CHAPTER 1

Group combinatorics and Freiman's Theorem

1.1. Introduction

Let A, B be non-empty subsets of a group G; we write, as usual, the set-product

$$AB = \{ab \mid a \in A, b \in B\}.$$

For commutative groups - and to distinguish them - we use the additive notation

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

Similarly, for the "symmetric" set of A, we write $A^{-1} = \{a^{-1} \mid a \in A\}$ in the general case, and $-A = \{-a \mid a \in A\}$ in the commutative one, when we also define $A - B := A + (-B)$; if $A = \{a\}$, we write aB and Ba for, respectively, $\{a\}B$ and $B\{a\}$ ($a + B$ in the commutative case). For, $n \geq 2$ we use exponential notation:

$$A^n = \{a_1 a_2 \cdots a_n \mid a_1, \ldots, a_n \in A\} = (A^{n-1})A$$

which becomes 'multiple' notation in the commutative case:

$$nA = \{a_1 + a_2 + \cdots + a_n \mid a_1, \ldots, a_n \in A\}.$$

Clearly, the usual rules for integral exponents and multiples hold. In this chapter we will mostly deal with commutative groups; in this case, set-product is not only associative but also commutative: $A + B = B + A$ for all subsets A, B of a commutative group.

One of our main concerns will be sizes of set-products; let us therefore begin with some very obvious facts about those. Let A, B be finite non-empty subsets of a group G; then

i) $|A^{-1}| = |A|$, and $|AB| = |B^{-1}A^{-1}|$;
ii) $\max\{|A|, |B|\} \leq |AB| \leq |A||B|$.

The approach is that, while the upper bound in (ii) is expected to represent the random case, something should happen when te cardinality of the set-product approaches the lower bound, not much with regard the relation between A and B (in many interesting cases they will be the same) but with respect to inner structural properties of A (and B), and the more the cardinality of the product is "small" the closer the factors approximate a structured piece of the ambient group. While this may not be totally unexpected, it is somehow surprising that they are able, in many

cases, to precisely recognize such structural properties and describe quantitatively the discrepancy from them.
In this chapter we will then be interested in what kind of information one can retrive about the algebraic (or arithmetic) structure of the factors (or about the rate longer products grow) from arithmetical condition on the cardinalities $|AB|$, $|AB^{-1}|$ (these may well be different), of the set-products (or sum-set); a kind of questions usually called *inverse problems* in additive combinatorics (see Nathanson's monograph [**19**]). Expecting, as said, that if any influence the cardinality $|AB|$ has on A (or B), this should be more effective when $|AB|$ is "close" to the cardinalities of the factors.

The easiest of such instances (which is nevertheless useful to remember) is the fact that, for a finite subset A of a group G, $|AA| = |A|$ if and only if $A = xH = Hx$ for some subgroup H of G and some $x \in G$. In fact, a slightly more general observation we may do. Let A be a non-empty subset of the group G. It is then immediate to check that $S_A = \{x \in G \mid xA = A\}$ is a subgroup of G; observing that S_A acts by left multiplication on A with regular orbits, we have that, if A is finite, S_A is finite and $|S_A|$ divides $|A|$. Let B be another non-empty subset of G and suppose $|BA| = |A|$. Then for every $b \in B$, $|bA| = |A| = |BA|$, and so $bA = BA$. This implies that, for every $b, b_1 \in B$ and any $a \in A$, $b^{-1}b_1a \in A$. Hence $B^{-1}BA = A$, or, in other terms, $B^{-1}B \subseteq S_A$. We have therefore the following,

LEMMA 1.1. *Let A, B be non-empty finite subsets of a group. Then $|BA| = |A|$ if and only if B is contained in a left coset of the subgroup S_A.*

We now move to commutative groups. Remember that a group G is said to be *torsion-free* if it does not contain non-trivial elements of finite order; hence, a commutative group G is torsion-free if (and only if) $nx \neq 0$ for every $0 \neq x \in G$ and $0 \neq n \in \mathbb{Z}$.
The basic torsion–free (commutative group) is the additive group of integers, which we will denote by $\mathbb{Z}$. We ask first for the "direct" question, i.e.: what can, in general, be said about the cardinality of the sum of two finite subsets of $\mathbb{Z}$? The answer involves the notion of arithmetic progression, by which we mean what is usually considered to be a finite segment of an arithmetic progression. Precisely

DEFINITION 1.2. An *arithmetic progression* in $\mathbb{Z}$ is a finite set of type

$$a + I_{(d,n)} = \{a + dx \mid x = 0, 1, \dots, n-1\}$$

with $a, d, n \in \mathbb{Z}$, $d \neq 0$, $n \geq 1$ (and $I_{(d,n)} = \{dx \mid 0 \leq x \leq n-1\}$). The number n is the *length* of the progression (of course, it is also the cardinality of it), while the positive integer d is called the *common difference* of the progression.

EXAMPLE 1. Let $A = \{a + xb \mid 0 \leq x < n\}$ and $A_1 = \{a_1 + yb_1 \mid 0 \leq y < m\}$ be two arithmetic progressions of length, respectively, n and m. Then, we have

$$A + A_1 = \big\{(a + a_1) + xb + yb_1 \mid (x, y) \in \{0, \dots, n-1\} \times \{0, \dots, m-1\}\big\},$$

and point out the following

- *If $b = b_1$, then $A + A_1$ is an arithmetic progression of length $n + m - 1$ (and common difference b); in other terms $|A + A_1| = |A| + |A_1| - 1$.*

In particular, if A is an arithmetic progression then, for every $n \geq 1$, nA is an arithmetic progression and

$$|nA| \leq n|A| - n < n|A|.$$

An arithmetic progression is then something we regard to be "slowly growing". On the opposite side stand, for instance, geometric progressions: considering something like $U = \{1, d, d^2, \dots, d^{n-1}\}$ for $2 \leq d \in \mathbb{N}$, we get

$$|U + U| = (n^2 + n)/2 \sim |U|^2,$$

and growth is fast in this case.

LEMMA 1.3. *Let A, B be finite subsets of $\mathbb{Z}$; then*

(i) $|A + B| \geq |A| + |B| - 1$.
(ii) $|A + B| = |A| + |B| - 1$ *if and only if A and B are arithmetic progressions with the same common difference.*

PROOF. (i) Let $a = \max A$, and $b = \min B$. Then $(a + B) \cup (A + b) \subseteq A + B$. Let $y \in B$ and $x \in A$ such that $a + y = x + b$; then $0 \leq y - b = x - a \leq 0$; hence $y = b, x = a$ and thus $(a + B) \cap (A + b) = \{(a, b)\}$. Therefore

$$|A + B| \geq |(a + B) \cup (A + b)| = |a + B| + |A + b| - 1 = |A| + |B| - 1.$$

(ii) We have already observed that if A and B are arithmetic progressions with the same common difference, then equality holds in (i).
For the converse we may well assume that A and B contain at least two elements. Thus, let $a_1 < a_2 < \ldots < a_m$ and $b_1 < b_2 < \ldots < b_n$ be, respectively, the elements of A and of B, and suppose $|A + B| = m + n - 1$. Then, as in the proof of (i),

$$A + B = (A + b_1) \cup (a_m + B);$$

moreover the whole $A + B$ is ordered as:

$$a_1 + b_1 < a_2 + b_1 < \ldots < a_m + b_1 < a_m + b_2 < \ldots < a_m + b_{n-1} < a_m + b_n. \tag{1.1}$$

Now, look at $A + b_2$; it has m elements and is included in the integers interval $[a_1 + b_1, a_m + b_2] \cap (A + B)$, which also contains m elements; hence, by comparing to (1.1) we have

$$a_i + b_2 = a_{i+1} + b_1 \tag{1.2}$$

for all $i = 1, \cdots, m-1$. We now do the same for $a_{m-1} + B$; by comparing it to (1.1) we obtain

$$a_m + b_i = a_{m-1} + b_{j+1} \tag{1.3}$$

for all $j = 1, \cdots, n-1$. Then, putting together (1.2) and (1.3), we have

$$a_{i+1} - a_i = b_2 - b_1 = a_m - a_{m-1} = b_{j+1} - b_j,$$

for all $i = 1, \cdots, m-1$ and $j = 1, \cdots, n-1$. This clearly finishes the proof. ∎

Suppose we want to find finite subsets A of $\mathbb{Z}$, other than arithmetic progressions, such that $|A+A|$ is small when compared to $|A|$; putting it in a quantitative way, fixed a real number $c \geq 2$, we look for large (with respect to c) finite subsets A of $\mathbb{Z}$ such that $|A+A| < c|A|$. We may then consider any sufficiently long arithmetic progression B and let A be a big portion of it: $A \subseteq B$ with $|A| \geq (2/c)|B|$. Then

$$|A+A| \leq |B+B| < 2|B| \leq c|A|.$$

There is another fundamental way to obtain subsets of $\mathbb{Z}$ with small doubles, which is related to a generalization of the concept of arithmetic progression.

Definition 1.4. Let $1 \leq k \in \mathbb{N}$. A *k-dimensional generalized progression* (or *multi-progression*) in $\mathbb{Z}$ is a finite set of type

$$A = a + I_{(d_1,n_1)} + \cdots + I_{(d_k,n_k)} = \{a + d_1x_1 + \cdots + d_kx_k \mid 0 \leq x_i < n_i,\ i = 1, \ldots, k\}$$

with $a, d_1, \ldots, d_k \in \mathbb{Z}$, and $n_1, \ldots, n_k$ positive integers. The number $\ell(A) = n_1n_2 \cdots n_k$ is the *length* of the progression (or, its *volume*). In general one has $|A| \leq \ell(A)$; the generalized progression A is *proper* if $|A| = \ell(A)$.

It is then easy to check that

- *if A is a proper generalized progression of dimension k then $|A+A| < 2^k|A|$.*

Exercise 1. Prove this claim.

Exercise 2. Let A be a generalized progression of dimension k in $\mathbb{Z}$. Prove that $A - A$ is a k-dimensional generalized progression and $|A-A| < 2^k|A|$.

The fundamental Theorem of Freiman, which we will be ready to prove towards the end of this chapter, says that finite subsets of $\mathbb{Z}$ with small double are obtained by a conjunction of these two procedures: if $|A+A|$ is small then A is a large subset of a generalized progression.

Theorem 1.5 (Freiman). *Let $c \geq 2$, and let A be a finite subset of $\mathbb{Z}$ such that $|A+A| < c|A|$. Then A is contained in a generalized progression of dimension $k(c)$ and length $\ell(c)|A|$, where the positive integers $k(c)$ and $\ell(c)$ depend on c only.*

Search for good estimates of $k(c)$ and $\ell(c)$ is still an ongoing problem. The following nice special case, for which the best bounds are known, is often quoted.

THEOREM 1.6 (Freiman). *Let A be a finite subset of $\mathbb{N}$ such that $|A+A| < 3|A|-3$; then A is contained in a arithmetic progression of length $\ell \leq 2|A|-3$.*

EXAMPLE 2. Let $t \geq m \geq 1$, be positive integers, and consider

$$A = \{1, 2, \dots, m\} \cup \{t+1, t+2, \dots, t+m\}$$

Then $|A+A| = 3(2m-1) = 6m-3 = 3|A|-3$, while the shortest arithmetic progression containing A has length at least $m+t$, which may be arbitrary large. Indeed, A is sort of intrinsically 2-dimensional (it is a 2-dimensional progression).

Freiman isomorphisms. The notion of Freiman isomorphism (or, more in general, homomorphism), introduced by Freiman himself, is a very useful basic tool in studying sum-sets in commutative groups.

DEFINITION 1.7. Let A, B be non empty subsets of, respectively, the commutative groups G and H, and $k \geq 2$; a *Freiman isomorphism of order k* from A to B is a bijective map $\phi : A \to B$ such that

$$\phi(a_1) + \ldots + \phi(a_k) = \phi(a'_1) + \ldots + \phi(a'_k)$$

if and only if

$$a_1 + \ldots + a_k = a'_1 + \ldots + a'_k$$

for every $a_1, \dots, a_k, a'_1, \dots a'_k \in A$.

We say that two non-empty subsets A, B of some commutative groups are *Freiman k-isomorphic* if there exists a Freiman isomorphism of order k from A to B.

EXAMPLE 3. Let $A = \{(0,0), (1,0), (0,1), (1,1)\} \subseteq \mathbb{Z}^2$, $B = \{0, 1, 3, 4\} \subseteq \mathbb{Z}$. The map $(a, b) \mapsto a+3b$ induces a bijection from A to B which is a Freiman isomorphism of order 2 but not of order 3.

EXAMPLE 4. Let $a, b \in \mathbb{Z}$, $b \neq 0$; then the "affine" map $\phi(x) = a + xb$ induces a Freiman isomorphism of order k, for every $k \geq 2$, from A to $\phi(A) \subseteq \mathbb{Z}$, for any non-empty subset A of $\mathbb{Z}$.

In general, let $k \geq 2$, let $f : G \to H$ be a homomorphism of commutative groups, $b \in H$ and A a non-empty subset of G; if the restriction of f to kA is injective then $\phi(x) = b + f(x)$ induces a Freiman isomorphism of order k from A to $\phi(A) \subseteq H$ (we just need to observe that if the restriction of f to kA is injective, then the restriction of f to A is injective).

Clearly, the composition of two Freiman isomorphisms of the same order $k \geq 2$ is a Freiman isomorphism of order k. Also, it is not difficult to show that a Freiman isomorphism of order k is a Freiman isomorphism of order k' for every $2 \leq k' \leq k$

Freiman isomorphisms may be used in reducing sumset questions from generic torsion-free commutative groups to the group of integers $\mathbb{Z}$. This is the content

of Theorem 1.8 below. Before, let us recall the well know structure Theorem for finitely generated commutative groups, which says in particular the following.

• *A finitely generated commutative group is isomorphic to a direct product of a finite number of cyclic groups. Thus, a finitely generated torsion-free commutative group is isomorphic to* $\mathbb{Z}^n$ *for some* $1 \leq n \in \mathbb{N}$.

THEOREM 1.8. *Let* A *be a non-empty finite subset of a torsion-free abelian group* G*; then, for every* $k \geq 2$*,* A *is Freiman* k*-isomorphic to a subset of* $\mathbb{Z}$.

PROOF. We may suppose that G coincides with the subgroup generated by A; hence G is a finitely generated torsion-free commutative group, and so $G = \mathbb{Z}^m$ for some positive integer m.
Let $A = \{x_1, \ldots, x_n\}$ with, for each $i = 1, \ldots, n$,

$$x_i = (x_{i1}, \ldots, x_{im}) \in \mathbb{Z}^m.$$

By translating by a suitable element in $\mathbb{Z}^m$, we may assume $x_{ij} \geq 0$ for every i, j. Let M be a positive integer with

$$M > k \cdot \max\{a_{ij} \mid i = 1, \ldots, n,\ j = 1, \ldots, m\},$$

and consider the group homomorphism $\phi : \mathbb{Z}^m \to \mathbb{Z}$ defined by

$$\phi(a_1, \ldots, a_m) = a_1 + a_2 M + \cdots + a_m M^{m-1}.$$

The choice of M ensures that the restriction of ϕ to kA is injective, hence (see Example 4) ϕ induces a Freiman isomorphism of order k from A to $\phi(A) \subseteq \mathbb{Z}$. ■

As an immediate sample application of this Theorem, we obtain the following from Lemma 1.3.

PROPOSITION 1.9. *Let* G *be a torsion-free commutative group, and* A, B *two finite non-empty subsets of* G*; then* $|A + B| \geq |A| + |B| - 1$.

Thus, the total ordering in $\mathbb{Z}$, which was an essential ingredient in the proof of Lemma 1.3, it is not really the point of it (showing, I guess, the power of the idea of Freiman isomorphism even at such rather simple instances).

Of course, there is no difficulty in extending the definition of multi-progression of dimension, say, r, to any commutative group G: for $a_0, a_1, \ldots, a_r \in G$ and $\ell_1, \ldots, \ell_r \in \mathbb{N}$, one has the r-dimensional progression of length $\ell(P) = \ell_1 \cdots \ell_r$:

$$P = \{a_0 + n_1 a_1 + \cdots n_r a_r \mid 0 \leq n_i < \ell_i,\ i = 1, \ldots, r\}.$$

EXERCISE 3. Prove that the property of being a generalized progression of dimension r is preserved under Freiman 2-isomorphisms.

EXERCISE 4. Let A, B two subsets of some commutative groups, and assume that both A and B contain 0 (of the appropriate group). Prove that if $A+A$ and $B+B$ are Freiman k-isomorphic, then A and B are Freiman $2k$ isomorphic. Does the converse hold?

1.2. Ruzsa and Plünnecke inequalities

Freiman's original proof was highly non-trivial and, at points, – experts say – difficult to follow (the interested reader may refer to the monograph [**9**]); it is perhaps for this reason that his work did not immediately gained the wide recognition it deserved. In 1994, I. Ruzsa produced its own proof [**22**], much shorter and easier to understand; it was this proof that put Frieman's results in their right prominent place, revealing to many their deep and seminal nature. It is Ruzsa proof, with some further simplifications that have been devised since its first appearance, that will occupy most of the rest of this chapter; although simpler that the original it is still far from being straightforward, and is full of ingenious arguments, that have entered the tool box of anybody in the area.

We indeed start with one of these arguments, pointing out the fact that it does not assume a commutative setting.

LEMMA 1.10 (Ruzsa triangle inequality). *Let A, B, C be non-empty finite subsets of the group G; then*

$$|A||BC^{-1}| \leq |BA^{-1}||AC^{-1}|. \tag{1.4}$$

PROOF. The map $B \times C \to BC^{-1}$ given by $(b,c) \mapsto bc^{-1}$ is surjective; let $\pi : BC^{-1} \to B \times C$ be a fixed right inverse of it (that is $\pi(x) = (b_x, c_x) \in B \times C$ with $b_x c_x^{-1} = x$). Then define

$$\begin{aligned} \phi : A \times BC^{-1} &\to BA^{-1} \times AC^{-1} \\ (a,x) &\mapsto (b_x a^{-1}, a c_x^{-1}). \end{aligned}$$

The map ϕ is injective, and this proves the claim. ∎

Let us observe the following immediate, but not completely trivial, consequence of Ruzsa inequality. For a non-empty finite subset A of a group, (1.4) yields

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

hence

$$|AA^{-1}| \leq \frac{|AA|^2}{|A|}. \tag{1.5}$$

The Plünneke–Ruzsa inequality (Theorem 1.15) is a far-reaching generalization of this, which only holds for commutative groups. In proving it, we will follow the brilliant approach by Petridis in [**20**], which avoids use of graph theory. We

emphasize that, again, the first two results do not assume commutativity of the ambient group.

LEMMA 1.11. *Let X, B be finite non-empty subsets of the group G, and suppose that*

$$\alpha := \frac{|XB|}{|X|} \leq \frac{|ZB|}{|Z|},$$

for all $\emptyset \neq Z \subseteq X$. Then, for every finite $\emptyset \neq C \subseteq G$,

$$|CXB| \leq \alpha |CX|. \tag{1.6}$$

PROOF. Let X and B as in the assumptions, and $C = \{c_1, \ldots, c_n\}$ a non-empty subset of G. Set $X_1 = X$ and, for $2 \leq i \leq n$,

$$X_i = \{x \in X \mid c_i x \notin c_1 X \cup \ldots \cup c_{i-1} X\}.$$

Then, CX is the disjoint union

$$CX = c_1 X_1 \cup c_2 X_2 \cup \ldots c_n X_n,$$

and, for any $1 \leq j \leq n$

$$|\{c_1, \ldots, c_j\} X| = |c_1 X_1 \cup \ldots \cup c_j X_j| = \sum_{i=1}^{j} |c_i X_i| = \sum_{i=1}^{j} |X_i|.$$

We now prove that (1.6) holds by induction on n. If $n = 1$, i.e. $C = \{c\}$,

$$|CXB| = |cXB| = |XB| = \alpha |X| = \alpha |cX|.$$

Let $n \geq 2$, and write $Y = X \setminus X_n$. Then $c_n YB \subseteq \{c_1, \ldots, c_{n-1}\} XB$, by definition of X_n. Thus

$$CXB = (\{c_1, \ldots, c_{n-1}\} XB) \cup (c_n XB \setminus c_n YB). \tag{1.7}$$

Now, $|c_n XB \setminus c_n YB| = |c_n XB| - |c_n YB| = |XB| - |YB|$, and, by choice of X,

$$|XB| - |YB| \leq \alpha |X| - \alpha |Y| = \alpha (|X| - |Y|) = \alpha |X_n|.$$

Also, by inductive assumption

$$|\{c_1, \ldots, c_{n-1}\} XB| \leq \alpha |\{c_1, \ldots, c_{n-1}\} X| = \alpha \sum_{1+1}^{n-1} |X_i|.$$

Therefore, from (1.7) we obtain

$$|CXB| \leq |\{c_1, \ldots, c_{n-1}\} XB| + \alpha |X_n| \leq \alpha \sum_{i=1}^{n-1} |X_i| + \alpha |X_n| = \alpha \sum_{i=1}^{n} |X_i| = \alpha |CX|$$

thus finishing the proof. ∎

THEOREM 1.12. *Let A, B be finite non-empty subsets of the group G such that*

$$|AB| \leq \alpha |A|$$

for a positive real number α. Then there exists $\emptyset \neq X \subseteq A$ such that

$$|CXB| \leq \alpha |CX|$$

for every finite subset C of G.

PROOF. Choose $\emptyset \neq X \subseteq A$ such that $|XB|/|X|$ is as small as possible. Then $|XB|/|X| \leq \alpha$ and X, B are as in the assumptions of Lemma 1.11. Now the Theorem follows at once from Lemma 1.11. ∎

THEOREM 1.13 (Plünnecke). *Let A, B be finite non-empty subsets of the commutative group G such that*

$$|A + B| \leq \alpha |A|$$

for a positive real number α. Then there exists $\emptyset \neq X \subseteq A$ such that

$$|X + hB| \leq \alpha^h |X|$$

for every $1 \leq h \in \mathbb{N}$.

PROOF. Select $X \subseteq A$ as in Theorem 1.12. Arguing by induction on $h \geq 1$, we show that the claim holds for X. For $h = 1$ we have $|X+B|/|X| \leq |A+B|/|A| \leq \alpha$, and we are done. Let $h \geq 2$ and set $C = (h-1)B$; then, by Theorem 1.12 and inductive assumption,

$$|X + hB| = |X + C + B| = |C + X + B| \leq \alpha |X + C| \leq \alpha \alpha^{h-1} |X| = \alpha^h |X|.$$

∎

In this proof, I have expressly reported the equality $X + C + B = C + X + B$, which may seem unduly fastidious, but I wanted to stress in which, rather subtle, way commutativity enters the play.
A relevant special case, which immediately follows, is when $A = B$:

COROLLARY 1.14. *Let A be finite non-empty subset of the commutative group G with $|A + A| \leq \alpha |A|$, for a positive real number α. Then, for every $1 \leq h \in \mathbb{N}$,*

$$|hA| \leq \alpha^h |A|.$$

Let us pause to observe that part of the content of this Corollary is that, for a finite non-empty subset A of a *commutative* group, the size of its double $A + A$ controls the sizes of the other multiples hA; it in fact says that, for every $h \geq 2$,

$$|hA| \leq \frac{|A + A|^h}{|A|^{h-1}}. \tag{1.8}$$

In a sense, in the commutative case, it is the doubling $A + A$ that sets the pace of the growth of the sets hA. We will observe in due course (section 1.6) that this is no longer the case for non-commutative groups.

THEOREM 1.15 (Plünnecke-Ruzsa inequality). *Let A, B be finite non-empty subsets of the commutative group G such that $|A + B| \leq \alpha|A|$, for a positive real number α. Then for every $k, \ell \in \mathbb{N}$ with $k + \ell > 1$,*

$$|kB - \ell B| \leq \alpha^{k+\ell}|A|.$$

PROOF. Let $X \subseteq A$ as in Theorem 1.13. Then, by Ruzsa triangle inequality (Lemma 1.10),

$$|-X||kB - \ell B| \leq |X + kB||-X - \ell B| = |X + kB||X + \ell B| \leq \alpha^{k+\ell}|X|^2;$$

whence

$$|kB - \ell B| \leq \alpha^{k+\ell}|X| \leq \alpha^{k+\ell}|A|.$$

■

REMARK. By Ruzsa triangle inequality, the case $k = \ell = 1$ holds in the non commutative case as well. In fact, if $|BA| \leq \alpha|A|$, then by Lemma 1.10:

$$|A^{-1}||BB^{-1}| \leq |BA||A^{-1}B^{-1}| = |BA|^2 \leq \alpha^2|A|^2$$

and so $|BB^{-1}| \leq \alpha^2|A|$. Observe, however, that in a non-commutative group, given a non-empty finite set B, the sizes of BB^{-1} and $B^{-1}B$ may be as divergent as possible (try $B = Hx \cup H$, with H a finite subgroup and $x \notin H$).

EXERCISE 5. [Ruzsa] Prove that if $A, B_1, \ldots, B_n$ are non-empty finite subsets of the commutative group G, with $|A + B_i| \leq c_i|A|$ for $i = 1, \ldots, n$, then

$$|A + B_1 + \cdots + B_n| \leq c_1 \cdots c_n|A|.$$

We are now going to apply Plünneke-Ruzsa inequality to sum-sets in commutative groups of finite exponent. The following trick (for which commutativity is not required) will be the fundamental step in the proof.

LEMMA 1.16 (Ruzsa covering Lemma). *Let A, B be finite non-empty subsets of a group. Then there exists $X \subseteq B$ such that $|X| \leq |BA|/|A|$ and $B \subseteq XAA^{-1}$.*

PROOF. Just take $X \subseteq B$ maximal such that $xA \cap yA = \emptyset$ for $x, y \in X, x \neq y$. Then, by the very choice of X,

$$|BA| \geq |XA| = \Big|\bigcup_{x \in X} xA\Big| = \sum_{x \in X} |xA| = |X||A|,$$

hence $|X| \leq |BA|/|A|$. Now, let $b \in B$; then, by maximality of X, there exists $x \in X$ such that $bA \cap xA \neq \emptyset$. Thus, $ba = xa_1$ for some $a, a_1 \in A$ and therefore $b = xa_1a^{-1} \in XAA^{-1}$. ■

Let $1 \leq r \in \mathbb{N}$; a group G is said to have *exponent* r if $g^r = 1$ ($rg = 0$ in additive notation) for every $g \in G$, and r is the smallest positive integer with this property. Let us observe that if G is a k-generated commutative group of exponent r, then $|G| \leq r^k$.

THEOREM 1.17. *Let r be a positive integer, and A be a finite non-empty subset of a commutative group of exponent r, such that $|A + A| \leq C|A|$, for some real number C. Let $H = \langle A \rangle$ be the subgroup generated by A. Then $|H| \leq C^2 r^{C^4} |A|$.*

PROOF. By Theorem 1.15,

$$|A + (2A - A)| = |3A - A| \leq C^4 |A|.$$

Let $X \subseteq 2A - A$ as in Lemma 1.16; then $|X| \leq C^4$ and

$$2A - A \subseteq X + (A - A). \tag{1.9}$$

Let Q be the subgroup generated by X; then $|Q| \leq r^{C^4}$. By adding A to both sides in (1.9) we have

$$3A - A \subseteq X + 2A - A \subseteq 2X + (A - A) \subseteq Q + (A - A),$$

and by the same step in induction on m,

$$mA - A \subseteq Q + (A - A) \tag{1.10}$$

for every $m \geq 2$. Now, if H is the subgroup generated by A. Since we are inside a periodic group, it is then clear that

$$H = \bigcup_{m \geq 1} (mA - A).$$

Hence, by (1.10), $H \subseteq Q + (A - A) \subseteq H$. Therefore, $H = Q + (A - A)$ and

$$|H| \leq |Q||A - A| \leq r^{C^4} C^2 |A|.$$

■

1.3. Fourier analysis

Let $2 \leq m \in \mathbb{N}$; in the rest of these notes we denote by $\mathbb{Z}_m$ the ring $\mathbb{Z}/m\mathbb{Z}$ of residue classes modulo m, and by $\mathbb{Z}_m^*$ the set of its non-zero elements. Remember that, as an additive group, $\mathbb{Z}_m$ is cyclic.

The proof of Freiman's Theorem will be achieved by first proving the same type of statement for the cyclic groups $\mathbb{Z}_m$, then showing how to pass from $\mathbb{Z}$ to a suitable $\mathbb{Z}_m$. This final part (section 1.5) is by a clever argument of Ruzsa, while the $\mathbb{Z}_m$ case is accomplished in two steps: the first, which is the content of this section, uses Fourier analysis on $\mathbb{Z}_m$, the second (section 1.4) relies on Minkowski's Theorems about lattices in $\mathbb{R}^n$.

In what follows, G will be a finite commutative group and $|G| = n$. For $z \in \mathbb{C}$, $\overline{z}$ denotes its complex conjugate.) We denote by $\ell^2(G)$ the set of all functions $G \to \mathbb{C}$. Then $\ell^2(G)$ is in a natural way a n-dimensional vector space over $\mathbb{C}$, and it is endowed with the inner product

$$\langle f, g\rangle = \sum_{x\in G} f(x)\overline{g(x)} \tag{1.11}$$

(Usually, especially when dealing with characters, the inner product is normalized by multiplying by $|G|^{-1}$. However, I prefer the unscaled version, as there is no harm by adopting it in this section, while in this form such inner product will return later on in these notes.)

DEFINITION 1.18. A *character* of G is a group homomorphism $\mu : G \to \mathbb{C}^*$ (where $\mathbb{C}^*$ is the multiplicative group of all non–zero complex numbers).

Let μ be a character of G. Since G is finite, $\mu(x)$ is a root of unity for every $x \in G$, hence $\mu(G)$ is a subgroup of the complex torus $\{z \in \mathbb{C} \mid |z| = 1\}$.
We denote by $\widehat{G}$ the set of all characters of G (this is often called the dual of G). Then $\widehat{G}$ is a group by pointwise multiplication: $(\eta\mu)(x) = \eta(x)\mu(x)$ for $\eta, \mu \in \widehat{G}$ and $x \in G$; the identical element of $\widehat{G}$ is the principal character 1_G (that is the constant map 1 on G), and for every $\mu \in \widehat{G}$ and $x \in G$, $\mu^{-1}(x) = \overline{\mu(x)}$.

EXERCISE 6. Show that for every $0 \neq x \in G$ there is a character $\mu \in \widehat{G}$ such that $\mu(x) \neq 1$.

PROPOSITION 1.19. *Let G be a finite commutative group and $\widehat{G}$ the group of its characters. Then*

(1) $\langle \alpha, \beta\rangle = 0$ *for every* $\alpha, \beta \in \widehat{G}$, $\alpha \neq \beta$.
(2) $\sum_{\mu\in\widehat{G}} \mu(x) = 0$ *for every* $0 \neq x \in G$.
(3) $|\widehat{G}| = |G|$.
(4) $\widehat{G}$ *is an orthogonal basis of the* $\mathbb{C}$*-svector space* $\ell^2(G)$.

PROOF. Of course, (4) is just a restatement of (1) and (3).

(1) Let $\alpha, \beta \in \widehat{G}$ and suppose $c = \langle \alpha, \beta\rangle \neq 0$. Then, for every $g \in G$,

$$c = \sum_{x\in G} \alpha(x)\overline{\beta(x)} = \sum_{x\in G} \alpha(g+x)\overline{\beta(g+x)} = \sum_{x\in G} \alpha(g)\alpha(x)\overline{\beta(g)\beta(x)} = \alpha(g)\overline{\beta(g)}c,$$

hence $\alpha(g)\overline{\beta(g)} = 1$, and so $\alpha(g) = \beta(g)$. Thus, $\alpha = \beta$.

(2) Let $0 \neq x \in G$; by exercise 6 there is a $\alpha \in \widehat{G}$ such that $\alpha(x) \neq 1$. Now, since $\widehat{G}$ is a group,

$$\sum_{\mu\in\widehat{G}} \mu(x) = \sum_{\mu\in\widehat{G}} (\alpha\mu)(x) = \alpha(x) \sum_{\mu\in\widehat{G}} \mu(x),$$

and the claim follows.

(3) By the previous points we have

$$|\widehat{G}| = \sum_{\mu\in\widehat{G}} \mu(0) = \sum_{x\in G}\sum_{\mu\in\widehat{G}} \mu(x) = \sum_{\mu\in\widehat{G}}\sum_{x\in G} \mu(x) = \sum_{\mu\in\widehat{G}} \langle \mu, 1_G\rangle = \langle 1_G, 1_G\rangle = |G|$$

and the proof is done. ∎

EXERCISE 7. Let G be a finite commutative group, $x, y \in G$ with $x \neq y$. Prove

$$\sum_{\mu\in\widehat{G}} \mu(x)\overline{\mu(y)} = 0.$$

Now, the Fourier transform is the tool that allows to describe the coefficients of any $f \in \ell^2(G)$ with respect to the basis $\widehat{G}$.

DEFINITION 1.20. Let $f \in \ell^2(G)$; the *Fourier transform* of f is the function $\hat{f} \in \ell^2(\widehat{G})$ defined by

$$\hat{f}(\mu) = \sum_{x\in G} f(x)\mu(x)$$

for every $\mu \in \widehat{G}$.

THEOREM 1.21 (Fourier inversion formula). *For every $f \in \ell^2(G)$ we have*

$$f(x) = |G|^{-1} \sum_{\mu\in\widehat{G}} \hat{f}(\mu)\overline{\mu(x)}.$$

PROOF. Let $f \in \ell^2(G)$; by standard linear algebra:

$$f = \sum_{\mu\in\widehat{G}} \frac{\langle f, \mu\rangle}{\langle \mu, \mu\rangle} \cdot \mu = \frac{1}{|G|} \sum_{\mu\in\widehat{G}} \langle f, \mu^{-1}\rangle \cdot \mu^{-1}.$$

Hence, for any $x \in G$

$$f(x) = \frac{1}{|G|} \sum_{\mu\in\widehat{G}} \Big(\sum_{y\in G} f(y)\mu(y)\Big)\mu^{-1}(x) = \frac{1}{|G|} \sum_{\mu\in\widehat{G}} \hat{f}(\mu)\overline{\mu(x)}.$$

∎

Now, a useful identity, whose proof we leave as an exercise.

LEMMA 1.22 (Perseval/Plancherel identity). *For every $f \in \ell^2(G)$, we have*

$$\sum_{\mu\in\widehat{G}} |\hat{f}(\mu)|^2 = |G| \sum_{x\in G} |f(x)|^2.$$

If $f \in \ell^2(G)$, its reflection is the function $\bar{f} \in \ell^2(G)$ defined by

$$\bar{f}(x) = \overline{f(-x)}$$

for every $x \in G$. Clearly, $\bar{\bar{f}} = f$.
Together with pointwise product, in $\ell^2(G)$ we also have the important *convolution* product

$$(f * g)(x) = \sum_{y\in G} f(y)g(x - y),$$

for $f, g \in \ell^2(G)$ and any $x \in G$. The following is immediate.

LEMMA 1.23. *For every $f, g \in \ell^2(G)$ we have:*

(1) $\overline{\hat{f}} = \widehat{\overline{f}}$;
(2) $\widehat{f * g} = \hat{f}\hat{g}$.

We observe one first reason why this is of interest in our contest. For $A \subseteq G$ let χ_A be the characteristic function of A; then for every $x \in G$,

$$\chi_A * \chi_A(x) = \sum_{x_1+x_2=x} \chi_A(x_1)\chi_A(x_2),$$

hence $\chi_A * \chi_A(x)$ counts the number of ordered pairs $(x_1, x_2) \in A \times A$ such that $x = x_1 + x_2$. In an analogue way, since clearly $\overline{\chi}_A = \chi_{-A}$, for any $x \in G$

$$\chi_A * \chi_A * \overline{\chi}_A * \overline{\chi}_A(x)$$

is not zero only for $x \in 2A - 2A$, and for any such x it counts the number of quadruples $(x_1, x_2, x_3, x_4) \in A \times A \times A \times A$ such that $x = x_1 + x_2 - x_3 - x_4$. This will be of use in the proof of Lemma 1.25 below.

Bohr neighborhoods in $\mathbb{Z}_m$. Now, we are specially interested in the case $G = \mathbb{Z}_m$. Then G is cyclic, and a character μ is determined by the image of the generator 1 of $\mathbb{Z}_m$, which may be any m-th root of unity. If we write $\omega = e^{2\pi i/m}$ (or any other primitive m-th root of unit), then $\widehat{\mathbb{Z}}_m = \{\gamma_0, \dots, \gamma_{m-1}\}$, where, for $j = 0, \dots, m-1$, and $a \in \mathbb{Z}$,

$$\gamma_j(a + m\mathbb{Z}) = \omega^{ja}. \tag{1.12}$$

Observe that $\gamma_0 = 1_G$ is the principal character.

For any $r \in \mathbb{R}$, let $||r||$ denote the distance from r to the nearest integer. Let $x, y \in \mathbb{R}$ and m a positive integer: if $x - y \in m\mathbb{Z}$ then $||x/m|| = ||y/m||$. Hence we have a well defined function $\mathbb{Z}_m \to [0, 1)$ by setting

$$\left\| \frac{a + m\mathbb{Z}}{m} \right\| := \left\| \frac{a}{m} \right\|.$$

DEFINITION 1.24. Let $2 \leq m \in \mathbb{N}$. Given $a_1, \dots a_k \in \mathbb{Z}_m$ $(k \geq 1)$ and $0 < \delta \in \mathbb{R}$, we define the *Bohr neighborhood* as the set

$$B(a_1, \dots, a_k; \delta) = \{g \in \mathbb{Z}_m \mid \|ga_i/m\| \leq \delta, \text{ for } i = 1, \dots k\}.$$

The proof of the following Lemma is essentially due to Bogolyubov (1936).

LEMMA 1.25. *Let $2 \leq m \in \mathbb{N}$, and let A be a non-empty subset of the group $\mathbb{Z}_m$ with $\beta = |A|/m < 1$. Then $2A - 2A$ contains a Bohr neighborhood $B(j_1, \dots, j_k; 1/4)$ for an integer $1 \leq k < \beta^{-2}$.*

PROOF. Let $\widehat{\mathbb{Z}}_m = \{\gamma_0, \dots, \gamma_{m-1}\}$ as defined in (1.12), and write χ_A for the characteristic function on A. Then, for $j = 0, \dots, m-1$

$$A(j) := \widehat{\chi}_A(\gamma_j) = \sum_{x \in A} \gamma_j(x) = \sum_{x \in A} \omega^{xj},$$

where $\omega = e^{2\pi i/m}$. Observe that $A(0) = |A|$, and that (by Perseval identity)

$$\sum_{j=0}^{m-1} |A(j)|^2 = m|A| = \beta m^2. \tag{1.13}$$

Let $f = \chi_A * \chi_A * \overline{\chi}_A * \overline{\chi}_A$; by Lemma 1.23, for every $j = 0, \dots, m-1$,

$$\hat{f}(\gamma_j) = |\widehat{\chi}_A(\gamma_j)|^4 = |A(j)|^4, \tag{1.14}$$

hence, by Fourier inversion formula,

$$f(x) = \frac{1}{m} \sum_{j=0}^{m-1} |A(j)|^4 \overline{\gamma_j(x)} = \frac{1}{m} \sum_{j=0}^{m-1} |A(j)|^4 \omega^{-jx}.$$

Recall that $f(x)$ takes only integral values and has support in $2A - 2A$; in particular

$$f(x) = Re(f(x)) = \frac{1}{m} \sum_{j=0}^{m-1} |A(j)|^4 Re(\omega^{jx}). \tag{1.15}$$

Now, let $S = \{j \in \{0, \dots, m-1\} \mid |A(j)| \geq \beta^{3/2} m\}$. Then $S \neq \emptyset$; in fact, $A(0) = |A| = \beta m$ and so, since $\beta < 1$, $0 \in S$. Moreover, from (1.13)

$$\beta m^2 \geq \sum_{j \in S} |A(j)|^2 \geq \beta^3 m^2 |S|$$

whence $1 \leq |S| \leq \beta^{-2}$. Let $k = |S|$ and $S = \{j_1, \dots, j_k\}$; we want to show that the Bohr neighborhood $B(S; 1/4) = B(j_1, \dots, j_k; 1/4)$ is contained in $2A - 2A$ or, equivalently, that $f(x) \neq 0$ for every $x \in B(S; 1/4)$. By definition, if $d \in B(S; 1/4)$ then $\|dj/4\| \leq 1/4$ for every $j \in S$, and this is equivalent to

$$Re(\omega^{dj}) \geq 0 \text{ for every } j \in S. \tag{1.16}$$

Now observe that, by (1.13),

$$\sum_{j \notin S} |A(j)|^4 < \beta^3 m^2 \sum_{j=0}^{m-1} |A(j)|^2 \leq \beta^4 m^4 = |A|^4. \tag{1.17}$$

If $d \in B(S; 1/4)$ then, from (1.15) and (1.16),

$$mf(d) = \sum_{j=0}^{m-1} |A(j)|^4 Re(\omega^{jd}) \geq |A(0)|^4 - \left| \sum_{j \notin S} |A(j)|^4 \omega^{-jx} \right| > |A|^4 - |A|^4 \geq 0.$$

Hence $f(d) > 0$ and so $d \in 2A - 2A$. ∎

EXAMPLE 5. Suppose (for simplicity) that m is odd, and $0 < \delta < 1/2$. Then, for $u \in \mathbb{Z}$, $||u/m|| \leq \delta$ if and only if u is congruent to an integer y with $|y| \leq \delta m$; thus, the number of $g \in \mathbb{Z}_m$ such that $||g/m|| \leq \delta$ is $k = 2[\delta m] + 1$. Let $a \in \mathbb{Z}$ with $(a, m) = 1$; then multiplying by a is a bijection in $\mathbb{Z}_m$, hence $|B(a; \delta)| = k$ (here, and in the following, we use the same letter to denote an integer and its congruence class modulo m). Now, let u be the multiplicative inverse of a in $\mathbb{Z}_m$, then for every $y \in \mathbb{Z}_m$, $||a(uy)/m|| = ||y/m||$. It thus follow that

$$B(a; \delta) = \{yu \in \mathbb{Z}_m \mid -[\delta m] \leq y \leq [\delta m]\},$$

that is, $B(a; \delta)$ is an arithmetic progression in $\mathbb{Z}_m$ of length k.

In the next section we extend this by showing that, in general, Bohr neighborhoods contain long generalized arithmetic progressions.

1.4. Geometry of numbers

DEFINITION 1.26. Let $n \geq 1$, a *lattice* Λ in the euclidean space $\mathbb{R}^n$ is a subgroup of the additive group of $\mathbb{R}^n$ generated by n independent vectors. Thus, if $U = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ is a set of n independent vectors in $\mathbb{R}$, the lattice generated by U is the set

$$\Lambda = \mathbb{Z}\mathbf{u}_1 \oplus \cdots \oplus \mathbb{Z}\mathbf{u}_n. \tag{1.18}$$

Let me recall the equivalent definition

- *A lattice in $\mathbb{R}^n$ is a discrete subgroup that is not contained in any subspace of smaller dimension.*

Where a subgroup H of the additive group $\mathbb{R}^n$ is discrete if for every $\mathbf{a} \in H$ there is an open ball $B(\mathbf{a}, \delta)$ of radius $\delta > 0$ such that

$$H \cap B(\mathbf{a}, \delta) = \{\mathbf{a}\}.$$

Let $\Lambda = \mathbb{Z}\mathbf{u}_1 \oplus \cdots \oplus \mathbb{Z}\mathbf{u}_n$ be a lattice; a *basis* for Λ is just a set of n generators of it. If $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ is a basis for the lattice Λ, the set $F \subseteq \mathbb{R}^n$

$$\{x_1\mathbf{u}_1 + \ldots + x_n\mathbf{u}_n \mid x_i \in \mathbb{R},\ 0 \leq x_i < 1\}$$

is called a *fundamental domain* of Λ. The following fact is easily established.

LEMMA 1.27. *Let F be a fundamental domain of the lattice Λ; then $\mathbb{R}^n = \Lambda + F$.*

As the lattice Λ has many different bases, it has many different fundamental domains. However the fundamental domains all have the same volume, which is obtained as the absolute value of the determinant of the $n \times n$ real matrix whose columns are the vectors of a basis of Λ. This is called the *determinant* or also the *volume* of Λ. Thus, if $\Lambda = \mathbb{Z}\mathbf{u}_1 \oplus \cdots \oplus \mathbb{Z}\mathbf{u}_n$,

$$\det(\Lambda) = |\det(\mathbf{u}_1, \ldots, \mathbf{u}_n)|\,.$$

(This is because different bases of Λ are obtained from each other by applying a linear map whose matrix has integral entries and determinant ± 1.)

EXERCISE 8. Prove Lemma 1.27.

DEFINITION 1.28. 1) A subset $X \neq \emptyset$ of $\mathbb{R}^n$ is *convex* if, for every $\mathbf{a}, \mathbf{b} \in X$, the whole line segment from $\mathbf{a}$ to $\mathbf{b}$, $\{t\mathbf{a} + (1-t)\mathbf{b} \mid 0 \leq t \leq 1\}$, is contained in X.
2) A *convex body* in $\mathbb{R}^n$ is a bounded open set $X \subset \mathbb{R}^n$ which is convex.
3) A convex body X is *centrally symmetric* if: $\mathbf{a} \in X \Rightarrow -\mathbf{a} \in X$.

Observe that a centrally symmetric convex body always contains the origin, for $0 = \frac{1}{2}\mathbf{a} + \frac{1}{2}(-\mathbf{a})$.

EXERCISE 9. Prove that a subset X of $\mathbb{R}^n$ is convex if and only if $aX + bX = (a+b)X$ for all $a, b \in \mathbb{R}$, $a, b > 0$.

EXAMPLE 6. The example of a centrally symmetric convex body that we essentially need in the following is that of a *box*. Let $l = (\lambda_1, \ldots, \lambda_n) \in \mathbb{R}^n$ with $\lambda_i > 0$ for every $i = 1, \ldots, n$. The *box* defined by l,

$$B_l = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid |x_i| < \lambda_i, \text{ for } i = 1, \ldots, n\}$$

is a centrally symmetric convex body of $\mathbb{R}^n$.

The proof that Bohr neighborhoods contain progressions is an application of the second Minkowski Theorem on lattices, whose statement is better understood when recalling also the first Minkowski Theorem. Because lack of time, both these theorems will go without proof (dedicated readers may consult the textbook [**13**]).

THEOREM 1.29 (First Minkowski Theorem). *Let Λ be a lattice in $\mathbb{R}^n$ and $X \subset \mathbb{R}^n$ a centrally symmetric convex body. If $\mathrm{vol}(X) > \det(\Lambda)$ then X contains a non-zero element of Λ.*

Thus, given a centrally convex body X and a lattice Λ there is a smallest positive real number λ_1 such that the closure $\overline{\lambda_1 X}$ of the dilation $\lambda_1 X$ contains a non-zero element of Λ; indeed

$$\lambda_1 = \inf\{0 < \lambda \in \mathbb{R} \mid \lambda X \cap \Lambda \text{ contains a vector } \mathbf{b} \neq 0\}.$$

For $i = 1, \ldots, n$, one then defines λ_i as the smallest positive real number such that $\overline{\lambda_i X}$ contains i linearly independent elements of Λ; the numbers $\lambda_1, \ldots, \lambda_n$ are called the *successive minima* of X with respect Λ; clearly $0 < \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n$.

THEOREM 1.30 (Second Minkowski Theorem). *Let Λ be a lattice in $\mathbb{R}^n$ and $X \subset \mathbb{R}^n$ a centrally symmetric convex body. Let $\lambda_1, \ldots, \lambda_n$ be the successive minima of X with respect Λ. Then*

$$\lambda_1 \lambda_2 \cdots \lambda_n \mathrm{vol}(X) \leq 2^n \det(\Lambda).$$

To make things a little shorter, we prove the result on Bohr neighborhoods in the case m is a prime, which is enough for our purposes.

LEMMA 1.31. *Let $m \in \mathbb{N}$ be an odd prime, $a_1, \cdots, a_n$ non-zero elements of $\mathbb{Z}_m$, and $0 < \delta < 1/2$. Then the Bohr neighborhood $B(a_1, \dots, a_n; \delta)$ contains a proper n-dimensional generalized progression P with $\ell(P) \geq (\delta/n)^n m$.*

PROOF. In this proof, we denote by a_i both the congruence class mod m and a (fixed) integer belonging to it; this will not cause any troubles.
In $\mathbb{R}^n$ let $\mathbf{a} = (a_1, \dots, a_n)$ and consider

$$\Lambda = \mathbb{Z}\mathbf{a} + (m\mathbb{Z})^n. \tag{1.19}$$

This is a subgroup of $\mathbb{Z}^n$ of rank n and so it is a lattice in $\mathbb{R}^n$. Also, because m is a prime and the a_i are not multiples of it, Λ is the disjoint union of the m distinct cosets $k\mathbf{a} + (m\mathbb{Z})^n$ for $k = 0, \dots, m-1$. Since $\det((m\mathbb{Z})^n) = m^n$, we have $\det(\Lambda) = m^{n-1}$ (if you do't believe this then go to exercise 10 below).
Then, let B be the box

$$B = \{(x_1, \dots, x_n \in \mathbb{R}^n \mid |x_i| < \delta,\ i = 1, \dots, n\},$$

and observe that $\mathrm{vol}(B) = (2\delta)^n$. Let $\lambda_1, \dots, \lambda_n$ be the successive minima of B with respect to Λ, and $\mathbf{b}_1, \dots, \mathbf{b}_n$ linearly independent vectors such that

$$\mathbf{b}_i = (b_{i1}, \dots, b_{in}) \in \overline{\lambda_i B} \cap \Lambda,$$

for each $i = 0, \dots, n$. By Theorem 1.30, we have

$$\lambda_1 \lambda_2 \cdots \lambda_n \leq 2^n \frac{\det(\Lambda)}{\mathrm{vol}(B)} = \frac{m^{n-1}}{\delta^n}. \tag{1.20}$$

The fact that $\mathbf{b}_i \in \overline{\lambda_i B}$ implies

$$|b_{ij}| \leq \lambda_i \delta \tag{1.21}$$

for all $i, j = 0, \dots, n$; on the other hand, since $\mathbf{b}_i \in \Lambda$, it follows from (1.19) that there exists $v_i \in \mathbb{Z}$ (and, by abuse of notation, $v_i \in \mathbb{Z}_m$) such that

$$\mathbf{b}_i - v_i \mathbf{a} \in (m\mathbb{Z})^n. \tag{1.22}$$

For $i = 1, \dots, n$, we set

$$\ell_i = \left[\frac{m}{n\lambda_i} \right],$$

then, in $\mathbb{Z}_m$ we consider the n-dimensional multi-progression

$$P = \{x_1 v_1 + \cdots + x_n v_n \mid x_i \in \mathbb{Z},\ |x_i| \leq \ell_i\}.$$

Let $x = x_1 v_1 + \cdots + x_n v_n \in P$, then, by (1.22),

$$x\mathbf{a} - \sum_{i=1}^{n} x_i \mathbf{b}_i \in (m\mathbb{Z})^n.$$

Therefore, because of (1.21), for $j = 1, \dots, n$ we have

$$\left\| \frac{xa_j}{m} \right\| = \left\| \sum_{i=1}^{n} \frac{x_i b_{ij}}{m} \right\| \leq \sum_{i=1}^{n} \left| \frac{x_i b_{ij}}{m} \right| \leq \sum_{i=1}^{n} \frac{\ell_i \lambda_i \delta}{m} \leq \sum_{i=1}^{n} \frac{\delta}{n} = \delta.$$

This proves $P \subseteq B(a_1, \dots, a_n; \delta)$. Now,

$$\ell(P) \geq (\ell_1 + 1) \cdots (\ell_n + 1) \geq \prod_{i=1}^{n} \frac{m}{n\lambda_i} = \frac{m^n}{n^n} \prod_{i=1}^{n} \lambda_i^{-1},$$

and so, by (1.20),

$$\ell(P) \geq \frac{m\delta^n}{n^n}.$$

It remains to show that P is proper. Thus, let

$$x_1 v_1 + \cdots + x_n v_n \equiv x_1' v_1 + \cdots + x_n' v_n \pmod{m}$$

with $-\ell_i \leq x_i, x_i' \leq \ell_i$, hence $|x_i - x_i'| \leq 2\ell_i$, for each $i = 1, \dots, n$. Then, arguing as above (i.e. multiplying by $\mathbf{a}_j$), we obtain, for every $j = 1, \dots, n$

$$\sum_{i=1}^{n} (x_i - x_i') b_{ij} \equiv 0 \pmod{m}. \tag{1.23}$$

On the other hand, since $0 < \delta < 1/2$,

$$\left| \sum_{i=1}^{n} (x_i - x_i') b_{ij} \right| \leq \sum_{i=1}^{n} |x_i - x_i'||b_{ij}| \leq \sum_{i=1}^{n} 2\ell_i \lambda_i \delta \leq 2\delta m < m.$$

Therefore $\sum_{i=1}^{n} (x_i - x_i') b_{ij}$, for every $j = 1, \dots, n$ and, consequently

$$\sum_{i=1}^{n} (x_i - x_i') \mathbf{b}_i = 0.$$

Because of the linear independence of the $\mathbf{b}_i' s$ we conclude that $x_i = x_i'$ for every $i = 1, \dots, n$, which is what oit is needed for P to be proper. This completes the proof of the Lemma. ∎

Exercise 10. Let $m, a_1, \dots, a_n$ as in the statement of Lemma 1.31, and let $u \in \mathbb{Z}$ such that $ua_1 \equiv 1 \pmod{m}$. In $\mathbb{R}^n$ consider the vectors

$$\mathbf{u}_1 = (1, ua_2, \dots, ua_n), \mathbf{u}_2 = (0, m, 0, \dots, 0), \dots, \mathbf{u}_n = (0, 0, 0, \dots, m).$$

Prove that

$$\Lambda = \mathbb{Z}\mathbf{u}_1 \oplus \mathbb{Z}\mathbf{u}_2 \oplus \cdots \oplus \mathbb{Z}\mathbf{u}_n$$

Where Λ is the subgroup defined by (1.19) in the proof of Lemma 1.31. Now you can compute $\det(\Lambda)$ directly by the determinant of the vectors $\mathbf{u}_1, \dots, \mathbf{u}_n$.

1.5. Proof of Freiman's Theorem

In this section, to expedite writing, we use the standard interval notation for the real line as meant to be restricted to $\mathbb{Z}$; thus, for instance $(a, b]$ will be the set of all $z \in \mathbb{Z}$, $a < z \leq b$ (for a $a, b \in \mathbb{R}, a < b$).

LEMMA 1.32 (Ruzsa). *Let A be a finite subset of $\mathbb{Z}$, with $|A| = n$ and $|A+A| = Cn$. Let $2 \leq k \in \mathbb{N}$; then for every $m > C^{2k}n$ there exists $A' \subseteq A$ with $|A'| \geq n/k$ and A' Freiman k-isomorphic to a subset of $\mathbb{Z}_m$.*

PROOF. We begin with an easy observation. For a positive integer p (not necessarily a prime), let $\psi_p : \mathbb{Z}_p \to \mathbb{Z}$ be the map that assigns to every element in $\mathbb{Z}_p$ its unique representative in $[0, p)$, and let $k \geq 2$. This map is injective, but not a homomorphism, and it does not induce a Freiman k-isomorphism on $\mathbb{Z}_p$. However, let $1 \leq i \leq k$ and $L_i = [\frac{i-1}{k}p, \frac{i}{k}p)$; then ψ_p does induce a Freiman k-isomorphism from $U_i = \pi_p(L_i)$ to L_i (here, π_p is the projection modulo p, a left inverse of ψ_p). In fact, let $\bar{x}_1 = x_1 + p\mathbb{Z}, \ldots, \bar{x}_k = x_k + p\mathbb{Z}$, be elements of U_i, then

$$[(i-1)p, ip) \ni \psi_p(\bar{x}_1) + \cdots + \psi_p(\bar{x}_k) \equiv x_1 + \cdots + x_k \pmod{p}.$$

Since $[(i-1)p, ip)$ is a set of representatives modulo p, if $\bar{y}_1, \ldots, \bar{y}_k$ are others elements of U_i, then $\psi_p(\bar{x}_1) + \cdots + \psi_p(\bar{x}_k) = \psi_p(\bar{y}_1) + \cdots + \psi_p(\bar{y}_k)$ if and only if $\bar{x}_1 + \cdots + \bar{x}_k = \bar{y}_1 + \cdots + \bar{y}_k$, and $\psi_p|_{U_i}$ is a Freiman k-isomorphism.

Now for the proof of the Lemma. Fix a prime p such that the reduction mod p, $\pi_p : \mathbb{Z} \to \mathbb{Z}_p$ is injective on kA (for instance, $p > k(\max A - \min A)$); so that (see Example 4) $\pi_p|_A$ is a Freiman k-isomorphism.
For $1 \leq q \leq p-1$ let $\mu_q : \mathbb{Z}_p \to \mathbb{Z}_p$ be the multiplication by q in $\mathbb{Z}_p$; since $(p, q) = 1$, μ_q is a group isomorphism. It follows that the restriction to A of $\mu_q \circ \pi_p$ is again a Freiman k-isomorphism.
Let $\psi_p : \mathbb{Z}_p \to \mathbb{Z}$ be the map defined above. For every $1 \leq i \leq k$, let

$$L_i = \left[\frac{i-1}{k}p, \frac{i}{k}p\right) \quad \text{and} \quad A_i = \{x \in A \mid \mu_q(\pi_p(x)) \in L_i\}.$$

By what observed so far we have that the composition map $\psi_p \circ \mu_q \circ \pi_p$ induces a Freiman k-isomorphism $A_i \to L_i$. By the pigeon-hole principle, there is $1 \leq j \leq k$ such that $|A_j| \geq |A|/k = n/k$; we write $A' = A_j$ (notice that A' depends on q which at the moment is any integer coprime to p).
Let $\pi_m : \mathbb{Z} \to \mathbb{Z}_m$ be the projection modulo m; thus we have the following composition chain

$$\mathbb{Z} \xrightarrow{\pi_p} \mathbb{Z}_p \xrightarrow{\mu_q} \mathbb{Z}_p \xrightarrow{\psi_p} \mathbb{Z} \xrightarrow{\pi_m} \mathbb{Z}_m.$$

The proof will be complete if we show that for some $1 \leq q \leq p-1$, the restriction to A' of the composite map $\psi = \pi_m \circ \psi_p \circ \mu_q \circ \pi_p$ is a Freiman k-isomorphism.

Since π_m is a group homomorphism and the restriction to A' of $\psi_p \circ \mu_q \circ \pi_p$ induces a Freiman k-isomorphism, we have only to prove that, for a proper choice of q,

$$\psi(x_1) + \cdots \psi(x_k) = \psi(y_1) + \cdots + \psi(y_k) \;\Rightarrow\; x_1 + \cdots + x_k = y_1 + \cdots + y_k \tag{1.24}$$

for any $x_1, \ldots, x_k, y_1, \ldots y_k \in A'$ (injectivity of ψ on A' follows easily from this). Let $0 \neq a \in kA - kA$; since then $(a, p) = 1$, multiplying by a in $\mathbb{Z}_p^*$ is a bijection, hence

$$\{\psi_p(qa + \mathbb{Z}_p) \mid 1 \leq q \leq p-1\} = [1, p-1].$$

Now $|[1, p-1] \cap \ker \pi_m| \leq (p-1)/m$, so there are at most $(p-1)/m$ elements $q \in [1, p-1]$ such that

$$\psi_p(qa + \mathbb{Z}_p) \equiv 0 \pmod{m} \tag{1.25}$$

But, by the Plünneke-Ruzsa inequality (Theorem 1.15), $|kA - kA| \leq C^{2k}|A|$. Since

$$C^{2k}|A|\frac{p-1}{m} < p - 1$$

we conclude that there is at least an integer $q \in [1, p-1]$ such that (1.25) fails for every $0 \neq a \in kA - kA$. Picking such q to define ψ, and remembering that the restriction to A' of the map $\psi_p \circ \mu_q \circ \pi_p$ is a Freiman k-isomorphism, it is now an easy task to conclude that (1.24) holds for every $x_1, \ldots, x_k, y_1, \ldots, y_k \in A'$, thus completing the proof that A' is Frieman k-isomorphic to a subset of $\mathbb{Z}_m$. ∎

LEMMA 1.33. *Let A be a finite subset of $\mathbb{Z}$, with $|A| = n$ and $|A + A| = Cn$. Then $2A - 2A$ contains a proper generalized progression Q of dimension $r \leq 2^8 C^{32}$, and size $|Q| \geq f(C)|A|$ ($f(C)$ depends on C only).*

PROOF. Let p be a prime with $C^{16}n \leq p \leq 2C^{16}n$ (it exists by Bertrand Postulate). By Lemma 1.32, with $k = 8$, there exists $A' \subseteq A$ with $|A'| \geq n/8$ and A' Freiman 8-isomorphic to a subset X of $\mathbb{Z}_p$. Observe that

$$\frac{p}{16C^{16}} \leq |A'| = |X| \leq \frac{p}{8C^{16}}.$$

By Lemma 1.25, $2X - 2X$ contains a Bohr neighborhood $B(j_1, \ldots, j_r; 1/4)$ with $r < (16C^{16})^2$. It then follows from Lemma 1.31 that $2X - 2X$ contains a proper r-dimensional generalized progression Q of size $|Q| \geq (1/4r)^r p$. Since X and A' are Freiman 8-isomorphic, we easily have that $2X - 2X$ and $2A' - 2A'$ are Freiman 2-isomorphic, hence (see exercise 3) $2A' - 2A'$ (and $2A - 2A$) contains a proper r-dimensional generalized progression Q' of size $|Q'| \geq (1/4r)^r p \geq (1/4r)^r C^{16} n$. ∎

From Lemma 1.33 to Freiman's Theorem only a last step remains, which just requires an application of Ruzsa covering Lemma.

THEOREM 1.34 (Freiman). *Let $C \geq 2$, and let A be a finite subset of $\mathbb{Z}$ such that $|A + A| < C|A|$. Then A is contained in a generalized progression of dimension $k(C)$ and length $q(C)|A|$, where the numbers $k(C)$ and $q(C)$ depend on C only.*

PROOF. Let Q be a proper generalized progression contained in $2A-2A$, of dimension r_1 bounded by a function of C and length $\ell(Q)=|Q|\geq f(C)|A|$, whose existence is granted by Lemma 1.33. By Plünnecke-Ruzsa inequality (Theorem 1.15)

$$|A+Q|\leq |A+(2A-2A)|\leq C^5|A|\leq C^5 f(C)^{-1}|Q|;$$

hence, by Lemma 1.16 there exists $X\subseteq A$, with $|X|=r_2\leq C^5 f(C)^{-1}$ such that

$$A\subseteq X+(Q-Q). \tag{1.26}$$

Now, $X=\{x_1,\ldots,x_{r_2}\}$ is a finite set, so it is trivially contained in the generalized progression

$$Q_1=\{\alpha_1 x_1+\ldots+\alpha_{r_2}x_{r_2}\mid \alpha_i\in\{0,1\}\},$$

of dimension r_2 and length $\ell(Q_1)=2^{r_2}$. On the other hand $Q-Q$ is a generalized progression of dimension r_1 and length $2^{r_1}|Q|$ (see Exercise 2). Thus,

$$P=Q_1+(Q-Q)$$

is a generalized progression of dimension at most r_1+r_2, which is a number bounded by a function of C only. Because of (1.26) it remains to check that $\ell(P)/|A|$ is also bounded by a function of C. Now, since $|Q|\leq |2A-2A|\leq C^4|A|$, we have

$$\ell(P)\leq \ell(Q_1)\ell(Q-Q)=2^{r_2}2^{r_1}|Q|\leq 2^{r_2}2^{r_1}C^4|A|.$$

This completes the proof of Freiman's Theorem. ∎

REMARK. The actual bounds for $k(C)$ and $q(C)$ that are obtained by tracing back them along the proofs of the various steps we have presented are vary crude. The search for good bounds (more exactly, for good pairs of bounds) by various authors led to the best ones presently known, due to Sanders [**25**]: slightly better than $k(C)=O(K\log^5 K)$ and $q(C)=\exp^{O(K\log^5 K)}$.

The general commutative case. Freiman's Theorem has been extended (by Ruzsa) to arbitrary torsion-free commutative groups (the proof is technically a bit more delicate, but essentially the same we gave for $\mathbb{Z}$).
However, in commutative groups that have torsion (i.e. non-trivial elements of finite order), non-trivial finite subgroups exists and their cosets are small-doubling subsets. Thus, mixing finite subgroups and multi-progression, the following definition reveals to be the right one.

DEFINITION 1.35. Let G be a commutative group. A *coset–progression* Q of dimension r is a subset $Q=H+P$ of G, where H is a finite subgroup of G and P a set of representatives of a multi-progression of dimension r in G/H.

We may now state a result that extends to arbitrary commutative groups Freiman's Theorem (and reduces to it when $G=\mathbb{Z}$).

THEOREM 1.36 (Green and Ruzsa [**12**]). *Let A be a non-empty finite subset of the commutative group G, with $|A+A| \leq c|A|$. Then A is contained in as coset progression of dimension at most $r(c)$ and cardinality at most $|A|\ell(c)$, where $k(c)$ and $\ell(c)$ depend on c only.*

1.6. The non-commutative case: approximate subgroups

Extending, in some way, Freiman's Theorem to the non-commutative case, or also some of the other results we have established along its proof (like e.g. Plünnecke inequalities), or even just putting the right questions, is complicated by many factors. In this section we prove a couple of results at an elementary level about products of few copies of a finite non-empty subset of a group, that we will be useful in later applications. Following that, we will not be able to avoid mentioning a recent generalization of Freiman's Theorem (due to Breuillard, Green and Tao): nothing more that giving its mere statement, plus a few explanations on its meaning, can be done within the scope of these lectures.

In the general setting, it is the concept of *approximate subgroup*, introduced by T.Tao, that has proved to better suited to manipulation, and has the advantage of making sense for infinite subsets as well as finite ones. Before giving the definition, let us agree to saying that a subset U of a (multiplicative) group is *symmetric* if $1 \in U$ and $U^{-1} = U$.

DEFINITION 1.37. Let $1 \leq K \in \mathbb{R}$ be a parameter. A finite symmetric subset A of a group G is called a *K-approximate subgroup* if there exists $X \subseteq G$ with $|X| \leq K$ and $A \cdot A \subseteq X \cdot A$ (that is, A^2 is covered by K left translates of A).

If A is K-approximate subgroup of the group G and $X \subseteq G$ is such that $|X| \leq K$ and $A^2 \subseteq X \cdot A$, then $|A^2| \leq K|A|$ and, by an obvious induction,

$$A^{n+k} \subseteq X^n A^k \qquad \text{and} \qquad |A^{n+1}| \leq K^n |A|.$$

for every $1 \leq n, k \in \mathbb{N}$. In particular, A^n is a K^n-approximate subgroup. Also, we see that a K-approximate subgroup is a slowly growing subset.
For commutative groups the connection between approximate subgroups and small doubling subsets is tight.

PROPOSITION 1.38. *Let A be a finite non-empty subset of the commutative group G and $|A+A| \leq c|A|$ for some real number $c \geq 1$. Then $A-A$ is a c^5-approximate subgroup of G.*

PROOF. Now, $U = A - A$ is a symmetric subset of G, and, by Theorem 1.15,

$$|A + 2U| = |3A - 2A| \leq c^5 |A|.$$

By Ruzsa covering trick (Lemma 1.16) there is a set $X \subseteq 2U$ such that $|X| \leq c^5$ and $2U \subseteq A - A + X = X + U$, showing that U is a c^5-approximate subgroup of G. ∎

This, in general, does not hold in the non-commutative case; for small doubling does not always imply slow growth.

EXAMPLE 7. The standard example is $A = H \cup \{g\}$, where H is a subgroup of the non-commutative group G and $g \in G \setminus H$; then $A^2 = AA = H \cup gH \cup Hg \cup \{g^2\}$, whence $|A^2| \leq 3|A|$, while A^3 contains the double class HgH, whose cardinality may be arbitrary large with respect to the coefficient $\alpha = 3$ (in fact, one easily finds cases in which $|HgH| = |H|^2$). Therefore, neither A nor A^2 may be K-approximate subgroups for any K independent on $|A|$.

However, small tripling works.

LEMMA 1.39. *Let A be a finite non-empty subset of a group G with $|A^3| \leq c|A|$ for some real number $c \geq 1$. Then AA^{-1} is a c^5-approximate subgroup of G.*

PROOF. By Ruzsa triangle inequality (Lemma 1.10),

$$|A||A^{-1}A^{-1}A| \leq |A^{-1}A^{-1}A^{-1}||AA| \leq |A^3||A^3| \leq c^2|A|^2,$$

hence $|A^{-1}A^{-1}A| \leq c^2|A|$. Similarly one proves $|AAA^{-1}| \leq c^2|A|$. Again

$$|A^{-1}||AAA^{-1}A| \leq |AAA||A^{-1}A^{-1}A| \leq c|A|c^2|A| = c^3|A|^2,$$

and so $|AAA^{-1}A| \leq c^3|A|$. One more application of Lemma 1.10 yields

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

Therefore

$$|AA^{-1}AA^{-1} \cdot A| \leq c^5|A|. \tag{1.27}$$

Now the proof proceeds as in Proposition 1.38. Write $U = AA^{-1}$; then (1.27) becomes $|U^2A| \leq c^5|A|$. By Lemma 1.16 there exists $X \subseteq U^2$ such that $|X| \leq c^5$ and

$$U^2 \subseteq XAA^{-1} = XU.$$

Since U is symmetric, it is a c^5-approximate subgroup of G. ∎

Thus, small tripling implies slow growth. This fact may be directly proved by using Ruzsa triangle inequality, in essentially the same way as we did in the proof of Lemma 1.39.

LEMMA 1.40. *Let A be a finite symmetric subset of a group with $|A^3| \leq K|A|$ for $1 \leq K \in \mathbb{R}$; then, for every $n \geq 3$*

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

However, despite example 7, a rather strict connection between small doubling subsets and approximate subgroups exists in arbitrary groups, as shown by the following result.

PROPOSITION 1.41 (Tao [**26**]). *Let A be a finite subset of a group, with $|A^2| \leq c|A|$ for $1 \leq c \in \mathbb{R}$; then A is contained in the union of at most c right–translates of a c^{10}-approximate subgroup Q, with $c^{-1}|A| \leq |Q| \leq c^2|A|$.*

PROOF. Let $\emptyset \neq X \subseteq A$ be minimal such that $|XA|/|X| \leq c$. Then, by Petridis Lemma 1.11 we have

$$|X^3| \leq |XXA| \leq c|XX| \leq c|XA| \leq c^2|X|.$$

Hence, $Q = X^{-1}X$ is a c^{10}-approximate subgroup by Lemma 1.39 (applied to X^{-1}). Now, from $|XA| \leq c|X|$ and Lemma 1.16 turned the other way, there exists a subset $Y \subseteq A$, such that $|Y| \leq c$ and

$$A \subseteq X^{-1}XY = QY,$$

and so A is contained in c right translates of the approximate subgroup Q. Finally, by Ruzsa triangle inequality,

$$|X||X^{-1}X| \leq |X^{-1}X^{-1}||XX| \leq |X^2||XA| \leq c|X||X^2|,$$

whence $c^{-1}|A| \leq |Q| = |X^{-1}X| \leq c|X^2| \leq c|A^2| \leq c^2|A|$. ∎

This allows to establish that small-doubling subsets are *roughly* equivalent to approximate subgroups, where the term 'roughly' may be given a precise technical meaning, which we will not give here (see exercise 30).
In fact, a slightly stronger form of Proposition 1.41, which will need later on, holds.

PROPOSITION 1.42. *Let A be a finite subset of a group G such that*

$$\max\{|AA^{-1}|, |A^{-1}A|\} \leq c|A|$$

for $1 \leq c \in \mathbb{R}$; then A is contained in the union of at most c right–translates of a c^{20}-approximate subgroup Q, with $c^{-1}|A| \leq |Q| \leq c^4|A|$.

PROOF. By Lemma 1.11 we find $X, Y \subseteq A$ such that $|DXA^{-1}| \leq c|DX|$ and $|DY^{-1}A| \leq c|DY^{-1}|$ for every finite $U \subseteq G$. Let $U = XY^{-1}$; then

$$|U^3| = |XY^{-1}XY^{-1}XY^{-1}| \leq c|XY^{-1}XY^{-1}X| \leq c^2|XY^{-1}XY^{-1}| \leq c^4|U|.$$

Hence, $Q = U^{-1}U$ is a c^{20}-approximate subgroup by Lemma 1.39. Now we have $|QA| = |YX^{-1}XY^{-1}A| \leq c|YX^{-1}XY^{-1}| = c|Q|$, and to conclude as in the previous proof we just need to observe that

$$c^{-1}|A| \leq |Q| = |U^{-1}U| \leq c|XY^{-1}XY^{-1}| \leq c^3|XY^{-1}| \leq c^2|AA^{-1}| \leq c^4|A|.$$

∎

EXERCISE 11. Working out the proof of Lemma 1.39 in an inductive argument try to prove a Plünnecke-type inequality for arbitrary groups, as follows: let A be a non-empty finite subset of a group, with $|A^3| \leq c|A|$ for some $1 \leq c \in \mathbb{R}$; then for every $n \geq 3$ and $\epsilon_1, \epsilon_2, \ldots, \epsilon_n \in \{-1, 1\}$,

$$|A^{\epsilon_1} A^{\epsilon_2} \cdots A^{\epsilon_m}| \leq c^{3(n-2)}|A|.$$

EXERCISE 12. (Freiman, Tao) Let X be a non-empty finite subset of a group G, and suppose $|X^{-1}X| < \frac{3}{2}|X|$. Write $U = \{g \in G \mid X \cap gX \neq \emptyset\}$, and prove the following facts.

(1) If $g \in U$ then $|X \cap gX| > \frac{1}{2}|X|$;
(2) $U = XX^{-1}$;
(3) XX^{-1} and $X^{-1}X$ are (conjugate) subgroups of G.

Progressions in arbitrary groups. In the rest of this section we like to introduce (without proofs, needless to say) an impressive result, due to Breuillard, Green and Tao (but the fundamental contribution of Hrushovski should also be acknowledged) providing a rather outstanding extension of Freiman's Theorem to arbitrary groups.

We start by observing that, in a general group G, analogues of progressions in $\mathbb{Z}$ look like

$$A = \{b^t \mid 0 \leq t < n\}$$

for $1 \neq b \in G$ and n a positive integer. In this case $A^2 = \{b^t \mid 0 \leq t < 2n-1\}$, hence, if $|A| = n$ then (as in the commutative case) $|A^2| \leq 2|A| - 1$. Also, $A \cup A^{-1}$ is a 2-approximate subgroup (take $X = \{b^{1-n}, b^{n-1}\}$).
However, if we just add an "initial point", that is, for $a, b \in G \setminus \{1\}$, we consider

$$A = \{ab^t \mid 0 \leq t < n\}$$

we have $A^2 = \{ab^i ab^j \mid 0 \leq i, j < n\}$. Recalling the definition of the commutator: $[x, y] = x^{-1}y^{-1}xy$, (for $x, y \in G$), we write

$$A^2 = \{a^2 b^i [b^i, a] b^j \mid 0 \leq i, j < n\}$$

which may have order as large as n^2.

EXAMPLE 8. In the group $G = GL(2, \mathbb{R})$ let $a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$; then, for every $r, s \in \mathbb{Z}$,

$$ab^r ab^s = \begin{pmatrix} 2^r & 0 \\ 0 & 2^s \end{pmatrix}$$

For a fixed $n \geq 1$, if $A = \{ab^t \mid 0 \leq t < n\}$, then $|A| = n$ and $|A^2| = n^2 = |A|^2$.

Of course, this a fortiori apply to natural analogues of generalized d-dimensional arithmetic progressions; in a non-commutative group G, things like

$$A = \{a^i b^j \mid 0 \le i < n_1, 0 \le j < n_2\} \tag{1.28}$$

for $a, b \in G$, are in general far from having small doubling.

Assume for simplicity that, in (1.28), $|A| = n_1 n_2$ (in the terminology of the commutative case, A is *proper*). Of course, if a and b commute (i.e. $[a, b] = 1$) then $|A^2| < 4n_1 n_2 = 4|A|$. Troubles begin when a and b do not commute; let us then suppose that they are close to be commuting, in the sense that $c = [b, a]$ commutes with both a and b (for those who know about groups, a and b generate a class-2 nilpotent group). Now, an easy fact in basic commutator calculus says that, for every $r, s \in \mathbb{Z}$,

$$[b^r, a^s] = c^{rs} = [a^s, b^r]^{-1}. \tag{1.29}$$

This suggest that, rather than A as in (1.28), we consider an extended kind of progression:

$$P = P(a, b, c \mid n_1, n_2, n_{1,2}) = \{a^r b^s c^t \mid 0 \le r < n_1,\ 0 \le s < n_2,\ 0 \le t < n_{1,2}\}$$

where $c = [b, a]$ commutes with both a and b. Suppose that P is proper and that $n_{1,2} \ge n_1 n_2$; then, by using (1.29) we easily obtain

$$P^2 \subseteq \{a^r b^s c^t \mid 0 \le r < 2n_1 - 1,\ 0 \le s < 2n_2 - 1,\ 0 \le t < n_1 n_2 + 2n_{1,2}\}$$

whence

$$|P^2| < n_1 n_2 + 2n_{1,2} \le 4n_1 n_2 \cdot 3n_{1,2} \le 12|A|.$$

Let us exhibit a tangible example.

Example 9. In the Heisenberg group G of 3×3 upper unitriangular matrices over $\mathbb{Z}$ consider

$$a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},\ b = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ \text{and } c = [b, a] = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then c commutes with a and b (in fact c is in the centre of G). Given positive integers $n_1, n_2 \ge 1$, consider

$$A = \{a^r b^s c^t \mid 0 \le r < n_1,\ 0 \le s < n_2,\ 0 \le t < n_1 n_2\}.$$

Since one easily checks that

$$a^r b^s c^t = \begin{pmatrix} 1 & s & t \\ 0 & 1 & r \\ 0 & 0 & 1 \end{pmatrix}, \tag{1.30}$$

we have $|A| = (n_1 n_2)^2$. Similarly, all elements of A^2 are matrices of type (1.30) with

$$0 \leq r < 2n_1 - 1, \quad 0 \leq s < 2n_2 - 1, \quad 0 \leq t < 2n_1 n_2 - (n_1 + n_2),$$

whence

$$|A^2| \leq 4n_1 n_2 \cdot 2n_1 n_2 = 8|A|.$$

This is the easiest (non-commutative) example of what is called a nil-progression; or, more precisely, of in what it is a *complete* nil-progression; the definition of a generic nil-progression is less strict, but still enough to provide small-growing subsets (and approximate subgroups).

DEFINITION 1.43. 1) Let $g_1, \ldots, g_r$ be elements of a group G, and $t_1, \ldots t_r$ positive integers. The associated *progression of rank* r is the set $P(g_1, \ldots, g_r; t_1, \ldots, t_r)$ of all elements of G that are product of the elements g_i and their inverses, with at most t_i ocurencies of g_i and g_i^{-1}, for every $i = 1, \ldots, r$.
2) A progression $P(g_1, \ldots, g_r; t_1, \ldots, t_r)$ is called a *nil-progression* of step s, if $\langle g_1, \ldots, g_r \rangle$ is a nilpotent group of nilpotency class s.

Recall that the *normalizer* $N_G(H)$ of a subgroup H in a group G is the set of all $g \in G$ such that $H^g = g^{-1}Hg = H$. Clearly, $N_G(H)$ is a subgroup of G containing H as a normal subgroup.

DEFINITION 1.44. A *coset nil-progression* in a group G is a subset $Q = HP$ where H is a finite subgroup of G, $P \subseteq N_G(H)$ and P is a set of representatives for a nil-progression $\{Hx \mid x \in P\}$ in $N_G(H)/H$. Rank and step of a coset nil-progression HP are those of the nil-progression HP/H.

Observe that if Q is a coset nil-progression in a group G then the subgroup $\langle Q \rangle$, generated by Q, has a finite normal subgroup H such that the factor group $\langle Q \rangle / H$ is nilpotent. Form standard group theory it follows that $\langle Q \rangle$ is *virtually nilpotent*.

DEFINITION 1.45. A group G is *virtually nilpotent* if it contains a (normal) nilpotent subgroup of finite index.

We may now state the fundamental result of Breuillard, Green and Tao [**5**], presenting - as authors do - two versions of it. As said, the proofs are beyond the scope of this course. They are based on fundamental work of Hrushovski ([**17**]), combined with Gleason-Yamabe structure theorem for locally compact groups, and much more. As a first approach, the interested reader may look for the expository papers [**6**], [**2**], [**8**] (the last one, by L. van den Dries, is recommended to those interested in the part of the proof using tools from logic), that also include some comments on applications.

THEOREM 1.46 (Br.Gr.T. - weak form). *Let A be a finite non-empty subset of a group G with $|AA| \leq c|A|$ for a parameter $c \geq 1$. Then there exist a finite subset X of G and a virtually nilpotent subgroup $\Gamma \leq G$ such that $|X| \leq \gamma(c)$ and $A \subseteq X\Gamma$.*

THEOREM 1.47 (Br.Gr.T. - strong form). *Let $K \geq 1$ and A a K-approximate subgroup of a group G. Then there exist a finite subset X of G, with $|X| \leq \gamma(K)$, and a coset nil-progression P of G of rank and step bounded by a function of K, such that $A \subseteq XP$ and $|P|/|A|$ is bounded in terms of K only. $|X| \leq \gamma(c)$ and $A \subseteq XS$.*

An application. These are deep (and difficult) Theorems. As an illustration, let us show how the celebrated Gromov's Theorem on groups with polynomial growth may be easily deducted from 1.46.

DEFINITION 1.48. A finitely generated group G is said to have *polynomial growth* if given a finite symmetric set S of generators of G there exist positive constants M and D such that

$$|S^n| \leq Mn^D$$

for every $n \geq 1$. This fact does not depend on the choice of the finite set of generators S (this is easy to prove).

In 1968, J. Wolf proved that a finitely generated (virtually) nilpotent group has polynomial growth. Gromov's Theorem says that the converse is true.

THEOREM 1.49 (M.Gromov, 1981). *Every finitely generated group of polynomial growth is virtually nilpotent.*

PROOF. Let G have polynomial growth, S a finite symmetric set of generators of G, and let M, D be constants such that $|S^n| \leq Mn^D$ for every $n \geq 1$.
We first observe the following:

- *for every $n_0 \in \mathbb{N}$ there exists $n \geq n_0$ such that*

$$|S^{4n}| < 5^D|S^n|. \tag{1.31}$$

In fact, suppose by contradiction, that for some $n_0 \geq 1$ and every $n \geq n_0$, we have $|S^{4n}| \geq 5^D|S^n|$. Then, via a simple induction, for every $t \geq 1$ we obtain

$$M(4^t n_0)^D \geq |S^{4^t n_0}| \geq 5^{tD}|S^{n_0}| \geq 5^{tD}$$

which is false for sufficiently large t.

Now, let $R = \gamma(5^D)$ (γ is the function in the statement of 1.46), and let $n \geq 5^D R$ satisfying (1.31). Write $A = S^n$; then $|A^2| \leq |A^4| < 5^D|A|$; hence by Theorem 1.46 there exist a virtually nilpotent subgroup Γ and a subset X of G such that $|X| \leq R$ and $A \subseteq X\Gamma$. Observe that we may then take $X \subseteq A$.

Let $a \in X \subseteq A$ such that $|a\Gamma \cap A|$ is maximum. Then

$$|A| = \Big| \bigcup_{x \in X} (x\Gamma \cap A) \Big| \leq |X||a\Gamma \cap A| \leq R|a\Gamma \cap A|.$$

Hence

$$|A^2 \cap \Gamma| \geq |A \cap a\Gamma| \geq \frac{|A|}{R} > \frac{|A^4|}{5^d R} \geq \frac{|A^4|}{n}. \tag{1.32}$$

where the first inequality we have by multiplying on the left by a^{-1}.
Suppose that $|G : \Gamma| = \infty$. Then, since $G = \langle S \rangle$, there exist at least $2n$ elements $g_1, \ldots, g_{2n} \in S^{2n} = A^2$ such that $g_i\Gamma = g_j\Gamma \ \Rightarrow \ i = j$. Thus, from (1.32),

$$|A^4| \geq \Big| \bigcup_{i=1}^{2n} (A^2 \cap g_i\Gamma)(A^2 \cap \Gamma) \Big| \geq 2n|A^2 \cap \Gamma| \geq 2|A^4|,$$

a contradiction. Therefore, $|G : \Gamma|$ is finite and so, being Γ virtually nilpotent, G is virtually nilpotent. ∎

Note. The material of the first five sections of this chapter is by now classic and may be learnt from several sources, in surveys and notes by various authors. In particular I have taken a lot from Ruzsa [**24**] and Green [**11**] lecture notes, which are both available on web (the second at the author's website), and contain a wealth of interesting additional material. The book of Nathanson [**19**] includes a very detailed proof of Freiman's Theorem, as well as that by Tao and Vu [**28**], which is of course more up-to-date, somehow more demanding to read, but an indispensable reference for the scholar. For a continuous source of interesting facts about the subject of this, as well as of the others, chapter, T. Tao weblog (https://terrytao.wordpress.com) is a compelling reference.

In section 1.6, I just meant to take a peep at recent important achievements. The reader interested in seeing more may begin from a number of valuable expository papers like Breuillard, Green and Tao [**6**] or Breuillard [**3**] (available at author's websiite). For an account (after Hrushovski) of the model theoretic methods involved in the proofs see van den Driess [**8**].