

Part III – Introduction to Approximate Groups (Ongoing course, rough)

Based on lectures by Dr M. Tointon
Notes taken by Bhavik Mehta

Lent 2019

Contents

1	Small doubling	2
2	Covering and higher sum and product sets	5
3	Approximate Groups	8
4	Stability of approximate closure under basic operations	10
5	Coset progressions, Bohr sets and the Freiman-Green-Ruzsa theorem	13
6	Geometry of Numbers	16
7	Progressions in the Heisenberg group	19
8	Nilpotent Groups	21
9	Torsion-free Nilpotent Approximate Groups: an overview	24
10	Torsion-free Nilpotent Approximate Groups: the details	26
11	p-groups	27
	Index	29

1 Small doubling

Lecture 1 A subgroup $H < G$ is a non-empty set closed under products and inverses. Roughly, an ‘approximate subgroup’ is a subset that is only ‘approximately closed’ under products. (We will make this precise soon). Such sets arise naturally in a number of branches of mathematics, and as such approximate groups have had a broad range of applications. In this course, we will look in detail, for example, at applications to *polynomial growth* (fundamental in geometric group theory) and touch on construction of expander graphs (important in theoretical computer science).

To start with, we will look at a preliminary notion of approximate closure called *small doubling*. In this course, G is always a group, arbitrary unless specified otherwise.

Notation. Given $A, B \subset G$, write

$$\begin{aligned} AB &:= \{ab \mid a \in A, b \in B\} \quad \text{‘Product sets’} \\ A^n &= \underbrace{A \cdot A \cdots A}_{n \text{ times}} \\ A^{-1} &= \{a^{-1} \mid a \in A\} \\ A^{-n} &= (A^{-1})^n \end{aligned}$$

When G is abelian, often switch to additive notation, e.g. $A + B$, nA , $-A$, $-nA$, called ‘Sum sets’.

To say A is closed is to say $A^2 = A$. If A is finite, one way to say that A is ‘approximately closed’ is to say that

$$|A^2| \text{ is ‘not much bigger’ than } |A|.$$

This is the notion of approximate closure that arises when studying polynomial growth or expansion, for example.

To get a feel for what this should mean, let’s look at the possible values of $|A^2|$. Trivially, $|A| \leq |A^2| \leq |A|^2$. Both bounds are attained. However, although the quadratic upper bound on $|A^2|$ in terms of $|A|$ is extremal, in a strict sense, it should not be seen as atypical for the size of A^2 . We will see, for example, in Example Sheet 1 that if A is a set of size n chosen uniformly from $\{1, \dots, n^{100}\}$, then $\mathbb{E}(|A + A|)$ is close to $\frac{1}{2}|A|^2$ (about as large as it can be, because abelian). Therefore, we can view sets satisfying

$$|A^2| = o(|A|^2) \tag{1.1}$$

as being ‘exceptional’, and so condition (1.1) can already be seen as a form of ‘approximate closure’. In this course, we will concentrate on the strongest form of (1.1), where $|A^2|$ is *linear* in $|A|$, in the sense that

$$|A^2| \leq K|A| \tag{1.2}$$

for some $K \geq 1$ fixed a priori.

Since such sets are ‘far from random’ we can expect (1.2) to impose a significant restriction on A . The main aim of this course is to work out how significant.

Definition. Given $A \subset G$, the ratio $\frac{|A^2|}{|A|}$ is called the **doubling constant** of A . If A satisfies (1.2), we’ll say that A has **doubling** at most K , or simply **small doubling**.

Example (Some simple examples).

- (Empty set)

- A a finite subgroup ($K = 1$)
- $|A| \leq K$
- $A \subset \mathbb{Z}$, $A = \{-n, \dots, n\}$, $|A + A| \leq 2|A|$.

This last example is especially important as it shows the theory does not just reduce to subgroups and ‘small’ sets. We’ll develop these examples later in the course.

One main aim will be to prove theorems along the lines of:

A has **small doubling** $\Rightarrow A$ has a certain structure.

When K is very small, this is quite easy, as follows:

Theorem 1.1 (Freiman; proof due to Tao). Let $K < \frac{3}{2}$. Suppose $A \subset G$ and $|A^2| \leq K|A|$. Then there is a subgroup $H < G$ with $|H| = |A^2| (\leq K|A|)$ such that

$$A \subset aH = Ha \quad \forall a \in A$$

(i.e. A is a large portion of a coset of a finite subgroup).

Remark. Converse: If $A \subset xH = Hx$ for $x \in G$, with $H < G$ and $|H| \leq K|A|$ then $|H^2| \leq K|A|$. So this is a complete classification of sets of very **small doubling**.

Lemma 1.2 (Identify H). If $|A^2| < \frac{3}{2}|A|$ then $H = A^{-1}A$ is a subgroup. Moreover, $A^{-1}A = AA^{-1}$ and $|H| < 2|A|$.

Proof. Let $a, b \in A$. The hypothesis gives $|aA \cap bA| > \frac{1}{2}|A|$, so there are more than $\frac{1}{2}|A|$ pairs $(x, y) \in A \times A$ such that $ax = by$, i.e. $a^{-1}b = xy^{-1}$. This immediately gives $A^{-1}A \subseteq AA^{-1}$, and replacing A by A^{-1} gives $AA^{-1} \subseteq A^{-1}A$, so $A^{-1}A = AA^{-1}$ as required.

Since $|A \times A| = |A|^2$ it also implies that

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

(dividing by number of repetitions), as claimed.

Note also that $A^{-1}A$ is symmetric, so it remains to show that $A^{-1}A$ is closed under products.

Let $c, d \in A$. As above, there are more than $\frac{1}{2}|A|$ pairs $(u, v) \in A \times A$ such that $c^{-1}d = uv^{-1}$. This means that for at least one pair (x, y) as above and one pair (u, v) , we have $y = u$. In particular, $a^{-1}bc^{-1}d = xv^{-1} \in AA^{-1} = A^{-1}A$. \square

Lemma 1.3 (Size bound). If $|A^2| < \frac{3}{2}|A|$ then $A^2 = aHa \quad \forall a \in A$ (H as before). In particular, $|H| = |A^2|$.

Proof. First, note that

$$A \subset aH \cap Ha \tag{1.3}$$

by definition of H , so certainly $A^2 \subset aHa$. For the reverse inclusion, let $z \in aHa$. Since H is a subgroup, there are $|H|$ pairs $(x, y) \in aH \times Ha$ such that $z = xy$.

Moreover, by (1.3) and the bound $|H| < 2|A|$ from **Lemma 1.2**, more than half of these x and more than half of these y belong to A . In particular, this means that for at least one pair x, y , both have to belong to A . Hence $z = xy \in A^2$, as required. \square

Proof of Theorem 1.1. Given $a \in A$, we have $Aa^{-1} \subset aHa^{-1} \cap H$ so

$$|aHa^{-1} \cap H| \geq |A| > \frac{1}{2}|H|$$

by Lemma 1.2, but the only subgroup of H of size $> \frac{1}{2}|H|$ is H itself. Hence $aHa^{-1} = H$, so indeed $A \subset aH = Ha$ by (1.3). \square

Classifying the sets of [small doubling](#) is much harder than this in general, and uses a much wider range of techniques, e.g. group theory, harmonic analysis, geometry of numbers...

2 Covering and higher sum and product sets

Lecture 2 We introduce two techniques we'll use repeatedly: *covering* and *bounding higher product sets*. A nice way to do this is by proving the following theorem.

Theorem 2.1 (Ruzsa). Suppose $A \subset \mathbb{F}_p^r$ satisfies $|A + A| \leq K|A|$. Then $\exists H \leq \mathbb{F}_p^r$ with

$$|H| \leq p^{K^4} K^2 |A| \quad \text{such that } A \subset H.$$

So again, like [Theorem 1.1](#), A is a large proportion of a finite subgroup.

Remark. It is not ideal that $\frac{|A|}{|H|}$ depends on p . We will remove this dependency in a few lectures' time.

We'll start by proving the following weaker version:

Proposition 2.2. Suppose $A \subset \mathbb{F}_p^r$ satisfies $|2A - 2A| \leq K|A|$. Then $\exists H < \mathbb{F}_p^r$ with

$$|H| \leq p^K |A - A| (\leq p^K K |A|) \quad \text{such that } A \subset H.$$

We'll prove this using 'covering', encapsulated by the following lemma

Lemma 2.3 (Ruzsa's covering lemma). Suppose $A, B \subset G$ and $|AB| \leq K|B|$. Then $\exists X \subset A$ with $|X| \leq K$ such that $A \subset XBB^{-1}$. Indeed, we may take $X \subset A$ maximal such that the sets xB (for $x \in X$) are disjoint.

The term 'covering' refers to the conclusion $A \subset XBB^{-1}$, which says ' A can be covered by a few left-translates of BB^{-1} '.

Proof. First, disjointness of xB gives that $|XB| = |X||B|$. Since $X \subset A$,

$$|XB| \leq |AB| \leq K|B|,$$

so $|X| \leq K$. By maximality, for all $a \in A$, there is $x \in X$ such that $aB \cap xB \neq \emptyset$, and hence $a \in xBB^{-1}$. Hence $A \subset XBB^{-1}$, as required. \square

Lemma 2.4. Suppose $A \subset G$ satisfies $|A^{-1}A^2A^{-1}| \leq K|A|$. Then $\exists X \subset A^{-1}A^2$, with $|X| \leq K$ such that $A^{-1}A^n \subset X^{n-1}A^{-1}A$ for any $n \in \mathbb{N}$.

Proof. By [Lemma 2.3](#), $\exists X \subset A^{-1}A^2$, $|X| \leq K$ such that

$$A^{-1}A^2 \subset XA^{-1}A. \tag{2.1}$$

We then have

$$\begin{aligned} A^{-1}A^n &= A^{-1}A^{n-1}A \\ &\subset X^{n-2}A^{-1}A^2 \quad \text{by induction} \\ &\subset X^{n-1}A^{-1}A. \quad \text{by (2.1)} \end{aligned} \quad \square$$

Proof of Proposition 2.2. By [Lemma 2.4](#), $\exists X$ with $|X| \leq K$ such that

$$nA - A \subset (n-1)X + A - A \quad \forall n \in \mathbb{N}.$$

This means that $\langle A \rangle \subset \langle X \rangle + A - A$, so

$$|\langle A \rangle| \leq |\langle X \rangle| |A - A| \leq p^K |A - A|$$

as claimed. \square

To strengthen [Proposition 2.2](#) to [Theorem 2.1](#), we use the second technique of this section, bounding higher sum/product sets. The key result is the following, at least in the abelian case.

Theorem 2.5 (Plünnecke-Ruzsa). Suppose $A \subset G$ for G abelian, and $|A + A| \leq K|A|$. Then for all $m, n \geq 0$,

$$|mA - nA| \leq K^{m+n}|A|.$$

This was proved in Introduction to Discrete Analysis last term. We won't redo the whole proof in lectures, but we will reprove some parts of it. See the Example Sheet for the full result.

Proof of Theorem 2.1. Using [Theorem 2.5](#), $|2A - 2A| \leq K^4|A|$, and $|A - A| \leq K^2|A|$. Then immediate from [Proposition 2.2](#). \square

We'll spend the rest of this section discussing [Theorem 2.5](#) and variants of it. We've seen it's useful, at least in one context. To see more philosophically why it's useful, let's think about what the genuine closure of subgroups under products and inverses means. One useful feature is that it can be iterated: given $h_1, h_2, \dots \in H$, a subgroup, this means that $h_1^{\epsilon_1} \cdots h_m^{\epsilon_m} \in H \forall \epsilon_i = \pm 1, \forall m, \forall h_i \in H$. [Theorem 2.5](#) allows us to 'iterate' the 'approximate closure' of a set of [small doubling](#): $a_1 + \cdots + a_m - a'_1 - \cdots - a'_n$ may not belong to A , but at least it belongs to $mA - nA$, which is

- (a) not too large ($|mA - nA| \leq K^{m+n}|A|$)
- (b) itself a set of small doubling ($|2(mA - nA)| \leq K^{2m+2n}|mA - nA|$).

This is an important part of why the theory works so well.

It is therefore unfortunate that [Theorem 2.5](#) does not hold for non-abelian groups:

Example 2.6. Let x generate an infinite cyclic group $\langle x \rangle$, H be a finite group, set $G = H * \langle x \rangle$ (the free product, which has the important property that $x^{-1}Hx \neq H$). Set $A = H \cup \{x\}$. $A^2 = H \cup xH \cup Hx \cup \{x^2\}$, so $|A^2| \leq 3|A|$. But A^3 contains HxH , which has size $|H|^2 \sim |A|^2$.

So as $|H| \rightarrow \infty$, [Theorem 2.5](#) cannot hold.

Nonetheless, if we strengthen [small doubling](#) slightly, we can recover a form of [Theorem 2.5](#). One way is to replace small doubling with [small tripling](#): $|A^3| \leq K|A|$.

Proposition 2.7. Suppose $A \subset G$, $|A^3| \leq K|A|$. Then $|A^{\epsilon_1} \cdots A^{\epsilon_m}| \leq K^{3(m-2)}|A| \forall \epsilon_i = \pm 1, \forall m \geq 3$.

The key ingredient is the following:

Lemma 2.8 (Ruzsa's triangle inequality). Given $U, V, W \subset G$, all finite, we have

$$|U||V^{-1}W| \leq |UV||UW|.$$

Proof. We'll define an injection $\varphi : U \times V^{-1}W \rightarrow UV \times UW$. First, for $x \in V^{-1}W$, set $v(x) \in V$ and $w(x) \in W$ such that $x = v(x)^{-1}w(x)$. Set $\varphi(u, x) = (uv(x), uw(x))$. To see that φ is injective, first observe

$$(uv(x))^{-1}(uw(x)) = x,$$

so x determined by $\varphi(u, x)$, and then

$$(uv(x))v(x)^{-1} = u,$$

so u is also determined by $\varphi(u, x)$. \square

Proof of Proposition 2.7. First we'll do the case $m = 3$.

- $|A^3| = |A^{-3}| \leq K|A|$.
- Apply [Ruzsa's triangle inequality](#) with $U = W = A$, $V = A^2$:

$$|A||A^{-2}A| \leq |A^3||A^2| \leq K^2|A|^2,$$

$$\text{so } |A^{-2}A| \leq K^2|A|.$$

- Note that $(A^{-2}A)^{-1} = A^{-1}A^2$, so $|A^{-1}A^2| = |A^{-2}A| \leq K^2|A|$.
- Replacing A by A^{-1} we get

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

- Finally, [Ruzsa's triangle inequality](#) with $U = V = A$, $W = AA^{-1}$ gives

$$|A||A^{-1}AA^{-1}| \leq |A^2||A^2A^{-1}| \leq K^3|A|^2.$$

$$\text{So } |A^{-1}AA^{-1}| \leq K^3|A|.$$

- For the last case, swap A, A^{-1} again.

For $m \geq 4$, [Ruzsa's triangle inequality](#) gives

$$\begin{aligned} |A||A^{\epsilon_1} \dots A^{\epsilon_m}| &\leq |AA^{-\epsilon_2}A^{-\epsilon_1}||AA^{\epsilon_3} \dots A^{\epsilon_m}| \\ &\leq K^3|A| K^{3(m-3)}|A|. \end{aligned}$$

□

3 Approximate Groups

Lecture 3 In the last section, we saw that assuming [small tripling](#) instead of [small doubling](#) allowed us to control higher product sets of the form $A^{\epsilon_1} \cdots A^{\epsilon_m}$. In this section, we'll see another possible strengthening of small doubling. We also saw, in the proofs of [Theorem 2.1](#) and [Proposition 2.2](#), an advantage of having a 'covering' condition in place of a size bound. This motivates in part the following definition.

Definition. A set $A \subset G$ is called a **K -approximate group** (or K -approximate subgroup) if $1 \in A$, $A^{-1} = A$ and $\exists X \subset G$ with $|X| \leq K$ such that $A^2 \subset XA$.

Note that A need not be finite, although in this course it almost always will be. Also, if A is finite, then $|A^2| \leq K|A|$. The conditions $1 \in A$ and $A^{-1} = A$ are convenient 'notationally': for example, this lets us write A^m instead of $A^{\epsilon_1} \cdots A^{\epsilon_m}$ and $1 \in A$ gives us that $A \subset A^2 \subset A^3 \subset \cdots$, which is also convenient at times. It's the condition $A^2 \subset XA$ that is most important.

For [approximate groups](#), bounding higher product sets is easy:

Lemma 3.1. If A is a finite [K-approximate group](#) then $|A^m| \leq K^{m-1}|A|$.

Proof. If X is as in the definition of [approximate group](#), in fact we have $A^m \subset X^{m-1}A$:

$$\begin{aligned} A^m &= A^{m-1}A \\ &\subset X^{m-2}A^2 \quad \text{induction} \\ &\subset X^{m-1}A \quad \text{definition of } X \end{aligned} \quad \square$$

Another advantage of approximate groups is that if $\pi : G \rightarrow H$ is a homomorphism and $A \subset G$ is a [K-approximate group](#) then $\pi(A)$ is also trivially a K -approximate group (although we'll see that there is a version of this for small tripling).

It turns out that sets of [small tripling](#) and [approximate groups](#) are essentially equivalent, in the following sense:

Proposition 3.2. Let $A \subset G$ be finite. If A is a [K-approximate group](#) then $|A^3| \leq K^2|A|$. Conversely if $|A^3| \leq K|A|$ then there is a $\mathcal{O}(K^{12})$ -approximate group B with $A \subset B$ and $|B| \leq 7K^3|A|$ (' A is a large proportion of an approximate group'). In fact, we may take $B = (A \cup \{1\} \cup A^{-1})^2$.

Proof. First bit is just [Lemma 3.1](#). For the converse, set $\hat{A} = A \cup \{1\} \cup A^{-1}$, and note that

$$B = \hat{A}^2 = \{1\} \cup A \cup A^{-1} \cup A^2 \cup A^{-1}A \cup AA^{-1} \cup A^{-2}.$$

Each set in this union has size $\leq K^3|A|$ by [Proposition 2.7](#), so $|B| \leq 7K^3|A|$, as claimed. Similarly,

$$\hat{A}^4 = \bigcup_{\substack{\epsilon_i = \pm 1 \\ 0 \leq m \leq 4}} A^{\epsilon_1} \cdots A^{\epsilon_m},$$

and the sets in this union have size $\leq K^6|A|$. It follows that $|\hat{A}^4| \leq \mathcal{O}(K^6)|\hat{A}|$.

So, [Lemma 2.4](#) implies $\exists X \subset G$ with $|X| \leq \mathcal{O}(K^6)$ such that $\hat{A}^n \subset X^{n-2}\hat{A}^2$ for every $n \geq 2$. In particular, $|X^2| \leq \mathcal{O}(K^{12})$ and $\hat{A}^4 = (\hat{A}^2)^2 \subset X^2\hat{A}^2$, so \hat{A}^2 is an $\mathcal{O}(K^{12})$ -approximate group, as claimed. \square

This is all well and good, but what if we are faced with a set like that from [Example 2.6](#) which only has [small doubling](#)? In that specific example, a large proportion of A was a set of [small tripling](#), namely H . Rather helpfully, that turns out to be a general phenomenon:

Theorem 3.3. If $A \subset G$ satisfies $|A^2| \leq K|A|$ then there is $U \subset A$ with $|U| \geq \frac{1}{K}|A|$ such that $|U^m| \leq K^{m-1}|U| \forall m \in \mathbb{N}$.

So [small doubling](#) reduces to [small tripling](#), which reduces to [approximate groups](#). In Example Sheet 1, we'll see a direct reduction from small doubling to approximate group.

Tao proved a version of [Theorem 3.3](#) when he introduced the definition of approximate groups. We will use instead a lemma of Petridis, which he proved when proving the [Plünnecke-Ruzsa](#) inequalities.

Lemma 3.4 (Petridis). Suppose $A, B \subset G$ are finite, let $U \subset A$ be non-empty, chosen to minimise the ratio $|UB|/|U|$, and write $R = |UB|/|U|$. Then for any finite $C \subset G$, we have

$$|CUB| \leq R|CU|.$$

Proof. Trivial if $C = \emptyset$, so we may assume $\exists x \in C$. Defining $C' = C \setminus \{x\}$, we may also assume by induction that $|C'UB| \leq R|C'U|$. Set $W = \{u \in U \mid xu \in C'U\}$. Then

$$CU = C'U \cup (xU \setminus xW)$$

is a disjoint union, so in particular

$$|CU| = |C'U| + |U| - |W|. \quad (3.1)$$

We also have $xUB \subset C'UB$ by definition of W , so

$$CUB \subset C'UB \cup (xUB \setminus xWB)$$

and hence

$$|CUB| \leq |C'UB| + |UB| - |WB|. \quad (3.2)$$

We have $|C'UB| \leq R|C'U|$ by the induction hypothesis, $|UB| = R|U|$ by definition of R , and $|WB| \geq R|W|$ by minimality in the definition of U . So

$$\begin{aligned} |CUB| &\leq R(|C'U| + |U| - |W|) \quad \text{by (3.2)} \\ &= R|CU| \quad \text{by (3.1)}. \end{aligned} \quad \square$$

Proof of Theorem 3.3. Set $U \subset A$ to be non-empty minimising $|UA|/|U|$, and write R for this ratio, noting that $R \leq K$ by minimality. Also, U non-empty, so $|UA| \geq |A|$, so $|U| \geq \frac{|A|}{K}$, as required. [Lemma 2.4](#) also implies that $|U^m A| \leq K|U^m| \forall m$ (taking $C = U^{m-1}$) and since $U \subset A$, this gives $|U^{m+1}| \leq K|U^m| \forall m$, so $|U^m| \leq K^{m-1}|U|$. \square

*Bonus content

The reason A in [Example 2.6](#) failed to have [small tripling](#) was the existence of $x \in A$ with AxA large. It turns out that this is the only obstruction to [small doubling](#) having [small tripling](#):

***Theorem 3.5** (Tao; Petridis). If $|A^2| \leq K|A|$ and $|AxA| \leq K|A| \forall x \in A$ then

$$|A^m| \leq K^{O(m)}|A| \forall m \geq 3.$$

4 Stability of approximate closure under basic operations

Lecture 4 Two familiar properties of genuine subgroups are that they behave well under quotients and intersections: if $H < G$ and $\pi : G \rightarrow \Gamma$ is a homomorphism, then $\pi(H) < \Gamma$, and if $H_1, H_2 < G$ then $H_1 \cap H_2 < G$. In this lecture, we'll see versions of these properties for [approximate groups](#) and sets of [small tripling](#).

It's trivial that if $A \subset G$ is a K -approximate group then $\pi(A)$ is also a K -approximate group. The following is the corresponding result for sets of small tripling.

Lemma 4.1 (Stability of [small tripling](#) under homomorphisms). Let $A \subset G$ be finite, symmetric containing the identity. Suppose $\pi : G \rightarrow H$ is a homomorphism. Then

$$\frac{|\pi(A)^m|}{|\pi(A)|} \leq \frac{|A^{m+2}|}{|A|} \quad \forall m \in \mathbb{N}.$$

In particular, if $|A^3| \leq K|A|$ then $|\pi(A)^3| \leq K^9|\pi(A)|$ by [Proposition 2.7](#). We can prove this using an argument of Helfgott. We'll start with a simple observation that we'll use repeatedly in the course.

Lemma 4.2. Let $H < G$, let $A \subset G$ be finite, and let $x \in G$. Then

$$|A^{-1}A \cap H| \geq |A \cap xH|.$$

Proof. We have $(A \cap xH)^{-1}(A \cap xH) \subset A^{-1}A \cap H$. □

Remark. Most of the lemmas and propositions in this section will have familiar/trivial analogues for genuine subgroups. It is a useful exercise to think about what they are.

Lemma 4.3. Let $H < G$, write $\pi : G \rightarrow G/H$ for the quotient map, let $A \subset G$ be finite. Then

$$|A^{-1}A \cap H| \geq \frac{|A|}{|\pi(A)|}.$$

Note that H is not assumed normal, so G/H is just the space of left cosets xH , not necessarily a group.

Proof. The pigeonhole principle gives $\exists x \in G$ such that $|A \cap xH| \geq |A|/|\pi(A)|$. Then apply [Lemma 4.2](#). □

Lemma 4.4. Let $H < G$, write $\pi : G \rightarrow G/H$ for the quotient map, and let $A \subset G$ be finite. Then

$$|\pi(A^m)| |A^n \cap H| \leq |A^{m+n}| \quad \forall m, n \geq 0.$$

Proof. Define $\varphi : \pi(A^m) \rightarrow A^m$ by picking arbitrarily for each $x \in \pi(A^m)$ some $\varphi(x)$ such that $\pi(\varphi(x)) = x$. Then the cosets $\varphi(x)H$ for $x \in \pi(A^m)$ are all distinct by definition, so

$$|\varphi(\pi(A^m))| |(A^n \cap H)| = |\pi(A^m)| |A^n \cap H|.$$

But also, $\varphi(\pi(A^m))(A^n \cap H) \subset A^{m+n}$. □

Proof of [Lemma 4.1](#). Take $H = \ker \pi$. [Lemma 4.4](#) gives

$$|\pi(A^m)| \leq \frac{|A^{m+2}|}{|A^2 \cap H|}.$$

[Lemma 4.3](#) gives

$$|A^2 \cap H| \geq \frac{|A|}{|\pi(A)|}.$$

The proposition follows by combining these inequalities. □

Now we'll look at intersections.

Proposition 4.5 (Stability of [small tripling](#) under intersections with subgroups). Let $A \subset G$ be finite, symmetric, contain 1. Let $H < G$. Then

$$\frac{|A^m \cap H|}{|A^2 \cap H|} \leq \frac{|A^{m+1}|}{|A|}.$$

In particular, by [Proposition 2.7](#), if $|A^3| \leq K|A|$ then $|(A^m \cap H)^3| \leq K^9 |A^m \cap H|$ for any $m \geq 2$.

Remark. We'll see in Example Sheet 1 that even if A has [small tripling](#), $A \cap H$ need not. So $m \geq 2$ really is important for this last conclusion.

Proof. Take $\pi : G \rightarrow G/H$ as before. [Lemma 4.4](#) gives

$$|A^m \cap H| \leq \frac{|A^{m+1}|}{|\pi(A)|}.$$

[Lemma 4.3](#) gives

$$|A^2 \cap H| \geq \frac{|A|}{|\pi(A)|}.$$

Combine these two inequalities. □

Proposition 4.6 (Stability of [approximate groups](#) under intersections with subgroups). Let $H < G$, let $A \subset G$ be a [K-approximate group](#). Then $A^m \cap H$ is covered by $\leq K^{m-1}$ left-translates of $A^2 \cap H$. In particular, $A^m \cap H$ is a K^{2m-1} -approximate group (since $A^2 \cap H \subset A^m \cap H$ and $(A^m \cap H)^2 \subset A^{2m} \cap H$).

Proof. By definition, $\exists X \subset G$ with $|X| = K^{m-1}$ such that $A^m \subset XA$. In particular,

$$A^m \cap H \subset \bigcup_{x \in X} (xA \cap H).$$

For each $xA \cap H$ that is not empty, $\exists h = xa \in H$ for some $a \in A$. This means that

$$xA \cap H \subset h(a^{-1}A \cap H) \subset h(A^2 \cap H).$$

Hence each set $xA \cap H$ in this union is contained in a single left translate of $A^2 \cap H$. □

In Introduction to Discrete Analysis, we saw that when studying [small doubling](#) or [tripling](#) there is a more general notion of homomorphism that comes into play: the Freiman homomorphism. To motivate this, consider two sets $A = \{-n, \dots, n\} \subset \mathbb{Z}/p\mathbb{Z}$, and $B = \{-n, \dots, n\} \subset \mathbb{Z}/q\mathbb{Z}$ for p, q two primes $\geq 10n$, say. These two sets are intuitively 'isomorphic' from the perspective of $A + A$ or $B + B$, but there is no way of encoding this with a group homomorphism $\mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$. Freiman homomorphisms give us a way to encode this.

Definition. Let $m \in \mathbb{N}$, let A, B be subsets of groups.

- A map $\varphi : A \rightarrow B$ is a **Freiman m -homomorphism** if $\forall x_1, \dots, x_m, y_1, \dots, y_m \in A$,

$$x_1 \cdots x_m = y_1 \cdots y_m \implies \varphi(x_1) \cdots \varphi(x_m) = \varphi(y_1) \cdots \varphi(y_m).$$
- If $1 \in A$ and $\varphi(1) = 1$ then we say that φ is **centered**.
- If φ is injective and its inverse $\varphi(A) \rightarrow A$ is also a Freiman m -homomorphism then we say $\varphi : A \rightarrow \varphi(A)$ is a **Freiman m -isomorphism**.

- We often simply write that φ is a ‘Freiman homomorphism’ when it is a Freiman 2-homomorphism.

Remark.

- (1) Every map is trivially a [1-homomorphism](#), so we only care about the cases $m \geq 2$.
- (2) This definition gets stronger as m increases: we may assume $A \neq \emptyset$, and then, picking $a \in A$ arbitrarily, if $x_1 \cdots x_k = y_1 \cdots y_k$ for $k \leq m$ then

$$x_1 \cdots x_k \underbrace{a \cdots a}_{m-k} = y_1 \cdots y_k \underbrace{a \cdots a}_{m-k}.$$

- (3) If φ is a centered m -homomorphism and $a, a^{-1} \in A$ then exercise to check that $\varphi(a^{-1}) = \varphi(a)^{-1}$ (for $m \geq 2$).

Lemma 4.7. Suppose $\varphi : A \rightarrow \Gamma$ is a [Freiman \$m\$ -homomorphism](#). Then

$$|\varphi(A)^m| \leq |A^m|.$$

In particular, if φ is injective then

$$\frac{|\varphi(A)^m|}{|\varphi(A)|} \leq \frac{|A^m|}{|A|},$$

and if φ is a Freiman m -isomorphism then

$$\frac{|\varphi(A)^m|}{|\varphi(A)|} = \frac{|A^m|}{|A|}.$$

Proof. Exercise. □

Lemma 4.8. Let $A \subset G$ be a [K-approximate group](#), and suppose $\varphi : A^3 \rightarrow \Gamma$ is a [centred Freiman homomorphism](#). Then $\varphi(A)$ is also a K -approximate group.

Proof. Take X , $|X| \leq K$ such that $A^2 \subset XA$ as in the definition of [K-approximate group](#). So given $a_1, a_2 \in A \exists x \in X, a_3 \in A$ such that $a_1 a_2 = x a_3$. In particular, $x \in A^3$ so $\varphi(x)$ is defined, and

$$\varphi(a_1)\varphi(a_2) = \varphi(x)\varphi(a_3)$$

Hence $\varphi(A)^2 \subset \varphi(X \cap A^3)\varphi(A)$. Also φ is [centred](#) so $\varphi(A)$ is symmetric and contains 1. □

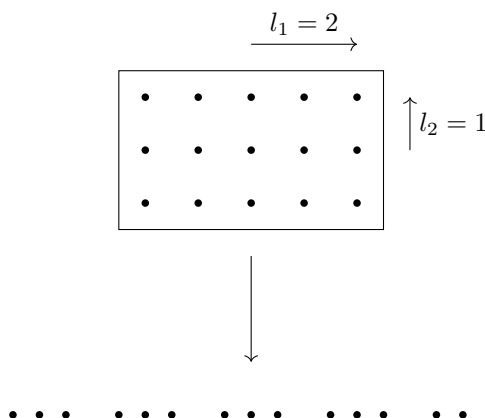
5 Coset progressions, Bohr sets and the Freiman-Green-Ruzsa theorem

Lecture 5 **Definition.** Let G be abelian, $x_1, \dots, x_r \in G$, $L_1, \dots, L_r \in \mathbb{N}$. Then the set

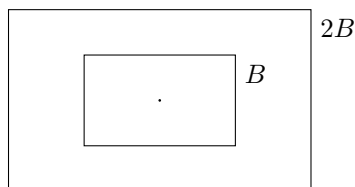
$$P(x; L) = P(x_1, \dots, x_r; L_1, \dots, L_r) = \{l_1 x_1 + \dots + l_r x_r \mid |l_i| \leq L_i \forall i\}$$

is called a **progression** of rank r . If in addition $H < G$ is finite, then $H + P(x, L)$ is called a **coset progression** of rank r .

It is useful to think of $P(x; L)$ as a homomorphic image of a ‘box’ in \mathbb{Z}^r , e.g. if $G = \mathbb{Z}$ and $r = 2$:



It is easy to see that such a box B in \mathbb{Z}^r is a 2^r -approximate group, e.g. in $r = 2$



Hence $P(x; L)$ is also a 2^r -approximate group, as is $H + P(x; L)$. Remarkably, these are essentially the only examples:

Theorem 5.1 (Freiman ($G = \mathbb{Z}$); Green-Ruzsa (arbitrary abelian G)). Suppose $A \subset G$ (abelian) satisfies $|A + A| \leq K|A|$. Then there is a **coset progression** $H + P$ of rank $\leq \mathcal{O}(K^{\mathcal{O}(1)})$ such that

$$A \subset H + P \subset \mathcal{O}(K^{\mathcal{O}(1)})(A \cup \{0\} \cup -A).$$

In particular, **Plünnecke-Ruzsa** gives $|H + P| \leq \exp(\mathcal{O}(K^{\mathcal{O}(1)}))|A|$. So A is a large proportion of $H + P$.

A substantial part of this result was proved in Introduction to Discrete Analysis, but with a slightly less explicit version of coset progressions.

Definition. Let G be a finite abelian group, let

$$\Gamma = \{\gamma_1, \dots, \gamma_r\} \subset \hat{G}$$

(recall $\hat{G} = \text{Hom}(G, \mathbb{R}/\mathbb{Z})$), and let $p \in [0, \frac{1}{2}]$. Then the set

$$B(\Gamma, p) = \{g \in G : \forall i \ \|\gamma_i(g)\|_{\mathbb{R}/\mathbb{Z}} \leq p\}$$

is called a **Bohr set** of rank r . Here, given $x \in \mathbb{R}/\mathbb{Z}$ with representative $\hat{x} \in (-\frac{1}{2}, \frac{1}{2}]$, we write $\|x\|_{\mathbb{R}/\mathbb{Z}} = |\hat{x}|$.

We will see on Sheet 1 that $B(\Gamma, p)$ is a **4^r -approximate group**. Whereas progressions were homomorphic images of boxes, $B(\Gamma, p)$ is the pullback of $[-p, p]^r$ under $(\gamma_1, \dots, \gamma_r) \in \hat{G}^r$.

It turns out that the notions of coset progression and Bohr set are essentially equivalent. In Sheet 2, we will see that every coset progression is a Freiman image of a Bohr set of the same rank. Moreover, every Freiman image of a Bohr set is a large proportion of some coset progression. We will see a special case of that shortly.

Proposition 5.2. Suppose $A \subset G$ (abelian) with $|A + A| \leq K|A|$. Then $\exists B \subset 2A - 2A$, a finite abelian group Z with $|Z| \geq |A|$, a set $\Gamma \subset \hat{Z}$ with $|\Gamma| \leq \mathcal{O}(K^{\mathcal{O}(1)})$, some $p \geq \frac{1}{\mathcal{O}(K^{\mathcal{O}(1)})}$, and a **centered Freiman 2-isomorphism** $\varphi : B(\Gamma, p) \rightarrow B$.

‘ $2A - 2A$ contains a large set isomorphic to a **Bohr set** of bounded rank’.

In Introduction to Discrete Analysis, we saw this in the special case of G torsion-free. The general case is harder, but nonetheless conceptually very similar, so we will assume this result from now on.

To pass from **Proposition 5.2** to **Theorem 5.1**, we use the following results.

Proposition 5.3. Suppose G is a finite abelian group, $\Gamma \subset \hat{G}$ is of size r , $p < \frac{1}{10}$. Then there is a **coset progression** $H + P \subset B(\Gamma, p)$ with rank r and

$$|H + P| \geq \left(\frac{p}{r}\right)^r |G|.$$

Lemma 5.4. Suppose $H + P$ is a **coset progression** of rank r , and $\varphi : H + P \rightarrow G$ (abelian) is a **centered Freiman 2-homomorphism**. Then $\varphi(H + P)$ is also a coset progression of rank r .

Proof. Exercise: If H a group and $\varphi : H \rightarrow G$ is a centered Freiman 2-homomorphism, then φ is also a group homomorphism. In particular, in this lemma $\varphi(H)$ is a finite subgroup. Therefore sufficient to show that

$$\varphi(H + P(x; L)) = \varphi(H) + P(\varphi(x_1), \dots, \varphi(x_i); L_1, \dots, L_r).$$

In fact, we will show that $\forall h \in H, |l_i| \leq L_i$ we have

$$\varphi(h + l_1 x_1 + \dots + l_r x_r) = \varphi(h) + l_1 \varphi(x_1) + \dots + l_r \varphi(x_r). \quad (5.1)$$

Since φ centered, $\varphi(-x_i) = -\varphi(x_i)$, so we may assume $l_i \geq 0 \ \forall i$. Also (5.1) is trivial if $l_i = 0 \ \forall i$, so may assume $\exists l_j > 0$. Then

$$\begin{aligned} \varphi(h + l_1 x_1 + \dots + l_r x_r) &= \varphi(h + l_1 x_1 + \dots + l_r x_r) + \varphi(0) \\ &= \varphi(h + l_1 x_r + \dots + (l_j - 1)x_j + \dots + l_r x_r) + \varphi(x_j) \end{aligned}$$

so the result follows by induction on $\sum_i l_i$. \square

Proof of Theorem 5.1. By **Proposition 5.2** and **Proposition 5.3** and **Lemma 5.4**, $\exists H + P$ a coset progression of rank $\leq \mathcal{O}(K^{\mathcal{O}(1)})$ such that $H + P \subset 2A - 2A$ and $|H + P| \geq \exp(-\mathcal{O}(K^{\mathcal{O}(1)}))|A|$. We will now apply a version of Ruzsa’s covering lemma due to Chang.

Define recursively sets $S_1, S_2, \dots \subset A$ such that S_i is a maximal subset of size $\leq 2K$ such that the translates

$$x + S_{i-1} + \dots + S_1 + H + P \quad x \in S_i$$

are all disjoint. If ever $|S_i| < 2K$ we stop. Now suppose we get as far as S_1, \dots, S_t . Then

$$S_t + \dots + S_1 + H + P \subset 2A - 2A + tA,$$

so [Theorem 2.5](#) gives

$$|S_t + \dots + S_1 + H + P| \leq K^{4+t}|A|.$$

On the other hand, disjointness of the translates in the definition of S_i means that

$$\begin{aligned} |S_t + \dots + S_1 + H + P| &\geq |S_t| \cdots |S_1| |H + P| \\ &\geq (2K)^{t-1} \exp(-\mathcal{O}(K^{\mathcal{O}(1)})) |A|. \end{aligned}$$

Putting these together, we have $2^{t-1} \leq K^5 \exp(\mathcal{O}(K^{\mathcal{O}(1)}))$, hence $t \leq \mathcal{O}(K^{\mathcal{O}(1)})$. In particular, this process terminates. But also, since S_t is therefore maximal among all subsets of A such that

$$x + S_{t-1} + \dots + S_1 + H + P$$

are disjoint for $x \in S_t$, Ruzsa's covering lemma implies that

$$A \subset H + 2P + S_1 - S_1 + \dots + S_{t-1} - S_{t-1} + S_t.$$

Enumerating $\bigcup_i S_i$ as S_1, \dots, S_d , we have $d \leq \mathcal{O}(K^{\mathcal{O}(1)})$ and

$$A \subset H + 2P + P(s_1, \dots, s_d; 1, \dots, 1) \subset \mathcal{O}(K^{\mathcal{O}(1)})(A \cup \{0\} \cup -A)$$

as claimed. □

Exercise. See what bounds are given if you apply Ruzsa's covering lemma directly, instead of Chang's argument.

6 Geometry of Numbers

Lecture 6 To prove [Proposition 5.3](#), we'll use a field called the *geometry of numbers* which is concerned with lattices in \mathbb{R}^d . For us, a lattice $\Lambda \subset \mathbb{R}^d$ will simply be the additive subgroup (not subspace) generated by some basis x_1, \dots, x_d for \mathbb{R}^d . So

$$\Lambda = \{l_1x_1 + \dots + \lambda_dx_d \mid l_i \in \mathbb{Z}\}$$

If $\Gamma \subset \Lambda$ is another lattice we call it a sublattice, and write $\Gamma < \Lambda$. On sheet two, we will see

$$\frac{\det(y_1, \dots, y_d)}{\det(x_1, \dots, x_d)} = [\Lambda : \Gamma] \quad (6.1)$$

where y_1, \dots, y_d are a basis for Λ and x_1, \dots, x_d are a basis for Γ .

In particular, if x_1, \dots, x_d and x'_1, \dots, x'_d are bases for the same lattice Λ then

$$\det(x_1, \dots, x_d) = \det(x'_1, \dots, x'_d).$$

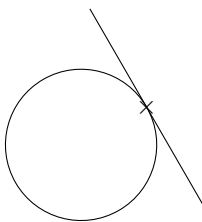
We define this to be $\det(\Lambda)$. The relevance of lattices to [Proposition 5.3](#) is the following:

Lemma 6.1. Let G, Λ be as in [Proposition 5.3](#), and set $\gamma : G \rightarrow \mathbb{R}^d/\mathbb{Z}^d$ by enumerating Γ as $\{\gamma_1, \dots, \gamma_d\}$ and setting $\gamma = (\gamma_1, \dots, \gamma_d)$. Then $\Lambda = \gamma(G) + \mathbb{Z}^d$ is a lattice with determinant $\frac{|\ker \gamma|}{|G|}$.

Proof. Λ is finitely generated as G is finite, and torsion-free as in \mathbb{R}^d , so isomorphic to \mathbb{Z}^k for some k . Also, Λ has \mathbb{Z}^d as a finite-index subgroup. So $k = d$ and $\text{span}_{\mathbb{R}}(\Lambda) = \mathbb{R}^d$. So we may take a generating set for Λ of size d , which is then a basis for \mathbb{R}^d . Determinant follows from (6.1) because $\det(\mathbb{Z}^d) = 1$. \square

We'll investigate the interaction of $[-p, p]^d$ with Λ . To do this, we introduce another definition:

Definition. A set $A \subset \mathbb{R}^d$ is convex if $\forall x \in \mathbb{R}^d \setminus A^\circ$ there is a hyperplane h_x with $x \in h_x$ and $h_x \cap A^\circ = \emptyset$.



Definition. A set $B \subset \mathbb{R}^d$ is a convex body if it is bounded and convex and $B^\circ \neq \emptyset$. It is symmetric if $\forall x \in B$ we have $-x \in B$. Given a symmetric convex body B and a lattice Λ , define the successive minima $\lambda_1 \leq \dots \leq \lambda_d$ of B with respect to Λ via

$$\lambda_i = \inf\{\lambda > 0 \mid \dim \text{span}_{\mathbb{R}}(\lambda \cdot B \cap \Lambda) \geq i\}$$

We may then inductively define linearly independent vectors $v_1, \dots, v_d \in \Lambda^1$ such that $v_1, \dots, v_i \in \lambda_i \bar{B}$. We'll call such a set a directional basis for Λ with respect to B . Note i is not unique, and not necessarily a basis for Λ in the earlier sense (See Ex Sheet 2).

Theorem 6.2 (Minkowski's Second Theorem). Suppose B is a symmetric convex body, Λ a lattice in \mathbb{R}^d and $\lambda_1, \dots, \lambda_d$ are the successive minima. Then $\lambda_1 \dots \lambda_d \text{vol}(B) \leq 2^d \det(\lambda)$.

Lemma 6.3 (Blichfeldt). Suppose $A \subset \mathbb{R}^d$ is a measurable set, Λ a lattice and $\forall a, b \in A$ distinct we have $a - b \notin \Lambda$. Then $\text{vol}(A) \leq \det(\Lambda)$.

Proof. Fix a basis x_1, \dots, x_d for Λ and define the **fundamental parallelopiped** P with respect to x_1, \dots, x_d via

$$P = \{l_1x_1 + \dots + l_dx_d \mid l_i \in [0, 1)\}$$

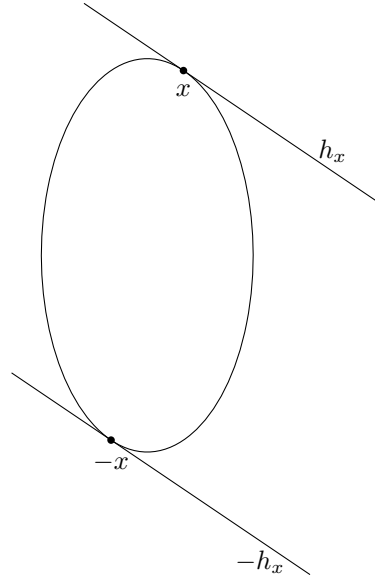
Since x_1, \dots, x_d is a basis for \mathbb{R}^d , $\forall v \in \mathbb{R}^d$ there are unique $x_v \in \Lambda$ and $p_v \in P$ such that $v = x_v + p_v$. Define a map $\varphi : \mathbb{R}^d \rightarrow P$ via $\varphi(v) = p_v$. This cuts A into countably many measurable pieces, and translates these pieces into P . It is injective by hypothesis, hence volume preserving, and so

$$\text{vol}(A) = \text{vol}(\varphi(A)) \leq \text{vol}(P) = \det(\Lambda). \quad \square$$

Proof of Theorem 6.2. Let v_1, \dots, v_d be a directional basis for Λ with respect to B . Set $V_i = \text{span}_{\mathbb{R}}(v_1, \dots, v_i)$ (including $V_0 = \{0\}$), and set $\Lambda_i = \Lambda \cap (V_i \setminus V_{i-1})$. Λ is a disjoint union $\bigcup_{i=0}^d \Lambda_i$.

Claim 1: We have $\lambda_d B^\circ \cap (\lambda_d B^\circ + \alpha x) = \emptyset$ whenever $x \in \Lambda_j$ and $\alpha \geq \frac{2\lambda_d}{\lambda_j}$.

Proof of claim Given $x \in \Lambda_j$, by definition $x \notin \lambda_j B^\circ$, so by convexity there is a hyperplane h_x such that $x \in h_x$ and $h_x \cap \lambda_j B^\circ = \emptyset$. By symmetry, we may take $h_{-x} = -h_x$.



Note, however, that $-h_x = h_x - 2x$. That means that $x_j B^\circ$ is contained in the slice of space S_x between the parallel hyperplanes h_x and $h_x - 2x$. Clearly $S_x \cap (S_x + \alpha x) = \emptyset$ for all $\alpha \geq 2$, so in particular

$$\lambda_j B^\circ \cap (\lambda_j B^\circ + \alpha x) = \emptyset$$

for all such α as well. Scaling by λ_d/λ_j , we see that $\lambda_d B^\circ \cap (\lambda_d B^\circ + \alpha x) = \emptyset$ whenever $\alpha \geq 2\frac{\lambda_d}{\lambda_j}$, proving the claim. ■

Claim 2: There are sets $B_1 \subset B_2 \subset \dots \subset B_d = \lambda_d B^\circ$ such that

$$1. \text{ vol}(B_i) = \left(\frac{\lambda_i}{\lambda_{i+1}}\right)^i \text{vol}(B_{i+1}) \quad \forall i$$

2. we have $B_i \cap (B_i + \alpha x) = \emptyset$ whenever $x \in \Lambda_j$ and $\alpha \geq 2 \max\{\frac{\lambda_i}{\lambda_j}, 1\}$. $B_i \cap (B_i + \alpha x) = \emptyset$ whenever $x \in \Lambda_j$ and $\alpha \geq 2 \max\{\frac{\lambda_i}{\lambda_j}, 1\}$. $B_i \cap (B_i + \alpha x) = \emptyset$ whenever $x \in \Lambda_j$ and $\alpha \geq 2 \max\{\frac{\lambda_i}{\lambda_j}, 1\}$. $B_i \cap (B_i + \alpha x) = \emptyset$ whenever $x \in \Lambda_j$ and $\alpha \geq 2 \max\{\frac{\lambda_i}{\lambda_j}, 1\}$.

Proof of claim 2: Define operations $\sigma_1, \dots, \sigma_{d-1}$ on suitable subsets of \mathbb{R}^d as follows. Given L bounded and open, define σ_i separately on each affine subspace $z + V_i$ with $z \in L$. For each affine subspace, fix a particular $z \in L$, and define

$$\varphi(z + v) = z + \frac{\lambda_i}{\lambda_{i+1}} v \quad \forall v \in V_i$$

On each slice, σ_i scales L by a factor of $\frac{\lambda_i}{\lambda_{i+1}}$, centred at z parallel to v_i . Note the following properties

- (i) $\text{vol}(\sigma_i(L)) = (\frac{\lambda_i}{\lambda_{i+1}}) \text{vol}(L)$ (by Fubini)
- (ii) If $L \cap (z + V_i)$ is open and convex for every z , then $\sigma_i(L) \subset L$ because $z \in L$.
- (iii) If $L \cap (z + V_i)$ is open and convex then so is $\sigma_i(L) \cap (z + V_i)$, and indeed so is $\sigma_i(L) \cap \bigcap_{j < i} (z + V_j)$

Set $B_d = \lambda_d B^\circ$, and $B_i = \sigma_i(B_{i+1})$ otherwise.

Conclusion 1 is immediate from property (i). Conclusion 2 follows from Claim 1 when $i = d$. For $i < d$, it follows by induction and repeated application of (ii) and (iii). Indeed, (2) for $i \geq j$ follows from (2) for $i + 1$ because σ_i scales by $\frac{\lambda_i}{\lambda_{i+1}}$ in direction x . For $i < j$, it follows from $B_i \subset B_{i+1}$. ■

To prove the theorem, note that $\text{vol}(B_i) = \lambda_i \cdots \lambda_d \text{vol}(B)$ and by 2, $a - b \notin 2\Lambda$ for every $a, b \in B_1$, so Blichfeldt gives $\text{vol}(B_1) \leq 2^d \det(\Lambda)$. □

Lecture 7 Proof of Proposition 5.3. Write $\gamma = (\gamma_1, \dots, \gamma_r) \in \hat{G}^r$, define $\Lambda = \gamma(4) + \mathbb{Z}^r$, which is a lattice of determinant $\frac{|\ker \gamma|}{|G|}$ by Lemma 6.1. Let $\lambda_1, \dots, \lambda_r$ be the successive minima of $[-1, 1]^r$ with respect to Λ , and v_1, \dots, v_r a directional basis. Set $L_i = \lfloor \frac{p}{r\lambda_i} \rfloor$ for each i . Then $P(v_1, \dots, v_r; L_1, \dots, L_r) \subset [-p, p]^r$. Pick for each i , pick $x_i \in G$ such that $\gamma(x_i) = v_i$, and set $H = \ker \gamma$. Write $p = P(x_1, \dots, x_r; L_1, \dots, L_r)$. Then $H + P \subset$

Claim: If l_1, \dots, l_r and l'_1, \dots, l'_r satisfy $|l_i|, |l'_i| \leq L_i$, and

$$l_1 x_1 + \dots + l_r x_r \in l'_1 x_1 + \dots + l'_r x_r + H \quad (*)$$

then in fact $l_i = l'_i$ for all i . Indeed, (*) implies that

$$(l_1 - l'_1)v_1 + \dots + (l_r - l'_r)v_r \in \mathbb{Z}^r \cap [-2p, 2p]^r.$$

But since $p < \frac{1}{2}$, this last intersection is just $\{0\}$, proving the claim (as v_i are linearly independent in \mathbb{R}^r). ■

Then

$$\begin{aligned} |H + P| &\geq |H|(L_1 + 1) \cdots (L_r + 1) \\ &\geq |H| \left(\frac{p}{r}\right)^r \frac{1}{\lambda_1 \cdots \lambda_r} \\ &\geq |G| \left(\frac{p}{r}\right)^r \end{aligned}$$

by Minkowski's second theorem. □

7 Progressions in the Heisenberg group

Let

$$H(\mathbb{Z}) = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & n_1 & n_2 \\ 0 & 1 & n_1 \\ 0 & 0 & 1 \end{pmatrix} : n_i \in \mathbb{Z} \right\}$$

be the **Heisenberg group**.

Set

$$u_1 = \begin{pmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix}, u_2 = \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}, u_3 = \begin{pmatrix} 1 & 0 & 1 \\ & 1 & 0 \\ & & 1 \end{pmatrix}$$

and note that any element of $H(\mathbb{Z})$ can be expressed in the form

$$\begin{pmatrix} 1 & n_2 & n_3 \\ & 1 & n_1 \\ & & 1 \end{pmatrix} = u_1^{n_1} u_2^{n_2} u_3^{n_3}$$

and we have the following formula for multiplying elements in this form:

$$(u_1^{n_1} u_2^{n_2} u_3^{n_3})(u_1^{n'_1} u_2^{n'_2} u_3^{n'_3}) = u_1^{n_1+n'_1} u_2^{n_2+n'_2} u_3^{n_3+n'_3+n'_1 n_2} \quad (7.1)$$

This is easy to verify by multiplying matrices, but there is a more abstract reason for it. To see this, given $x, y \in G$, define the commutator $[x, y] = x^{-1}y^{-1}xy$. In light of the identity $xy = yx[x, y]$, we can view the commutator as being the ‘error’ or ‘cost’ incurred when interchanging two elements. For example, the fact that commutators are trivial in abelian groups can be viewed as capturing the notion that elements can be interchanged freely in an abelian group. The $n'_1 n_2$ term in (7.1) arises because we swap the order of $n'_1 n_2$ pairs of elements u_1 and u_2 .

Now let’s see one possible generalisation of progression to non-abelian groups.

Definition. Given $x_1, \dots, x_r \in G$, $L_1, \dots, L_r \geq 0$, we define the **ordered progression** of rank r

$$P_{\text{ord}}(x, L) = P_{\text{ord}}(x_1, \dots, x_r; L_1, \dots, L_r) = \{x_1^{l_1} \cdots x_r^{l_r} : |l_i| \leq L_i \ \forall i\}.$$

Now consider $P = P_{\text{ord}}(u_1, u'_2, L_1, L_2)$ for $u_1, u_2 \in H(\mathbb{Z})$ as before, and $L_1, L_2 \geq 0$. We have

$$(u_1^{l_1} u_2^{l_2})(u_1^{l'_1} u_2^{l'_2}) = u_1^{l_1+l'_1} u_2^{l_2+l'_2} u_3^{l'_1 l_2} \quad (7.2)$$

and it is then easy to check that $\frac{|P^2|}{|P|} \rightarrow \infty$ as $L_1, L_2 \rightarrow \infty$, essentially because by varying l_1, l'_1, l_2, l'_2 within their ranges one can change $l_1 l'_2$ without changing $l_1 + l'_1$ or $l_2 + l'_2$. This can be thought of as an extra degree of freedom in P^2 compared to P . Coming back to commutators and recalling that $u_3 = [u_2, u_1]$, we see that this corresponds to the freedom to interchange the order of some of the u_1, u_2 in P^2 , as seen in the LHS of (7.2). This is a freedom that the definition of ordered progression explicitly denies us.

It turns out that if we introduce this freedom to P as well then this does force P to have small tripling.

Definition. Given $x_1, \dots, x_r \in G$, $L_1, \dots, L_r \geq 0$, the **nonabelian progression** $P(x; L)$ of rank r is defined to consist of those elements of G expressible as products of $x_1^{\pm 1}, \dots, x_r^{\pm 1}$ in which each x_i, x_i^{-1} appear at most L_i times between them.

It turns out $P(u_1, u_2, L_1, L_2)$ does have small tripling (Example Sheet 2).

A note of caution: nonabelian progressions don't always have small tripling; consider $P(x_1, x_2; L_1, L_2)$ for x_1, x_2 generators of a nonabelian free group. In the case of $H(\mathbb{Z})$, the formula (7.1) is simplified by the fact that $u_3 = [u_2, u_1]$ is central in $H(\mathbb{Z})$. If this were not the case, we'd end up with elements of the form $[[u_2, u_1], u_1]$, for example. This is in fact a specific example of a property called nilpotence.

To define this, first define a normal series for a group G to be a sequence

$$G = G_1 > G_2 > \cdots$$

of normal subgroups $G_i \triangleleft G$, and a central series to be such a normal series in which each G_i/G_{i+1} is central in G/G_{i+1} .

Definition. A group G is **nilpotent** if there is a finite central series

$$G = G_1 > \cdots > G_{s+1} = \{1\}$$

The smallest s for which such a series exists is called the step or nilpotency class of G .

Exercise. $H(\mathbb{Z})$ is 2-step nilpotent.

8 Nilpotent Groups

Lecture 8 The reasons we focus on nilpotent groups are twofold: there is a clean generalization of Freiman-Green-Ruzsa to nilpotent groups, and a deep theorem of Breuillard, Green and Tao essentially reduces the general case to the nilpotent case.

Given $x_1, \dots, x_k \in G$, define the simple commutator $[x_1, \dots, x_k] = [x_1, \dots, x_k]_t$ recursively as follows:

$$\begin{aligned} [x_1] &= x_1 \\ [x_1, \dots, x_k] &= [[x_1, \dots, x_{k-1}], x_k] \end{aligned}$$

(recall $[x, y] = x^{-1}y^{-1}xy$).

Given subgroups $H, N < G$, define $[H, N] = \langle [h, n] \mid h \in H, n \in N \rangle$, and then given $H_1, \dots, H_k < G$, set

$$\begin{aligned} [H_1] &= H_1 \\ [H_1, \dots, H_k] &= [[H_1, \dots, H_{k-1}], H_k]. \end{aligned}$$

Note that

$$[H, N] = [N, H] \tag{8.1}$$

since $[h, n] = [n, h]^{-1}$.

Lemma 8.1. Let $H_1, \dots, H_k, N \triangleleft G$, let S_i be a generating set of H_i for each i . Suppose $[s_1, \dots, s_k] \in N$ whenever $s_i \in H_i$ for each i . Then $[H_1, \dots, H_k] < N$.

Proof. Case $k = 1$ is trivial, so assume $k > 1$. If $[s_1, \dots, s_k] \in N$ for each $s_i \in S_i$ then we have $[[s_1, \dots, s_{k-1}], s_k] \in N$ for each $s_i \in S_i$, and hence $[s_1, \dots, s_{k-1}] \in C_{G/N}(H_k) = \{g \in G \mid [g, h] \in N \forall h \in H_k\}$. The centraliser of a normal subgroup is itself normal, so by induction we have $[H_1, \dots, H_{k-1}] \subset C_{G/N}(H_k)$, and hence $[H_1, \dots, H_k] \subset N$, as claimed. \square

Definition. Given a group G , we define the **lower central series** $G = G_1 > G_2 > \dots$ of G via

$$G_k := \langle [g_1, \dots, g_k] \mid g_i \in G \rangle.$$

Note that $G_k > G_{k+1}$, because $[g_1, \dots, g_{k+1}] = [[g_1, g_2], g_3, \dots, g_{k+1}]$. Also, since $[g_1, \dots, g_k]^h = [g_1^h, \dots, g_k^h]$, each G_k is normal in G (recall $x^y = y^{-1}xy$). The fact that this is a central series (i.e. G_k/G_{k+1} is central in G/G_{k+1}) follows from the following result.

Proposition 8.2. We have $G_{k+1} = [G_k, G]$ for every k . In particular, $G_k = [G, \dots, G]_k$.

Proof. First, $G_{k+1} < [G_k, G]$ by definition. The fact that $[G_k, G] \subset G_{k+1}$ follows from [Lemma 8.1](#) since $[g_1, \dots, g_{k-1}]$ generate G_k and G_i, G_k, G_{k+1} are normal. \square

Proposition 8.3. Let G be a group generated by S , then

$$G_k = \langle [s_1, \dots, s_k]G_{k+1} \mid s_i \in S \forall i \rangle.$$

‘ G_k is generated mod G_{k+1} by simple commutators of generators’.

Proof. Note that $[s_1, \dots, s_k]^g \in [s_1, \dots, s_k]G_{k+1}$ by definition of G_{k+1} , so

$$\langle [s_1, \dots, s_k]G_{k+1} \mid s_i \in S \rangle$$

is normal in G . Moreover,

$$[s_1, \dots, s_k] \in \langle [t_1, \dots, t_k]G_{k+1} \mid t_i \in S \rangle$$

whenever $s_i \in S$ for every i , so [Lemma 8.1](#) implies that $[G, \dots, G]_k \subseteq \langle [s_1, \dots, s_k]G_{k+1} \mid t_i \in S \rangle$. [Proposition 8.2](#) gives $[G, \dots, G]_k = G_k$, so we have $G_k \subseteq \langle [s_1, \dots, s_k]G_{k+1} \mid s_i \in S \rangle$. The reverse inclusion is immediate. \square

Proposition 8.4. We have $[G_i, G_j] \subset G_{i+j}$ for every i, j .

For this we'll need the following commutator identity, which you can check directly:

$$[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1. \quad (8.2)$$

Proof of [Proposition 8.4](#). The case $j = 1$ follows from [Proposition 8.2](#). So we can assume $j > 1$ and, by induction,

$$[G_k, G_{j-1}] \subset G_{k+j-1} \forall k. \quad (8.3)$$

Now note that

$$[G_i, G_j] = [G_i, [G_{j-1}, G]] = [[G, G_{j-1}], G_i] \quad (8.4)$$

by [Proposition 8.2](#) and (8.1). We also have

$$[[G_{j-1}, G_i], G] = [[G_i, G_{j-1}], G] \subset [G_{i+j-1}, G] = G_{k+j}. \quad (8.5)$$

by (8.1), (8.3) and [Proposition 8.2](#), and

$$[[G_{i+1}, G], G_{j-1}] = [G_{i+1}, G_{j-1}] \subset G_{i+j}. \quad (8.6)$$

by [Proposition 8.2](#) and (8.3). Given $x \in G$, $y \in G_{j-1}$ and $z \in G_i$, we therefore have

$$\begin{aligned} [x, y, z] &= (([y^{-1}, z^{-1}, x]^z, [z, x^{-1}, y^{-1}]^x)^{-1})^y && \text{by (8.2)} \\ &\subset G_{i+j} && \text{by (8.5) and (8.6).} \end{aligned}$$

The proposition follows from (8.4) and [Lemma 8.1](#). \square

Definition. Given a group G , the upper central series

$$\{1\} = Z_0(G) < Z_1(G) < Z_2(G) < \dots$$

is defined recursively by setting $Z_{i+1}(G)$ so that $Z_{i+1}(G)/Z_i(G)$ is the centre of $G/Z_i(G)$. Note that each $Z_i(G)$ is normal by induction, since the centre of any group is normal.

Theorem 8.5. Let $G = H_1 > H_2 > \dots > H_{r+1} = \{1\}$ be a finite central series for G (so G is nilpotent). Then we have $H_i > G_i \forall i = 1, \dots, r+1$ and $H_{r+1-i} \subset Z_i(G)$ for every $0 \leq i \leq r$.

This justifies the names upper and lower central series:

$Z_r(G)$		$Z_{r-1}(G)$		$Z_1(G)$		$Z_0(G)$		
\vee		\vee		\vee		\vee		
H_1	$>$	H_2	$>$	\dots	$>$	H_r	$>$	H_{r+1}
\vee		\vee		\vee		\vee		
G_1		G_2		G_r		G_{r+1}		

Corollary 8.6. If G is s -step nilpotent, then both the upper and lower central series have length $s + 1$.

Proof. $H_i > G_1$ by definition, so we may assume $i > 1$, and then we have

$$\begin{aligned} H_i &\supset [H_{i-1}, G] && \text{central series} \\ &\supset [G_{i+1}, G] && \text{by induction} \\ &= G_i && \text{by Proposition 8.2.} \end{aligned}$$

We also have $Z_0(G) > H_{r+1}$ by definition, so we may assume $i > 0$ and, by induction, that $H_{r+2-i} \subset Z_{i-1}(G)$. But that

$$G/Z_{i-1}(G) = \frac{G/H_{r+2-i}}{Z_i(G)/H_{r+2-i}}$$

because (H_j) is a central series, H_{r+1-i}/H_{r+2-i} is central in G/H_{r+2-i} , so its image in $G/Z_{i-1}(G)$ in the above quotient is central. But the centre of $G/Z_{i-1}(G)$ is $Z_i(G)/Z_{i-1}(G)$, so $H_{r+1-i} \subset Z_i(G)$, as required. \square

These results say

- G is nilpotent of step $\leq s \iff G_{s+1} = \{1\} \iff Z_s(G) = G$
- If $G = \langle s \rangle$, we can verify this just by checking that $[t_1, \dots, t_{s+1}] = 1$ for all $t_i \in S$.
- If G is nilpotent of step $\leq s$, then any commutator like $[[[q_1, q_2], q_3], [q_4, q_5]]$ with more than s entries is trivial.

9 Torsion-free Nilpotent Approximate Groups: an overview

Lecture 9 **Definition.** If $\langle x_1, \dots, x_r \rangle$ is s -step nilpotent then the nonabelian progression $P(x; L)$ is called a **nilprogression** of rank r and step s . In this case, we write $P_{\text{nil}}(x; L)$ instead of $P(x; L)$.

***Proposition 9.1.** Given $r, s \in \mathbb{N}$, $\exists \lambda = \lambda_{r,s}$ such that if x_1, \dots, x_r generate an s -step nilpotent group and $L_1, \dots, L_r \geq \lambda_{r,s}$ then $P_{\text{nil}}(x; L)$ is an $O_{r,s}(1)$ -approximate group (the implied constant can depend on r, s but nothing else).

We won't have time to prove this, but we will do a special case on Sheet 2, where we will also see that it is necessary to have $L_i \geq \lambda_{r,s}$.

As in the abelian setting, it turns out that these are essentially the only examples of finite nilpotent approximate groups, apart from genuine subgroups.

Theorem 9.2. Let G be s -step nilpotent, $A \subset G$ a finite K -approximate group. Then $\exists H \triangleleft \langle A \rangle$ and a nilprogression P_{nil} of rank $\leq K^{O_s(1)}$ such that $A \subset HP_{\text{nil}} \subset A^{K^{O_s(1)}}$. In particular, $|HP_{\text{nil}}| \leq \exp(K^{O_s(1)})|A|$.

Remark. If $K < 2$, the theorem is trivial. For $K \geq 2$, we have $\mathcal{O}(K^{O(1)}) \leq K^{O(1)}$ i.e. multiplicative constants can be absorbed into exponents. So it is not cheating to write $K^{O(1)}$ instead of $\mathcal{O}(K^{O(1)})$.

We won't have time to prove this in full, but in the next few sections we will prove some special cases that contain most of the main ideas. We will start with the case where G is torsion-free, where [Theorem 9.2](#) is originally due to Breuillard and Green (although we will give a different proof). We start with the following weakened version:

Theorem 9.3. Let G be torsion-free s -step nilpotent, $A \subset G$ a finite K -approximate group. Then \exists an ordered progression P_{ord} of rank $\leq K^{O_s(1)}$ such that $A \subset P_{\text{ord}} \subset A^{K^{O_s(1)}}$.

The basic idea is to write A as a product of approximate groups of step $\leq s$, and then apply induction to reduce to the step 1 case, i.e. the abelian case, and apply the Freiman-Green-Rusza theorem. The result we use to do this is as follows:

Proposition 9.4. Let G be torsion-free s -step nilpotent, $A \subset G$ a finite K -approximate group. Then $k \leq K^{O(1)}$, and $K^{O(1)}$ -approximate subgroups $A_1, \dots, A_k \subset A^{O(1)}$ such that $A \subset A_1 \cdots A_k \subset A^{K^{O(1)}}$, and $\langle A_i \rangle$ is of step $< s$ for every i .

Proof of Theorem 9.3. An easy induction gives $K^{O_s(1)}$ -approximate groups $B_1, \dots, B_m \subset A^{O_s(1)}$ with $m \leq K^{O_s(1)}$. Freiman-Green-Rusza then gives abelian progressions - in particular ordered progressions - P_1, \dots, P_m , each of rank $\leq K^{O_s(1)}$, such that $B_i \subset P_i \subset B_i^{K^{O_s(1)}}$, and hence $A \subset P_1 \cdots P_m \subset A^{K^{O_s(1)}}$. $P_1 \cdots P_m$ is an ordered progression of rank $\leq mK^{O_s(1)} \leq K^{O_s(1)}$, so we are done. \square

Recall that in proving Freiman-Green-Rusza, we wanted ' $A \subset$ small progression', but we first proved ' $A^c \supset$ large progression'. We then used Chang's covering argument to get what we wanted. We will use a similar approach here, starting with the following:

Proposition 9.5. Take G torsion-free nilpotent, $A \subset G$ finite K -approximate group. Then $\exists r \leq K^{O(1)}$ and $K^{O(1)}$ -approximate groups $A_0, A_1, \dots, A_r \subset A^{O(1)}$, each generating a group of step $< s$, such that

$$|A_0 A_1 \cdots A_r| \geq \exp(-K^{O(1)})|A|.$$

In the next section, we will see that passing from [Proposition 9.5](#) to [Proposition 9.4](#) is very similar to the Chang covering part of the proof of Freiman-Green-Ruzsa.

In proving [Proposition 9.5](#), we actually use the preliminary version of Freiman-Green-Ruzsa in which A^c contains a large progression. As we noted in that proof, combining [Proposition 5.2](#), [Proposition 5.3](#) and [Lemma 5.4](#) gives the following result:

Theorem 9.6 (Green-Ruzsa). Let G be abelian and $A \subset G$ be a finite K -approximate group. Then $\exists H < G$ and x_1, \dots, x_r with $r \leq K^{\mathcal{O}(1)}$, and $L_1, \dots, L_r \in \mathbb{N}$ such that $HP(x; L) \subset A^4$ and

$$|HP(x; L)| \geq \exp(-K^{\mathcal{O}(1)})|A|.$$

We will apply this to [Proposition 9.5](#) via the following result:

Proposition 9.7. Let G be s -step nilpotent and $A \subset G$ a finite K -approximate group. Write $\pi : G \rightarrow G/[G, G]$ for the quotient homomorphism. Noting that $G/[G, G]$ is abelian and that $\pi(A)$ is a K -approximate group, let $H < G/[G, G]$ and $x_1, \dots, x_r \in G/[G, G]$ be as coming from applying [Theorem 9.6](#) to $\pi(A)$. Then

$$\left| (A^{24} \cap \pi^{-1}(H)) \prod_{i=1}^r (A^{24} \cap \pi^{-1}(\langle x_i \rangle)) \right| \geq \exp(-K^{\mathcal{O}(1)})|A|.$$

We will prove [Proposition 9.7](#) next time. For now, let's see how it implies [Proposition 9.5](#). [Proposition 4.6](#) immediately tells us that $A^{24} \cap \pi^{-1}(H)$ and $A^{24} \cap \pi^{-1}(\langle x_i \rangle)$ are $K^{\mathcal{O}(1)}$ -approximate groups.

It turns out that they also generate subgroups of step $< s$, at least when G is torsion-free.

Lemma 9.8. Let G be s -step nilpotent, and write $\pi : G \rightarrow G/[G, G]$ as before. Then

- (i) $\forall x \in G/[G, G]$, $\pi^{-1}(\langle x \rangle)$ is of step $< s$.
- (ii) If $H < G/[G, G]$ is a finite subgroup and G is torsion-free, then $\pi^{-1}(H)$ is of step $< s$.

Lemma 9.9. Let G be an arbitrary group. Then the simple commutator map

$$\begin{aligned} [\cdot, \dots, \cdot]_k : G^k &\longrightarrow G_k \\ (x_1, \dots, x_k) &\longmapsto [x_1, \dots, x_k] \end{aligned}$$

is a homomorphism in each variable mod G_{k+1} . Moreover, $[G, G]$ is contained in the kernel of each of these homomorphisms.

In the next section, we will prove this, use it to prove [Lemma 9.8](#) (which is also an exercise in the meantime), and prove the outstanding statements from this section.

10 Torsion-free Nilpotent Approximate Groups: the details

11 p -groups

In the last two sections, we looked at approximate subgroups of torsion-free nilpotent groups. Today we'll move on to consider nilpotent groups with elements of finite order. We won't need the following result, but it motivates this section.

***Proposition 11.1.** A finite group is nilpotent if and only if it is a direct product of p -groups.

Given a prime p , a p -group is a group in which every element has a power of p as its order. Motivated by [*Proposition 11.1](#), we'll focus on p -groups.

In the torsion-free setting, we needed to show that a certain subgroup $\pi^{-1}(H)$ was nilpotent of step $< s$, i.e. that $[\pi^{-1}(H), \dots, \pi^{-1}(H)]_s = \{1\}$. We did this by showing that $(\pi^{-1}(+1), \dots, \pi^{-1}(+1))_s$ was generated by a union of finite subgroups (i.e. the subgroups $[\pi^{-1}H, q_1, \dots, q_{s-1}]$ with $q_i \in \pi^{-1}(H)$.) Since the ambient group was torsion-free, these finite subgroups were all automatically trivial, hence so was $[\pi^{-1}(H), \dots, \pi^{-1}(H)]_s$.

This does not work if the ambient group has two elements of finite order, so we need to find a more sophisticated way of controlling groups like $[\pi^{-1}(+1), \dots, \pi^{-1}(H)]_s$ that are generated by unions of subgroups.

In this section we will prove the following result giving a means by which to do this.

Proposition 11.2. Let Γ be a (finite) abelian p -group of rank $\leq r$, and let $X \subset \Gamma$ be a union of subgroups. Then $\langle x \rangle \subset rX$.

The **rank** of a group here is the smallest possible size of a generating set.

Given a group G , a subgroup $H < G$ is a **maximal subgroup** if $H \neq G$ but the only subgroup $N < G$ satisfying $H \leq N < G$ is G itself.

Lemma 11.3. Let Γ be a finite abelian p -group. Then $H < \Gamma$ is maximal iff $\Gamma/H \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. The fundamental theorem of finitely generated abelian groups tells us that

$$\Gamma/H \cong \bigoplus_{i=1}^k \frac{\mathbb{Z}}{p^{n_i}\mathbb{Z}}$$

for some $k \geq 0$ and $n_i \in \mathbb{N}$. The lemma follows immediately. \square

Lemma 11.4. Let Γ be a finite abelian p -group, and let $S \subset \Gamma$. Then S generates Γ iff $S + (p \cdot \Gamma)$ generates Γ . (We write $p \cdot \Gamma$ to mean $\{px : x \in \Gamma\}$).

As a slogan, “ S generates $\Gamma \iff S$ generates $\Gamma/(p \cdot \Gamma)$ ”.

Proof. Clearly if S generates Γ then so does $S + (p \cdot \Gamma)$. Conversely, if S does not generate Γ then S is contained in some maximal subgroup H . We know from [Lemma 11.3](#) that $\Gamma/H \cong \mathbb{Z}/p\mathbb{Z}$, so $(p \cdot \Gamma) \subset H$ because px is trivial in Γ/H for every $x \in \Gamma/H$. Hence $S + (p \cdot \Gamma) \subset H$, so does not generate Γ . \square

Corollary 11.5. Let Γ be a finite abelian p -group. Then every minimal generating set for Γ has the same size.

Proof. The fundamental theorem of finitely generated abelian groups implies that $\Gamma/(p \cdot \Gamma) \cong \mathbb{F}_p^n$. [Lemma 11.4](#) says that S generates Γ iff its image in $\Gamma/(p \cdot \Gamma)$ generates \mathbb{F}_p^n . A minimal generating set therefore has as its image in $\Gamma/(p \cdot \Gamma)$ a basis for \mathbb{F}_p^n , and, moreover, no two elements of S project to the same element of $\Gamma/(p \cdot \Gamma)$. Hence $|S| = n$ (which does not depend on S). \square

Lemma 11.6. Let Γ be a finite abelian p -group of rank r , and suppose $\Gamma' < \Gamma$. Then the rank of Γ' is also $\leq r$.

Proof. The case $r = 0$ is trivial, so we may assume $r > 1$ and proceed by induction. We have a generating set x_1, \dots, x_r for Γ . Let m be maximal such that $\Gamma' \subset p^m \cdot \Gamma$. Since $p^m \cdot \Gamma$ is generated by $p^m x_1, \dots, p^m x_r$, $p^m \cdot \Gamma$ also has rank $\leq r$, so without loss of generality we may replace Γ with $p^m \cdot \Gamma$, and hence assume that Γ' is not contained in $p \cdot \Gamma$ (by maximality of m).

That means $\exists y \in \Gamma \setminus p \cdot \Gamma$, i.e. y is of the form $l_1 x_1 + \dots + l_r x_r$ with at least one l_i (WLOG l_r) not a multiple of p . That means that l_r has a multiplicative inverse, say q , mod the order of x_r , and hence

$$x_r = q(y - l_1 x_1 - \dots - l_{r-1} x_{r-1}).$$

This means that $\Gamma/\langle y \rangle$ has rank $\leq r - 1$ and hence, by induction, so does $\Gamma'/\langle y \rangle$. In particular, Γ' has rank $\leq r$ (add y to a generating set for $\Gamma'/\langle y \rangle$). \square

Proof of Proposition 11.2. Lemma 11.6 implies that $\langle x \rangle$ has rank $\leq r$, and so Corollary 11.5 implies that $\exists x_1, \dots, x_r \in X$ such that

$$\langle x \rangle = \langle x_1, \dots, x_r \rangle = \langle x_1 \rangle + \dots + \langle x_r \rangle.$$

Since X is a union of subgroups, each $\langle x_i \rangle \subset X$, so in fact $\langle x \rangle \subset rX$, as required. \square

(Note that $p \cdot \Gamma$ referred to multiplying each element of Γ by p , and rX refers to higher sumsets as in earlier parts of the course).

*Bonus content

We showed in lectures 9 and 10 that if A is a finite K -approximate subgroup of a torsion-free nilpotent group then \exists ordered progression P_{ord} of rank $\leq K^{\mathcal{O}(1)}$ such that $A \subset P_{\text{ord}} \subset A^{K^{\mathcal{O}_s(1)}}$. However, in the general theorem we had a nilprogression instead. To get around this, one uses the following result.

***Proposition 11.7.** Let $x_1, \dots, x_r \in G$ (where G is s -step nilpotent), and $L_1, \dots, L_r \geq 0$. Then

$$P_{\text{ord}}(x; L) \subset P_{\text{nil}}(x; L) \subset P_{\text{ord}}(x; L)^{\mathcal{O}_s(r^{\mathcal{O}(s)})}.$$

Index

- Bohr set, [14](#)
- coset progression, [13](#)
- covering, [5](#)
- doubling, [2](#)
- doubling constant, [2](#)
- Freiman homomorphism, [11](#)
 - centered, [11](#)
- fundamental parallelopiped, [17](#)
- Heisenberg group, [19](#)
- lower central series, [21](#)
- maximal subgroup, [27](#)
- nilpotent, [20](#)
- nilprogression, [24](#)
- nonabelian progression, [19](#)
- ordered progression, [19](#)
- progression, [13](#)
 - coset, [13](#)
- rank, [27](#)
- small doubling, [2](#)
- small tripling, [6](#)