$$\begin{aligned}|A + \mathcal{L}A| &\geq \sum_{l \neq i} |A_l + \mathcal{L}A_l| + |A_i + \mathcal{L}A_i| \\ &\geq \left((1 + k^{1/d})^d - \alpha\right) \sum_{l \neq i} |A_l| - (k-1)D_1|A|^{1-\sigma_1} \\ &\quad + \left((1 + k^{1/d})^d - \max\left(\alpha - 1, \frac{k-1}{k}\alpha\right)\right)|A_i| - (D + (k-1)D_1)|A|^{1-\sigma_1} \\ &= \left((1 + k^{1/d})^d - \alpha\right)|A| + \min\left(1, \frac{\alpha}{k}\right)|A_i| - (D + 2(k-1)D_1)|A|^{1-\sigma_1} \\ &\geq \left((1 + k^{1/d})^d - \alpha\right)|A| + \min\left(\frac{1}{k}, \frac{\alpha}{k^2}\right)|A| - (D + 2(k-1)D_1)|A|^{1-\sigma_1} \\ &\geq \left((1 + k^{1/d})^d - \max\left(\alpha - \frac{1}{k}, \frac{k^2-1}{k^2}\alpha\right)\right)|A| - (D + k^2 D_1)|A|^{1-\sigma_1}.\end{aligned}$$

Hence, we may assume that, for all i, j, either $A_{ij} = \emptyset$ or $|A_{ij}| > |A_i|/k > |A|/k^2$. This assumption will be crucial in many of the estimates that follow.

Let X be the image of A in $G = \mathbb{Z}^d/\mathcal{L}^2\mathbb{Z}^d$ and let $H = \mathcal{L}\mathbb{Z}^d/\mathcal{L}^2\mathbb{Z}^d \subseteq G$. Applying Lemma 3.2.2 to X, we have the following 3 cases:

Case 1: $X + H$ does not generate G

Let $E \subset \mathbb{Z}^d$ be the lattice that is the preimage of the subgroup of G generated by $X + H$ with respect to the quotient map $q : \mathbb{Z}^d \to \mathbb{Z}^d/\mathcal{L}^2\mathbb{Z}^d = G$. In other words, $E = \langle A \rangle + \mathcal{L}\mathbb{Z}^d$. Since A does not lie on a hyperplane, E is d-dimensional and, since $X + H$ does not generate G, $E \neq \mathbb{Z}^d$. Consider a linear transformation $\mathcal{P} \in \mathrm{Mat}_d(\mathbb{Z})$ such that $\mathcal{P}\mathbb{Z}^d = E$, so that $|\det \mathcal{P}| > 1$. Then

$$|A + \mathcal{L}A| = |\mathcal{P}\mathcal{P}^{-1}A + \mathcal{P}\mathcal{P}^{-1}\mathcal{L}\mathcal{P}\mathcal{P}^{-1}A| = |\mathcal{P}^{-1}A + (\mathcal{P}^{-1}\mathcal{L}\mathcal{P})(\mathcal{P}^{-1}A)|.$$

Since $\mathcal{L}E \subset \mathcal{L}\mathbb{Z}^d = q^{-1}(H) \subseteq E$, we have

$$\mathcal{P}^{-1}\mathcal{L}\mathcal{P}\mathbb{Z}^d = \mathcal{P}^{-1}\mathcal{L}E \subset \mathcal{P}^{-1}E = \mathbb{Z}^d,$$

so that $\mathcal{P}^{-1}\mathcal{L}\mathcal{P} \in \mathrm{Mat}_d(\mathbb{Z})$ and $|\det \mathcal{P}^{-1}\mathcal{L}\mathcal{P}| = |\det \mathcal{P}|^{-1}|\det \mathcal{L}||\det \mathcal{P}| = k$. Now replace A by $\mathcal{P}^{-1}A \subset \mathbb{Z}^d$ and $\mathcal{L}$ by $\mathcal{P}^{-1}\mathcal{L}\mathcal{P}$. But then the index of $\left\langle \mathcal{P}^{-1}A \right\rangle$ is

$$[\mathbb{Z}^d : \left\langle \mathcal{P}^{-1}A \right\rangle] = [\mathcal{P}\mathbb{Z}^d : \langle A \rangle] = [\mathbb{Z}^d : \langle A \rangle]/[\mathbb{Z}^d : \mathcal{P}\mathbb{Z}^d] = |\det \mathcal{P}|^{-1}[\mathbb{Z}^d : \langle A \rangle].$$

Thus, $\left\langle \mathcal{P}^{-1}A \right\rangle$ has strictly smaller index than $\langle A \rangle$, so the pair $(\mathcal{P}^{-1}A, \mathcal{P}^{-1}\mathcal{L}\mathcal{P})$ contradicts the minimality of the pair $(A, \mathcal{L})$.

Case 2: $X + \mathcal{L}X \supsetneq X$

This case is saying that $A + \mathcal{L}A$ intersects strictly more cosets of $\mathcal{L}^2\mathbb{Z}^d$ than A, so we can exploit the extra cosets to obtain a better lower bound. Let $I = \left\{(i,j) \in [k]^2 : A_{ij} \neq \emptyset\right\}$. Suppose $(i,j), (i',j') \in I$ are distinct pairs. We claim that $A_{ij} + \mathcal{L}A_{ij}$ and $A_{i'j'} + \mathcal{L}A_{i'j'}$ belong to different cosets of $\mathcal{L}^2\mathbb{Z}^d$. Indeed, suppose they belong to the same coset. $A_{ij} + \mathcal{L}A_{ij}$ belongs to the coset $v_i + \mathcal{L}v_j + \mathcal{L}v_i + \mathcal{L}^2\mathbb{Z}^d$, while $A_{i'j'} + \mathcal{L}A_{i'j'} \subset v_{i'} + \mathcal{L}v_{j'} + \mathcal{L}v_{i'} + \mathcal{L}^2\mathbb{Z}^d$. So if they belong to the same coset, we must have $i = i'$ and $j = j'$. Now, since $A + \mathcal{L}A$ intersects more than $|I|$ cosets, there are $(i_1, j_1), (i_2, j_2) \in I$ such that $A_{i_1j_1} + \mathcal{L}A_{i_2j_2}$ belongs to a coset different from $A_{ij} + \mathcal{L}A_{ij}$ for all $(i,j) \in I$. Since $A_{i_1j_1}$ is non-empty, $|A_{i_1j_1}| \geq |A|/k^2$, so we have

$$\begin{aligned}
|A + \mathcal{L}A| &\geq \sum_{(i,j)\in I} |A_{ij} + \mathcal{L}A_{ij}| + |A_{i_1j_1} + \mathcal{L}A_{i_2j_2}| \\
&\geq ((1 + k^{1/d})^d - \alpha)|A| - k^2 D_1 |A|^{1-\sigma_1} + |A_{i_1j_1}| \\
&\geq ((1 + k^{1/d})^d - \alpha)|A| - k^2 D_1 |A|^{1-\sigma_1} + \frac{1}{k^2}|A| \\
&= ((1 + k^{1/d})^d - (\alpha - 1/k^2))|A| - k^2 D_1 |A|^{1-\sigma_1}.
\end{aligned}$$

Case 3: $H \subseteq X$

In this case, $A_{1j} \neq \emptyset$ for $j = 1, \ldots, k$. But, since the A_{1j} partition A_1, there is then some j for which $|A_{1j}| \leq |A_1|/k$, contradicting our assumption. This completes the proof of the lemma. □

It is now a simple matter to complete the proof of Theorem 3.0.5 in the special case where $\mathcal{L}_1$ is the identity.

Theorem 3.2.4. *Let $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Z})$ be a linear transformation with no non-trivial invariant subspace over $\mathbb{Q}$ and $k = |\det \mathcal{L}|$. Then there are $D_2, \sigma_2 > 0$ depending only on d and k such that*

$$|A + \mathcal{L}A| \geq (1 + k^{1/d})^d |A| - D_2 |A|^{1-\sigma_2}$$

for all finite $A \subset \mathbb{Z}^d$.

Proof. Let $\sigma_1, D > 0$ be as in Lemma 3.2.3. Using the trivial base case $|A + \mathcal{L}A| \geq |A|$ and repeatedly applying Lemma 3.2.3, we can find some $0 < \epsilon < 1$ and $D_2' > D$ such that

$$|A + \mathcal{L}A| \geq ((1 + k^{1/d})^d - \epsilon)|A| - D_2' |A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$.

Applying Lemma 3.2.3 m more times, we have

$$|A + \mathcal{L}A| \geq \left((1 + k^{1/d})^d - \left(\frac{k^2 - 1}{k^2}\right)^m \epsilon\right)|A| - (k^2 + 1)^m D_2' |A|^{1-\sigma_1}.$$

Taking $m = \frac{\sigma_1 \log |A|}{2 \log(k^2+1)}$ (and ignoring integer rounding issues), we have

$$(k^2 + 1)^m D_2' |A|^{1-\sigma_1} = D_2' |A|^{1-\sigma_1/2}$$

and

$$\left(\frac{k^2 - 1}{k^2}\right)^m \epsilon |A| = \epsilon |A|^{1 + \frac{\sigma_1(\log(k^2-1) - \log k^2)}{2 \log(k^2+1)}}.$$

Now, taking $\sigma_2 = \min\left(\frac{\sigma_1}{2}, \frac{\sigma_1(\log k^2 - \log(k^2-1))}{2 \log(k^2+1)}\right)$, we get

$$|A + \mathcal{L}A| \geq (1 + k^{1/d})^d |A| - D_2 |A|^{1-\sigma_2},$$

where $D_2 = \epsilon + D_2'$. □

3.3 Bounding $\mathcal{L}_1 A + \mathcal{L}_2 A$

In this section, we prove our main result, our lower bound on $|\mathcal{L}_1 A + \mathcal{L}_2 A|$ when $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Note that we may assume that both $\mathcal{L}_1$ and $\mathcal{L}_2$ are invertible over $\mathbb{Q}$. Indeed, if $\mathcal{L}_1$, say, is not invertible, then there is a line L such that $\mathcal{L}_1 L = 0$, so $\mathcal{L}_1, \mathcal{L}_2$ would not be irreducible.

We first note the following elementary fact about abelian groups.

Lemma 3.3.1. *Let G be an abelian group and H_1, H_2 be subgroups of finite index such that $H_1 + H_2 = G$. Then*

$$[G : H_1 \cap H_2] = [G : H_1][G : H_2].$$

Proof. By the isomorphism theorems, we have that

$$H_1/(H_1 \cap H_2) \equiv (H_1 + H_2)/H_2,$$

$$G/H_1 \equiv (G/(H_1 \cap H_2))/(H_1/(H_1 \cap H_2)).$$

Hence, $[H_1 : H_1 \cap H_2] = [G : H_2]$ and $[G : H_1 \cap H_2] = [G : H_1][H_1 : H_1 \cap H_2] = [G : H_1][G : H_2]$. □

For the proof, we will need to introduce a number of additional linear transformations associated with $\mathcal{L}_1$ and $\mathcal{L}_2$. Indeed, let $p = |\det \mathcal{L}_1|$ and $q = |\det \mathcal{L}_2|$. Since $\mathcal{L}_1, \mathcal{L}_2$ are coprime, we know that $\mathcal{L}_1\mathbb{Z}^d + \mathcal{L}_2\mathbb{Z}^d = \mathbb{Z}^d$. Thus, by Lemma 3.3.1 with $G = \mathbb{Z}^d$, $H_1 = \mathcal{L}_1\mathbb{Z}^d$ and $H_2 = \mathcal{L}_2\mathbb{Z}^d$, we have

$$[\mathbb{Z}^d : \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d] = [\mathbb{Z}^d : \mathcal{L}_1\mathbb{Z}^d][\mathbb{Z}^d : \mathcal{L}_2\mathbb{Z}^d] = pq.$$

Hence,

$$[\mathcal{L}_1\mathbb{Z}^d : \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d] = q, \quad [\mathcal{L}_2\mathbb{Z}^d : \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d] = p$$

and so

$$[\mathbb{Z}^d : \mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d] = q, \quad [\mathbb{Z}^d : \mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathbb{Z}^d] = p.$$

We now let $\mathcal{P}_1, \mathcal{P}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ be linear transformations such that $\mathcal{P}_1\mathbb{Z}^d = \mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathbb{Z}^d$ and $\mathcal{P}_2\mathbb{Z}^d = \mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d$, noting that $|\det \mathcal{P}_1| = p$ and $|\det \mathcal{P}_2| = q$.

As in the $A + \mathcal{L}A$ case, we begin the proof proper with a weak bootstrapping lemma.

Lemma 3.3.2. *Let $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ be irreducible, coprime linear transformations with $|\det \mathcal{L}_1| = p$ and $|\det \mathcal{L}_2| = q$. Then there are constants $\sigma_1 > 0$ and $D > 0$ depending only on d, p and q such that the following holds. Suppose that there are $0 < \alpha < (p^{1/d} + q^{1/d})^d$ and $D_1 > 0$ such that*

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq ((p^{1/d} + q^{1/d})^d - \alpha)|A| - D_1|A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$. Let $I_1, \dots, I_p$ be the cosets of $\mathcal{P}_1\mathbb{Z}^d$ in $\mathbb{Z}^d$ and $I^1, \dots, I^q$ the cosets of $\mathcal{P}_2\mathbb{Z}^d$ and let $A_i = A \cap I_i$, $A^j = A \cap I^j$ and $A_i^j = A \cap I_i \cap I^j$. If either

1. $A_i, A^j \neq \emptyset$ *for all* $1 \leq i \leq p, 1 \leq j \leq q$ *or*

2. *there are some* i, j *such that* $A_i, A^j \neq \emptyset$ *and* $|A_i^j| \leq c|A|$, *where* $c = \frac{1}{2p(p^{1/d}+q^{1/d})^{2d}}$,

then

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq ((p^{1/d} + q^{1/d})^d - (1-c)\alpha)|A| - ((p+q)D_1 + D)|A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$.

Proof. Since $\mathcal{L}_1, \mathcal{L}_2$ are irreducible, $\mathcal{L}_1^{-1}\mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Q})$ has no non-trivial invariant subspace over $\mathbb{Q}$. We may also assume that $|\mathcal{L}_1 A + \mathcal{L}_2 A| \leq (p^{1/d} + q^{1/d})^d |A|$, so that, by Lemma 3.1.5 with $\mathcal{L} = \mathcal{L}_1^{-1}\mathcal{L}_2$, there are $\sigma_1, D > 0$ such that, for any $B_1, B_2 \subseteq A$,

$$|\mathcal{L}_1 B_1 + \mathcal{L}_2 B_2| = |B_1 + \mathcal{L} B_2| \geq (|B_1|^{1/d} + |B_2|^{1/d})^d - D|A|^{1-\sigma_1}.$$

We claim that there is a choice of i and j such that $A_i, A^j \neq \emptyset$ and

$$(|A_i|^{1/d} + |A^j|^{1/d})^d - ((p^{1/d} + q^{1/d})^d - \alpha)|A_i^j| \geq \alpha c|A|.$$

Suppose first that $A_i, A^j \neq \emptyset$ for all i, j. Pick i and j such that $|A_i^j|$ is minimal. If $|A_i^j| \leq c|A|$, then we may pass to the second case. Otherwise, $|A_i^j| > c|A|$. Since, for any i', j', we have $|A_{i'}^j| \geq |A_i^j|$ and $|A_i^{j'}| \geq |A_i^j|$, we see that $|A^j| \geq p|A_i^j|$ and $|A_i| \geq q|A_i^j|$. Hence,

$$(|A_i|^{1/d} + |A^j|^{1/d})^d - ((p^{1/d} + q^{1/d})^d - \alpha)|A_i^j| \geq \alpha|A_i^j| \geq \alpha c|A|.$$

Suppose now that there are i, j such that $A_i, A^j \neq \emptyset$ and $|A_i^j| \leq c|A|$. If there is some i' such that $|A_{i'}^j| > (p^{1/d} + q^{1/d})^d c|A|$, then

$$\begin{aligned}
&(|A_i|^{1/d} + |A^j|^{1/d})^d - ((p^{1/d} + q^{1/d})^d - \alpha)|A_i^j| \\
&\geq |A_{i'}^j| - ((p^{1/d} + q^{1/d})^d - \alpha)|A_i^j| \\
&\geq (p^{1/d} + q^{1/d})^d c|A| - ((p^{1/d} + q^{1/d})^d - \alpha)c|A| \\
&= \alpha c|A|.
\end{aligned}$$

Otherwise, we may assume that $|A^j_{i'}| \leq (p^{1/d}+q^{1/d})^d c|A|$ for all i'. Since $\sum_i |A_i| = |A|$, there is some i' such that $|A_{i'}| \geq |A|/p$. Thus,

$$\begin{aligned}
&(|A_{i'}|^{1/d} + |A^j|^{1/d})^d - ((p^{1/d}+q^{1/d})^d - \alpha)|A^j_{i'}| \\
&\geq |A_{i'}| - ((p^{1/d}+q^{1/d})^d - \alpha)|A^j_{i'}| \\
&\geq \frac{1}{p}|A| - ((p^{1/d}+q^{1/d})^d - \alpha)(p^{1/d}+q^{1/d})^d c|A| \\
&\geq \frac{1}{2p}|A| > \alpha c|A|.
\end{aligned}$$

This proves the claim. From here on, without loss of generality, we will assume that $A_1, A^1 \neq \emptyset$ and

$$(|A_1|^{1/d} + |A^1|^{1/d})^d - ((p^{1/d}+q^{1/d})^d - \alpha)|A^1_1| \geq \alpha c|A|. \tag{3.1}$$

We will now show that the sets $\mathcal{L}_1 A + \mathcal{L}_2 A_i$ belong to different cosets of $\mathcal{L}_1\mathbb{Z}^d$ for $i = 1, \dots, p$ and so are disjoint. Note that $\mathcal{L}_2\mathcal{P}_1\mathbb{Z}^d \subseteq \mathcal{L}_1\mathbb{Z}^d$, so the sets do indeed belong to cosets of $\mathcal{L}_1\mathbb{Z}^d$. If, for some i, i', the corresponding sets belong to the same coset, then $\mathcal{L}_2 I_i - \mathcal{L}_2 I_{i'} \subseteq \mathcal{L}_1\mathbb{Z}^d$, so $I_i - I_{i'} \subseteq \mathcal{L}_2^{-1}\mathcal{L}_1\mathbb{Z}^d$. But this means that I_i and $I_{i'}$ are the same coset of $\mathcal{P}_1\mathbb{Z}^d$. Hence, $\mathcal{L}_1 A + \mathcal{L}_2 A$ can be partitioned into the sets $\mathcal{L}_1 A + \mathcal{L}_2 A_i$ for $i = 1, \dots, p$. Similarly, the sets $\mathcal{L}_1 A^j + \mathcal{L}_2 A_1$ belong to disjoint cosets of $\mathcal{L}_2\mathbb{Z}^d$, so $\mathcal{L}_1 A + \mathcal{L}_2 A_1$ can be partitioned into the sets $\mathcal{L}_1 A^j + \mathcal{L}_2 A_1$ for $j = 1, 2, \dots, q$.

Note now that, by our choice of σ_1 and D, we have

$$|\mathcal{L}_1 A^1 + \mathcal{L}_2 A_1| \geq (|A^1|^{1/d} + |A_1|^{1/d})^d - D|A|^{1-\sigma_1}.$$

Thus, using our earlier claim, we have

$$\begin{aligned}
|\mathcal{L}_1 A + \mathcal{L}_2 A| &= \sum_{i=2}^{p} |\mathcal{L}_1 A + \mathcal{L}_2 A_i| + \sum_{j=2}^{q} |\mathcal{L}_1 A^j + \mathcal{L}_2 A_1| + |\mathcal{L}_1 A^1 + \mathcal{L}_2 A_1| \\
&\geq \sum_{i=2}^{p} |\mathcal{L}_1 A_i + \mathcal{L}_2 A_i| + \sum_{j=2}^{q} |\mathcal{L}_1 A^j_1 + \mathcal{L}_2 A^j_1| + |\mathcal{L}_1 A^1 + \mathcal{L}_2 A_1| \\
&\geq ((p^{1/d}+q^{1/d})^d - \alpha)(|A| - |A^1_1|) - (p+q)D_1|A|^{1-\sigma_1} \\
&\quad + (|A^1|^{1/d} + |A_1|^{1/d})^d - D|A|^{1-\sigma_1} \\
&\geq ((p^{1/d}+q^{1/d})^d - \alpha)|A| + \alpha c|A| - ((p+q)D_1 + D)|A|^{1-\sigma_1} \\
&= ((p^{1/d}+q^{1/d})^d - (1-c)\alpha)|A| - ((p+q)D_1 + D)|A|^{1-\sigma_1},
\end{aligned}$$

as required, where we used (3.1) in going from the third to the fourth line. □

We now introduce some further notation. Indeed, let $\mathcal{P} \in \mathrm{Mat}_d(\mathbb{Z})$ be a linear transformation such that

$$\mathcal{P}\mathbb{Z}^d = \mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathbb{Z}^d = \mathcal{P}_1\mathbb{Z}^d \cap \mathcal{P}_2\mathbb{Z}^d.$$

Then, by Lemma 3.3.1,

$$\begin{aligned} |\det \mathcal{P}| &= [\mathbb{Z}^d : \mathcal{P}\mathbb{Z}^d] = [\mathbb{Z}^d : \mathcal{P}_1\mathbb{Z}^d + \mathcal{P}_2\mathbb{Z}^d][\mathcal{P}_1\mathbb{Z}^d + \mathcal{P}_2\mathbb{Z}^d : \mathcal{P}_1\mathbb{Z}^d \cap \mathcal{P}_2\mathbb{Z}^d] \\ &= [\mathbb{Z}^d : \mathcal{P}_1\mathbb{Z}^d + \mathcal{P}_2\mathbb{Z}^d][\mathcal{P}_1\mathbb{Z}^d + \mathcal{P}_2\mathbb{Z}^d : \mathcal{P}_1\mathbb{Z}^d][\mathcal{P}_1\mathbb{Z}^d + \mathcal{P}_2\mathbb{Z}^d : \mathcal{P}_2\mathbb{Z}^d] \\ &\leq [\mathbb{Z}^d : \mathcal{P}_1\mathbb{Z}^d][\mathbb{Z}^d : \mathcal{P}_2\mathbb{Z}^d] = |\det \mathcal{P}_1||\det \mathcal{P}_2| = pq. \end{aligned}$$

Moreover, let $\mathcal{Q} \in \mathrm{Mat}_d(\mathbb{Z})$ be such that

$$\mathcal{Q}\mathbb{Z}^d = \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d,$$

so that, as above, $|\det \mathcal{Q}| = |\det \mathcal{L}_1||\det \mathcal{L}_2| = pq$.

Note that $\mathcal{L}_1\mathcal{P}\mathbb{Z}^d, \mathcal{L}_2\mathcal{P}\mathbb{Z}^d \subseteq \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d = \mathcal{Q}\mathbb{Z}^d$, so $\mathcal{Q}^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d, \mathcal{Q}^{-1}\mathcal{L}_2\mathcal{P}\mathbb{Z}^d \subseteq \mathbb{Z}^d$, implying that $\mathcal{Q}^{-1}\mathcal{L}_1\mathcal{P}, \mathcal{Q}^{-1}\mathcal{L}_2\mathcal{P} \in \mathrm{Mat}_d(\mathbb{Z})$. Therefore, since $\mathcal{L}_1, \mathcal{L}_2$ are coprime,

$$|\det \mathcal{Q}^{-1}\mathcal{P}| \geq 1.$$

But $|\det \mathcal{Q}| = pq$ and $|\det \mathcal{P}| \leq pq$, so we must have $|\det \mathcal{P}| = pq$.

Finally, we let L_1 be the lattice $\mathcal{P}\mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ and $L_2 = \mathcal{P}\mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathcal{P}\mathbb{Z}^d$. The next lemma will be important in the proof of Lemma 3.3.4 below, which, like Lemma 3.2.2 in the last section, says that any set A falls into one of three categories, each helpful for our bootstrap.

Lemma 3.3.3. *The linear maps $\mathcal{L}_1, \mathcal{L}_2$ induce homomorphisms*

$$\phi_1, \phi_2 : \mathbb{Z}^d/L_1 \to \mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$$

of finite abelian groups. Furthermore, $\phi_1 + \phi_2$ is an isomorphism.

Proof. If $x \in L_1$, then $\mathcal{L}_1 x \in \mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ and $\mathcal{L}_2 x \in \mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, so ϕ_1 and ϕ_2 are well-defined group homomorphisms. Now let $\phi' : \mathbb{Z}^d \to \mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ be the map induced by $\mathcal{L}_1 + \mathcal{L}_2$.

We first show that $\ker \phi' = L_1$. We have already seen above that $\ker \phi' \supseteq L_1$. For the converse, suppose that $x \in \ker \phi'$, so that $\mathcal{L}_1 x + \mathcal{L}_2 x = \mathcal{L}_1\mathcal{P}y$ for some $y \in \mathbb{Z}^d$. This implies that

$$x = \mathcal{P}y - \mathcal{L}_1^{-1}\mathcal{L}_2 x,$$

$$x = \mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}y - \mathcal{L}_2^{-1}\mathcal{L}_1 x.$$

Since $\mathcal{P}y \in \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d$, the first equation implies that $x \in \mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d$. From the second equation, we have $x \in \mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathbb{Z}^d$, so that $x \in \mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathbb{Z}^d = \mathcal{P}\mathbb{Z}^d$. It then follows from applying the second equation again that $x \in \mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, so that $x \in \mathcal{P}\mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d = L_1$, proving that $\ker\phi' = L_1$.

Hence, the induced map $\phi : \mathbb{Z}^d/L_1 \to \mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ is injective. To show that it is in fact an isomorphism, we shall show that $|\mathbb{Z}^d/L_1| = |\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d|$. From injectivity, we have $|\mathbb{Z}^d/L_1| \le |\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d|$, so it suffices to show that $|\mathbb{Z}^d/L_1| \ge |\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d|$.

Let $\mathcal{R} \in \mathrm{Mat}_d(\mathbb{Z})$ be such that $\mathcal{R}\mathbb{Z}^d = \mathcal{L}_1\mathcal{P}\mathbb{Z}^d + \mathcal{L}_2\mathcal{P}\mathbb{Z}^d$. Then $\mathcal{R}^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d \subseteq \mathbb{Z}^d$ and $\mathcal{R}^{-1}\mathcal{L}_2\mathcal{P}\mathbb{Z}^d \subseteq \mathbb{Z}^d$, so $\mathcal{R}^{-1}\mathcal{L}_1\mathcal{P}$ and $\mathcal{R}^{-1}\mathcal{L}_2\mathcal{P}$ are integer matrices. By coprimality, we have $|\det\mathcal{R}| \le |\det\mathcal{P}|$. By Lemma 3.3.1, we have

$$\begin{aligned}&[\mathcal{L}_1\mathcal{P}\mathbb{Z}^d + \mathcal{L}_2\mathcal{P}\mathbb{Z}^d : \mathcal{L}_1\mathcal{P}\mathbb{Z}^d \cap \mathcal{L}_2\mathcal{P}\mathbb{Z}^d]\\ &= [\mathcal{L}_1\mathcal{P}\mathbb{Z}^d + \mathcal{L}_2\mathcal{P}\mathbb{Z}^d : \mathcal{L}_1\mathcal{P}\mathbb{Z}^d][\mathcal{L}_1\mathcal{P}\mathbb{Z}^d + \mathcal{L}_2\mathcal{P}\mathbb{Z}^d : \mathcal{L}_2\mathcal{P}\mathbb{Z}^d].\end{aligned}$$

In other words, $[\mathbb{Z}^d : \mathcal{L}_2L_1]|\det\mathcal{R}| = [\mathbb{Z}^d : \mathcal{L}_1\mathcal{P}\mathbb{Z}^d][\mathbb{Z}^d : \mathcal{L}_2\mathcal{P}\mathbb{Z}^d]$. Since $|\det\mathcal{R}| \le |\det\mathcal{P}|$, it follows from $[\mathbb{Z}^d : \mathcal{L}_2L_1] = |\det\mathcal{L}_2|[\mathbb{Z}^d : L_1]$ and $[\mathbb{Z}^d : \mathcal{L}_2\mathcal{P}\mathbb{Z}^d] = |\det\mathcal{L}_2|[\mathbb{Z}^d : \mathcal{P}\mathbb{Z}^d]$ that $[\mathbb{Z}^d : L_1] \ge [\mathbb{Z}^d : \mathcal{L}_1\mathcal{P}\mathbb{Z}^d]$, as required. □

Since $\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ has index $|\det\mathcal{L}_1\mathcal{P}| = p^2q$ and $\phi_1+\phi_2$ is an isomorphism, the lemma implies that L_1 also has index p^2q. Similarly, L_2 has index pq^2.

Lemma 3.3.4. *Let X be a subset of $G = \mathbb{Z}^d/L_1$ containing 0 and define ϕ_1, ϕ_2 as in the previous lemma. Then at least one of the following holds:*

1. *X does not generate G;*
2. *$|\phi_1(X) + \phi_2(X)| > |X|$;*
3. *$\mathcal{P}\mathbb{Z}^d/L_1 \subseteq X$.*

Proof. Suppose all 3 do not hold. Let $\phi = \phi_1 + \phi_2$, which is an isomorphism by Lemma 3.3.3. Note that $\phi(X) \subseteq \phi_1(X) + \phi_2(X)$, so $|\phi_1(X) + \phi_2(X)| \ge |X|$ always holds. By assumption, we must have $\phi_1(X) + \phi_2(X) = \phi(X)$. Hence, for any $x, y \in X$, we have $\phi^{-1}\phi_1(x) + \phi^{-1}\phi_2(y) \in X$. In particular, since $0 \in X$, we have $\phi^{-1}\phi_1(x), \phi^{-1}\phi_2(x) \in X$.

We claim that $\phi^{-1}\phi_2(G) = \mathcal{P}_2\mathbb{Z}^d/L_1$ and $\phi^{-1}\phi_1(\mathcal{P}_2\mathbb{Z}^d/L_1) = \mathcal{P}\mathbb{Z}^d/L_1$. For the first claim, note that $\phi_2(G) = \mathcal{L}_2\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, so it suffices to show that $\phi(\mathcal{P}_2\mathbb{Z}^d/L_1) =$

$\mathcal{L}_2\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$. Note that, for any $x \in \mathcal{P}_2\mathbb{Z}^d = \mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d$, we have $\mathcal{L}_1 x, \mathcal{L}_2 x \in \mathcal{L}_2\mathbb{Z}^d$, so that $\phi(\mathcal{P}_2\mathbb{Z}^d/L_1) \subseteq \mathcal{L}_2\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$. Since $\mathcal{P}_2\mathbb{Z}^d$ and $\mathcal{L}_2\mathbb{Z}^d$ have index q and L_1 and $\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ have index p^2q, we have $|\mathcal{P}_2\mathbb{Z}^d/L_1| = |\mathcal{L}_2\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d| = p^2$. Since ϕ is an isomorphism, we must then have $\phi(\mathcal{P}_2\mathbb{Z}^d/L_1) = \mathcal{L}_2\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$.

For the second claim, note that $\phi_1(\mathcal{P}_2\mathbb{Z}^d/L_1) = \mathcal{L}_1\mathcal{P}_2\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d = (\mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d)/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, so it suffices to show that $\phi(\mathcal{P}\mathbb{Z}^d/L_1) = (\mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d)/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$. If $x \in \mathcal{P}\mathbb{Z}^d$, then $\mathcal{L}_1 x, \mathcal{L}_2 x \in \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d$, so we have the inclusion $\phi(\mathcal{P}\mathbb{Z}^d/L_1) \subseteq (\mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d)/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$. By again counting sizes, we have $|\mathcal{P}\mathbb{Z}^d/L_1| = |(\mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d)/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d| = p$, so $\phi(\mathcal{P}\mathbb{Z}^d/L_1) = (\mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d)/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, proving our claim.

Let $X' = X \cap \mathcal{P}_2\mathbb{Z}^d/L_1$. Since $\phi^{-1}\phi_2(X) \subseteq X'$ and X generates G, we have that X' generates $\mathcal{P}_2\mathbb{Z}^d/L_1$. Moreover, $\phi^{-1}\phi_1(X') \subseteq X$ and generates $\mathcal{P}\mathbb{Z}^d/L_1$. Note that, for any $x \in \mathcal{P}\mathbb{Z}^d/L_1$, $\phi_1(x) = 0$, so $\phi^{-1}\phi_2(x) = x$. This implies that, for any $x \in X \cap \mathcal{P}\mathbb{Z}^d/L_1$ and $y \in X'$, we have $\phi^{-1}\phi_1(y) + x = \phi^{-1}\phi_1(y) + \phi^{-1}\phi_2(x) \in X \cap \mathcal{P}\mathbb{Z}^d/L_1$, so $X \cap \mathcal{P}\mathbb{Z}^d/L_1$ is closed under adding elements of $\phi^{-1}\phi_1(X')$. But $\phi^{-1}\phi_1(X')$ generates $\mathcal{P}\mathbb{Z}^d/L_1$ and $0 \in X \cap \mathcal{P}\mathbb{Z}^d/L_1$. It follows that $X \cap \mathcal{P}\mathbb{Z}^d/L_1 = \mathcal{P}\mathbb{Z}^d/L_1$, contradicting our third assumption. □

We now come to our main bootstrapping lemma.

Lemma 3.3.5. *Let d, p and q be positive integers. Then there are constants $\sigma_1 > 0$ and $D > 0$ depending only on d, p and q such that the following holds. Suppose that there are $0 < \alpha < (p^{1/d} + q^{1/d})^d$ and $D_1 > 0$ such that*

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq ((p^{1/d} + q^{1/d})^d - \alpha)|A| - D_1|A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$ and all irreducible, coprime linear transformations $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ with $|\det \mathcal{L}_1| = p$ and $|\det \mathcal{L}_2| = q$. Then

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq ((p^{1/d} + q^{1/d})^d - (1 - c^2)\alpha)|A| - (4p^2q^2D_1 + D)|A|^{1-\sigma_1}$$

holds for all such $A \subset \mathbb{Z}^d$ and $\mathcal{L}_1, \mathcal{L}_2$, where $c = \frac{1}{2\max(p,q)(p^{1/d}+q^{1/d})^{2d}}$.

Proof. Take σ_1, D as in Lemma 3.3.2. By translating A, we may assume that $0 \in A$. We may also assume that $|\mathcal{L}_1 A + \mathcal{L}_2 A| \leq (p^{1/d} + q^{1/d})^d |A|$, so that, by Lemma 3.1.4, A cannot lie on a hyperplane. Suppose now that A is a counterexample to the lemma with $[\mathbb{Z}^d : \langle A \rangle]$ minimal. Let A' be the image of A in $\mathbb{Z}^d/L_1$. By Lemma 3.3.4, one of the following possibilities holds:

1. A' does not generate $\mathbb{Z}^d/L_1$;
2. $|\phi_1(A') + \phi_2(A')| > |A'|$;
3. $\mathcal{P}\mathbb{Z}^d/L_1 \subseteq A'$.

We consider each case separately.

Case 1: (1) holds, but not (2)

The fact that (1) holds means that $\langle A\rangle + L_1 \neq \mathbb{Z}^d$, so it must be a strictly smaller sublattice of $\mathbb{Z}^d$ of some index $k > 1$. Let $Q \in \mathrm{Mat}_d(\mathbb{Z})$ be such that $Q\mathbb{Z}^d = \langle A\rangle + L_1$, so that $|\det Q| = k$. Since (2) does not hold, we have $\phi_1(A') + \phi_2(A') = \phi(A')$, so $\langle \phi_1(A') + \phi_2(A')\rangle = \phi(\langle A'\rangle)$. Since ϕ is an isomorphism and $\langle A'\rangle$ is a subgroup of $\mathbb{Z}/L_1$ of index k, $\phi(\langle A'\rangle)$ is a subgroup of $\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ of index k. Thus, $\langle \mathcal{L}_1 A + \mathcal{L}_2 A\rangle + \mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ is a sublattice of $\mathbb{Z}^d$ of index k.

Let $Q' \in \mathrm{Mat}_d(\mathbb{Z})$ be such that $Q'\mathbb{Z}^d = \langle \mathcal{L}_1 A + \mathcal{L}_2 A\rangle + \mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, so that $|\det Q'| = k$. Notice that

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| = |Q'^{-1}\mathcal{L}_1 Q(Q^{-1}A) + Q'^{-1}\mathcal{L}_2 Q(Q^{-1}A)|,$$

so we may replace the triple $(\mathcal{L}_1, \mathcal{L}_2, A)$ with $(Q'^{-1}\mathcal{L}_1 Q, Q'^{-1}\mathcal{L}_2 Q, Q^{-1}A)$. It is easy to see that $Q'^{-1}\mathcal{L}_1 Q, Q'^{-1}\mathcal{L}_2 Q$ are still irreducible and coprime and $Q^{-1}A \subset \mathbb{Z}^d$. However, this contradicts the minimality of $[\mathbb{Z}^d : \langle A\rangle]$, since $[\mathbb{Z}^d : \langle Q^{-1}A\rangle] = [\mathbb{Z}^d : \langle A\rangle]/k$.

Case 2: (2) holds

Let $I_1, \ldots, I_{pq}$ be the cosets of $\mathcal{P}\mathbb{Z}^d$ with $0 \in I_1$ and let $A_i = A \cap I_i$ for $i = 1, \ldots, pq$. Note that the cosets I_i are the intersections of the cosets of $\mathcal{P}_1\mathbb{Z}^d$ and the cosets of $\mathcal{P}_2\mathbb{Z}^d$. If $0 < |A_i| \leq c|A|$ for some i, then condition 2 of Lemma 3.3.2 implies that

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq ((p^{1/d} + q^{1/d})^d - (1-c)\alpha)|A| - ((p+q)D_1 + D)|A|^{1-\sigma_1}.$$

We may therefore assume that $|A_i| > c|A|$ whenever $A_i \neq \emptyset$. Let $I_{i,k}$ be the cosets of $\mathcal{P}\mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ in I_i for $k = 1, \ldots, p$, where $0 \in I_{1,1}$, and let $A_{i,k} = A \cap I_{i,k} = A_i \cap I_{i,k}$.

Suppose that $|A_{i,k}| > c^2|A|$ whenever $A_{i,k} \neq \emptyset$. By (2), $|\phi_1(A') + \phi_2(A')| > |A'| = |\phi(A')|$. Hence, since $\phi(A') \subseteq \phi_1(A') + \phi_2(A')$, there are $a_1, a_2 \in A$ such that

$$\mathcal{L}_1 a_1 + \mathcal{L}_2 a_2 \notin (\mathcal{L}_1 + \mathcal{L}_2)a + \mathcal{L}_1\mathcal{P}\mathbb{Z}^d$$

for all $a \in A$. Take i_1, k_1, i_2, k_2 such that $a_1 \in A_{i_1,k_1}, a_2 \in A_{i_2,k_2}$, so they are both non-empty. Then

$$\mathcal{L}_1 A_{i_1,k_1} + \mathcal{L}_2 A_{i_2,k_2} \subset \mathcal{L}_1 a_1 + \mathcal{L}_2 a_2 + \mathcal{L}_1 \mathcal{P}\mathbb{Z}^d,$$

which is disjoint from any of the $\mathcal{L}_1 A_{i,k} + \mathcal{L}_2 A_{i,k}$. Therefore,

$$\begin{aligned}
|\mathcal{L}_1 A + \mathcal{L}_2 A| &\geq \sum_{i=1}^{pq} \sum_{k=1}^{p} |\mathcal{L}_1 A_{i,k} + \mathcal{L}_2 A_{i,k}| + |\mathcal{L}_1 A_{i_1,k_1} + \mathcal{L}_2 A_{i_2,k_2}| \\
&\geq ((p^{1/d} + q^{1/d})^d - \alpha)|A| - p^2 q D_1 |A|^{1-\sigma_1} + |A_{i_1,k_1}| \\
&\geq ((p^{1/d} + q^{1/d})^d - (1 - c^2)\alpha)|A| - p^2 q D_1 |A|^{1-\sigma_1}.
\end{aligned}$$

Otherwise, by translating if necessary, we may assume that $|A_{1,1}| \leq c^2|A| \leq c|A_1|$ and $0 \in A_{1,1}$. Let $Q \in \mathrm{Mat}_d(\mathbb{Z})$ be such that $Q\mathbb{Z}^d = \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d$, so that $|\det Q| = pq$. Set $\mathcal{M}_i = Q^{-1}\mathcal{L}_i\mathcal{P}$. Since $\mathcal{L}_i\mathcal{P}\mathbb{Z}^d \subseteq \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d = Q\mathbb{Z}^d$, we have $\mathcal{M}_i\mathbb{Z}^d \subseteq \mathbb{Z}^d$ for $i = 1, 2$, so $\mathcal{M}_i \in \mathrm{Mat}_d(\mathbb{Z})$. Moreover, $\mathcal{M}_1, \mathcal{M}_2$ are irreducible and coprime, with determinants of absolute value p and q, respectively.

If we let $B = \mathcal{P}^{-1}A_1 \subset \mathbb{Z}^d$, our aim now is to apply Lemma 3.3.2 to the sum $\mathcal{M}_1 B + \mathcal{M}_2 B$. Indeed, if we replace $\mathcal{P}_1, \mathcal{P}_2$ in that lemma by $\mathcal{P}_1', \mathcal{P}_2'$ chosen so that $\mathcal{P}_1'\mathbb{Z}^d = \mathbb{Z}^d \cap \mathcal{M}_2^{-1}\mathcal{M}_1\mathbb{Z}^d$ and $\mathcal{P}_2'\mathbb{Z}^d = \mathbb{Z}^d \cap \mathcal{M}_1^{-1}\mathcal{M}_2\mathbb{Z}^d$, the set A_1 by $B_1 = \mathcal{P}^{-1}A_{1,1}$, which, since $A_{1,1} = A_1 \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, satisfies $B_1 = B \cap \mathcal{P}^{-1}\mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d = B \cap \mathcal{M}_2^{-1}\mathcal{M}_1\mathbb{Z}^d$, and A_1^1 by an appropriate non-empty subset $B_1^1 \subseteq B_1$ (which is possible since B_1 contains 0), then we have $0 < |B_1^1| \leq |B_1| \leq c|B|$, so condition 2 of Lemma 3.3.2 holds. Hence, by that lemma,

$$|\mathcal{M}_1 B + \mathcal{M}_2 B| \geq ((p^{1/d} + q^{1/d})^d - (1 - c)\alpha)|B| - ((p + q)D_1 + D)|B|^{1-\sigma_1}.$$

This implies that

$$\begin{aligned}
|\mathcal{L}_1 A_1 + \mathcal{L}_2 A_1| &= |Q^{-1}\mathcal{L}_1\mathcal{P}(\mathcal{P}^{-1}A_1) + Q^{-1}\mathcal{L}_2\mathcal{P}(\mathcal{P}^{-1}A_1)| \\
&= |\mathcal{M}_1 B + \mathcal{M}_2 B| \\
&\geq ((p^{1/d} + q^{1/d})^d - (1 - c)\alpha)|B| - ((p + q)D_1 + D)|B|^{1-\sigma_1} \\
&\geq ((p^{1/d} + q^{1/d})^d - (1 - c)\alpha)|A_1| - ((p + q)D_1 + D)|A|^{1-\sigma_1}.
\end{aligned}$$

Thus, since $|A_1| \geq c|A|$,

$$\begin{aligned}
|\mathcal{L}_1 A + \mathcal{L}_2 A| &\geq \sum_{i=2}^{pq} |\mathcal{L}_1 A_i + \mathcal{L}_2 A_i| + |\mathcal{L}_1 A_1 + \mathcal{L}_2 A_1| \\
&\geq ((p^{1/d} + q^{1/d})^d - \alpha)(|A| - |A_1|) - pqD_1|A|^{1-\sigma_1} \\
&\quad + ((p^{1/d} + q^{1/d})^d - (1-c)\alpha)|A_1| - ((p+q)D_1 + D)|A|^{1-\sigma_1} \\
&\geq ((p^{1/d} + q^{1/d})^d - \alpha)|A| + c\alpha|A_1| - ((p+q+pq)D_1 + D)|A|^{1-\sigma_1} \\
&\geq ((p^{1/d} + q^{1/d})^d - \alpha)|A| + c^2\alpha|A| - ((p+q+pq)D_1 + D)|A|^{1-\sigma_1} \\
&\geq ((p^{1/d} + q^{1/d})^d - (1-c^2)\alpha)|A| - (4p^2q^2D_1 + D)|A|^{1-\sigma_1}.
\end{aligned}$$

Case 3: (3) holds

Let A'' be the image of A in $\mathbb{Z}^d/L_2$. If we apply Lemma 3.3.4 to A'', but with the roles of $\mathcal{L}_1, \mathcal{L}_2$ swapped, we arrive at three similar cases. If either of the first two occurs, then we are again done as above. Otherwise, the third case holds, i.e., $\mathcal{P}\mathbb{Z}^d/L_2 \subseteq A''$. Define $A_1, \mathcal{M}_1, \mathcal{M}_2, B$ as in Case 2 and partition B into $B_1 \cup \cdots \cup B_p$, where the B_i belong to different cosets of $\mathbb{Z}^d \cap \mathcal{M}_2^{-1}\mathcal{M}_1\mathbb{Z}^d$, and into $B^1 \cup \cdots \cup B^q$, where the B^j belong to different cosets of $\mathbb{Z}^d \cap \mathcal{M}_1^{-1}\mathcal{M}_2\mathbb{Z}^d$.

Since $\mathcal{P}\mathbb{Z}^d/L_1 \subseteq A'$, we have $\mathcal{P}\mathbb{Z}^d \subseteq A + L_1$ and so $\mathcal{P}\mathbb{Z}^d \subseteq A_1 + L_1$, since $A_1 = A \cap \mathcal{P}\mathbb{Z}^d$. Thus, $\mathbb{Z}^d = \mathcal{P}^{-1}A_1 + \mathcal{P}^{-1}L_1$, which means that $B = \mathcal{P}^{-1}A_1$ intersects every coset of $\mathcal{P}^{-1}L_1 = \mathbb{Z}^d \cap \mathcal{P}^{-1}\mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d = \mathbb{Z}^d \cap \mathcal{M}_2^{-1}\mathcal{M}_1\mathbb{Z}^d$, so all the B_i are non-empty. Similarly, all of the B^j are non-empty. Thus, condition 1 of Lemma 3.3.2 holds, so that

$$|\mathcal{M}_1 B + \mathcal{M}_2 B| \geq ((p^{1/d} + q^{1/d})^d - (1-c)\alpha)|B| - ((p+q)D_1 + D)|B|^{1-\sigma_1}.$$

The same calculation as in Case 2 then shows that

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq ((p^{1/d} + q^{1/d})^d - (1-c^2)\alpha)|A| - (4p^2q^2D_1 + D)|A|^{1-\sigma_1},$$

as required. □

Theorem 3.3.6. *Let $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ be irreducible, coprime linear transformations with $|\det \mathcal{L}_1| = p$ and $|\det \mathcal{L}_2| = q$. Then there are constants $\sigma_2 > 0$ and $D_2 > 0$ depending only on d, p and q such that*

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq (p^{1/d} + q^{1/d})^d |A| - D_2|A|^{1-\sigma_2}$$

for all finite $A \subset \mathbb{Z}^d$.

Proof. This follows from Lemma 3.3.5, identical to how Theorem 3.2.4 follows from Lemma 3.2.3. □

3.4 Concluding remarks

Better bounds. Although Theorem 3.0.5 can be tight, there is a stronger general bound. In analogy with the algebraic number setting, given $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Q})$ with minimal polynomial $f(x) \in \mathbb{Z}[x]$, which we assume to have coprime coefficients, suppose that $f(x) = \prod_{i=1}^{d}(a_i x + b_i)$ is a full complex factorization of f and let $H(\mathcal{L}) = \prod_{i=1}^{d}(|a_i| + |b_i|)$. We will prove the following, a variant of a recent conjecture of Krachun and Petrov [28, Conjecture 2] that was itself inspired by a continuous analogue [28, Theorem 2].

Theorem 3.4.1. *Let $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ be irreducible. Then, for any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq H(\mathcal{L}_1^{-1}\mathcal{L}_2)|A| - o(|A|).$$

The proof of the above will be delayed to Chapter 7. Note that the coprimeness condition is unnecessary here, since if we were to replace $\mathcal{L}_1, \mathcal{L}_2$ with $\mathcal{P}\mathcal{L}_1\mathcal{Q}, \mathcal{P}\mathcal{L}_2\mathcal{Q}$ to make them coprime, then

$$H((\mathcal{P}\mathcal{L}_1\mathcal{Q})^{-1}(\mathcal{P}\mathcal{L}_2\mathcal{Q})) = H(\mathcal{Q}^{-1}\mathcal{L}_1^{-1}\mathcal{L}_2\mathcal{Q}) = H(\mathcal{L}_1^{-1}\mathcal{L}_2).$$

Moreover, Theorem 3.4.1 implies our Theorem 3.0.5, since if $\mathcal{L}_1, \mathcal{L}_2$ are coprime, then it can be shown that the minimal polynomial of $\mathcal{L}_1^{-1}\mathcal{L}_2$ over $\mathbb{Z}$ is $c_d x^d + c_{d-1}x^{d-1} + \cdots + c_0$, where $|c_d| = |\det(\mathcal{L}_1)|$ and $|c_0| = |c_d||\det(\mathcal{L}_1^{-1}\mathcal{L}_2)| = |\det(\mathcal{L}_2)|$. Therefore, by Hölder's inequality,

$$H(\mathcal{L}_1^{-1}\mathcal{L}_2) = \prod_{i=1}^{d}(|a_i| + |b_i|) \geq \left(\prod_{i=1}^{d}|a_i|^{1/d} + \prod_{i=1}^{d}|b_i|^{1/d}\right)^d = (|c_d|^{1/d} + |c_0|^{1/d})^d.$$

There should also be a suitable generalization of Theorem 3.4.1 to more than two variables, but, unlike Conjecture 3.0.4, which itself remains open for three or more variables, it is not at all obvious what this should be.

Lower-order terms. Unlike with sums of dilates (see, for instance, [2, 25, 42] and Chapter 2), we cannot in general hope for the error term in Theorem 3.0.5 to be a constant. Indeed, in two dimensions, if we set $A = \{(x, y) : 0 \leq x, y \leq n-1\}$ and $\mathcal{L}$ to be the anti-clockwise rotation about the origin through $\pi/2$, then $|A| = n^2$, but $|A + \mathcal{L}A| = (2n-1)^2 = 4|A| - 4|A|^{1/2} + 1$. That is, the error term in this case is a multiple of $|A|^{1/2}$. Similarly, in d dimensions, there are examples for which the

error term is a multiple of $|A|^{1-1/d}$. Following Shakan [42], we conjecture that there are no significantly worse examples.

Conjecture 3.4.2. *Suppose that $\mathcal{L}_1, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Then there is a constant D such that, for any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_1 A + \cdots + \mathcal{L}_k A| \geq \left(|\det(\mathcal{L}_1)|^{1/d} + \cdots + |\det(\mathcal{L}_k)|^{1/d}\right)^d |A| - D|A|^{1-1/d}.$$

A proof of this conjecture when $k = 2$ would already constitute a significant improvement on our Theorem 3.0.5, which gives an error term of the form $D|A|^{1-\sigma}$ for some $\sigma > 0$ which depends not only on d, but also on $|\det(\mathcal{L}_1)|$ and $|\det(\mathcal{L}_2)|$.

Real-valued analogues. Our main result, Theorem 3.0.5, can be extended to subsets of $\mathbb{R}^d$ as follows.

Theorem 3.4.3. *Suppose that $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Then there are constants D, $\sigma > 0$ such that, for any finite subset A of $\mathbb{R}^d$,*

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq \left(|\det(\mathcal{L}_1)|^{1/d} + |\det(\mathcal{L}_2)|^{1/d}\right)^d |A| - D|A|^{1-\sigma}.$$

To see this, suppose that $A \subset \mathbb{R}^d$ and let $B \subset \mathbb{R}$ be the set consisting of all real numbers that appear as a coordinate of some element of A. For any fixed natural number k, a standard result in additive combinatorics (see, for instance, [48, Lemma 5.25]) allows us to find a set $B' \subset \mathbb{Z}$ which has a Freiman isomorphism of order k with B. We then obtain a set $A' \subset \mathbb{Z}^d$ by replacing each coordinate of each element of A with its image in B'. Provided k is chosen sufficiently large in terms of the coefficients of $\mathcal{L}_1$ and $\mathcal{L}_2$, it is now easy to verify that $|\mathcal{L}_1 A' + \mathcal{L}_2 A'| = |\mathcal{L}_1 A + \mathcal{L}_2 A|$. Therefore, since the conclusion of the theorem is known for all $A' \subset \mathbb{Z}^d$, it is also true for all $A \subset \mathbb{R}^d$.

Chapter 4

SUMS OF TRANSCENDENTAL DILATES

Parts of this chapter are based on the author's publications. The materials have been adapted for inclusion in this thesis.

[1] D. Conlon and J. Lim, Sums of transcendental dilates, *Bulletin of the London Mathematical Society* **55** (2023), no. 5, 2400–2406, DOI: 10.1112/blms.12870.

Our interest here will be in estimating the minimum size $A + \lambda \cdot A$ given $|A|$, for a transcendental $\lambda \in \mathbb{C}$ and subset $A \subset \mathbb{C}$.

Let us first recall what happens when λ is not transcendental. When λ is rational, say $\lambda = p/q$ with p and q coprime, a result of Bukh [8] implies that

$$|A + \lambda \cdot A| \geq (|p| + |q|)|A| - o(|A|),$$

which is best possible up to the lower-order term (though see [2] for an improvement of the lower-order term to a constant depending only on λ). Moreover, as noted by Krachun and Petrov [28], for any fixed algebraic number λ, the minimum size of $|A + \lambda \cdot A|$ is always at most linear in $|A|$. We postpone further discussion of the algebraic case to Chapter 6.

For λ transcendental, the picture is very different. Indeed, Konyagin and Łaba [27] showed that in this case there exists an absolute constant $c > 0$ such that

$$|A + \lambda \cdot A| \geq c\frac{\log |A|}{\log \log |A|}|A|.$$

That is, $|A + \lambda \cdot A|$ can no longer be linear in $|A|$. This result was subsequently improved by Sanders [39], by Schoen [41] and again by Sanders [40] using successive quantitative refinements of Freiman's theorem [17] on sets of small doubling, with Sanders' second bound saying that there exists an absolute constant $c > 0$ such that, for $|A|$ sufficiently large,

$$|A + \lambda \cdot A| \geq e^{\log^c |A|}|A|.$$

This already comes quite close to matching the best known upper bound, due to Konyagin and Łaba [27], which says that there exists $c' > 0$ and, for any fixed transcendental number λ, arbitrarily large finite subsets A of $\mathbb{R}$ such that

$$|A + \lambda \cdot A| \leq e^{c'\sqrt{\log |A|}}|A|.$$

Our main result this chapter says that this upper bound is in fact best possible up to the constant c'.

Theorem 4.0.1. *There is an absolute constant $c > 0$ such that*

$$|A + \lambda \cdot A| \geq e^{c\sqrt{\log |A|}}|A|$$

for any finite subset A of $\mathbb{R}$ and any transcendental number $\lambda \in \mathbb{R}$.

Before proceeding to the proof of this theorem, let us briefly look at the upper bound, which comes from considering sets of the form

$$A = \left\{ \sum_{i=1}^{m} a_i \lambda^i : (a_1, \ldots, a_m) \in [n]^m \right\}.$$

This set has size n^m and

$$A + \lambda \cdot A \subset \left\{ \sum_{i=1}^{m+1} b_i \lambda^i : (b_1, \ldots, b_{m+1}) \in [2n]^{m+1} \right\},$$

which has size $(2n)^{m+1}$. If we take $n = 2^m$, we have $|A| = n^m = 2^{m^2}$, so that

$$|A + \lambda \cdot A| \leq (2n)^{m+1} = 2^{(m+1)^2} \leq e^{c'\sqrt{\log |A|}}|A|$$

for some $c' > 0$, as required. This bound is reminiscent, both in its form and its proof, of Behrend's lower bound [4] for the largest subset of $[n]$ containing no three-term arithmetic progressions. Our Theorem 4.0.1 is arguably the first example where such a bound is known to be tight to this level of accuracy.

4.1 Proof of Theorem 4.0.1

To begin, we use a simple observation of Krachun and Petrov to recast the problem.

Lemma 4.1.1 (Krachun–Petrov [28])**.** *Suppose that $\lambda \in \mathbb{C}$ and A is a finite subset of $\mathbb{C}$. Then there exists $B \subset \mathbb{Q}[\lambda]$ such that $|B| = |A|$ and $|B + \lambda \cdot B| \leq |A + \lambda \cdot A|$.*

Suppose now that V is the $\mathbb{Q}$-vector space $\mathbb{Q}[\lambda]$ with basis $\{1, \lambda, \lambda^2, \ldots\}$. For any positive integer d, let $V_d \subset V$ be the d-dimensional subspace spanned by $\{1, \lambda, \lambda^2, \ldots, \lambda^{d-1}\}$, noting that $V = \bigcup_d V_d$. For any finite $A \subset V$, we must have

$A \subset V_d$ for some d. Multiplication by λ therefore corresponds to taking the linear map $\Phi : V \to V$ given by the union of the maps $V_d \to V_{d+1}$ with

$$(x_1, \dots, x_d) \mapsto (0, x_1, \dots, x_d).$$

Thus, the problem of estimating $|A + \lambda \cdot A|$ for finite $A \subset \mathbb{R}$ and λ transcendental is equivalent to estimating $|A + \Phi(A)|$ for finite $A \subset V$. In particular, we may reformulate Theorem 4.0.1 in the following terms.

Theorem 4.1.2. *There is an absolute constant $c > 0$ such that if $A \subset V$ with $|A| = n$, then*

$$|A + \Phi(A)| \geq e^{c\sqrt{\log n}} n.$$

We will focus on proving this latter result from here on.

Before getting to the proof proper, we first note a few additional results that we will need. The first is a discrete variant of the Brunn–Minkowski theorem taken from Chapter 3. In what follows, for each $I \subseteq [d]$, we write $p_I : \mathbb{R}^d \to \mathbb{R}^d$ for the projection onto the coordinates indexed by I, setting all other coordinates to 0. Note that we may naturally extend the definition of p_I to V_d, and hence to V, by identifying V_d with $\mathbb{Q}^d$.

Lemma 4.1.3 (also Lemma 3.1.1)**.** *For any finite subsets A, B of $\mathbb{R}^d$,*

$$\sum_{I \subseteq [d]} |p_I(A + B)| \geq (|A|^{1/d} + |B|^{1/d})^d.$$

For our next result, we need the following estimate of Ruzsa [37] for the size of sumsets in $\mathbb{R}^d$. We say that a subset C of $\mathbb{R}^d$ is k-dimensional and write $\dim(C) = k$ if the dimension of the affine subspace spanned by C is k.

Lemma 4.1.4 (Ruzsa [37])**.** *If $A, B \subset \mathbb{R}^d$, $|A| \geq |B|$ and $\dim(A + B) = d$, then*

$$|A + B| \geq |A| + d|B| - \frac{d(d+1)}{2}.$$

For $a \in V$, write $p_k(a)$ for the vector obtained by removing the k-th coordinate from a. For $A \subset V$ and $x \in p_k(A)$, let $A_x = p_k^{-1}(x)$. We define the compression $C_k(A)$ of A along the k-th coordinate to be the set A' such that $p_k(A') = p_k(A)$ and, for each $x \in p_k(A)$, the k-th coordinates of A'_x are $0, 1, \dots, |A_x| - 1$. It is known (see, for example, Lemma 3.1.1 in Chapter 3) that $|C_k(A) + C_k(B)| \leq |A + B|$ for any

finite $A, B \subset V$. We say that A is compressed if $C_k(A) = A$ for all k. A compressed set $A \subset V_d$ has the property that if $(a_1, \dots, a_d) \in A$ and $b_i \in \mathbb{Z}$ with $0 \leq b_i \leq a_i$ for all $1 \leq i \leq d$, then $(b_1, \dots, b_d) \in A$. The next lemma will allow us to assume that A is both compressed and of low dimension when proving our main result.

Lemma 4.1.5. *Suppose that $A \subset V$ is finite with $|A + \Phi(A)| = K|A|$. Then there is some $d \leq 2K$ and $A' \subset V_d$ with $|A'| = |A|$ such that A' is compressed and $|A' + \Phi(A')| \leq |A + \Phi(A)|$.*

Proof. Since A is finite, $A \subset V_D$ for some D. Note that $\Phi \circ C_i = C_{i+1} \circ \Phi$ for all i. Denote by $C_{[i]}$ the composition $C_1 \circ C_2 \circ \cdots \circ C_i$. Then $C_{[D+1]}(A) = C_{[D]}(A)$ and $C_{[D+1]}(\Phi(A)) = \Phi(C_{[D]}(A))$. Thus, setting $A_1 = C_{[D]}(A)$, we have $|A_1| = |A|$ and

$$\begin{aligned} |A_1 + \Phi(A_1)| &= |C_{[D]}(A) + \Phi(C_{[D]}(A))| \\ &= |C_{[D+1]}(A) + C_{[D+1]}(\Phi(A))| \leq |A + \Phi(A)|. \end{aligned}$$

Furthermore, A_1 is compressed.

Let $e_k = \lambda^{k-1}$ be the basis vectors for $k = 1, \dots, D$. If $e_k \notin A_1$, then the k-th coordinate of every point of A_1 is 0. Let A_1' be the set formed by replacing each point $(x_1, \dots, x_{k-1}, 0, x_k, \dots, x_{D-1})$ of A_1 with the point $(x_1, \dots, x_{k-1}, x_k, \dots, x_{D-1})$, so that $A_1' \subset V_{D-1}$. We claim that $|A_1' + \Phi(A_1')| \leq |A_1 + \Phi(A_1)|$. Indeed, every point of $A_1 + \Phi(A_1)$ is of the form

$$(x_1, x_2 + y_1, x_3 + y_2, \dots, x_{k-1} + y_{k-2}, y_{k-1}, x_k, x_{k+1} + y_k, \dots, x_{D-1} + y_{D-2}, y_{D-1})$$

for some $(x_1, \dots, x_{k-1}, 0, x_k, \dots, x_{D-1}), (y_1, \dots, y_{k-1}, 0, y_k, \dots, y_{D-1}) \in A_1$, whereas every point of $A_1' + \Phi(A_1')$ is of the form

$$(x_1, x_2 + y_1, x_3 + y_2, \dots, x_{D-1} + y_{D-2}, y_{D-1}).$$

There is a clear surjection from $A_1 + \Phi(A_1)$ to $A_1' + \Phi(A_1')$ by summing and combining the k-th and $(k+1)$-th coordinates.

Repeating the above procedure whenever possible for each k, we obtain a set A' with $|A'| = |A|$, $|A' + \Phi(A')| \leq |A + \Phi(A)|$ and $A' \subset V_d$ for some d with $e_k \in A'$ for $k = 1, \dots, d$. By this last condition, A' is d-dimensional and, moreover, $A' + \Phi(A')$ is $(d+1)$-dimensional. Hence, by Lemma 4.1.4, we have $|A' + \Phi(A')| \geq (d+2)|A'| - \frac{(d+1)(d+2)}{2}$. Using that $|A' + \Phi(A')| \leq K|A'|$ and $|A'| \geq d + 1$, we get $d \leq 2K$, as required. □

We also note the following result of Plünnecke–Ruzsa type.

Lemma 4.1.6. *Suppose $A \subset V$ is finite. If $|A+\Phi(A)| \leq K|A|$ for some $K > 0$, then $|(A+\Phi(A))+\Phi(A+\Phi(A))| \leq K^{10}|A|$.*

Proof. By the sum version of Ruzsa's triangle inequality (Lemma 1.6.1), setting $X = \Phi(A)$, $Y = Z = A$ and noting that $|\Phi(A)| = |A|$, we have

$$|\Phi(A)||A+A| \leq |A+\Phi(A)||A+\Phi(A)|,$$

so that $|A+A| \leq K^2|A|$. Hence, by the Plünnecke–Ruzsa inequality (Lemma 1.6.2), $|A+A+A+A| \leq K^8|A|$. Thus, another application of Ruzsa's triangle inequality (with $X = \Phi(A)$, $Y = A$, $Z = \Phi(A)+\Phi(A)+\Phi(A)$) yields

$$|\Phi(A)||A+\Phi(A)+\Phi(A)+\Phi(A)| \leq |A+\Phi(A)||\Phi(A)+\Phi(A)+\Phi(A)+\Phi(A)|,$$

so that $|A+\Phi(A)+\Phi(A)+\Phi(A)| \leq K^9|A|$. Applying Ruzsa's triangle inequality once more (with $X = \Phi(A)$, $Y = A+\Phi(A)+\Phi(A)$, $Z = \Phi^2(A)$), we see that

$$|\Phi(A)||A+\Phi(A)+\Phi(A)+\Phi^2(A)| \leq |A+\Phi(A)+\Phi(A)+\Phi(A)||\Phi(A)+\Phi^2(A)|,$$

so that $|A+\Phi(A)+\Phi(A)+\Phi^2(A)| \leq K^{10}|A|$, as required. □

We now come to the main novel ingredient in our proof, which is a strong upper bound for the size of the projections of any compressed $A \subset V_d$ in terms of $|A+\Phi(A)|$. Given a set $I \subseteq [d]$, we will write $\alpha(I)$ for the length of the longest set of consecutive integers in I.

Lemma 4.1.7. *Let $A \subset V_d$ be finite and compressed with $|A+\Phi(A)| = N$. Then, for any subset $I \subseteq [d]$,*

$$|p_I(A)| \leq N^{\frac{k}{k+1}},$$

where $k = \alpha(I)$.

Proof. For any set of integers J, define $\phi(J) = \{j+1 : j \in J\}$. We claim that, for any $J_1, J_2 \subset [d]$,

$$\frac{|p_{J_1}(A)||p_{J_2}(A)|}{|p_{J_1\cap\phi(J_2)}(A)|} \leq N.$$

To show this, we will exhibit an injection $p_{J_1}(A) \times p_{J_2}(A) \to p_{J_1\cap\phi(J_2)}(A) \times (A+\Phi(A))$. Let $(x,y) \in p_{J_1}(A) \times p_{J_2}(A)$ and consider the map

$$(x,y) \mapsto (p_{J_1\cap\phi(J_2)}(x), x+\Phi(y)).$$

Since A is compressed, $p_J(A) \subseteq A$ for every J, which easily implies that $(p_{J_1\cap\phi(J_2)}(x), x+\Phi(y))$ is indeed in $p_{J_1\cap\phi(J_2)}(A) \times (A + \Phi(A))$. To see that the map is injective, it is enough to observe that

$$x = p_{J_1\cap\phi(J_2)}(x) + p_{J_1\setminus\phi(J_2)}(x) = p_{J_1\cap\phi(J_2)}(x) + p_{J_1\setminus\phi(J_2)}(x + \Phi(y))$$

and

$$\Phi(y) = p_{\phi(J_2)}(\Phi(y)) = p_{\phi(J_2)}(x+\Phi(y)) - p_{\phi(J_2)}(x) = p_{\phi(J_2)}(x+\Phi(y)) - p_{J_1\cap\phi(J_2)}(x).$$

For $i = 0, 1, \ldots, k$, let

$$I_i = \{j \in I : \{j, j-1, \ldots, j-i\} \subseteq I\}.$$

Then $I = I_0 \supset I_1 \supset \cdots \supset I_k = \emptyset$ and, for each $i = 0, 1, \ldots, k-1$, $I \cap \phi(I_i) = I_{i+1}$. Thus, by the claim above,

$$\frac{|p_I(A)||p_{I_i}(A)|}{|p_{I_{i+1}}(A)|} \leq N.$$

Taking the product of this inequality over all $i = 0, 1 \ldots, k-1$, we get

$$|p_I(A)|^{k+1} \leq N^k$$

and the lemma follows. □

We are now ready to prove our main result.

Proof of Theorem 4.1.2. Suppose instead that $|A+\Phi(A)| = Kn$, where $K < e^{c\sqrt{\log n}}$ for some $c > 0$ that will be fixed later. By Lemma 4.1.5, we may assume that A is compressed and $A \subset V_d$ with $d \leq 2K$.

By Lemma 4.1.6, we have

$$|A + \Phi(A) + \Phi(A + \Phi(A))| \leq K^{10}n.$$

Since A is compressed, so are $\Phi(A)$ and, therefore, $A + \Phi(A)$. Hence, Lemma 4.1.7 implies that

$$|p_I(A + \Phi(A))| \leq (K^{10}n)^{\frac{k}{k+1}}$$

for any $I \subseteq [d+1]$, where $k = \alpha(I)$. But the number of $I \subseteq [d+1]$ with $\alpha(I) = k$ is at most

$$\sum_{i=1}^{d+2-k} |\{I \subseteq [d+1] : i, i+1, \ldots, i+k-1 \in I\}| \leq (d+2)2^{d+1-k}.$$

Thus, by Lemma 4.1.3, we have that

$$\begin{aligned} 2^{d+1}n &\leq \sum_{I\subseteq[d+1]} |p_I(A+\Phi(A))| \leq \sum_{k=0}^{d+1} |\{I \subseteq [d+1] : \alpha(I) = k\}|\, (K^{10}n)^{\frac{k}{k+1}} \\ &\leq \sum_{k=0}^{d+1} (d+2)2^{d+1-k}(K^{10}n)^{\frac{k}{k+1}}. \end{aligned}$$

Therefore,

$$\begin{aligned} 1 &\leq \sum_{k=0}^{d+1} (d+2)2^{-k}K^{\frac{10k}{k+1}}n^{-\frac{1}{k+1}} \leq 2(d+2)\sum_{k=0}^{d+1} 2^{-k-1}K^{10}n^{-\frac{1}{k+1}} \\ &\leq 2(d+2)\sum_{k=0}^{d+1} e^{-(k+1)\log 2 + 10c\sqrt{\log n} - \frac{\log n}{k+1}} \\ &\leq 2(d+2)\sum_{k=0}^{d+1} e^{-2\sqrt{(\log 2)\log n} + 10c\sqrt{\log n}} \\ &\qquad \left(\text{using } (k+1)\log 2 + \frac{\log n}{k+1} \geq 2\sqrt{(\log 2)\log n}\right) \\ &= 2(d+2)^2 e^{(10c-2\sqrt{\log 2})\sqrt{\log n}} \leq e^{(13c-2\sqrt{\log 2})\sqrt{\log n}}, \end{aligned}$$

which is a contradiction for $c = 0.1$ and n sufficiently large. For smaller n, we may use the trivial estimate $|A+\Phi(A)| \geq 2|A| - 1$ to choose an appropriate c that works for all n. □

As a final remark, we note that the conclusion of Theorem 4.0.1 also holds for any finite subset A of $\mathbb{C}$ and any transcendental $\lambda \in \mathbb{C}$. Indeed, Lemma 4.1.1 again reduces the problem to estimating $|A + \lambda \cdot A|$ for finite $A \subset \mathbb{Q}[\lambda]$ and then to estimating $|A+\Phi(A)|$ for finite $A \subset V$, so the rest of the proof goes through without change.

Chapter 5

STRUCTURE THEOREM FOR SUMS OF DILATES

Parts of this chapter are based on the author's publications. The materials have been adapted for inclusion in this thesis.

[1] D. Conlon and J. Lim, Sums of algebraic dilates, *in preparation*.

A fundamental result in additive combinatorics is Freiman's structure theorem. Recall that a *generalized arithmetic progression* (or *GAP* for short) is a set P of the form

$$P = \{v_0 + a_1 v_1 + \cdots + a_d v_d : 0 \leq a_i < L_1 \text{ for all } i\}, \tag{5.1}$$

for some integers $v_0, v_1, \ldots, v_d, L_1, \ldots, L_d$, where d is the dimension of the GAP P. We say that P is *proper* if the terms in (5.1) are distinct. Freiman's theorem can then be stated as:

Theorem 5.0.1 (Freiman [17])**.** *Let $K > 0$. Then there exist $d, F > 0$ depending only on K such that the following holds. If $A \subset \mathbb{Z}$ satisfies $|A + A| \leq K|A|$, then A is contained in a proper GAP of dimension at most d and size at most $F|A|$.*

In this chapter, we prove an analogous version of Freiman's theorem for sets with small sums of algebraic dilates. Let $\lambda_1, \ldots, \lambda_k$ be algebraic integers and $K = \mathbb{Q}(\lambda_1, \ldots, \lambda_k)$. Denote by O_K the ring of algebraic integers in K. Our main result is as follows, which is a crucial ingredient in our proof of Theorem 1.4.5 in Chapter 6.

Theorem 5.0.2. *Let $C, p > 0$. Then there are constants $n = n(C, p)$ and $F = F(C, p)$ such that for any $A \subset O_K$ satisfying*

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq C|A|,$$

there exists a p-proper O_K-GAP $P \subset O_K$ containing A of dimension at most n and size at most $F|A|$.

We will define O_K-GAPs in Section 5.4. This result is qualitatively best possible, in the sense that any O_K-GAP has small sums of dilates.

In order to prove this result, we extend several results from additive geometry, a term we borrow from Tao and Vu [48, Chapter 3], to rings of integers, culminating in the version of Freiman's theorem for sums of dilates mentioned in the introduction. Along the way, we prove several results that may be of independent interest, including versions of Minkowski's second theorem and John's theorem for lattices over rings of integers.

5.1 Notation

Throughout this chapter, we will use the following notation:

- $\lambda_0, \lambda_1, \ldots, \lambda_k$ are algebraic numbers with $\lambda_0 = 1$.
- $K := \mathbb{Q}(\lambda_1, \ldots, \lambda_k)$ is the number field generated by $\lambda_1, \ldots, \lambda_k$.
- The degree of K over $\mathbb{Q}$ is $d := \deg(K/\mathbb{Q})$, so $K \cong \mathbb{Q}^d$.
- The ring of integers over K is denoted O_K, so $O_K \cong \mathbb{Z}^d$.
- We write $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R} = O_K \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^d$ and $K_{\mathbb{C}} := K \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}^d$.
- A convex body in $\mathbb{R}^n$ is assumed to be convex, open, non-empty and bounded.
- We will generally use i to index $1, \ldots, d$, j to index $1, \ldots, n$ and l to index $1, \ldots, k$ (possibly starting at 0). However, this is not strict and the usage can depend on context.

5.2 A norm on O_K and $K_{\mathbb{R}}$

In this section, we define a norm on O_K and $K_{\mathbb{R}}$ and note some of its basic properties (this is not to be confused with the field norm $N_{K/\mathbb{Q}}(\cdot)$ on K, which we also use).

Fix a $\mathbb{Z}$-basis $e_1, \ldots, e_d$ of O_K, and define the isomorphism $\Phi : O_K \to \mathbb{Z}^d$ given by sending a basis $e_1, \ldots, e_d$ of O_K to the standard basis of $\mathbb{Z}^d$. By pulling back Φ, the ∞-norm on $\mathbb{Z}^d$ defines a norm $\|\cdot\|$ on O_K, namely, for $l_1, \ldots, l_d \in \mathbb{Z}$,

$$\|l_1 e_1 + \cdots + l_d e_d\| := \max_i |l_i|.$$

The open ball $B(L)$ of radius $L > 0$ under this norm is then given by

$$B(L) := \{l_1 e_1 + \cdots + l_d e_d \in O_K : |l_i| < L \text{ for all } i\}.$$

$\|\cdot\|$ extends linearly and continuously to a norm on $K_{\mathbb{R}}$, which we also denote by $\|\cdot\|$. The open ball $B_{\mathbb{R}}(R)$ of radius $R > 0$ in $K_{\mathbb{R}}$ is then

$$B_{\mathbb{R}}(R) := \{e_1 \otimes r_1 + \cdots + e_d \otimes r_d \in K_{\mathbb{R}} : |r_i| < R \text{ for all } i\}.$$

The following lemma may be seen as defining some constants associated to the norm $\|\cdot\|$.

Lemma 5.2.1. *There exist constants $C_1, C_2, C_3 \in \mathbb{N}$ such that the following hold:*

1. *For all $x, y \in K_{\mathbb{R}}$, $\|xy\| \leq C_1 \|x\| \|y\|$.*
2. *For all $l = 0, \ldots, k$, $C_2\lambda_l \in \mathcal{O}_K$.*
3. *For all $l = 0, \ldots, k$ and $x \in \mathcal{O}_K$, $\lambda_l x \in \frac{1}{C_2} \cdot B(C_3 \|x\|)$.*

Proof. 1. Let $M > 0$ be the maximum of $\left\|e_i e_j\right\|$ over all pairs $i, j \in [d]$. Now, for any $x = e_1 \otimes x_1 + \cdots + e_d \otimes x_d$ and $y = e_1 \otimes y_1 + \cdots + e_d \otimes y_d$ with $x_i, y_i \in \mathbb{R}$, we have $|x_i| \leq \|x\|$ and $|y_i| \leq \|y\|$. Therefore,

$$\begin{aligned}\|xy\| = \|\sum_{i,j} e_i e_j \otimes x_i y_i\| &\leq \sum_{i,j} \left\|e_i e_j \otimes x_i y_i\right\| \\ &= \sum_{i,j} \left\|e_i e_j\right\| |x_i y_i| \leq d^2 M \|x\| \|y\|,\end{aligned}$$

so we may pick $C_1 = d^2 M$.

2. Since $\mathcal{O}_K$ is of full rank, for any $\lambda \in K$, there is some integer $C > 0$ such that $C\lambda \in \mathcal{O}_K$. Thus, we may pick C_2 to be the lowest common multiple of the C's corresponding to each λ_l.

3. Pick an integer C_3 such that $C_3 > C_1 C_2 \max_l \|\lambda_l\|$. Then we have $C_2\lambda_l x \in \mathcal{O}_K$ and $\|C_2\lambda_l x\| \leq C_1 C_2 \|\lambda_l\| \|x\| < C_3 \|x\|$. Therefore, $\lambda_l x \in \frac{1}{C_2} \cdot B(C_3 \|x\|)$.

□

Throughout the rest of this chapter and the next, we will use the constants C_1, C_2, C_3 as given by this lemma.

5.3 An algebraic Minkowski's second theorem

In this section, we prove a variant of Minkowski's second theorem for lattices over rings of integers. Before we state this result, let us recall the original theorem of Minkowski. We first need a definition, noting that here a *convex body* is assumed to be convex, open, non-empty and bounded.

Definition 5.3.1. Let $\Gamma \subset \mathbb{R}^n$ be a lattice of rank m and $B \subset \mathbb{R}^n$ a convex body containing 0. We define the *successive minima* $\ell_j = \ell_j(B, \Gamma)$ of B with respect to Γ by

$$\ell_j := \inf \{\ell > 0 : \ell \cdot B \text{ contains } j \text{ linearly independent elements of } \Gamma\}$$

for each $1 \leq j \leq m$. Note that $0 < \ell_1 \leq \cdots \leq \ell_m < \infty$.

Minkowski's second theorem (see, for example, [48, Theorem 3.30]) is then as follows.

Theorem 5.3.2 (Minkowski's second theorem)**.** *Let $\Gamma \subset \mathbb{R}^n$ be a lattice of full rank and let B be a centrally symmetric convex body in $\mathbb{R}^n$ with successive minima $0 < \ell_1 \leq \cdots \leq \ell_n$. Then there exist n linearly independent vectors $v_1, \ldots, v_n \in \Gamma$ with the following properties:*

- *for each $1 \leq j \leq n$, v_j lies in the boundary of $\ell_j \cdot B$, but $\ell_j \cdot B$ itself does not contain any vectors in Γ outside the span of $v_1, \ldots, v_{j-1}$;*
- *the octahedron with vertices $\pm v_j$ for $1 \leq j \leq n$ contains no elements of Γ in its interior other than the origin;*
- *one has*
$$\frac{2^n[\Gamma : \langle v_1, \ldots, v_n\rangle_{\mathbb{Z}}]}{n!} \leq \frac{\ell_1 \cdots \ell_n \operatorname{Vol}(B)}{\operatorname{Vol}(\mathbb{R}^n/\Gamma)} \leq 2^n.$$

To state our variant of this theorem, we need to first clarify what we mean by a lattice over a ring of integers.

Definition 5.3.3. An *O_K-lattice* is a lattice Γ in $K^n \cong \mathbb{Q}^{dn}$ that is closed under multiplication by O_K. That is, for any $v \in \Gamma$ and $a \in O_K$, $av \in \Gamma$. Equivalently, Γ is a discrete O_K-submodule of K^n. Observe that $\mathbb{Q} \cdot \Gamma = K \cdot \Gamma$ is a K-subspace of K^n. The *O_K-rank* of Γ is the dimension m of this subspace.

Note that, when viewed as an ordinary lattice, the rank of Γ is md.

For the next definition, we recall, from Section 5.2, that we view O_K as having a fixed $\mathbb{Z}$-basis $e_1, \ldots, e_d$.

Definition 5.3.4. For a real number $r \geq 1$, a subset $B \subseteq K_{\mathbb{R}}^n$ is said to be *r-thick* if $e_i \cdot B \subseteq r \cdot B$ for all $i \in [d]$.

For example, by Lemma 5.2.1, $\|e_i x\| \leq C_1 \|e_i\| \|x\| = C_1 \|x\|$ for all $x \in K_{\mathbb{R}}$, so that $B_{\mathbb{R}}(L)$ is C_1-thick for any $L > 0$.

We now redefine successive minima, but with respect to $\mathcal{O}_K$-lattices.

Definition 5.3.5. Let Γ be an $\mathcal{O}_K$-lattice of $\mathcal{O}_K$-rank m and B a convex body in $K_{\mathbb{R}}^n$ containing 0. We define the *successive minima* $\ell_j = \ell_j(B, \Gamma)$ of B with respect to Γ by

$$\ell_j := \inf \{\ell > 0 : \ell \cdot B \text{ contains } j \text{ } K\text{-linearly independent elements of } \Gamma\}$$

for each $1 \leq j \leq m$. Note that we again have $0 < \ell_1 \leq \cdots \leq \ell_m < \infty$, since Γ has $\mathcal{O}_K$-rank m and so contains m K-linearly independent elements of K^n.

We may now state and prove our version of Minkowski's second theorem for $\mathcal{O}_K$-lattices.

Lemma 5.3.6. *Let $r \geq 1$ be a real number, let $\Gamma \subset K^n$ be an $\mathcal{O}_K$-lattice of full rank and let B be an r-thick centrally symmetric convex body in $K_{\mathbb{R}}^n$ with successive minima $0 < \ell_1 \leq \cdots \leq \ell_n$. Then there exist n K-linearly independent vectors $v_1, \ldots, v_n \in \Gamma$ with the following properties:*

- *for each $1 \leq j \leq n$, v_j lies on the boundary of $\ell_j \cdot B$, but $\ell_j \cdot B$ does not contain any vectors in Γ outside the K-span of $v_1, \ldots, v_{j-1}$;*
- *the octahedron with vertices $\pm \frac{1}{r} e_i v_j$ for $i \in [d]$, $j \in [n]$ contains no elements of Γ in its interior other than the origin;*
- *if Γ' is the $\mathcal{O}_K$-lattice generated by $v_1, \ldots, v_n$, then*

$$\frac{(2/r)^{nd}[\Gamma : \Gamma']}{(nd)!} \leq \frac{(\ell_1 \cdots \ell_n)^d \operatorname{Vol}(B)}{\operatorname{Vol}(K_{\mathbb{R}}^n/\Gamma)} \leq 2^{nd}. \tag{5.2}$$

We note that here the volume of a set $B \subset K_{\mathbb{R}}^n$ is defined by fixing some isomorphism $K_{\mathbb{R}}^n \cong \mathbb{R}^{nd}$ and using the standard Lebesgue measure on $\mathbb{R}^{nd}$. Crucially, the statement of the lemma does not depend on the particular identification $K_{\mathbb{R}}^n \cong \mathbb{R}^{nd}$, since any two volume forms differ by a scalar.

Proof of Lemma 5.3.6. The proof is essentially identical to that of the original theorem given in [48, Theorem 3.30], though some care is required to differentiate between the $\mathbb{Q}$-span and K-span.

By the definition of ℓ_1, we may find $v_1 \in \Gamma$ on the boundary of $\ell_1 \cdot B$, where $\ell_1 \cdot B$ does not contain any non-zero elements of Γ. By the definition of λ_2, we may then find $v_2 \in \Gamma$ on the boundary of $\ell_2 \cdot B$ which is K-linearly independent of v_1, where $\ell_2 \cdot B$ contains no elements of Γ outside the K-span of v_1. Continuing, we have a K-basis $v_1, \dots, v_n$ such that v_j is on the boundary of $\ell_j \cdot B$, where $\ell_j \cdot B$ does not contain any element of Γ other than then K-span of $v_1, \dots, v_{j-1}$, as required by the first property.

Since $v_1, \dots, v_n$ are K-linearly independent, the vectors $e_i v_j$ are $\mathbb{Q}$-linearly independent. Therefore, the octahedron S with vertices $\pm\frac{1}{r} e_i v_j$ is non-degenerate and spans K^n over $\mathbb{Q}$. Suppose the interior of S contains a non-zero point $v \in \Gamma$. Let m be the smallest positive integer such that v lies in the K-span of $v_1, \dots, v_m$. Then v does not lie in the K-span of $v_1, \dots, v_{m-1}$. Since $\ell_m \cdot \overline{B}$ contains $v_1, \dots, v_m$ and B is r-thick, $r\ell_m \cdot \overline{B}$ contains $e_i v_j$ for all $i \in [d]$ and $j \le m$. Therefore, $\ell_m \cdot \overline{B}$ contains $\frac{1}{r} e_i v_j$, so its interior $\ell_m \cdot B$ contains v. But this contradicts the definition of ℓ_m, since $\ell_m \cdot B$ cannot contain any vector outside the K-span of $v_1, \dots, v_{m-1}$, including v. Hence, the interior of S contains no vector in Γ, verifying the second property.

Since $e_i v_j \in r\ell_j \cdot \overline{B}$, we have that $\overline{B}$ contains the vectors $\frac{1}{r\ell_j} e_i v_j$ and, hence, the octahedron S' with vertices $\pm\frac{1}{r\ell_j} e_i v_j$. The volume of the simplex with vertices 0 and $e_i v_j$ for all i, j is $\frac{1}{(nd)!} \operatorname{Vol}(K^n_{\mathbb{R}}/\Gamma')$. Since S' is the union of 2^{nd} many such scaled simplices, the volume of S' is

$$\operatorname{Vol}(S') = \frac{1}{r^{nd} \ell_1^d \cdots \ell_n^d} \frac{2^{nd}}{(nd)!} \operatorname{Vol}(K^n_{\mathbb{R}}/\Gamma').$$

Therefore, since B contains S', we have

$$\begin{aligned} \operatorname{Vol}(B) \ge \operatorname{Vol}(S') &= \frac{1}{r^{nd} \ell_1^d \cdots \ell_n^d} \frac{2^{nd}}{(nd)!} \operatorname{Vol}(K^n_{\mathbb{R}}/\Gamma') \\ &= \left(\frac{(2/r)^n}{\ell_1 \cdots \ell_n} \right)^d \frac{[\Gamma : \Gamma']}{(nd)!} \operatorname{Vol}(K^n_{\mathbb{R}}/\Gamma), \end{aligned}$$

establishing the lower bound in (5.2).

For the upper bound, we require the following lemma.

Lemma 5.3.7 (Squeezing lemma [48, Lemma 3.31])**.** *Let S be a centrally symmetric convex body in $\mathbb{R}^n$, A be an open subset of S, V be a m-dimensional subspace of $\mathbb{R}^n$ and $0 < \theta \le 1$. Then there exists an open subset A' of S such that $\operatorname{Vol}(A') = \theta^m \operatorname{Vol}(A)$ and $(A' - A') \cap V \subseteq \theta \cdot (A - A) \cap V$.*

Let V_j be the $\mathbb{R}$-span of the K-span of $v_1, \ldots, v_j$, so that V_j is a jd-dimensional real subspace of $K_{\mathbb{R}}^n$. We apply the squeezing lemma iteratively, starting with $A_0 := \frac{\ell_n}{2} \cdot B$, to create open sets $A_1, \ldots, A_{n-1} \subseteq A_0$ such that

$$\mathrm{Vol}(A_j) = \left(\frac{\ell_j}{\ell_{j+1}}\right)^{jd} \mathrm{Vol}(A_{j-1})$$

and

$$(A_j - A_j) \cap V_j \subseteq \frac{\ell_j}{\ell_{j+1}} \cdot (A_{j-1} - A_{j-1}) \cap V_j$$

for $j = 1, \ldots, n-1$. Then $\mathrm{Vol}(A_{n-1}) = (\ell_1 \cdots \ell_n 2^{-n})^d \mathrm{Vol}(B)$ and one can show by induction that

$$(A_{n-1} - A_{n-1}) \cap V_j \subseteq \frac{\ell_j}{\ell_n} \cdot (A_{j-1} - A_{j-1}) \cap V_j.$$

On the other hand, $A_{j-1} \subseteq A_0 = \frac{\ell_n}{2} \cdot B$ and B is centrally symmetric, so $A_{j-1} - A_{j-1} \subseteq \ell_n \cdot B$. It follows that

$$(A_{n-1} - A_{n-1}) \cap V_j \subseteq \lambda_j \cdot B \cap V_j$$

for $j = 1, \ldots, n$. By the definition of successive minima, $\lambda_j \cdot B \cap V_j$ does not contain any point in Γ except for those in V_{j-1}. This implies that $A_{n-1} - A_{n-1}$ does not contain any point in Γ other than the origin. If $\mathrm{Vol}(A_{n-1}) > \mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma)$, then one can find a translate $A_{n-1} + t$ of A_{n-1} containing two distinct points of Γ. Thus, $A_{n-1} - A_{n-1}$ contains a non-zero point of Γ, a contradiction. Therefore, we have $\mathrm{Vol}(A_{n-1}) \leq \mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma)$. Hence, we have

$$(\ell_1 \cdots \ell_n 2^{-n})^d \mathrm{Vol}(B) \leq \mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma),$$

giving the upper bound in (5.2). □

5.4 O_K-GAPs and an algebraic John's theorem

Recall that a *generalized arithmetic progression (or GAP)* $P \subset \mathbb{Z}^d$ is a set of the form

$$P = \left\{v_0 + l_1 v_1 + \cdots + l_n v_n : 0 \leq l_j < L_j \text{ for all } j\right\}$$

for some $v_0, \ldots, v_n \in \mathbb{Z}^d$ and $L_1, \ldots, L_n \in \mathbb{N}$. The *dimension* of P is n. We say that P is *proper* if all elements on the RHS are distinct and k-proper if

$$\left\{l_1 v_1 + \cdots + l_n v_n : 0 \leq l_j < kL_j \text{ for all } j\right\}$$

has all elements distinct.

Our object of study in this section is the following algebraic analogue of a GAP which we call an $\mathcal{O}_K$-GAP.

Definition 5.4.1. An *$\mathcal{O}_K$-GAP* is a set $P \subset K$ of the form

$$P = \left\{ v_0 + l_1 v_1 + \cdots + l_n v_n : l_j \in B(L_j) \text{ for all } j \right\} \tag{5.3}$$

for some $v_0, \ldots, v_n \in K$ and $L_1, \ldots, L_n \in \mathbb{N}$. The *dimension* of P is n. For $p \in \mathbb{N}$, define

$$p \star P := \left\{ p v_0 + l_1 v_1 + \cdots + l_n v_n : l_j \in B(pL_j) \text{ for all } j \right\}. \tag{5.4}$$

We say that P is *proper* if all the elements on the RHS of (5.3) are distinct and *p-proper* if all the elements on the RHS of (5.4) are distinct. Note that $p \star P$ is similar, but, because $B(L_j)$ is an *open* ball, not exactly equal, to the p-fold sumset pP.

Lemma 5.4.2. *For any real number $r \geq 1$, there are integer constants $D_1, D_2 > 0$ such that the following holds. Let $\Gamma \subseteq K^n$ be an $\mathcal{O}_K$-lattice of full rank and $B \subset K^n_{\mathbb{R}}$ be an r-thick convex centrally symmetric body. Then there exist $v_1, \ldots, v_n \in K$ and positive integers $L_1, \ldots, L_n$ such that the $\mathcal{O}_K$-GAPs given by*

$$P_1 := \{ l_1 v_1 + \cdots + l_n v_n : l_i \in B(L_i) \text{ for all } i \},$$
$$P_2 := \{ l_1 v_1 + \cdots + l_n v_n : l_i \in B(D_1 L_i) \text{ for all } i \}$$

satisfy

$$P_1 \subseteq B \cap \Gamma \subseteq \frac{1}{D_2} \cdot P_2. \tag{5.5}$$

Unlike for the discrete John's theorem for ordinary lattices, the constant D_2 is necessary here. Indeed, if K has non-trivial ideal class group, then, for $\Gamma \subset \mathcal{O}_K$ a non-principal ideal, we cannot hope for a one-dimensional $\mathcal{O}_K$-GAP to span the same lattice as Γ, since any such $\mathcal{O}_K$-GAP is generated by a single element.

Proof of Lemma 5.4.2. The first ingredient we need is the classical John's theorem (see [26] or [48, Theorem 3.13]), which says that for a symmetric convex body $A \subset \mathbb{R}^d$, there exists an open centrally symmetric ellipsoid $E \subset \mathbb{R}^d$ such that $E \subseteq A \subseteq \sqrt{d} \cdot E$.

Applying John's theorem to $B \subset K^n_{\mathbb{R}} \cong \mathbb{R}^{dn}$, we obtain open centrally symmetric ellipsoid $E \subset K^n_{\mathbb{R}}$ such that $E \subseteq B \subseteq \sqrt{dn} \cdot E$. For any $x \in E$ and $i \in [d]$,

$e_i x \in e_i \cdot B \subseteq r \cdot B \subseteq r\sqrt{dn} \cdot E$, so E is r_1-thick with $r_1 := r\sqrt{dn}$. Define the norm $\|\cdot\|_E$ on $K_{\mathbb{R}}^n$ whose unit ball is E, that is,

$$\|x\|_E := \inf\{\ell > 0 : x \in \ell \cdot E\}.$$

Since E is r_1-thick, for any $\ell > 0$ and $x \in K_{\mathbb{R}}^n$, $x \in \ell \cdot E$ implies that $e_i x \in r_1 \ell \cdot E$. Therefore,

$$\|e_i x\|_E \leq r_1 \|x\|_E . \tag{5.6}$$

Since $|a_i| \leq \|l\|$ for any $l = a_1 e_1 + \cdots + a_d e_d \in \mathcal{O}_K$, we have that

$$\|lx\|_E \leq \sum_{i=1}^{d} \|a_i e_i x\|_E \leq dr_1 \|l\| \|x\|_E . \tag{5.7}$$

Let $v_1, \ldots, v_n \in K$ be as in Lemma 5.3.6, when applied to the centrally symmetric convex body E. For each j, let

$$L_j := \left\lceil \frac{1}{ndr_1 \|v_j\|_E} \right\rceil.$$

Then, for any $l_j \in B(L_j)$, $\|l_j\| \leq \frac{1}{ndr_1 \|v_j\|_E}$. Thus, by (5.7),

$$\|l_j v_j\|_E \leq dr_1 \|l_j\| \|v_j\|_E \leq \frac{1}{n}.$$

Therefore, for $l_j \in B(L_j)$,

$$\|l_1 v_1 + \cdots + l_n v_n\|_E \leq \sum_{j=1}^{n} \|l_j v_j\|_E \leq 1.$$

In other words, $P_1 \subseteq E \cap \Gamma \subseteq B \cap \Gamma$, giving the first inclusion in (5.5).

Let $\Gamma' \subseteq \Gamma$ be the $\mathcal{O}_K$-span of $v_1, \ldots, v_n$. Then, from Lemma 5.3.6, $[\Gamma : \Gamma'] \leq D := \lfloor r^{nd}(nd)! \rfloor$. As a finite abelian group, Γ/Γ' has order at most D, so every element has order dividing $D!$. Therefore, $D! \cdot \Gamma \subseteq \Gamma'$ or, equivalently, $\Gamma \subseteq \frac{1}{D!}\Gamma'$.

Since E is a centrally symmetric ellipsoid, the norm $\|\cdot\|_E$ arises from an inner product on $K_{\mathbb{R}}^n$. Define the volume form on $K_{\mathbb{R}}^n$ based on this inner product. Then $\mathrm{Vol}(E) = V_{nd}$, the volume of the unit ball in $\mathbb{R}^{nd}$. For $u_1, \ldots, u_{nd} \in K_{\mathbb{R}}^n$, write $u_1 \wedge \cdots \wedge u_{nd}$ for the parallelepiped in $K_{\mathbb{R}}^n$ spanned by $u_1, \ldots u_{nd}$. Then $\mathrm{Vol}(u_1 \wedge \cdots \wedge u_{nd}) \leq \|u_1\|_E \cdots \|u_{nd}\|_E$.

Let the successive minima of E with respect to Γ be $\ell_1, \dots, \ell_n$, so we have $\|v_j\|_E = \ell_j$. Let $x \in B \cap \Gamma \subseteq \sqrt{dn} \cdot E$, so that $\|x\|_E \leq \sqrt{dn}$. Since $x \in \Gamma \subseteq \frac{1}{D!}\Gamma'$, we can find unique integers l_{ij} for $i = 1, \dots, d$ and $j = 1, \dots, n$ such that

$$x = \frac{1}{D!}(l_{11}e_1v_1 + \cdots + l_{dn}e_dv_n).$$

Using Cramer's rule, we can solve for $|l_{ij}|$. This gives

$$\begin{aligned}
|l_{ij}| &= D!\frac{\mathrm{Vol}(e_1v_1 \wedge \cdots \wedge x \wedge \cdots \wedge e_dv_n)}{\mathrm{Vol}(e_1v_1 \wedge \cdots \wedge e_dv_n)} && \text{here, } x \text{ is in place of } e_iv_j \\
&= D!\frac{\mathrm{Vol}(e_1v_1 \wedge \cdots \wedge x \wedge \cdots \wedge e_dv_n)}{\mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma')} \\
&\leq D!\frac{\|x\|_E \prod_{(i',j')\neq(i,j)} \|e_{i'}v_{j'}\|_E}{\mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma')} \\
&\leq D!\frac{r_1^{nd-1}\|x\|_E \prod_{(i',j')\neq(i,j)} \|v_{j'}\|_E}{\mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma')} && \text{by (5.6)} \\
&= D!r_1^{nd-1}\frac{(\ell_1 \cdots \ell_n)^d \|x\|_E}{\ell_j \mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma')}.
\end{aligned}$$

From Lemma 5.3.6, we have

$$\mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma') \geq \mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma) \geq \left(\frac{\ell_1 \cdots \ell_n}{2^n}\right)^d \mathrm{Vol}(E) = \left(\frac{\ell_1 \cdots \ell_n}{2^n}\right)^d V_{nd}.$$

Therefore, using that $\|x\|_E \leq \sqrt{dn}$ and $L_j \geq \frac{1}{ndr_1\|v_j\|_E}$, we have

$$|l_{ij}| \leq \frac{D!r_1^{nd-1}2^{nd}\|x\|_E}{\ell_j V_{nd}} < \frac{D!r_1^{nd}2^{nd+1}nd\sqrt{nd}}{V_{nd}}L_j.$$

We obtain the second inclusion in (5.5) by setting $D_2 = D!$ and

$$D_1 = \left\lceil D!r_1^{nd}2^{nd+1}nd\sqrt{nd}/V_{nd} \right\rceil.$$

□

We now come to a key lemma, saying that if P is an O_K-GAP that is not p-proper, then there is an O_K-GAP of smaller dimension which contains and is not too much larger than P.

Lemma 5.4.3. *If P is an O_K-GAP of dimension n that is not p-proper, then there is an O_K-GAP Q of dimension $n-1$ containing P with $|Q| \ll_{n,p} |P|$.*

Proof. Assume that P is centered and of the form

$$P = \left\{ l_1 v_1 + \cdots + l_n v_n : l_j \in B(L_j) \right\}.$$

Since P is not p-proper, there exist $l_j, l_j' \in B(pL_j)$ such that $l_j \neq l_j'$ for some j and

$$l_1 v_1 + \cdots + l_n v_n = l_1' v_1 + \cdots + l_n' v_n.$$

Setting $a_j = l_j - l_j' \in B(2pL_j)$, we have that the a_j are not all 0 and $a_1 v_1 + \cdots + a_n v_n = 0$. We may assume without loss of generality that $a_n \neq 0$. Then we have the relation

$$v_n = -\frac{a_1 v_1}{a_n} - \cdots - \frac{a_{n-1} v_{n-1}}{a_n}. \tag{5.8}$$

Let $w = (-\frac{a_1}{a_n}, \ldots, -\frac{a_{n-1}}{a_n}) \in K^{n-1}$. Let $\Gamma := O_K^{n-1} + O_K \cdot w \subset K^{n-1}$. Then Γ is a discrete lattice which is invariant under multiplication by O_K and so is an O_K-lattice. Γ is also of full rank, since it contains O_K^{n-1}. Consider the homomorphism $f : \Gamma \to K$ given by

$$f((x_1, \ldots, x_{n-1}) + x_n w) := x_1 v_1 + \cdots + x_n v_n.$$

Then f is well-defined because of the relation (5.8). Note also that f is O_K-linear, that is, f is linear and $f(ax) = af(x)$ for any $a \in O_K, x \in \Gamma$. We may also extend f O_K-linearly to a K-linear map $f : K^{n-1} \to K$.

Let $B_0 \subset K_{\mathbb{R}}^{n-1}$ be the convex centrally symmetric body

$$B_0 := \left\{ (x_1, \ldots, x_{n-1}) \in K_{\mathbb{R}}^{n-1} : x_i \in B_{\mathbb{R}}(L_i) \right\}.$$

Let $B = B_0 + B_{\mathbb{R}}(L_n) \cdot w$, which is also a convex centrally symmetric body. Since B_0 and $B_{\mathbb{R}}(L_n) \cdot w$ are C_1-thick, so is B. Indeed, if $x \in B_0$ and $y \in B_{\mathbb{R}}(L_n) \cdot w$, then $e_i \cdot (x + y) = e_i \cdot x + e_i \cdot y \in C_1 \cdot B_0 + C_1 \cdot (B_{\mathbb{R}}(L_n) \cdot w) = C_1 \cdot (B_0 + B_{\mathbb{R}}(L_n) \cdot w)$.

Claim 5.4.4. *One has the inclusions*

$$P \subseteq f(B \cap \Gamma) \subseteq (2pC_1 + 1)P.$$

Proof. For the first inclusion, let $v = l_1 v_1 + \cdots + l_n v_n \in P$ with $l_j \in B(L_j)$. Then $v = f((l_1, \ldots, l_{n-1}) + l_n w)$ with $\left\| l_j \right\| < L_j$, so that $(l_1, \ldots, l_{n-1}) + l_n w \in B \cap \Gamma$.

For the second inclusion, let $(l_1, \ldots, l_{n-1}) + l_n w \in B \cap \Gamma$ with $l_j \in O_K$. Since $(l_1, \ldots, l_{n-1}) + l_n w \in B$, there exist $x_1, \ldots, x_n \in K_{\mathbb{R}}$ with $\left\| x_j \right\| < L_j$ such that

$(l_1, \dots, l_{n-1}) + l_n w = (x_1, \dots, x_{n-1}) + x_n w$. In other words, $l_j - \frac{a_j l_n}{a_n} = x_j - \frac{a_j x_n}{a_n}$ for $j = 1, \dots, n-1$. Let $z = \frac{l_n - x_n}{a_n} \in K_{\mathbb{R}}$, so we have

$$l_j - x_j = a_j z \tag{5.9}$$

for all $j = 1, \dots, n$. Let $x \in \mathcal{O}_K$ be the closest element to z according to the metric $\|\cdot\|$. Recall that this is the ∞-norm, so we have $\|x - z\| \leq 1$. Let $l'_j = l_j - a_j x \in \mathcal{O}_K$. Then $l_1 v_1 + \cdots + l_n v_n = l'_1 v_1 + \cdots + l'_n v_n$, so we have $f((l_1, \dots, l_{n-1}) + l_n w) = l'_1 v_1 + \cdots + l'_n v_n$. It suffices to show that $\left\|l'_j\right\| < (2pC_1 + 1)L_j$ for all j. Indeed, we have

$$\begin{aligned}
\left\|l'_j\right\| &= \left\|l_j - a_j x\right\| \\
&\leq \left\|l_j - a_j x - x_j\right\| + \left\|x_j\right\| \\
&< \left\|a_j(z - x)\right\| + L_j && \text{by (5.9)} \\
&\leq C_1 \left\|a_j\right\| \|z - x\| + L_j && \text{by Lemma 5.2.1} \\
&\leq (2pC_1 + 1)L_j,
\end{aligned}$$

as required. □

By Lemma 5.4.2, we can find constants $D_1, D_2 = O_n(1)$ and $\mathcal{O}_K$-GAPs P_1, P_2 of dimension $n-1$ such that $P_2 = D_1 \star P_1$ and $P_1 \subseteq B \cap \Gamma \subseteq \frac{1}{D_2} \cdot P_2$. In particular, P_2 can be covered by D_1^{n-1} translates of P_1.

Applying the homomorphism f, we obtain

$$f(P_1) \subseteq f(B \cap \Gamma) \subseteq \frac{1}{D_2} f(P_2).$$

Since f is $\mathcal{O}_K$-linear, $f(P_1)$ and $f(P_2)$ are also $\mathcal{O}_K$-GAPs of dimension $n-1$. Setting $Q = \frac{1}{D_2} f(P_2)$, which is an $\mathcal{O}_K$-GAP of dimension $n-1$, we have, by the claim above, that $P \subseteq f(B \cap \Gamma) \subseteq Q$, so it suffices to show that Q is small. Since P_2 can be covered by $D_1^{n-1} = O_n(1)$-many translates of P_1, $f(P_2)$ can also be covered by $O_n(1)$-many translates of $f(P_1)$. But then

$$|f(P_2)| \ll_n |f(P_1)| \leq |f(B \cap \Gamma)| \leq |(2pC_1 + 1)P| \ll_{n,p} |P|,$$

as required. □

5.5 Freiman's theorem for sums of dilates

We have now built up sufficient background to prove the promised Freiman-type structure theorem for sets with small sums of dilates, which we restate for the reader's convenience.

Theorem 5.5.1. *For every $C > 0$ and $p \in \mathbb{N}$, there are constants n and F such that for any $A \subset K$ satisfying*

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq C|A|,$$

there exists a p-proper O_K-GAP $P \subset K$ containing A of dimension at most n and size at most $F|A|$.

Recall, from Lemma 5.2.1, that we have constants $C_2, C_3 \in \mathbb{N}$ with the property that $\lambda_l x \in \frac{1}{C_2} \cdot B(C_3 \|x\|)$ for all $l = 0, \ldots, k$ and $x \in O_K$. Thus, if P is an O_K-GAP, then $\lambda_l \cdot P$ lies in a translate of $\frac{1}{C_2} \cdot (C_3 \star P)$. Therefore,

$$\begin{aligned} |P + \lambda_1 \cdot P + \cdots + \lambda_k \cdot P| &\leq |(k+1)C_3 \star P| \\ &\leq ((k+1)C_3)^{nd}|P|. \end{aligned}$$

In other words, P has a small sum of dilates. That is, Theorem 5.5.1 embeds a set A with a small sum of dilates into another, more structured set which, unlike an ordinary GAP, also has a small set of dilates. We now proceed to the proof of this statement.

Proof of Theorem 5.5.1. By translating, we may assume that $0 \in A$. By the Ruzsa triangle inequality,

$$|A + A||\lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq |A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A|^2 \leq C^2|A|^2.$$

Using the trivial bound $|\lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \geq |A|$, we obtain $|A + A| \leq C^2|A|$. By the Plünnecke–Ruzsa inequality, $|A + A + A| \leq C^6|A|$. By the Ruzsa triangle inequality again,

$$|(A + A) + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A||A| \leq |A + A + A||A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq C^7|A|^2,$$

so $|(A + A) + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq C^7|A|$. Similar repeated applications of the triangle inequality gives $|(A + A) + \lambda_1 \cdot (A + A) + \cdots + \lambda_k \cdot (A + A)| \leq C^{7+6k}|A|$. Thus, $A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A$ has small doubling constant. Therefore, by Freiman's theorem, $A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A$ is contained in a proper GAP

$$P_0 = \left\{ l_1 v_1 + \cdots + l_{n_0} v_{n_0} : -L_i < l_i < L_i \right\}$$

of dimension n_0 with $|P_0| \ll |A|$. Note that since $0 \in A \subseteq P_0$, we are free to assume that P_0 is centered.

Now let P_1 be the O_K-GAP given by

$$P_1 = \left\{ l_1 v_1 + \cdots + l_{n_0} v_{n_0} : l_i \in B(L_i) \right\}.$$

Then P_1 contains P_0. At first glance, it might seem that the size of P_1 could be as large as $|P_0|^d$. However, we now show that this is not the case.

Claim 5.5.2. $|P_1| \ll |P_0|$.

Proof. For a subset $X \subseteq K$ and $c > 0$, we say that X is (c, P_0)-*small* if X can be covered by c-many translates of P_0. For brevity, we will simply say that X is P_0-small if c is a bounded constant independent of X, P_0. Thus, if X, Y are P_0-small, so is their sumset $X + Y$. Indeed, if X, Y can be covered by x, y-many translates of P_0, respectively, then $X + Y$ can be covered by xy-many translates of $P_0 + P_0$, which itself can be covered by 2^{n_0}-many translates of P_0.

We shall show that for each $i \in [d]$, $j \in [n_0]$, the set $S_{ij} := \left\{ e_i v_j, 2e_i v_j, \ldots, L_j e_i v_j \right\}$ is P_0-small. Then we would have proved the claim, since $\left\{ -L_j e_i v_j, \ldots, L_j e_i v_j \right\}$ is P_0-small, P_1 is the sum of these sets, and there are only a bounded number of such sets.

Since $\lambda_1, \ldots, \lambda_k$ generate K, there exist (fixed) integers $b, a_1, \ldots, a_k$ with $b > 0$ such that $be_i = a_1\lambda_1 + \cdots + a_k\lambda_k$. It will suffice to show that the set $S := \left\{ be_i v_j, 2be_i v_j, \ldots, L_j be_i v_j \right\}$ is P_0-small, since S_{ij} can be covered by b translates of it. But then it suffices to show that $S'_l := \left\{ a_l \lambda_l v_j, 2a_l \lambda_l v_j, \ldots, L_j a_l \lambda_l v_j \right\}$ is P_0-small, since S is contained in $S'_1 + \cdots + S'_k$. But then, finally, it suffices to show that $S_l := \left\{ \lambda_l v_j, 2\lambda_l v_j, \ldots, L_j \lambda_l v_j \right\}$ is P_0-small for each l, since S'_l is covered by $|a_l|$-many translates of S_l.

Suppose $|P_0 + P_0| < c|A|$, where $c = O(1)$ is a positive integer. Let s be an arbitrary positive integer with $s < L_j/c$. Consider the sets

$$A, A + sv_j, A + 2sv_j, \ldots, A + csv_j.$$

All these sets have size $|A|$ and are contained in $P_0 + P_0$. But $|P_0 + P_0| < c|A|$, so two of these sets intersect, say $(A + msv_j) \cap (A + m'sv_j) \neq \emptyset$ for $0 \leq m < m' \leq c$. Thus, $(m' - m)sv_j \in A - A$. Therefore, $c!s\lambda_l v_j \in c!(\lambda_l \cdot A) - c!(\lambda_l \cdot A) \subseteq c!P_0 - c!P_0$. Since $1 \leq s < L_j/c$ was arbitrary, we have that the set

$$\left\{ c!\lambda_l v_j, 2c!\lambda_l v_j, \ldots, \left\lfloor L_j/c \right\rfloor c!\lambda_l v_j \right\} \subseteq c!P_0 - c!P_0$$

is P_0-small. Thus, the set $T := \left\{ c!\lambda_l v_j, 2c!\lambda_l v_j, \ldots, L_j c!\lambda_l v_j \right\}$ is P_0-small. Finally, S_l is P_0-small since it can be covered by $c!$-many translates of T. □

If P_1 is p-proper, then we are done. Otherwise, by Lemma 5.4.3, we can find an $\mathcal{O}_K$-GAP P_2 of one dimension smaller containing P_1 with $|P_2| \ll |P_1|$. If P_2 is also not p-proper, we invoke Lemma 5.4.3 again to obtain P_3 and so on. Note that we can only do this at most n_0 times, since any $\mathcal{O}_K$-GAP of dimension 1 is necessarily p-proper. Thus, we will eventually find a p-proper $\mathcal{O}_K$-GAP P containing A of dimension $O(1)$ with $|P| \ll |A|$. □

Chapter 6

SUMS OF ALGEBRAIC DILATES

Parts of this chapter are based on the author's publications. The materials have been adapted for inclusion in this thesis.

[1] D. Conlon and J. Lim, Sums of algebraic dilates, *in preparation*.

Our concern in this chapter will be with estimating the minimum size of $|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$ in terms of $|A|$. For $\lambda_1, \ldots, \lambda_k \in \mathbb{Q}$, this problem was essentially solved by Bukh [8], from whose results it follows that if $\lambda_i = p_i/q$ for q as small as possible for such a common denominator, then, for finite subsets A of $\mathbb{C}$,

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \geq (|p_1| + \cdots + |p_k| + |q|)|A| - o(|A|),$$

which is best possible up to the lower-order term. This result was later sharpened by Balog and Shakan [2] when $k = 2$ and then Shakan [42] in the general case, improving the $o(|A|)$ term to a constant depending only on $\lambda_1, \ldots, \lambda_k$.

When at least one of the λ_i is transcendental, it was shown by Konyagin and Łaba [27] that

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| = \omega(|A|).$$

The problem of giving more precise estimates for $|A+\lambda \cdot A|$ when λ is transcendental was discussed in Chapter 4.

Our focus here will be on the complementary case, where each of $\lambda_1, \ldots, \lambda_k$ is algebraic. Early results in this direction were proved by Breuillard and Green [7] and Chen and Fang [10], with the latter showing that, for any fixed $\lambda \geq 1$, $|A+\lambda \cdot A| \geq (1 + \lambda)|A| - o(|A|)$ for finite subsets A of $\mathbb{R}$. The problem of estimating $|A + \lambda \cdot A|$ for λ algebraic was raised explicitly by Shakan [42] and by Krachun and Petrov [28], with the latter authors conducting the first systematic study and making the first concrete conjectures.

To state their conjecture, suppose that $f(x) \in \mathbb{Z}[x]$ is the minimal polynomial of λ, assumed to have coprime coefficients, and $f(x) = \prod_{i=1}^{d}(a_i x + b)$ is a full complex factorization of f. If we set $H(\lambda) := \prod_{i=1}^{d}(|a_i| + |b_i|)$, the conjecture of Krachun and Petrov [28] is then as follows.

Conjecture 6.0.1. *For any algebraic number λ,*

$$|A + \lambda \cdot A| \geq H(\lambda)|A| - o(|A|)$$

for finite subsets A of $\mathbb{C}$.

Krachun and Petrov [28] gave some evidence for their conjecture by proving it in the special case where $\lambda = \sqrt{2}$. Subsequently, we verified the conjecture for all λ of the form $(p/q)^{1/d}$ with $p, q, d \in \mathbb{N}$, to be discussed in Chapter 7. Assuming all of p, q and d are as small as possible for such a representation, our results, which includes that of Krachun and Petrov, says that

$$|A + \lambda \cdot A| \geq (p^{1/d} + q^{1/d})^d |A| - o(|A|).$$

Our results also imply a general lower bound for sums of algebraic dilates, though this bound only matches the conjectured one in the cases above.

More recently, Krachun and Petrov [29] have revisited the problem, proving their conjecture in full whenever λ is an algebraic integer. This is somewhat incomparable to our previously mentioned result, since $(p/q)^{1/d}$, when written in lowest terms, is only an algebraic integer when $q = 1$. Here we again revisit the problem, proving Conjecture 6.0.1 in full for all algebraic numbers. Our method also extends to longer sums of algebraic dilates, so we will state our results in that level of generality.

To state the result, given a field extension $K := \mathbb{Q}(\lambda_1, \ldots, \lambda_k)$ of $\mathbb{Q}$ of degree $d = \deg(K/\mathbb{Q})$, we first recall that there are exactly d different complex embeddings $\sigma_1, \ldots, \sigma_d : K \to \mathbb{C}$. We also need to define the *denominator ideal*, which is the ideal in the ring of integers O_K given by

$$\mathfrak{D}_{\lambda_1,\ldots,\lambda_k;K} := \{\alpha \in O_K : \alpha\lambda_l \in O_K \text{ for } l = 1, \ldots, k\}.$$

The key quantity $H(\lambda_1, \ldots, \lambda_k)$ that plays the role of $H(\lambda)$ for sums of many algebraic dilates is then

$$H(\lambda_1, \ldots, \lambda_k) := N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda_1,\ldots,\lambda_k;K}) \prod_{i=1}^{d} (1 + |\sigma_i(\lambda_1)| + |\sigma_i(\lambda_2)| + \cdots + |\sigma_i(\lambda_k)|).$$

To see that this indeed generalizes $H(\lambda)$, observe that we can write the integer minimal polynomial $f(x) \in \mathbb{Z}[x]$ of λ as $f(x) = D(x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_d)$, for some integer D and $\lambda_1, \ldots, \lambda_d$ are all the conjugates of λ. Then, $H(\lambda) = |D|(1 + |\lambda_1|)\cdots(1 + |\lambda_d|)$ and it can be shown that $|D| = N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda;K})$. With this definition in place, our main result, which is best possible up to the behaviour of the lower-order terms, is as follows.

Theorem 6.0.2. *For any algebraic numbers $\lambda_1, \dots, \lambda_k$,*

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \geq H(\lambda_1, \dots, \lambda_k)|A| - o(|A|)$$

for finite subsets A of $\mathbb{C}$.

Sketch of proof

Our general strategy is similar to that of Krachun and Petrov [29], which can be summarized as the following three steps:

1. Reduction to the case when A is a dense subset of the box.
2. A continuous variant of sums of dilates.
3. A representation of the discrete set A by a continuous set $\overline{A}$.

Step 1 guarantees that the $\overline{A}$ obtained in step 3 is well-behaved. One then applies the continuous variant from step 2 on $\overline{A}$, and the corresponding result in the discrete world follows.

Despite having the same overall strategy, the methods used in steps 1 and 3 are significantly more complex.

In step 1, we use the Freiman-type structure theorem for sets A with small sum of dilates, proved in Chapter 5. Using this structure theorem, we can then map A to a dense subset of the box $[0, N)^d$ via a Freiman isomorphism of the surrounding $\mathcal{O}_K$-GAP, reducing the problem to the case of a dense set.

In step 2, our proof is similar to that of Krachun and Petrov, by partitioning space into eigenspaces, then symmetrizing our set along those eigenspaces.

Step 3 is the main and most difficult step. We first describe the method used by Krachun and Petrov [29] to prove the case $|A + \lambda \cdot A|$ where λ is an algebraic integer. This is equivalent to the problem of estimating the size of $|A + \mathcal{L}A|$ when A is a dense subset of the box $[N]^d$ and $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Z})$ is a linear transformation corresponding to multiplication by λ.

A naive way of representing A with a continuous set $\overline{A}$, is to divide the box $[N]^d$ into tiny cubes, and setting $\overline{A} \subset \mathbb{R}^d$ to be the union of the cubes which intersect A. This is not a good representation, since the volume of $\overline{A}$ can be very different from $|A|$. Indeed, if A consists of all points in $[N]^d$ with even coordinates, its representation $\overline{A}$ is the same as if A consists of all points of $[N]^d$.

Krachun and Petrov's solution is to introduce a new dimension to encode the "local density" of A, which is, roughly speaking, the relative density of A within a small box containing x. Their continuous representation is a (compact) set $\overline{A} \subset \mathbb{R}^{d+1}$, which can be seen as having a base in $\mathbb{R}^d$ resembling A, as described in the naive way above, and fibers in $\mathbb{R}$. The fiber at some point $x \in \mathbb{R}^d$ is the interval $[0, r]$, where r is the local density of A at x. Therefore, the volume of $\overline{A}$ matches the size $|A|$. A key fact is the following simple observation:

Observation 6.0.3. *The local density of $B = A + \mathcal{L}A$ at $x + \mathcal{L}y$ is at least the local density of A at x.*

If $\overline{B}$ is the continuous representation of B, then the above observation is equivalent to $\overline{B}$ containing $\overline{A} + \mathcal{L}'(\overline{A})$, where $\mathcal{L}' : \mathbb{R}^{d+1} \to \mathbb{R}^{d+1}$ is given by $\mathcal{L}'(x, y) = (\mathcal{L}x, 0)$ for $x \in \mathbb{R}^d$ and $y \in \mathbb{R}$. Therefore, $\mathrm{Vol}(\overline{B}) \geq \mathrm{Vol}(\overline{A} + \mathcal{L}'(\overline{A}))$. One can then apply the continuous version of sums of dilates to obtain a tight lower bound for $\mathrm{Vol}(\overline{A} + \mathcal{L}'(\overline{A}))$ in terms of $\mathrm{Vol}(\overline{A})$, then translate the result back to the discrete world using the fact that $\mathrm{Vol}(\overline{A}) = |A|$.

The problem with extending this method to general algebraic λ is that Observation 6.0.3 is too weak. Indeed, if λ is not integral, estimating $|A + \lambda \cdot A|$ is equivalent to estimating $|\mathcal{L}_1 A + \mathcal{L}_2 A|$ for some $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ and A a dense subset of $[N]^d$. The observation here is that the local density of $\mathcal{L}_1 A + \mathcal{L}_2 A$ at $\mathcal{L}_1 x + \mathcal{L}_2 y$ is only at least $\frac{1}{|\det \mathcal{L}_1|}$ times the local density of A at x. This is not tight, since if A contains all lattice points in some convex region, then the local density of A is 1 uniformly, and we also expect the local density of $\mathcal{L}_1 A + \mathcal{L}_2 A$ to be 1 uniformly. The observation only guarantees that the local density of $\mathcal{L}_1 A + \mathcal{L}_2 A$ is at least $\frac{1}{|\det \mathcal{L}_1|}$, which is less than 1 if λ is not integral.

This indicates that recording local density is insufficient, and we require a deeper understanding of how the points are arranged locally in A. Our innovation here is to record how A is locally arranged in certain lattices, and compress that information as a high-dimensional compact set we call the "lattice density."

For a (periodic) set $A \subseteq \mathbb{Z}^d$ and a flag of lattices $\mathcal{F} = \{L_0 \subseteq L_1 \subseteq \cdots \subseteq L_k\}$, the lattice density $\mathrm{LD}(A; \mathcal{F})$ is a compact down-set in $[0, 1]^{k+1}$, which encodes various information about the density of A within the lattices L_l. Our continuous representation $\overline{A}$ will then be a compact subset of $\mathbb{R}^{d+k+1}$, with a base in $\mathbb{R}^d$ looking like A, and fibers in $\mathbb{R}^{k+1}$ equal to the local lattice density at each point of A.

Estimating $|A+\lambda_1\cdot A+\cdots+\lambda_k\cdot A|$ is equivalent to estimating $|\mathcal{L}_0A+\cdots+\mathcal{L}_kA|$ for some $\mathcal{L}_1,\dots,\mathcal{L}_k\in \mathrm{Mat}_d(\mathbb{Z})$. The key now is that one can find two flags $\mathcal{F},\mathcal{G}$ such that for each $i=0,\dots,k$, $\pi_{i+1}(\mathrm{LD}(\mathcal{L}_iA;\mathcal{G}))\approx\pi_{i+1}(\mathrm{LD}(A;\mathcal{F}))$. One should think of this as "transformation by $\mathcal{L}_i$ is analogous to the projection π_{i+1} of the lattice density." This analogy extends nicely to sumsets. If $A_0,\dots,A_k$ are periodic sets in $\mathbb{Z}^d$, then $\mathrm{LD}(\mathcal{L}_0A_0+\cdots+\mathcal{L}_kA_k;\mathcal{G})$ roughly contains the cuboid of side lengths

$$|\pi_1(\mathrm{LD}(\mathcal{L}_0A_0))|,\dots,|\pi_{k+1}(\mathrm{LD}(\mathcal{L}_kA_k))|.$$

Just like Observation 6.0.3 above, this implies that if $B=\mathcal{L}_0A+\cdots+\mathcal{L}_kA$, then $\overline{B}$ contains the sumset $\mathcal{L}_0'\overline{A}+\cdots+\mathcal{L}_k'\overline{A}$, where $\mathcal{L}_i':\mathbb{R}^{d+k+1}\to\mathbb{R}^{d+k+1}$ is given by $\mathcal{L}_i'(x,y)=(\mathcal{L}_ix,\pi_{i+1}(y))$ for $x\in\mathbb{R}^d$ and $y\in\mathbb{R}^{k+1}$. We can then apply the continuous variant to $\mathcal{L}_0'\overline{A}+\cdots+\mathcal{L}_k'\overline{A}$, which would then correspond to our desired result on the discrete set A.

Notation

Throughout the chapter, we will use the following notation:

- $\lambda_0,\lambda_1,\dots,\lambda_k$ are algebraic numbers with $\lambda_0=1$.
- $K:=\mathbb{Q}(\lambda_1,\dots,\lambda_k)$ is the number field generated by $\lambda_1,\dots,\lambda_k$.
- The degree of K over $\mathbb{Q}$ is $d:=\deg(K/\mathbb{Q})$, so $K\cong\mathbb{Q}^d$.
- The ring of integers over K is denoted O_K, so $O_K\cong\mathbb{Z}^d$.
- We write $K_{\mathbb{R}}:=K\otimes_{\mathbb{Q}}\mathbb{R}=O_K\otimes_{\mathbb{Z}}\mathbb{R}\cong\mathbb{R}^d$ and $K_{\mathbb{C}}:=K\otimes_{\mathbb{Q}}\mathbb{C}\cong\mathbb{C}^d$.
- We will generally use i to index $1,\dots,d$, j to index $1,\dots,n$ and l to index $1,\dots,k$ (possibly starting at 0). However, this is not strict and the usage can depend on context.

Acknowledgements

The authors thank Deepesh Singhal for helpful discussions on the algebraic number theory aspects of this chapter.

6.1 Mapping to $\mathbb{Z}^d$

In this section, we show how the problem of estimating sums of algebraic dilates can be recast in terms of estimating sums of linear transformations. Our first lemma, generalising [29, Lemma 3.1], will allow us to assume that A is a subset of K.

Lemma 6.1.1. *Suppose that $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$ and $A \subset \mathbb{C}$ is finite. Then there exists a finite set $B \subset K = \mathbb{Q}(\lambda_1, \ldots, \lambda_k)$ such that $|B| = |A|$ and $|B + \lambda_1 \cdot B + \cdots + \lambda_k \cdot B| \leq |A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$.*

Proof. Let L be the field extension of K generated by A. Pick any K-linear map $f : L \to K$ which is injective on A. Such a map exists since A is finite. Set $B = f(A)$. Then $|B| = |A|$ and, for any $a_0, \ldots, a_k \in A$,

$$f(a_0 + \lambda_1 a_1 + \cdots + \lambda_k a_k) = f(a_0) + \lambda_1 f(a_1) + \cdots + \lambda_k f(a_k).$$

Hence, $|B+\lambda_1 \cdot B+\cdots+\lambda_k \cdot B| = |f(A+\lambda_1 \cdot A+\cdots+\lambda_k \cdot A)| \leq |A+\lambda_1 \cdot A+\cdots+\lambda_k \cdot A|$. □

In light of this result, we will henceforth assume that $A \subset K$. For any $a \in K$, there exists a positive integer n such that $na \in \mathcal{O}_K$. In fact, this is true for any fractional ideal $\mathcal{I} \subseteq \mathcal{O}_K$ – for any $a \in K$, there exists a positive integer n such that $na \in \mathcal{I}$. Thus, since A is finite, by rescaling A to $n \cdot A$ for an appropriately large n, we may assume that $A \subset \mathcal{I}$ if we wish to without any loss of generality.

To pass to linear transformations, we fix a $\mathbb{Z}$-basis $e_1 = 1, e_2, \ldots, e_d$ of $\mathcal{O}_K$ and let $\Phi : \mathcal{O}_K \to \mathbb{Z}^d$ be the isomorphism mapping the e_i to the standard basis of $\mathbb{Z}^d$. This map extends linearly to an isomorphism $\Phi : K \to \mathbb{Q}^d$. Under this isomorphism, multiplication by λ_l corresponds to the linear map $\mathcal{M}_l \in \mathrm{Mat}_d(\mathbb{Q})$ defined by

$$\mathcal{M}_l(x) = \Phi(\lambda_l \cdot \Phi^{-1}(x)).$$

The problem of estimating $|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$ for $A \subset K$ is then equivalent to estimating $|A + \mathcal{M}_1 A + \cdots + \mathcal{M}_k A|$ for $A \subset \mathbb{Q}^d$.

One further step allows us to convert the problem into one about sums of linear transformations with *integer* entries. Recall, from the introduction, that the denominator ideal of $\lambda_1, \ldots, \lambda_k$ is the non-zero ideal $\mathfrak{D} = \mathcal{O}_K \cap \lambda_1^{-1}\mathcal{O}_K \cap \cdots \cap \lambda_k^{-1}\mathcal{O}_K$ with the property that $\lambda_l \mathfrak{D} \subseteq \mathcal{O}_K$ for all $l = 0, \ldots, k$. If we fix an isomorphism $\Phi' : \mathfrak{D} \to \mathbb{Z}^d$, then multiplication of the elements of $\mathfrak{D}$ by λ_l corresponds to the linear map $\mathcal{L}_l : \mathbb{Z}^d \to \mathbb{Z}^d$ defined by

$$\mathcal{L}_l(x) = \Phi(\lambda_l \cdot \Phi'^{-1}(x)).$$

By rescaling, we may assume that $A \subset \mathfrak{D}$, so that Theorem 6.0.2 becomes equivalent to the following result, whose proof will now be our principal goal.

Theorem 6.1.2. *For finite subsets A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| \geq H(\lambda_1, \ldots, \lambda_k)|A| - o(|A|).$$

The next lemma determines all the (simultaneous) eigenvalues of the λ_l, when they are viewed as $\mathbb{Q}$-linear maps on K. In the statement and proof, we will use the fact that there are exactly d different complex embeddings (that is, injective field homomorphisms) of K in $\mathbb{C}$, which we denote by $\sigma_1, \ldots, \sigma_d$ with σ_1 the identity.

Lemma 6.1.3. *Viewing $K \cong \mathbb{Q}^d$, multiplication by λ_l induces a $\mathbb{Q}$-linear map $\mathcal{M}_l : \mathbb{Q}^d \to \mathbb{Q}^d$. Then the maps $\mathcal{M}_0, \ldots, \mathcal{M}_k$ are simultaneously diagonalizable over $\mathbb{C}$ into the diagonal matrices $\mathcal{D}_0, \ldots, \mathcal{D}_k$, where $\mathcal{D}_l$ has diagonal entries $(\sigma_1(\lambda_l), \ldots, \sigma_d(\lambda_l))$ for $l = 0, \ldots, k$.*

Proof. Let $K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C}$ and define $\sigma : K_{\mathbb{C}} \to \mathbb{C}^d$ be the $\mathbb{C}$-linear map defined by $\sigma(\alpha \otimes c) = (c\sigma_1(\alpha), \ldots, c\sigma_d(\alpha))$. We claim that σ is an isomorphism. Indeed, let $\alpha \in K$ be a generator of K, i.e., $K = \mathbb{Q}(\alpha)$. Then $(1, \alpha, \ldots, \alpha^{d-1})$ is a $\mathbb{Q}$-basis for K, and $\sigma_1(\alpha), \ldots, \sigma_d(\alpha)$ are all distinct. Under this basis, which is also a basis for $K_{\mathbb{C}}$, σ is represented by the matrix

$$\begin{pmatrix} 1 & \sigma_1(\alpha) & \sigma_1(\alpha)^2 & \cdots & \sigma_1(\alpha)^{d-1} \\ 1 & \sigma_2(\alpha) & \sigma_2(\alpha)^2 & \cdots & \sigma_2(\alpha)^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_d(\alpha) & \sigma_d(\alpha)^2 & \cdots & \sigma_d(\alpha)^{d-1} \end{pmatrix},$$

which is non-singular, since it is a Vandemonde matrix. Let $e_1, \ldots, e_d \in \mathbb{C}^d$ be the standard basis of $\mathbb{C}^d$ and $v_i = \sigma^{-1}(e_i)$. Then $v_1, \ldots, v_d$ form a basis for $K_{\mathbb{C}}$. We claim that, in this basis, $\mathcal{M}_l$ diagonalizes into the desired form. It suffices to check that $\mathcal{M}_l(v_i) = \sigma_i(\lambda_l)v_i$.

Let $x_1, \ldots, x_d \in K$ be a $\mathbb{Q}$-basis for K. Then v_i can be written in the form $v_i = x_1 \otimes c_{i1} + \cdots + x_k \otimes c_{ik}$ for some $c_{il} \in \mathbb{C}$, so that $\sigma(v_i) = e_i$ says that

$$\sum_{l=1}^{k} c_{il}\sigma_j(x_l) = \delta_{ij}.$$

But then

$$\begin{aligned}\sigma_j(\mathcal{M}_l(v_i)) &= \sigma_j\left(\mathcal{M}_l\left(\sum_{m=1}^{k} x_m \otimes c_{im}\right)\right) = \sigma_j\left(\sum_{m=1}^{k}(\lambda_l x_m)\otimes c_{im}\right)\\ &= \sum_{m=1}^{k} c_{im}\sigma_j(\lambda_l x_m) = \sigma_j(\lambda_l)\sum_{m=1}^{k} c_{im}\sigma_j(x_m)\\ &= \sigma_j(\lambda_l)\delta_{ij} = \sigma_i(\lambda_l)\delta_{ij}.\end{aligned}$$

It follows that $\mathcal{M}_l(v_i) = \sigma_i(\lambda_l)v_i$, as required. □

We will also recall the norm $\|\cdot\|$ defined on O_K and $K_{\mathbb{R}}$ in Chapter 5. By pulling back Φ, the ∞-norm on $\mathbb{Z}^d$ defines a norm $\|\cdot\|$ on O_K, namely, for $l_1, \dots, l_d \in \mathbb{Z}$,

$$\|l_1 e_1 + \cdots + l_d e_d\| := \max_i |l_i|.$$

The open ball $B(L)$ of radius $L > 0$ under this norm is then given by

$$B(L) := \{l_1 e_1 + \cdots + l_d e_d \in O_K : |l_i| < L \text{ for all } i\}.$$

$\|\cdot\|$ extends linearly and continuously to a norm on $K_{\mathbb{R}}$, which we also denote by $\|\cdot\|$. The open ball $B_{\mathbb{R}}(R)$ of radius $R > 0$ in $K_{\mathbb{R}}$ is then

$$B_{\mathbb{R}}(R) := \{e_1 \otimes r_1 + \cdots + e_d \otimes r_d \in K_{\mathbb{R}} : |r_i| < R \text{ for all } i\}.$$

We have the following constants associated to the norm $\|\cdot\|$ from Chapter 5.

Lemma 6.1.4 (Lemma 5.2.1)**.** *There exist constants $C_1, C_2, C_3 \in \mathbb{N}$ such that the following hold:*

1. *For all $x, y \in K_{\mathbb{R}}$, $\|xy\| \le C_1 \|x\| \|y\|$.*
2. *For all $l = 0, \dots, k$, $C_2\lambda_l \in O_K$.*
3. *For all $l = 0, \dots, k$ and $x \in O_K$, $\lambda_l x \in \frac{1}{C_2} \cdot B(C_3 \|x\|)$.*

6.2 The continuous version

We now come to the first part of our argument, which is to extend an estimate of Krachun and Petrov [29, Theorem 2] on sums of linear transformations of compact sets to more than two variables. We will need to assume that the linear transformations are simultaneously diagonalizable. But, as we have seen in Lemma 6.1.3 above, this is exactly the situation we are concerned with.

Throughout this section, we will fix an identification $K_{\mathbb{R}} \cong \mathbb{R}^d$ and take μ to be the Lebesgue measure on $\mathbb{R}^d$ and, hence, on $K_{\mathbb{R}}$. Our main result may then be stated as follows.

Theorem 6.2.1. *Suppose $\mathcal{L}_1, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{R})$ are simultaneously diagonalizable over $\mathbb{C}$ into the diagonal matrices $\mathcal{D}_1, \ldots, \mathcal{D}_k$, where $\mathcal{D}_l = \mathrm{diag}(\lambda_{l1}, \ldots, \lambda_{ld})$ with each $\lambda_{li} \in \mathbb{C}$. Then, for any compact $A \subset \mathbb{R}^d$,*

$$\mu(\mathcal{L}_1 A + \mathcal{L}_2 A + \cdots + \mathcal{L}_k A) \geq \left(\prod_{i=1}^{d} \sum_{l=1}^{k} |\lambda_{li}| \right) \mu(A).$$

Moreover, equality holds for some A with $\mu(A) > 0$.

Proof. Let $\Lambda = \{(\lambda_{1i}, \lambda_{2i}, \ldots, \lambda_{ki})\}_{i=1}^{d}$. Since complex conjugation preserves each $\mathcal{L}_l$, it permutes the elements of Λ. Thus, we can split Λ into two parts Λ_1 and Λ_2, where $\Lambda_1 \subset \mathbb{R}^k$ consists of those tuples fixed by conjugation and Λ_2 consists of conjugate pairs of tuples. Then we may decompose $\mathbb{R}^d$ into the eigenspaces

$$\mathbb{R}^d = \bigoplus_{\lambda \in \Lambda_1} E_\lambda \oplus \bigoplus_{(\lambda, \overline{\lambda}) \in \Lambda_2} E_{\lambda, \overline{\lambda}},$$

where each E_λ is 1-dimensional and each $E_{\lambda, \overline{\lambda}}$ is 2-dimensional. For $\lambda = (\lambda_1, \ldots, \lambda_k) \in \Lambda_1$, each $\mathcal{L}_l$ acts on E_λ by λ_l. For $(\lambda, \overline{\lambda}) \in \Lambda_2$, each $\mathcal{L}_l$ acts on $E_{\lambda, \overline{\lambda}}$ by $|\lambda_l| R_{\arg(\lambda_l)}$, where R_θ is the rotation map on $\mathbb{R}^2$ by θ.

We prove the theorem in the following more general form. Suppose we have a decomposition

$$\mathbb{R}^d = \bigoplus_{j=1}^{n} E_j,$$

where $\dim E_j = d_j$ and $\mathcal{L}_l$ acts on E_j by $r_{lj} P_{lj}$, where $r_{lj} \geq 0$ and P_{lj} is an orthogonal matrix acting on E_j. In other words, for any vector $v \in \mathbb{R}^d$, if we decompose it into $v = v_1 + \cdots + v_n$ with $v_j \in E_j$ for all $1 \leq j \leq n$, then $\mathcal{L}_l v = r_{l1} P_{l1} v_1 + \cdots + r_{ln} P_{ln} v_n$. We will show that

$$\mu(\mathcal{L}_1 A + \mathcal{L}_2 A + \cdots + \mathcal{L}_k A) \geq \left(\prod_{j=1}^{n} \left(\sum_{l=1}^{k} r_{lj} \right)^{d_j} \right) \mu(A).$$

We perform Steiner symmetrization, a continuous analogue of compression introduced by Steiner in his classical work on the isoperimetric problem, along each of the eigenspaces E_j as follows. Write $\mathbb{R}^d = E_j \oplus E$, where E is the direct sum of the

remaining spaces. Let $\pi_1 : \mathbb{R}^d \to E_j$ and $\pi_2 : \mathbb{R}^d \to E$ be the projections onto E_j and E, respectively. For a compact $A \subset \mathbb{R}^d$ and $x \in E$, write $A_x := \pi_1(\pi_2^{-1}(x)) \subset E_j$ for the fiber of A at x. Then $\mu(A) = \int_x \mu(A_x) d\mu(x)$. The *Steiner symmetrization* of A along E_j is the set $S_j(A) \subset \mathbb{R}^d$ with the same support as A on E and such that, for each $x \in \pi_2(A)$, $S_j(A)_x$ is the closed ball centered at 0 with the same volume as A_x.

Claim 6.2.2. *The Steiner symmetrization has the following properties:*

1. $\mu(S_j(A)) = \mu(A)$.
2. $S_j(A)$ *is invariant under any orthogonal transformation of* E_j.
3. $S_j(\mathcal{L}_l A) \supseteq \mathcal{L}_l(S_j(A))$ *for all* l.
4. $S_j(A)$ *is compact.*
5. *If* B *is compact, then* $S_j(A + B) \supseteq S_j(A) + S_j(B)$.
6. *If* $F \in \mathrm{GL}(E)$ *and* $F' \in \mathrm{GL}_d(\mathbb{R})$ *is given by* $I_{E_j} \oplus F$ *and* $F'(A) = A$, *then* $F'(S_j(A)) = S_j(A)$.

Proof.

1. This is true since $\mu(S_j(A)_x) = \mu(A_x)$ for all $x \in E$.
2. This is true since $S_j(A)_x$ is a ball for all $x \in E$.
3. Let $x \in \pi_2(A)$ and $B = S_j(A)_x$, a ball. Then $\mathcal{L}_l(S_j(A)) = \bigcup_{x \in \pi_2(A)} \mathcal{L}_l|_{E_j}(B) \oplus \mathcal{L}_l x$. Note that $\mathcal{L}_l|_{E_j}(B)$ is also a ball of volume $\mu(\mathcal{L}_l|_{E_j}(A_x)) \leq \mu((\mathcal{L}_l A)_{\mathcal{L}_l x})$. Thus, $\mathcal{L}_l|_{E_j}(B) \oplus \mathcal{L}_l x \subseteq S_j(\mathcal{L}_l A)$ and the result follows.
4. Since A is bounded, so is $S_j(A)$. To show that $S_j(A)$ is closed, it is sufficient to show that for any sequence $x_1, x_2, \ldots \in E$ converging to $x \in E$, we have $\mu(A_x) \geq \limsup_n \mu(A_{x_n})$. Since A is closed, $A_x \supseteq \limsup_i A_{x_i}$, so it suffices to show that $\mu(\limsup_i A_{x_i}) \geq \limsup_i \mu(A_{x_i})$. But this is true since the A_{x_i} are uniformly bounded.
5. For $x \in \pi_2(A)$ and $y \in \pi_2(B)$, let r, r' be the radii of the balls $S_j(A)_x$ and $S_j(B)_y$, with volumes V, V'. Then $(S_j(A) + S_j(B))_{x+y}$ is a ball of radius

$r + r'$, maximized over all x, y with the same fixed sum. But, by the Brunn–Minkowski inequality,

$$\begin{aligned}\mu(S_j(A+B)_{x+y}) &\geq \mu(S_j(A)_x + S_j(B)_y)\\ &\geq (\mu(S_j(A)_x)^{1/d_j} + \mu(S_j(B)_y)^{1/d_j})^{d_j}\\ &= (V^{1/d_j} + V'^{1/d_j})^{d_j}\\ &= \mu((S_j(A) + S_j(B))_{x+y}).\end{aligned}$$

Thus, $S_j(A+B)_{x+y} \supseteq (S_j(A) + S_j(B))_{x+y}$ and the result follows.

6. Let $x \in E$. Since $F'(A) = A$, we have $A_{F(x)} = A_x$. Therefore, $S_j(A)_{F(x)} = S_j(A)_x$, so we have $F'(S_j(A)) = S_j(A)$. □

Perform Steiner symmetrization on A successively along $E_1, \ldots, E_n$ to obtain, by Claim 6.2.2(4), the compact set $B = S_1(S_2(\cdots S_n(A)\cdots))$. By Claim 6.2.2(1), (5) and (3),

$$\begin{aligned}\mu(\mathcal{L}_1 A + \cdots + \mathcal{L}_k A) &= \mu(S_j(\mathcal{L}_1 A + \cdots + \mathcal{L}_k A))\\ &\geq \mu(S_j(\mathcal{L}_1 A) + \cdots + S_j(\mathcal{L}_k A))\\ &\geq \mu(\mathcal{L}_1(S_j(A)) + \cdots + \mathcal{L}_k(S_j(A))).\end{aligned}$$

Iterating, we see that $\mu(\mathcal{L}_1 A + \cdots + \mathcal{L}_k A) \geq \mu(\mathcal{L}_1 B + \cdots + \mathcal{L}_k B)$, where we also have $\mu(B) = \mu(A)$.

Let $\mathcal{L}'_l$ be the linear map that just scales by r_{lj} on each E_j, i.e., $\mathcal{L}'_l(v_1 + \cdots + v_n) = r_{l1}v_1 + \cdots + r_{ln}v_n$ for any $v_j \in E_j$. By repeated applications of Claim 6.2.2(2) and (6), we may check that B is rotationally invariant on each E_j, so we have $\mathcal{L}'_l B = \mathcal{L}_l B$. Thus,

$$\begin{aligned}\mu(\mathcal{L}_1 B + \cdots + \mathcal{L}_k B) &= \mu(\mathcal{L}'_1 B + \cdots + \mathcal{L}'_k B)\\ &\geq \mu((\mathcal{L}'_1 + \cdots + \mathcal{L}'_k)(B))\\ &= |\det(\mathcal{L}'_1 + \cdots + \mathcal{L}'_k)|\mu(B)\\ &= \left(\prod_{j=1}^{l}\left(\sum_{l=1}^{k} r_{lj}\right)^{d_j}\right)\mu(B).\end{aligned}$$

Finally, to see that equality may hold, observe that we can take A to be the product of the unit balls in each E_j. □

In particular, this yields the smallest possible value of $\mu(A+\lambda_1\cdot A+\cdots+\lambda_k\cdot A)$ in terms of $\mu(A)$. To see this, let $\mathcal{M}_l \in \mathrm{Mat}_d(\mathbb{Q})$ be the matrix representing multiplication by λ_l for $l = 0,\dots,k$, as defined in Section 6.1. Then, by Lemma 6.1.3, the $\mathcal{M}_l$ are simultaneously diagonalizable into the diagonal matrices $\mathcal{D}_l$ with entries $(\sigma_1(\lambda_l),\dots,\sigma_d(\lambda_l))$, where $\sigma_1,\dots,\sigma_d$ are all the complex embeddings of K. By Theorem 6.2.1, we therefore have

$$\begin{aligned}\mu(A+\lambda_1\cdot A+\cdots+\lambda_k\cdot A) &= \mu(\mathcal{M}_0A+\cdots+\mathcal{M}_kA)\\ &\geq \left(\prod_{i=1}^{d}(1+|\sigma_i(\lambda_1)|+\cdots+|\sigma_i(\lambda_k)|)\right)\mu(A).\end{aligned}$$

Comparing this to our main result, Theorem 6.0.2, we see that the discrete version differs from the continuous one only in the factor $N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda_1,\dots,\lambda_k;K})$, which is a measure of the non-integrality of $\lambda_1,\dots,\lambda_k$. We say more below.

Lower bound construction

In this short subsection, we give a lower bound construction for the discrete case, showing that the constant $H(\lambda_1,\dots,\lambda_k)$ in Theorem 6.0.2 is best possible. In brief, the construction is a discretized version of the equality case in Theorem 6.2.1.

Proposition 6.2.3. *Let $\lambda_1,\dots,\lambda_k \in K = \mathbb{Q}(\lambda_1,\dots,\lambda_k)$ be algebraic numbers. Then there exist arbitrarily large $A \subset \mathbb{C}$ such that*

$$|A+\lambda_1\cdot A+\cdots+\lambda_k\cdot A| \leq H(\lambda_1,\dots,\lambda_k)|A| + O(|A|^{\frac{d-1}{d}}),$$

where $d = \deg(K/\mathbb{Q})$.

Proof. Let $\sigma_1,\dots,\sigma_d : K \to \mathbb{C}$ be the complex embeddings of K and set $\mathfrak{D} = \mathfrak{D}_{\lambda_1,\dots,\lambda_k;K}$. Viewing multiplication by λ_l as a $\mathbb{Q}$-linear map $\mathcal{M}_l : K \to K$ for each l, take $A' \subset K_{\mathbb{R}}$ satisfying the equality case in Theorem 6.2.1 with $\mu(A') = 1$. Then $\mu(A'+\lambda_1\cdot A'+\cdots+\lambda_k\cdot A') = \left(\prod_{i=1}^{d}(1+|\sigma_i(\lambda_1)|+\cdots+|\sigma_i(\lambda_k)|)\right)\mu(A')$.

Let n be an arbitrarily large positive integer and let $A = nA' \cap \mathfrak{D}$, so that

$$|A| = \mu(nA')/\mathrm{Vol}(K_{\mathbb{R}}/\mathfrak{D}) + O(n^{d-1}) = n^d/\mathrm{Vol}(K_{\mathbb{R}}/\mathfrak{D}) + O(n^{d-1}).$$

On the other hand, for each l, $\lambda_l\cdot A \subset \lambda_l\cdot\mathfrak{D} \subseteq \mathcal{O}_K$, so we have

$$A+\lambda_1\cdot A+\cdots+\lambda_k\cdot A \subseteq n(A'+\lambda_1\cdot A'+\cdots+\lambda_k\cdot A') \cap \mathcal{O}_K.$$

Therefore,

$$\begin{aligned}
&|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \\
&\leq \mu(n(A' + \lambda_1 \cdot A' + \cdots + \lambda_k \cdot A'))/\mathrm{Vol}(K_{\mathbb{R}}/\mathcal{O}_K) + O(n^{d-1}) \\
&= n^d \left(\prod_{i=1}^{d} (1 + |\sigma_i(\lambda_1)| + \cdots + |\sigma_i(\lambda_k)|) \right) / \mathrm{Vol}(K_{\mathbb{R}}/\mathcal{O}_K) + O(n^{d-1}).
\end{aligned}$$

Since $\mathrm{Vol}(K_{\mathbb{R}}/\mathfrak{D})/\mathrm{Vol}(K_{\mathbb{R}}/\mathcal{O}_K) = [\mathcal{O}_K : \mathfrak{D}] = N_{K/\mathbb{Q}}(\mathfrak{D})$, we obtain that

$$\begin{aligned}
&|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \\
&\leq N_{K/\mathbb{Q}}(\mathfrak{D}) \left(\prod_{i=1}^{d} (1 + |\sigma_i(\lambda_1)| + \cdots + |\sigma_i(\lambda_k)|) \right) |A| + O(n^{d-1}) \\
&= H(\lambda_1, \ldots, \lambda_k)|A| + O(|A|^{\frac{d-1}{d}}).
\end{aligned}$$

□

6.3 Reduction to a dense subset of the box

We recall our structure theorem for sets with small sums of dilates from Chapter 5.

Theorem 6.3.1 (Theorem 5.0.2)**.** *Let $C, p > 0$. Then there are constants $n = n(C, p)$ and $F = F(C, p)$ such that for any $A \subset \mathcal{O}_K$ satisfying*

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq C|A|,$$

there exists a p-proper $\mathcal{O}_K$-GAP $P \subset \mathcal{O}_K$ containing A of dimension at most n and size at most $F|A|$.

With this result in hand, we are now able to complete the second part of our plan, reducing the proof of our main result, in the form of Theorem 6.1.2, to the case where A is a dense subset of the box $[0, N)^d$.

Lemma 6.3.2. *For any $\varepsilon > 0$, there exists N_0 such that if $N \geq N_0$ and $A \subseteq [0, N)^d$ with $|A| \geq \varepsilon N^d$, then*

$$|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| \geq H(\lambda_1, \ldots, \lambda_k)|A| - o_\varepsilon(|A|).$$

The proof of Lemma 6.3.2, which is the heart of this paper, will occupy us for the next few sections. Before moving on to this, we first show that, together with our version of Freiman's theorem for sums of dilates, Lemma 6.3.2 completes the proof of Theorem 6.1.2.

Proof of Theorem 6.1.2 assuming Lemma 6.3.2. Let $A \subset \mathbb{Z}^d$ be finite and suppose that

$$|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| \leq H|A|,$$

where $H = H(\lambda_1, \ldots, \lambda_k)$. Let $\Phi, \Phi', \mathfrak{D}$ be as in Section 6.1. Setting $A' = \Phi'^{-1}(A) \subseteq \mathfrak{D} \subseteq \mathcal{O}_K$, we have

$$|A' + \lambda_1 \cdot A' + \cdots + \lambda_k \cdot A'| \leq H|A'|.$$

Let C_3 be as in Lemma 6.1.4. By Theorem 6.3.1, our version of Freiman's theorem for sums of dilates applied with $p = (k+1)C_3$, A' is contained in a $(k+1)C_3$-proper $\mathcal{O}_K$-GAP $P \subset K$ of dimension $n = O(1)$ and size $|P| = O(|A'|)$. Suppose P is of the form

$$\left\{v_0 + l_1 v_1 + \cdots + l_n v_n : l_j \in B(L_j)\right\}.$$

Then $|P| \sim (\prod_{j=1}^n L_j)^d$, where the notation $A \sim B$ indicates that the quantities A and B are equal up to a constant multiplicative factor depending only on $\lambda_1, \ldots, \lambda_k$. By translating A', we may assume that $v_0 = 0$. By Lemma 6.1.4, we have $\lambda_l \cdot B(L_j) \subseteq \frac{1}{C_2} \cdot B(C_3 L_j)$ for all j, l. Thus, $\lambda_l \cdot A' \subseteq \lambda_l \cdot P \subseteq \frac{1}{C_2} \cdot (C_3 \star P)$ for all l.

We will now map P to a dense subset of a box via a Freiman isomorphism. Let $v_1^* = 1$ and $v_l^* = 3(k+1)C_3 L_{l-1} v_{l-1}^*$ for $l = 2, \ldots, n$. Let P^* be the $\mathcal{O}_K$-GAP

$$P^* := \left\{l_1 v_1^* + l_2 v_2^* + \cdots + l_n v_n^* : l_j \in B(L_j)\right\}.$$

Then P^* is $(k+1)C_3$-proper. Indeed, if $l_1 v_1^* + l_2 v_2^* + \cdots + l_n v_n^* = l_1' v_1^* + l_2' v_2^* + \cdots + l_n' v_n^*$ for some $l_j, l_j' \in B((k+1)C_3 L_j)$, then we have

$$(l_1 - l_1')v_1^* + \cdots + (l_n - l_n')v_n^* = 0.$$

Suppose $l_t \neq l_t'$ for some $t \in [n]$. Let t be the largest such index, so we have

$$(l_t' - l_t)v_t^* = (l_1 - l_1')v_1^* + \cdots + (l_{t-1} - l_{t-1}')v_{t-1}^*.$$

However, $\left\|(l_t' - l_t)v_t^*\right\| \geq v_t^* = 3(k+1)C_3 L_{t-1} v_{t-1}^*$, whereas

$$\begin{aligned}
&\left\|(l_1 - l_1')v_1^* + \cdots + (l_{t-1} - l_{t-1}')v_{t-1}^*\right\| \\
&\leq \left\|(l_1 - l_1')v_1^*\right\| + \cdots + \left\|(l_{t-1} - l_{t-1}')v_{t-1}^*\right\| \\
&\leq (\|l_1\| + \left\|l_1'\right\|)v_1^* + \cdots + (\|l_{t-1}\| + \left\|l_{t-1}'\right\|)v_{t-1}^* \\
&< 2(k+1)C_3 L_1 v_1^* + \cdots + 2(k+1)C_3 L_{t-1} v_{t-1}^* \\
&\leq 3(k+1)C_3 L_{t-1} v_{t-1}^*,
\end{aligned}$$

a contradiction. This proves that P^* is $(k+1)C_3$-proper.

Consider $\Psi : (k+1)C_3 \star P \to (k+1)C_3 \star P^*$, the natural bijection given by

$$l_1 v_1 + \cdots + l_n v_n \longleftrightarrow l_1 v_1^* + l_2 v_2^* + \cdots + l_n v_n^*.$$

Let $A^* = \Psi(A')$, so that $|A^*| = |A'|$. We claim that for $l = 0, \ldots, k$, we have $\Psi(C_2\lambda_l \cdot A') = C_2\lambda_l \cdot A^*$. Indeed, first observe that the LHS is well-defined, since $\lambda_l \cdot P \subseteq \frac{1}{C_2} \cdot (C_3 \star P)$, so we have $C_2\lambda_l \cdot P \subseteq C_3 \star P$, which is in the domain of Ψ. For any $a = l_1 v_1 + \cdots + l_n v_n \in A'$, set $l'_{jl} = C_2\lambda_l \cdot l_j$, which belongs to $B(C_3 L_j)$ by Lemma 6.1.4. Then

$$\begin{aligned}\Psi(C_2\lambda_l \cdot a) &= \Psi(l'_{1l} v_1 + \cdots + l'_{nl} v_n) = l'_{1l} v_1^* + \cdots + l'_{nl} v_n^* \\ &= C_2\lambda_l \cdot (l_1 v_1^* + \cdots + l_n v_n^*) = C_2\lambda_l \Psi(a).\end{aligned}$$

This proves the stated claim that $\Psi(C_2\lambda_l \cdot A') = C_2\lambda_l \cdot A^*$.

Since P is $(k+1)C_3$-proper, $C_3 \star P$ is $(k+1)$-proper. Hence, Ψ is a $(k+1)$-Freiman isomorphism on $C_3 \star P$ and, therefore, since $C_3 > C_2$,

$$\begin{aligned}&\Psi(C_2 \cdot (A' + \lambda_1 \cdot A' + \cdots + \lambda_k \cdot A')) \\ &= \Psi(C_2\lambda_0 \cdot A' + C_2\lambda_1 \cdot A' + \cdots + C_2\lambda_k \cdot A') \\ &= \Psi(C_2\lambda_0 \cdot A') + \Psi(C_2\lambda_1 \cdot A') + \cdots + \Psi(C_2\lambda_k \cdot A') \\ &= C_2\lambda_0 \cdot A^* + C_2\lambda_1 \cdot A^* + \cdots + C_2\lambda_k \cdot A^* \\ &= C_2 \cdot (A^* + \lambda_1 \cdot A^* + \cdots + \lambda_k \cdot A^*).\end{aligned}$$

It follows that

$$|A^* + \lambda_1 \cdot A^* + \cdots + \lambda_k \cdot A^*| = |A' + \lambda_1 \cdot A' + \cdots + \lambda_k \cdot A'|.$$

Note that $P^* \subseteq B(L)$ for some $L \sim \prod_{j=1}^n L_j$. Recall that C_2 is an integer satisyfing $C_2\lambda_l \in O_K$ for all l. In particular, $C_2 \in \mathfrak{D}$, and since $P^* \subset O_K$, $C_2 \cdot P^* \subset \mathfrak{D}$. Since $C_2 \cdot P^* \subseteq B(C_2 L)$, $\Phi'(C_2 \cdot P^*)$ is contained in a box $[-N, N]^d$ with $N \sim L$. But $N^d \sim |P| \sim |A|$ and so $\Phi'(C_2 \cdot A^*)$ is a dense subset of the box $[-N, N]^d$. By Lemma 6.3.2 (after translating into the box $[0, 2N+1)^d$), we have

$$\begin{aligned}|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| &= |A' + \lambda_1 \cdot A' + \cdots + \lambda_k \cdot A'| \\ &= |A^* + \lambda_1 \cdot A^* + \cdots + \lambda_k \cdot A^*| \\ &= |\mathcal{L}_0(\Phi'(C_2 \cdot A^*)) + \cdots + \mathcal{L}_k(\Phi'(C_2 \cdot A^*))| \\ &\geq H|A^*| - o(|A^*|) \\ &= H|A| - o(|A|),\end{aligned}$$

as required. □

6.4 Lattice densities

As already mentioned in the introduction, the key to proving Lemma 6.3.2 is to represent each discrete set A by a continuous set $\overline{A}$, which we call a lattice density, to which we can apply the continuous estimate given by Theorem 6.2.1. In this section, we introduce these lattice densities and prove some general facts about them. Very roughly, the lattice density of a set $A \subseteq \mathbb{Z}^d$ will encode the density of A with respect to certain lattices.

Lattice densities for periodic sets

Let L be a lattice of rank d, that is, $L \cong \mathbb{Z}^d$. We say that $A \subseteq L$ is *d-periodic* if its group of translational symmetries has rank d. Let $\mathcal{F} = \{L_1 \subseteq L_2 \subseteq \cdots \subseteq L_k\}$ be a flag of sublattices of L, each of which has rank d. In this section, we will define the *lattice density* of any d-periodic set $A \subseteq L$ with respect to the flag $\mathcal{F}$, denoted by $\mathrm{LD}(A;\mathcal{F})$, which will be a subset of $[0,1]^k$ that is a finite union of closed axis-aligned boxes.

For any affine lattice $M \subseteq L$ of rank d, we write $\rho_M(A)$ for the density of $A \cap M$ in M. Since A is d-periodic, this density is always well-defined. In particular, $0 \leq \rho_M(A) \leq 1$. This already allows us to define the lattice density for $k = 1$. Indeed, if $\mathcal{F} = \{L_1\}$ and $A \cap L_1 \neq \emptyset$, we set $\mathrm{LD}(A;\mathcal{F})$ to be the interval $[0, \rho_{L_1}(A)] \subset \mathbb{R}$, while if $A \cap L_1 = \emptyset$, we set $\mathrm{LD}(A;\mathcal{F}) = \emptyset$.

For $k > 1$, let $a_1, \ldots, a_m \in L_k$ be any set of coset representatives of L_k/L_{k-1}, where $m = [L_k : L_{k-1}]$. Let $D_j = \mathrm{LD}(A + a_j; \mathcal{F} \setminus L_k) \subseteq [0,1]^{k-1}$ for each $j \in [m]$ and

$$D = \bigcup_{j=1}^{m} \left(D_j \times \left[\frac{j-1}{m}, \frac{j}{m} \right] \right) \subseteq [0,1]^k.$$

Finally, set $\mathrm{LD}(A;\mathcal{F}) = C_k(D)$, where C_k is the compression in the k-th direction, defined as follows.

In our case, we will only be compressing sets which are finite unions of axis-aligned closed boxes. Let $X \subset \mathbb{R}^d$ be such a set and $1 \leq i \leq d$. Let $\pi_i : \mathbb{R}^d \to \mathbb{R}^{d-1}$ be the projection along the i-th axis. For $x \in \mathbb{R}^{d-1}$, let $X_x = \pi_i^{-1}(x)$, viewed as a subset of $\mathbb{R}$, and write $|X_x|$ for the measure of X_x. Now define $C_i'(X)$ to be the set Y such that $\pi_i(X) = \pi_i(Y)$ and, for each $x \in \pi_i(X)$, Y_x is the interval $[0, |X_x|]$. However, because of boundary issues, this is not quite the compression we want. For example, if $X = [0,1]^2 \cup [1,2]^2 \subset \mathbb{R}^2$, then $C_2'(X) = [0,2] \times [0,1] \cup \{1\} \times [1,2]$. The artifact $\{1\} \times [1,2]$ is undesirable and only arises because the boundaries of the

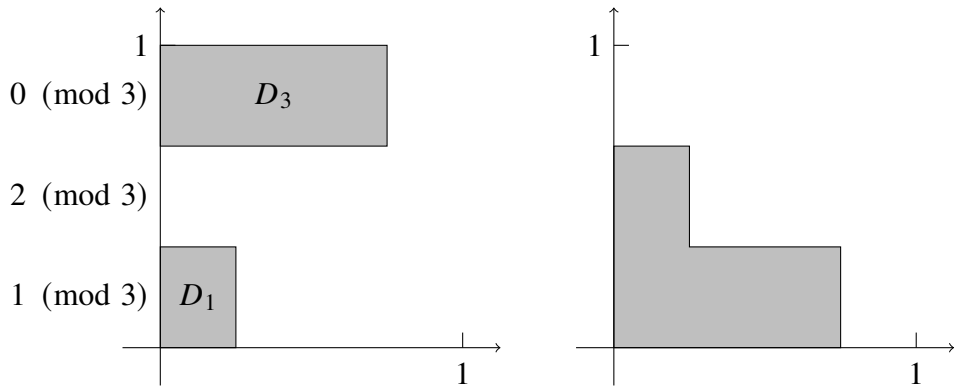

Figure 6.1: On the left, the D_i are stacked, while on the right they are compressed to give the final lattice density.

two squares $[0,1]^2$ and $[1,2]^2$ overlap in the projection. To remove this artifact, we formally define $C_i(X)$ to be the closure of the interior of $C_i'(X)$. Since we will only be compressing sets which are finite unions of axis-aligned closed boxes, we still enjoy the main properties of compressions, such as preservation of the measure of X and that $C_i(X)$ is also a finite union of axis-aligned closed boxes. We will say that X is C_i*-compressed* if $C_i(X) = X$ and *compressed* if it is C_i-compressed for all i.

Observe that, because of the compression, $\mathrm{LD}(A;\mathcal{F})$ is independent of the ordering $a_1, \ldots, a_m$.

Example 6.4.1. Suppose $d = 1$, $k = 2$, $L = \mathbb{Z}$, $\mathcal{F} = \{3\mathbb{Z} \subset \mathbb{Z}\}$ and $A = 12\mathbb{Z} \cup (12\mathbb{Z}+1) \cup (6\mathbb{Z}+3)$. Pick $a_i = -i$ for $i = 1,2,3$ to be the coset representatives of $\mathbb{Z}/3\mathbb{Z}$. Let $A_i = (A-i) \cap 3\mathbb{Z}$ for $i = 1,2,3$. Thus, A_1, A_2, A_3 are the parts of A in the residue classes mod 3, translated so they all lie in $3\mathbb{Z}$. We can easily check that

- $A_1 = 12\mathbb{Z}$,
- $A_2 = \emptyset$,
- $A_3 = 12\mathbb{Z} + \{0, 6, 9\}$.

From the definition, $D_i = \mathrm{LD}(A_i; \{3\mathbb{Z}\}) = [0, \rho_{3\mathbb{Z}}(A_i)]$, so we have $D_1 = [0, 1/4]$, $D_2 = \emptyset$ and $D_3 = [0, 3/4]$. Stacking these intervals vertically and compressing, we get $\mathrm{LD}(A;\mathcal{F}) \subset [0,1]^2$ as shown in Figure 6.1.

Throughout the rest of this section, $\mathcal{F} = \{L_1 \subseteq \cdots \subseteq L_k\}$ will be a flag of full-rank sublattices of a lattice $L \cong \mathbb{Z}^d$ and $A \subseteq L$ a d-periodic subset of L, our aim being

to understand the properties of the lattice density $\mathrm{LD}(A;\mathcal{F})$. We begin with some basic observations.

Lemma 6.4.2. *The following are true:*

1. *For any $a \in L_k$, $\mathrm{LD}(A;\mathcal{F}) = \mathrm{LD}(A+a;\mathcal{F})$.*
2. *$\mathrm{LD}(A;\mathcal{F})$ is compressed.*
3. *If $B \subseteq A$ is d-periodic, then $\mathrm{LD}(B;\mathcal{F}) \subseteq \mathrm{LD}(A;\mathcal{F})$.*
4. *$\rho_{L_k}(A) = \mathrm{Vol}(\mathrm{LD}(A;\mathcal{F}))$.*
5. *$\mathrm{LD}(A;\mathcal{F})$ is a finite union of boxes of the form*

$$[0,r] \times \left[0, \frac{m_2}{[L_2 : L_1]}\right] \times \cdots \times \left[0, \frac{m_k}{[L_k : L_{k-1}]}\right],$$

where $r \in (0,1]$ and $m_2, \ldots, m_k$ are positive integers.

Proof. We proceed by induction on k. In the base case $k = 1$, we have $\mathrm{LD}(A;\mathcal{F}) = [0, \rho_{L_1}(A)]$ and it is easy to check that all of the required properties hold.

Assume therefore that $k > 1$. Let $D_1, \ldots, D_k, D$ be as defined above. We verify each property in turn:

1. Addition by a permutes the cosets L_k/L_{k-1}, so let $a'_1, \ldots, a'_m$ be a permutation of $a_1, \ldots, a_m$ such that $a_j + a = a'_j + b_j$ for some $b_j \in L_{k-1}$. Let $D'_j = \mathrm{LD}(A + a + a_j; \mathcal{F} \setminus L_k)$. By the induction hypothesis, $D'_j = \mathrm{LD}(A + a'_j + b_j; \mathcal{F} \setminus L_k) = \mathrm{LD}(A + a'_j; \mathcal{F} \setminus L_k)$, so $D'_1, \ldots, D'_m$ is a permutation of $D_1, \ldots, D_m$. After compression, it follows that $\mathrm{LD}(A;\mathcal{F}) = \mathrm{LD}(A+a;\mathcal{F})$.
2. Each of the D_j are C_l-compressed for $l = 1, \ldots, k-1$. Thus, D is C_l-compressed for $l = 1, \ldots, k-1$ and, therefore, $\mathrm{LD}(A;\mathcal{F}) = C_k(D)$ is C_l-compressed for $l = 1, \ldots, k$.
3. Let $D'_j = \mathrm{LD}(B + a_j; \mathcal{F} \setminus L_k)$. By the induction hypothesis, $D'_j \subseteq D_j$, so the corresponding D' satisfies $D' \subseteq D$. Therefore, $\mathrm{LD}(B;\mathcal{F}) \subseteq \mathrm{LD}(A;\mathcal{F})$.

4. By definition, $D_j = \mathrm{LD}(A + a_j; \mathcal{F} \setminus L_k)$ and, by the induction hypothesis, we have $\rho_{L_{k-1}}(A + a_j) = \mathrm{Vol}(D_j)$. Therefore,

$$\begin{aligned}\mathrm{Vol}(\mathrm{LD}(A;\mathcal{F})) = \mathrm{Vol}(D) &= \frac{1}{m}\sum_{j=1}^{m}\mathrm{Vol}(D_j) = \frac{1}{m}\sum_{j=1}^{m}\rho_{L_{k-1}}(A + a_j)\\ &= \frac{[L_k : L_{k-1}]}{m}\sum_{j=1}^{m}\rho_{L_k}((A + a_j) \cap L_{k-1})\\ &= \sum_{j=1}^{m}\rho_{L_k}(A \cap (L_{k-1} - a_j)) = \rho_{L_k}(A).\end{aligned}$$

5. We show by induction that $\mathrm{LD}(A;\mathcal{F})$ is an interior-disjoint union of boxes of the form

$$v + [0, r] \times \left[0, \frac{1}{[L_2 : L_1]}\right] \times \cdots \times \left[0, \frac{1}{[L_k : L_{k-1}]}\right],$$

where v is of the form

$$\left(0, \frac{m_2}{[L_2 : L_1]}, \ldots, \frac{m_k}{[L_k : L_{k-1}]}\right)$$

with $m_2, \ldots, m_k$ non-negative integers. The base case is trivial since $\mathrm{LD}(A;\mathcal{F})$ is an interval.

By the induction hypothesis, each D_j is an interior-disjoint union of boxes of the form

$$v + [0, r] \times \left[0, \frac{1}{[L_2 : L_1]}\right] \times \cdots \times \left[0, \frac{1}{[L_{k-1} : L_{k-2}]}\right].$$

Thus, D is also the interior-disjoint union of boxes of the same kind and compressing preserves this property.

Finally, since $\mathrm{LD}(A;\mathcal{F})$ is compressed, it is the finite union of boxes of the required form. □

The next lemma fully determines $\mathrm{LD}(A;\mathcal{F})$ by giving a precise condition for when the lattice density contains any given point.

Lemma 6.4.3. *Suppose $k \geq 2$, $r \in (0, 1]$ is real and $m_2, \ldots, m_k$ are positive integers. Then the following are equivalent:*

1. $\mathrm{LD}(A;\mathcal{F})$ *contains the point*

$$\left(r, \frac{m_2}{[L_2 : L_1]}, \frac{m_3}{[L_3 : L_2]}, \ldots, \frac{m_k}{[L_k : L_{k-1}]}\right).$$

2. *For each* $l = 2, \ldots, k$ *and* $(i_l, i_{l+1}, \ldots, i_k) \in [m_l] \times [m_{l+1}] \times \cdots \times [m_k]$*, there exist* $b_{i_l,\ldots,i_k} \in L_k$ *such that:*

   a) *For* $l < k$, $b_{i_l,i_{l+1},\ldots,i_k} \in b_{i_{l+1},\ldots,i_k} + L_l$.

   b) $b_{i,i_{l+1},\ldots,i_k} - b_{j,i_{l+1},\ldots,i_k} \notin L_{l-1}$ *for each* $i \neq j$ *with* $i, j \in [m_l]$.

   c) $\rho_{L_1}(A + b_{i_2,\ldots,i_k}) \geq r$ *for each* $i_2, \ldots, i_k$.

Proof. We proceed by induction on k. Let $a_1, \ldots, a_m$ be any coset representatives of L_k/L_{k-1} with $m = [L_k : L_{k-1}]$ and $D_i = \mathrm{LD}(A + a_i; \mathcal{F} \setminus L_k)$.

$1 \Rightarrow 2$: From the construction of $\mathrm{LD}(A; \mathcal{F})$, m_k of the D_i contain the point

$$\left(r, \frac{m_2}{[L_2 : L_1]}, \frac{m_3}{[L_3 : L_2]}, \ldots, \frac{m_{k-1}}{[L_{k-1} : L_{k-2}]}\right).$$

Without loss of generality, assume that they are $D_1, \ldots, D_{m_k}$. Set $b_i = a_i \in L_k$ for $i = 1, \ldots, m_k$. Then $b_i - b_j \notin L_{k-1}$ for $i \neq j$.

If $k = 2$, then each D_i with $i \in [m_k]$ contains r, meaning that $\rho_{L_1}(A + a_i) \geq r$. Thus, $\rho_{L_1}(A + b_i) \geq r$ for each $i \in [m_k]$, completing the proof of the base case.

Now suppose that $k > 2$. By the induction hypothesis applied to each D_{i_k}, there exist $b'_{i_l,\ldots,i_k} \in L_{k-1}$ for each $(i_l, i_{l+1}, \ldots, i_k) \in [m_l] \times [m_{l+1}] \times \cdots \times [m_k]$ such that

(a) For $l < k - 1$, $b'_{i_l,\ldots,i_k} \in b'_{i_{l+1},\ldots,i_k} + L_l$.

(b) For $l < k$, $b'_{i,i_{l+1},\ldots,i_k} - b'_{j,i_{l+1},\ldots,i_k} \notin L_{l-1}$ for each $i \neq j$ with $i, j \in [m_l]$.

(c) $\rho_{L_1}(A + b_{i_k} + b'_{i_2,\ldots,i_k}) \geq r$ for each $i_2, \ldots, i_k$.

Set $b_{i_l,\ldots,i_k} = b'_{i_l,\ldots,i_k} + b_{i_k}$. Then property (a) holds for $l < k - 1$; property (b) holds for $l < k$ and property (c) holds. It remains to check that $b_{i_{k-1},i_k} \in b_{i_k} + L_{k-1}$ and $b_i - b_j \notin L_{k-1}$ for each $i \neq j$. The former holds since $b_{i_{k-1},i_k} = b'_{i_{k-1},i_k} + b_{i_k} \in b_{i_k} + L_{k-1}$ and the latter was observed earlier.

$2 \Leftarrow 1$: Since $a_1, \ldots, a_m$ are any coset representatives, we may pick $a_i = b_i$ for $i = 1, \ldots, m_k$.

For $k = 2$, since $\rho_{L_1}(A + b_i) \geq r$, D_i contains r for $i = 1, \ldots, m_2$. Thus, $\mathrm{LD}(A; \mathcal{F})$ contains the point $(r, \frac{m_2}{|L_2/L_1|})$.

Now assume $k > 2$. Let $b'_{i_l,\ldots,i_k} = b_{i_l,\ldots,i_k} - b_{i_k}$. Then we have the following properties, inherited from the b:

(a) For $l < k-1$, $b'_{i_l,\ldots,i_k} \in b'_{i_{l+1},\ldots,i_k} + L_l$.

(b) For $l < k$, $b'_{i,i_{l+1},\ldots,i_k} - b'_{j,i_{l+1},\ldots,i_k} \notin L_{l-1}$ for each $i \neq j$ with $i, j \in [m_l]$.

(c) $\rho_{L_1}(A + b_{i_k} + b'_{i_2,\ldots,i_k}) \geq r$ for each $i_2, \ldots, i_k$.

By the induction hypothesis, for $i = 1, \ldots, m_k$, D_i contains the point

$$\left(r, \frac{m_2}{[L_2 : L_1]}, \frac{m_3}{[L_3 : L_2]}, \ldots, \frac{m_{k-1}}{[L_{k-1} : L_{k-2}]}\right).$$

Therefore, by the definition of $\mathrm{LD}(A; \mathcal{F})$, it contains the point

$$\left(r, \frac{m_2}{[L_2 : L_1]}, \frac{m_3}{[L_3 : L_2]}, \ldots, \frac{m_k}{[L_k : L_{k-1}]}\right),$$

as required. □

As an application of this lemma, we now show how to compute the projections of lattice densities.

Lemma 6.4.4. *The following are true:*

1. $\pi_1(\mathrm{LD}(A; \mathcal{F}))$ *is the interval* $[0, r]$*, where*

$$r = \max_{a \in L_k} \left\{\rho_{L_1}(A + a)\right\}.$$

In particular, $\pi_1(\mathrm{LD}(A; \mathcal{F}))$ *depends only on A,* L_1 *and* L_k*.*

2. *For* $2 \leq l \leq k$, $\pi_l(\mathrm{LD}(A; \mathcal{F}))$ *is the interval*

$$\left[0, \frac{m}{[L_l : L_{l-1}]}\right],$$

where $m \in \mathbb{Z}$ *is the maximum number of elements* $a_1, \ldots, a_m \in A \cap L_k$ *such that* $a_i - a_j \in L_l \setminus L_{l-1}$ *for any* $i \neq j$*. In particular,* $\pi_l(\mathrm{LD}(A; \mathcal{F}))$ *depends only on A,* L_{l-1}*,* L_l *and* L_k*.*

Proof. We first observe that the maxima are well-defined. Indeed, ρ_{L_1} is invariant under translations by elements of L_1, so, for (1), we may take the maximum over the finitely many coset representatives of L_k/L_1. For (2), we see that each a_i must belong to a different coset of L_l/L_{l-1}, so $m \leq [L_l : L_{l-1}]$.

1. If $\pi_1(\mathrm{LD}(A;\mathcal{F})) = [0,r]$, then $\mathrm{LD}(A;\mathcal{F})$ contains the point

$$\left(r, \frac{1}{[L_2 : L_1]}, \frac{1}{[L_3 : L_2]}, \ldots, \frac{1}{[L_k : L_{k-1}]}\right)$$

and r is the maximum such real number. By Lemma 6.4.3, this is equivalent to the existence of some $b \in L_k$ such that $\rho_{L_1}(A+b) \geq r$. Thus,

$$r = \max_{b \in L_k} \left\{\rho_{L_1}(A+b)\right\}.$$

2. Suppose $\mathrm{LD}(A;\mathcal{F})$ contains the point

$$\left(r, \frac{1}{[L_2 : L_1]}, \ldots, \frac{m}{[L_{l+1} : L_l]}, \ldots, \frac{1}{[L_k : L_{k-1}]}\right)$$

for some $r > 0$ and m is the maximum such integer. By Lemma 6.4.3, this is equivalent to the existence of $b \in L_k$ and $b_1, \ldots, b_m \in b + L_l$ such that $b_i - b_j \notin L_{l-1}$ for each $i \neq j$ and $\rho_{L_1}(A+b_i) \geq r$ for each i. Since we may take r to be the minimum of $\rho_{L_1}(A+b_i)$ over all i, we are just requiring that $\rho_{L_1}(A+b_i) > 0$, that is, $(A+b_i) \cap L_1 \neq \emptyset$ for each i.

Suppose such b, b_i exist. Let $a_i \in A$ be such that $a_i + b_i \in L_1$, which exists since $(A+b_i) \cap L_1 \neq \emptyset$. Note that $a_i \in L_k$ since $a_i \in -b_i + L_1 \subseteq L_k$. Moreover, for any $i \neq j$, $a_i - a_j \in b_j - b_i + L_1 \subseteq L_l \setminus L_{l-1}$, as required.

On the other hand, suppose we have $a_1, \ldots, a_m \in A \cap L_k$ such that $a_i - a_j \in L_l \setminus L_{l-1}$ for all $i \neq j$. Set $b = -a_1$ and $b_i = -a_i$ for each i. Then $b_i = b + a_1 - a_i \in b + L_l$ and $b_i - b_j = a_j - a_i \notin L_{l-1}$ for $i \neq j$. Finally, note that $(A+b_i) \cap L_1 \neq \emptyset$ for each i, since it contains 0. □

The next result, which again makes use of Lemma 6.4.3, describes lattice densities of sumsets.

Theorem 6.4.5. *Suppose $B \subseteq L$ is d-periodic. If $p = (p_1, \ldots, p_k) \in \mathrm{LD}(A;\mathcal{F})$ and $q = (q_1, \ldots, q_k) \in \mathrm{LD}(B;\mathcal{F})$, then*

$$\max(p,q) \in \mathrm{LD}(A+B;\mathcal{F}),$$

where $\max(p,q) = (\max(p_1,q_1), \ldots, \max(p_k,q_k))$.

Proof. Since $\mathrm{LD}(A;\mathcal{F})$ and $\mathrm{LD}(B;\mathcal{F})$ are both unions of boxes of the form

$$[0,r] \times \left[0, \frac{m_2}{[L_2 : L_1]}\right] \times \cdots \times \left[0, \frac{m_k}{[L_k : L_{k-1}]}\right]$$

for $r \in (0,1]$ and $m_2, \dots, m_k$ positive integers, we may assume that p, q are of the form

$$p = \left(r, \frac{m_2}{[L_2 : L_1]}, \frac{m_3}{[L_3 : L_2]}, \dots, \frac{m_k}{[L_k : L_{k-1}]}\right),$$
$$q = \left(r', \frac{m_2'}{[L_2 : L_1]}, \frac{m_3'}{[L_3 : L_2]}, \dots, \frac{m_k'}{[L_k : L_{k-1}]}\right).$$

Without loss of generality, we assume that $r \geq r'$. By Lemma 6.4.3, we obtain $b_{i_l,\dots,i_k}, b'_{i_l,\dots,i_k} \in L_k$ with the properties given in the lemma. Let $I = \left\{i \in [2,k] : m_i \geq m_i'\right\}$ and $J = [2,k] \setminus I$. Set $c_{i_l,\dots,i_k} = b_{i_l',\dots,i_k'} + b'_{i_l'',\dots,i_k''}$, where

$$i_j' = \begin{cases} i_j & \text{if } j \in I \\ 1 & \text{otherwise} \end{cases} \quad \text{and} \quad i_j'' = \begin{cases} i_j & \text{if } j \in J \\ 1 & \text{otherwise} \end{cases}$$

for $(i_l, \dots, i_k) \in [\max(m_l, m_l')] \times \cdots \times [\max(m_k, m_k')]$. We wish to show that the $c_{i_l,\dots,i_k}$ satisfy properties (a)–(c) in Lemma 6.4.3 for $\mathrm{LD}(A+B;\mathcal{F})$. Note that we have $c_{i_l,\dots,i_k} \in L_k$ since $b_{i_l',\dots,i_k'}, b'_{i_l'',\dots,i_k''} \in L_k$. We now prove each of (a)–(c) in turn:

(a) For $l < k$, we have $b_{i_l',i_{l+1}',\dots,i_k'} \in b_{i_{l+1}',\dots,i_k'} + L_l$ and $b'_{i_l'',i_{l+1}'',\dots,i_k''} \in b'_{i_{l+1}'',\dots,i_k''} + L_l$. Thus, $c_{i_l,i_{l+1},\dots,i_k} \in c_{i_{l+1},\dots,i_k} + L_l$.

(b) Suppose $l \in I$. Then, for $i \neq j$, $c_{i,i_{l+1},\dots,i_k} - c_{j,i_{l+1},\dots,i_k} = b_{i,i_{l+1}',\dots,i_k'} - b_{j,i_{l+1}',\dots,i_k'} \notin L_{l-1}$. The case $l \in J$ is similar.

(c) We have $\rho_{L_1}(B + b'_{i_2'',\dots,i_k''}) \geq r' > 0$. In particular, $B + b'_{i_2'',\dots,i_k''}$ contains some element $x \in L_1$. Thus, $A + B + c_{i_2,\dots,i_k} \supseteq A + b_{i_2',\dots,i_k'} + x$, so we have $\rho_{L_1}(A + B + c_{i_2,\dots,i_k}) \geq \rho_{L_1}(A + b_{i_2',\dots,i_k'} + x) = \rho_{L_1}(A + b_{i_2',\dots,i_k'}) \geq r$. □

The final result of this subsection relates projections of lattice densities with respect to different flags.

Lemma 6.4.6. *Suppose $\mathcal{F}' = \left\{L_1' \subseteq \cdots \subseteq L_{k-1}' \subseteq L_k\right\}$ is a flag of full-rank sublattices of L. Then the following are true:*

1. *If $L_1' \subseteq L_1$, then*

$$|\pi_1(\mathrm{LD}(A;\mathcal{F}))| \leq |\pi_1(\mathrm{LD}(A;\mathcal{F}'))|.$$

2. *For $2 \leq l \leq k$, if $L_l' = L_l$ and $L_{l-1}' \subseteq L_{l-1}$, then*

$$|\pi_l(\mathrm{LD}(A;\mathcal{F}))| \geq |\pi_l(\mathrm{LD}(A;\mathcal{F}'))|.$$

Proof. 1. Let

$$r = \max_{a \in L_k} \left\{ \rho_{L_1}(A + a) \right\} \quad \text{and} \quad r' = \max_{a \in L_k} \left\{ \rho_{L'_1}(A + a) \right\}.$$

By Lemma 6.4.4, it suffices to show that $r \leq r'$. Suppose r is attained by $a \in L_k$. Let $s = [L_1 : L'_1]$ and $c_1, \ldots, c_s$ be coset representatives of L_1/L'_1. We can split $(A+a) \cap L_1$ into the disjoint union $\bigcup_{i=1}^{s} (A+a+c_i) \cap L'_1$, so that

$$\rho_{L_1}(A + a) = \frac{1}{s} \sum_{i=1}^{s} \rho_{L'_1}(A + a + c_i).$$

Therefore, there is some i such that $\rho_{L'_1}(A + a + c_i) \geq r$, so $r' \geq r$.

2. Suppose $|\pi_l(\mathrm{LD}(A; \mathcal{F}'))| = \frac{n}{[L'_l : L'_{l-1}]}$. By Lemma 6.4.4, there are $b_1, \ldots, b_n \in A \cap L_k$ such that $b_i - b_j \in L'_l \setminus L'_{l-1}$. Let $s = [L_{l-1} : L'_{l-1}]$. Define an equivalence relation by setting $b_i \sim b_j$ if $b_i - b_j \in L_{l-1}$. Then each equivalence class has at most s elements, since no two elements belong to the same coset of L_{l-1}/L'_{l-1}. Let $a_1, \ldots, a_m$ be any representatives of the equivalence classes of $b_1, \ldots, b_n$, so that $ms \geq n$. Since the a_i are in different equivalence classes, we have $a_i - a_j \notin L_{l-1}$ for $i \neq j$. By Lemma 6.4.4 again, we have

$$|\pi_l(\mathrm{LD}(A; \mathcal{F}))| \geq \frac{m}{[L_l : L_{l-1}]} = \frac{ms}{[L_l : L'_{l-1}]} \geq \frac{n}{[L_l : L'_{l-1}]} = |\pi_l(\mathrm{LD}(A; \mathcal{F}'))|,$$

as required. □

Local lattice densities

We will also make use of a local variant of lattice density. Intuitively, the local lattice density of A at some point x is the lattice density of a tiny region of A around x. However, A is a discrete set, so we cannot simply take an infinitesimally small ball around x. Instead, we define the local lattice density around some small region $S \subset \mathbb{R}^d$ to be the lattice density of repeating copies $A \cap S$, in order to be d-periodic. To fit the repeating copies nicely, we require S to be tileable. In practice, we will only consider S to be affine transformations of cubes.

We continue to use notation from the previous subsection. In particular, $\mathcal{F} = \{L_1 \subseteq \cdots \subseteq L_k\}$ is a flag of full-rank sublattices of a lattice $L \cong \mathbb{Z}^d$ and $A \subseteq L$ is always assumed to be d-periodic.

Let $L_{\mathbb{R}} = L \otimes \mathbb{R} \cong \mathbb{R}^d$. We say that $S \subset L_{\mathbb{R}}$ is *tileable* if there is a sublattice $P \subseteq L_1$ of full rank such that $S \oplus P = L_{\mathbb{R}}$. In this case, we say that S is *tiled* by P. For

example, if $L = \mathbb{Z}^d$, the box $[0, M)^d \subset \mathbb{R}^d$ is tileable, as long as $M\mathbb{Z}^d \subseteq L_1$. In all of our applications, S will be a half-open box of the form $[0, M)^d$ or an affine transformation of it.

Let $P \subseteq L_1$ and $S \subset L_{\mathbb{R}}$ be such that S is tiled by P. For any $A \subseteq L$, define the *local lattice density*

$$\mathrm{LD}_S(A; \mathcal{F}) := \mathrm{LD}((A \cap S) + P; \mathcal{F}),$$

noting that $(A \cap S) + P$ is d-periodic. Using Lemma 6.4.3, it is not hard to check that $\mathrm{LD}_S(A; \mathcal{F})$ is independent of the choice of P as long as $P \subseteq L_1$.

Before moving on, we note some basic properties of these local lattice densities.

Lemma 6.4.7. *Let $S, T \subset L_{\mathbb{R}}$ be tileable and $A \subseteq S \cap T \cap L$. Then*

$$\mathrm{LD}_S(A; \mathcal{F}) = \Psi(\mathrm{LD}_T(A; \mathcal{F})),$$

where $\Psi : \mathbb{R}^d \to \mathbb{R}^d$ is given by

$$(x_1, \ldots, x_k) \mapsto \left(\frac{\mathrm{Vol}(T)}{\mathrm{Vol}(S)} x_1, x_2, \ldots, x_k\right).$$

Proof. Suppose T is tiled by $P \subseteq L_1$. Let $x = \left(r, \frac{m_2}{[L_2:L_1]}, \ldots, \frac{m_k}{[L_k:L_{k-1}]}\right) \in \mathrm{LD}_T(A; \mathcal{F})$. By Lemma 6.4.3, there exist $b_{i_l,\ldots,i_k} \in L_k$ satisfying the conditions in the lemma, one of which is that $\rho_{L_1}(A + P + b_{i_2,\ldots,i_k}) \geq r$.

Suppose S is tiled by $Q \subseteq L_1$. Since $T \oplus P = L_{\mathbb{R}}$, $\det(P) = \mathrm{Vol}(T)$ and similarly $\det(Q) = \mathrm{Vol}(S)$. Since $A + Q + b_{i_2,\ldots,i_k}$ consists of translates $A + b_{i_2,\ldots,i_k}$ for each point of Q, its density within L_1, $\rho_{L_1}(A + Q + b_{i_2,\ldots,i_k})$, is inversely proportional to $\det(Q)$. In other words, $\rho_{L_1}(A+Q+b_{i_2,\ldots,i_k})/\det(Q) = \rho_{L_1}(A+P+b_{i_2,\ldots,i_k})/\det(P)$. Then

$$\rho_{L_1}(A + Q + b_{i_2,\ldots,i_k}) = \frac{\det(Q)}{\det(P)} \rho_{L_1}(A + P + b_{i_2,\ldots,i_k}) \geq \frac{\mathrm{Vol}(T)}{\mathrm{Vol}(S)} r.$$

Therefore, by Lemma 6.4.3, $\Psi(x) \in \mathrm{LD}_S(A; \mathcal{F})$, so we have $\mathrm{LD}_S(A; \mathcal{F}) \supseteq \Psi(\mathrm{LD}_T(A; \mathcal{F}))$. The converse follows similarly. □

Lemma 6.4.8. *Let $S, T \subset L_{\mathbb{R}}$ be tileable with $T \subseteq S$. Then, for $2 \leq l \leq k$,*

$$|\pi_l(\mathrm{LD}_T(A; \mathcal{F}))| \leq |\pi_l(\mathrm{LD}_S(A; \mathcal{F}))|.$$

Proof. By Lemma 6.4.7,

$$\begin{aligned}|\pi_l(\mathrm{LD}_T(A;\mathcal{F}))| &= |\pi_l(\mathrm{LD}_T(A\cap T;\mathcal{F}))|\\ &= |\pi_l(\mathrm{LD}_S(A\cap T;\mathcal{F}))|\\ &\le |\pi_l(\mathrm{LD}_S(A;\mathcal{F}))|,\end{aligned}$$

as required. □

6.5 Families of flags

In this section, we construct suitable flags such that "multiplication by λ_i is analogous to taking the projection π_{i+1} of the lattice density." More precisely, we want to find a flag $\mathcal{F}$ in $\mathfrak{D}_{\lambda_1,\dots,\lambda_k;K}$ and a flag $\mathcal{G}$ in $\mathcal{O}_K$ such that, for any d-periodic $A \subseteq \mathfrak{D}_{\lambda_1,\dots,\lambda_k;K}$,

$$\pi_{l+1}(\mathrm{LD}(A;\mathcal{F})) \subseteq \pi_{l+1}(\mathrm{LD}(\lambda_l\cdot A;\mathcal{G})) \tag{6.1}$$

for $l = 0, 1, \dots, k$. We can find such flags for each l, but, unfortunately, it may not be possible to find $\mathcal{F}, \mathcal{G}$ that work simultaneously for all l. To overcome this, we construct families of flags $\mathcal{F}_{\vec{n}}, \mathcal{G}_{\vec{n}}$ and show that for $\vec{n}$ "sufficiently large" these pairs of flags satisfy (6.1) approximately for all l.

Algebraic families of flags

Recall that $\lambda_1, \dots, \lambda_k \in K = \mathbb{Q}(\lambda_1, \dots, \lambda_k)$ and $d = \deg(K/\mathbb{Q})$. Let $\mathfrak{a}_l$ be the ideal $\mathcal{O}_K \cap \lambda_1^{-1}\mathcal{O}_K \cap \cdots \cap \lambda_l^{-1}\mathcal{O}_K$ for $l = 0, 1, \dots, k$. In particular, $\mathfrak{a}_k = \mathfrak{D}_{\lambda_1,\dots,\lambda_k;K}$. Then $\mathfrak{a}_l^{-1}$ is the fractional ideal $\mathcal{O}_K + \lambda_1\mathcal{O}_K + \ldots + \lambda_l\mathcal{O}_K$. We also have $\mathcal{O}_K = \mathfrak{a}_0 \mid \mathfrak{a}_1 \mid \cdots \mid \mathfrak{a}_k$. Let $\mathfrak{b}_l \subseteq \mathcal{O}_K$ be the ideal such that $\mathfrak{a}_l = \mathfrak{b}_l\mathfrak{a}_{l-1}$ for each $l = 1, \dots, k$. For each $\vec{n} = (n_1, \dots, n_k) \in \mathbb{Z}^k_{\ge 0}$ and $l = 0, 1, \dots, k$, let $\mathfrak{c}_{\vec{n},l} = \mathfrak{b}_{l+1}^{n_{l+1}} \cdots \mathfrak{b}_k^{n_k}$. Define two flags of lattices by

$$\begin{aligned}\mathcal{F}^K_{\vec{n}} &:= \left\{\mathfrak{a}_k\mathfrak{c}_{\vec{n},0} \subseteq \mathfrak{a}_k\mathfrak{c}_{\vec{n},1} \subseteq \cdots \subseteq \mathfrak{a}_k\mathfrak{c}_{\vec{n},k-1} \subseteq \mathfrak{a}_k\right\},\\ \mathcal{G}^K_{\vec{n}} &:= \left\{\mathfrak{c}_{\vec{n},0} \subseteq \mathfrak{c}_{\vec{n},1} \subseteq \cdots \subseteq \mathfrak{c}_{\vec{n},k-1} \subseteq \mathcal{O}_K\right\}.\end{aligned}$$

These families of flags will serve as candidates for satisfying (6.1). The following two lemmas make this precise. Note that for any two vectors $\vec{n}, \vec{m} \in \mathbb{Z}^k$, we write $\vec{n} \ge \vec{m}$ if $n_i \ge m_i$ for all i. We also write $\vec{n}+c$ to denote the vector $(n_1+c, \dots, n_k+c)$.

Lemma 6.5.1. *Let $A \subseteq \mathfrak{a}_k$ be d-periodic. Then, for any $\vec{n} \ge 0$,*

$$\pi_1(\mathrm{LD}(A;\mathcal{F}^K_{\vec{n}})) = \pi_1(\mathrm{LD}(A;\mathcal{G}^K_{\vec{n}+1})).$$

Proof. Let

$$r = \max_{a \in \mathfrak{a}_k} \left\{ \rho_{\mathfrak{a}_k \mathfrak{c}_{\vec{n},0}}(A + a) \right\} \quad \text{and} \quad r' = \max_{a \in O_K} \left\{ \rho_{\mathfrak{a}_k \mathfrak{c}_{\vec{n},0}}(A + a) \right\}.$$

Note that $\mathfrak{b}_1 \cdots \mathfrak{b}_k = \mathfrak{a}_k$, so that $\mathfrak{c}_{\vec{n}+1,0} = \mathfrak{a}_k \mathfrak{c}_{\vec{n},0}$. By Lemma 6.4.4(1), it suffices to show that $r = r'$. Since $\mathfrak{a}_k \subseteq O_K$, we clearly have $r' \geq r$. To see that $r \geq r'$, observe that, since $A \subseteq \mathfrak{a}_k$, $(A + a) \cap \mathfrak{a}_k = \emptyset$ for any $a \in O_K \setminus \mathfrak{a}_k$. In particular, $\rho_{\mathfrak{a}_k \mathfrak{c}_{\vec{n},0}}(A + a) = 0$. □

Recall that $\mathcal{M}_l : K \to K$ is the $\mathbb{Q}$-linear map corresponding to multiplication by λ_l. Then each $\mathcal{M}_l$ restricts to the map $\mathfrak{a}_k \to O_K$.

Lemma 6.5.2. *Let $A \subseteq \mathfrak{a}_k$ be d-periodic and $l \in [k]$. Then, for $\vec{n}, \vec{m} \geq 0$ with $m_i = n_i + 1$ for $i = l+1, l+2, \ldots, k$ and $m_l = n_l$,*

$$|\pi_{l+1}(\mathrm{LD}(A; \mathcal{F}_{\vec{n}}^K))| \leq |\pi_{l+1}(\mathrm{LD}(\mathcal{M}_l A; \mathcal{G}_{\vec{m}}^K))|.$$

Proof. Let r be the maximum number of elements $a_1, \ldots, a_r \in A$ such that $a_i - a_j \in \mathfrak{a}_k \mathfrak{c}_{\vec{n},l} \setminus \mathfrak{a}_k \mathfrak{c}_{\vec{n},l-1}$ for $i \neq j$. Then by Lemma 6.4.4(2), $|\pi_{l+1}(\mathrm{LD}(A; \mathcal{F}_{\vec{n}}^K))| = r / [\mathfrak{a}_k \mathfrak{c}_{\vec{n},l} : \mathfrak{a}_k \mathfrak{c}_{\vec{n},l-1}]$. Since $m_l = n_l$, we have $[\mathfrak{a}_k \mathfrak{c}_{\vec{n},l} : \mathfrak{a}_k \mathfrak{c}_{\vec{n},l-1}] = [\mathfrak{c}_{\vec{n},l} : \mathfrak{c}_{\vec{n},l-1}] = N_{K/\mathbb{Q}}(\mathfrak{b}_l^{n_l}) = [\mathfrak{a}_k \mathfrak{c}_{\vec{m},l} : \mathfrak{a}_k \mathfrak{c}_{\vec{m},l-1}]$. By Lemma 6.4.4(2) applied to $|\pi_{l+1}(\mathrm{LD}(\mathcal{M}_l A; \mathcal{G}_{\vec{m}}^K))|$, it suffices to find $b_1, \ldots, b_r \in \mathcal{M}_l A = \lambda_l \cdot A$ such that $b_i - b_j \in \mathfrak{c}_{\vec{m},l} \setminus \mathfrak{c}_{\vec{m},l-1}$.

Set $b_i = \lambda_l a_i$, then it is clear that $b_i \in \lambda_l \cdot A$. It suffices to show:

(a) $b_i - b_j \in \mathfrak{c}_{\vec{m},l}$,

(b) $b_i - b_j \notin \mathfrak{c}_{\vec{m},l-1}$ for $i \neq j$.

For (a), observe that $\lambda_l \mathfrak{a}_k \mathfrak{c}_{\vec{n},l} \subseteq \mathfrak{a}_l^{-1} \mathfrak{a}_k \mathfrak{c}_{\vec{n},l} = \mathfrak{b}_{l+1} \cdots \mathfrak{b}_k \mathfrak{c}_{\vec{n},l} = \mathfrak{c}_{\vec{m},l}$. Thus, $b_i - b_j = \lambda_l (a_i - a_j) \in \lambda_l \mathfrak{a}_k \mathfrak{c}_{\vec{n},l} \subseteq \mathfrak{c}_{\vec{m},l}$.

For (b), suppose that $b_i - b_j \in \mathfrak{c}_{\vec{m},l-1}$ for some $i \neq j$. Then $a_i - a_j \in \lambda_l^{-1} \mathfrak{c}_{\vec{m},l-1}$. On the other hand, $a_i - a_j \in \mathfrak{a}_k \mathfrak{c}_{\vec{n},l}$. Together, we have $a_i - a_j \in \lambda_l^{-1} \mathfrak{c}_{\vec{m},l-1} \cap \mathfrak{a}_k \mathfrak{c}_{\vec{n},l}$.

We claim that $\lambda_l^{-1} \mathfrak{c}_{\vec{m},l-1} \cap \mathfrak{a}_k \mathfrak{c}_{\vec{n},l} \subseteq \mathfrak{a}_k \mathfrak{c}_{\vec{n},l-1}$, which will lead to a contradiction, since $a_i - a_j \notin \mathfrak{a}_k \mathfrak{c}_{\vec{n},l-1}$. We prove the claim by proving it locally at every prime ideal $\mathfrak{p} \subseteq O_K$, that is, that $\nu_{\mathfrak{p}}(\lambda_l^{-1} \mathfrak{c}_{\vec{m},l-1} \cap \mathfrak{a}_k \mathfrak{c}_{\vec{n},l}) \geq \nu_{\mathfrak{p}}(\mathfrak{a}_k \mathfrak{c}_{\vec{n},l-1})$.

Recall that $\mathfrak{a}_l = \mathfrak{a}_{l-1} \cap \lambda_l^{-1} O_K$, so $\nu_\mathfrak{p}(\mathfrak{a}_l) = \max(\nu_\mathfrak{p}(\mathfrak{a}_{l-1}), \nu_\mathfrak{p}(\lambda_l^{-1}))$, which implies that $\nu_\mathfrak{p}(\mathfrak{b}_l) = \max(0, \nu_\mathfrak{p}(\lambda_l^{-1}) - \nu_\mathfrak{p}(\mathfrak{a}_{l-1}))$. We have

$$\begin{aligned}\nu_\mathfrak{p}(\lambda_l^{-1}\mathfrak{c}_{\vec{m},l-1} \cap \mathfrak{a}_k \mathfrak{c}_{\vec{n},l}) &= \nu_\mathfrak{p}(\lambda_l^{-1}\mathfrak{a}_k\mathfrak{a}_l^{-1}\mathfrak{c}_{\vec{n},l-1} \cap \mathfrak{a}_k\mathfrak{b}_l^{-1}\mathfrak{c}_{\vec{n},l-1}) \\ &= \nu_\mathfrak{p}(\mathfrak{a}_k\mathfrak{c}_{\vec{n},l-1})) + \max(\nu_\mathfrak{p}(\lambda_l^{-1}) - \nu_\mathfrak{p}(\mathfrak{a}_l), -\nu_\mathfrak{p}(\mathfrak{b}_l)).\end{aligned}$$

If $\nu_\mathfrak{p}(\mathfrak{a}_{l-1}) \geq \nu_\mathfrak{p}(\lambda_l^{-1}))$, then $\nu_\mathfrak{p}(\mathfrak{b}_l) = 0$. Otherwise, $\nu_\mathfrak{p}(\mathfrak{a}_l) = \nu_\mathfrak{p}(\lambda_l^{-1})$. In either case, $\max(\nu_\mathfrak{p}(\lambda_l^{-1}) - \nu_\mathfrak{p}(\mathfrak{a}_l), -\nu_\mathfrak{p}(\mathfrak{b}_l)) \geq 0$, proving the claim and the lemma. □

Unfortunately, there are no pairs of flags $\mathcal{F}_{\vec{n}}^K$ and $\mathcal{G}_{\vec{m}}^K$ that simultaneously satisfy Lemmas 6.5.1 and 6.5.2 for all l. Indeed, for $\pi_1(\mathrm{LD}(A; \mathcal{F}_{\vec{n}}^K)) = \pi_1(\mathrm{LD}(A; \mathcal{G}_{\vec{m}}^K))$ and $|\pi_{l+1}(\mathrm{LD}(A; \mathcal{F}_{\vec{n}}^K))| \leq |\pi_{l+1}(\mathrm{LD}(\mathcal{M}_l A; \mathcal{G}_{\vec{m}}^K))|$ to hold for all l by the lemmas, we require that $m_l = n_l$ and $m_l = n_l + 1$ simultaneously. To overcome this, in the next subsection, we show that for $\vec{n}$ sufficiently large the projections of the lattice densities stabilise, so we may use $\mathcal{F}_{\vec{n}}^K$ and $\mathcal{G}_{\vec{n}}^K$. This seems to suggest that, as $\vec{n}$ tends to infinity, the lattice densities $\mathrm{LD}(A; \mathcal{F}_{\vec{n}})$ themselves converge as compact subsets. However, we make no attempt to formally prove this, since all we require is that their projections converge.

Regularity

For this subsection, we consider a more general setup, where we have, for each $\vec{n} = (n_1, \ldots, n_k) \in \mathbb{N}^k$, two flags

$$\begin{aligned}\mathcal{F}_{\vec{n}} &= \left\{L_{\vec{n},1} \subseteq L_{\vec{n},2} \subseteq \cdots \subseteq L_{\vec{n},k} \subseteq \mathbb{Z}^d\right\}, \\ \mathcal{G}_{\vec{n}} &= \left\{M_{\vec{n},1} \subseteq M_{\vec{n},2} \subseteq \cdots \subseteq M_{\vec{n},k} \subseteq \mathbb{Z}^d\right\},\end{aligned}$$

where $L_{\vec{n},l}$ depends only on $n_l, n_{l+1}, \ldots, n_k$ and $L_{\vec{n},l} \subseteq L_{\vec{n}',l}$ if $\vec{n} \geq \vec{n}'$ and similarly for $M_{\vec{n},l}$. We also fix a set $A \subseteq \mathbb{Z}^d$.

For a positive integer R, an *R-cube* is a set that comes from taking the set $[0, R)^d \subset \mathbb{R}^d$ and shifting it by an element of $R\mathbb{Z}^d$. Let P be an R-cube for some R. For natural numbers $M, n_l, n_{l+1}, \ldots, n_k$ with $M > 0$ and a real number $\delta > 0$, we say that P is *$(M, \delta, n_l, \ldots, n_k)$-regular* if each of the M^d different R/M-subcubes Q of P satisfies

$$|\pi_{l+1}(\mathrm{LD}_Q(A; \mathcal{F}_{\vec{n}'}))| \geq (1 - \delta)|\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}}))|,$$

where $\vec{n} = (0, \ldots, 0, n_l, \ldots, n_k)$ and $\vec{n}' = (0, \ldots, 0, n_l + 1, \ldots, n_k)$.

Remark. *Here we are implicitly assuming that R/M is an integer. Throughout the remainder of the paper, whenever we mention a local density $\mathrm{LD}_P(A; \mathcal{F})$, we will*

assume that P is tileable. In particular, this means that R and R/M will always be multiples of every bounded number, so that the lattices $R\mathbb{Z}^d$ and $(R/M)\mathbb{Z}^d$ are contained in $L_{\vec{n},1}$. In practice, we will only be considering $\mathcal{F}_{\vec{n}}$ where $\vec{n}$ is bounded and (N/M)-cubes where M is bounded and N can be taken to be a multiple of a sufficiently large integer.

By Lemmas 6.4.6 and 6.4.8, we always have

$$|\pi_{l+1}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}'}))| \le |\pi_{l+1}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}}))| \le |\pi_{l+1}(\mathrm{LD}_P(A;\mathcal{F}_{\vec{n}}))|,$$

so regularity says that both inequalities are close to equalities. In other words, our notion of regularity really encompasses two different types of regularity. The first is that the size of the projection π_{l+1} does not change much when we replace $\vec{n}$ with $\vec{n}'$. The second is that the local lattice density does not change much when we shrink the local region from P to Q. Note that in the definition of regularity, we may replace $\vec{n}, \vec{n}'$ with $\vec{n} = (*, \dots, *, n_l, \dots, n_k)$ and $\vec{n}' = (*, \dots, *, n_l + 1, \dots, n_k)$, where the $*$ could be any (possibly distinct) natural number, since that does not change the relevant projection of the lattice density.

Before proving our main result on regularity, we note some simple consequences of the definition.

Lemma 6.5.3. *Let M_1, M_2 be positive integers and P be an $(M_1M_2, \delta, n_l, \dots, n_k)$-regular R-cube. Then the following hold:*

1. *P is $(M_1, \delta, n_l, \dots, n_k)$-regular.*
2. *For any R/M_1-subcube Q of P, Q is $(M_2, \delta, n_l, \dots, n_k)$-regular.*

Proof. Let Q be any R/M_1-subcube of P and S be any $R/(M_1M_2)$-subcube of Q. By regularity, we have

$$|\pi_{l+1}(\mathrm{LD}_S(A;\mathcal{F}_{\vec{n}'}))| \ge (1-\delta)|\pi_{l+1}(\mathrm{LD}_P(A;\mathcal{F}_{\vec{n}}))|.$$

By Lemma 6.4.8, we have $|\pi_{l+1}(\mathrm{LD}_P(A;\mathcal{F}_{\vec{n}}))| \ge |\pi_{l+1}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}}))|$ and $|\pi_{l+1}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}'}))| \ge |\pi_{l+1}(\mathrm{LD}_S(A;\mathcal{F}_{\vec{n}'}))|$. Therefore,

$$|\pi_{l+1}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}'}))| \ge (1-\delta)|\pi_{l+1}(\mathrm{LD}_P(A;\mathcal{F}_{\vec{n}}))|,$$
$$|\pi_{l+1}(\mathrm{LD}_S(A;\mathcal{F}_{\vec{n}'}))| \ge (1-\delta)|\pi_{l+1}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}}))|,$$

which prove the first and second parts of the lemma, respectively. □

We now come to our main result on regularity, which says that, for any dense $A \subseteq [0,N)^d$, one can cut the box $[0,N)^d$ into a bounded number of subcubes, most of which are regular and such that the union of the regular subcubes covers most of A. We first prove such a result with respect to a single projection π_{l+1}, before iterating it to establish regularity with respect to all projections.

Lemma 6.5.4. *Fix $\varepsilon, \delta > 0$ and $l \in [k]$, a positive integer M and non-negative integers $n_{l+1}, \dots, n_k$. Then there exists $R_0 = R_0(M, \varepsilon, \delta)$ such that if $A \subseteq [0,N)^d$ is of size at least εN^d and $N' \mid N$, then there exists a natural number $r \leq R_0$ and a collection $\mathcal{P}$ of disjoint N'/M^r-cubes such that, for $A' = A \cap \bigcup_{P \in \mathcal{P}} P$,*

1. *$|A'| \geq (1-\delta)|A|$,*
2. *P is $(M, \delta, r, n_{l+1}, \dots, n_k)$-regular for all $P \in \mathcal{P}$.*

Proof. Let $\mathcal{P}^{(r)}$ be the collection of N'/M^r-cubes in $[0,N)^d$, $A^{(r)} = A \cap \bigcup_{P \in \mathcal{P}^{(r)}} P$ and $\mathcal{P}_0^{(r)}$ be the collection of all $(M, \delta, r, n_{l+1}, \dots, n_k)$-regular cubes in $\mathcal{P}^{(r)}$. We will set $A' = A^{(r)}$ and $\mathcal{P} = \mathcal{P}_0^{(r)}$, so we wish to show that there is some bounded r such that $|A^{(r)}| \geq (1-\delta)|A|$.

Let $\mathcal{P}_1^{(r)}$ be the collection of all cubes in $\mathcal{P}^{(r)}$ which are not $(M, \delta, r, n_{l+1}, \dots, n_k)$-regular. Writing $\vec{n}^{(r)} = (0, \dots, 0, r, n_{l+1}, \dots, n_k)$, consider the quantity

$$D_r := \frac{(N'/N)^d}{M^{rd}} \sum_{P \in \mathcal{P}^{(r)}} |\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r)}}))| \leq \frac{(N'/N)^d}{M^{rd}} |\mathcal{P}^{(r)}| = 1.$$

For any $P \in \mathcal{P}^{(r)}$ and subcube $Q \in \mathcal{P}^{(r+1)}$, we have the inequalities

$$|\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r)}}))| \geq |\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r+1)}}))| \geq |\pi_{l+1}(\mathrm{LD}_Q(A; \mathcal{F}_{\vec{n}^{(r+1)}}))|.$$

Therefore, D_r is decreasing in r. Set $R_0 := \frac{M^d}{\varepsilon \delta^2}$. Since D_r is decreasing and in $[0,1]$, there is some $r \leq R_0$ such that $D_r \geq D_{r+1} \geq D_r - \frac{\varepsilon \delta^2}{M^d}$. For each $P \in \mathcal{P}_1^{(r)}$, since P is not regular, there is some subcube $Q \in \mathcal{P}^{(r+1)}$ of P such that

$$|\pi_{l+1}(\mathrm{LD}_Q(A; \mathcal{F}_{\vec{n}^{(r+1)}}))| \leq (1-\delta)|\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r)}}))|.$$

Therefore,

$$\begin{aligned} D_r - D_{r+1} &= \frac{(N'/N)^d}{M^{rd}} \sum_{P\in\mathcal{P}^{(r)}} \left(|\pi_{l+1}(\mathrm{LD}_P(A;\mathcal{F}_{\vec{n}^{(r)}}))| - \frac{1}{M^d} \sum_{\substack{Q\in\mathcal{P}^{(r+1)}\\ Q\subset P}} |\pi_{l+1}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}^{(r+1)}}))| \right) \\ &\geq \frac{(N'/N)^d}{M^{rd}} \sum_{P\in\mathcal{P}_1^{(r)}} \frac{\delta}{M^d} |\pi_{l+1}(\mathrm{LD}_P(A;\mathcal{F}_{\vec{n}^{(r)}}))| \\ &= \frac{(N'/N)^d\delta}{M^{(r+1)d}} \sum_{P\in\mathcal{P}_1^{(r)}} |\pi_{l+1}(\mathrm{LD}_P(A;\mathcal{F}_{\vec{n}^{(r)}}))|. \end{aligned}$$

On the other hand,

$$\begin{aligned} |A \setminus A^{(r)}| &= \sum_{P\in\mathcal{P}_1^{(r)}} |A\cap P| = \frac{N'^d}{M^{rd}} \sum_{P\in\mathcal{P}_1^{(r)}} \mathrm{Vol}(\mathrm{LD}_P(A;\mathcal{F}_{\vec{n}^{(r)}})) \\ &\leq \frac{N'^d}{M^{rd}} \sum_{P\in\mathcal{P}_1^{(r)}} |\pi_{l+1}(\mathrm{LD}_P(A;\mathcal{F}_{\vec{n}^{(r)}}))|. \end{aligned}$$

Therefore, we have

$$|A \setminus A^{(r)}| \leq \frac{N^d M^d}{\delta}(D_r - D_{r+1}) \leq \varepsilon\delta N^d \leq \delta|A|,$$

as required. □

Lemma 6.5.5. *Fix $\varepsilon, \delta > 0$ and a positive integer M and suppose that $A \subseteq [0,N)^d$ is of size at least εN^d. Then there exist $n_1, \dots, n_k$, $r \leq R_1 = R_1(M,\varepsilon,\delta)$ and a collection $\mathcal{P}$ of disjoint N/M^r-cubes such that, for $A' = A \cap \bigcup_{P\in\mathcal{P}} P$,*

1. *$|A'| \geq (1-\delta)|A|$,*
2. *P is $(M,\delta,n_l,\dots,n_k)$-regular for all $P \in \mathcal{P}$ and $l \in [k]$.*

Proof. Following the notation of Lemma 6.5.4, set $S_1 = R_0(M,\varepsilon/2,\delta/k)$ and, for $l = 2,\dots,k$,

$$S_l = R_0(M^{S_1+\cdots+S_{l-1}+1}, \varepsilon/2, \delta/k).$$

We then set $R_1 := S_1 + \cdots + S_k$. We shall apply Lemma 6.5.4 k times in succession to obtain $n_k, n_{k-1}, \dots, n_1 \leq R_1$.

First, we obtain $n_k \leq S_k$ and a collection $\mathcal{P}^{(k)}$ of disjoint N/M^{n_k}-cubes, so that, for $A^{(k)} = A \cap \bigcup_{P\in\mathcal{P}^{(k)}} P$, we have

1. $|A^{(k)}| \geq \left(1 - \frac{\delta}{k}\right)|A|$,
2. P is $(M^{S_1+\cdots+S_{k-1}+1}, \delta, n_k)$-regular for all $P \in \mathcal{P}^{(k)}$.

Suppose we have constructed $n_k, n_{k-1}, \ldots, n_{l+1}$ for some $l \geq 1$. Then, using Lemma 6.5.4, we obtain $n_l \leq S_l$ and a collection $\mathcal{P}^{(l)}$ of disjoint $N/M^{n_k+\cdots+n_l}$-cubes, so that, for $A^{(l)} = A^{(l+1)} \cap \bigcup_{P\in\mathcal{P}^{(l)}} P$, we have

1. $|A^{(l)}| \geq \left(1 - \frac{\delta}{k}\right)|A^{(l+1)}|$,
2. P is $(M^{S_1+\cdots+S_{l-1}+1}, \delta, n_l, \ldots, n_k)$-regular for all $P \in \mathcal{P}^{(l)}$.

We may assume that the collection $\mathcal{P}^{(l)}$ is a subset of a refinement of $\mathcal{P}^{(l+1)}$.

Finally, set $\mathcal{P} = \mathcal{P}^{(1)}$, a collection of N/M^r-cubes, where $r = n_1 + \cdots + n_k \leq R_1$. Then, for $A' = A \cap \bigcup_{P\in\mathcal{P}} P$, we have

1. $|A'| \geq \left(1 - \frac{\delta}{k}\right)^k |A| \geq (1-\delta)|A|$,
2. for each $l \in [k]$ and each $P \in \mathcal{P}$, P is a subcube of some $P^{(l)} \in \mathcal{P}^{(l)}$, which is, by construction, $(M^{S_1+\cdots+S_{l-1}+1}, \delta, n_l, \ldots, n_k)$-regular. But then, by Lemma 6.5.3, P is $(M, \delta, n_l, \ldots, n_k)$-regular. □

6.6 Proof of the dense case

In this section, we make use of everything we have developed previously to prove the dense case, Lemma 6.3.2, which we state again for the readers' convenience.

Lemma 6.6.1. *For any $\varepsilon > 0$, there exists N_0 such that if $N \geq N_0$ and $A \subset [0,N)^d$ with $|A| \geq \varepsilon N^d$, then*

$$|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| \geq H(\lambda_1, \ldots, \lambda_k)|A| - o_\varepsilon(|A|).$$

Recall that from Section 6.1, we have isomorphisms $\Phi' : \mathfrak{D} \to \mathbb{Z}^d$ and $\Phi : O_K \to \mathbb{Z}^d$. Multiplication by λ_l translates to the map $\mathcal{L}_l : \mathbb{Z}^d \to \mathbb{Z}^d$ given by $\mathcal{L}_l = \Phi \circ \mathcal{M}_l \circ \Phi'^{-1}$, then $|\det \mathcal{L}_0| = N_{K/\mathbb{Q}}(\mathfrak{D})$.

Let $\mathcal{F}^K_{\vec{n}}, \mathcal{G}^K_{\vec{n}}$ be the families of flags of sublattices of $\mathfrak{D}$ and O_K as defined in Section 6.5. Under isomorphisms Φ, Φ', these families translate to families $\mathcal{F}_{\vec{n}}, \mathcal{G}_{\vec{n}}$ in $\mathbb{Z}^d$, given by $\mathcal{F}_{\vec{n}} := \Phi'(\mathcal{F}^K_{\vec{n}})$ and $\mathcal{G}_{\vec{n}} := \Phi(\mathcal{G}^K_{\vec{n}})$. By Lemmas 6.5.1 and 6.5.2, we have the following two properties:

1. For d-periodic $A \subseteq \mathbb{Z}^d$,

$$\pi_1(\mathrm{LD}(A; \mathcal{F}_{\vec{n}})) = \pi_1(\mathrm{LD}(\mathcal{L}_0 A; \mathcal{G}_{\vec{n}+1})). \tag{6.2}$$

2. For d-periodic $A \subseteq \mathbb{Z}^d$, and $l \in [k]$,

$$|\pi_{l+1}(\mathrm{LD}(A; \mathcal{F}_{\vec{n}}))| \leq |\pi_{l+1}(\mathrm{LD}(\mathcal{L}_l A; \mathcal{G}_{\vec{m}}))| \tag{6.3}$$

   if $m_i = n_i + 1$ for $i = l+1, \ldots, k$ and $m_l = n_l$.

Let $\varepsilon > 0$ and $A \subseteq [0, N)^d$ with $|A| \geq \varepsilon N^d$. Let $\delta > 0$ be arbitrary, D be a large integer and M be a sufficiently large multiple of D. All these constants may depend on ε, but not on N, which is assumed to be very large. By Lemma 6.5.5, we obtain bounded $n_1, \ldots, n_k, r$ and a collection $\mathcal{P}$ of disjoint N/M^r-cubes such that for $A' = A \cap \bigcup_{P \in \mathcal{P}} P$, we have

1. $|A'| \geq (1 - \delta)|A|$;
2. P is $(M^2, \delta, n_l, \ldots, n_k)$-regular for all $P \in \mathcal{P}$ and $l \in [k]$.

Let $\mathcal{Q}$ be the collection of N/M^{r+1}-cubes Q such that $Q \subset P$ for some $P \in \mathcal{P}$ and Q is at least distance DN/M^{r+1} away from the boundary of P. In particular, $|\mathcal{Q}| = (M - 2D)^d |\mathcal{P}|$. By Lemma 6.5.3, each Q is $(M, \delta, n_l, \ldots, n_k)$-regular for all $l \in [k]$. Set $A'' = A \cap \bigcup_{Q \in \mathcal{Q}} Q$. Then $A' \setminus A''$ consists of points covered by $\mathcal{P}$ but not $\mathcal{Q}$, therefore,

$$\begin{aligned} |A' \setminus A''| &\leq \left(1 - \left(\frac{M - 2D}{M}\right)^d\right) N^d \leq \varepsilon^{-1} \left(1 - \left(\frac{M - 2D}{M}\right)^d\right) |A| \\ &\leq \frac{2Dd}{M\varepsilon} |A| \leq \delta |A| \end{aligned}$$

for $M \geq 2Dd/\delta\varepsilon$. It follows that $|A''| \geq (1 - 2\delta)|A|$. Let $\mathcal{Q}_0$ be the collection of all N/M^{r+1}-cubes, including those outside $[0, N)^d$. For $Q \in \mathcal{Q}_0$, denote by Q^+ the slightly expanded cube $Q + [-\frac{DN}{M^{r+2}}, -\frac{DN}{M^{r+2}}]^d$. Then, for M sufficiently large ($M \geq 4Dd/\delta$ suffice),

$$\mathrm{Vol}(Q^+) = \left(1 + \frac{2D}{M}\right)^d \mathrm{Vol}(Q) \leq (1 + \delta)\,\mathrm{Vol}(Q).$$

Define the bodies $X, Y \subset \mathbb{R}^{d+k+1} = \mathbb{R}^d \times \mathbb{R}^{k+1}$ by

$$X := \bigcup_{Q \in \mathcal{Q}} (Q \times \mathrm{LD}_Q(A; \mathcal{F}_{\vec{n}})),$$
$$Y := \bigcup_{Q \in \mathcal{Q}_0} (\mathcal{L}_0 Q \times ((1+2\delta)\,\mathrm{LD}_{\mathcal{L}_0(Q^+)}(\mathcal{L}_0 A + \cdots + \mathcal{L}_k A; \mathcal{G}_{\vec{n}+1}))).$$

We remark that in order for $\mathrm{LD}_{\mathcal{L}_0(Q^+)}$ to make sense, we require that $\mathcal{L}_0(Q^+)$ be tileable, with respect to the sparsest lattice in $\mathcal{G}_{\vec{n}+1}$. But this is possible for N a multiple of a large enough number, since $\vec{n}$ is bounded.

For each $l = 0, \ldots, k$, let $\mathcal{L}_l' : \mathbb{R}^{d+k+1} \to \mathbb{R}^{d+k+1}$ be the linear map given by

$$\mathcal{L}_l'(\vec{x}, y_0, y_1, \ldots, y_k) = (\mathcal{L}_l \vec{x}, 0, \ldots, 0, y_l, 0, \ldots, 0).$$

Claim 6.6.2. *We have*

$$\mathcal{L}_0' X + \cdots + \mathcal{L}_k' X \subseteq Y.$$

We finish the proof of Lemma 6.6.1 assuming the claim. Let $\mathcal{L}^* : \mathbb{R}^{d+k+1} \to \mathbb{R}^{d+k+1}$ be given by $\mathcal{L}^*(x, y) = (\mathcal{L}_0^{-1} x, y)$, where $x \in \mathbb{R}^d$ and $y \in \mathbb{R}^{k+1}$.

Note that $\mathcal{L}_0^{-1}\mathcal{L}_l$ is conjugate to $\mathcal{M}_l$, the map given by multiplication by λ_l on K. By Lemma 6.1.3, the maps $1, \mathcal{L}_0^{-1}\mathcal{L}_1, \ldots, \mathcal{L}_0^{-1}\mathcal{L}_k$ are simultaneously diagonalizable over $\mathbb{C}$, where the diagonal matrix corresponding to $\mathcal{L}_0^{-1}\mathcal{L}_l$ has diagonal entries $(\sigma_1(\lambda_l), \ldots, \sigma_d(\lambda_l))$. Therefore, $\mathcal{L}^*\mathcal{L}_l'$ are simultaneously diagonalizable with corresponding diagonal matrix entries $(\sigma_1(\lambda_l), \ldots, \sigma_d(\lambda_l), 0, \ldots, 0, 1, 0, \ldots, 0)$. Thus, by Theorem 6.2.1, we have

$$\mu(\mathcal{L}^*\mathcal{L}_0' X + \cdots + \mathcal{L}^*\mathcal{L}_k' X) \geq \prod_{i=1}^{d} (1 + |\sigma_i(\lambda_1)| + |\sigma_i(\lambda_2)| + \cdots + |\sigma_i(\lambda_k)|)\mu(X).$$

Therefore,

$$\begin{aligned}
\mu(Y) &\geq \mu(\mathcal{L}_0' X + \cdots + \mathcal{L}_k' X) \\
&= \frac{1}{\det(\mathcal{L}^*)} \mu(\mathcal{L}^*\mathcal{L}_0' X + \cdots + \mathcal{L}^*\mathcal{L}_k' X) \\
&\geq \det(\mathcal{L}_0) \prod_{i=1}^{d} (1 + |\sigma_i(\lambda_1)| + |\sigma_i(\lambda_2)| + \cdots + |\sigma_i(\lambda_k)|)\mu(X) \\
&= H(\lambda_1, \ldots, \lambda_k)\mu(X).
\end{aligned}$$

By properties of lattice densities,

$$\begin{aligned}\mu(X) &= \sum_{Q\in\mathcal{Q}} \mathrm{Vol}(Q)\times \mathrm{Vol}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}}))\\ &= \sum_{Q\in\mathcal{Q}} |A\cap Q| = |A''| \geq (1-2\delta)|A|.\end{aligned}$$

Recall from the definition of C_1, since A lies in the cube $(-N,N)^d$, the sum $A+\mathcal{L}_0^{-1}\mathcal{L}_1A+\cdots+\mathcal{L}_0^{-1}\mathcal{L}_kA$ lies in the cube $(-(k+1)C_1N,(k+1)C_1N)^d\subset\mathbb{R}^d$. There are at most $(4(k+1)C_1)^dM^{d(r+1)}$ different $Q\in\mathcal{Q}_0$ such that Q^+ intersects $(-(k+1)C_1N,(k+1)C_1N)^d$. For simplicity, assume that $D>(4(k+1)C_1)^d$, so that there are at most $DM^{d(r+1)}$ such Q's. Thus, there are at most $DM^{d(r+1)}$ different $Q\in\mathcal{Q}_0$ such that $\mathcal{L}_0(Q^+)\cap(\mathcal{L}_0A+\cdots+\mathcal{L}_kA)\neq\emptyset$. For each such Q, we have

$$\begin{aligned}&|\mathcal{L}_0(Q^+)\cap(\mathcal{L}_0A+\cdots+\mathcal{L}_kA)| - |\mathcal{L}_0Q\cap(\mathcal{L}_0A+\cdots+\mathcal{L}_kA)|\\ &\leq \det(\mathcal{L}_0)(\mathrm{Vol}(Q^+)-\mathrm{Vol}(Q))\\ &= O\left(\frac{DN^d}{M^{(r+1)d+1}}\right)\\ &\leq \delta(N/M^{r+1})^d.\end{aligned}$$

Therefore,

$$\begin{aligned}\mu(Y) &= \sum_{Q\in\mathcal{Q}_0}\mathrm{Vol}(\mathcal{L}_0Q)\times(1+2\delta)^{k+1}\,\mathrm{Vol}(\mathrm{LD}_{\mathcal{L}_0(Q^+)}(\mathcal{L}_0A+\cdots+\mathcal{L}_kA;\mathcal{G}_{\vec{n}+1}))\\ &\leq (1+2\delta)^{k+1}\sum_{Q\in\mathcal{Q}_0}\frac{\mathrm{Vol}(\mathcal{L}_0Q)}{\mathrm{Vol}(\mathcal{L}_0(Q^+))}|\mathcal{L}_0(Q^+)\cap(\mathcal{L}_0A+\cdots+\mathcal{L}_kA)|\\ &\leq (1+2\delta)^{k+1}\sum_{Q\in\mathcal{Q}_0}|\mathcal{L}_0(Q^+)\cap(\mathcal{L}_0A+\cdots+\mathcal{L}_kA)|\\ &\leq (1+2\delta)^{k+1}\left(\sum_{Q\in\mathcal{Q}_0}|\mathcal{L}_0Q\cap(\mathcal{L}_0A+\cdots+\mathcal{L}_kA)| + DM^{d(r+1)}\cdot\delta(N/M^{r+1})^d\right)\\ &\leq (1+2\delta)^{k+1}|\mathcal{L}_0A+\cdots+\mathcal{L}_kA| + D\delta N^d.\end{aligned}$$

Thus, we have

$$\begin{aligned}|\mathcal{L}_0A+\cdots+\mathcal{L}_kA| &\geq (1+2\delta)^{-(k+1)}\mu(Y) - O_D(\delta)N^d\\ &= (1-O(\delta))\mu(Y) - O_D(\delta)N^d\\ &\geq (1-O(\delta))H(\lambda_1,\ldots,\lambda_k)\mu(X) - O_D(\delta)N^d\\ &\geq (1-O(\delta))H(\lambda_1,\ldots,\lambda_k)(1-2\delta)|A| - O_D(\delta)N^d\\ &= H(\lambda_1,\ldots,\lambda_k)|A| - O_D(\delta)N^d.\end{aligned}$$

This proves the Lemma 6.6.1 since δ is arbitrary.

Proof of Claim 6.6.2. Let $(x_l, y_l) \in X$ for $l = 0, \dots, k$, where $Q_l \in \mathcal{Q}$ is the cube containing x_l, and $y_l \in \mathrm{LD}_{Q_l}(A; \mathcal{F}_{\vec{n}})$. Our aim is to show that $(\sum_l \mathcal{L}_l x_l, y) \in Y$, where $y = (\pi_1(y_0), \dots, \pi_{k+1}(y_k))$.

Let $Q^* \in \mathcal{Q}_0$ be the cube containing $x := x_0 + \mathcal{L}_0^{-1}\mathcal{L}_1 x_1 + \cdots + \mathcal{L}_0^{-1}\mathcal{L}_k x_k$. Then $\mathcal{L}_0 x_0 + \cdots + \mathcal{L}_k x_k = \mathcal{L}_0 x \in \mathcal{L}_0 Q^*$, so it suffices to show that $y \in (1+2\delta)\,\mathrm{LD}_{\mathcal{L}_0(Q^{*+})}(\mathcal{L}_0 A + \cdots + \mathcal{L}_k A; \mathcal{G}_{\vec{n}+1})$.

Suppose $Q^* = Q_0 + t$ for some translate $t \in \frac{N}{M^{r+1}}\mathbb{Z}^d$. Then $t = \mathcal{L}_0^{-1}\mathcal{L}_1 x_1 + \cdots + \mathcal{L}_0^{-1}\mathcal{L}_k x_k + t_0$, for some $t_0 \in [0, \frac{N}{M^{r+1}})^d$. Let R_l be the unique N/M^{r+2}-cube containing x_l, for $l = 1, \dots, k$. Let $x_k^* = x_k + \mathcal{L}_k^{-1}\mathcal{L}_0 t_0$, then

$$x_k^* - x_k = \mathcal{L}_k^{-1}\mathcal{L}_0 t_0 \in \left[-\frac{C_1 N}{M^{r+1}}, \frac{C_1 N}{M^{r+1}}\right]^d \subseteq \left[-\frac{DN}{M^{r+1}}, \frac{DN}{M^{r+1}}\right]^d.$$

If $P_k \in \mathcal{P}$ is the cube containing Q_k and $Q_k^* \in \mathcal{Q}_0$ is the unique cube containing x_k^*, then $Q_k^* \subset P_k$, since $Q_k \in \mathcal{Q}$ is at least a distance DN/M^{r+1} away from the boundary of P_k. Let R_k^* be the N/M^{r+2}-cube containing x_k^*, then $R_k^* \subset P_k$.

Define the following sets:

- $A_0 = A \cap Q_0$,
- $A_l = A \cap R_l$ for $l = 1, \dots, k-1$,
- $A_k = A \cap R_k^*$.

We have $x_l \in A_l$ for $l = 0, \dots, k-1$ and $x_k^* \in A_k$, and $t = \mathcal{L}_0^{-1}\mathcal{L}_1 x_1 + \cdots + \mathcal{L}_0^{-1}\mathcal{L}_k x_k^*$. Since A_l is contained in a N/M^{r+2}-cube for $l = 1, \dots, k$, $\mathcal{L}_0^{-1}\mathcal{L}_1 A_1 + \cdots + \mathcal{L}_0^{-1}\mathcal{L}_k A_k$ is contained in a cube of side length DN/M^{r+2} if D is sufficiently large. Therefore, $A_0 + \mathcal{L}_0^{-1}\mathcal{L}_1 A_1 + \cdots + \mathcal{L}_0^{-1}\mathcal{L}_k A_k \subseteq Q^{*+}$.

Let Q^+ be tiled by a lattice L, for any $Q \in \mathcal{Q}_0$. By repeatedly applying Theorem 6.4.5, we have the following inclusion of the rectangular box

$$\begin{aligned}\prod_{l=0}^{k} \pi_{l+1}(\mathrm{LD}(\mathcal{L}_l A_l + \mathcal{L}_0 L; \mathcal{G}_{\vec{n}+1})) &\subseteq \mathrm{LD}(\mathcal{L}_0 A_0 + \cdots + \mathcal{L}_k A_k + \mathcal{L}_0 L; \mathcal{G}_{\vec{n}+1}) \\ &= \mathrm{LD}_{\mathcal{L}_0(Q^{*+})}(\mathcal{L}_0 A_0 + \cdots + \mathcal{L}_k A_k; \mathcal{G}_{\vec{n}+1}).\end{aligned}$$

Denote by $\vec{n}^{(l)}$ the vector $(n_1+1,\ldots,n_l+1,n_{l+1},\ldots,n_k)$. We shall show that $|\pi_{l+1}(\mathrm{LD}(\mathcal{L}_l A_l+\mathcal{L}_0 L;\mathcal{G}_{\vec{n}+1}))|\geq(1-\delta)\pi_{l+1}(y_l)$ for all l, by showing separately for the three cases $l=0$, $1\leq l\leq k-1$ and $l=k$.

For $l=0$, we have

$$\begin{aligned}
|\pi_1(\mathrm{LD}(\mathcal{L}_0A_0+\mathcal{L}_0L;\mathcal{G}_{\vec{n}+1}))| &= |\pi_1(\mathrm{LD}(A_0+L;\mathcal{F}_{\vec{n}}))| && \text{by (6.2)}\\
&= |\pi_1(\mathrm{LD}_{Q_0^+}(A_0;\mathcal{F}_{\vec{n}}))|\\
&\geq \frac{\mathrm{Vol}(Q_0)}{\mathrm{Vol}(Q_0^+)}|\pi_1(\mathrm{LD}_{Q_0}(A_0;\mathcal{F}_{\vec{n}}))| && \text{by Lemma 6.4.7}\\
&\geq (1-\delta)|\pi_1(\mathrm{LD}_{Q_0}(A;\mathcal{F}_{\vec{n}}))|\\
&\geq (1-\delta)\pi_1(y_0).
\end{aligned}$$

For $l=1,\ldots,k-1$, since Q_l is $(M,\delta,n_l,\ldots,n_k)$-regular, we have

$$|\pi_{l+1}(\mathrm{LD}_{R_l}(A;\mathcal{F}_{\vec{n}^{(l)}}))|\geq(1-\delta)|\pi_{l+1}(\mathrm{LD}_{Q_l}(A;\mathcal{F}_{\vec{n}}))|.$$

Therefore,

$$\begin{aligned}
&|\pi_{l+1}(\mathrm{LD}(\mathcal{L}_lA_l+\mathcal{L}_0L;\mathcal{G}_{\vec{n}+1}))|\\
&\geq |\pi_{l+1}(\mathrm{LD}(A_l+\mathcal{L}_l^{-1}\mathcal{L}_0L;\mathcal{F}_{\vec{n}^{(l)}}))| && \text{by (6.3)}\\
&= |\pi_{l+1}(\mathrm{LD}_{R_l}(A_l;\mathcal{F}_{\vec{n}^{(l)}}))| && \text{by Lemma 6.4.8}\\
&= |\pi_{l+1}(\mathrm{LD}_{R_l}(A;\mathcal{F}_{\vec{n}^{(l)}}))|\\
&\geq (1-\delta)|\pi_{l+1}(\mathrm{LD}_{Q_l}(A;\mathcal{F}_{\vec{n}}))| && \text{by regularity}\\
&\geq (1-\delta)\pi_{l+1}(y_l).
\end{aligned}$$

Similarly, for $l=k$, we have

$$\begin{aligned}
&|\pi_{k+1}(\mathrm{LD}(\mathcal{L}_kA_k+\mathcal{L}_0L;\mathcal{G}_{\vec{n}+1}))|\\
&\geq |\pi_{k+1}(\mathrm{LD}(A_k+\mathcal{L}_k^{-1}\mathcal{L}_0L;\mathcal{F}_{\vec{n}^{(k)}}))| && \text{by (6.3)}\\
&\geq |\pi_{k+1}(\mathrm{LD}_{Q_k^{*+}}(A_k;\mathcal{F}_{\vec{n}^{(k)}}))|\\
&= |\pi_{k+1}(\mathrm{LD}_{R_k^*}(A_k;\mathcal{F}_{\vec{n}^{(k)}}))| && \text{by Lemma 6.4.8}\\
&= |\pi_{k+1}(\mathrm{LD}_{R_k^*}(A;\mathcal{F}_{\vec{n}^{(k)}}))|\\
&\geq (1-\delta)|\pi_{k+1}(\mathrm{LD}_{P_k}(A;\mathcal{F}_{\vec{n}}))| && \text{by regularity of } P_k\\
&\geq (1-\delta)|\pi_{k+1}(\mathrm{LD}_{Q_k}(A;\mathcal{F}_{\vec{n}}))| && \text{by Lemma 6.4.8}\\
&\geq (1-\delta)\pi_{k+1}(y_k).
\end{aligned}$$

Therefore, we have

$$\begin{aligned}(1-\delta)y &= ((1-\delta)\pi_1(y_0),\dots,(1-\delta)\pi_{k+1}(y_k))\\ &\in \mathrm{LD}_{\mathcal{L}_0(Q^{*+})}(\mathcal{L}_0A_0+\cdots+\mathcal{L}_kA_k;\mathcal{G}_{\vec{n}+1})\\ &\subseteq \mathrm{LD}_{\mathcal{L}_0(Q^{*+})}(\mathcal{L}_0A+\cdots+\mathcal{L}_kA;\mathcal{G}_{\vec{n}+1}),\end{aligned}$$

which implies that $y \in (1+2\delta)\,\mathrm{LD}_{\mathcal{L}_0(Q^{*+})}(\mathcal{L}_0A+\cdots+\mathcal{L}_kA;\mathcal{G}_{\vec{n}+1})$, as required. □

6.7 Concluding remarks

A careful analysis of our arguments gives the $o(|A|)$ error term in Theorem 6.0.2 as $O(|A|/\sqrt{\log^{(k)}|A|})$, where $\log^{(k)}$ is the k-iterate log. As seen in Proposition 6.2.3, there are constructions giving a polynomial error of $O(|A|^{\frac{d-1}{d}})$, which we suspect is closer to the truth. We conjecture that the error term should at least be polynomial in size.

Conjecture 6.7.1. *For any algebraic numbers $\lambda_1,\dots,\lambda_k$, there exists a constant $\sigma > 0$ such that*

$$|A+\lambda_1\cdot A+\cdots+\lambda_k\cdot A| \geq H(\lambda_1,\dots,\lambda_k)|A| - O(|A|^{1-\sigma})$$

for finite subsets A of $\mathbb{C}$.

As a final remark, we note that Theorem 3.0.5 in Chapter 3 does give an error $O(|A|^{1-\sigma})$. Chapter 7 discusses how to translate a problem on algebraic dilates to linear transformations and vice versa, so the above conjecture is true for $k = 1$ and λ_1 of the form $(p/q)^{1/d}$.

Chapter 7

SUMS OF LINEAR TRANSFORMATIONS, REVISITED

Parts of this chapter are based on the author's publications. The materials have been adapted for inclusion in this thesis.

[1] D. Conlon and J. Lim, Sums of algebraic dilates, *in preparation*.

[2] D. Conlon and J. Lim, Sums of linear transformations, *to appear in Transactions of the American Mathematical Society* (2025), arXiv:2203.09827, DOI: 10.1090/tran/9433.

We revisit the following problem mentioned in the introduction.

Problem 7.0.1. *Given $\mathcal{L}_0, \mathcal{L}_1, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ which are irreducible and coprime, determine the largest possible constant $H = H(\mathcal{L}_0, \dots, \mathcal{L}_k)$ such that the following holds. For any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_0 A + \mathcal{L}_1 A + \cdots + \mathcal{L}_k A| \geq H|A| - o(|A|).$$

We first recall what it means for a set of matrices to be irreducible and coprime, defined in Chapter 3.

Definition 7.0.2. We say that $\mathcal{L}_0, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Q})$ are *irreducible* if there are no non-trivial subspaces U, V of $\mathbb{Q}^d$ of the same dimension such that $\mathcal{L}_l U \subseteq V$ for all $l = 0, \dots, k$.

Definition 7.0.3. We say that $\mathcal{L}_0, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are *coprime* if there are no $\mathcal{P}, \mathcal{Q} \in \mathrm{GL}_d(\mathbb{Q})$ with $0 < |\det(\mathcal{P}) \det(\mathcal{Q})| < 1$ such that

$$\mathcal{P}\mathcal{L}_0\mathcal{Q}, \mathcal{P}\mathcal{L}_1\mathcal{Q}, \dots, \mathcal{P}\mathcal{L}_k\mathcal{Q} \in \mathrm{Mat}_d(\mathbb{Z}).$$

These are reasonable assumptions to have. If $\mathcal{L}_0, \dots, \mathcal{L}_k$ were not irreducible, then we may consider A to just be in the subspace U, and restrict $\mathcal{L}_0, \dots, \mathcal{L}_k$ to U. If $\mathcal{L}_0, \dots, \mathcal{L}_k$ are not coprime, then we may replace them with

$$\mathcal{P}\mathcal{L}_0\mathcal{Q}, \mathcal{P}\mathcal{L}_1\mathcal{Q}, \dots, \mathcal{P}\mathcal{L}_k\mathcal{Q} \in \mathrm{Mat}_d(\mathbb{Z}),$$

which are "smaller." For more details, we refer the reader to Chapter 3.

The main purpose of this chapter is to formalize the equivalence between the problems of estimating sums of algebraic dilates and sums of *pre-commuting* linear transformations, defined below.

Definition 7.0.4. We say that $\mathcal{L}_0, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Q})$ are *pre-commuting* if there is some $\mathcal{P} \in \mathrm{GL}_d(\mathbb{Q})$ such that $\mathcal{P}\mathcal{L}_0, \dots, \mathcal{P}\mathcal{L}_k$ pairwise commute.

In particular, using Theorem 3.0.5, we prove the following.

Theorem 7.0.5. *Suppose that $\lambda \in \mathbb{C}$ is an algebraic number with minimal polynomial $p(x) = a_d x^d + \cdots + a_0 \in \mathbb{Z}[x]$, where all the a_i are coprime. Then there are constants D, $\sigma > 0$ such that*

$$|A + \lambda \cdot A| \geq (|a_d|^{1/d} + |a_0|^{1/d})^d |A| - D|A|^{1-\sigma}$$

holds for all finite subsets A of $\mathbb{C}$.

Going the other way, using Theorem 6.0.2, we prove the following.

Theorem 7.0.6. *Let $\mathcal{L}_0, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ be pre-commuting, irreducible and coprime matrices. Then for any finite $A \subset \mathbb{Z}^d$,*

$$|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| \geq H(\mathcal{L}_0, \dots, \mathcal{L}_k)|A| - o(|A|),$$

where $H(\mathcal{L}_0, \dots, \mathcal{L}_k)$ is to be defined later in the chapter. Furthermore, the value of $H(\mathcal{L}_0, \dots, \mathcal{L}_k)$ is optimal.

7.1 Two linear transformations

To get started, we first consider the case $k = 1$. Our aim is to show that estimating $|A + \lambda \cdot A|$ for some algebraic $\lambda \in \mathbb{C}$ reduces to estimating $|\mathcal{L}_1 A + \mathcal{L}_2 A|$. In this section, we prove Theorem 7.0.5 by reducing it to Theorem 3.0.5. Though our estimate applies for all finite $A \subset \mathbb{C}$, the following simple lemma of Krachun and Petrov [28, Lemma 2.1] allows us to restrict attention to sets $A \subset \mathbb{Q}[\lambda]$.

Lemma 7.1.1. *Suppose that $\lambda \in \mathbb{C}$ and A is a finite set of complex numbers. Then there exists a finite set $B \subset \mathbb{Q}[\lambda]$ such that $|B| = |A|$ and $|B + \lambda \cdot B| \leq |A + \lambda \cdot A|$.*

Suppose now that λ is algebraic and has minimal polynomial $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in \mathbb{Q}[x]$. If we view $\mathbb{Q}[\lambda]$ as a d-dimensional $\mathbb{Q}$-vector space with basis $1, \lambda, \lambda^2, \dots, \lambda^{d-1}$, then multiplication by λ is given by the linear transformation

$$\mathcal{L} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix} \in \mathrm{GL}_d(\mathbb{Q}).$$

Thus, the problem of estimating $|A + \lambda \cdot A|$ reduces to that of bounding $|A + \mathcal{L}A|$ for $A \subset \mathbb{Q}^d$. Let b be the smallest positive integer such that $ba_i \in \mathbb{Z}$ for all $i = 0, 1, \ldots, d-1$. Then, if we let

$$\mathcal{L}_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & b \end{pmatrix}, \quad \mathcal{L}_2 = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -ba_0 \\ 1 & 0 & 0 & \cdots & 0 & -ba_1 \\ 0 & 1 & 0 & \cdots & 0 & -ba_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -ba_{d-1} \end{pmatrix} \in \mathrm{Mat}_d(\mathbb{Z}),$$

we see that $|A + \mathcal{L}A| = |\mathcal{L}_1(\mathcal{L}_1^{-1}A) + \mathcal{L}_2(\mathcal{L}_1^{-1}A)|$. Setting $B = \mathcal{L}_1^{-1}A$, the problem becomes that of bounding $|\mathcal{L}_1 B + \mathcal{L}_2 B|$ for $B \subset \mathbb{Q}^d$. By scaling, we may even assume that $B \subset \mathbb{Z}^d$. Therefore, in order to apply Theorem 3.3.6, we only need to verify that $\mathcal{L}_1, \mathcal{L}_2$ are irreducible and coprime. For this, we now derive general conditions for irreducibility and coprimeness. We first look at irreducibility.

Theorem 7.1.2. *$P, Q \in \mathrm{Mat}_d(\mathbb{Q})$ are irreducible if and only if they are invertible and the characteristic polynomial of $P^{-1}Q$ is irreducible over $\mathbb{Q}$.*

Proof. Suppose P, Q are irreducible. If P, say, is not invertible, then there is a one-dimensional subspace $U \subset \mathbb{Q}^d$ such that $PU = 0$. But then both PU and QU lie in the subspace QU of dimension at most 1, contradicting irreducibility.

Note that P, Q are irreducible iff $R = P^{-1}Q$ has no non-trivial invariant subspace over $\mathbb{Q}$. Let $p(x) \in \mathbb{Q}[x]$ be the characteristic polynomial of $P^{-1}Q$. If $P^{-1}Q$ has a non-trivial invariant subspace U, then restricting to U gives a linear transformation $R|_U : U \to U$. But the characteristic polynomial of $R|_U$ divides p, so p is reducible.

Conversely, suppose that $p = fg$ is reducible, with $\deg f, \deg g < d$. Then at least one of $f(R), g(R)$ is not invertible, since $0 = p(R) = f(R)g(R)$. Without loss of generality, assume that $f(R)$ is not invertible, so there is some $v \in \mathbb{Q}^d - \{0\}$ such that $f(R)v = 0$. If f has degree $e < d$, then $R^e v$ lies in the space $U = \langle v, Rv, \ldots, R^{e-1}v \rangle$. Thus, U is a non-trivial invariant subspace. □

For our coprimeness condition, we need the following lemma.

Lemma 7.1.3. *Let $P \in \mathrm{Mat}_d(\mathbb{Q})$ and $Q \in \mathrm{Mat}_d(\mathbb{Z})$ be such that $QP \in \mathrm{Mat}_d(\mathbb{Z})$. For $1 \leq k \leq d$, let m be a $k \times k$ minor of P, i.e., the determinant of a $k \times k$ submatrix. Then $m \det(Q) \in \mathbb{Z}$.*

Proof. Let m be the $k \times k$ minor corresponding to rows $S \subseteq [d]$ and columns $T \subseteq [d]$. Construct a matrix $R \in \mathrm{Mat}_d(\mathbb{Q})$ as follows: the T columns of R are just the T columns of P; the $S \times T^c$ submatrix of R is all zeroes; and the $S^c \times T^c$ submatrix of R is the identity matrix. Then $\det R = \pm m$, so that $\det(QR) = \pm m \det Q$. But the T columns of QR are the T columns of QP, which has all integer entries, and each of the other columns of QR is a column of Q, which also has integer entries. Thus, $QR \in \mathrm{Mat}_d(\mathbb{Z})$, so that $m \det Q = \pm \det(QR) \in \mathbb{Z}$. □

Theorem 7.1.4. *Suppose that $P, Q \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and $p(x) \in \mathbb{Q}[x]$ is the characteristic polynomial of $P^{-1}Q$. Then P, Q are coprime if and only if $|\det P|$ is the smallest positive integer g such that $gp \in \mathbb{Z}[x]$.*

Proof. Let g be the smallest positive integer such that $gp \in \mathbb{Z}[x]$. Let $R, S \in \mathrm{GL}_d(\mathbb{Q})$ be such that $RPS, RQS \in \mathrm{Mat}_d(\mathbb{Z})$. Let $M = (RPS)^{-1}RQS = S^{-1}P^{-1}QS \in \mathrm{Mat}_d(\mathbb{Q})$. Then the characteristic polynomial of M is again p. By Lemma 7.1.3 with M and RPS as P and Q, if m is any $k \times k$ minor of M, then $m \det(RPS) \in \mathbb{Z}$. Suppose $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$. By looking at the expansion of $p(x) = \det(xI - M)$, we see that a_{d-k} can be written as a $\mathbb{Z}$-linear combination of $k \times k$ minors of M. Thus, $a_{d-k} \det(RPS) \in \mathbb{Z}$ for all k, so $g \mid \det(RPS) = \pm |\det P| \det(RS)$. In particular, if we take both R and S to be the identity matrix, then $g \mid |\det P|$.

Suppose now that $g = |\det P|$. Then this implies that $|\det(RS)| \geq 1$, so P, Q are indeed coprime. Conversely, suppose that P, Q are coprime. Consider the rational canonical form of $P^{-1}Q$, which is a block diagonal matrix similar to $P^{-1}Q$ where each block looks like

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{k-1} \end{pmatrix}.$$

The characteristic polynomial of such a block is $x^k + c_{k-1}x^{k-1} + \cdots + c_0$ and the characteristic polynomial p of $P^{-1}Q$ is the product of the characteristic polynomials of its blocks. But, by Theorem 7.1.2, $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ is irreducible, so the rational canonical form of $P^{-1}Q$ consists of a single block. That is, there is some $S \in \mathrm{GL}_d(\mathbb{Q})$ such that

$$S^{-1}P^{-1}QS = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{d-1} \end{pmatrix}.$$

Let D be the diagonal matrix with entries $(1, 1, \ldots, 1, g)$. Then D and $DS^{-1}P^{-1}QS$ are integer matrices. Now set $R = DS^{-1}P^{-1}$, so that $RPS, RQS \in \mathrm{Mat}_d(\mathbb{Z})$. By coprimeness, $|\det R \det S| \geq 1$. But this implies that $g/|\det P| \geq 1$, so $|\det P| \leq g$. However, from before, we have $g \mid |\det P|$, so that $|\det P| = g$, as required. □

Using Theorems 7.1.2 and 7.1.4, it is now a simple matter to verify that $\mathcal{L}_1, \mathcal{L}_2$ are irreducible and coprime. Thus, by Theorem 3.3.6, we have that if $\lambda \in \mathbb{C}$ is an algebraic number with minimal polynomial $p(x) = a_d x^d + \cdots + a_0 \in \mathbb{Z}[x]$, where all the a_i are coprime, then there are $D, \sigma > 0$ such that

$$|A + \lambda \cdot A| \geq (|\det(\mathcal{L}_1)|^{1/d} + |\det(\mathcal{L}_2)|^{1/d})^d |A| - D|A|^{1-\sigma}$$

holds for all finite $A \subset \mathbb{Q}[\lambda]$. But, taking the rescaling of the characteristic polynomial into account, $|\det(\mathcal{L}_1)| = |a_d|$ and $|\det(\mathcal{L}_2)| = |a_0|$, completing the proof of Theorem 7.0.5.

7.2 Sufficient conditions for irreducibility and coprimality

For the remainder of this chapter, let $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$. As we saw in Theorems 7.1.2 and 7.1.4, we have necessary and sufficient conditions for when two linear transformations $\mathcal{L}_0, \mathcal{L}_1$ are irreducible and coprime. For $k > 1$, we do not know whether irreducibility and coprimality are decidable. Nevertheless, we give some simple sufficient conditions for $\mathcal{L}_0, \ldots, \mathcal{L}_k$ to be irreducible and coprime, which are necessary for $k = 1$. Let F be the integer polynomial

$$F(x_0, \ldots, x_k) := \det(x_0\mathcal{L}_0 + \cdots + x_k\mathcal{L}_k) \in \mathbb{Z}[x_0, \ldots, x_k], \tag{7.1}$$

which will be used throughout this chapter.

Lemma 7.2.1. *The following holds.*

1. *If F is irreducible over $\mathbb{Q}$, then $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are irreducible.*
2. *If the coefficients of F are coprime, then $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are coprime.*

Proof. 1. Suppose $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are reducible, then there are non-trivial subspaces $U, V \subset \mathbb{Q}^d$ of dimension c with $0 < c < d$, such that $\mathcal{L}_l(U) \subseteq V$. By changing basis, assume that $U = V = \mathbb{Q}^c$ corresponds to the first c coordinates of $\mathbb{Q}^d$. Then $\mathcal{L}_l$ has the form

$$\mathcal{L}_l = \begin{pmatrix} P_l & Q_l \\ 0 & R_l \end{pmatrix},$$

where $P_l \in \mathrm{Mat}_{c\times c}(\mathbb{Z})$, $Q_l \in \mathrm{Mat}_{c\times(d-c)}(\mathbb{Z})$ and $R_l \in \mathrm{Mat}_{(d-c)\times(d-c)}(\mathbb{Z})$. Then

$$F(x_0, \ldots, x_k) = \det(x_0P_0 + \cdots + x_kP_k)\det(x_0R_0 + \cdots + x_kR_k)$$

is reducible.

2. Suppose $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are not coprime, then there are $\mathcal{P}, \mathcal{Q} \in \mathrm{GL}_d(\mathbb{Q})$ with $0 < |\det(\mathcal{P})\det(\mathcal{Q})| < 1$ such that

$$\mathcal{P}\mathcal{L}_0\mathcal{Q}, \mathcal{P}\mathcal{L}_1\mathcal{Q}, \ldots, \mathcal{P}\mathcal{L}_k\mathcal{Q} \in \mathrm{Mat}_d(\mathbb{Z}).$$

But now, the polynomial

$$\det(\mathcal{P})\det(\mathcal{Q})F = \det(x_0\mathcal{P}\mathcal{L}_0\mathcal{Q} + \cdots + x_k\mathcal{P}\mathcal{L}_k\mathcal{Q})$$

has integer coefficients, so the coefficients of F are not coprime.

□

The converse to the two statements above are not true for $k > 1$. We give a counter example in Section 7.6.

7.3 Algebraic number theory preliminaries

Before continuing, we will state some standard results from algebraic number theory and prove some new ones that we require later. For general background on algebraic number theory, we refer to [34].

For any $\alpha \in K$, the multiplication map $\mathcal{M} : K \to K$ given by $\mathcal{M}(x) = \alpha x$ is a $\mathbb{Q}$-linear map. The field norm of α, denoted by $N_{K/\mathbb{Q}}(\alpha)$, is the determinant of $\mathcal{M}$,

as a $\mathbb{Q}$-linear map. For a non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, the ideal norm of $\mathfrak{a}$, also denoted $N_{K/\mathbb{Q}}(\mathfrak{a})$, is the index $[\mathcal{O}_K : \mathfrak{a}]$.

For $\alpha_1, \ldots, \alpha_k \in K$, define the *denominator ideal*

$$\mathfrak{D}_{\alpha_1,\ldots,\alpha_k;K} := \{x \in \mathcal{O}_K : x\alpha_i \in \mathcal{O}_K \text{ for all } i = 1, \ldots, k\}.$$

Equivalently, $\mathfrak{D}_{\alpha_1,\ldots,\alpha_k;K} = \mathcal{O}_K \cap \alpha_1^{-1}\mathcal{O}_K \cap \cdots \cap \alpha_k^{-1}\mathcal{O}_K$. Such ideals have been studied before, for example in [43].

For algebraic numbers $\alpha_1, \ldots, \alpha_k$, we recall the definition of $H(\alpha_1, \ldots, \alpha_k)$, first defined in Chapter 6.

Definition 7.3.1. Let $\alpha_1, \ldots, \alpha_k \in K = \mathbb{Q}[\alpha_1, \ldots, \alpha_k]$. Define the quantity

$$H(\alpha_1, \ldots, \alpha_k) := N_{K/\mathbb{Q}}(\mathfrak{D}_{\alpha_1,\ldots,\alpha_k;K}) \prod_{i=1}^{d} (1 + |\sigma_i(\alpha_1)| + |\sigma_i(\alpha_2)| + \cdots + |\sigma_i(\alpha_k)|).$$

The following result gives an alternative way to compute the norm of the denominator ideal.

Theorem 7.3.2. *Let $\alpha_1, \ldots, \alpha_k \in K$ for some number field K. Consider the polynomial*

$$F(x_0, \ldots, x_k) := N_{K/\mathbb{Q}}(x_0 + x_1\alpha_1 + \ldots + x_k\alpha_k) \in \mathbb{Q}[x_0, x_1, \ldots, x_k].$$

Let $D > 0$ be the smallest positive integer such that DF has integer coefficients. Then $D = N_{K/\mathbb{Q}}(\mathfrak{D}_{\alpha_1,\ldots,\alpha_k;K})$.

To prove this, we require the following variant of Gauss's Lemma over the ring of integers. We first define the content of a polynomial with coefficients in K.

Definition 7.3.3. Let $F(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$. Define the *content* of F, denoted $\mathrm{cont}_K(F)$, to be the fractional ideal $a_0\mathcal{O}_K + a_1\mathcal{O}_K + \cdots + a_n\mathcal{O}_K \subseteq K$. If it is clear from context, we omit the subscript and simply write $\mathrm{cont}(F)$.

If $F \in \mathbb{Z}[x]$, then $\mathrm{cont}_{\mathbb{Q}}(F) = c\mathbb{Z}$, where $c \in \mathbb{Z}$ is the usual content of F as used in the usual Gauss's Lemma.

If $K \leq L$ is a field extension and $F \in K[x]$, then $\mathrm{cont}_L(F) = \mathrm{cont}_K(F) \cdot \mathcal{O}_L$. In particular, if $F \in \mathbb{Q}[x]$, then $\mathrm{cont}_K(F) = \mathrm{cont}_{\mathbb{Q}}(F) \cdot \mathcal{O}_K$.

Theorem 7.3.4 (Gauss's Lemma over O_K)**.** *Let $F, G \in K[x]$ be two polynomials. Then* $\mathrm{cont}(FG) = \mathrm{cont}(F)\,\mathrm{cont}(G)$.

Proof. Let $F(x) = a_0 + a_1x + \cdots + a_nx^n$ and $G(x) = b_0 + b_1x + \cdots + b_mx^m$. Then their product $F(x)G(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$ has coefficients $c_j = a_0b_j + a_1b_{j-1} + \cdots + a_jb_0$. It is clear that $\mathrm{cont}(FG) \subseteq \mathrm{cont}(F)\,\mathrm{cont}(G)$. To show that $\mathrm{cont}(FG) \supseteq \mathrm{cont}(F)\,\mathrm{cont}(G)$, it suffices to show for any prime ideal $\mathfrak{p} \subseteq O_K$, $\nu_\mathfrak{p}(\mathrm{cont}(FG)) \leq \nu_\mathfrak{p}(\mathrm{cont}(F)) + \nu_\mathfrak{p}(\mathrm{cont}(G))$.

Suppose $\nu_\mathfrak{p}(\mathrm{cont}(F)) = s$ and $\nu_\mathfrak{p}(\mathrm{cont}(G)) = t$. Since

$$\nu_\mathfrak{p}(\mathrm{cont}(F)) = \min(\nu_\mathfrak{p}(a_0), \ldots, \nu_\mathfrak{p}(a_n)),$$

there exists an index k such that $\nu_\mathfrak{p}(a_k) = s$. Let k be the smallest such index, so that $\nu_\mathfrak{p}(a_j) \geq s+1$ for $j = 0, \ldots, k-1$. Similarly, let l be the smallest index such that $\nu_\mathfrak{p}(b_l) = t$, so that $\nu_\mathfrak{p}(b_j) \geq t+1$ for $j = 0, \ldots, l-1$.

Consider the coefficient $c_{k+l} = \sum_{j=0}^{k+l} a_jb_{k+l-j}$. For $j = k$, the term a_kb_l satisfies $\nu_\mathfrak{p}(a_kb_l) = \nu_\mathfrak{p}(a_k) + \nu_\mathfrak{p}(b_l) = s+t$. For every other $j \neq k$, either $j < k$ (for which $\nu_\mathfrak{p}(a_j) \geq s+1$) or $j > k$ (for which $\nu_\mathfrak{p}(b_{k+l-j}) \geq t+1$). In either case, we have $\nu_\mathfrak{p}(a_kb_l) \geq s+t+1$. Therefore, $\nu_\mathfrak{p}(c_{k+l}) = s+t$, so we have $\nu_\mathfrak{p}(\mathrm{cont}(FG)) \leq s+t$ as required. □

Observe that we may define content for multivariate polynomials $F \in K[x_0, \ldots, x_k]$ and our Gauss's Lemma also holds for multivariate polynomials. Indeed, the set of coefficients for $F(x_0, \ldots, x_k)$ is the same as for $F(x, x^{N_1}, \ldots, x^{N_k})$ for sufficiently large $N_k \gg N_{k-1} \gg \cdots \gg N_1 \gg 1$. Thus, the content of F is the same as the content of $F(x, x^{N_1}, \ldots, x^{N_k})$, so we may apply the univariate case.

Proof of Theorem 7.3.2. Let $\sigma_1, \ldots, \sigma_d : K \to \mathbb{C}$ be the complex embeddings of K, with σ_1 being the identity. Set $\mathfrak{D} = \mathfrak{D}_{\alpha_1,\ldots,\alpha_k;K}$. Then

$$F(x_0, \ldots, x_k) = N_{K/\mathbb{Q}}(x_0 + x_1\alpha_1 + \ldots + x_k\alpha_k) = \prod_{i=1}^{d}(x_0 + x_1\sigma_i(\alpha_1) + \cdots + x_k\sigma_i(\alpha_k)).$$

Let $K' \subseteq \mathbb{C}$ be the smallest field containing $\sigma_1(K), \ldots, \sigma_d(K)$, that is, K' is the normal closure of K over $\mathbb{Q}$. By definition, $D^{-1}\mathbb{Z} = \mathrm{cont}_\mathbb{Q}(F)$, so we have $\mathrm{cont}_{K'}(F) = D^{-1}O_{K'}$. On the other hand, by Lemma 7.3.4,

$$\mathrm{cont}_{K'}(F) = \prod_i \mathrm{cont}_{K'}(x_0 + x_1\sigma_i(\alpha_1) + \cdots + x_k\sigma_i(\alpha_k)).$$

But we have

$$\begin{aligned}\mathrm{cont}_{K'}(x_0 + x_1\sigma_i(\alpha_1) + \cdots + x_k\sigma_i(\alpha_k)) &= O_{K'} + \sigma_i(\alpha_1)O_{K'} + \cdots + \sigma_i(\alpha_k)O_{K'} \\ &= \sigma_i(O_{K'} + \alpha_1 O_{K'} + \cdots + \alpha_k O_{K'}) \\ &= \sigma_i(\mathfrak{D}^{-1} \cdot O_{K'}) = \sigma_i(\mathfrak{D})^{-1} \cdot O_{K'}.\end{aligned}$$

Multiplying across all i, we get $\prod_i \sigma_i(\mathfrak{D})^{-1} \cdot O_{K'} = N_{K/\mathbb{Q}}(\mathfrak{D})^{-1} \cdot O_{K'}$, thus $D = N_{K/\mathbb{Q}}(\mathfrak{D})$. □

7.4 Pre-commuting matrices

In general, we do not know the value of $H(\mathcal{L}_0, \ldots, \mathcal{L}_k)$ in Problem 7.0.1. However, we are able to solve the problem completely for the class of pre-commuting linear transformations, defined below.

Definition 7.4.1. We say that $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Q})$ are *pre-commuting* if there is some $\mathcal{P} \in \mathrm{GL}_d(\mathbb{Q})$ such that $\mathcal{P}\mathcal{L}_0, \ldots, \mathcal{P}\mathcal{L}_k$ pairwise commute.

For example, given algebraic numbers $\lambda_1, \ldots, \lambda_k$, the linear maps $\mathcal{L}_0, \ldots, \mathcal{L}_k$ obtained from Chapter 6, Section 6.1 are pre-commuting. Indeed, $\mathcal{L}_0^{-1}\mathcal{L}_l = \mathcal{M}_l$ are pairwise commuting, since they are equivalent to the map given by multiplication by λ_l.

We remark that if there are only two linear transformations $\mathcal{L}_0, \mathcal{L}_1$, then pre-commuting is a weak condition. Indeed, if $\mathcal{L}_0$ is non-singular (which holds if $\mathcal{L}_0, \mathcal{L}_1$ are irreducible), then $\mathcal{L}_0, \mathcal{L}_1$ are pre-commuting, since $\mathcal{L}_0^{-1}\mathcal{L}_0 = I$ and $\mathcal{L}_0^{-1}\mathcal{L}_1$ commute.

For pre-commuting matrices, the converses of Lemma 7.2.1 are true.

Theorem 7.4.2. *Suppose $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are pre-commuting. Let F be the polynomial defined in (7.1). Then, the following holds.*

1. *F is irreducible if and only if $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are irreducible.*
2. *The coefficients of F are coprime if and only if $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are coprime.*

We also have the following characterization of pre-commutative, irreducible, coprime matrices. Roughly speaking, it says that if $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible, coprime and pre-commuting, then they arise from some algebraic numbers $\lambda_1, \ldots, \lambda_k$.

Theorem 7.4.3. *Suppose $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are non-zero, pre-commuting, irreducible and coprime. Then there exists a number field K with $\deg(K/\mathbb{Q}) = d$ and $\lambda_1, \ldots, \lambda_k \in K$, together with an isomorphism $\Psi : K \to \mathbb{Q}^d$ such that $|\det(\mathcal{L}_0)| = N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda_1,\ldots,\lambda_k;K})$ and for all $u \in \mathbb{Q}^d$ and $l = 1, \ldots, k$,*

$$\mathcal{L}_0^{-1}\mathcal{L}_l(u) = \Psi(\lambda_l \cdot \Psi^{-1}(u)).$$

Before proving these results, we prove some general results about commuting matrices. The following folklore result (see, for example, [24, Corollary 2.4.6.4]) says that pairwise-commuting maps are simultaneously upper-triangularizable. For a vector space V over a field K, denote by $\mathrm{End}_K(V)$ the space of K-linear maps $V \to V$. If the field is clear in context, we omit the subscript and simply write $\mathrm{End}(V)$.

Theorem 7.4.4. *Let V be a d-dimensional complex vector space. Let $\mathcal{L}_1, \ldots, \mathcal{L}_k \in \mathrm{End}(V)$ be pairwise-commuting matrices. Then, there is a basis $B = \{v_1, \ldots, v_d\}$ of V such that for $l = 1, \ldots, k$, $\mathcal{L}_l$ is represented by an upper-triangular matrix with respect to B. In particular, v_1 is a common eigenvector.*

This gives the following about pre-commuting matrices.

Lemma 7.4.5. *If $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Q})$ are pre-commuting and F is defined as in (7.1), then F factorizes over $\mathbb{C}$ into linear terms*

$$F(x_0, \ldots, x_k) = \prod_{i=1}^{d} (a_{0i}x_0 + \cdots + a_{ki}x_k)$$

for some $a_{li} \in \mathbb{C}$.

Proof. Let $\mathcal{P} \in \mathrm{GL}_d(\mathbb{Q})$ be such that $\mathcal{P}\mathcal{L}_0, \ldots, \mathcal{P}\mathcal{L}_k$ pairwise commute. By Theorem 7.4.4, we may pick a basis such that the matrices $\mathcal{P}\mathcal{L}_l$ are simultaneously upper triangular, say $\mathcal{M}_0, \ldots, \mathcal{M}_k \in \mathrm{Mat}_d(\mathbb{C})$. Let the diagonal entries of $\mathcal{M}_l$ be $a_{l1}, \ldots, a_{ld}$. Then,

$$\begin{aligned} F &= \frac{1}{\det \mathcal{P}} \det(x_0\mathcal{P}\mathcal{L}_0 + \cdots + x_k\mathcal{P}\mathcal{L}_k) \\ &= \frac{1}{\det \mathcal{P}} \det(x_0\mathcal{M}_0 + \cdots + x_k\mathcal{M}_k) \\ &= \frac{1}{\det \mathcal{P}} \prod_{i=1}^{d} (a_{0i}x_0 + \cdots + a_{ki}x_k). \end{aligned}$$

The lemma follows by absorbing $\frac{1}{\det \mathcal{P}}$ into one of the linear terms. □

In general, commuting matrices may not be simultaneously diagonalizable. However, we can always decompose the space into simultaneous generalized eigenspaces.

Definition 7.4.6. Let V be a finite dimensional complex vector space and $\mathcal{L}_1, \ldots, \mathcal{L}_k$ be linear maps in $\mathrm{End}(V)$. For $\overline{\lambda} = (\lambda_1, \ldots, \lambda_k) \in \mathbb{C}^k$, the *simultaneous generalized $\overline{\lambda}$-eigenspace* $E_{\overline{\lambda}}$ is the subspace of vectors $v \in V$ such that for $l = 1, \ldots, k$, there exists a positive integer m such that $(\mathcal{L}_l - \lambda_l I)^m v = 0$.

Theorem 7.4.7 ([24, Corollary 2.4.6.4])**.** *Let V be a finite dimensional complex vector space and $\mathcal{L}_1, \ldots, \mathcal{L}_k \in \mathrm{End}(V)$ be pairwise-commuting. Then, V can be decomposed into simultaneous generalized eigenspaces. In other words, there is a finite $\Lambda \subset \mathbb{C}^k$ such that for each $\overline{\lambda} \in \Lambda$, the simultaneous generalized eigenspace $E_{\overline{\lambda}}$ are non-trivial and we have the decomposition*

$$V = \bigoplus_{\overline{\lambda} \in \Lambda} E_{\overline{\lambda}}.$$

Let $\mathcal{L}_0, \ldots, \mathcal{L}_k$ be pairwise-commuting, then there exists a basis for which they are simultaneously upper-triangular. If $\mathcal{L}_0, \ldots, \mathcal{L}_k$ have rational entries, we do not expect the entries of the upper-triangular matrices to be rational in general. Nevertheless, we have the following structural result about pairwise-commuting matrices with rational coefficients, which roughly says that they must come from upper-triangular matrices over some number field K.

Theorem 7.4.8. *Let $\mathcal{L}_1, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Q})$ be pairwise-commuting. Then, there is a positive integer r, number fields $K_1, \ldots, K_r$, positive integers $e_1, \ldots, e_r$, and a $\mathbb{Q}$-isomorphism $\Psi : \bigoplus_{i=1}^r K_i^{e_i} \to \mathbb{Q}^d$, such that for each $i = 1, \ldots, r$ and $l = 1, \ldots, k$,*

1. *$K_i^{e_i}$ is an invariant subspace of $\Psi^{-1}\mathcal{L}_l\Psi \in \mathrm{End}_{\mathbb{Q}}(\bigoplus_{i=1}^r K_i^{e_i})$;*
2. *the restriction $(\Psi^{-1}\mathcal{L}_l\Psi)|_{K_i^{e_i}} \in \mathrm{End}_{\mathbb{Q}}(K_i^{e_i})$ is in fact in $\mathrm{End}_{K_i}(K_i^{e_i})$;*
3. *there is an upper-triangular matrix $M_l^{(i)} \in \mathrm{Mat}_{e_i}(K_i)$, such that the K_i-linear map $(\Psi^{-1}\mathcal{L}_l\Psi)|_{K_i^{e_i}} \in \mathrm{End}_{K_i}(K_i^{e_i})$ is represented by the matrix $M_l^{(i)}$ with respect to the standard basis of $K_i^{e_i}$;*
4. *there are $\lambda_1^{(i)}, \ldots, \lambda_k^{(i)} \in K_i$ such that $K_i = \mathbb{Q}(\lambda_1^{(i)}, \ldots, \lambda_k^{(i)})$ and the diagonal entries of $M_l^{(i)}$ are all $\lambda_l^{(i)}$.*

Proof. Viewing $\mathcal{L}_1, \ldots, \mathcal{L}_k$ as linear maps on $\mathbb{C}^d$, Theorem 7.4.7 gives us a decomposition $\mathbb{C}^k = \bigoplus_{\overline{\lambda} \in \Lambda} E_{\overline{\lambda}}$ into simultaneous generalized eigenspaces $E_{\overline{\lambda}} \subseteq \mathbb{C}^k$.

Let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ be any automorphism of $\mathbb{C}$ over $\mathbb{Q}$. Let $\overline{\lambda} = (\lambda_1, \ldots, \lambda_k) \in \Lambda$ and $v \in E_{\overline{\lambda}}$ be any vector. Then for each $l = 1, \ldots, k$, there is a positive integer m such that $(\mathcal{L}_l - \lambda_l I)^m v = 0$. Then we have

$$0 = \sigma((\mathcal{L}_l - \lambda_l I)^m v) = (\mathcal{L}_l - \sigma(\lambda_l))^m \sigma(v).$$

Therefore, $\sigma(\overline{\lambda}) \in \Lambda$ and $\sigma(v) \in E_{\sigma(\overline{\lambda})}$. It follows that Λ is closed under σ and $\sigma(E_{\overline{\lambda}}) = E_{\sigma(\overline{\lambda})}$, so Λ can be partitioned into orbits under the action of $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$. Denote by $\Lambda(\overline{\lambda})$ the orbit containing $\overline{\lambda}$, and let $\Lambda^* \subseteq \Lambda$ be any collection of orbit representatives. In particular, we have the partition $\Lambda = \bigsqcup_{\overline{\lambda} \in \Lambda^*} \Lambda(\overline{\lambda})$.

Let $\Lambda^* = \left\{\overline{\lambda}^{(1)}, \overline{\lambda}^{(2)}, \ldots, \overline{\lambda}^{(r)}\right\}$. For $i = 1, \ldots, r$, let $K_i = \mathbb{Q}(\lambda_1^{(i)}, \ldots, \lambda_k^{(i)})$ and $e_i = \dim_{\mathbb{C}} E_{\overline{\lambda}^{(i)}}$. Let $d_i = \deg(K_i/\mathbb{Q})$, then there are exactly d_i different field embeddings $\sigma : K_i \to \mathbb{C}$, each determined by the image $\sigma(\overline{\lambda}^{(r)})$. Therefore, $|\Lambda(\overline{\lambda}^{(r)})| = d_i$. Define the subspace of $\mathbb{C}^d$

$$E_i := \bigoplus_{\overline{\lambda} \in \Lambda(\overline{\lambda}^{(i)})} E_{\overline{\lambda}},$$

then $\dim_{\mathbb{C}} E_i = d_i e_i$. We also have the $(\mathcal{L}_1, \ldots, \mathcal{L}_k)$-invariant decomposition

$$\mathbb{C}^d = \bigoplus_{i=1}^{r} E_i,$$

so that $d = d_1 e_1 + \cdots + d_r e_r$.

By Theorem 7.4.4, we can find a basis $B_i = \left\{v_1^{(i)}, \ldots, v_{e_i}^{(i)}\right\}$ of $E_{\overline{\lambda}^{(i)}}$ such that for $l = 1, \ldots, k$, the restriction $\mathcal{L}_l|_{E_{\overline{\lambda}^{(i)}}}$ is given by an upper-triangular matrix $M_l^{(i)} \in \mathrm{Mat}_{e_i}(\mathbb{C})$ with respect to B_i. Since $K_i = \mathbb{Q}(\overline{\lambda}^{(i)})$, we may even assume that $B_i \subset K_i^d$ and $M_l^{(i)} \in \mathrm{Mat}_{e_i}(K_i)$. Since the $\mathcal{L}_l$'s commute, so do the $M_l^{(i)}$'s. Note that $M_l^{(i)}$ has $\lambda_l^{(i)}$ along the whole diagonal. In particular, its top left entry is $\lambda_l^{(i)}$. Therefore K_i is generated by the top left entries of $M_1^{(i)}, \ldots, M_k^{(i)}$, proving (4) in the theorem.

Let $\sigma_1, \ldots, \sigma_{d_i} : K_i \to \mathbb{C}$ be all the field embeddings of K_i into $\mathbb{C}$. Since $B_i \subset K_i^d$ is a basis for $E_{\overline{\lambda}^{(i)}}$, for each $j = 1, \ldots, d_i$, $\sigma_j(B_i) \subset \sigma_j(K_i)^d$ is a basis for $E_{\sigma_j(\overline{\lambda}^{(i)})}$. Furthermore, the restriction $\mathcal{L}_l|_{E_{\sigma_j(\overline{\lambda}^{(i)})}}$ is given by the upper-triangular

matrix $\sigma_j(M_l^{(i)}) \in \mathrm{Mat}_{e_i}(\sigma_j(K_i))$ with respect to $\sigma_j(B_i)$. Therefore, the union $B = \bigcup_{j=1}^{d_i} \sigma_j(B_i)$ is a basis for

$$\bigoplus_{j=1}^{d_i} E_{\sigma_j(\overline{\lambda}^{(i)})} = E_i.$$

Claim 7.4.9. $\dim_{\mathbb{Q}}(E_i \cap \mathbb{Q}^d) = d_i e_i$.

Proof. Let $\alpha \in K_i$ be a generator, i.e., $K_i = \mathbb{Q}(\alpha)$. Then, $\sigma_1(\alpha), \ldots, \sigma_{d_i}(\alpha)$ are all distinct. For $m = 1, \ldots, e_i$ and $j = 1, \ldots, d_i$, define the vector

$$u_{mj} := \sigma_1(\alpha^{j-1} v_m^{(i)}) + \sigma_2(\alpha^{j-1} v_m^{(i)}) + \cdots + \sigma_{d_i}(\alpha^{j-1} v_m^{(i)}) \in \mathbb{C}^d.$$

We see that u_{mj} is a $\mathbb{C}$-linear combination of vectors in E_i, thus $u_{mj} \in E_i$. On the other hand, we can write $u_{mj} = \mathrm{Tr}_{K_i/\mathbb{Q}}(\alpha^{j-1} v_m^{(i)}) \in \mathbb{Q}^d$, thus $u_{mj} \in E_i \cap \mathbb{Q}^d$. It suffices to show that the vectors u_{mj} form a basis for $E_i \cap \mathbb{Q}^d$. To this end, we show that each $\sigma_j(v_m^{(i)})$ can be written as a $\mathbb{C}$-linear combination of the u_{mj}'s.

We can express the u_{mj}'s in the following way. Fix an m. Then, viewing u_{mj} and $\sigma_j(v_m^{(i)})$ as column vectors, we have the following identity of $d \times d_i$ matrices

$$\begin{pmatrix} u_{m1} & \cdots & u_{md_i} \end{pmatrix} = \begin{pmatrix} \sigma_1(v_m^{(i)}) & \cdots & \sigma_{d_i}(v_m^{(i)}) \end{pmatrix} \begin{pmatrix} \sigma_1(1) & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha^{d_i-1}) \\ \sigma_2(1) & \sigma_2(\alpha) & \cdots & \sigma_2(\alpha^{d_i-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{d_i}(1) & \sigma_{d_i}(\alpha) & \cdots & \sigma_{d_i}(\alpha^{d_i-1}) \end{pmatrix}.$$

Note that the Vandermonde matrix

$$S = \begin{pmatrix} \sigma_1(1) & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha^{d_i-1}) \\ \sigma_2(1) & \sigma_2(\alpha) & \cdots & \sigma_2(\alpha^{d_i-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{d_i}(1) & \sigma_{d_i}(\alpha) & \cdots & \sigma_{d_i}(\alpha^{d_i-1}) \end{pmatrix}$$

has non-zero determinant, hence is invertible. Thus, we have

$$\begin{pmatrix} u_{m1} & \cdots & u_{md_i} \end{pmatrix} S^{-1} = \begin{pmatrix} \sigma_1(v_m^{(i)}) & \cdots & \sigma_{d_i}(v_m^{(i)}) \end{pmatrix}.$$

This shows that each $\sigma_j(v_m^{(i)})$ can be expressed as a $\mathbb{C}$-linear combination of the u_{mj}'s, as desired.

□

From the claim, we have a $(\mathcal{L}_1, \ldots, \mathcal{L}_k)$-invariant decomposition

$$\mathbb{Q}^d = \bigoplus_{i=1}^{r} (E_i \cap \mathbb{Q}^d).$$

By focusing on each subspace $E_i \cap \mathbb{Q}^d$, we may assume that $r = 1$.

We will now define the $\mathbb{Q}$-isomorphism $\Psi : K_1^{e_1} \to \mathbb{Q}^d$. First observe that $d = e_1 d_1$, so the dimensions match. Let $x_1, \ldots, x_{e_1}$ be the standard basis for $K_1^{e_1}$. Note that for $l = 1, \ldots, k$, the upper-triangular matrix $M_l^{(1)} \in \mathrm{Mat}_{e_1}(K_1)$ has diagonal entries all $\lambda_l^{(1)}$. Since $\lambda_1^{(1)}, \ldots, \lambda_k^{(1)}$ generate K_1, it follows that any $v \in K_1^{e_1}$ can be written in the form

$$v = P_1(M_1^{(1)}, \ldots, M_k^{(1)})x_1 + \cdots + P_{e_1}(M_1^{(1)}, \ldots, M_k^{(1)})x_{e_1},$$

for some polynomials $P_1, \ldots, P_{e_1}$ in k variables and rational coefficients.

For $m = 1, \ldots, e_1$, let $u_m = \sigma_1(v_m^{(1)}) + \sigma_2(v_m^{(1)}) + \cdots + \sigma_{d_1}(v_m^{(1)})$. From the proof of the claim, we have $u_m \in \mathbb{Q}^d$. Define Ψ by setting

$$\Psi(v) = P_1(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_1 + \cdots + P_{e_1}(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_{e_1}.$$

Claim 7.4.10. *Ψ is well-defined and is an isomorphism.*

Proof. We first show that Ψ is well-defined. Suppose we have two different representations of v,

$$\begin{aligned} v &= P_1(M_1^{(1)}, \ldots, M_k^{(1)})x_1 + \cdots + P_{e_1}(M_1^{(1)}, \ldots, M_k^{(1)})x_{e_1} \\ &= P_1'(M_1^{(1)}, \ldots, M_k^{(1)})x_1 + \cdots + P_{e_1}'(M_1^{(1)}, \ldots, M_k^{(1)})x_{e_1}. \end{aligned}$$

We wish to show that

$$\begin{aligned} &P_1(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_1 + \cdots + P_{e_1}(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_{e_1} \\ &= P_1'(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_1 + \cdots + P_{e_1}'(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_{e_1}. \end{aligned}$$

Without loss of generality, suppose that σ_1 is the identity. For $j = 1, \ldots, d_1$, let π_j be the projection

$$\pi_j : \mathbb{C}^d = \bigoplus_{j'=1}^{d_1} E_{\sigma_{j'}(\overline{\lambda}^{(1)})} \to E_{\sigma_j(\overline{\lambda}^{(1)})}.$$

Note that π_j commutes with $\mathcal{L}_1, \ldots, \mathcal{L}_k$, since their simultaneous generalized eigenspaces are $(\mathcal{L}_1, \ldots, \mathcal{L}_k)$-invariant. Recall that in $E_{\sigma_j(\overline{\lambda}^{(1)})}$, we have a basis $\sigma_j(B_1)$ such that $\mathcal{L}_l$ is represented by the matrix $\sigma_j(M_l^{(1)})$. In other words, for

any polynomial P in k variables and rational coefficients, for any $m = 1, \ldots, e_1$, the vector $P(\mathcal{L}_1, \ldots, \mathcal{L}_k)\sigma_j(v_m^{(1)})$ is represented by $P(\sigma_j(M_1^{(1)}), \ldots, \sigma_j(M_k^{(1)}))x_m$ with respect to $\sigma_j(B_1)$. Therefore,

$$\begin{aligned}
&\pi_j(P_1(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_1 + \cdots + P_{e_1}(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_{e_1}) \\
&= P_1(\mathcal{L}_1, \ldots, \mathcal{L}_k)\pi_j(u_1) + \cdots + P_{e_1}(\mathcal{L}_1, \ldots, \mathcal{L}_k)\pi_j(u_{e_1}) \\
&= P_1(\mathcal{L}_1, \ldots, \mathcal{L}_k)\sigma_j(v_1^{(1)}) + \cdots + P_{e_1}(\mathcal{L}_1, \ldots, \mathcal{L}_k)\sigma_j(v_{e_1}^{(1)}).
\end{aligned}$$

With respect to the basis $\sigma_j(B_1)$, the above is represented by

$$\begin{aligned}
&P_1(\sigma_j(M_1^{(1)}), \ldots, \sigma_j(M_k^{(1)}))x_1 + \cdots + P_{e_1}(\sigma_j(M_1^{(1)}), \ldots, \sigma_j(M_k^{(1)}))x_{e_1} \\
&= \sigma_j(P_1(M_1^{(1)}, \ldots, M_k^{(1)})x_1 + \cdots + P_{e_1}(M_1^{(1)}, \ldots, M_k^{(1)})x_{e_1}) \\
&= \sigma_j(P_1'(M_1^{(1)}, \ldots, M_k^{(1)})x_1 + \cdots + P_{e_1}'(M_1^{(1)}, \ldots, M_k^{(1)})x_{e_1}).
\end{aligned}$$

It follows that

$$\begin{aligned}
&\pi_j(P_1(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_1 + \cdots + P_{e_1}(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_{e_1}) \\
&= \pi_j(P_1'(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_1 + \cdots + P_{e_1}'(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_{e_1}).
\end{aligned}$$

Since this holds for all j, we have

$$\begin{aligned}
&P_1(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_1 + \cdots + P_{e_1}(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_{e_1} \\
&= P_1'(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_1 + \cdots + P_{e_1}'(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_{e_1}.
\end{aligned}$$

This proves that Ψ is well-defined.

Next, we show that Ψ is an isomorphism. It is not hard to see that Ψ is $\mathbb{Q}$-linear. Since the dimensions of $\mathbb{Q}^d$ and $K_1^{e_1}$ agree, it suffices to show that Ψ has trivial kernel. Indeed, suppose that for some $v = P_1(M_1^{(1)}, \ldots, M_k^{(1)})x_1 + \cdots + P_{e_1}(M_1^{(1)}, \ldots, M_k^{(1)})x_{e_1}$, we have $P_1(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_1 + \cdots + P_{e_1}(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_{e_1} = 0$. From the arguments above, this implies that for each $j = 1, \ldots, d_1$, we have

$$\pi_j(P_1(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_1 + \cdots + P_{e_1}(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_{e_1}) = 0.$$

This shows that $P_1(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_1 + \cdots + P_{e_1}(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_{e_1} = 0$. Therefore, Ψ is injective, hence an isomorphism. □

To finish the theorem, it suffices to show that:

1. $\Psi^{-1}\mathcal{L}_l\Psi \in \mathrm{End}_{K_1}(K_1^{e_1})$;

2. $\Psi^{-1}\mathcal{L}_l\Psi$ is represented by $M_l^{(1)}$ with respect to the standard basis of $K_1^{e_1}$.

To this end, it suffices to show that for any $v \in K_1^{e_1}$, we have $\Psi^{-1}\mathcal{L}_l\Psi(v) = M_l^{(1)}v$.

Write v in the form

$$v = P_1(M_1^{(1)}, \ldots, M_k^{(1)})x_1 + \cdots + P_{e_1}(M_1^{(1)}, \ldots, M_k^{(1)})x_{e_1}.$$

For $m = 1, \ldots, e_1$, let P'_m be the polynomial $P'_m(z_1, \ldots, z_k) = z_l P_m(z_1, \ldots, z_k)$. Then, we have

$$\begin{aligned}
\Psi^{-1}\mathcal{L}_l\Psi(v) &= \Psi^{-1}\mathcal{L}_l\Psi(P_1(M_1^{(1)}, \ldots, M_k^{(1)})x_1 + \cdots + P_{e_1}(M_1^{(1)}, \ldots, M_k^{(1)})x_{e_1}) \\
&= \Psi^{-1}\mathcal{L}_l(P_1(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_1 + \cdots + P_{e_1}(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_{e_1}) \\
&= \Psi^{-1}(P'_1(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_1 + \cdots + P'_{e_1}(\mathcal{L}_1, \ldots, \mathcal{L}_k)u_{e_1}) \\
&= P'_1(M_1^{(1)}, \ldots, M_k^{(1)})x_1 + \cdots + P'_{e_1}(M_1^{(1)}, \ldots, M_k^{(1)})x_{e_1} \\
&= M_l^{(1)}(P_1(M_1^{(1)}, \ldots, M_k^{(1)})x_1 + \cdots + P_{e_1}(M_1^{(1)}, \ldots, M_k^{(1)})x_{e_1}) \\
&= M_l^{(1)}v.
\end{aligned}$$

□

If in addition, $\mathcal{L}_1, \ldots, \mathcal{L}_k$ have no non-trivial common invariant subspace, then we can say a lot more about their structure. Roughly speaking, this says that $\mathcal{L}_1, \ldots, \mathcal{L}_k$ are similar to multiplication by algebraic numbers.

Lemma 7.4.11. *Let $\mathcal{L}_1, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Q})$ be pairwise-commuting and have no non-trivial common invariant subspace. Then, there is a number field K of degree d, algebraic numbers $\lambda_1, \ldots, \lambda_k \in K$ and a $\mathbb{Q}$-isomorphism $\Psi : K \to \mathbb{Q}^d$ such that*

1. *$K = \mathbb{Q}(\lambda_1, \ldots, \lambda_k)$;*
2. *for $l = 1, \ldots, k$, the map $\Psi^{-1}\mathcal{L}_l\Psi : K \to K$ is given by multiplication by λ_l.*

Proof. By Theorem 7.4.8, there is a $(\mathcal{L}_1, \ldots, \mathcal{L}_k)$-invariant decomposition

$$\mathbb{Q}^d \cong \bigoplus_{i=1}^{r} K_i^{e_i}.$$

Since $\mathcal{L}_0, \ldots, \mathcal{L}_k$ have no non-trivial common invariant subspace, $r = 1$. So we have an isomorphism $\Psi : K^e \to \mathbb{Q}^d$ for some number field K and positive integer

e. For $l = 1, \ldots, k$, let $M_l = \Psi^{-1}\mathcal{P}\mathcal{L}_l\Psi \in \mathrm{Mat}_e(K)$ be upper-triangular. Then, the subspace $K \times 0^{e-1} \subset K^e$ is M_l-invariant for all l. Thus, $\Psi(K \times 0^{e-1})$ is $\mathcal{L}_l$-invariant. Since $\mathcal{L}_0, \ldots, \mathcal{L}_k$ have no non-trivial common invariant subspace, we must have $e = 1$.

This gives an isomorphism $\Psi : K \to \mathbb{Q}^d$, and the matrices M_l are just single elements $\lambda_l \in K$, so that $\Psi^{-1}\mathcal{L}_l\Psi$ acts on K as multiplication by λ_l. Furthermore, by Theorem 7.4.8(4), $K = \mathbb{Q}(\lambda_1, \ldots, \lambda_k)$. □

We now prove the first part of Theorem 7.4.2, which can be stated as follows.

Lemma 7.4.12. *Suppose $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are pre-commuting and F is defined as in (7.1). Then F is irreducible over $\mathbb{Q}$ if and only if $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are irreducible.*

Proof. The forward direction is already proven in Lemma 7.2.1, so we only have to prove the reverse direction. Assume that $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are irreducible.

Let $\mathcal{P} \in \mathrm{GL}_d(\mathbb{Q})$ be such that $\mathcal{P}\mathcal{L}_0, \ldots, \mathcal{P}\mathcal{L}_k$ are pairwise commuting. Since $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are irreducible, $\mathcal{P}\mathcal{L}_0, \ldots, \mathcal{P}\mathcal{L}_k$ have no non-trivial common invariant subspace. By Lemma 7.4.11, there is a number field K of degree d, algebraic numbers $\lambda_0, \ldots, \lambda_k \in K$ and a $\mathbb{Q}$-isomorphism $\Psi : K \to \mathbb{Q}^d$ such that

1. $K = \mathbb{Q}(\lambda_0, \ldots, \lambda_k)$;
2. for $l = 0, \ldots, k$, the map $\Psi^{-1}\mathcal{P}\mathcal{L}_l\Psi : K \to K$ is given by multiplication by λ_l.

We have

$$\begin{aligned} F(x_0, \ldots, x_k) &= \det(x_0\mathcal{L}_0 + \cdots + x_k\mathcal{L}_k) \\ &= \frac{1}{\det \mathcal{P}} \det(x_0\mathcal{P}\mathcal{L}_0 + \cdots + x_k\mathcal{P}\mathcal{L}_k) \\ &= \frac{1}{\det \mathcal{P}} N_{K/\mathbb{Q}}(x_0\lambda_0 + \cdots + x_k\lambda_k) \\ &= \frac{1}{\det \mathcal{P}} \prod_{i=1}^{d} (x_0\sigma_i(\lambda_0) + \cdots + x_k\sigma_i(\lambda_k)), \end{aligned}$$

where $\sigma_1, \ldots, \sigma_d : K \to \mathbb{C}$ are all the field embeddings of K into $\mathbb{C}$.

Suppose F is reducible into $F = GH$. Then, one of G or H, say G, contains the linear factor $(x_0\lambda_0 + \cdots + x_k\lambda_k)$. Since G has rational coefficients, it must also contain the factors $\sigma_i(x_0\lambda_0 + \cdots + x_k\lambda_k) = x_0\sigma_i(\lambda_0) + \cdots + x_k\sigma_i(\lambda_k)$ for $i = 1, \ldots, d$.

Recall that K is generated by $\lambda_0, \ldots, \lambda_k$, thus the tuples $(\sigma_i(\lambda_0), \ldots, \sigma_i(\lambda_k))$ are distinct for $i = 1, \ldots, d$. Therefore, G contains all the factors of F, contradicting the irreducibility of F.

□

Next, we prove Theorem 7.4.3. We leave the second part of Theorem 7.4.2 for last since it is the trickiest.

Proof of Theorem 7.4.3. Let $\mathcal{P} \in \mathrm{GL}_d(\mathbb{Q})$ be such that $\mathcal{P}\mathcal{L}_0, \ldots, \mathcal{P}\mathcal{L}_k$ are pairwise commuting. Since $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are irreducible, $\mathcal{P}\mathcal{L}_0, \ldots, \mathcal{P}\mathcal{L}_k$ have no non-trivial common invariant subspace. Let $K, \lambda_0, \ldots, \lambda_k, \Psi$ be as in the conclusion of Lemma 7.4.11.

Since all of the $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are non-zero, all of the $\lambda_0, \ldots, \lambda_k$ are non-zero. In particular, $\mathcal{L}_0$ is invertible over $\mathbb{Q}$. Since $I, (\mathcal{P}\mathcal{L}_0)^{-1}\mathcal{P}\mathcal{L}_1, \ldots, (\mathcal{P}\mathcal{L}_0)^{-1}\mathcal{P}\mathcal{L}_k$ are also pairwise-commuting, we may assume without loss of generality that $\mathcal{P} = \mathcal{L}_0^{-1}$. Thus, $\lambda_0 = 1$. By definition of Ψ and $\lambda_1, \ldots, \lambda_k$, we have for all $u \in \mathbb{Q}^d$ and $l = 1, \ldots, k$,

$$\mathcal{L}_0^{-1}\mathcal{L}_l(u) = \Psi(\lambda_l \cdot \Psi^{-1}(u)).$$

It suffices to show that $|\det(\mathcal{L}_0)| = N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda_1,\ldots,\lambda_k;K})$. We have

$$\begin{aligned} F &= \det(x_0\mathcal{L}_0 + \cdots + x_k\mathcal{L}_k) \\ &= \det(\mathcal{L}_0)\det(x_0 + x_1\mathcal{L}_0^{-1}\mathcal{L}_1 + \cdots + x_k\mathcal{L}_0^{-1}\mathcal{L}_k) \\ &= \det(\mathcal{L}_0)N_{K/\mathbb{Q}}(x_0 + x_1\lambda_1 + \cdots + x_k\lambda_k). \end{aligned}$$

Since $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are coprime, F has coprime integer coefficients. By Theorem 7.3.2, $N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda_1,\ldots,\lambda_k;K})$ is the smallest positive integer required to scale $N_{K/\mathbb{Q}}(x_0 + x_1\lambda_1 + \cdots + x_k\lambda_k)$ into an integer polynomial. Thus, $|\det(\mathcal{L}_0)| = N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda_1,\ldots,\lambda_k;K})$.

□

Finally, we prove the second part of Theorem 7.4.2. For a d-dimensional $\mathbb{Q}$-vector space V and d-dimensional lattices $Z_1, Z_2 \subset V$, set $[Z_1 : Z_2] = [Z : Z_2]/[Z : Z_1]$,

where $Z \subset V$ is any lattice containing Z_1, Z_2 (for instance, $Z = Z_1 + Z_2$). We begin with the following lemma.

Lemma 7.4.13. *Let V be a d-dimensional $\mathbb{Q}$-vector space and let $\mathcal{L}_1, \ldots, \mathcal{L}_k \in \mathrm{End}(V)$ be pairwise-commuting. Define the k-variate polynomial*

$$F_V(x_1, \ldots, x_k) = \det(x_1\mathcal{L}_1 + \cdots + x_k\mathcal{L}_k).$$

Let $c = \mathrm{cont}(F_V)$ be the content of F_V.

1. *If $c = 0$, then $\mathcal{L}_1(V) + \cdots + \mathcal{L}_k(V)$ is a stict subspace of V.*
2. *If $c > 0$, then there are d-dimensional lattices $Z_1, Z_2 \subset V$ such that $[Z_1 : Z_2] = c$ and for $l = 1, \ldots, k$, $\mathcal{L}_l(Z_1) \subseteq Z_2$.*

Proof. We induct on d. Suppose V can be decomposed into $U \oplus W$ where $U, W \subset V$ are non-trivial and $(\mathcal{L}_1, \ldots, \mathcal{L}_k)$-invariant. Let F_U, F_W be the corresponding polynomials for the restriction of $\mathcal{L}_1, \ldots, \mathcal{L}_k$ onto U, W, respectively. Then $F_V = F_U F_W$ and $c = \mathrm{cont}(F_U)\,\mathrm{cont}(F_W)$. If $c = 0$, then one of $\mathrm{cont}(F_U)$ or $\mathrm{cont}(F_W)$ is zero, and the lemma follows by our induction hypothesis. Otherwise, $\mathrm{cont}(F_U)\,\mathrm{cont}(F_W) \neq 0$.

By our induction hypothesis, we can find full lattices $X_1, X_2 \subset U$ and $Y_1, Y_2 \subset W$ such that $[X_1 : X_2] = \mathrm{cont}(F_U)$, $[Y_1 : Y_2] = \mathrm{cont}(F_W)$ and for $l = 1, \ldots, k$, $\mathcal{L}_l(X_1) \subseteq X_2$ and $\mathcal{L}_l(Y_1) \subseteq Y_2$. Take $Z_i = X_i \oplus Y_i \subset V$ for $i = 1, 2$. Then, $[Z_1 : Z_2] = [X_1 : X_2][Y_1 : Y_2] = c$ and $\mathcal{L}_l(Z_1) = \mathcal{L}_l(X_1) + \mathcal{L}_l(Y_1) \subseteq X_2 + Y_2 = Z_2$.

Thus, we may assume that V cannot be decomposed into such $U \oplus W$. By Theorem 7.4.8 and the indecomposability of V, there is a number field K, a positive integer e, a $\mathbb{Q}$-isomorphism $\Psi : K^e \to V$, and for each $l = 1, \ldots, k$, an element $\lambda_l \in K$ and an upper-triangular matrix $M_l \in \mathrm{Mat}_e(K)$ with diagonal entries λ_l, satisfying $K = \mathbb{Q}(\lambda_1, \ldots, \lambda_k)$ and for each $v \in K^e$,

$$\Psi^{-1}\mathcal{L}_l\Psi v = M_l v.$$

We have

$$\begin{aligned} F_V &= \det(x_1\mathcal{L}_1 + \cdots + x_k\mathcal{L}_k) \\ &= N_{K/\mathbb{Q}} \det(x_1M_1 + \cdots + x_kM_k) \\ &= N_{K/\mathbb{Q}}(x_1\lambda_1 + \cdots + x_k\lambda_k)^e. \end{aligned}$$

So if $c = 0$, then $\lambda_1 = \cdots = \lambda_k = 0$. Since M_l are upper-triangular with zeros on the diagonal, their images lie in a common strict subspace. Thus, $\mathcal{L}_1(V) + \cdots + \mathcal{L}_k(V)$ is a stict subspace of V.

Otherwise, assume that $c \neq 0$, so that not all λ_l are zero. Let $f = \deg(K/\mathbb{Q})$, then $d = ef$. Let $\mathfrak{b}$ be the fractional ideal $\lambda_1 O_K + \cdots + \lambda_k O_K$. By Theorem 7.3.2, $N_{K/\mathbb{Q}}(\mathfrak{b})$ is equal to the content of the polynomial $N_{K/\mathbb{Q}}(x_1\lambda_1 + \cdots + x_k\lambda_k)$. Thus, $c = N_{K/\mathbb{Q}}(\mathfrak{b})^e$.

We will now define fractional ideals $\mathfrak{a}_e, \ldots, \mathfrak{a}_1$ as inductively. Let $\mathfrak{a}_e = O_K$. Suppose we have defined down to $\mathfrak{a}_{i+1}$ for some $i \geq 1$. To define $\mathfrak{a}_i$, let $\mathfrak{c}_l = (M_l)_{ie}\mathfrak{a}_e + (M_l)_{i(e-1)}\mathfrak{a}_{e-1} + \cdots + (M_l)_{i(i+1)}\mathfrak{a}_{i+1}$. Then, define

$$\mathfrak{a}_i = O_K + \mathfrak{c}_1\mathfrak{b}^{-1} + \cdots + \mathfrak{c}_k\mathfrak{b}^{-1}.$$

From the definition, it is easy to check that for $l = 1, \ldots, k$,

$$M_l(\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_e) \subseteq \mathfrak{a}_1\mathfrak{b} \times \cdots \times \mathfrak{a}_e\mathfrak{b}.$$

Taking $Z_1 = \Psi(\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_e)$ and $Z_2 = \Psi(\mathfrak{a}_1\mathfrak{b} \times \cdots \times \mathfrak{a}_e\mathfrak{b})$, we have $[Z_1 : Z_2] = N_{K/\mathbb{Q}}(\mathfrak{b})^e = c$ and

$$\begin{aligned}\mathcal{L}_l(Z_1) &= \Psi M_l(\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_e)\\ &\subseteq \Psi(\mathfrak{a}_1\mathfrak{b} \times \cdots \times \mathfrak{a}_e\mathfrak{b})\\ &= Z_2.\end{aligned}$$

□

We are now ready to prove the second part of Theorem 7.4.2, which we can state as follows.

Lemma 7.4.14. *Suppose $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are pre-commuting. Then the coefficients of F, defined in (7.1), are coprime if and only if $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are coprime.*

Proof. The forward direction is already proven in Lemma 7.2.1, so we only have to prove the reverse direction. Assume that $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are coprime. Let $\mathcal{P} \in \mathrm{GL}_d(\mathbb{Q})$ be such that $\mathcal{P}\mathcal{L}_0, \ldots, \mathcal{P}\mathcal{L}_k$ are pairwise commuting.

Define

$$\begin{aligned}F'(x_0, \ldots, x_k) &= \det(x_0\mathcal{P}\mathcal{L}_0 + \cdots + x_k\mathcal{P}\mathcal{L}_k) = \det(\mathcal{P})\det(x_0\mathcal{L}_0 + \cdots + x_k\mathcal{L}_k)\\ &= \det(\mathcal{P})F(x_0, \ldots, x_k)\end{aligned}$$

and $c = \mathrm{cont}(F') \geq |\det(\mathcal{P})|$. By Lemma 7.4.13, if $c \neq 0$, we can find full rank lattices $Z_1, Z_2 \subset \mathbb{Q}^d$ such that $[Z_1 : Z_2] = c$ and $\mathcal{P}\mathcal{L}_l(Z_1) \subseteq Z_2$. Let $\mathcal{Q} : \mathbb{Z}^d \to Z_1$ and $\mathcal{R} : Z_2 \to \mathbb{Z}^d$ be arbitrary isomorphisms, which can be viewed as matrices in $\mathrm{GL}_d(\mathbb{Q})$. Then $|\det(\mathcal{Q}\mathcal{R})| = [Z_2 : Z_1] = c^{-1}$ and $\mathcal{R}\mathcal{P}\mathcal{L}_l\mathcal{Q} : \mathbb{Z}^d \to \mathbb{Z}^d$, so they are in $\mathrm{Mat}_d(\mathbb{Z})$. By coprimality of $\mathcal{L}_1, \ldots, \mathcal{L}_k$, we have $1 \leq |\det(\mathcal{Q}\mathcal{P}\mathcal{R})| = |\det(\mathcal{P})|c^{-1}$. Thus, $c \leq |\det(\mathcal{P})|$. But we have $c = \mathrm{cont}(F') \geq |\det(\mathcal{P})|$, so equality holds, therefore F has coprime coefficients.

If $c = 0$, then the images of $\mathcal{P}\mathcal{L}_0, \ldots, \mathcal{P}\mathcal{L}_k$ lie in a strict subspace of $\mathbb{Q}^d$. In particular, we can find full rank lattices $Z_1, Z_2 \subset \mathbb{Q}^d$ such that $[Z_1 : Z_2] = c'$ and $\mathcal{P}\mathcal{L}_l(Z_1) \subseteq Z_2$, for arbitrarily large $c' > 0$. By the same argument above, we have $|\det(\mathcal{P})| \geq c'$, which is absurd since c' can be taken to be arbitrarily large. □

7.5 Sums of pre-commuting linear transformations

Suppose $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are non-zero, pre-commuting, irreducible and coprime, then F, defined in (7.1), factorizes into linear terms

$$F(x_0, \ldots, x_n) = \prod_{i=1}^{d} (a_{0i}x_0 + \cdots + a_{ki}x_k).$$

We define $H(\mathcal{L}_0, \ldots, \mathcal{L}_k)$ as the quantity

$$H(\mathcal{L}_0, \ldots, \mathcal{L}_k) := \prod_{i=1}^{d} (|a_{0i}| + \cdots + |a_{ki}|).$$

Note that the factorization is only unique up to scalars, but the quantity $H(\mathcal{L}_0, \ldots, \mathcal{L}_k)$ is well-defined.

We now prove Theorem 7.0.6, which we state again for the reader's convenience.

Theorem 7.5.1. *Let $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ be pre-commuting, irreducible and coprime matrices. Then for any finite $A \subset \mathbb{Z}^d$,*

$$|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| \geq H(\mathcal{L}_0, \ldots, \mathcal{L}_k)|A| - o(|A|).$$

Proof. We may assume that $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are non-zero. By Theorem 7.4.3, this becomes equivalent to Theorem 6.0.2. The only thing we have to show is that $H(\mathcal{L}_0, \ldots, \mathcal{L}_k) = H(\lambda_1, \ldots, \lambda_k)$. Indeed, if $\mathcal{M}_l : K \to K$ is the homomorphism given by multiplication by λ_l, which is similar to $\mathcal{L}_0^{-1}\mathcal{L}_l$, then we have

$$\begin{aligned} F(x_0,\dots,x_k) &= \det(x_0\mathcal{L}_0+\cdots+x_k\mathcal{L}_k) \\ &= \det(\mathcal{L}_0)\det(x_0+x_1\mathcal{M}_1+\cdots+x_k\mathcal{M}_k) \\ &= \det(\mathcal{L}_0)\prod_{i=1}^{d}(x_0+\sigma_i(\lambda_1)x_1+\cdots+\sigma_i(\lambda_k)x_k). \end{aligned}$$

Therefore,

$$\begin{aligned} H(\mathcal{L}_0,\dots,\mathcal{L}_k) &= |\det(\mathcal{L}_0)|\prod_{i=1}^{d}(1+|\sigma_i(\lambda_1)|+\cdots+|\sigma_i(\lambda_k)|) \\ &= N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda_1,\dots,\lambda_k;K})\prod_{i=1}^{d}(1+|\sigma_i(\lambda_1)|+\cdots+|\sigma_i(\lambda_k)|) \\ &= H(\lambda_1,\dots,\lambda_k). \end{aligned}$$

□

Corollary 7.5.2. *Let $\mathcal{L}_0,\mathcal{L}_1\in \mathrm{Mat}_d(\mathbb{Z})$ be irreducible and coprime. Then for any finite $A\subset\mathbb{Z}^d$,*

$$|\mathcal{L}_0A+\mathcal{L}_1A|\geq H(\mathcal{L}_0,\mathcal{L}_1)|A|-o(|A|).$$

Proof. This follows from the $k=1$ case of Theorem 7.0.6, and noting that if $\mathcal{L}_0,\mathcal{L}_1$ are irreducible, then they are non-singular and hence pre-commuting. □

7.6 An example

Consider the following matrices:

$$\mathcal{L}_0=\begin{pmatrix}0&1&0\\-1&0&0\\0&0&0\end{pmatrix},\quad \mathcal{L}_1=\begin{pmatrix}0&0&1\\0&0&0\\-1&0&0\end{pmatrix},\quad \mathcal{L}_2=\begin{pmatrix}0&0&0\\0&0&1\\0&-1&0\end{pmatrix}.$$

The corresponding polynomial F is the zero polynomial. However, we claim that $\mathcal{L}_0,\mathcal{L}_1,\mathcal{L}_2$ are irreducible and coprime, giving a counter-example to Lemma 7.2.1.

We first show that they are irreducible. If not, then there are non-trivial subspaces $U,V\subset\mathbb{Q}^3$ such that $\mathcal{L}_i(U)\subseteq V$ for all i. Let $u=(a,b,c)\in\mathbb{Q}^3$ be any non-zero vector. Then the span of $\mathcal{L}_0u,\mathcal{L}_1u,\mathcal{L}_2u$ is

$$V_u:=\left\{(x,y,z)\in\mathbb{Q}^3:ax+by+cz=0\right\}.$$

This is a 2-dimensional subspace contained in V, thus $\dim U=\dim V=2$. Moreover, V_u is distinct for different u (up to scalar), so picking $u_1,u_2\in U$ as a basis, the subspaces V_{u_1},V_{u_2} are distinct but are contained in V, so V can only be $\mathbb{Q}^3$.

Suppose $\mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_2$ are not coprime, then there are $\mathcal{P}, \mathcal{Q} \in \mathrm{GL}_3(\mathbb{Q})$ with $0 < |\det \mathcal{P}\mathcal{Q}| < 1$ and $\mathcal{P}\mathcal{L}_i\mathcal{Q} \in \mathrm{Mat}_3(\mathbb{Z})$. There exists invertible $\mathcal{R}_1, \mathcal{R}_2 \in \mathrm{Mat}_3(\mathbb{Z})$ such that $\mathcal{R}_1\mathcal{P}$ is upper triangular and $\mathcal{Q}\mathcal{R}_2$ is lower triangular. Thus by replacing $\mathcal{P}, \mathcal{Q}$ with $\mathcal{R}_1\mathcal{P}, \mathcal{Q}\mathcal{R}_2$, we may assume that $\mathcal{P}, \mathcal{Q}$ are of the form

$$\mathcal{P} = \begin{pmatrix} P_{11} & P_{12} & P_{13} \\ 0 & P_{22} & P_{23} \\ 0 & 0 & P_{33} \end{pmatrix}, \qquad \mathcal{Q} = \begin{pmatrix} Q_{11} & 0 & 0 \\ Q_{21} & Q_{22} & 0 \\ Q_{31} & Q_{32} & Q_{33} \end{pmatrix}.$$

Then $\mathcal{P}\mathcal{L}_i\mathcal{Q}$ is an integer matrix implies that the following matrices have integer entries:

$$\begin{pmatrix} -P_{12}Q_{11} + P_{11}Q_{21} & P_{11}Q_{22} & 0 \\ -P_{22}Q_{11} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} -P_{13}Q_{11} + P_{11}Q_{31} & P_{11}Q_{32} & P_{11}Q_{33} \\ -P_{23}Q_{11} & 0 & 0 \\ -P_{33}Q_{11} & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} -P_{13}Q_{21} + P_{12}Q_{31} & -P_{13}Q_{22} + P_{12}Q_{32} & P_{12}Q_{33} \\ -P_{23}Q_{21} + P_{22}Q_{31} & -P_{23}Q_{22} + P_{22}Q_{32} & P_{22}Q_{33} \\ -P_{33}Q_{21} & P_{33}Q_{22} & 0 \end{pmatrix}.$$

In particular, $P_{11}Q_{22}, P_{22}Q_{33}, P_{33}Q_{11} \in \mathbb{Z}$, hence $P_{11}P_{22}P_{33}Q_{11}Q_{22}Q_{33} \in \mathbb{Z}$. But $0 < |\det \mathcal{P}\mathcal{Q}| = |P_{11}P_{22}P_{33}Q_{11}Q_{22}Q_{33}| < 1$, a contradiction.

We believe that $H(\mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_2) = 8$ in this case, which will be tight by considering A to be an $N \times N \times N$ cube. However, the methods developed in this thesis are insufficient to even prove that it is positive.

Chapter 8

SUMS OF DILATES OVER GROUPS OF PRIME ORDER

Parts of this chapter are based on the author's publications. The materials have been adapted for inclusion in this thesis.

[1] D. Conlon and J. Lim, Sums of dilates over groups of prime order, *to appear in American Mathematical Monthly* (2025), arXiv:2409.17112.

Our concern in this chapter will be with estimating the minimum size of $|A + \lambda \cdot A|$, for $A \subset \mathbb{Z}/p\mathbb{Z}$, with p prime. This problem over $\mathbb{Z}/p\mathbb{Z}$ was first studied in detail by Plagne [35] and by Fiz Pontiveros [16]. For instance, using a rectification argument, which allows one to treat small subsets of $\mathbb{Z}/p\mathbb{Z}$ as though they are sets of integers, the latter showed that for every $\lambda \in \mathbb{Z}$ there exists $\alpha > 0$ such that

$$|A + \lambda \cdot A| \geq (|\lambda| + 1)|A| - C_\lambda$$

for all $|A| \leq \alpha p$. On the other hand, he showed that for every $\lambda \in \mathbb{Z}$ and $\epsilon > 0$ there exists $\delta > 0$ such that, for every sufficiently large prime p, there is a set $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|A| \geq (\frac{1}{2} - \epsilon)p$ such that $|A + \lambda \cdot A| \leq (1 - \delta)p$. That is, as $|A|$ approaches $p/2$, one cannot do much better than the Cauchy–Davenport theorem, which tells us that $|A + \lambda \cdot A| \geq 2|A| - 1$.

Recall the following terminology defined in the introduction. For p prime, $\lambda \in \mathbb{Z}$ and $\alpha \in (0, 1)$, we let

$$\mathrm{ex}(\mathbb{Z}/p\mathbb{Z}, \lambda, \alpha) = \min \{|A + \lambda \cdot A|/p : A \subseteq \mathbb{Z}/p\mathbb{Z},\ |A| \geq \alpha p\}$$

and then define $\mathrm{ex}(\lambda, \alpha) = \limsup_p \mathrm{ex}(\mathbb{Z}/p\mathbb{Z}, \lambda, \alpha)$. The problem of asymptotically estimating the minimum size of sums of dilates over $\mathbb{Z}/p\mathbb{Z}$ may then be rephrased as the problem of determining $\mathrm{ex}(\lambda, \alpha)$. This seems very difficult in full generality, though the results of Fiz Pontiveros described above imply that

- $\mathrm{ex}(\lambda, \alpha) = (|\lambda| + 1)\alpha$ for λ fixed and α sufficiently small in terms of λ and
- $\mathrm{ex}(\lambda, \alpha) < 1$ for $\alpha < \frac{1}{2}$.

Here we look at the case where α is fixed and λ is allowed to grow. In rough terms, we wish to understand how small the sum of dilates $A + \lambda \cdot A$ can be if we fix the density α of A and let λ tend to infinity. More precisely, we set $\mathrm{ex}(\alpha) = \limsup_{\lambda \to \infty} \mathrm{ex}(\lambda, \alpha)$ and investigate the behavior of $\mathrm{ex}(\alpha)$.

By Cauchy–Davenport, if $\alpha \geq \frac{1}{2}$, then $\mathrm{ex}(\alpha) = 1$. Moreover, if $\alpha \leq \frac{1}{2}$, then, again by Cauchy–Davenport, $|A + \lambda \cdot A| \geq 2|A| - 1$, so $\mathrm{ex}(\alpha) \geq 2\alpha$. On the other hand, since $|A + \lambda \cdot A| \leq p$, we always have the trivial upper bound $\mathrm{ex}(\alpha) \leq 1$. Our main result improves these simple bounds significantly, giving a reasonably complete picture of the behavior of $\mathrm{ex}(\alpha)$.

Theorem 8.0.1. *There exist constants $C, C', c > 0$ such that*

$$e^{C' \log^c(1/\alpha)}\alpha \leq \mathrm{ex}(\alpha) \leq e^{C\sqrt{\log(1/\alpha)}}\alpha$$

for all $\alpha \in (0, \frac{1}{2})$. Moreover, $\mathrm{ex}(\alpha) < 1$ for all $\alpha \in (0, \frac{1}{2})$.

Unlike in the fixed λ case, we cannot improve the trivial upper bound $\mathrm{ex}(\alpha) \leq 1$ by just taking A to be an interval. Instead, what we do is show that $\mathrm{ex}(\alpha)$ is bounded above by a continuous variant defined over the torus $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ and then provide an upper bound for that variant. We go straight into the details of this construction, before returning to the lower bound, which makes use of several classical tools from additive combinatorics, in Section 8.2.

8.1 The upper bound

Let $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, $n > 1$ be an integer and μ be the Lebesgue measure on $\mathbb{T}^k$ for any positive integer k. Let $\pi_1 : \mathbb{T}^n \to \mathbb{T}^{n-1}$ be the projection map ignoring the first coordinate and $\pi_n : \mathbb{T}^n \to \mathbb{T}^{n-1}$ the projection map ignoring the last coordinate. Consider the following problem: given $0 < \alpha < 1$, what is the smallest possible value of $\mu(\pi_1(B) + \pi_n(B))$ over all open sets $B \subseteq \mathbb{T}^n$ with $\mu(B) > \alpha$?

Equivalently, we can ask for the smallest possible value of $\mu(B \times \mathbb{T} + \mathbb{T} \times B)$ over all open sets $B \subseteq \mathbb{T}^n$ with $\mu(B) > \alpha$. In this form, written as a problem about sums of shifts rather than sums of projections, there is a ready analogy with the problem of estimating sums of transcendental dilates, which can also be phrased in terms of sums of shifts and ultimately has bounds of a similar form (see Chapter 4). This analogy partly motivates the methods we use here for both the upper and lower bounds.

To capture this question more succinctly, we define

$$\mathrm{ex}_T(n,\alpha) = \inf\{\mu(\pi_1(B)+\pi_n(B)) : B \subseteq \mathbb{T}^n \text{ open}, \ \mu(B) > \alpha\}$$

and set $\mathrm{ex}_T(\alpha) = \lim_{n\to\infty} \mathrm{ex}_T(n,\alpha)$. This limit exists since $\mathrm{ex}_T(n,\alpha)$ is decreasing in n. Indeed, if $B \subseteq \mathbb{T}^n$ with $\mu(\pi_1(B)+\pi_n(B)) = \beta$, consider $B' = B\times\mathbb{T} \subseteq \mathbb{T}^{n+1}$. Then $\mu(B') = \mu(B)$ and $\mu(\pi_1(B')+\pi_{n+1}(B')) = \mu(\pi_1(B)\times\mathbb{T}+B) = \mu(\pi_1(B)+\pi_n(B)) = \beta$, so that $\mathrm{ex}_T(n+1,\alpha) \le \mathrm{ex}_T(n,\alpha)$.

The main result of this section says that $\mathrm{ex}(\alpha) \le \mathrm{ex}_T(\alpha)$, thereby allowing us to give an upper bound on $\mathrm{ex}(\alpha)$ by instead bounding $\mathrm{ex}_T(\alpha)$. The idea of the proof is to construct an example in $\mathbb{Z}/p\mathbb{Z}$ from one in $\mathbb{T}^n$ by approximating each point of $\mathbb{T}^n$ by a number in $\mathbb{Z}/p\mathbb{Z}$ written in base λ, with each point $(x_1,\dots,x_n) \in \mathbb{T}^n$ roughly corresponding to $\lfloor (x_1 + \frac{x_2}{\lambda} + \cdots + \frac{x_n}{\lambda^{n-1}})p \rfloor \in \mathbb{Z}/p\mathbb{Z}$.

Theorem 8.1.1. $\mathrm{ex}(\alpha) \le \mathrm{ex}_T(\alpha)$.

Proof. Let $n > 1$ and $B \subseteq \mathbb{T}^n$ be an open set such that $\mu(B) = \alpha' > \alpha$ and $\mu(\pi_1(B)+\pi_n(B)) = \beta$. We will show that $\mathrm{ex}(\alpha) \le \beta$.

Let $\epsilon > 0$ be arbitrary, λ be a positive integer, $T = \mathbb{Z}/\lambda\mathbb{Z}$ and discretize $\mathbb{T}^n$ into T^n. For $x = (x_1,\dots,x_n) \in T^n$ (with integers $0 \le x_i < \lambda$ for each i), define $C_x \subseteq \mathbb{T}^n$ to be the cubical box

$$\prod_{i=1}^{n} \left[\frac{x_i}{\lambda}, \frac{x_i+1}{\lambda}\right).$$

Let $S = \{x \in T^n : C_x \subseteq B\}$ and $B' = \bigcup_{x\in S} C_x \subseteq B$. As $\lambda \to \infty$, $\mu(B')$ approaches $\mu(B) = \alpha'$ since B is open. Therefore, for λ sufficiently large in terms of ϵ, we have $\mu(B') \ge \alpha' - \epsilon$. For $x \in T^n$, define I_x to be the interval $[y, y+\lambda^{-n})$, where

$$y = \frac{x_1}{\lambda} + \frac{x_2}{\lambda^2} + \cdots + \frac{x_n}{\lambda^n}.$$

Set $A = \bigcup_{x\in S} I_x \subseteq \mathbb{T}$. Then $\mu(A) = |S|/\lambda^n = \mu(B') \ge \alpha' - \epsilon$. We claim that

$$\mu(A + \lambda\cdot A) \le \mu(\pi_1(B') + \pi_n(B')).$$

To see how the theorem follows from this claim, we again discretize $\mathbb{T}$ into $\mathbb{Z}/p\mathbb{Z}$. Set $A' \subseteq \mathbb{Z}/p\mathbb{Z}$ to be $A' = \{0 \le a < p : \left[\frac{a}{p}, \frac{a+1}{p}\right) \subseteq A\}$. By construction, $|A'|/p \le \mu(A)$. Moreover, since A is a finite union of half-closed intervals, $|A'|/p$ approaches $\mu(A)$ as $p \to \infty$. Therefore, for p sufficiently large in terms of ϵ, we have $|A'| \ge (\mu(A)-\epsilon)p$. For any $a+\lambda b \in A'+\lambda\cdot A'$ with $a, b \in A'$, we have $\left[\frac{a}{p}, \frac{a+1}{p}\right) \subseteq A$

and $\frac{b}{p} \in A$. Thus, $\left[\frac{a+\lambda b}{p}, \frac{a+\lambda b+1}{p}\right) \subseteq A + \lambda \cdot A$. Hence, $|A' + \lambda \cdot A'|/p \leq \mu(A + \lambda \cdot A)$. From the claim,

$$\frac{|A' + \lambda \cdot A'|}{p} \leq \mu(A + \lambda \cdot A) \leq \mu(\pi_1(B') + \pi_n(B')) \leq \beta.$$

Since $|A'| \geq (\mu(A) - \epsilon)p \geq (\alpha' - 2\epsilon)p$, taking $\epsilon = \frac{\alpha' - \alpha}{2}$ gives $\mathrm{ex}(\alpha) \leq \beta$, as required.

To prove the claim, let $S' = \pi_1(S) + \pi_n(S) + \{0,1\}^{n-1}$. Then S' is the set of all $z = (z_1, z_2, \ldots, z_{n-1}) \in T^{n-1}$ with $z_k = a_{k+1} + b_k + \epsilon_k$ for some $a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n) \in S$ and $\epsilon_k \in \{0,1\}$ for all k. Since B' is the union of boxes $\bigcup_{x \in S} C_x$, we have that $\pi_1(B') + \pi_n(B')$ is the union of boxes $\bigcup_{x \in S'} C_x$, though now with each $C_x \subseteq \mathbb{T}^{n-1}$. Thus,

$$|S'|/\lambda^{n-1} = \mu(\pi_1(B') + \pi_n(B')).$$

On the other hand, $A + \lambda \cdot A$ consists of all points in $\mathbb{T}$ of the form

$$\frac{b_1 + a_2}{\lambda} + \frac{b_2 + a_3}{\lambda^2} + \cdots + \frac{b_{n-1} + a_n}{\lambda^{n-1}} + \frac{b_n}{\lambda^n} + \epsilon,$$

where $a, b \in S$ and $\epsilon \in [0, \lambda^{-n} + \lambda^{-n+1})$. Here, we are viewing a_i and b_i as integers in $[0, \lambda - 1]$, so $b_i + a_{i+1}$ could "overflow." Nevertheless, each element of $A + \lambda \cdot A$ is of the form

$$\frac{c_1}{\lambda} + \frac{c_2}{\lambda^2} + \cdots + \frac{c_{n-1}}{\lambda^{n-1}} + \delta,$$

where $c_i = b_i + a_{i+1} \bmod \lambda$ or $b_i + a_{i+1} + 1 \bmod \lambda$ and $\delta \in [0, \lambda^{-n+1})$. Thus, $A + \lambda \cdot A \subseteq \bigcup_{x \in S'} I_x$, so we have

$$\mu(A + \lambda \cdot A) \leq |S'|/\lambda^{n-1} = \mu(\pi_1(B') + \pi_n(B')),$$

as required. □

We believe that the two functions $\mathrm{ex}(\alpha)$ and $\mathrm{ex}_T(\alpha)$ should in fact be equal, but leave the task of proving that $\mathrm{ex}(\alpha) \geq \mathrm{ex}_T(\alpha)$ as an open problem.

We now give an upper bound for $\mathrm{ex}_T(\alpha)$, and therefore $\mathrm{ex}(\alpha)$, by considering a suitable set $B \subseteq \mathbb{T}^n$.

Theorem 8.1.2. *For any positive integer d, $\mathrm{ex}_T(\alpha) \leq 2^{d-1}\alpha^{1-1/d}$ for all $\alpha \in (0, 2^{-d})$. In particular, there is a constant $C > 0$ such that $\mathrm{ex}_T(\alpha) \leq e^{C\sqrt{\log(1/\alpha)}}\alpha$ for all $\alpha \in (0, \frac{1}{2})$.*

Proof. If $B = (0, \gamma^{1/d})^d \subseteq \mathbb{T}^d$, then $\mu(B) = \gamma$. Furthermore, $\pi_1(B) = \pi_d(B) = (0, \gamma^{1/d})^{d-1} \subseteq \mathbb{T}^{d-1}$, so we have $\mu(\pi_1(B) + \pi_d(B)) = (2\gamma^{1/d})^{d-1} = 2^{d-1}\gamma^{1-1/d}$. Taking the infimum over all $\gamma > \alpha$ then gives the required upper bound $\mathrm{ex}_T(\alpha) \leq \mathrm{ex}_T(d, \alpha) \leq 2^{d-1}\alpha^{1-1/d}$. To get a general bound independent of d, we simply optimize by setting $d = \sqrt{\log(1/\alpha)}$ and the bound follows. □

Remark. *The constant term 2^{d-1} in Theorem 8.1.2 is not optimal. For example, for $d = 3$, instead of picking B to be the $\gamma^{1/3} \times \gamma^{1/3} \times \gamma^{1/3}$ box, we could optimize the side lengths of the box by picking B to be $(2\gamma)^{1/3} \times (\gamma/4)^{1/3} \times (2\gamma)^{1/3}$. This yields $\mu(\pi_1(B) + \pi_3(B)) = \frac{9}{2^{4/3}}\gamma^{2/3}$, where we note that $\frac{9}{2^{4/3}} < 2^2$. We made no attempt to optimize these constants for higher values of d, as any improvement would not change the form of the bound $e^{C\sqrt{\log(1/\alpha)}}\alpha$.*

While Theorem 8.1.2 proves the first upper bound in Theorem 8.0.1, the following result proves the second upper bound $\mathrm{ex}(\alpha) < 1$.

Theorem 8.1.3. $\mathrm{ex}_T(\alpha) < 1$ *for all* $\alpha \in (0, \frac{1}{2})$.

Proof. Let n be sufficiently large and set $B = \{x \in \mathbb{T}^n : x_i > 0 \text{ for all } i,\ \sum_{i=1}^n x_i < \frac{n}{2} - 1\}$, where x_i is considered an element of $[0, 1)$ for all i. As $n \to \infty$, $\mu(B) \to \frac{1}{2}$, since, if $x \in \mathbb{T}^n$ is picked uniformly randomly, $\sum x_i$ is approximately normal with mean $\frac{n}{2}$ and variance $\Theta(n)$. Thus, for sufficiently large n, $\alpha < \mu(B) < \frac{1}{2}$. Fix such an n. Now both $\pi_1(B)$ and $\pi_n(B)$ are contained in the set $C = \{x \in \mathbb{T}^{n-1} : \sum_{i=1}^{n-1} x_i < \frac{n}{2} - 1\}$, so

$$\pi_1(B) + \pi_n(B) \subseteq C + C = \{x \in \mathbb{T}^{n-1} : \sum_{i=1}^{n-1} x_i < n - 2\} \subsetneq \mathbb{T}^{n-1}.$$

Hence, $\mu(\pi_1(B) + \pi_n(B)) < 1$, so that $\mathrm{ex}_T(\alpha) \leq \mathrm{ex}_T(n, \alpha) < 1$. □

8.2 The lower bound

We now prove the lower bound in Theorem 8.0.1, which we restate as follows. As prefaced in the previous section, the proof of this result makes use of ideas similar to those used in [39] for studying sums of transcendental dilates.

Theorem 8.2.1. *There are constants $C', c > 0$ such that $\mathrm{ex}(\alpha) \geq e^{C' \log^c(1/\alpha)}\alpha$ for all $\alpha \in (0, 1/2)$. In particular, one may take $c = \frac{1}{7}$.*

In what follows, as well as the notation $\lambda \cdot B = \{\lambda b : b \in B\}$ for dilates, we will use mB to denote the m-fold sumset

$$mB = \underbrace{B + B + \cdots + B}_{m \text{ times}}.$$

Before proving Theorem 8.2.1, we require the following result, a variant of the Plünnecke–Ruzsa inequality allowing for dilates of each term.

Lemma 8.2.2. *Let B be a finite subset of an abelian group, λ an integer and $K > 0$ such that $|B + \lambda \cdot B| \leq K|B|$. Then, for any positive integer l,*

$$|B + \lambda \cdot B + \lambda^2 \cdot B + \cdots + \lambda^l \cdot B| \leq K^{7l-6}|B|.$$

Proof. Apply the sum version of Ruzsa's triangle inequality (Lemma 1.6.1) with $X = \lambda \cdot B$, $Y = Z = B$ and noting that $|\lambda \cdot B| = |B|$, we have $|B + B| \leq K^2|B|$. Hence, by the Plünnecke–Ruzsa inequality (Lemma 1.6.2), $|B + B + B| \leq K^6|B|$. Thus, another application of Ruzsa's triangle inequality (with $X = B$, $Y = B + B$, $Z = \lambda \cdot B$) yields

$$|B + B + \lambda \cdot B| \leq |B + B + B||B + \lambda \cdot B|/|B| \leq K^7|B|.$$

We prove the lemma by induction on l, noting that the case $l = 1$ follows from the given assumption. Suppose now that we have

$$|B + \lambda \cdot B + \lambda^2 \cdot B + \cdots + \lambda^l \cdot B| \leq K^{7l-6}|B|$$

for some l and we wish to prove it for $l + 1$. Yet another application of Ruzsa's triangle inequality (with $X = \lambda^l \cdot B$, $Y = B + \lambda \cdot B + \cdots + \lambda^{l-1} \cdot B$, $Z = \lambda^l \cdot B + \lambda^{l+1} \cdot B$) yields

$$\begin{aligned}
|B + \lambda \cdot B + \cdots + \lambda^{l+1} \cdot B| &\leq |B + \lambda \cdot B + \cdots + \lambda^l \cdot B||\lambda^l \cdot B + \lambda^l \cdot B + \lambda^{l+1} \cdot B|/|B| \\
&\leq K^{7l-6}|\lambda^l \cdot B + \lambda^l \cdot B + \lambda^{l+1} \cdot B| \\
&= K^{7l-6}|B + B + \lambda \cdot B| \\
&\leq K^{7(l+1)-6}|B|,
\end{aligned}$$

as required. □

The other thing that we need for the proof of Theorem 8.2.1 is Sanders' quantitative version of the Bogolyubov–Ruzsa lemma [40, Theorem 1.1], which states that if A

is a finite subset of an abelian group with $|A + A| \leq K|A|$, then $2A - 2A$ contains a proper generalized arithmetic progression P of dimension $d \leq d_0(K) \leq C \log^6 K$ and size at least $C_1(K)|A|$, where C is an absolute constant. Here a generalized arithmetic progression P of dimension d is a set of the form

$$P = \{a + \sum_{i=1}^{d} n_i v_i : 0 \leq n_i \leq k_i - 1 \text{ for all } i\}$$

and such a generalized arithmetic progression is proper if all of its elements are distinct, that is, if $|P| = k_1 k_2 \cdots k_d$.

Proof of Theorem 8.2.1. Fix $\alpha \in (0, 1/2)$ and let $K = 2\exp(\alpha)/\alpha$. Let λ be sufficiently large and p be sufficiently large in terms of λ. Let $A \subseteq \mathbb{Z}/p\mathbb{Z}$, which we may assume has size $|A| = \alpha p$, be such that $|A + \lambda \cdot A| \leq 2\exp(\alpha)p = K|A|$. By Ruzsa's triangle inequality, we again have $|A + A| \leq K^2|A|$. Hence, by Sanders' quantitative version of the Bogolyubov–Ruzsa lemma, $2A - 2A$ contains a proper generalized arithmetic progression P of dimension $d \leq d_0(K) \leq C \log^6 K$ and size at least $C_1(K)\alpha p$, where C is an absolute constant. By the Plünnecke–Ruzsa inequality, we have $|2A - 2A + 2A - 2A| \leq K^{16}|A|$. By Ruzsa's triangle inequality (with $X = A$, $Y = 2A - 2A + A - 2A$, $Z = \lambda \cdot A$), we have

$$|2A - 2A + A - 2A + \lambda \cdot A| \leq |2A - 2A + 2A - 2A||A + \lambda \cdot A|/|A| \leq K^{17}|A|.$$

Repeating three more times, each time replacing an appropriate A term with $\lambda \cdot A$, we get

$$|(2A - 2A) + \lambda \cdot (2A - 2A)| \leq K^{20}|A|.$$

By Lemma 8.2.2 applied to $2A - 2A$, we then have that,

$$|(2A - 2A) + \lambda \cdot (2A - 2A) + \cdots + \lambda^d \cdot (2A - 2A)| \leq K^{140d}|A|.$$

Suppose $P = v_0 + P_0$ for some $v_0 \in \mathbb{Z}/p\mathbb{Z}$ and P_0 a proper Minkowski sum of d arithmetic progressions $\{0, v_i, 2v_i, \ldots, (k_i - 1)v_i\}$, $i = 1, \ldots, d$, with $|P| = |P_0| = k_1 k_2 \cdots k_d$ and $k_1 \geq k_2 \geq \cdots \geq k_d$. Let $m \leq d$ be the largest integer with $k_m \geq \lambda$. Since $|P_0| \geq \lambda^d$ for sufficiently large p, we have $m \geq 1$. Let $P' = \sum_{i=1}^{m} \{0, v_i, 2v_i, \ldots, (k_i - 1)v_i\}$. Then this is a proper sum with $|P'| \geq |P_0|/\lambda^{d-m}$. Since $k_1 \geq \cdots \geq k_m \geq \lambda$, we have that,

$$P' + \lambda \cdot P' + \lambda^2 \cdot P' + \cdots + \lambda^d \cdot P' \supseteq \sum_{i=1}^{m} \{0, v_i, 2v_i, \ldots, \lambda^d(k_i - 1)v_i\} = \lambda^d P'.$$

By repeated application of the Cauchy–Davenport theorem, we have that

$$|\lambda^d P'| \geq \min(\lambda^d |P'| - \lambda^d + 1, p) \geq \min(\lambda^m C_1 \alpha p - \lambda^d + 1, p) = p$$

for λ large enough that $\lambda C_1 \alpha \geq 2$ and p sufficiently large. Thus, $P' + \lambda \cdot P' + \lambda^2 \cdot P' + \cdots + \lambda^d \cdot P' = \mathbb{Z}/p\mathbb{Z}$. On the other hand,

$$\begin{aligned}
&|P' + \lambda \cdot P' + \lambda^2 \cdot P' + \cdots + \lambda^d \cdot P'| \\
&\leq |P + \lambda \cdot P + \lambda^2 \cdot P + \cdots + \lambda^d \cdot P| \\
&\leq |(2A - 2A) + \lambda \cdot (2A - 2A) + \lambda^2 \cdot (2A - 2A) + \cdots + \lambda^d \cdot (2A - 2A)| \\
&\leq K^{140d}|A| \leq K^{140d_0}|A|.
\end{aligned}$$

This implies that $K^{140d_0}\alpha \geq 1$. From $d_0 \leq C \log^6 K$, we obtain $e^{140C \log^7 K}\alpha \geq 1$, which implies that

$$\mathrm{ex}(\alpha) = K\alpha/2 \geq e^{C'(\log \frac{1}{\alpha})^c}\alpha$$

for some absolute constants c and C', where one may take $c = \frac{1}{7}$. □

If one could show that the Bogolyubov–Ruzsa lemma holds with $d_0(K) \leq C \log K$, which would be best possible, then we could take $c = \frac{1}{2}$, matching our upper bound.

To close, let us mention a variant of the problem we have studied, namely, that of estimating the minimum size of $|A + \cdots + A + \lambda \cdot A|$ over all $A \subseteq \mathbb{Z}/p\mathbb{Z}$ of given size. If there are k summands, we can again study the asymptotic behaviour of this minimum by considering

$$\mathrm{ex}(k, \lambda, \alpha) = \limsup_{p \to \infty} \min \left\{ |\underbrace{A + \cdots + A}_{k-1 \text{ times}} + \lambda \cdot A|/p : A \subseteq \mathbb{Z}/p\mathbb{Z},\ |A| \geq \alpha p \right\}.$$

As a possible extension of his result that $\mathrm{ex}(\lambda, \alpha) < 1$ for $\alpha < \frac{1}{2}$, Fiz Pontiveros [16, Conjecture 1.3] conjectured that $\mathrm{ex}(k, \lambda, \alpha) < 1$ for $\alpha < \frac{1}{k}$. However, this is easily seen to be false. Indeed, a simple consequence of the proof of Theorem 8.2.1 is that, provided k is sufficiently large, $|A + \lambda \cdot A| \geq 10|A|$ for all $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|A| = \lceil p/(k+1) \rceil$ and all λ sufficiently large in terms of k. But then, by repeated application of the Cauchy–Davenport inequality, $|A + \cdots + A + \lambda \cdot A| \geq \min\{(k+8)|A| - (k-2), p\} = p$. In particular, $\mathrm{ex}(k, \lambda, \alpha) = 1$ for $\alpha \geq 1/(k+1)$ and λ sufficiently large in terms of k. This bound on the minimum α such that $\mathrm{ex}(k, \lambda, \alpha) = 1$ for λ sufficiently large in terms of k can certainly be improved, though we have made no serious attempt to do so here. Instead, we leave it as an open problem to give more precise estimates on how this threshold changes with k.

BIBLIOGRAPHY

[1] N. Alon, M. B. Nathanson, and I. Ruzsa, Adding distinct congruence classes modulo a prime, *The American Mathematical Monthly* **102** (1995), no. 3, 250–255, DOI: 10.1080/00029890.1995.11990565.

[2] A. Balog and G. Shakan, On the sum of dilations of a set, *Acta Arithmetica* **164** (2014), no. 2, 153–162, DOI: 10.4064/aa164-2-5.

[3] A. Balog and G. Shakan, Sum of dilates in vector spaces, *North-Western European Journal of Mathematics* **1** (2015), 57–67.

[4] F. A. Behrend, On sets of integers which contain no three terms in arithmetical progression, *Proceedings of the National Academy of Sciences of the United States of America* **32** (1946), no. 12, 331–332, DOI: 10.1073/pnas.32.12.331.

[5] Y. Bilu, Structure of sets with small sumset, *Astérisque* **258** (1999), 77–108.

[6] B. Bollobás and I. Leader, Sums in the grid, *Discrete Mathematics* **162** (1996), no. 1-3, 31–48, DOI: 10.1016/S0012-365X(96)00303-2.

[7] E. Breuillard and B. Green, Contractions and expansion, *European Journal of Combinatorics* **34** (2013), no. 8, 1293–1296, DOI: 10.1016/j.ejc.2013.05.011.

[8] B. Bukh, Sums of dilates, *Combinatorics, Probability and Computing* **17** (2008), no. 5, 627–639, DOI: 10.1017/S096354830800919X.

[9] A.-L. Cauchy, Recherches sur les nombres, *Journal de l'École Polytechnique* **9** (1813), 99–116.

[10] Y.-G. Chen and J.-H. Fang, Sums of dilates in the real numbers, *Acta Arithmetica* **182** (2018), 231–241, DOI: 10.4064/aa170221-22-9.

[11] J. Cilleruelo, Y. O. Hamidoune, and O. Serra, On sums of dilates, *Combinatorics, Probability and Computing* **18** (2009), no. 6, 871–880, DOI: 10.1017/S0963548309990307.

[12] J. Cilleruelo, M. Silva, and C. Vinuesa, A sumset problem, *Journal of Combinatorics and Number Theory* **2** (2010), 79–89.

[13] E. Croot and V. F. Lev, Open problems in additive combinatorics, *Additive Combinatorics* **43** (2007), no. 207-233, 1.

[14] H. Davenport, On the addition of residue classes, *Journal of the London Mathematical Society* **10** (1935), no. 1, 30–32, DOI: 10.1112/jlms/s1-10.37.30.

[15] S.-S. Du, H.-Q. Cao, and Z.-W. Sun, On a sumset problem for integers, *Electronic Journal of Combinatorics* **21** (2014), Paper 1.13, 25 pp, DOI: 10.37236/2801.

[16] G. Fiz Pontiveros, Sums of dilates in $\mathbb{Z}_p$, *Combinatorics, Probability and Computing* **22** (2013), no. 2, 282–293, DOI: 10.1017/S0963548312000466.

[17] G. A. Freiman, Foundations of a structural theory of set addition, vol. 37, Translations of Mathematical Monographs, Providence, RI: American Mathematical Society, 1973.

[18] G. A. Freiman, A. Heppes, and B. Uhrin, A lower estimation for the cardinality of finite difference sets in $\mathbb{R}^n$, in: Number Theory, Vol. I (Budapest, 1987), vol. 51, Colloq. Math. Soc. János Bolyai, Amsterdam: North-Holland, 1990, pp. 125–139.

[19] R. J. Gardner, The Brunn–Minkowski inequality, *Bulletin of the American Mathematical Society* **39** (2002), 355–405.

[20] R. J. Gardner and P. Gronchi, A Brunn–Minkowski inequality for the integer lattice, *Transactions of the American Mathematical Society* **353** (2001), 3995–4024, DOI: 10.1090/S0002-9947-01-02763-5.

[21] B. Green and T. Tao, Compressions, convex geometry and the Freiman–Bilu theorem, *The Quarterly Journal of Mathematics* **57** (2006), no. 4, 495–504, DOI: 10.1093/qmath/hal009.

[22] D. J. Grynkiewicz and O. Serra, Properties of two-dimensional sets with small sumset, *Journal of Combinatorial Theory, Series A* **117** (2010), no. 2, 164–188, DOI: 10.1016/j.jcta.2009.06.001.

[23] Y. O. Hamidoune and J. Rué, A lower bound for the size of a Minkowski sum of dilates, *Combinatorics, Probability and Computing* **20** (2011), no. 2, 249–256, DOI: 10.1017/S0963548310000520.

[24] R. A. Horn and C. R. Johnson, Matrix Analysis, Cambridge, UK: Cambridge University Press, 1985, DOI: 10.1017/CBO9780511810817.

[25] M. Huicochea, On the sum of dilates in $\mathbb{R}^d$, *North-Western European Journal of Mathematics* **7** (2021), 7–26.

[26] F. John, Extremum problems with inequalities as subsidiary conditions, in: Studies and Essays Presented to R. Courant on his 60th Birthday, New York: Interscience Publishers, 1948, pp. 187–204, DOI: 10.1007/978-3-0348-0439-4_9.

[27] S. Konyagin and I. Łaba, Distance sets of well-distributed planar sets for polygonal norms, *Israel Journal of Mathematics* **152** (2006), 157–179, DOI: 10.1007/BF02771981.

[28] D. Krachun and F. Petrov, On the size of $A + \lambda A$ for algebraic λ, *Moscow Journal of Combinatorics and Number Theory* **12** (2023), no. 2, 117–126, DOI: 10.2140/moscow.2023.12.117.

[29] D. Krachun and F. Petrov, Tight lower bound on $|A+\lambda A|$ for algebraic integer λ, *arXiv preprint* (2023), arXiv: 2311.09399 [math.CO].

[30] Z. Ljujić, A lower bound for the size of a sum of dilates, *Journal of Combinatorics and Number Theory* **5** (2013), 31–51.

[31] A. Mudgal, Difference sets in higher dimensions, *Mathematical Proceedings of the Cambridge Philosophical Society* **171** (2021), no. 3, 467–480, DOI: 10.1017/S0305004120000298.

[32] A. Mudgal, New lower bounds for cardinalities of higher dimensional difference sets and sumsets, *Discrete Analysis* (2022), Paper No. 15, 19 pp, DOI: 10.19086/da.55552.

[33] A. Mudgal, Sums of linear transformations in higher dimensions, *The Quarterly Journal of Mathematics* **70** (2019), no. 3, 965–984, DOI: 10.1093/qmath/haz006.

[34] J. Neukirch, Algebraic Number Theory, vol. 322, Grundlehren der mathematischen Wissenschaften, Berlin: Springer, 1999, DOI: 10.1007/978-3-662-03983-0.

[35] A. Plagne, Sums of dilates in groups of prime order, *Combinatorics, Probability and Computing* **20** (2011), no. 6, 867–873, DOI: 10.1017/S0963548311000447.

[36] I. Z. Ruzsa, An application of graph theory to additive number theory, *Scientific Series A: Mathematical Sciences* **3** (1989), 97–109.

[37] I. Z. Ruzsa, Sum of sets in several dimensions, *Combinatorica* **14** (1994), 485–490, DOI: 10.1007/BF01302969.

[38] I. Z. Ruzsa, Sums of finite sets, in: Number Theory (New York, 1991–1995), New York: Springer, 1996, pp. 281–293.

[39] T. Sanders, Appendix to 'Roth's theorem on progressions revisited' by J. Bourgain, *Journal d'Analyse Mathématique* **104** (2008), 193–206, DOI: 10.1007/s11854-008-0021-9.

[40] T. Sanders, On the Bogolyubov–Ruzsa lemma, *Analysis & PDE* **5** (2012), no. 3, 627–655, DOI: 10.2140/apde.2012.5.627.

[41] T. Schoen, Near optimal bounds in Freiman's theorem, *Duke Mathematical Journal* **158** (2011), no. 1, 1–12, DOI: 10.1215/00127094-1276283.

[42] G. Shakan, Sum of many dilates, *Combinatorics, Probability and Computing* **25** (2016), no. 3, 460–469, DOI: 10.1017/S0963548315000164.

[43] D. Singhal and Y. Lin, Primes in denominators of algebraic numbers, *International Journal of Number Theory* **20** (2024), no. 2, 327–348, DOI: 10.1142/S1793042124500167.

[44] Y. Stanchescu, On finite difference sets, *Acta Mathematica Hungarica* **79** (1998), 123–138, DOI: 10.1023/A:1006513923148.

[45] Y. V. Stanchescu, An upper bound for d-dimensional difference sets, *Combinatorica* **21** (2001), 591–595, DOI: 10.1007/s004930100015.

[46] Y. V. Stanchescu, The structure of d-dimensional sets with small sumset, *Journal of Number Theory* **130** (2010), no. 2, 289–303, DOI: 10.1016/j.jnt.2009.08.004.

[47] Y. V. Stanchescu, Three-dimensional sets with small sumset, *Combinatorica* **28** (2008), 343–355, DOI: 10.1007/s00493-008-2205-4.

[48] T. Tao and V. H. Vu, Additive Combinatorics, vol. 105, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 2006, DOI: 10.1017/CBO9780511755149.

[49] B. Uhrin, Some useful estimations in the geometry of numbers, *Periodica Mathematica Hungarica* **11** (1980), 95–103, DOI: 10.1007/BF02017962.