Growth in groups: arithmetic combinatorics and expansion

Master's thesis

by

Maximilian Wötzel

Maximilian Wötzel
Matrikelnr.: 4378778
Konrad-Wolf-Str. 66b
13055 Berlin
m.woetzel@fu-berlin.de

Submission date:
January 16th 2015
Referee:
Prof. Juanjo Rué Perna (PhD.)

Abstract

This thesis will aim to present results on three primary topics. The largest portion will consist of results on the subject of *growth of sets in groups*, in particular the group $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ of 2-by-2 matrices with determinant 1 over the integers modulo some prime. At the heart of this is Harald A. Helfgott's article "Growth in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$", published in 2008 in volume 167 of *Annals of Mathematics*. The main result is that, for a subset $A \subset \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ either $|AAA| > |A|^{1+\varepsilon}$ for some absolute constant $\varepsilon > 0$, that is, it grows rapidly under multiplication with itself, or $(A \cup A^{-1} \cup \{1\})^k = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ for an absolute constant $k > 1$, that is, after a bounded number of multiplications with itself it already is the whole group. The first case occurs when A is small, while the latter happens for large A. In addition to these results, we will also have a look at approaches to generalize them to different groups.

This main result connects the topic of growth in groups to the other two, the first being *arithmetic combinatorics*. Tools of this mathematical field build much of the foundation for the proof of Helfgott's results and will be presented in that context in the course of the thesis.

The third and final topic will concern the concept of *expander graphs*, which are highly-connected, sparse graphs that represent a vital role in computer science and have recently also found applications in pure mathematics. The connection between expansion and growth in groups was already visible in Helfgott's paper: If one has a generating set A of a group G, there is a special graph, the *Cayley graph* of G with respect to A whose diameter is the largest number k needed to write every element of G as a product of elements of A. One directly sees that this is basically the second part of Helfgott's main result, while the first guarantees us that we can construct a large enough generator set in few steps. One could therefore already see that Cayley graphs of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ with respect to some generating sets have small diameter, which is one property of expander graphs, although expansion itself is stronger. Bourgain and Gamburd strengthened the results in this regard in "Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$" and showed that Cayley graphs of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ that have a large enough girth form a family of expander graphs. This will be presented in more detail towards the end of the thesis, and a formal introduction on the topic of expander graphs and some of their properties will be given beforehand.

Contents

Chapter 1

Introduction

1.1 The three main topics

We will begin by giving concise introductions to the three main topics of study in this thesis, namely the relatively new mathematical field of additive (or arithmetic) combinatorics, the study of growth in certain groups, and the concept of expansion. These will all be fairly informal, and more mathematically precise definitions will be given in subsequent chapters.

1.1.1 Additive and arithmetic combinatorics

Additive, or arithmetic, combinatorics is a comparatively new mathematical field; in his review of Tao and Vu's *Additive Combinatorics* ([TV06]), Ben Green calls it the "marriage of number theory, harmonic analysis, combinatorics, and ideas from ergodic theory [...] to understand very simple systems: the operations of addition and multiplication and how they interact", but admits that even this description may not be precise enough. Tao and Vu themselves describe it as the "theory of counting additive structures in sets". A good strategy to get an overview of the myriad of topics covered by this field may be to take a look at the table of contents of [TV06].

The name *additive combinatorics* was coined by Terrence Tao himself, where the *additive* refers to the fact the we operate in an abelian setting, whereas *arithmetic combinatorics* does not require this. Historically, because of the integers in particular, many classical results (which existed even before anyone used the term additive combinatorics) were set in the commutative case, and so a large part of early arithmetic combinatorics was concerned with translating these results to a general setting.

For our purposes, arithmetic combinatorics plays a large role in Helfgott's proof of his results on growth in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, and we will encounter most of the fundamental results of this field in the course of Chapter 2, particularly in **2.1.3**. Of course, recent years have seen rapid developments that will not be discussed, although at some points modern proofs that are purely arithmetic combinatorial will be used for older results, the main example being Plünnecke's inequality.

1.1.2 Growth in groups

The topic of growth in groups mainly asks how the cardinality of a subset grows as one multiplies it with itself. The connection to arithmetic combinatorics thus becomes clear, since classical results in that field like Plünnecke's inequality or the sum-product theorem are very much about this. Consequently, a lot of these results were used directly in Helfgott's paper "Growth in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$", the paper this thesis will present. Other arguments coming from group theory related to group actions were already utilized, as well, but recent developments have resulted in more of a shift towards them. This will be explained in greater detail in Chapter 3.

For this thesis, we will mainly explore the case of finite, simple, non-commutative groups, which, by the *Classification of Finite Simple Groups*, are basically either matrix or permutation groups. The case of matrix groups will, as mentioned, be discussed in detail regarding the special case of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, the group of 2-by-2 matrices with determinant 1 over the field of integers modulo some prime. This will be done in Chapter 2. Both generalizations of Helfgott's results to $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$, as well as to permutation groups will be explored, although the latter in less detail. For the former, we will talk about how one had to change his viewpoint; in particular, the main focus had to be taken off of the groups themselves, and placed onto group actions. In that specific case, the actions that were of interest were conjugation and multiplication.

This subject has seen a lot of developments over the last years, and one can trace this back to [Hel08], so even if the methods used there are not "up-to-date", it is still worthwhile to present them to see the basis of most modern results regarding growth in groups.

1.1.3 Expander graphs

Expander graphs are highly-connected, sparse graphs that play a major role in computer science; in particular, they are used in the context of network construction, error-correcting codes, algorithms and more. Recent years have also seen them be applied to many problems in pure mathematics, most notably number theory and group theory. These graphs were first defined by Bassalygo and Pisker, and their existence was first proved by Pisker in the early seventies. There are several ways to actually define these objects: the most intuitive one is combinatorial and just formalizes the "sparse but highly connected" philosophy mentioned before. Another definition utilizes the eigenvectors of a matrix that is associated to the graph, and a third uses random walks on the graph. All of these are equivalent, and helpful for different applications.

One early hurdle was that while their existence follows relatively easily by random considerations, explicit constructions are much more difficult to generate; these are of course very desirable for applications. In the context of this thesis, we will present one such construction, related to Helfgott's results on growth in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, due to Bourgain and Gamburd in [BG08]. One can associate a graph to a tuple (G, A), where G is a group and A is a generating set thereof. Bourgain-Gamburd then showed that, taking $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ and certain A, these graphs, called *Cayley graphs* form a family of expanders. This will be elaborated upon in **3.1.2**, in conjuncture with a formal definition, as well as the presentation of some important results related to the concept of expansion. The first explicit construction was due to Margulis, and this was later generalized to the so-called *Ramanujan graphs*, but this thesis will not go into further detail in this direction.

The topic of expander graphs is very rich, and has been a major point of study in computer science in the last few years. I could therefore not hope to cover it in any sufficient general detail. If the reader is so inclined, the survey "Expander graphs and their applications" by Hoory-Linial-Wigderson ([HLW06]) is an excellent place to get more acquainted with the topic in general, while Lubotzky's "Expander Graphs in Pure and Applied Mathematics" ([Lub11]) is recommended reading if one is interested in the applications of expander graphs in pure mathematics.

1.2 Acknowledgments

Special thanks go to Juanjo Rué Perna, who went above and beyond in his duties as an advisor to me and who was always available to answer questions in a concise and intuitive manner. Several hours of personal meetings, as well as the large amount of e-mail correspondence definitely helped to improve this thesis significantly. I would also like to thank Michael Brückner for providing support with some of the more technical aspects of creating this thesis.

Chapter 2

Growth in $\mathbf{SL_2}(\mathbb{Z}/\boldsymbol{p}\mathbb{Z})$

This chapter aims to present Helfgott's paper [Hel08], only omitting the later chapters where different applications are described, and hence we will use the same section names, so as to make direct comparisons easier. This has the direct consequence that some of the conventions when naming objects differ from current standard practice. There have also been further generalizations to a lot of the results that will be presented here, which have in turn given rise to changes in the proof of the $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ case, itself. This will be touched upon in chapter 3. If one is interested in this, a complete, modern proof of the results here can be found in [Hel14].

In the course of this chapter, we will also be introduced to core concepts and results of arithmetic combinatorics. It is particularly here that I added several statements and proofs that were only referenced in the original paper.

2.1 Preliminaries

2.1.1 General notation

Let K be some (finite) field, $A, B \subset K$ sets, f a function on K and r a positive integer. Then we denote the cardinality of A by $|A|$, and its characteristic function by A itself. Furthermore

$$\begin{aligned}
&(L_r\text{-norm}) && |f|_r = \left(\sum_{x\in K} |f(x)|^r\right)^{1/r} \\
&(\text{sum-set}) && A + B = \{\, a + b : a \in A, b \in B \,\} \\
&(\text{product-set}) && AB = \{\, ab : a \in A, b \in B \,\} \\
&(\text{convolution}) && A * B(x) = |\{\, (y, z) \in A \times B : y + z = x \,\}|
\end{aligned}$$

$$\begin{aligned} A^r &= \{\, a^r : a \in A \,\} \\ f(A) &= \{\, f(a) : a \in A \,\} \\ A_r &= \left\{\, a_1 a_2 \cdots a_r : a_i \in A \cup A^{-1} \cup \{1\} \,\right\}. \end{aligned}$$

Thus, $|A| = |A|_1$. Moreover, we will use the short forms $A + \xi$ and ξA for $A + \{\xi\}$ and $\{\xi\}A$, respectively. Finally, we will write $\langle A \rangle$ for the group generated by A.

One should take special note of this when reading other publications on similar topics, where nA and A^n are often used to denote $\underbrace{A + A + \cdots + A}_{n \text{ times}}$ and $\underbrace{AA \cdots A}_{n \text{ times}}$, respectively.

2.1.2 Fourier analysis over $\mathbb{Z}/p\mathbb{Z}$

The *Fourier transform* $\widehat{f}$ of a function $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is defined as

$$\widehat{f}(y) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} f(x) \exp(-2\pi i x y / p)$$

Lemma 2.1.1. (Parseval's theorem)
The Fourier transform is an isometry:

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} |\widehat{f}(x)|^2 = p \sum_{x \in \mathbb{Z}/p\mathbb{Z}} |f(x)|^2$$

Proof.

$$\begin{aligned} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} |\widehat{f}(x)|^2 &= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left| \sum_{y \in \mathbb{Z}/p\mathbb{Z}} f(y) \exp\left(-2\pi i x y / p\right) \right|^2 \\ &= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \sum_{y \in \mathbb{Z}/p\mathbb{Z}} \sum_{z \in \mathbb{Z}/p\mathbb{Z}} f(y) \overline{f(z)} \exp\left(2\pi i x (z - y)/p\right) \\ &= \sum_{y \in \mathbb{Z}/p\mathbb{Z}} \sum_{z \in \mathbb{Z}/p\mathbb{Z}} f(y) \overline{f(z)} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \exp\left(2\pi i x (z - y)/p\right) \\ &\overset{(*)}{=} \sum_{y \in \mathbb{Z}/p\mathbb{Z}} \sum_{z \in \mathbb{Z}/p\mathbb{Z}} f(y) \overline{f(z)}\, p \delta_{zy} \\ &= p \sum_{x \in \mathbb{Z}/p\mathbb{Z}} |f(x)|^2, \end{aligned}$$

where δ_{ij} denotes the *Kronecker delta*, that is $\delta_{ij} = 1$ if $i = j$ and 0 otherwise; $(*)$ follows from the fact that if $z = y$ the innermost sum equals p, and if $z \neq y$, we use that it is a geometric sum with value

$$\frac{\exp\left(2\pi i(z-y)\right) - 1}{\exp\left(2\pi i(z-y)/p\right) - 1} = 0.$$

□

Lemma 2.1.2. *Let $f, g : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ and $A, B \subset \mathbb{Z}/p\mathbb{Z}$. Then*

(a) $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$.

(b) $|A * B|_1 = |A||B|$

Proof. (a):

$$\begin{aligned}
\widehat{f * g}(y) &= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} f * g(x) \exp\left(-2\pi i x y/p\right) \\
&= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \sum_{z \in \mathbb{Z}/p\mathbb{Z}} f(z) g(x-z) \exp\left(-2\pi i x y/p\right) \\
&= \sum_{z \in \mathbb{Z}/p\mathbb{Z}} f(z) \sum_{x \in \mathbb{Z}/p\mathbb{Z}} g(x-z) \exp\left(-2\pi i x y/p\right) \\
&= \sum_{z \in \mathbb{Z}/p\mathbb{Z}} f(z) \sum_{\tilde{x} \in \mathbb{Z}/p\mathbb{Z}} g(\tilde{x}) \exp\left(-2\pi i(\tilde{x}+z) y/p\right) \\
&= \left(\sum_{z \in \mathbb{Z}/p\mathbb{Z}} f(z) \exp\left(-2\pi i z y/p\right) \right) \cdot \left(\sum_{\tilde{x} \in \mathbb{Z}/p\mathbb{Z}} g(\tilde{x}) \exp\left(-2\pi i \tilde{x} y/p\right) \right) \\
&= \widehat{f}(y) \cdot \widehat{g}(y)
\end{aligned}$$

(b):

$$\begin{aligned}
|A * B|_1 &= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} A * B(x) \\
&= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} |\{\, (y, z) \in A \times B : y + z = x \,\}| \\
&= |A \times B| \\
&= |A||B|
\end{aligned}$$

□

2.1.3 Basics of arithmetic combinatorics

In this section we will state some of basic results and applications of arithmetic combinatorics. If not otherwise noted, we do not require the group we work in to be abelian.

Lemma 2.1.3. *Let A be a subset of a finite group G. Suppose*

$$|A| > \frac{1}{2}|G|,$$

then $AA = G$.

Note that this is of course also true for the additive case.

Proof. Assume there exists a $g \in G$ such that $g \notin AA$. Since we have the obvious identity

$$g = x \cdot x^{-1} g$$

for any $x \in G$, either x or $x^{-1}g$ is not an element of A. Since $\tilde{x} = x^{-1}g$ happens for exactly one pair $x, \tilde{x}$, this implies

$$|A| \leq |G| - \frac{1}{2}|G| = \frac{1}{2}|G|$$

which is a contradiction to our assumption. □

Definition 2.1.4. (Ruzsa distance)
Let A, B be finite subsets of a group G. Then we define the Ruzsa distance as

$$d(A,B) = \log\left(\frac{|AB^{-1}|}{\sqrt{|A||B|}}\right).$$

In cases where we explicitly refer to the additive case, we will denote this by $d_+(A,B)$.

Note that in general, $d(A,A) \neq 0$, so the Ruzsa distance is not a metric. That said, it does satisfy the triangle inequality.

Lemma 2.1.5. (Ruzsa triangle inequality)
Let A, B and C be finite subsets of a group G. Then

$$d(A,C) \leq d(A,B) + d(B,C).$$

Proof. We use Definition 2.1.4 to get:

$$\begin{aligned} & \log\left(\frac{|AC^{-1}|}{\sqrt{|A||C|}}\right) \leq \log\left(\frac{|AB^{-1}|}{\sqrt{|A||B|}}\right) + \log\left(\frac{|BC^{-1}|}{\sqrt{|B||C|}}\right) \\ \iff \quad & \frac{|AC^{-1}|}{\sqrt{|A||C|}} \leq \frac{|AB^{-1}|}{\sqrt{|A||B|}}\frac{|BC^{-1}|}{\sqrt{|B||C|}} \\ \iff \quad & |AC^{-1}||B| \leq |AB^{-1}||BC^{-1}| \end{aligned} \tag{2.1.1}$$

To proof this (equivalent) statement, we will construct an injection Φ between $AC^{-1} \times B$ and $AB^{-1} \times BC^{-1}$ in the following way: For each $x \in AC^{-1}$, fix a pair $(a_x, c_x) \in A \times C$ such that $x = a_x c_x^{-1}$ and define $\Phi(x, b) = (a_x b^{-1}, bc_x^{-1})$. Now suppose we have some $x, \tilde{x} \in AC^{-1}$ and $b, \tilde{b} \in B$ such that

$$(a_x b^{-1}, bc_x^{-1}) = (a_{\tilde{x}}\tilde{b}^{-1}, \tilde{b}c_{\tilde{x}}^{-1}).$$

But then we get that

$$\begin{aligned} & a_x b^{-1} b c_x^{-1} = a_{\tilde{x}}\tilde{b}^{-1}\tilde{b}c_{\tilde{x}}^{-1} \\ \iff & a_x c_x^{-1} = a_{\tilde{x}} c_{\tilde{x}}^{-1} \\ \iff & x = \tilde{x}, \end{aligned}$$

and from this we can conclude

$$\begin{aligned} & c_x = c_{\tilde{x}} \text{ and } bc_x^{-1} = \tilde{b}c_{\tilde{x}}^{-1} \\ \iff & bc_x^{-1}c_x = \tilde{b}c_{\tilde{x}}^{-1}c_{\tilde{x}} \\ \iff & b = \tilde{b}, \end{aligned}$$

and thus Φ is an injection. □

In particular, we get that

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

In case G is an abelian group, we also have the following lemma.

Lemma 2.1.6. *Let A be a finite subset of an abelian group G. Then*

$$d(A, A^{-1}) \leq 2d(A, A).$$

To prove this, we first have to establish the notion of Plünnecke-type inequalities.

Theorem 2.1.7. (Plünnecke's inequality)
Let A, B be finite subsets of an abelian group G. Suppose $|AB| \leq K|A|$. Then there exists a subset $X \subset A$ such that

$$|X\underbrace{BB\cdots B}_{k \text{ times}}| \leq K^k|X|$$

holds for all $k \geq 1$. In particular, we have that

$$|\underbrace{BB\cdots B}_{k \text{ times}}| \leq K^k|A|.$$

This is actually a slightly stronger statement than how the inequality was originally stated. There, one only proved the existence of such subsets X_k for each positive integer k, but they could differ depending on how it was chosen.
We employ a proof due to Petridis in [Pet12] that centers around the following proposition.

Proposition 2.1.8. *Let X, B be finite subsets of a group G. Suppose that*

$$\frac{|XB|}{|X|} \leq \frac{|VB|}{|V|}$$

for all $V \subset X$. Then

$$|CXB| \leq \frac{|CX||XB|}{|X|}$$

for all finite sets $C \subset G$.

Proof. Let $C \subset G$ a finite subset and choose an arbitrary ordering of its elements such that $C = \{c_1, c_2, \dots, c_n\}$. We can now write

$$CX = \bigsqcup_{i=1}^{n}(c_iX_i) \tag{2.1.2}$$

where the X_i are defined as

$$X_i = \begin{cases} X, & \text{if } i = 1 \\ \{\, x \in X : c_ix \notin \{c_1, c_2, \dots, c_{i-1}\}X \,\}, & \text{if } i > 1 \end{cases}.$$

Observe that if we define $C_m = \{c_1, c_2, \dots, c_m\}$ for some $m \leq n$, we have

$$C_mX = \bigcup_{i=1}^{m}(c_iX) = \bigsqcup_{i=1}^{m}(c_iX_i).$$

Since the union in (2.1.2) is disjoint, we have

$$|C_m X| = \sum_{i=1}^{m} |c_i X_i| = \sum_{i=1}^{m} |X_i| \tag{2.1.3}$$

We proceed by induction on n.
$\underline{n = 1}$: We immediately get

$$|CXB| = |c_1 XB| = |XB| = \frac{|X||XB|}{|X|} = \frac{|c_1 X||XB|}{|X|} = \frac{|CX||XB|}{|X|}$$

$\underline{n > 1}$: Define $X_n^c = X \setminus X^n$ as the complement of X_n in X. By definition of X_n we have that $c_n X_n^c \subset C_{n-1} X$ and thus $c_n X_n^c B \subset C_{n-1} XB$. Hence

$$CXB = C_n XB \subset C_{n-1} XB \cup ((c_n XB) \setminus (c_n X_n^c B)).$$

Now note that $|(c_n XB) \setminus (c_n X_n^c B)| = |(XB) \setminus (X_n^c B)| = |XB| - |X_n^c B|$ and so, in particular,

$$|CXB| \leq |C_{n-1} XB| + (|XB| - |X_n^c B|). \tag{2.1.4}$$

Using induction hypothesis and (2.1.3) we get

$$|C_{n-1} XB| \leq \frac{|C_{n-1} X||XB|}{|X|} \leq \frac{|XB|}{|X|} \sum_{i=1}^{n-1} |X_i|. \tag{2.1.5}$$

Furthermore, the second term in (2.1.4) can be at most $|XB||X_n|/|X|$, since

$$\begin{aligned} |XB| - |X_n^c B| &\leq \frac{|XB||X|}{|X|} - \frac{|XB||X_n^c|}{|X|} \\ &= \frac{|XB|}{|X|}(|X| - |X_n^c|) \\ &= \frac{|XB||X_n|}{|X|} \end{aligned} \tag{2.1.6}$$

where the inequality follows from our minimality assumption in the proposition. Inserting (2.1.5) and (2.1.6) into (2.1.4) and using (2.1.3) results in

$$|CXB| \leq \frac{|XB|}{|X|} \sum_{i=1}^{n} |X_i| = \frac{|CX||XB|}{|X|}$$

which is what we wanted to show. □

This proposition allows us to quickly prove a theorem from which we will derive Plünnecke's inequality.

Theorem 2.1.9. *Let A, B be finite subsets of a group G. Suppose that $|AB| \leq K|A|$. Then there exists a subset $X \subset A$ such that*

$$|CXB| \leq K|CX|$$

holds for all finite sets $C \subset G$.

Proof. Let $X \subset A$ such that

$$\frac{|XB|}{|X|} \leq \frac{|VB|}{|V|}$$

for any subset $V \subset A$. We can apply Proposition 2.1.8 and get that

$$|CXB| \leq \frac{|XB|}{|X|}|CX| \leq \frac{|AB|}{|A|}|CX| \leq K|CX|.$$

□

Proof of Theorem 2.1.7. We proof this by induction on k. Let $X \subset A$ be such that

$$\frac{|XB|}{|X|} \leq \frac{|VB|}{|V|}$$

for any subset $V \subset A$.
$\underline{k=1}$: Our assumption on X immediately results in

$$|XB| \leq |AB||X|/|A| \leq K|X|.$$

$\underline{k>1}$: Since B is finite, so is $\underbrace{BB \cdots B}_{(k-1)\ times}$, so use Theorem 2.1.9 and the induction hypothesis to get

$$\begin{aligned} |X\underbrace{BB\cdots B}_{k\ times}| &= |\underbrace{BB\cdots B}_{(k-1)\ times}XB| \leq K|\underbrace{BB\cdots B}_{(k-1)\ times}X| = K|X\underbrace{BB\cdots B}_{(k-1)\ times}| \\ &\leq K^k|X|. \end{aligned}$$

□

Notice that we did in fact make use of the commutativity of our group in the last step of the proof. An interesting aspect of this proof strategy is that, historically, Plünnecke's inequality was proven first using graph-theoretical methods. Ruzsa then used these methods afterwards to prove a slightly different version of Theorem 2.1.9. We can now give a short prove of Lemma 2.1.6.

Proof of Lemma 2.1.6. First, note the simple identity

$$|AA^{-1}| = \frac{|AA^{-1}|}{|A|}|A|.$$

Now we apply Plünnecke's inequality using $B = A^{-1}$ to get

$$|AA| = |(AA)^{-1}| = |A^{-1}A^{-1}| \leq \frac{|AA^{-1}|^2}{|A|^2}|A| = \frac{|AA^{-1}|^2}{|A|},$$

which, using the definition of the Ruzsa distance, is equivalent to

$$d(A, A^{-1}) \leq 2d(A, A).$$

□

Using different methods, one can also prove a slightly weaker bound for arbitrary finite sets A, B, specifically

$$d(A, B^{-1}) \leq 3d(A, B).$$

Note that this still requires commutativity and is in general not true when A and B are not subsets of an abelian group. Let H be a non-normal subgroup of a group G (by definition of normal subgroups, this already requires G to not be abelian) and let $A = gH$ be a coset. Then note that

$$|AA^{-1}| = |gHHg^{-1}| = |gHg^{-1}| = |H| = |A|,$$

but

$$|AA| = |gHgH| = |HgH|$$

may be a lot larger. A specific example is $G = \mathrm{Sym}(n)$, the symmetric group of order n. Let H denote the subgroup generated by the cycle $c = (1, 2, 3, \dots, n)$ and $g = (1, 2)$ the transposition that swaps 1 and 2. Then H will be non-normal in G, and g and c do not commute. Now $|AA^{-1}| = |A| = n$, but $|AA| = |HgH|$ will be of order n^2.

Another peculiarity of the abelian case that can be directly seen from Plünnecke's inequality is that if $|AA \cdots A|$ is large, then $|AA|$ has to be large, as well. One can again use the example above to show that this is in general not true in the non-abelian setting. Take G, H and g as above and let $A = H \cup \{g\}$. Since H is a subgroup of G, we know that $|AA| \leq 3|A| = 3(n+1)$, while $|AAA| \geq |HgH| = n^2$.

However, if we replace AA by AAA, a statement of this kind will hold even in the non-abelian setting. We will now formulate the contrapositive of this.

Lemma 2.1.10. *Let $n > 2$ be an integer and A a finite subset of a group G. If*

$$|A_n| > c|A|^{1+\varepsilon}$$

for some $c, \varepsilon > 0$, then

$$|AAA| > C|A|^{1+\delta},$$

where $C, \delta > 0$ depend only on c, ε and n.

Proof. By (2.1.1) (using $A = A_{n-2}, B = A, C = A_2$) and noting that by definition $A_n^{-1} = A_n = A_k A_{n-k}$ for any integers $n > k > 0$, we get

$$\frac{|A_n|}{|A|} = \frac{|A_{n-2}A_2|}{|A|} \leq \frac{|A_{n-2}A^{-1}|}{|A|}\frac{|AA_2|}{|A|} \leq \frac{|A_{n-1}|}{|A|}\frac{|A_3|}{|A|}.$$

The last inequality follows from $A_{n-2}A^{-1} \subset A_{n-1}$ and $AA_2 \subset A_3$. We can now iterate this process until the numerator of the first fraction also becomes A_3. Thus, we get that

$$\frac{|A_n|}{|A|} \leq \left(\frac{|A_3|}{|A|}\right)^{n-2}.$$

To complete our proof, we have to bound $|A_3|/|A|$ from above by some power of $|AAA|/|A|$. To do this, note that

$$A_3 = \bigcup_{i,j,k \in \{0,\pm 1\}} A^i A^j A^k$$

and since we can fix an element $a_0 \in A^i$ and see that $a_0 A^j A^k \subset A^i A^j A^k$ and $|a_0 A^j A^k| = |A^j A^k|$, it suffices to bound the cardinalities of products of type $i, j, k \in \{\pm 1\}$. Additionally, note that the cardinality of a set is equal to that of the set of its inverses. Now use (2.1.1) again to obtain

$$|AAA^{-1}||A| = |AAA^{-1}||A^{-1}| \leq |AAA||A^{-1}A^{-1}| = |AAA||AA| \leq |AAA|^2$$

$$|AA^{-1}A||A| \leq |AA^{-1}A^{-1}||AA| = |AAA^{-1}||AA| \leq |AAA^{-1}||AAA| \leq \frac{|AAA|^3}{|A|}$$

$$|A^{-1}AA||A| \leq |A^{-1}A^{-1}||AAA| = |AA||AAA| \leq |AAA|^2$$

$$|AA^{-1}A^{-1}||A| = |AAA^{-1}||A| \leq |AAA|^2$$

$$|A^{-1}AA^{-1}||A| = |AA^{-1}A||A| \leq \frac{|AAA|^3}{|A|}$$

$$|A^{-1}A^{-1}A||A| = |A^{-1}AA||A| \leq |AAA|^2$$

$$|A^{-1}A^{-1}A^{-1}||A| = |AAA||A| \leq |AAA|^2.$$

Combining all of this, we conclude

$$\begin{aligned}\left(\frac{|A_3|}{|A|}\right)^{n-2} &\leq \left(\frac{4|AAA|}{|A|}+\frac{3|AAA^{-1}|}{|A|}+\frac{|AA^{-1}A|}{|A}+\frac{|A^{-1}AA|}{|A|}+\frac{2|AA^{-1}A^{-1}|}{|A|}\right.\\ &\qquad \left.+\frac{|A^{-1}AA^{-1}|}{|A|}+\frac{2|A^{-1}A^{-1}A|}{|A|}+\frac{|A^{-1}A^{-1}A^{-1}|}{|A|}\right)^{n-2}\\ &\leq \left(15\max\left(\frac{|AAA|^2}{|A|^2},\frac{|AAA|^3}{|A|^3}\right)\right)^{n-2}\end{aligned}$$

and therefore either

$$|AAA| > \frac{c^{1/2(n-2)}}{\sqrt{15}}|A|^{1+\varepsilon/2(n-2)},$$

or

$$|AAA| > \frac{c^{1/3(n-2)}}{\sqrt[3]{15}}|A|^{1+\varepsilon/3(n-2)}.$$

□

2.1.4 Regularity

A lot of the results up to now were dependent on knowledge of the whole sum-set $A+B$. In practice, this is often not the case and one only controls a partial collection of sums. We would now like to infer statements about the whole sum-set from these partial ones. The tool that will be used for this is the *Balog-Szemerédi-Gowers Theorem*, which we will present in this section. To start, one needs to formally define the notion of a partial sum-set.

Definition 2.1.11. (Partial sum-set)
Let G be a group and $A, B \subset G$. Let S be a subset of $A \times B$. Then the partial sum-set $A \overset{S}{+} B$ is defined as

$$A \overset{S}{+} B = \{\, a+b : (a,b) \in S \,\}.$$

Now, one ideally would want to have a statement of the sort that if $|A \overset{S}{+} B|$ is small for a large $|S|$, then $|A+B|$ will also have to be small. This is sadly not true in general. Let for example $V \subset \mathbb{Z}$ be a Sidon set (i.e. a set such that $|V+V| = |V|(|V|+1)/2$) of size n and

$$W = \{w, w+r, \ldots, w+(n-1)r\} \subset \mathbb{Z}$$

an arithmetic progression such that V and W are disjoint. This can always be done by going from V to $V \times \{0\} \subset \mathbb{Z}\times\mathbb{Z}$ and from W to $W \times \{1\}$ if necessary. Note that for arithmetic progressions, one can prove $|W+W| \leq 2|W|-1$ (cf. [TV06] ex. 2.2.2). Now define $A = V \sqcup W$. Then $N = |A| = 2n$. Set

$$S = \{\, (x,y) \in A \times A : x,y \in W \,\},$$

which means $|S| = |W|^2 = N^2/4$ and note that

$$|A \overset{S}{+} A| = |W+W| \leq 2|W| = N,$$

but

$$|A+A| \geq |V+V| \geq \frac{|V|^2}{2} = \frac{N^2}{8}.$$

However, what the Balog-Szemerédi-Gowers Theorem tells us is that we can find subsets A', B' that are only slightly smaller than A and B for which we can indeed make that statement.
Using the *Regularity Lemma* (hence the title of this section), Balog and Szemerédi were the first to formulate something in this direction in [BS94]. Later, a different proof was found by Gowers in [Gow98] with one of the most important aspects being that the constants were polynomial in nature. The version we will state and prove here is taken from [TV06].

Theorem 2.1.12. (Balog-Szemerédi-Gowers)
Let A, B be finite subsets of an additive abelian group G, and S a subset of $A \times B$ such that

$$|S| \geq \frac{|A||B|}{K} \text{ and } |A \overset{S}{+} B| \leq K'\sqrt{|A||B|}$$

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

$$\begin{aligned} |A'| &\geq c_1 \frac{|A|}{K} \\ |B'| &\geq c_2 \frac{|B|}{K} \\ |A'+B'| &\leq c_3 K^{C_1} K'^{C_2} \sqrt{|A||B|} \end{aligned}$$

for some absolute constants $c_1, c_2, c_3, C_1, C_2 > 0$.

We will only need this theorem for a special case.

Corollary 2.1.13. *Let A be a finite subset of an additive abelian group G, and S a subset of $A \times A$ such that*

$$|S| \geq \frac{|A|^2}{K} \text{ and } |A \overset{S}{+} A| \leq K|A|.$$

for some $K > 0$. Then there exists a subset $A' \subset A$ such that

$$\begin{aligned} |A'| &\geq cK^{-C}|A| \\ |A' + A'| &\leq CK^{C}|A| \end{aligned}$$

for some absolute constants $c, C > 0$.

The result obtained by Gowers, namely that the constant can be taken to be polynomial in K and K' is important, since this means that the theorem remains effective even with K, K' as large as $|A|^{\varepsilon}$. This will be essential to our work later.
We will use a proof from [TV06] that employs a graph-theoretical approach. Hence, we will first need to give some basic definitions.

Definition 2.1.14. (Undirected graph)
An undirected graph *$G = (V, E)$ is an ordered pair comprising a set V of* vertices *together with a set $E \subset \binom{V}{2}$ of* edges*. Here, $\binom{V}{2}$ denotes the set of 2-element subsets of V.*

Note that we always implicitly assume the vertex set V to be finite. We will not use them in this thesis, but there are also *directed* graphs, for which the edge set E is a subset of $V \times V$, and thus each edge $e \in E$ is an ordered tuple of elements of V, which enables one to differentiate between *initial* and *terminal* vertices of an edge. For our purposes, a special kind of undirected graphs is interesting, *bipartite* graphs. They have the property that one can split the vertex set into two subsets in such a way that there are no edges between vertices in the same subset. Let us be precise.

Definition 2.1.15. (Bipartite graph)
Let $G = (V, E)$ be an (undirected) graph. Then G is bipartite *if there exist disjoint subsets $V_1, V_2 \subset V$, $V_1 \cup V_2 = V$ such that*

$$\{\,\{v, w\} \in E : v, w \in V_i\,\} = \emptyset$$

for $i = 1, 2$.

We will write $G = (A \cup B, E)$ as a shorthand to mean that G is a bipartite graph with respect to the subsets A, B of V. We need the following definitions for a very basic counting argument due to Euler, the *handshake lemma*, which we will employ later.

Definition 2.1.16. *Let $G = (V, E)$ be an undirected graph. Then the* set of neighbors *of a subset $W \subset V$ is the set*

$$N(W) = \{\, v \in V : \exists w \in W \colon \{v, w\} \in E \,\}\,.$$

Let $W = \{w\}$ be a set comprised of a single vertex w. Then we will write $N(w)$ as a shorthand for $N(\{w\})$ and furthermore, we will call

$$\deg(w) = |N(w)|$$

the degree *of w.*

Lemma 2.1.17. (Handshake lemma)
Let $G = (V, E)$ be an undirected graph. Then

$$\sum_{v \in V} \deg(v) = 2|E|.$$

The proof of this is very easy, so we leave it to the reader.

Returning to the proof of the theorem, note that a partial sum-set $A \overset{S}{+} B$ can be seen as a bipartite graph on the vertex sets A, B in which two vertices have an edge if their sum is contained in S. Now consider the case that this bipartite graph has many edges, then it will have many pairs of vertices which are connected by paths of length one. We then expect there to be many vertices which are connected by paths of length two, three and so on, as well. Furthermore, this connectivity will become more uniform as the length of the path increases. Using a simple identity, we can identify paths of length three with different representations of the same sum-set element and use this uniformity to prove the theorem of Balog-Szemerédi-Gowers.

In these proofs, we will make use probabilistic notation; namely, if E is an event in our sample space, $\mathbf{P}(E)$ denotes its probability and $\mathbf{I}(E)$ its indicator function (i.e., $\mathbf{I}(E) = 1$ if E occurs and 0 otherwise). Furthermore, for some random variable X,

$$\mathbb{E}(X) = \sum_x x\,\mathbf{P}(X = x)$$

will denote the expectation of X. We will now formulate our arguments above concretely.

Lemma 2.1.18. (Paths of length two)
Let $G(A \cup B, E)$ be a bipartite graph with $|E| \geq |A||B|/K$ for some $K \geq 1$. Then, for any $0 < \varepsilon < 1$, there exists a subset $A' \subset A$ such that

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

and such that at least $(1-\varepsilon)|A'|^2$ *of the pairs of vertices* $a, a' \in A'$ *are connected by at least* $\frac{\varepsilon}{2K^2}|B|$ *paths of length two in* G.

Proof. By decreasing K if necessary we may assume $|E| = \frac{|A||B|}{K}$. Observe the identities

$$\mathbb{E}_{b\in B}\left[\frac{|N(b)|}{|A|}\right] = \mathbb{E}_{a\in A}\left[\frac{|N(a)|}{|B|}\right] = \frac{|E|}{|A||B|} = \frac{1}{K}$$

and

$$\mathbb{E}_{b\in B}\left[\frac{|N(b)|^2}{|A|^2}\right] = \mathbb{E}_{a,a'\in A}\left[\frac{|N(a)\cap N(a')|}{|B|}\right],$$

where the first follows from uniform distribution and the fact that the sum of degrees of one side of a bipartite graph equals its number of edges (with regards to G), and the second follows from the first equation with regards to the bipartite graph $G'((A\times A)\cup B, E')$ where

$$((a,a'),b) \in E' \iff (a,b)\in E \wedge (a',b)\in E.$$

Note that since for some $b \in B$

$$(a,a') \in N_{G'}(b) \iff a \in N(b) \wedge a' \in N(b),$$

we get that $|N_{G'}(b)| = |N(b)|^2$. Using Cauchy-Schwarz for expected values we get

$$\begin{aligned}\mathbb{E}_{a,a'\in A}\left[\frac{|N(a)\cap N(a')|}{|B|}\right] &= \mathbb{E}_{b\in B}\left[\frac{|N(b)^2|}{|A|^2}\right]\cdot \mathbb{E}_{b\in B}[\mathbb{1}^2] \\ &\geq \mathbb{E}_{b\in B}\left[\frac{|N(b)|}{|A|}\cdot \mathbb{1}\right]^2 \\ &= \frac{1}{K^2},\end{aligned}$$

where $\mathbb{1}$ denotes the constant one random variable. Now denote by Ω the set of all pairs (a,a') such that $|N(a)\cap N(a')| < \frac{\varepsilon}{2K^2}|B|$, that is $(a,a')\in\Omega$ if a, a' are *not* connected by at least $\frac{\varepsilon}{2K^2}|B|$ paths of length two.
Then we have

$$\mathbb{E}_{a,a'\in A}\left[\mathbf{I}((a,a')\in\Omega)\frac{|N(a)\cap N(a')|}{|B|}\right] < \frac{\varepsilon}{2K^2}$$

and hence by linearity of the expectation

$$\mathbb{E}_{a,a'\in A}\left[\left(1-\frac{1}{\varepsilon}\mathbf{I}((a,a')\in\Omega)\right)\frac{|N(a)\cap N(a')|}{|B|}\right] \geq \frac{1}{2K^2}.$$

The left-hand side can be rearranged as

$$\mathbb{E}_{b \in B}\left[\frac{1}{|A|^2}\sum_{a,a' \in N(b)}\left(1 - \frac{1}{\varepsilon}\mathbf{I}((a,a') \in \Omega)\right)\right]$$

and hence by pigeonhole principle there exists a $b \in B$ such that

$$\frac{1}{|A|^2}\sum_{a,a' \in N(b)}\left(1 - \frac{1}{\varepsilon}\mathbf{I}((a,a') \in \Omega)\right) \geq \frac{1}{2K^2}.$$

In particular this implies that

$$|N(b)| \geq \frac{|A|}{\sqrt{2}K}$$

and that

$$|\{\, a, a' \in N(b) : (a,a') \in \Omega \,\}| \leq \varepsilon |N(b)|^2.$$

The claim then follows by setting $A' = N(b)$. □

We now use this to get an analogous result for paths of length three.

Corollary 2.1.19. (Paths of length three)
Let $G(A \cup B, E)$ be a bipartite graph with $|E| \geq |A||B|/K$ for some $K \geq 1$. Then there exist subsets $A' \subset A, B' \subset B$ with

$$|A'| \geq \frac{|A|}{4\sqrt{2}K} \text{ and } |B'| \geq \frac{|B|}{4K},$$

such that every $a \in A'$ and $b \in B'$ is connected by at least $\frac{|A||B|}{2^{12}K^5}$ paths of length three.

Proof. Before applying the preceding lemma, it is convenient to prepare the graph G a bit. Let $\tilde{A}$ be the set of vertices in A that have degree at least $|B|/2K$, and let $\tilde{G} = \tilde{G}(\tilde{A} \cup B, \tilde{E})$ be the induced subgraph. Since at most $|A||B|/2K$ edges are removed when passing from G to $\tilde{G}$, we see that $\tilde{G}$ has at least $|A||B|/2K$ edges. Writing $|A| = L|\tilde{A}|$ for some $L \geq 1$ and applying Lemma 2.1.18 to $\tilde{G}$ (with K replaced by $2K/L$ and $\varepsilon = 1/16K$) we can find a subset $\tilde{A}'$ of $\tilde{A}$ of size

$$|\tilde{A}'| \geq \frac{|\tilde{A}|}{\sqrt{2}(2K/L)} = \frac{|A|}{2\sqrt{2}K}$$

and such that $\left(1 - \frac{1}{16K}\right)|\tilde{A}'|^2$ of the pairs $(a,a') \in \tilde{A}' \times \tilde{A}'$ are connected by at least $L^2|B|/128K^3$ paths of length two.

Let us call a pair $(a,a') \in \tilde{A}' \times \tilde{A}'$ *bad* if they are not connected by at least $L^2|B|/128K^3$ paths of length two; thus there are at most $\frac{1}{16K}|\tilde{A}'|^2$ bad pairs. Let A' be the set of all $a \in \tilde{A}'$ such that at most $\frac{1}{8K}|\tilde{A}'|$ of the pairs (a,a') with $a' \in \tilde{A}'$ are bad. Then $|\tilde{A}' \setminus A'| \le |\tilde{A}'|/2$, and thus

$$|A'| \ge \frac{|\tilde{A}'|}{2} \ge \frac{|A|}{4\sqrt{2}K}.$$

What remains is the construction of B'. Since every element in $\tilde{A}$ (so especially in $\tilde{A}'$) has degree at least $|B|/2K$, we have

$$\sum_{b\in B} \left|\left\{ a \in \tilde{A}' : (a,b) \in E) \right\}\right| = |\{ (a,b) \in E : a \in A' \}| \ge |\tilde{A}'|\frac{|B|}{2K},$$

so if we let

$$B' = \left\{ b \in B : \left|\left\{ a \in \tilde{A}' : (a,b) \in E) \right\}\right| \ge \frac{|\tilde{A}'|}{4K} \right\},$$

then we get

$$\begin{aligned}
|\tilde{A}'||B'| &\ge \sum_{b\in B'} \left|\left\{ a \in \tilde{A}' : (a,b) \in E \right\}\right| \\
&= \sum_{b\in B} \left|\left\{ a \in \tilde{A}' : (a,b) \in E \right\}\right| - \sum_{b\notin B'} \left|\left\{ a \in \tilde{A}' : (a,b) \in E \right\}\right| \\
&\ge |\tilde{A}'|\frac{|B|}{2K} - \frac{|\tilde{A}'|}{4K}|B \setminus B'| \\
&\ge |\tilde{A}'|\frac{|B|}{2K} - \frac{|\tilde{A}'|}{4K}|B| \\
&= \frac{|\tilde{A}'||B|}{4K}.
\end{aligned}$$

In particular we have $|B'| \ge |B|/4K$.

Finally, let $a \in A'$ and $b \in B'$ be arbitrary. By construction of B', b is adjacent to at least $|\tilde{A}'|/4K$ elements a' of $\tilde{A}'$. By construction of A', at most $|\tilde{A}'|/8K$ of the pairs (a,a') are bad. Thus there are at least $|\tilde{A}'|/8K \ge |A|/16\sqrt{2}K^2$ vertices a' which are simultaneously adjacent to b and connected to a by at least $L^2|B|/128K^3$ paths of length two. Thus a and b are connected by at least

$$\frac{|A|}{16\sqrt{2}K^2}\frac{L^2|B|}{128K^3} \ge \frac{|A||B|}{2^{12}K^5}$$

paths of length three. □

This corollary will now help us in proving the Balog-Szemerédi-Gowers Theorem.

Proof of Theorem 2.1.12. At first observe that, without loss of generality, we can assume A and B to be disjoint, since we can replace our group G by $G \times \mathbb{Z}$ and A (resp. B) by $A \times \{0\}$ (resp. $B \times \{1\}$). Now view the set $S \in A \times B$ as a bipartite graph on the vertex sets A and B. Thus we can apply Corollary 2.1.19 and get sets A', B' satisfying the conditions of Theorem 2.1.12 and such that every pair $(a,b) \in A' \times B'$ is connected by at least $|A||B|/2^{12}K^5$ paths of length three, that is

$$|\{\,(a',b') \in A \times B : (a,b'),(a',b'),(a',b) \in S\,\}| \geq \frac{|A||B|}{2^{12}K^5}.$$

We can now use the identity

$$a+b = \underbrace{(a+b')}_{x} - \underbrace{(a'+b')}_{y} + \underbrace{(a'+b)}_{z}$$

and conclude that

$$\left|\left\{\,(x,y,z) \in (A \overset{S}{+} B)\times(A \overset{S}{+} B)\times(A \overset{S}{+} B) : x-y+z = a+b\,\right\}\right| \geq \frac{|A||B|}{2^{12}K^5}.$$

Since the total number of triplets (x,y,z) is at most

$$|A \overset{S}{+} B|^3 \leq K'^3|A|^{3/2}|B|^{3/2}$$

we arrive at the conclusion that the total number of values for $a+b$ is at most $2^{12}K^5K'^3\sqrt{|A||B|}$. □

2.1.5 Sum-product estimates in finite fields

We will first state a version of a theorem due to Bourgain, Katz and Tao in [BKT04] about the growth of small sets in finite fields.

Theorem 2.1.20. (Bourgain-Katz-Tao theorem for finite fields)
Let $q = p^\alpha$ be a prime power and $\delta > 0$ be given. Then, for any subset $A \subset \mathbb{F}_q^*$ with $C < |A| < p^{1-\delta}$, we have

$$\max\left(|AA|, |A+A|\right) > |A|^{1+\varepsilon},$$

where $C, \varepsilon > 0$ depend only on δ.

Note that for any given $\delta > 0$, we are able to explicitly compute values for C and ε.

Proof. For the range $|A| < \sqrt{p}$, one can use the proof of this result for prime fields found e.g. in [Gar10] without any changes. For $|A| \geq \sqrt{p}$, Theorem 4.3 in [BKT04] tells us that, in essence, the theorem can only fail if A were a subfield or a large subset of a subfield of $\mathbb{F}_q$, but we avoid this because $|A| < p^{1-\delta}$. □

Note that the setting of finite fields makes the proof of this often strictly harder than using infinite ones. The reason for this is that we have no natural topology when using finite fields, while these can be used for infinite ones like the real numbers. For $\mathbb{R}$ in particular, one can give a very natural proof using the Szemerédi-Trotter theorem, which was first done by Elekes in [Ele97]. Now that we have a statement about small sets, we finish this section by formulating a lemma for large ones.

Lemma 2.1.21. *Let p be a prime and $A \subset \mathbb{F}_p, S \subset \mathbb{F}_p^*$ subsets. Then there is an element $\xi \in S$ such that*

$$|A + \xi A| \geq \left(\frac{1}{p} + \frac{p}{|S||A|^2}\right)^{-1} \geq \frac{1}{2}\min\left(p, \frac{|S||A|^2)}{p}\right).$$

Additionally, for every $c \in (0, 1]$, there are at least $(1 - c)|S|$ elements $\xi \in S$ such that

$$|A + \xi A| \geq c\left(\frac{1}{p} + \frac{p}{|S||A|^2}\right)^{-1}.$$

Proof. We take Fourier transforms so we can apply Parseval's theorem and Lemma 2.1.2:

$$\begin{aligned} p \cdot \sum_{\xi \in S} |A * \xi A|_2^2 &= \sum_{\xi \in S} |\widehat{A * \xi A}|_2^2 = \sum_{\xi \in S} |\widehat{A} \cdot \widehat{\xi A}|_2^2 = \sum_{\xi \in S} \sum_{x \in \mathbb{F}_p} |\widehat{A}(x) \cdot \widehat{A}(\xi x)|^2 \\ &\leq |S||\widehat{A}(0)|^4 + \sum_{x \in \mathbb{F}_p^*} \sum_{y \in \mathbb{F}_p^*} |\widehat{A}(x)\widehat{A}(y)|^2 \\ &= |S||A|^4 + \left(\sum_{x \in \mathbb{F}_p^*} |\widehat{A}(x)|^2\right)^2 \leq |S||A|^4 + p^2(|A|_2^2)^2 \\ &= |S||A|^4 + p^2|A|^2. \end{aligned}$$

Dividing by $|S|p$ results in

$$\frac{1}{|S|} \sum_{\xi \in S} |A * \xi A|_2^2 \leq \frac{|A|^4}{p} + \frac{p|A|^2}{|S|}$$

and hence by pigeonhole principle there must exist an $\xi_0 \in S$ such that

$$|A * \xi_0 A|_2^2 \leq \frac{|A|^4}{p} + \frac{p|A|^2}{|S|}.$$

Furthermore, for every $c \in (0,1]$, there are at least $(1-c)|S|$ elements $\xi \in S$ such that

$$|A * \xi A|_2^2 \leq \frac{1}{c}\left(\frac{|A|^4}{p} + \frac{p|A|^2}{|S|}\right).$$

Now because of the equivalence

$$\begin{aligned} A * \xi A(x) = 0 &\iff \forall y \in A, z \in \xi A : y + z \neq x \\ &\iff A + \xi A(x) = 0 \end{aligned}$$

for some $x \in \mathbb{F}_p$, using Cauchy-Schwarz inequality gives us

$$\begin{aligned} |A * \xi A|_1^2 &= \left|\sum_{x \in \mathbb{F}_p} A * \xi A(x) \cdot A + \xi A(x)\right|^2 \\ &\leq \sum_{x \in \mathbb{F}_p} |A * \xi A(x)|^2 \cdot \sum_{y \in \mathbb{F}_p} |A + \xi A(y)|^2 \\ &= |A * \xi A|_2^2 \cdot |A + \xi A| \end{aligned}$$

Now, since $|A * \chi A|_1 = |A||\chi A| = |A|^2$ for every $\chi \in \mathbb{F}_p^*$, we obtain that

$$|A + \xi_0 A| \geq \frac{|A * \xi_0 A|_1^2}{|A * \xi_0 A|_2^2} \geq \frac{|A|^4}{\frac{|A|^4}{p} + \frac{p|A|^2}{|S|}} = \left(\frac{1}{p} + \frac{p}{|S||A|^2}\right)^{-1}$$

for at least one $\xi_0 \in S$, and that for any $c \in (0,1]$

$$|A + \xi A| \geq \frac{|A * \xi A|_1^2}{|A * \xi A|_2^2} \geq \frac{c|A|^4}{\frac{|A|^4}{p} + \frac{p|A|^2}{|S|}} = c\left(\frac{1}{p} + \frac{p}{|S||A|^2}\right)^{-1}$$

for at least $(1-c)|S|$ elements $\xi \in S$. □

2.2 Expanding functions on $\mathbb{F}_q$

If we have some polynomial f on variables x and y, it is natural to suspect that for every $\delta > 0$ and some $r, \varepsilon > 0$ and $C > 0$ depending only on δ, every set $A \subset \mathbb{F}_p$ with $C < |A| < p^{1-\delta}$ must fulfill $|f(A_r, A_r)| > |A|^{1+\varepsilon}$. The work in [BKT04] that led to Theorem 2.1.20 basically amounts to this result for $f(x,y) = x + y$. In this section, we will use these results to formulate a similar statement for other choices of f. The naming of this section is also natural: these polynomials expand the set A in the sense that they increase the cardinality by an order of magnitude.

Proposition 2.2.1. *Let $q = p^\alpha$ be a prime power. Let $\delta > 0$ be given. Then, for any $A \subset \mathbb{F}_q^*$ with $C < |A| < p^{1-\delta}$, we have*

$$\left|\{\, (x + x^{-1})(y + y^{-1}) : x, y \in A_2 \,\}\right| \geq |A|^{1+\varepsilon},$$

where $C, \varepsilon > 0$ depend only on δ.

Proof. Let $w(x) = x + x^{-1}$ and suppose that $|\{\, w(x)w(y) : x, y \in A_2 \,\}| \leq |A|^{1+\varepsilon}$. Then we claim that

$$|A_2| \leq 2|A|^{1+\varepsilon}.$$

We will show this by proving $|\{\, w(x)w(y) : x, y \in A_2 \,\}| \geq |A_2|/2$. To do this, recall that $1 \in A_2$ and $w(1) = 2$. Now check when $2w(y) = 2w(\tilde{y})$ for some $y, \tilde{y} \in A_2$:

$$\begin{aligned} & 2(y + y^{-1}) = 2(\tilde{y} + \tilde{y}^{-1}) \\ \iff\ & y^2\tilde{y} + \tilde{y} \quad\ = \tilde{y}^2 y + y \\ \iff\ & y\tilde{y}(y - \tilde{y}) \ = y - \tilde{y}, \end{aligned}$$

which is true if either $y = \tilde{y}$ or $y\tilde{y} = 1$, that is $y = \tilde{y}^{-1}$. This immediately gives us our desired inequality.
Now, consider the set $S = \{\, (w(xy), w(xy^{-1})) : x, y \in A \,\}$. We claim that the cardinality of S is at least $|A|^2/8$. For this, fix $x_0, y_0 \in A$ and determine when $(w(x_0y_0), w(x_0, y_0^{-1})) = (w(xy), w(x, y^{-1}))$ for some $x, y \in A$. This obviously happens if and only if the corresponding components are equal. The trivial cases are of course $x_0y_0 = xy$ and $x_0y_0^{-1} = xy^{-1}$, so let us assume the contrary:

$$\begin{aligned} & x_0y_0 + x_0^{-1}y_0^{-1} && = xy + x^{-1}y^{-1} \\ \iff\ & x_0^2y_0^2xy + xy && = x^2y^2x_0y_0 + x_0y_0 \\ \iff\ & x_0y_0xy(x_0y_0 - xy) && = x_0y_0 - xy \\ \iff\ & x_0y_0 && = x^{-1}y^{-1} \end{aligned}$$

and

$$x_0y_0^{-1} + x_0^{-1}y_0 \qquad = xy^{-1} + x^{-1}y$$

$$\begin{aligned}
\iff\ & x_0^2 y_0^{-2} x y^{-1} + x y^{-1} &&= x^2 y^{-2} x_0 y_0^{-1} + x_0 y_0^{-1} \\
\iff\ & x_0 y_0^{-1} x y^{-1} (x_0 y_0^{-1} - x y^{-1}) &&= x_0 y_0^{-1} - x y^{-1} \\
\iff\ & x_0 y_0^{-1} &&= x^{-1} y.
\end{aligned}$$

So in addition to the trivial cases from above, we also get $x_0 y_0 = x^{-1} y^{-1}$ for the first component, and $x_0 y_0^{-1} = x^{-1} y$ for the second. We now have to consider each possible combination of them:

$$\begin{aligned}
x_0 y_0 = xy, x_0 y_0^{-1} = x y^{-1} \quad &\implies x_0^2 = x^2 &&\implies x = x_0, y = y_0 \\
& && \quad \text{or } x = -x_0, y = -y_0 \\
x_0 y_0 = xy, x_0 y_0^{-1} = x^{-1} y \quad &\implies x_0^2 = y^2 &&\implies x = y_0, y = x_0 \\
& && \quad \text{or } x = -y_0, y = -x_0 \\
x_0 y_0 = x^{-1} y^{-1}, x_0 y_0^{-1} = x^{-1} y &\implies x_0^2 = x^{-2} &&\implies x = x_0^{-1}, y = y_0^{-1} \\
& && \quad \text{or } x = -x_0^{-1}, y = -y_0^{-1} \\
x_0 y_0 = x^{-1} y^{-1}, x_0 y_0^{-1} = x y^{-1} &\implies x_0^2 = y^{-2} &&\implies x = y_0^{-1}, y = x_0^{-1} \\
& && \quad \text{or } x = -y_0^{-1}, y = -x_0^{-1},
\end{aligned}$$

and hence $|S| \geq |A|^2/8$.
Now, because of the trivial identity $w(x)w(y) = w(xy) + w(xy^{-1})$, we can apply Theorem 2.1.12 (using $K = |A|^\varepsilon$) and obtain a subset $A' \subset A_2$ (which may be taken to be closed under inversion) such that $|A'| > c'|A|^{1-C'\varepsilon}$ and $|w(A') + w(A')| < C'|A|^{1+C'\varepsilon}$. Simultaneously, we know that $|w(A')w(A')| \leq |w(A_2)w(A_2)| \leq |A|^{1+\varepsilon}$. We now have a contradiction to Theorem 2.1.20, provided ε is small enough, and C is large enough. □

The following is a non-commutative analogue to Ruzsa's covering lemma that first appeared as an argument in [Ruz99].

Lemma 2.2.2. *Let A, B be subsets of a group G. Then A can be covered by at most $|A \cdot B|/|B|$ cosets $a_j B_2$ of B_2, with $a_j \in A$.*

Proof. Let $\{a_1, a_2, \ldots, a_k\}$ be a maximal subset of A such that the cosets $a_j B$, $j \in [k]$ are all disjoint. It is clear that $k \leq |A \cdot B|/|B|$. Let $x \in A$. Since $\{a_1, a_2, \ldots, a_k\}$ is maximal, there is a j_x such that $a_{j_x} B \cap xB$ is non-empty. Then $x \in a_{j_x} B B^{-1} \subset a_{j_x} B_2$. Thus, the sets $a_{j_x} B_2$ cover A. □

Proposition 2.2.3. *Let $q = p^\alpha$ be a prime power, and $\delta > 0$ and $b_1, b_2 \in \mathbb{F}_q^*$ be given. Then, for any $A \subset \mathbb{F}_q^*$ with $C < |A| < p^{1-\delta}$,*

$$\left| \left\{ b_1(xy + x^{-1}y^{-1}) + b_2(x^{-1}y + xy^{-1}) : x, y \in A_{20} \right\} \right| > |A|^{1+\varepsilon},$$

where $C, \varepsilon > 0$ depend only on δ.

Proof. By Proposition 2.2.1 we know that

$$\begin{aligned}&\left|\left\{\,(x+x^{-1})(y+y^{-1}) : x,y \in A_2\,\right\}\right|\\ &=\left|\left\{\,xy+(xy)^{-1}+xy^{-1}+(xy^{-1})^{-1} : x,y \in A_2\,\right\}\right|\\ &>|A|^{1+\varepsilon}.\end{aligned}$$

Now, by Lemma 2.2.2, A_4 can be covered by at most $|A_4 \cdot A^2|/|A^2|$ cosets $a_1 A_2^2, \dots, a_k A_2^2$ of A_2^2, with $a_j \in A_4$. Further note that if we have some elements $x, y \in A_2$ such that $xy \in a_j A_2^2 \subset a_j A_4^2$, then we know that $xy^{-1} = (xy)y^{-2} \in a_j A_4^2$. This means

$$\sum_{j=1}^{k}\left|\left\{\,r+r^{-1}+s+s^{-1} : r,s \in a_j A_4^2\,\right\}\right| \geq \left|\left\{\,(x+x^{-1})(y+y^{-1}) : x,y \in A_2\,\right\}\right|$$

and hence, by pigeonhole principle, there is an index $j_0 \in [k]$ such that

$$\left|\left\{\,(r+r^{-1})+(s+s^{-1}) : r,s \in a_{j_0} A_4^2\,\right\}\right| > \frac{|A|^{1+\varepsilon}}{|A_4 \cdot A^2|/|A^2|}. \qquad (2.2.1)$$

Since $|A_4 A^2|/|A^2| \leq 2|A_6|/|A|$, we have

$$\begin{aligned}\frac{|A|^{1+\varepsilon}}{|A_4 A^2|/|A^2|} &> \frac{|A|}{|A_4 A^2|/|A^2|}\\ &\geq \frac{|A|}{2|A_6|/|A|}\\ \iff 2|A_6| \cdot \frac{|A|^{1+\varepsilon}}{|A_4 A^2|/|A^2|} &> |A|^2,\end{aligned}$$

and hence $2|A_6| > |A|^{1+\varepsilon/4}$ or $\frac{|A|^{1+\varepsilon}}{|A_4 A^2|/|A^2|} > |A|^{1+3\varepsilon/4}$. In the first case, we are already done, so assume $2|A_6| \leq |A|^{1+\varepsilon/4}$. Define $B = a_j A_4^2 \subset A_{12}$. Since $|B| \leq |A_4| \leq |A|^{1+\varepsilon/4}$, (2.2.1) implies that

$$\begin{aligned}d_+(w(B), -w(B)) &\overset{\text{def}}{=} \log\left(\frac{|w(B)+w(B)|}{|w(B)|}\right)\\ &\geq \log\left(\frac{|A|^{1+3\varepsilon/4}}{|A|^{1+\varepsilon/4}}\right)\\ &= \frac{\varepsilon}{2}\log|A|.\end{aligned}$$

Since we are in the abelian setting, we can use Lemma 2.1.6 and hence

$$d_+(w(B), w(B)) \geq \frac{\varepsilon}{4}\log|A|.$$

Now, use the Ruzsa triangle inequality to get

$$\begin{aligned}d_+(b_1w(B), -b_2w(B)) + d_+(-b_2w(B), b_1w(B)) &\geq d_+(b_1w(B), b_1w(B))\\ &= d_+(w(B), w(B)),\end{aligned}$$

which simplifies to

$$d_+(b_1w(B), -b_2w(B)) \geq \frac{1}{2}d_+(w(B), w(B)) \geq \frac{\varepsilon}{8}\log|A|,$$

or in other words,

$$\begin{aligned}\left|\left\{\, b_1(r+r^{-1}) + b_2(s+s^{-1}) : r, s \in B \,\right\}\right| &\geq |w(B)||A|^{\varepsilon/8}\\ &\geq \frac{1}{2}|B||A|^{\varepsilon/8} \qquad (2.2.2)\\ &\geq \frac{1}{4}|A|^{1+\varepsilon/8}.\end{aligned}$$

Now, for any $r, s \in B$, the ratio r/s is in $A_4^2A_4^{-2} \subset A_8^2$. Let $y \in A_8$ be such that $y^2 = r/s$ and define $x = r/y \in A_{20}$. Then $r = xy$ and $s = x/y$, and therefore

$$b_1w(B) + b_2w(B) \subset \left\{\, b_1(xy + x^{-1}y^{-1}) + b_2(x^{-1}y + xy^{-1}) : x, y \in A_{20} \,\right\}.$$

Using this and inequality (2.2.2), we are done. □

2.3 Traces and growth

The overarching objective of this section will be to show results on growth of small sets A in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. For this, we will first observe in **2.3.1** that if a subset $A \in \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ fails to grow, it must commute with itself to a fair extent. With tools developed in **2.3.2** and simple combinatorial arguments, we will be able to draw conclusions on the size of $|A|$ from the number of different traces in A_k in **2.3.3**. This, as well as the results from **2.2** will then be used to achieve our objective.

2.3.1 Growth and commutativity

Our goal in this subsection is to prove that a subset A of $\mathrm{SL}_2(K)$ either has to grow rapidly under multiplication by itself, or contain a large subset of simultaneously diagonalizable matrices (done in Corollary 2.3.3). We will start by showing that if A does not grow rapidly, there must be an element g in A

with wich many elements of A commute. We then continue by showing that there are many elements in A_2 that have distinct eigenvalues (Lemma 2.3.2) and use the fact that if a matrix h commutes with such an element, it will also be diagonal in the eigenbasis of g.

Proposition 2.3.1. *Let G be a group and A a non-empty finite subset. Let Λ_A be the set of conjugacy classes of G with non-zero intersection with A. For $g \in G$, let $C_G(g)$ be the centralizer of g in G. Then there is an element $g_0 \in A$ such that*

$$C_G(g_0) \cap (A^{-1}A) \geq \frac{|\Lambda_A||A|}{|AAA^{-1}|}$$

Proof. Let $g \in G$ and $h_1, h_2 \in A$. If $h_1 g h_1^{-1} = h_2 g h_2^{-1}$, then $h_2^{-1}h_1 \in A^{-1}A$ commutes with g. Hence, for any $g \in G$

$$\left|\left\{ hgh^{-1} : h \in A \right\}\right| \geq \frac{|A|}{|C_G(g) \cap A^{-1}A|}.$$

Let $\Upsilon \subset A$ be a set of representatives of Λ_A. Then

$$|AAA^{-1}| \geq \left|\left\{ hgh^{-1} : h \in A, g \in \Upsilon \right\}\right| \geq \sum_{g \in \Upsilon} \frac{|A|}{|C_G(g) \cap A^{-1}A|}. \tag{2.3.1}$$

Now suppose $|C_G(g) \cap A^{-1}A| < \frac{|\Lambda_A||A|}{|AAA^{-1}|}$ for every $g \in \Upsilon$, then

$$\sum_{g \in \Upsilon} \frac{|A|}{|C_G(g) \cap A^{-1}A|} > |\Upsilon| \frac{|AAA^{-1}|}{|\Lambda_A|} = |AAA^{-1}|,$$

which is a contradiction to (2.3.1). □

Lemma 2.3.2. *Let K be a field. Let A be a finite subset of $\mathrm{SL}_2(K)$ that is not contained in any proper subgroup thereof. Then A_2 has at least $\frac{1}{4}|A| - 1$ elements with trace other than ±2.*

Proof. Let $g \in A$ be an element of trace ± 2 other than $\pm I$. Let $B \subset A$ be the set of all elements of A with trace ± 2 and an eigenvector in common with g. Suppose $|B| \leq \frac{1}{4}|A| + 3$. Let $h \in A \setminus B$. We would like to show that if h has trace ± 2, then either gh or $g^{-1}h$ does not. To do this, first note that using elementary calculations, one can show that

$$\mathrm{Tr}(gh) + \mathrm{Tr}(gh^{-1}) = \mathrm{Tr}(g)\,\mathrm{Tr}(h).$$

We now have to consider the different possible combinations of values for the traces of g, h, gh and gh^{-1}. Since the techniques used to do this are very similar, we will only show this for the case where all four traces are equal to 2 and leave the rest to the reader. We start by determining the eigenvalues of g:

$$\begin{aligned}\det(\lambda I - g) &= (\lambda - g_{11})(\lambda - g_{22}) - g_{12}g_{21}\\ &= \lambda^2 - \lambda(\underbrace{g_{11} + g_{22}}_{\mathrm{Tr}(g)}) + \underbrace{g_{11}g_{22} - g_{12}g_{21}}_{\det(g)}\\ &= \lambda^2 - 2\lambda + 1\\ &= (\lambda - 1)(\lambda - 1).\end{aligned} \tag{2.3.2}$$

So g has eigenvalue 1 with multiplicity 2. Now denote by $G = PgP^{-1}$ the *Jordan normal form* of g and by H the matrix obtained by conjugating h with $P \in \mathrm{SL}_2(\overline{K})$. We know that $G = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$, write $H = \left(\begin{smallmatrix}H_1 & H_2\\ H_3 & H_4\end{smallmatrix}\right)$. Since traces and determinants are invariant under basis transformations, we can just work with G, H, GH and GH^{-1}. Further note

$$\begin{aligned}GH &= \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}H_1 & H_2\\ H_3 & H_4\end{pmatrix}\\ &= \begin{pmatrix}H_1 + H_3 & H_2 + H_4\\ H_3 & H_4\end{pmatrix}\end{aligned} \quad \text{and} \quad \begin{aligned}GH^{-1} &= \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}H_4 & -H_2\\ -H_3 & H_1\end{pmatrix}\\ &= \begin{pmatrix}H_4 - H_3 & H_1 - H_2\\ -H_3 & H_1\end{pmatrix}.\end{aligned}$$

Now,

$$\mathrm{Tr}(GH) = \underbrace{H_1 + H_4}_{\mathrm{Tr}(H)=2} + H_3 = 2,$$

which implies that $H_3 = 0$. But for some $v \in \overline{K} \times \overline{K}$, we can compute the product $Gv = (v_1 + v_2, v_2)$, so $Gv = v$ implies that $v = (v_1, 0)$. Let v be an eigenvector of g, then

$$\begin{aligned}Hv &= \begin{pmatrix}H_1 & H_2\\ 0 & H_4\end{pmatrix}\begin{pmatrix}v_1\\ 0\end{pmatrix}\\ &= \begin{pmatrix}H_1 v_1\\ 0\end{pmatrix}\\ &= H_1 v,\end{aligned}$$

so v would be an eigenvector of H, and thus of h. But we assumed $\mathrm{Tr}(h) = 2$, which together implies $h \in B$, a contradiction. Note that in cases where g has trace -2, (2.3.2) gives us the eigenvalue -1 with multiplicity 2 and therefore G, GH and GH^{-1} will change. We have now shown that if h has trace ± 2, either gh or gh^{-1} has trace other than ± 2. Therefore $A \cup AA \cup A^{-1}A$ has at least $\frac{1}{3}|A \setminus B| \geq \frac{1}{4}|A| - 1$ elements with trace other than 2.

Suppose now $|B| > \frac{1}{4}|A| + 3$ and let h be an element of A that does not have an eigenvector in common with g. Let $g' \in B$ such that $g'h$ has trace 2. Since g' is in B, it has an eigenvector in common with g, denote it by v. But then, as seen above, $v = (v_1, 0)$ (we only showed this for gs with trace 2, but it is also true for -2), and thus $g'_{21} = 0$; since h and g do not have eigenvectors in common, $h_{21} \neq 0$. We get the following system of linear equalities:

$$\begin{aligned} &\text{(I)} && \operatorname{Tr}(g'h) = g'_{11}h_{11} + g'_{12}h_{21} + g'_{22}h_{22} = 2 \\ &\text{(II)} && \det(g') = g'_{11}g'_{22} = 1 \\ &\text{(III)} && \operatorname{Tr}(g') = g'_{11} + g'_{22} = \pm 2 \end{aligned}$$

So there are at most two such elements g'. Hence AA has more than $\frac{1}{4}|A| + 1$ elements with trace other than ±2. □

Corollary 2.3.3. *Let K be a field. Let A be a non-empty finite subset of* $\mathrm{SL}_2(K)$ *not contained in any proper subgroup thereof. Assume* $|\operatorname{Tr}(A)| \geq 2, |A| \geq 4$. *Then there are at least* $\frac{(|\operatorname{Tr}(A)|-2)(\frac{1}{4}|A|-1)}{|A_6|}$ *simultaneously diagonalizable matrices in* A_4.

Proof. Let B be the set of elements of A_2 with trace other than ±2. By Lemma 2.3.2, $|B| \geq \frac{1}{4}|A| - 1$. We may now apply Proposition 2.3.1 and obtain that there is an element $g \in B$ such that

$$|C_G(g) \cap B^{-1}B| \geq \frac{|\Lambda_B||B|}{|BBB^{-1}|} \geq \frac{|\operatorname{Tr}(B)||B|}{|BBB^{-1}|} \geq \frac{(|\operatorname{Tr}(A)| - 2)(\frac{1}{4}|A| - 1)}{|A_6|}.$$

Let $h \in V = C_G(g) \cap B^{-1}B$ a matrix. It commutes with g and, since $\operatorname{Tr}(g) \neq \pm 2$, it follows that g has two distinct eigenvalues r, r^{-1} and hence is diagonalizable. Denote the eigenbasis of g by P. Let G (resp. H) denote g (resp. h) in basis P. Since

$$GH = PgP^{-1}PhP^{-1} = PghP^{-1} = PhgP^{-1} = PhP^{-1}PgP^{-1} = HG$$

g and h will also commute in basis P, so we restrict our work to that. If we write $H = \begin{pmatrix} H_1 & H_2 \\ H_3 & H_4 \end{pmatrix}$, we get

$$GH = \begin{pmatrix} H_1 r & H_2 r \\ H_3 r^{-1} & H_4 r^{-1} \end{pmatrix} = \begin{pmatrix} H_1 r & H_2 r^{-1} \\ H_3 r & H_4 r^{-1} \end{pmatrix} = HG.$$

Since $r \neq r^{-1}$, the identities $H_2 r = H_2 r^{-1}$ and $H_3 r = H_3 r^{-1}$ imply $H_2 = H_3 = 0$, i.e. h is diagonal in basis P, and hence all of V is simultaneously diagonalizable. □

2.3.2 Escaping from subvarieties

The following lemma will make use of *representation theory*, which is a branch of mathematics where elements of abstract algebraic structures get *represented* by linear transformations of vector spaces. This is useful since it reduces problems in abstract algebra to problems in linear algebra. We will not make much use of details here and only really require the definition of a *linear representation* of a group G. The theory goes a lot deeper, and, if one is interested, a good place to start reading is the classical *Linear Representations of Finite Groups* by Serre ([Ser77]).

Definition 2.3.4. (Linear representation)
Let G be a group, and V be a vector space over a field K. A linear representation *of G in V is a homomorphism*

$$\rho\colon G \to \mathrm{GL}(V),$$

where $\mathrm{GL}(V)$ is the group of automorphisms in V. That means, ρ maps an element of G to a bijective map from V to V such that

$$\rho(gh) = \rho(g) \circ \rho(h)$$

for any two elements g, h in G. One often writes ρ_g for $\rho(g)$.

We will interpret this in the context of the group G acting on V and write $g \cdot x$ instead of $\rho_g(x)$ for elements $g \in G$ and $x \in V$. By Definition 2.3.4, we directly see that $\rho_1 = \mathrm{id}_V$ and $\rho_{g^{-1}} = \rho_g^{-1}$, and, in the context of group actions,

$$\begin{aligned} 1 \cdot x &= x \\ gh \cdot x &= g \cdot (h \cdot x), \end{aligned}$$

for any elements $g, h \in G$ and $x \in V$. We will now see how one can escape from a proper subvariety of V by the actions of elements in G.

Lemma 2.3.5. *Let G be a group. Consider a linear representation of G on a vector space V over a field K. Let W be a union $W_1 \cup \cdots \cup W_n$ of proper subspaces of V.*
Let A be a subset of G and let $y \in V$ such that its orbit $\mathcal{O} = \langle A \rangle \cdot y$ is not contained in W. Then there are constants $\eta > 0$ and m depending only on n and $\dim V$ such that, for every $x \in \mathcal{O}$, there are at least $\max(1, \eta|A|)$ elements $g \in A_m$ such that $g \cdot x \notin W$.

In other words, if y can escape from W at all, it can do so in a bounded number of steps.

Proof. We will begin by showing that there are elements $g_1, \dots g_l \in A_r$ such that, for every $x \in \mathcal{O}$, at least one of the $g_i \cdot x$ is not in W. Note that here, l and r are bounded in terms of n and $d = \dim V$ alone. We will then proceed by induction on (d_W, s_W), where d_W is the maximal dimension of the spaces $W_1, \dots, W_n$, and s_W is the number of spaces of dimension d_W among them. We shall always pass from W to a union of the form $W' = W'_1 \cup \dots W'_{n'}$, where either (a) $d_{W'} < d_W$, or (b) $d_{W'} = d_W$ and $s_{W'} < s_W$. The base case of the inductive process will be $(d_W, s_W) = (0, 0)$, where the statement is clear. Now define W_+ as the union of subspaces $W_j, 1 \leq j \leq n$, that have dimension d_W. If W_+ and $\mathcal{O}$ are disjoint, we set $W' = W \setminus W_+$ and are done by using the induction hypothesis and adding 1.

So suppose otherwise. Since the sets are not disjoint, there exists an element $x_0 = h \cdot y \in W_+ \cap \mathcal{O}$. Now assume that $g \cdot x \in W_+$ for each $x \in \mathcal{O}$ and each $g \in A \cup A^{-1}$. We know that for each $x = \tilde{g} \cdot y \in \mathcal{O}$

$$x = \tilde{g} \cdot y = \tilde{g}h^{-1}h \cdot y = \tilde{g}h^{-1} \cdot (h \cdot y) = \tilde{g}h^{-1} \cdot x_0,$$

and since x_0 is an element of $W_+ \cap \mathcal{O}$ and $\tilde{g}h^{-1}$ is generated by elements of $A \cup A^{-1}$, our assumption implies that x is an element of $W_+ \cap \mathcal{O} \subset W_+$ and therefore $\mathcal{O} \subset W_+$, which we know to be false. So there exists an element $g \in A \cup A^{-1}$ such that $g \cdot x_0 \notin W_+$. Hence the set of subspaces of maximal dimension in W is not the same as the set of subspaces of maximal dimension in gW. It follow that $W' = gW \cap W$ does not contain W_+, and thus has fewer subspaces W'_j of dimension d_W than W has.

We have thus passed from W to W', where either (a) $d_{W'} < d_W$, or (b) $d_{W'} = d_W$ and $s_{W'} < s_W$. By the induction hypothesis, we already know that there are $g'_1, \dots, g'_{l'} \in A_{r'}$ such that, for every $x \in \mathcal{O}$, at least one of the $g'_i \cdot x$ is not in W'. Here l' and r' are bounded in terms of n' and $d = \dim V$ alone; the number n' of subspaces $W'_1, \dots, W'_{n'}$ is bounded by n^2. Since at least one of the $g'_i \cdot x$ is not in $W' = gW \cap W$, either one of the $g'_i \cdot x$ is not in W or one of the $g'_i \cdot x$ is not in gW, i.e., one of the $g^{-1}g'_i \cdot x$ is not in W. Set

$$\begin{aligned} g_1 = g'_1, g_2 = g'_2, \dots, g_l = g'_l \\ g_{l+1} = g^{-1}g'_1, g_{l+2} = g^{-1}g'_2, \dots, g_{2l} = g^{-1}g'_l, \qquad l' = 2l. \end{aligned}$$

Note that $g_i \in A_r$, where $r = r' + 1$. We conclude that, for every $x \in \mathcal{O}$, at least one of the $g_i \cdot x$ is not in W.

We are almost done: for each $x \in \mathcal{O}$ and each $g \in A$, at least one of the elements $g_i g \cdot x$, $1 \leq i \leq l \, (g_i \in A_r)$ will not be in W (since $g \cdot x \in \mathcal{O}$ and $g_i g \cdot x = g_i \cdot (g \cdot x)$). Now fix one $g_i g$ and check when some $g_j \tilde{g}$ is equal to it. This happens if and only if $\tilde{g} = g_j^{-1} g_i g$, so there are at most l different elements $\tilde{g}$ where this can happen; thus, there are at least $\max(1, |A|/l)$ elements $h = g_i g \in A_{r+1}$ such that $h \cdot x \notin W$. □

Corollary 2.3.6. *Let K be a field. Let A be a finite subset of $\mathrm{SL}_2(K)$ not contained in any proper subgroup of $\mathrm{SL}_2(K)$. If $|K| > 3$, the following holds: for any basis $\{v_1, v_2\}$ of $\overline{K} \times \overline{K}$, there is a $g \in A_k$ such that $gv_i \neq \lambda v_j$ for all choices of $\lambda \in \overline{K}$, $i, j \in \{1, 2\}$, where k is an absolute constant.*

Proof. Consider $G = \mathrm{SL}_2(K)$ and its natural action on the vector space $V = M_2(\overline{K})$ of 2-by-2 matrices. Let W be the subset of V consisting of all $h \in V$ such that $hv_i = v_j$ for some $i, j \in \{1, 2\}$. Let x be the identity in $M_2(\overline{K})$.

We would like to apply Lemma 2.3.5, but first we have to check that the orbit $\mathcal{O} = \mathrm{SL}_2(K)$ of x is not contained in W. Denote by $G_{i,j}$ the set of all matrices g in $\mathrm{SL}_2(K)$ such that gv_i is a multiple of v_j. Since $W(K) \cap \mathcal{O} = G_{1,1} \cup G_{1,2} \cup G_{2,1} \cup G_{2,2}$, we would like to bound $|G_{i,j}|$. Let $g \in G_{i,j}$ and choose a vector $v \in K \times K$ (say $v = (1, 0)$ or $v = (0, 1)$) that is not a multiple of v_i. Clearly gv and gv_i determine g, but we already know that $gv_i = \lambda v_j$, and, if gv is fixed, two different values of λ determine two matrices g with different determinants. In particular, at most one $\lambda \in \overline{K}$ gives us a $g \in \mathrm{SL}_2(K)$. Thus gv actually fully determines g. Since gv must be non-zero and lie in $K \times K$, we conclude that $|G_{i,j}| \leq |K|^2 - 1$.

The sets $G_{1,1}$ and $G_{2,2}$ intersect at the identity. Thus, $|W(K) \cap \mathcal{O}| \leq 4(|K|^2 - 1) - 1$. Since $|\mathrm{SL}_2(K)| = |K|(|K|^2 - 1)$ and $|K| \geq 4$, we conclude that $|W(K) \cap \mathcal{O}| < |\mathrm{SL}_2(K)|$. In particular, $\mathcal{O} = \mathrm{SL}_2(K)$ is not contained in W, so we can apply the Lemma and are done. □

Corollary 2.3.7. *Let K be a field. Let A be a finite subset of $\mathrm{SL}_2(K)$ not contained in any proper subgroup of $\mathrm{SL}_2(K)$. Then there are absolute constants $k, c > 0$ such that, given any two non-zero vectors $v_1, v_2 \in \overline{K} \times \overline{K}$,*

$$|A_k \setminus (H_{v_1} \cup H_{v_2})| > c|A|,$$

where $H_v = \{ g \in \mathrm{SL}_2(K) : v \text{ is not an eigenvector of } g \}$.

Proof. Consider $G = \mathrm{SL}_2(K)$ and its natural action on $V = M_2(\overline{K})$. Let $W = H'_{v_1} \cup H'_{v_2}$, where $H'_v = \left\{ g \in M_2(\overline{K}) : v \text{ is an eigenvector of } g \right\}$. Let $x = I$.

Before applying Lemma 2.3.5, we need to check that $\mathcal{O} = \mathrm{SL}_2(K)$ is not contained in $W(K)$. Since the matrices $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ share no eigenvectors, there is no pair of eigenvectors v_1, v_2 such that each of the three matrices has at least one of v_1, v_2 as an eigenvector. Thus $\mathrm{SL}_2(K) \not\subset W(K)$. Now apply the Lemma. □

2.3.3 Size from trace size

Given a large set V of diagonal matrices and a matrix $g \notin V$ with only non-zero entries, one can multiply V and g to obtain at least $\gg |V|^3$ different matrices.

Lemma 2.3.8. *Let K be a field. Let $V \subset \mathrm{SL}_2(K)$ be a finite set of simultaneously diagonalizable matrices with common eigenvectors v_1, v_2. Let $g \in \mathrm{SL}_2(K)$ be such that $gv_i \neq \lambda v_j$ for any $\lambda \in \overline{K}$, $i, j \in \{1,2\}$. Then*

$$|VgVg^{-1}V| \geq \frac{1}{2}\left(\frac{1}{4}|V| - 5\right)|V|^2.$$

Proof. Diagonalize V, conjugating by an element of $\mathrm{SL}_2(\overline{K})$ if necessary. Write $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. We want to show that our assumption about g implies $abcd \neq 0$, or in other words, no entry of g is 0. We work in basis $\{v_1, v_2\}$, so $v_1 = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), v_2 = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$. We can compute

$$\begin{aligned} gv_1 &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} a \\ c \end{pmatrix} \end{aligned} \qquad \text{and} \qquad \begin{aligned} gv_2 &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} b \\ d \end{pmatrix}, \end{aligned}$$

and see that if one of the entries of g were equal to 0, there would be indices $i, j \in \{1,2\}$ and a $\lambda \in \{a,b,c,d\} \subset \overline{K}$ such that $gv_i = \lambda v_j$. Since we assumed this to be impossible for g, we conclude that $abcd \neq 0$. Then

$$g\begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix} g^{-1} = \begin{pmatrix} rad - r^{-1}bc & (r^{-1} - r)ab \\ (r - r^{-1})cd & r^{-1}ad - rbc \end{pmatrix}. \tag{2.3.3}$$

The product of the upper-right and lower-left entries is $-(r - r^{-1})^2 abcd$, and the map $r \mapsto -(r - r^{-1})^2 abcd$ cannot send more than 4 distinct elements of K^*, namely $r, -r, r^{-1}$ and $-r^{-1}$, to the same element of K. Thus, the set $\{\, h_{12}h_{21} : h \in gVg^{-1} \,\}$ has cardinality at least $|V|/4$. Assume that the upper-left and lower-right entries of the matrix in the right-hand side of (2.3.3) are both equal to 0. Then

$$\begin{aligned} & rad = r^{-1}bc \\ \iff & r^2 = a^{-1}bcd^{-1} \end{aligned} \qquad \text{and} \qquad \begin{aligned} & r^{-1}ad = rbc \\ \iff & r^{-2} = a^{-1}bcd^{-1} \end{aligned}$$

So both entries can be equal to 0 only if $r^2 - r^{-2} = 0$, and this can happen for at most 4 values of r. Define

$$U = \left\{\, h \in gVg^{-1} : (h_{11}h_{12}h_{21} \neq 0) \vee (h_{22}h_{12}h_{21} \neq 0) \,\right\},$$

then we know that $|\{\, h_{11}h_{12} : h \in U \,\}| \geq \frac{1}{4}|V| - 5$ (we lose the 4 values of r above and $h_{11}h_{12} = 0$ itself). Let $h \in U$ be fixed, and define for $s, t \in K$

$$f_h(s,t) = \begin{pmatrix} s & 0 \\ 0 & s^{-1} \end{pmatrix} \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} = \begin{pmatrix} sth_{11} & st^{-1}h_{12} \\ s^{-1}th_{21} & s^{-1}t^{-1}h_{22} \end{pmatrix}.$$

The product of the upper-right and lower-left entries of $f_h(s,t)$ is $h_{12}h_{21}$, which is independent of s and t. Since $h \in U$, we may recover s^2, t^2 and st from h and $f_h(s,t)$ by multiplying appropriate entries of $f_h(s,t)$ with each other and taking inverses of corresponding entries of h. Thus, for h fixed, there cannot be more than two pairs (s,t) sharing the same value of $f_h(s,t)$. For each element of $\{\, h_{12}h_{21} : h \in U \,\}$, choose an h corresponding to it; let s and t vary. We obtain at least $\frac{1}{2}\,|\{\, h_{12}h_{21} : h \in U \,\}|\,|V|^2$ different values of $f_h(s,t) \in VgVg^{-1}V$. We conclude that $VgVg^{-1}V$ has cardinality at least $\frac{1}{2}\,|\{\, h_{12}h_{21} : h \in U \,\}|\,|V|^2 = \frac{1}{2}(\frac{1}{4}|V| - 5)|V|^2$. □

Proposition 2.3.9. *Let K be a field. Let A be a finite subset of* $\mathrm{SL}_2(K)$ *not contained in any proper subgroup thereof. Assume* $|\operatorname{Tr}(A)| \geq 2$, $|A| \geq 4$ *and* $|K| > 3$. *Then*

$$|A_k| \geq \frac{1}{2}\left(\frac{1}{4}\frac{(|\operatorname{Tr}(A)| - 2)(\frac{1}{4}|A| - 1)}{|A_6|} - 5\right)\left(\frac{(|\operatorname{Tr}(A)| - 2)(\frac{1}{4}|A| - 1)}{|A_6|}\right)^2,$$

where k is an absolute constant.

Proof. By Corollary 2.3.3, there is a simultaneously diagonalizable subset $V \subset A_4$ with $|V| \geq \frac{(|\operatorname{Tr}(A)|-2)(\frac{1}{4}|A|-1)}{|A_6|}$; call its common eigenvectors v_1 and v_2. Since A is not contained in any proper subgroup of $\mathrm{SL}_2(K)$, Corollary 2.3.6 yields a $g \in A_{k_0}$ such that $gv_i \neq \lambda v_j$ for all $\lambda \in K$, $i, j \in \{1, 2\}$ for some absolute constant k_0. Hence, by Lemma 2.3.8, $|VgVg^{-1}V| \geq \frac{1}{2}(\frac{1}{4}|V| - 5)|V|^2$. Since $VgVg^{-1}V \subset A_4A_{k_0}A_4A_{k_0}A_4 = A_{12+2k_0}$, this implies the statement. □

Lemma 2.3.10. *Let K be a field. Let A be a finite subset of* $\mathrm{SL}_2(K)$. *Write the matrices in* $\mathrm{SL}_2(K)$ *with respect to a basis $\{v_1, v_2\}$ of $\overline{K} \times \overline{K}$. Suppose $g_{12}g_{21} \neq 0$ for every $g \in A$. Then*

$$|\operatorname{Tr}(AA^{-1})| \geq \frac{1}{2}\frac{|A|}{|\{\, (g_{11}, g_{22}) : g \in A \,\}|}.$$

Proof. Consider any two distinct $g, g' \in A$ with $g_{11} = g'_{11}$ and $g_{22} = g'_{22}$. Then, using $\det(g') = 1$ and solving for g'_{12}, we compute that gg'^{-1} has trace

$$|\operatorname{Tr}(gg'^{-1})| = g_{11}g'_{22} + g_{22}g'_{11} - g_{12}g'_{21} - g_{21}\left(\frac{g'_{11}g'_{22} - 1}{g'_{21}}\right).$$

Thus, given a $g \in A$, there can be at most two $g' \in A$ with $g_{11} = g'_{11}$, $g_{22} = g'_{22}$ such that $\mathrm{Tr}(gg'^{-1})$ is equal to a given value.
Define $D_g = \{ g' \in A : g'_{11} = g_{11} \text{ and } g'_{22} = g_{22} \}$ and choose a $\tilde{g}$ such that the cardinality of $D_{\tilde{g}}$ is maximal. Then

$$|\,\mathrm{Tr}(AA^{-1})| \geq |\,\mathrm{Tr}(\tilde{g}D_{\tilde{g}}^{-1})| \geq \frac{1}{2}|D_{\tilde{g}}| \geq \frac{1}{2}\frac{|A|}{|\{ (g_{11}, g_{22}) : g \in A \}|}.$$

□

Proposition 2.3.11. *Let K be a field. Let A be a finite subset of $\mathrm{SL}_2(K)$ not contained in any proper subgroup thereof. Then*

$$|\,\mathrm{Tr}(A_k)| \geq c|A|^{1/3},$$

where k and $c > 0$ are absolute constants.

Proof. If A has an element of trace other than ± 2, let h be one such element. Otherwise, choose any $g_1 \in A$ other than $\pm I$, and any $g_2 \in A$ such that Pg_2P^{-1} is *not* an upper triangular matrix, where $P \in \mathrm{SL}_2(\overline{K})$ is the matrix used to transform g_1 to its Jordan normal form. This has to exist, since the upper triangular matrices form a proper subgroup of $\mathrm{SL}_2(K)$. As seen in the proof of Lemma 2.3.2, either $g_1g_2 \in AA$ or $g_1^{-1}g_2 \in A^{-1}A$ has trace other than ± 2; choose $h \in A_2$, $\mathrm{Tr}(h) \neq \pm 2$ to be one of the two. From now on, write all matrices with respect to the two eigenvectors v_1, v_2 of h. We denote by r and r^{-1} the two eigenvalues of h.
By Corollary 2.3.7, $|A_{k_0} \setminus (H_{v_1} \cup H_{v_2})| > c_0|A|$, where $k_0, c_0 > 0$ are absolute constants. For the sake of briefness, define $X = A_{k_0} \setminus (H_{v_1} \cup H_{v_2})$. We can now use Lemma 2.3.10 to get

$$|\,\mathrm{Tr}(A_{2k_0})| \geq |\,\mathrm{Tr}(XX^{-1})| \geq \frac{1}{2}\frac{|X|}{|\{ (g_{11}, g_{22}) : g \in A \}|}. \tag{2.3.4}$$

For $t \in K$, let $D_t = |\{ (g_{11}g_{22}) : g_{11} + g_{22} = t,\ g \in X \}|$. Choose a $\tilde{t} \in K$ such that the cardinality of $D_{\tilde{t}}$ is maximal. For any tuple (a, d) in $D_{\tilde{t}}$, we have the identity $ra + r^{-1}d = (r - r^{-1})a + r^{-1}\tilde{t}$. Thus, for any two distinct pairs $(a, d), (a', d')$ in $D_{\tilde{t}}$, the two values $ra + r^{-1}d$ and $ra' + r^{-1}d'$ must also be distinct. Therefore

$$|\,\mathrm{Tr}(A_{k_0+2})| \geq |\,\mathrm{Tr}(hX)| \geq |D_{\tilde{t}}| \geq \frac{|\{ (g_{11}, g_{22}) : g \in X \}|}{|\,\mathrm{Tr}(X)|}.$$

We multiply this by (2.3.4) to obtain

$$|\,\mathrm{Tr}(A_{k_0+2})||\,\mathrm{Tr}(A_{2k_0})| \geq \frac{|X|}{2|\,\mathrm{Tr}(X)|},$$

and so $|\operatorname{Tr}(A_{2k_0})|^3 \geq |\operatorname{Tr}(A_{k_0+2})||\operatorname{Tr}(A_{2k_0})||\operatorname{Tr}(X)| \geq |X|/2$, where we assume, as we may, that $k_0 \geq 2$. Define $c = (c_0/2)^{1/3}$ and $k = 2k_0$, then

$$|\operatorname{Tr}(A_k)| \geq \left(\frac{1}{2}|X|\right)^{1/3} \geq c|A|^{1/3}.$$

□

2.3.4 Growth of small sets

We can now conclude this section by proving a result on the growth of small sets.

Proposition 2.3.12. *Let p be a prime. Let A be a subset of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ not contained in any proper subgroup thereof. Assume that $|A| < p^{3-\delta}$ for some fixed $\delta > 0$. Then*

$$|AAA| > c|A|^{1+\varepsilon},$$

where $c, \varepsilon > 0$ depend only on δ.

The results in the sub-sections up to now reduce this problem to a question in $\mathbb{F}_{p^2}$, and that question can be answered using the results in **2.2**.

Proof. We may assume that p is larger than an absolute constant; otherwise we make our statement true simply by adjusting the constant c. By the same token, we may assume that $|A|$ is larger than an absolute constant.
By Proposition 2.3.11, $|\operatorname{Tr}(A_{k_0})| \geq c_0|A|^{1/3}$, where k_0 and c_0 are absolute constants. As we said, we may assume that $|A| \geq \max\{(4/c_0)^3, 8\}$. Thus, by Corollary 2.3.3, there are at least

$$\begin{aligned}\frac{|\operatorname{Tr}(A_{k_0})| - 2)(\frac{1}{4}|A_{k_0}| - 1)}{|A_{6k_0}|} &\geq \frac{(c_0|A|^{1/3} - 2)(\frac{1}{4}|A_{k_0}| - 1)}{|A_{6k_0}|}\\ &\geq \frac{(c_0|A|^{1/3} - \frac{1}{2}c_0|A|)(\frac{1}{4}|A_{k_0}| - \frac{1}{8}|A_{k_0}|)}{|A_{6k_0}|}\\ &= \frac{c_0|A|^{1/3}|A_{k_0}|}{16|A_{6k_0}|}\end{aligned}$$

simultaneously diagonalizable matrices in A_{4k_0}. Denote by V the set of the eigenvalues of $\left\lceil\frac{c_0|A|^{1/3}|A_{k_0}|}{16|A_{6k_0}|}\right\rceil$ such matrices. Note that, on average, each of these defines exactly one element in V, since for any $g \in A_{4k_0}$ with eigenvalues $r, r^{-1} \in V$, its inverse will also be in A_{4k_0} and have the same eigenvalues. Further, since they are all simultaneously diagonalizable, g and g^{-1} are the only matrices with eigenvalues r, r^{-1}. We can assume that $c_0 < 1$, and thus get

$$|V| = \left\lceil \frac{c_0 |A|^{1/3} |A_{k_0}|}{16 |A_{6k_0}|} \right\rceil \leq \left\lceil \frac{c_0 |A|^{1/3}}{16} \right\rceil < \frac{c_0 |A|^{1/3}}{16} + 1 \leq \frac{c_0 |A|^{1/3}}{16} + \frac{c_0 |A|^{1/3}}{4}$$

and consequently $|V| < |A|^{1/3} < p^{1-\delta/3}$. We can also assume that $|A_{6k_0}| < |A|^{7/6}$, otherwise, Lemma 2.1.10 already gives us our desired result. Thus

$$|V| \geq \frac{c_0}{16} \frac{|A|^{1/3} |A_{k_0}|}{|A_{6k_0}|} > \frac{c_0}{16} \frac{|A|^{1/3} |A|}{|A|^{7/6}} = \frac{c_0}{16} |A|^{1/6}. \tag{2.3.5}$$

Now, given a constant C depending only on δ, we may assume that $|V| > C$. Otherwise, (2.3.5) implies $1 > \frac{c_0}{16C}|A|^{1/6}$ and thus $|AAA| \geq |A| > \frac{c_0}{16C}|A|^{1+1/6}$ and we are done.
By Corollary 2.3.6, there is a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in A_{k_1}$ such that $abcd \neq 0$, where k_1 is an absolute constant. Now, for any scalars x, y, the trace of

$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

is $ad(xy + x^{-1}y^{-1}) - bc(x^{-1}y + xy^{-1})$. Now let x, y range over all of V, then we see that

$$\begin{aligned} \operatorname{Tr}(A_{160k_0+2k_1}) &= \operatorname{Tr}(A_{20 \cdot 4k_0 + k_1 + 20 \cdot 4k_0 + k_1}) \\ &\supset \left\{ ad(xy + x^{-1}y^{-1}) - bc(x^{-1}y + xy^{-1}) : x, y \in V_{20} \right\}. \end{aligned}$$

This, together with $|V| < p^{1-\delta/3}$ as seen above, allows us to apply Proposition 2.2.3 with $q = p^2$ to obtain

$$|\operatorname{Tr}(A_{160k_0+2k_1})| > |V|^{1+\varepsilon},$$

where $\varepsilon > 0$ depends only on δ. Here we have assumed, as permitted by our arguments above, that $|V| > C$, where C is the constant in the statement of Proposition 2.2.3. Note that we used $\delta/3$ when applying the proposition.
Using the same arguments as when we showed (2.3.5), we may assume that

$$\frac{|\operatorname{Tr}(A_{160k_0+2k_1})||A_{160k_0+2k_1}|}{|A_{6(160k_0+2k_1)}|} \geq 160. \tag{2.3.6}$$

Since $|A_{160k_0+2k_1}|/|A_{6(160k_0+2k_1)}| \leq 1$, this implies $|\operatorname{Tr}(A_{160k_0+2k_1})| \geq 160$; also, since for any matrix $g \in A_{160k_0+2k_1}$ its inverse will also be contained, we get $|A_{160k_0+2k_1}|/2 \geq |\operatorname{Tr}(A_{160k_0+2k_1})|$ which implies $|A_{160k_0+2k_1}| \geq 320$. Now apply Proposition 2.3.9 to $A_{160k_0+2k_1}$ (denote it by A') and obtain

$$\begin{aligned}
|A'_{k_2}| &\geq \frac{1}{2}\left(\frac{1}{4}\frac{(|\operatorname{Tr}(A')|-2)(\frac{1}{4}|A'|-1)}{|A'_6|} - 5\right)\left(\frac{1}{4}\frac{(|\operatorname{Tr}(A')|-2)(\frac{1}{4}|A'|-1)}{|A'_6|}\right)^2 \\
&\geq \frac{1}{2}\left(\left[\frac{1\cdot 79\cdot 79}{4\cdot 80\cdot 320} - \frac{1}{32}\right]\frac{|\operatorname{Tr}(A')||A'|}{|A'_6|}\right)\left(\frac{1\cdot 79\cdot 79}{4\cdot 80\cdot 320}\cdot\frac{|\operatorname{Tr}(A')||A'|}{|A'_6|}\right)^2 \\
&> \frac{1}{2}\cdot\frac{1}{2^6}\cdot\frac{|\operatorname{Tr}(A')||A'|}{|A'_6|}\cdot\frac{1}{2^9}\cdot\frac{|\operatorname{Tr}(A')|^2|A'|^2}{|A'_6|^2} \\
&= \frac{1}{2^{16}}\frac{|\operatorname{Tr}(A')|^3|A'|^3}{|A'_6|^3},
\end{aligned}$$

where k_2 is an absolute constant. We can now use (2.3.6) and the first inequality of (2.3.5) to obtain

$$\begin{aligned}
|A_{k_2(160k_0+2k_1)}| &\geq \frac{1}{2^{16}}\frac{|\operatorname{Tr}(A_{160k_0+2k_1})|^3|A_{160k_0+2k_1}|^3}{|A_{6(160k_0+2k_1)}|^3} \\
&> \frac{1}{2^{16}}\frac{|A_{160k_0+2k_1}|^3}{|A_{6(160k_0+2k_1)}|^3}|V|^{3(1+\varepsilon)} \\
&\geq \frac{1}{2^{16}}\frac{|A_{160k_0+2k_1}|^3}{|A_{6(160k_0+2k_1)}|^3}\frac{c_0^{3+3\varepsilon}|A_{k_0}|^{3+3\varepsilon}}{2^{12+12\varepsilon}|A_{6k_0}|^{3+3\varepsilon}}|A|^{1+\varepsilon} \\
&\geq \frac{c_0^{3+3\varepsilon}}{2^{28+12\varepsilon}}\frac{|A|^{6+3\varepsilon}}{|A_{160k_0+2k_1}|^{6+3\varepsilon}}|A|^{1+\varepsilon},
\end{aligned}$$

and hence,

$$\max\left\{|A_{k_2(160k_0+2k_1)}|,\, |A_{6(160k_0+2k_1)}|\right\} \geq \frac{c_0^{(3+3\varepsilon)/(7+3\varepsilon)}}{16}|A|^{1+\varepsilon/(7+3\varepsilon)}.$$

by Lemma 2.1.10, we are done. □

2.4 Generating the whole group

Since we have successfully proved Proposition 2.3.12, we know how to attain a set of cardinality $p^{3-\delta}, \delta > 0$, by multiplying a given set of generators A by itself $(\log(p/|A|))^c$ times. What we would like to show now is how to produce the whole group $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ in a bounded number of steps from a set almost as large as $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ itself. As might be expected, instead of the sum-product estimates for small sets formulated in Theorem 2.1.20, we will use the estimates for large sets stated in Lemma 2.1.21.

We will use the fact that each element of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ can be written as the product of some upper and lower-triangular matrices with trace 2. To get these matrices, we will first show that if we have a sufficiently large subset of upper-triangular matrices, multiplying this set a few times with itself suffices to achieve that all other upper-triangular matrices with trace 2 are in that product (Lemma 2.4.2). Afterwards, we will employ a simple combinatorial argument to show that if a subset $A \subset \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is large, there has to be a large number of matrices in A whose lower row is the same up to multiplication by a scalar. These, using products, can then be used to generate many upper and lower-diagonal matrices.
The use of upper and lower-diagonal matrices is due to the fact that they are special cases of a more general type of subgroups, *Borel subgroups.*

Definition 2.4.1. (Borel subgroup)
Let G be a linear algebraic group. A Borel subgroup *of G is a (Zariski)-closed, connected, solvable subgroup H of G which is maximal with respect to all these properties.*

We will not go into too much detail about this definition, other than to say that the set of upper-triangular matrices in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is a Borel subgroup, and that by Theorem 6.4 in [MT11] all Borel subgroups are conjugates. This fact will help us in proving the following lemma.

Lemma 2.4.2. *Let p be a prime. Let H be a Borel subgroup of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Let $A \subset H$ be given with $|A| > 2p^{5/3} + 1$. Then A_8 contains all elements of H with trace 2.*

Proof. By our statements above, we may assume that H is the set of upper-triangular matrices. Define $P_r(A) = \left\{ x \in \mathbb{Z}/p\mathbb{Z} : \begin{pmatrix} r & x \\ 0 & r^{-1} \end{pmatrix} \in A \right\}$. By the pigeonhole principle, there is an $\tilde{r} \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $|P_{\tilde{r}}(A)| > 2p^{2/3}$. Let $\begin{pmatrix} t & u \\ 0 & t^{-1} \end{pmatrix}$ be any element of A with $t \neq \tilde{r}$. Then

$$\begin{aligned}
&\begin{pmatrix} t & u \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} \tilde{r} & x \\ 0 & \tilde{r}^{-1} \end{pmatrix} \begin{pmatrix} t^{-1} & -u \\ 0 & t \end{pmatrix} \begin{pmatrix} \tilde{r}^{-1} & -x' \\ 0 & \tilde{r} \end{pmatrix} \\
&= \begin{pmatrix} t\tilde{r} & tx + u\tilde{r}^{-1} \\ 0 & t^{-1}\tilde{r}^{-1} \end{pmatrix} \begin{pmatrix} t^{-1} & -u \\ 0 & t \end{pmatrix} \begin{pmatrix} \tilde{r}^{-1} & -x' \\ 0 & \tilde{r} \end{pmatrix} \\
&= \begin{pmatrix} \tilde{r} & t^2x + (\tilde{r}^{-1} - \tilde{r})ut \\ 0 & \tilde{r}^{-1} \end{pmatrix} \begin{pmatrix} \tilde{r}^{-1} & -x' \\ 0 & \tilde{r} \end{pmatrix} \\
&= \begin{pmatrix} 1 & \tilde{r}(-x' + t^2x) + (1 - \tilde{r}^2)ut \\ 0 & 1 \end{pmatrix},
\end{aligned}$$

and thus, $P_1(AAA^{-1}A^{-1})$ is a superset of $\tilde{r}(-P_{\tilde{r}}(A)+t^2P_{\tilde{r}}(A))+(1-\tilde{r}^2)ut$. Define

$$S=\{\, t\in(\mathbb{Z}/p\mathbb{Z})^*\setminus\tilde{r} : P_t(A)\neq\emptyset\,\}\,.$$

Since $|A|>2p^{5/3}$ and $|P_{\tilde{r}}(A)|\leq p$, we know that $|S|>\frac{1}{p}(2p^{5/3}-p)>p^{2/3}$. By Lemma 2.1.21, there is a $\tilde{t}\in S$ such that

$$\begin{aligned}|\tilde{r}(-P_{\tilde{r}}(A)+\tilde{t}^2P_{\tilde{r}}(A))+(1-\tilde{r}^2)u\tilde{t}| &= |P_{\tilde{r}}(A)-\tilde{t}^2P_{\tilde{r}}(A)|\\ &\geq\left(\frac{1}{p}+\frac{p}{\frac{1}{2}|S||P_{\tilde{r}}(A)|^2|}\right)^{-1}\\ &>\left(\frac{1}{p}+\frac{1}{2p}\right)^{-1}\\ &=\frac{2}{3}p.\end{aligned}$$

Thus, by Lemma 2.1.3,

$$\tilde{r}(-P_{\tilde{r}}(A)+\tilde{t}^2P_{\tilde{r}}(A))+(1-\tilde{r}^2)u\tilde{t}+\tilde{r}(-P_{\tilde{r}}(A)+\tilde{t}^2P_{\tilde{r}}(A))+(1-\tilde{r}^2)u\tilde{t}=\mathbb{Z}/p\mathbb{Z},$$

and it follows that $AAA^{-1}A^{-1}AAA^{-1}A^{-1}$ contains all matrices $\begin{pmatrix}1&x\\0&1\end{pmatrix}, x\in\mathbb{Z}/p\mathbb{Z}$. □

We can now use this lemma about the behavior in Borel subgroups to make a statement on the general case.

Proposition 2.4.3. *Let p be a prime. Let A be a subset of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ not contained in any proper subgroup thereof. Assume that $|A|>p^\delta$ for some fixed $\delta>0$. Then there is an integer $k>0$, depending only on δ, such that every element of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ can be expressed as a product of at most k elements of $A\cup A^{-1}$.*

Proof. By Proposition 2.3.12, we may assume that

$$|A|>6p^{8/3}>(2p^{5/3}+1)(p+1).$$

We also know that for some fixed tuple (a,b) with $a,b\in(\mathbb{Z}/p\mathbb{Z})^*$, there are exactly $(p-1)$ tuples that are just products of (a,b) with a scalar in $(\mathbb{Z}/p\mathbb{Z})^*$. This means that there are exactly

$$\frac{p(p-1)}{p-1}+1=p+1$$

tuples (a,b) with $a,b\in\mathbb{Z}/p\mathbb{Z}$ such that no tuple is the product of another with some scalar in $(\mathbb{Z}/p\mathbb{Z})^*$. Hence, by the pigeonhole principle, there are at least $(2p^{5/3}+1)$ matrices in A with the same lower row up to multiplication by a scalar in $(\mathbb{Z}/p\mathbb{Z})^*$; the same holds, naturally, for the upper row. Since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ \lambda c & \lambda d \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \lambda d & -b' \\ -\lambda c & a' \end{pmatrix} = \begin{pmatrix} \lambda(ad-bc) & a'b-ab' \\ 0 & a'd-b'c \end{pmatrix},$$

this means that there are at least $(2p^{5/3}+1)$ upper-diagonal matrices and at least $(2p^{5/3}+1)$ lower-diagonal matrices in $C = AA^{-1}$. By Lemma 2.4.2, C_8 contains all matrices of the form $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$, $x, y \in \mathbb{Z}/p\mathbb{Z}$. Every element of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ can be written in the form

$$\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y' & 1 \end{pmatrix} \begin{pmatrix} 1 & x' \\ 0 & 1 \end{pmatrix},$$

where $x, y, x', y' \in \mathbb{Z}/p\mathbb{Z}$. Hence $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = C_8C_8C_8C_8 \subset A_{64}$. □

Chapter 3

Consequences and further outlook

This chapter is split into two sections. The first deals with how Helfgott's results on growth in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ led to other results in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ itself, while the second discusses generalizations of the methods used to prove similar statements for other groups. We will make extensive use of Landau-notation, in particular big O notation; that is, for two functions f, g, we say that $f(x) = O(g(x))$ if there is a constant K such that $|f(x)| \leq K|g(x)|$ for all x large enough.

3.1 Results in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$

The discussion here will be twofold. In **3.1.1** we will start by taking a look at a result on the diameter of subsets in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ that was included in [Hel08] itself, which motivates a statement on expander graphs by Bourgain and Gamburd in [BG08] that will be presented in **3.1.2**.

3.1.1 On the diameter of groups

Most of the statements in this chapter are based on [Hel08] and [Hel14]. Let us start by stating what we mean by the *diameter* of a group with respect to a generator-set.

Definition 3.1.1. *Let G be a finite group and A a subset that is not contained in any proper subgroup thereof (or, equivalently, that generates G). Then we define the* diameter *of G with respect to A as*

$$\mathrm{diam}_A(G) = \min\left\{ k \in \mathbb{Z} : \underbrace{AA\cdots A}_{k\ times} = G \right\},$$

or in other words, the smallest integer k such that every element of G can be expressed as a product of at most k elements of A.

Hence, Proposition 2.4.3 tells us that for any symmetric set A of generators of $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ with $|A| > p^{\delta}$, there will be an integer k that only depends on δ such that $\mathrm{diam}_A(G) \leq k$. Notably, this means that k does not depend on the choice of A.
The choice of words is not arbitrary; it stems from the fact the diameter of G will be the graph-theoretical diameter of its *Cayley graph.* Let us formulate what we mean.

Definition 3.1.2. (Cayley graph)
Let A be a subset of a finite group G. Then the associated Cayley graph *will be the graph $\Gamma(G, A)$ that has the elements of G as vertices, and two vertices $g, h \in G$ have an edge (g, h) if there exists an element a in A such that $h = ga$, i.e.*

$$\begin{aligned} &V\left(\Gamma(G, A)\right) = G \\ &E\left(\Gamma(G, A)\right) = \left\{\, (g, ga) : g \in G, a \in A \,\right\}. \end{aligned}$$

If A is symmetric (i.e. $A{=}A^{-1}$), this graph is undirected, and, as can be seen by the definition, $|A|$-regular, i.e. each vertex g will appear in exactly $|A|$ edges.

Definition 3.1.3. (Diameter of a graph)
Let $G = (V, E)$ be a finite graph. Denote by $P(v, w)$ the set of paths between two vertices v, w. Then the diameter *of G is defined as*

$$\mathrm{diam}(G) = \max_{v,w \in V} \mathrm{dist}(v, w),$$

where $\mathrm{dist}(v, w) = \min\limits_{p \in P(v,w)} \mathrm{length}(p)$ *denotes the* distance *of v and w in G.*

One directly sees how the definitions of the diameter of the Cayley graph of G with respect to the generator set A and the diameter of A itself coincide, provided that the set is symmetric and that the identity 1 is contained in it. This way of seeing groups as geometric objects is one of the main ideas of the field of *geometric group theory.* If the reader is so inclined, a good place to start reading about how algebraic properties of groups affect the associated Cayley graph is a blog post by Tao ([Tao10]). Let us return to the topic at hand. Babai conjectured in [BS88] that, for any finite, non-abelian simple group G and any set of generators A, the diameter of G with respect to A is $O\left((\log |G|^c)\right)$, where c is an absolute constant. Helfgott used Propositions 2.3.12 and 2.4.3 to prove this conjecture for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ in [Hel08].

Theorem 3.1.4. *Let p be a prime. Let A be a set of generators of $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Then the Cayley graph $\Gamma(G, A)$ has diameter $O((\log p)^c)$, where c and the implied constant are absolute.*

Proof. The statement follows immediately from Propositions 2.3.12 and 2.4.3, provided $|A|$ is larger than an absolute constant. But since $|A \cup AA| \geq |A| + 1$ for any A that is not a subgroup of G, we may increase the cardinality of A by an absolute constant C simply by multiplying A by itself C times. Further note Theorem 1.4 in [Bab06], which states that the diameter of a group G with respect to a set of generators A is at most $d^2(\log |G|)^3$, where d denotes the diameter of G with respect to the set of generators $A \cup A^{-1}$. □

Note that, technically, $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is not simple, so the conjecture was actually proved for $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$, the *projective special linear group.* If we now look at special generator-sets, we can make even stronger statements. Take for example a subset A of $G = \mathrm{SL}_2(\mathbb{Z})$ such that its projection A_p modulo p generates $G_p = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. One can then show (cf. [Hel14] §5.5) that the diameter of G_p with respect to A_p will have a logarithmic bound $O_A(\log |G|)$, which obviously implies the same for the diameters of associated Cayley graphs. This leads directly into the next section.

3.1.2 Expansion

We have already introduced the concept of *expander graphs* informally in **1.1.3**. One property of them is the fact that they have small (meaning logarithmic) diameter; while the reverse is not true in general, the results in **3.1.1** still lead one to consider checking those Cayley graphs for expansion properties. Bourgain and Gamburd did as much in [BG08] and proved important results related to the construction of families of expander graphs in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

Before getting to this, we will give a formal introduction to the topic of expansion based on [HLW06]; this survey by Hoory, Linial and Wigderson is also a good place for further reading on the topic, should one be so inclined.

Definition 3.1.5. (Expansion, expansion coefficient)
Let $G = (V, E)$ be an undirected d-regular graph (i.e., each vertex $v \in V$ appears in exactly d edges $e \in E$), and $W \subset V$ a vertex-subset. Then the expansion *of W is defined as*

$$h(W) = \frac{|\partial(W)|}{|W|},$$

where $\partial(W) = \{\, v \in V : \mathrm{dist}(v, W) = 1 \,\}$ *is the* edge boundary *of* W*. The* expansion coefficient *is then defined as*

$$h(G) = \inf \left\{ \, h(X) : |X| \le \frac{1}{2}|V| \, \right\}.$$

We now come to the first definition of expander graphs, which, as would be expected by the definitions above, is combinatorial in nature.

Definition 3.1.6. *A sequence* $(G_n = (V_n, E_n))_{n\in\mathbb{N}}$ *of d-regular, undirected graphs forms a* family of ϵ-expander graphs *if there exists a fixed constant* $\epsilon > 0$ *such that*

$$\liminf_{n\to\infty} h(G_n) \ge \epsilon.$$

Let us now formally prove a property of expanders that we already mentioned above, they have diameter that is logarithmic regarding their number of vertices.

Lemma 3.1.7. *Let* $\epsilon > 0$ *be fixed and let* $G = (V, E)$ *be an* ϵ*-expander, i.e.* $h(G) \ge \epsilon$*. Then*

$$\mathrm{diam}(G) = O(\log |V|)$$

Proof. Since $h(G) \ge \epsilon$, we know by definition that $h(W) \ge \epsilon$ for any subset $W \subset V$ with cardinality $|W| \le |V|/2$. Define the n-th neighborhood of W recursively by $\partial^1(W) = \partial(W)$ and $\partial^n(W) = \partial(\partial^{n-1}(W))$ for any $n \ge 2$. By definition of $\partial(W)$, this will be the set of vertices in V that have distance at most n from W. Now let v, w be vertices of G. Then, because of the expansion property, we get that

$$|\partial^n(\{v\})| \ge \min\{|V|/2, \epsilon^n\}.$$

Now because of the identity

$$\epsilon^{C\log(|V|)} = e^{\log\left(\epsilon^{C\log(|V|)}\right)} = e^{C\log(|V|)\log(\epsilon)} = e^{\log\left(|V|^{C\log(\epsilon)}\right)} = |V|^{\log(\epsilon^C)}$$

we can find a constant $C > 0$ such that $\epsilon^{C\log(|V|)}$ is larger than $|V|/2$ and thus, at least half of all vertices have distance at most $C\log(|V|)$ from v. The same argument can of course be done for w. By the pigeonhole principle, there has to be a vertex $u \in V$ that has distance at most $C\log(|V|)$ from both, which implies that there is a path from v to w of length at most $2C\log(|V|)$. Hence, $\mathrm{diam}(G) = O(\log |V|)$. □

We will now work towards a different, but equivalent definition of expander graphs that is more algebraic in nature. For this, we first have to define the *adjacency matrix* of a graph.

Definition 3.1.8. (Adjacency matrix)
Let $G = (V, E)$ be a graph on n vertices, fix an ordering $\{v_1, \ldots, v_n\}$. Then the adjacency matrix *of G is the $n \times n$ matrix $A(G)$ where*

$$a_{ij} = |\{\, e \in E : e \textit{ is an edge from } v_i \textit{ to } v_j \,\}| \,.$$

This is a matrix with real entries and, at least for the undirected case, it is also symmetric. Hence, it has n real eigenvalues which we can order by size and denote $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. We call this the *spectrum* of $A(G)$. It also has an orthonormal basis of eigenvectors $x_1, \ldots, x_n$ such that $A(G)x_i = \lambda_i A(G)$. Let us state some important facts about this matrix

Lemma 3.1.9. *Let $G = (V, E)$ be an undirected, d-regular graph on n vertices $v_1, \ldots, v_n$. Let $A = A(G)$ denote its adjacency matrix, and* $\mathrm{Spec}(A) = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n)$ *the spectrum thereof. Then A has the following properties:*

i) *For an integer m, the entry a'_{ij} of the m-fold product A^m is the number of different walks (meaning paths where the same edge may appear multiple times) from v_i to v_j.*

ii) *$\lambda_1 = d$ with associated (normalized) eigenvector* $(1/\sqrt{n}, \ldots, 1/\sqrt{n})$.

iii) *G is connected if and only if $\lambda_1 > \lambda_2$.*

iv) *If G is bipartite, then $\lambda_n = -\lambda_1$.*

Proof. The first property follows directly from the definition of the adjacency matrix and induction on m. Properties iii-v) follow from the *Perron-Frobenius Theorem* (cf. [GR01] Theorem 8.8.1). □

One notes that the first property holds for arbitrary graphs. The third property interests us the most, because the difference between the two largest eigenvalues is directly related to the graph's expansion coefficient. This is expressed in the Cheeger-Buser inequality.

Theorem 3.1.10. *Let G be an undirected d-regular graph on n vertices, with spectrum $\lambda_1 \geq \cdots \geq \lambda_n$. Then*

$$\frac{d - \lambda_2}{2} \leq h(G) \leq \sqrt{2d(d - \lambda_2)}.$$

For the continuous case, this was first proved by Cheeger in [Che79] and Buser in [Bus82]. The discrete analogue that interests us was proved independently by Dodziuk in [Dod84] and Alon-Milman in [AM95]. The term $d - \lambda_2$ is called the *spectral gap*, and the theorem states that this gap provides us with an estimate of a graph's expansion coefficient. We can now use this theorem to arrive at an equivalent definition of expanders using the spectral gap.

Definition 3.1.11. *Let $(G_n)_{n\in\mathbb{N}}$ be a sequence of undirected d-regular graphs, and denote by $A_n = A(G_n)$ their adjacency matrices. Then the G_n form a family of expander graphs if*

$$\limsup_{n\to\infty} \lambda_2(A_n) < d.$$

We will finish this introductory segment by stating another important fact about expander graphs related to random walks, the *expander mixing lemma*.

Lemma 3.1.12. *Let $G = (V, E)$ be an undirected, d-regular graph with n vertices. Denote $\lambda = \max\{|\lambda_2|, |\lambda_n|\}$, the eigenvalue with largest absolute value apart from $\lambda_1 = d$. Then, for all $S, T \subset V$*

$$\left| |E(S,T)| - \frac{d|S||T|}{n} \right| \leq \lambda\sqrt{|S||T|},$$

where $|E(S,T)|$ is the number of edges from S to T.

Proof. Cf. [HLW06] Lemma 2.5. □

Let us talk a bit what exactly this lemma tells us. The edge density of an undirected graph is the quotient

$$D = \frac{2|E|}{|V|(|V|-1)}.$$

As a quick aside, the maximal number of edges a graph can have is $|V|(|V|-1)/2$, which is realized by the *complete graph*, so the maximal edge density is 1. The minimal edge density is 0, which was proved by Coleman and Moré in [CM83].

The term $d|S||T|/n$ refers to the expected number of edges between S and T in a random graph of edge density d/n. So a small λ (and hence a large spectral gap) implies that this deviation is small or, in other words, the graph is nearly random under this aspect.

We now return to the case of Cayley graphs of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ with respect to different generator-sets. Proposition 2.3.12 served as a starting point for Bourgain and Gamburd to take a different approach (namely, one related to arithmetic combinatorics) to tackle this problem. Work in this regard was of course done before. Let for example A be a subset of $G = \mathrm{SL}_2(\mathbb{Z})$ with finite index (i.e. there are only finitely many cosets of A in G), and let A_p denote the natural projection of A to $G_p = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Using Selberg's 3/16 theorem (cf. [Sel65]), one can prove (see e.g. Theorem 4.3.2 in [Lub94]) that the Cayley graphs $\Gamma(G_p, A_p)$ then form a family of expanders as p tends to infinity. Now, one naturally asks whether this is also true for arbitrary projections of subsets of $\mathrm{SL}_2(\mathbb{Z})$, provided they are generating $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. This remained unanswered for a long time, and even seemingly simply examples were not solved. For example, taking

$$A_1 = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$$
$$A_2 = \left\{ \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \right\},$$

Selberg's theorem implies that the $\Gamma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), A_1 \bmod p)$ form a family of expanders, but A_2 has infinite index in $SL_2(\mathbb{Z})$, so one could not apply this. Bourgain and Gamburd answered this question conclusively.

Theorem 3.1.13. *Let A be a subset of $\mathrm{SL}_2(\mathbb{Z})$. Then the Cayley graphs $\Gamma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), A \bmod p)$ form a family of expanders if and only if $\langle A \rangle$ contains no solvable subgroup of finite index.*

In the same paper, they also proved a result on expansion for random sets.

Theorem 3.1.14. *Fix a $k \geq 2$. Let $a_1, \ldots, a_k$ be chosen uniformly at random in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ and denote $A_p^{rand} = \{a_1, a_1^{-1}, \ldots, a_k, a_k^{-1}\}$. Then there is a constant K that only depends on k such that as $p \to \infty$ asymptotically almost surely*

$$\lambda_2(A(\Gamma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), A_p^{rand}))) \leq K < 2k.$$

Both of these are results are consequences of a third theorem. Remember that the *girth* of a graph $G = (V, E)$ is the length of its shortest cycle (where cycles are paths with identical starting and ending point).

Theorem 3.1.15. *Fix a $k \geq 2$ and suppose that $A_p = \{a_1, a_1^{-1}, \ldots, a_k, a_k^{-1}\}$ is a (symmetric) generating set for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ such that*

$$\mathrm{girth}(\Gamma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), A_p)) \geq C \log_{2k} p,$$

for a fixed absolute constant C. Then the Cayley graphs $\Gamma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), A_p)$ form a family of expanders.

We will first explain how one obtains Theorems 3.1.13 and 3.1.14 from Theorem 3.1.15.

Proof of Theorem 3.1.13. We use the fact that if $\langle A \rangle$ is a *free group*, the girth of the associated Cayley graph has the required bound in order to apply Theorem 3.1.15. For a proof of this, see e.g. [Gam02].
Free groups are (up to isomorphy) groups that are generated by an *alphabet* A such that two expressions are different unless their equality follows from *reduction* (meaning, if an element x and its inverse are next to each other, they are both omitted, and the expression xx^2 would be replaced by x^3).
Another way to define free groups is by their universal property: A group G is a free group generated by a subset A if and only if for any group H and any map $f\colon A \to H$, there is a unique group homomorphism $\varphi\colon G \to H$ such that $f = \varphi \circ i$, where i is the inclusion map from A into G. For the general case, one uses the fact that

$$\langle A \rangle \cap \left\{ x \in \mathrm{SL}_2(\mathbb{Z}) : x \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p \right\}$$

is a free group. □

Proof of Theorem 3.1.14. Let $k \geq 2$ be fixed. We use the following result, proved in [Gam+09]: As $p \to \infty$, asymptotically almost surely the girth of the k-regular random Cayley graph of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ fulfills the requirements of Theorem 3.1.15. □

We will not go into detail in regards to the proof of Thm 3.1.15, but the general strategy and ideas will be presented. Bourgain and Gamburd use an approach due to Sarnak and Xue in [SX91] that obtains results on the spectral gap by exploiting two properties: The first is the fact that nontrivial eigenvalues of $A(\Gamma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), A_p))$ must appear with high multiplicity. This essentially follows from a result going back to Frobenius. The second property is an upper bound on the number of returns to the identity for random walks of length of order $\log|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})|$. Bourgain and Gamburd's approach was novel in how they obtained this upper bound, namely the usage of arithmetic combinatorics. The main argument is a statement on the ℓ_2 "flattening" of measures that they derive from a non-commutative version of the Balog-Szemerédi-Gowers theorem (proved by Tao in [Tao08]) and prove using Proposition 2.3.12.
One question that still remains open is whether the $\Gamma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), A_p)$ form a family of expanders as A_p ranges over all generating sets of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. We will now get to a different question, namely what happens if we change the group itself.

3.2 Generalization to different groups

The first section of this part will discuss how some specific parts of Helfgott's proof of the $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ case presented in Chapter 2 had to be changed in order to generalize the result to $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$ and onwards. The general approach is based mostly on work done by Helfgott himself in [Hel11], but important aspects where developed by Pyber-Szabó in [PS] and Breuillard-Green-Tao in [BGT11] that will also be included here. After that, we will take a quick look at recent developments concerning the topic of the diameter of permutation groups, based on results by Helfgott and Seress in [HS14].

3.2.1 A new approach for $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$

Let us begin by stating the result, and then continue on to explain the problems that caused some aspects of the proof for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ to not be applicable for more general cases. Propositions 2.3.12 and 2.4.3 (and hence, Thm 3.1.4) are true for $\mathrm{SL}_n(\mathbb{F}_p)$, with p a prime, but only if the constants are allowed to depend on n. This was proved independently by Pyber-Szabó in [PS] and Breuillard-Green-Tao in [BGT11]. Note that for $n = 3$, Helfgott proved this for an absolute constant in [Hel11]. Now we will talk abot some of the adjustments that had to be made to generalize the two propostitions. This was definitely not an easy problem (even just for the case $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$), so most of the discussion here will be somewhat superficial, and a more thorough and formal analysis can for example be seen in [Hel14].
A key change that had to be made was the general view point. Instead of viewing groups themselves as the main object of study, one should actually focus on group actions. The escape lemma continues to play an important role, and one can easily see that statements like Lemma 2.3.2 could just as well have been stated as a corollary thereof, although the direct proofs used in the approach of Helfgott in [Hel08] did provide us with better bounds. Another basic, but helpful tool is the *orbit-stabilizer theorem for sets.* Note that if a group G acts on a set X and $x \in X$, the *stabilizer* of x is the set $\mathrm{Stab}(x) = \{ g \in G : g \cdot x = x \}$.

Theorem 3.2.1. (Orbit-stabilizer theorem for sets)
Let G be a group acting on a set X. Let $x \in X$, and let $A \subset G$ be non-empty. Then

$$|(A^{-1}A) \cap \mathrm{Stab}(x)| \geq \frac{|A|}{|A \cdot x|}.$$

Moreover, for every $B \in G$,

$$|BA| \geq |A \cap \mathrm{Stab}(x)||B \cdot x|.$$

Again, one sees that the actual object of study are group actions. Applying this theorem to the group action $G \curvearrowright X = G/H$ defined by group multiplication, or to the action $G \curvearrowright G$ defined by conjugation gives several helpful results (cf. [Hel14] Lemmata 4.2-4.5).
Another aspect that made that proof hard to generalize was the usage of the sum-product theorem by Bourgain-Katz-Tao. Let us start by recalling how exactly this theorem was applied in the proof. Helfgott made use of the identity

$$\mathrm{Tr}(g)\,\mathrm{Tr}(h) = \mathrm{Tr}(gh) + \mathrm{Tr}(gh^{-1}),$$

which is valid for $g, h \in A \subset \mathrm{SL}_2(K)$ for some subset A and a field K. Now, the sum-product theorem will imply that either the product or the sum-set of $\mathrm{Tr}(A)$ will grow, and by the identity above, actually both will (cf. Proposition 2.2.1). We continue and ultimately arrive at Proposition 2.3.11, in which we relate growth of $\mathrm{Tr}(A_k)$ as k increases to growth of A itself. While it was shown that one can take just about any identity involving traces (see e.g. [Hel11]), the reliance on these kinds of identities still made generalizations for some specific cases impossible. The papers by Breuillard-Green-Tao and Pyber-Szabó cited above showed that one can forgo identities of these kinds altogether. They use a dimensional estimate similar to, but more general than Lemma 2.3.8, which then, together with the orbit-stabilizer theorem implies a stronger version of Proposition 2.3.1. Specifically, the proposition Helfgott proved in the SL_2 case only stated that there are certain group elements g such that their centralizer has a large intersection with A_2. One could then use the same argument to show that it is in fact true for *most* elements g. But the same could not be said for all of them. This problem proved to be a rather large nuisance, because it required the rest of the arguments to be more indirect and harder to generalize. The version we obtain (cf. [Hel14] Corollary 5.4) by the new adjustments gives this statement for all regular semisimple elements (which in case of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ implies a trace different from ± 2).
An important aspect of the overall strategy is the use of *pivots*, which are elements $\xi \in A$ such that the function

$$\begin{aligned} A/\{\pm e\} \times T/\{\pm e\} &\to G/\{\pm e\} \\ (a,t) &\mapsto a\xi t\xi^{-1} \end{aligned}$$

is injective, where T is a maximal torus (in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ this would just be the set of matrices that are diagonal in some fixed basis). This injection will then help in proving statements on growth. One has to be a bit more precise and consider the cases that there are no pivots or pivots as well as non-pivots (cf. [Hel14] Proof of Theorem 5.7).

All these changes helped to generalize the statement and prove Propositions 2.3.12 and 2.4.3 to $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$, provided that ε is allowed to depend on n. We also know that there are counterexamples for these statements for fixed $\varepsilon > 0$ when $n \to \infty$ (cf. [PS] §14). But while we therefore cannot infer Theorem 3.1.4 from these propositions like we did before, the question still remains open if it may be true for (implied) constants independent of n. The mentioned counterexamples are similar in their arguments to ones that were given for permutation groups, so one expects ways of dealing with the combinatorial difficulties of those groups to also help with the problem of unbounded rank in matrix groups.

3.2.2 Permutation groups

Let us first talk about why the question of permutation and their diameter comes natural. By the *Classification of Finite Simple Groups*, every finite, simple, non-abelian group is either a matrix group, $\mathrm{Alt}(n)$, that is, the alternating group of order at least 5 or one of a finite list of exceptions which are irrelevant for our asymptotic statements. So while the work before answers a lot of the questions regarding Babai's conjecture and growth in groups for matrix groups, the case of permutation groups remained fairly wide open. Of course, questions about the diameter of permutation groups were already posed independently of the context of finite simple groups, since they have a very intuitive interpretation even for non-mathematicians. Permutation based puzzle (think Rubik's Cube) can be associated with a certain group, so the question of the diameter becomes the question of the longest *short solution* to a given position of the puzzle. So we can paraphrase the question of a small diameter to: "If a permutation puzzle has a solution, does it also have a *short* solution?" The answer is yes, as Helfgott and Seress found in [HS14], provided that the group is transitive, meaning that for every two elements x, y in the finite set being acted upon (by permutation), there is a succession of moves that takes x to y. To be more specific, they proved the following quasipolynomial bound for the diameter of $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$.

Theorem 3.2.2. *Let* $G = \mathrm{Sym}(n)$ *or* $\mathrm{Alt}(n)$. *Then*

$$\mathrm{diam}(G) \leq \exp\left(O((\log n)^4 \log\log n)\right),$$

where the implied constant is absolute.

Note that by $\mathrm{diam}(G)$, we mean the maximal diameter $\mathrm{diam}_A(G)$ over all generating sets A of G. Babai and Seress already proved in [BS92], that you can bound the diameter of an arbitrary transitive permutation group by the diameter of the alternating group.

Theorem 3.2.3. *Let G be a transitive permutation group of degree n. Then*

$$\operatorname{diam}(G) \leq \exp\left(O(\log n)^3\right) \operatorname{diam}(\operatorname{Alt}(k)),$$

where $\operatorname{Alt}(k)$ *is the largest alternating composition factor of G.*

Helfgott and Seress now use this result and Theorem 3.2.2 to come to the following conclusion for transitive permutation groups, which also provides an affirming answer to a conjecture stated in [BS92].

Corollary 3.2.4. *Let G be a transitive permutation group of degree n. Then*

$$\operatorname{diam}(G) \leq \exp\left(O((\log n)^4 \log\log n)\right).$$

One should note that Helfgott and Seress' use of Theorem 3.2.3 is not restricted to the proof of Corollary 3.2.4, but is also applied in the proof of their main theorem itself. Therefore, since Theorem 3.2.3 relies on the Classification of Finite Simple Groups, so does Theorem 3.2.2. Another aspect is that we require transitivity. Babai and Seress proved the bound

$$\operatorname{diam}(G) \leq \exp\left((1+o(1))\sqrt{n\log n}\right)$$

for general permutation groups G of degree n, which one can show to be tight for some non-transitive groups.
So how does the proof relate to the work done in Chapter 2 and the general changes introduced in **3.2.1**? The orbit-stabilizer theorem for sets still plays a large role, and so naturally does the general concept of looking at group actions instead of groups. There are still big changes though, mainly due to the fact that one cannot use dimensional estimates or escape-from-subvarieties arguments. Some of the main tools Helfgott and Seress use are *classification-free arguments* on the properties of subgroups of $\operatorname{Sym}(n)$, including [Bab82] and [Pyb93] which state useful results for 2-transitive groups. Like before, what is used are often not the main results of these particular articles, but rather intermediate ones that can then be used to generalize. For [Bab82], for example, what is actually used is the *splitting lemma* (cf. [HS14] Proposition 5.2). One can then use the orbit-stabilizer theorem for sets to change these statements on subgroups to results on slowly growing sets.

3.3 Conclusion

Let us summarize what was covered in the process of this thesis. We started by giving a general idea of the situation regarding the topic of *growth in* *groups* before the publication of [Hel08]. Chapter 2 was dedicated to presenting the proof of Helfgott's main results regarding growth in $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, namely that for every generating subset $A \subset G$, there are absolute constant $\varepsilon > 0$ and $k \geq 1$ such that either $|AAA| > |A|^{1+\varepsilon}$, or every element of G can be written as the product of at most k elements of $A \cup A^{-1} \cup \{1\}$. In the process, we also were able to present proofs of several standard results in the relatively new mathematical field of *arithmetic combinatorics*, as well as see how commutativity changes arguments therein. The strategy we presented followed [Hel08] directly and therefore used arguments like certain identities only valid for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ that complicated generalizations to matrix groups of higher ranks. This was elaborated upon in **3.2**, giving a general idea how arguments made by Pyber-Seress and Breuillard-Green-Tao remedied some of these problems, which led to the affirmation of Helfgott's $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ results for $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$, provided that the ε may depend on the rank of the group. We also had a quick look at recent results on growth in permutation groups, due to Helfgott-Seress. This was natural in our context, since the *Classification of Finite Simple Groups* tells us that the alternating group $\mathrm{Alt}(n)$ is the only other relevant examples of non-abelian, finite, simple groups. Helfgott and Seress proved a quasipolynomial bound for the diameter of any permutation group with regards to any generating set thereof, provided the group is transitive. This gave an affirmative answer to a conjecture of Babai-Seress from 1992. Since the problems encountered with matrix groups of very large rank and permutation groups are fairly similar, in that counterexamples for more general statements follow a common line of thought, these results showed that striving for rank independence in statements about the diameter of matrix groups is a feasible goal.

The other important topic of this thesis was the concept of *expander graphs.* We started by giving the general idea, they are highly-connected sparse graphs, and continued by giving a general historical overview, as well as some applications of them. Chapter 3 then provided a more formal introduction, as well as the presentation of some of their basic properties. The reason for the inclusion of this topic was made clear as well: Bourgain-Gamburd used Helfgott's result on the growth in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ to give constructions for families of expander graphs in [BG08]. More specifically, they showed that the Cayley graphs of $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ with respect to a subset A_p form a family of expanders, provided A_p is either a projection of a fixed set $A \subset \mathrm{SL}_2(\mathbb{Z})$ that generates G, or a symmetric random set of generators taken uniformly. In proving this, they adapted a classical result of arithmetic combinatorics for sets, the *Balog-Szemerédi-Gowers Theorem* to a statement on measures. This strengthening also helps when one tries to compute good bounds for the diameter of matrix groups over infinite fields like $\mathbb{C}$.

Let us now have a look at some of the open problems that still exist, both with regards to expander graphs in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, as well as growth in groups in general. For the topic of expander graphs in $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, one major open question is whether or not Cayley graphs of G form a family of ϵ-expanders with regards to any symmetric generating set A for some fixed $\epsilon > 0$. There are also conjectures regarding this for general G of bounded rank. Regarding growth in groups, when restricting ourselves to the parts of the problem that we talked about, there are mainly two big questions. The first pertains to $G = \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$: Is it possible to give a bound of the type $\mathrm{diam}_A(G) = O((\log |G|)^c)$, where both $c > 0$ and the implied constant are independent of the rank of G? We already know that rank dependence is necessary for the other statement mentioned above, and thus we were not able to infer a rank independent statement on the diameter from them. On the other hand, as mentioned before, the results on permutation groups give hope that an absolute bound can be given for the diameter. For permutation groups themselves, an older conjecture asks which properties have to be required of the group to get a bound on the diameter of the type $O(n^c)$, where $c > 0$ and the implied constant should be absolute. This conjecture predates Babai's more general conjecture on the diameter of non-abelian, finite, simple groups. Obtaining an answer to this is hard, and there is currently not even a real consensus on whether it should be true or not.

Hopefully, this thesis was able to present some of the rapid development regarding the topic of growth in groups and some of its applications following Helfgott's 2008 paper, as well as the crucial part the tools of arithmetic combinatorics played in it.

References

[AM95] N. Alon and V. Milman. "λ_1, Isoperimetric inequalities for graphs, and superconcentrators". In: *Journal of Combinatorial Theory, Series B* 38.1 (1995), pp. 73–88.

[Bab82] L. Babai. "On the order of doubly transitive permutation groups". In: *Inventiones mathematicae* 65.3 (1982), pp. 473–484.

[Bab06] L. Babai. "On the diameter of Eulerian orientations of graphs". In: *SODA 06: Proceedings of the Seventeenth Annual ACM-SIAM Symposium on Discrete Algorithm.* (Miami, Florida). ACM-SIAM, 2006, pp. 822–831. ISBN: 978-0898716054.

[BS88] L. Babai and Á. Seress. "On the diameter of cayley graphs of the symmetric group". In: *Journal of Combinatorial Theory, Series A* 49.1 (1988), pp. 175–179.

[BS92] L. Babai and Á. Seress. "On the diameter of permutation groups". In: *European Journal of Combinatorics* 13.4 (1992), pp. 231–243.

[BS94] A. Balog and E. Szemerédi. "A statistical theorem of set addition". In: *Combinatorica* 14.3 (1994), pp. 263–268.

[BG08] J. Bourgain and A. Gamburd. "Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$". In: *Annals of Mathematics* 167 (2008), pp. 625–642.

[BKT04] J. Bourgain, N. Katz, and T. Tao. "A sum-product estimate in finite fields, and applications". In: *Geometric and Functional Analysis* 14 (2004), pp. 27–57. arXiv: `math/0301343v3`.

[BGT11] E. Breuillard, B. Green, and T. Tao. "Approximate Subgroups of Linear Groups". In: *Geometric and Functional Analysis* 21.4 (2011), pp. 774–819. arXiv: `1005.1881 [math.GR]`.

[Bus82] P. Buser. “A note on the isoperimetric constant”. In: *Annales scientifiques de l’École Normale Supérieure* 15.2 (1982), pp. 213–230.

[Che79] J. Cheeger. “A lower bound for the smallest eigenvalue of the Laplacian”. In: *Problems in analysis (Papers dedicated to Salomon Bochner, 1969)* (1979), pp. 195–199.

[CM83] T. F. Coleman and J. J. Moré. “Estimation of Sparse Jacobian Matrices and Graph Coloring Blems”. In: *SIAM Journal on Numerical Analysis* 20.1 (1983), pp. 187–209.

[Dod84] J. Dodziuk. “Difference equations, isoperimetric inequality and transience of certain random walks”. In: *Transactions of the American Mathematical Society* 284.2 (1984), pp. 787–794.

[Ele97] G. Elekes. “On the Number of Sums and Products”. In: *Acta Arithmetica* 81.4 (1997), pp. 365–367.

[Gam02] A. Gamburd. “On the spectral gap for infinite index “congruence” subgroups of $\mathrm{SL}_2(\mathbb{Z})$”. In: *Israel Journal of Mathematics* 127.1 (2002), pp. 157–200.

[Gam+09] A. Gamburd et al. “On the girth of random Cayley graphs”. In: *Random Structures and Algorithms* 35.1 (2009), pp. 100–117. arXiv: `0707.1833v1 [math.PR]`.

[Gar10] M. Z. Garaev. “Sums and products of sets and estimates of rational trigonometric sums in fields of prime order”. In: *Russian Mathematical Surveys* 64.4 (2010), pp. 599–658.

[GR01] C. Godsil and G. Royle. *Algebraic Graph Theory*. Graduate Texts in Mathematics 207. Springer, 2001. ISBN: 978-0387952208.

[Gow98] T. Gowers. “A new proof of Szemerédi’s theorem”. In: *GAFA* 8 (1998), pp. 529–551.

[Hel08] H. A. Helfgott. “Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$”. In: *Annals of Mathematics* 167 (2008), pp. 601–623. arXiv: `math/0509024v4`.

[Hel11] H. A. Helfgott. “Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$”. In: *Journal of the European Mathematical Society* 13.3 (2011), pp. 761–851. arXiv: `0807.2027v3 [math.GR]`.

[Hel14] H. A. Helfgott. *Growth in groups: ideas and perspectives*. 2014. arXiv: `1303.0239v6 [math.GR]`.

[HS14] H. A. Helfgott and A. Seress. "On the diameter of permutation groups". In: *Annals of Mathematics* 179.2 (2014), pp. 611–658. arXiv: `1109.3550v5 [math.GR]`.

[HLW06] S. Hoory, N. Linial, and A. Wigderson. "Expander graphs and their applications". In: *Bulletin (New Series) of the American Mathematical Society* 43.4 (2006), pp. 439–561.

[Lub94] A. Lubotzky. *Discrete Groups, Expanding Graphs and Invariant Measures.* Modern Birkhäuser Classics. Birkhäuser, 1994. ISBN: 978-3034603317.

[Lub11] A. Lubotzky. *Expander Graphs in Pure and Applied Mathematics.* 2011. arXiv: `1105.2389 [math.CO]`.

[MT11] G. Malle and D. Testerman. *Linear Algebraic Groups and Finite Groups of Lie Type.* Cambridge Studies in Advanced Mathematics 133. Cambridge University Press, 2011. ISBN: 978-1107008540.

[Pet12] G. Petridis. "New Proofs of Plünnecke-type Estimates for Product Sets in Groups". In: *Combinatorica* 32.6 (2012), pp. 721–733. arXiv: `1101.3507v3 [math.CO]`.

[Pyb93] L. Pyber. "On the orders of doubly transitive permutation groups, elementary estimates". In: *Journal of Combinatorial Theory, Series A* 62.2 (1993), pp. 361–366.

[PS] L. Pyber and E. Szabó. *Growth in finite simple groups of Lie type of bounded rank.* Submitted. arXiv: `1005.1858v2 [math.GR]`.

[Ruz99] I. Ruzsa. "An analog of Freiman's theorem in groups". In: *Structure Theory of Set Addition, Astérisque* 258 (1999), pp. 323–326.

[SX91] P. Sarnak and X. Xue. "Bounds for multiplicities of automorphic representations". In: *Duke Mathematical Journal* 64.1 (1991), pp. 207–227.

[Sel65] A. Selberg. "On the estimation of Fourier coefficients of modular forms". In: *Proceedings of Symposia in Pure Mathematics.* Vol. 8. American Mathematical Society, 1965, pp. 1–15.

[Ser77] J.-P. Serre. *Linear Representations of Finite Groups.* Trans. by L. L. Scott. Graduate Texts in Mathematics 42. Springer, 1977. ISBN: 978-0387901909.

[Tao08] T. Tao. “Product set estimates for non-commutative groups”. In: *Combinatorica* 28.5 (2008), pp. 547–594. arXiv: `math/0601431v3`.

[Tao10] T. Tao. *Cayley graphs and the geometry of groups*. 2010. URL: `https://terrytao.wordpress.com/2010/07/10/cayley-graphs-and-the-geometry-of-groups`.

[TV06] T. Tao and V. H. Vu. *Additive Combinatorics*. Cambridge Studies in Advanced Mathematics 105. Cambridge University Press, 2006. ISBN: 978-0521136563.

Statutory declaration

Ich versichere, die Masterarbeit selbständig und lediglich unter Benutzung der angegebenen Quellen und Hilfsmittel verfasst zu haben.

Ich erkläre weiterhin, dass die vorliegende Arbeit noch nicht im Rahmen eines anderen Prüfungsverfahrens eingereicht wurde.

Berlin, den ....

(Unterschrift)