LECTURES ON APPROXIMATE GROUPS

EMMANUEL BREUILLARD

Abstract. These notes are based on a series of lectures given at Clermont-Ferrand in June 2010 and at IHP (Paris) in February-March 2011. They give an introduction to the theory of approximate groups.

Contents

Part 1. Tools from combinatorics

In this first chapter, we introduce the basic combinatorial machinery that will be used in later chapters and give the general properties that hold for all approximate groups.

1. Approximate groups: introduction and definition

The notion of an approximate subgroup of an ambient group was defined by T. Tao in [29] as follows:

Definition 1.1. *Let $K \geqslant 1$. A finite subset A of an ambient group G is said to be a K-approximate subgroup of G if the following conditions hold*

Date: March 14th 2011.

- *A contains* id *and is symmetric (i.e. $A^{-1} = A$), and*
- *there exists a subset X in G such that $AA \subset AX$ and $|X| \leqslant K$.*

Here AA denotes the product set $AA = \{xy | x, y \in A\}$ and $|X|$ the cardinality of the subset X. Note that $AA \subset AX$ is equivalent to $AA \subset X^{-1}A$ since A is assumed symmetric. By a slight abuse of language, we talk about an "approximate group", when we really mean a K-approximate subgroup of some ambient group.

This definition suggests that approximate groups are finite subsets of G that are *almost* closed under multiplication. As the reader will easily check, when $K = 1$ we recover subgroups, i.e. 1-approximate subgroups are the same thing as finite subgroups of G. So approximate groups can be thought of as a way to quantify how close a finite subset of a group is to be a genuine subgroup. Here K is thought of as a fixed parameter and A is a potentially huge subset of G.

Note that we always assume that approximate groups are subsets of an ambient group.[1]

Example. [arithmetic progressions] The archetypal example of an approximate group that is far from being a subgroup is the interval $A = [-N, N] = \{x \in \mathbb{Z}, -N \leqslant x \leqslant N\}$ in the ambient group $\mathbb{Z}$. Clearly $AA = [-2N, 2N] = XA$, where $X = \{-N, N\}$. Hence A is a 2-approximate subgroup of the ambient group $G = \mathbb{Z}$. ◇

Example. [generalized (or multidimensional) arithmetic progressions]. The previous example can be extended to higher dimensions. For example the box $B = \prod_{i=1}^{d}[-L_i, L_i]$ in $\mathbb{Z}^d$ with $L_i \in \mathbb{N}$ satisfies $BB \subset \prod_{i=1}^{d}[2L_i, 2L_i]$, thus $BB \subset XB$, where X is the subset of the 2^d vectors with coordinates $\pm L_i$. So B is a 2^d-approximate subgroup of $\mathbb{Z}^d$. Note moreover that if π is any group homomorphism $\mathbb{Z}^d \to \mathbb{Z}$, then $\pi(B)$ is a 2^d-approximate subgroup of $\mathbb{Z}$. Those are called (symmetric) "generalized arithmetic progressions". ◇

Exercise 1.2. *Let H be a finite group and $A := H \backslash Y$, where Y is a symmetric subset of H of size $|Y| \leqslant \sqrt{|H|}$ and not containing* id. *Show that A is a 2-approximate subgroup of H.*

Hint: find $x \in H$ such that $Y \cap xY = \varnothing$.

Exercise 1.3. *Let H be a finite group of cardinal N. Let A be a random symmetric subset of H containing* id. *(a) Show that $AA = H$ with overwhelming probability as $N \to \infty$. (b) Show that for every fixed $K \geqslant 1$, although A constitutes a positive proportion of H with overwhelming probability as $N \to \infty$ (in fact typically half of H), the probability that A is a K-approximate subgroup of H decays to zero exponentially fast as $N \to \infty$.*

Hint: (a) given $x \in H$, estimate the probability that $A \cap Ax = \varnothing$. (b) given $X \subset H$ of size K, estimate the probability that $H \subset AX$ using the fact that for disjoint sets Y_i in H the events "A hits Y_i" are independent.

We will sometimes need the concept of a Freiman homomorphism between finite subsets of various groups. This notion is a weakening of the notion of group homomorphism that is particularly well suited to approximate groups.

[1] It is possible to define a "local" version of the notion of approximate group. Namely we could drop the requirement that A lies inside an ambient group, and ask instead to be given the multiplication table of the first few power sets of A without reference to any preexistent group. Most of the basic yoga extends without difficulty to this local setting.

Definition 1.4 (Freiman homomorphism)**.** *Let $k \geqslant 1$. A Freiman k-homomorphism is a map $\phi : A \to B$ between a finite subset A of an ambient group G and another such set B in an another ambient group H, such that for all $m \leqslant 2k$,*

$$\phi(x_1)^{\varepsilon_1} \cdot ... \cdot \phi(x_m)^{\varepsilon_m} = 1 \tag{1.4.1}$$

whenever $x_1^{\varepsilon_1} \cdot ... \cdot x_m^{\varepsilon_m} = 1$ for every $x_1, ..., x_m \in A$ and every choice of $\varepsilon_1, ..., \varepsilon_m \in \{\pm 1\}$.

Moreover we say that ϕ is a Freiman k-isomorphism if ϕ is one-to-one and $\phi^{-1} : \phi^{-1}(A) \to A$ is a Freiman k-homomorphism. This is equivalent to the requirements that (1.4.1) *holds if and only if $x_1^{\varepsilon_1} \cdot ... \cdot x_m^{\varepsilon_m} = 1$.*

We warn the reader that our terminology for a Freiman isomorphism differs slightly from that of other authors in the commutative context (e.g. [31]). The difference is minor, but Definition 1.4 seems to be better suited to the non-commutative context (see Exercise 1.7 below).

Observe that a Freiman 1-homomorphism is nothing else but a map satisfying $\phi(1) = 1$ and $\phi(a^{-1}) = \phi(a)^{-1}$ whenever $1, a, a^{-1} \in A$. Moreover a group homomorphism (resp. injective group homomorphism) is a Freiman k-homomorphism (resp. k-isomorphism) for every $k \geqslant 2$.

Observe further that if ϕ is a Freiman k-homomorphism defined on A, then ϕ extends to a map defined on $(A \cup A^{-1} \cup \{1\})^k$ by setting $\phi(1) = 1$ and $\phi(a_1^{\varepsilon_1} ... a_k^{\varepsilon_k}) = \phi(a_1)^{\varepsilon_1} ... \phi(a_k)^{\varepsilon_k}$ for $a_1, ..., a_k \in A$. This extension satisfies $\phi(uv) = \phi(u)\phi(v)$ for all $u, v \in (A \cup A^{-1} \cup \{1\})^{[\frac{k}{2}]}$.

Conversely, any map ϕ defined on $(A \cup A^{-1} \cup \{1\})^{2k}$ taking values in a group H and satisfying $\phi(1) = 1$ (resp. $\phi(x) = 1$ iff $x = 1$ for all $x \in (A \cup A^{-1} \cup \{1\})^{2k}$) and $\phi(uv) = \phi(u)\phi(v)$ for all $u, v \in (A \cup A^{-1} \cup \{1\})^k$ induces on A a Freiman k-homomorphism (resp. k-isomorphism).

We also have:

Proposition 1.5 (Invariance under Freiman homomorphism)**.** *If A is a K-approximate group and ϕ a Freiman 2-homomorphism, then $\phi(A)$ is a K-approximate group too. Similarly, if A is a (symmetric) generalized arithmetic progression of dimension d, then so is $\phi(A)$.*

Proof. Note that $\phi(1) = 1$, $\phi(a^{-1}) = \phi(a)^{-1}$ and $\phi(ab) = \phi(a)\phi(b)$ for every $a, b \in A$. The first assertion follows immediately. For the second, let $A = \pi(B) = \prod_1^d x_i^{[-L_i, L_i]}$ for commuting x_i's, and check by induction on n that $\phi(x_i^{n_i}) = \phi(x_i)^{n_i}$ for all n_i with $|n_i| \leqslant L_i$, and by induction on $j \leqslant d$ that $\phi(x_1^{n_1} ... x_j^{n_j}) = \phi(x_1)^{n_1} ... \phi(x_j)^{n_j}$ and that the $\phi(x_i)$ commute as well. □

Exercise 1.6. *Verify the claims after Definition1.4. Show that a map ϕ from a finite subset A of a group G into another group H extends to a homomorphism defined on the subgroup $\langle A \rangle$ generated by A if and only if ϕ is a Freiman k-homomorphism for every k. Suppose now that $\langle A \rangle \leqslant G$ is finitely presented as an abstract group. Show that there is some finite k such that any Freiman k-homomorphism from A to another group H extends to a group homomorphism defined on $\langle A \rangle$.*

Exercise 1.7. *In the additive combinatorics literature, a Freiman k-homomorphism is a map from a finite subset A of an abelian ambient group G to another abelian group H such that $\phi(x_1) + ... + \phi(x_k) = \phi(y_1) + ... + \phi(y_k)$ whenever $x_1 + ... + x_k =$*

$y_1 + ... + y_k$. Let $k \geqslant 2$. Show that every Freiman k-homomorphism in the sense of Definition 1.4 is a Freiman k-homomorphism in that sense. Conversely, show that every Freiman $2k$-homomorphism in that sense induces on $A - A$ a Freiman k-homomorphism in the sense of Definition 1.4 by setting $\phi(a-b) = \phi(a) - \phi(b)$.

2. Small doubling and small tripling

Approximate groups were introduced by Tao in order to understand a larger class of subsets, namely subsets A of an ambient group that have small doubling, or small tripling.

Definition 2.1 (small doubling/tripling)**.** *Let $K \geqslant 1$. We say that a finite subset A in G has doubling (resp. tripling) at most K, if $|AA| \leqslant K|A|$ (resp. $|AAA| \leqslant K|A|$).*

It is clear from the definitions that if A is a K-approximate group, then $\forall n \geqslant 1, |A^n| \leqslant K^{n-1}|A|$, thus A has doubling at most K and tripling at most K^2. The following is a converse to that statement and is one of the main justifications for the introduction of approximate groups.

Proposition 2.2 (small tripling implies approximate group)**.** *There is an (explicit) absolute constant C such that the following holds. Let A be a finite subset of an ambient group G. If A has tripling at most K, then $(A \cup A^{-1} \cup \{1\})^2$ is a CK^C-approximate group of size $\leqslant CK^C|A|$. More precisely:*

(i) *if A has tripling at most K, then $|A^n| \leqslant K^{2n-5}|A|$ for all $n \geqslant 3$.*
(ii) *if A has tripling at most K, then $B := A \cup A^{-1} \cup \{\mathrm{id}\}$ satisfies $|B^3| \leqslant 14K^3|A|$.*
(iii) *if $A = A^{-1}$ and $|A^5| \leqslant K|A|$, then A^2 is a K-approximate group.*

In other words, small tripling implies small "n-pling" and symmetrizing and taking the square of the subset and is enough to "smooth out" the subset A into an approximate group[2]. We postpone the proof to the next paragraph, where the necessary material will be introduced.

Remark. Note that we assume small tripling and not small doubling in this proposition. In general small doubling alone does not imply small tripling as the following example shows.

Example. Let $A := \{x\} \cup H$ where H is a finite subgroup of G and $x \in G$ is such that $H \cap xHx^{-1} = \{1\}$. Then clearly $A^2 = \{x^2\} \cup Hx \cup xH \cup H$, thus $|A^2| \leqslant 3|H| + 1 = 3|A| - 2 \leqslant 3|A|$ and A has doubling at most 3. On the other hand A^3 contains HxH and $|HxH| = |H|^2$, so $|A^3|$ is larger than any given multiple of $|A|$ as soon as $|H|$ is large enough.

This example is quite typical of the general case, and Tao proved in [29] that if A has small doubling but not small tripling then one of the "double cosets" AaA for some $a \in A$ must be significantly larger than A, see exercise **??**. $\diamond$

However, when G is abelian, it is true that small doubling implies small tripling. In fact, one has the Plunnecke-Ruzsa sumset estimates:

[2] If A has small tripling, it may not itself be an approximate group (see Exercise 1.3 for an example), although its symmetrized square is.

Proposition 2.3 (Plunnecke-Ruzsa sumset estimates)**.** *Suppose G is an abelian ambient group and A a finite subset such that $|AA| \leqslant K|A|$. Then for every $m, n \in \mathbb{N}$ one has $|A^nA^{-m}| \leqslant K^{m+n}|A|$. Moreover $H := AA^{-1}$ is a K^5-approximate group of size $\leqslant K^2|A|$.*

The original proof of the Plunnecke-Ruzsa estimates relied on a beautiful but rather intricate graph theoretical construction (see [31] or [16]). Compared to the simple proof of Proposition 2.2 we are about to give in the next section, the proof Proposition 2.3 required much more sophisticated tools. However, T. Tao later found a simple combinatorial proof with a slightly worse constant (K^{m+n} being replaced by $K^{6(m+n)}$, see [31]), which would be by far enough for our purposes. But this is not the end of the story, very recently and very unexpectedly G. Petridis, a graduate student of T. Gowers, found a very short proof of these estimates ([**?**]). We will give Petridis' argument in the next section, after we introduce the Ruzsa distance.

Assuming only small doubling, one can still say something about A even in the non-commutative case, and Petridis new argument allows to give a simple proof of the following.

Proposition 2.4 (Small doubling)**.** *There is an (explicit) absolute constant $C > 0$ such that the following holds. Suppose A is a finite subset of an ambient group G such that $|AA| \leqslant K|A|$. Then, there exists a subset A_0 of A with the following properties*

(i) *$|A_0| \geqslant |A|/K$ and $|A_0^3| \leqslant K^3|A_0|$.*

(ii) *$H = (A_0 \cup A_0^{-1} \cup \{1\})^2$ is a CK^C-approximate subgroup such that $A \subset XH \cap HY$, where X, Y are subsets of size at most K^2 and $|H| \leqslant CK^C|A_0|$.*

In Section 4, we will also establish the following similar result:

Proposition 2.5 (Control by an approximate group)**.** *Assume that A and B are two subsets of an ambient group such that $|AB| \leqslant K \min\{|A|, |B|\}$. Then there is a CK^C-approximate subgroup H of G, with size $\leqslant CK^C \min\{|A|, |B|\}$, such that $H \subset (A^{-1}A)^2 \cap (BB^{-1})^2$ for which $A \subset XH$ and $B \subset HY$ for some subsets X and Y of size at most CK^C.*

There is a wide literature on sets with small doubling in various groups, in $\mathbb{Z}$ in particular, where the celebrated Freiman theorem (see Part 2 below) provides the rough classification of sets of small doubling in $\mathbb{Z}$: any such set is very close (in some precise sense) to a generalized arithmetic progression.

The constant K here can take real values between 1 and infinity. The following simple lemma characterizes what happens when $K = 1$.

Proposition 2.6 (K=1)**.** *Suppose A is a finite subset of a group G. The following are equivalent:*

(*i*) *$|AA| \leqslant |A|$.*

(*ii*) *$A = xH$, where H is a finite subgroup of G and x normalizes H.*

Proof. Clearly (ii) implies (i), so we focus on (i) implies (ii). Given $a \in A$, the subset aA is contained in AA and both sets have the same size, so $aA = AA$. It follows that $aA = a'A$ for every $a, a' \in A$. In particular $A^{-1}A \subset AA^{-1}$. Similarly $AA^{-1} \subset A^{-1}A$ and so $A^{-1}A = AA^{-1}$. Set $H = A^{-1}A$. Since $aA = a'A$ for every $a, a' \in A$, we see that $HA \subset A$. It follows that $H^2A \subset A$, i.e. $H^2 \subset AA^{-1} = H$.

Hence H is a finite subset closed under multiplication: it must be a subgroup of G. Moreover $Ha = A$ for every $a \in A$, because $|H| = |Ha| \geqslant |A|$ and $Ha \subset A$. Similarly $aH = A$ for every $a \in A$. Hence $aH = Ha$ for every $a \in A$. □

When K is close to 1, the requirement that a subset A has doubling at most K is very strong and one can then deduce the following complete characterization of such sets, a result due to Freiman [13].

Proposition 2.7 ($K < \frac{3}{2}$)**.** *Suppose A is a finite subset of a group G. Let K be a positive number with $K < \frac{3}{2}$. The following are equivalent:*

(i) $|AA| \leqslant K|A|$.

(ii) There is a finite subgroup H in G such that $|A| \geqslant \frac{1}{K}|H|$ and $A \subset aH$ for some $a \in N_G(H)$, the normalizer of H in G.

If these conditions are satisfied, then one can take $H = A^{-1}A = AA^{-1}$, and H is normalized by every element of A.

Note that $\frac{3}{2}$ is sharp: if $A = \{0, 1\} \subset \mathbb{Z}$, then $|AA| = \frac{3}{2}|A|$ and yet A is not contained in a coset of a finite subgroup of $G = \mathbb{Z}$.

Proof. First observe that the second item implies the first: if $A \subset aH$, with $a \in N_G(H)$, then $AA \subset a^2H$, hence $|AA| \leqslant |H| \leqslant K|A|$. So from now on we focus on the other implication.

Recall that if a finite subset H of a group G is stable under multiplication, i.e. $HH \subset H$, then H is a subgroup of G. Let $H = AA^{-1}$. First let us check that $H = A^{-1}A$. Observe that for every $a, b \in A$, $aA \cap bA \neq \varnothing$; indeed $|aA \cap bA| = 2|A| - |aA \cup bA| \geqslant 2|A| - |AA| > \frac{1}{2}|A| > 0$. This means that there are $a', b' \in A$ such that $aa' = bb'$, i.e. $a^{-1}b = a'b'^{-1}$. In particular $A^{-1}A \subset AA^{-1}$. Reversing the roles of A and A^{-1}, we obtain $H = AA^{-1} = A^{-1}A$.

Now let us show that $HH \subset H$. The argument above shows that for all $a, b \in A$, $|b^{-1}aA \cap A| = |aA \cap bA| > \frac{1}{2}|A|$. In particular, there are strictly more that $|A|/2$ couples (c, d) with $c, d \in A$ such that $b^{-1}ac = d$, i.e. $b^{-1}a = dc^{-1}$. So for every $x \in H = A^{-1}A$, there are strictly more that $|A|/2$ representations of x as $x = dc^{-1}$, with $c, d \in A$. Consequently, given two elements $x, y \in H$, there must a representation $x = dc^{-1}$ and a representation of $y = ef^{-1}$ with $e = c$. Then $xy = df^{-1} \in AA^{-1} = H$.

So we have shown that H is a subgroup. Moreover, since $H = A^{-1}A$, we have $A \subset aH$ for every $a \in A$. Hence $H = AA^{-1} \subset aHa^{-1}$, and thus A normalizes H.

On the other hand $|H| < 2|A|$, because, as we have shown, all fibers of the map $A \times A \to H$, $(a, b) \mapsto a^{-1}b$ have size $> |A|/2$.

Let us write $A = aB$ for some subset $B \subset H$. We have $|B| > \frac{1}{2}|H|$. It follows that $a^{-1}BaB = H$, because hB^{-1} must intersect $a^{-1}Ba$ for every $h \in H$. However by assumption $|AA| = |a^{-1}BaB| \leqslant K|A|$. So $|H| \leqslant K|A|$, and we are done. □

Exercise 2.8. *In the situation of Proposition 2.7 prove that A^2 is a coset of a subgroup.*

Exercise 2.9. *Show that if $K < \frac{3}{2}$, then $|AB| \leqslant K \min\{|A|, |B|\}$ if and only if A lies in some left coset and B in some right coset of a finite subgroup H of size $\leqslant K \min\{|A|, |B|\}$.*

If the doubling constant K gets larger than $\frac{3}{2}$, no such complete characterization is available. However if $K < 2$ we will show in Section **??** that doubling at most K

forces A to be contained in the union $O_K(1)$ cosets of some finite subgroup of G. This follows from the well-known Kneser theorem when G is abelian (see [31]) and was recently generalized to non-commutative groups by Y. Hamidoune and by T. Sanders (see also Tao's blog, where a short proof of this is given for $K < \frac{1+\sqrt{5}}{2}$).

When K is larger than 2, no such strong results are available, but it is possible nonetheless to identify some structure. This will be the main topic of the last section of these notes.

3. Ruzsa calculus

In this paragraph, we prove the results about product sets stated in the last section and present the standard tool-kit of approximate groups. We will sometimes refer to this material as *Ruzsa calculus.* It is essentially due to Ruzsa, who first pioneered these ideas in the abelian setting, and to Tao who worked out these results in the non-commutative setting in [29].

The following two lemmas are the basic combinatorial tools that will be used all over the place: the Ruzsa triangle inequality, and the Ruzsa covering lemma. Let G be an ambient group and A, B, C three finite subsets in G. We set

$$d(A,B) = \log \frac{|AB^{-1}|}{\sqrt{|A||B|}}. \tag{3.0.1}$$

Note that $d(A,B) \geqslant 0$ always because $|AB^{-1}| \geqslant max\{|A|,|B|\} \geqslant \sqrt{|A||B|}$. Moreover $d(xA,yB) = d(Ax,Bx) = d(A,B)$ for all $x, y \in G$. The main reason for introducing this quantity is the

Lemma 3.1 (Ruzsa triangle inequality)**.** *Let A, B, C be finite subsets of G. We have $d(A,B) \leqslant d(A,C) + d(C,B)$. Moreover $d(A,B) = 0$ if and only if A and B are left cosets of a common finite subgroup H of G.*

Proof. For each $x \in AB^{-1}$ pick a couple $(a_x, b_x) \in A \times B$ such that $x = a_x b_x^{-1}$. Consider the map $AB^{-1} \times C \to AC^{-1} \times CB^{-1}$ sending $(x,c) \mapsto (a_x c^{-1}, cb_x)$. Then this map is clearly injective, thus $|AB^{-1}||C| \leqslant |AC^{-1}||CB^{-1}|$, which is equivalent to the desired triangle inequality.

If $d(A,B) = 0$, then $|A| = |B| = |AB^{-1}|$. Note that up to translating A and B on the left, we may assume that both contain the identity, so $A \subset AB^{-1}$ and $B^{-1} \subset AB^{-1}$. It follows that $A = AB^{-1} = B^{-1}$. And hence $AA = A$, so A is stable under multiplication. It must be a subgroup of G. We are done. □

Note that $d(A, A^{-1}) = 0$ if and only if $|AA| = |A|$, so this lemma gives another proof of Proposition 2.6 above.

The next key ingredient is the following simple observation:

Lemma 3.2 (Ruzsa covering lemma)**.** *Let A, B be finite subsets of G. Suppose $|AB| \leqslant K|A|$, then there is a subset $X \subset B$ with $|X| \leqslant K$ and $B \subset A^{-1}AX$.*

Proof. Let $X := \{b_1, ..., b_n\}$ be elements in B such that the Ab_i's form a maximal family of pairwise disjoint subsets of AB^{-1}. The bound $|AB| \leqslant K|A|$ forces $|X| \leqslant K$. But for every $b \in B$, Ab must intersect one of the Ab_i's, i.e. $b \in A^{-1}Ab_i$. We are done. □

We are now ready to prove Proposition 2.2 above.

Proof of Proposition 2.2 By Ruzsa's triangle inequality, we may write

$$d(A^n, A^{-2}) \leqslant d(A^{n-1}, A^{-1}) + d(A^{-1}, A) + d(A, A^{-2}).$$

This translates into the following inequality: $|A^{n+1}| \leqslant |A^n| \frac{|A^2|}{|A|} \frac{|A^3|}{|A|}$ for $n \geqslant 1$. Thus $|A^{n+1}| \leqslant K^2 |A^n|$. Iterating we obtain $|A^n| \leqslant K^{2n-5}|A|$ for all $n \geqslant 3$.

Let $B = A \cup A^{-1} \cup \text{id}$. The product set B^3 is a union of 14 subsets of the form $A^{\varepsilon_1} A^{\varepsilon_2} A^{\varepsilon_3}$, $\varepsilon_i \in \{0, \pm 1\}$. One needs to estimate $|AA^{-2}|$, $|A^{-1}A^2|$ and $|AA^{-1}A|$. The first two are at most $K^2|A|$ as can be seen by applying Ruzsa's triangle inequality in this way: $d(A, A^2) \leqslant d(A, A^{-1}) + d(A^{-1}, A^2)$ and then swapping A with A^{-1}. The last one, i.e. $|AA^{-1}A|$ is at most $K^3|A|$; this follows again from Ruzsa's inequality $d(A, A^{-1}A) \leqslant d(A, A^{-1}) + d(A^{-1}, A^{-1}A)$ using the estimate on $A^{-2}A$ just obtained to bound $d(A^{-1}, A^{-1}A)$. We then obtain $|B^3| \leqslant 2K(3 + 3K + K^2)|A| \leqslant 14K^3|A|$.

If $A = A^{-1}$, and $|A^5| \leqslant K|A|$, then Ruzsa's covering lemma implies that $(A^2)^2 \subset XA^2$, for some X of size at most K. Hence A^2 is a K-approximate group. □

In order to prove the Plunnecke-Ruzsa estimates (Proposition 2.3) and the structure result for sets of small doubling (Proposition 2.4) we first need to formulate Petridis' lemma.

Lemma 3.3 (Petridis lemma, [23]). *Let A, B be a finite subsets of an ambient group G such that $|BA| \leqslant K|A|$. Then there exists a subset $A_0 \subset A$ such that for every finite subset X in G, one has $|BA_0X| \leqslant K|A_0X|$.*

Proof. Let ϕ be the map from finite subsets of G to finite subsets of G defined by $\phi(X) = BX$. Choose a subset A_0 in A such that $|\phi(A_0)|/|A_0|$ is minimal and let K_0 be this minimal ratio. By the assumption on the doubling of A, we have $K_0 \leqslant K$. Also note that ϕ preserves inclusion: i.e. $A \subset A'$ implies $\phi(A) \subset \phi(A')$.

The proof proceeds by induction on $|X|$. Clearly the claim holds if $|X| = 1$. So, suppose it holds for X and let $X' = X \cup \{x\}$. Then $\phi(A_0X') = \phi(A_0X) \cup \phi(A_0x)$, so $|\phi(A_0X')| + |\phi(A_0X) \cap \phi(A_0x)| = |\phi(A_0X)| + |\phi(A_0x)|$. But $\phi(A_0X \cap A_0x) \subset \phi(A_0X) \cap \phi(A_0x)$, so

$$|\phi(A_0X')| + |\phi(A_0X \cap A_0x)| \leqslant |\phi(A_0X)| + |\phi(A_0x)|.$$

On the other hand, we may write $A_0X \cap A_0x = Sx$ for some subset $S \subset A_0$, and by minimality of A_0, we have $|\phi(Sx)| = |\phi(S)| \geqslant K_0|S| = K_0|Sx|$. In particular,

$$|\phi(A_0X')| + K_0|A_0X \cap A_0x| \leqslant |\phi(A_0X)| + |\phi(A_0x)| \leqslant K_0|A_0X| + K_0|A_0|,$$

hence

$$|\phi(A_0X')| \leqslant K_0|A_0X'|$$

as desired. □

We are now ready to prove the Plunnecke-Ruzsa estimates.

Proof of Proposition 2.3. We take $X = A^{n-1}$ in Petridis lemma, and using the assumption that G is abelian, we get $|A_0A^n| \leqslant K_0|A_0A^{n-1}| \leqslant ... \leqslant K_0^n|A_0|$. In particular $|A^n| \leqslant K^n|A|$. Moreover, by the Ruzsa triangle inequality, $d(A^n, A^m) \leqslant d(A^n, A_0^{-1}) + d(A_0^{-1}, A^m)$, so $|A_0||A^nA^{-m}| \leqslant |A^nA_0||A^mA_0| \leqslant K_0^{n+m}|A_0|^2$, and in particular $|A^nA^{-m}| \leqslant K^{n+m}|A|$ as desired.

Letting $H = A^{-1}A$, we have $|AH^2| = |A^3A^{-2}| \leqslant K^5|A|$ by the above. Hence by Ruzsa covering, $H^2 \subset XH$ for some subset X of size at most K^5. Hence H is a K^5-approximate group. □

Petridis lemma also gives a quick proof of Proposition 2.4.

Proof of Proposition 2.4. From Petridis lemma we have $|AA_0| \leqslant K|A_0|$, so in particular $|A_0| \leqslant |A|/K$, and also $|AA_0X| \leqslant K|A_0X|$ for every X, hence setting $X = A_0$ we obtain $|A_0^3| \leqslant K|A_0^2| \leqslant K^2|A| \leqslant K^3|A_0|$.

By Proposition 2.2 applied to A_0, we see that $H = (A_0 \cup A_0^{-1} \cup \{1\})^2$ is a CK^C-approximate subgroup of size $\leqslant CK^C|A_0|$. By Ruzsa covering, since $|AA_0| \leqslant K|A_0|$ we get $A \subset XA_0A_0^{-1} \subset XH$ for some set X of size $\leqslant K$.

On the other hand $|A_0A| \leqslant K|A| \leqslant K^2|A_0|$. Hence by Ruzsa covering $A \subset A_0^{-1}A_0Y \subset HY$ for some Y of size $\leqslant K^2$. We are done. □

Exercise 3.4. *Let $K \geqslant 2$ and assume A, B are two finite subsets of an abelian group G such that and $|A + B| \leqslant K\sqrt{|A||B|}$. Show that $|n_1A - n_2A + n_3B - n_4B| \leqslant K^{O_{n_1,\dots,n_4}(1)}\sqrt{|A||B|}$ for any $n_1, ..., n_4 \in \mathbb{N}$.*

With these basic tools in hand, we can now understand what happens to an approximate group when it is intersected with a subgroup, or when it is mapped into another ambient group by a homomorphism, or when it acts on a set via a group action.

Proposition 3.5 (inheritance to subgroups and quotients)**.** *Let A be a K-approximate subgroup of G.*

(i) *if H is a subgroup of G, then $A^2 \cap H$ is a K^3-approximate subgroup of G. Moreover*
$$\forall k \geqslant 1, |A^k \cap H| \leqslant K^{k-1}|A^2 \cap H|.$$
(ii) *if B is an L-approximate group, then $A^2 \cap B^2$ is a $(KL)^3$-approximate group, in fact*
$$\forall k, l \geqslant 1, |A^k \cap B^l| \leqslant K^{k-1}L^{l-1}|A^2 \cap B^2|.$$
(iii) *if π is a group homomorphism $G \to Q$, then $\pi(A)$ is a K-approximate subgroup of Q.*

Proof. The proofs are simple applications of the definitions and the Ruzsa covering lemma. Item (iii) is obvious (see also Proposition 1.5). Let us prove (i). We have $A^k \subset X^{k-1}A$. But every set of the form $(xA) \cap H$ is contained in $y(A^2 \cap H)$ for some $y \in xA \cap H$. So $A^k \cap H \subset Y(A^2 \cap H)$ for some set Y of size at most K^{k-1}. In particular $A^2 \cap H$ is a K^3-approximate group.

We now prove (ii). $A^k \cap B^l$ is contained in at most $K^{k-1}L^{l-1}$ "cosets" of the form $xA \cap yB$. Each of them is contained in a "coset" of $A^2 \cap B^2$. In particular $(A^2 \cap B^2)^2 \subset A^4 \cap B^4$ is contained in at most $(KL)^3$ cosets of $A^2 \cap B^2$, i.e. $A^2 \cap B^2$ is a $(KL)^3$-approximate group. □

Proposition 3.6 (Behavior w.r.t group actions)**.** *Let G act on a set Ω and A a K-approximate subgroup of G.*

(i) *(size of an orbit) If $x \in \Omega$, and H_x is the stabilizer of x, then*

$$\forall k \geqslant 1, |A| \leqslant |A \cdot x||A^2 \cap H_x| \leqslant K^2|A|.$$

Moreover if $y \in A \cdot x$, then $\frac{1}{K} \leqslant \frac{|A \cdot y|}{|A \cdot x|} \leqslant K$.

(ii) *(partition into orbits) Let Y be a maximal subset of Ω such that all $A \cdot y$'s, $y \in Y$ are disjoint. Then Ω is covered by the $A^2 \cdot y$ for $y \in Y$ and the multiplicity of the cover is at most K^4.*

(iii) *(number of orbits) If Y_1 and Y_2 are two such maximal subsets, and Ω is finite, then $\frac{1}{K^4} \leqslant \frac{|Y_1|}{|Y_2|} \leqslant K^4$.*

Proof. We first prove (i). Consider the map $A \to A \cdot x$. The cardinal of the largest fiber is at most $|A^2 \cap H_x|$. This shows that $|A| \leqslant |A \cdot x||A^2 \cap H_x|$. Now for each $y \in A \cdot x$, let $a_y \in A$ be such that $a_y \cdot x = y$. Then $|\cup_y a_y(A^2 \cap H_x)| \geqslant |A \cdot x||A^2 \cap H_x|$ because this is a disjoint union. Hence $|A \cdot x||A^2 \cap H_x| \leqslant |A^3| \leqslant K^2|A|$. Finally if $y \in A \cdot x$, then $A \cdot y \subset A^2 \cdot x \subset XA \cdot x$, so $|A \cdot y| \leqslant K|A \cdot x|$ and reversing the roles of x and y we get the required bound.

We now consider item (ii). If $x \in \Omega$, then by maximality of Y, $A \cdot x$ intersects $A \cdot y$ for some $y \in Y$. Hence $x \in A^2 \cdot y$. So the $A^2 \cdot y$, $y \in Y$, cover Ω. Moreover if $x \in A^2 \cdot y$, then $|A \cdot x| \leqslant K^2|A \cdot y|$. Also $y \in A^2 \cdot x$ so $A \cdot y \subset A^3 \cdot x$. Therefore, if x lies in N sets $A^2 \cdot y_i$, for $y_1, ..., y_N \in Y$, then

$$\frac{N}{K^2}|A \cdot x| \leqslant \sum |A \cdot y_i| \leqslant |A^3 \cdot x| \leqslant K^2|A \cdot x|.$$

In particular $N \leqslant K^4$.

Regarding item (iii), note that (ii) shows that given $y \in Y_2$ there are at most K^4 elements $y_1 \in Y_1$ such that $A \cdot y_1 \cap A \cdot y \neq \varnothing$. So the map $Y_1 \to Y_2$ that associates to every $y_1 \in Y_1$ an element $y_2 \in Y_2$ such that $A \cdot y_1 \cap A \cdot y_2 \neq \varnothing$ has all its fibers of size at most K^4. This map is well defined because of the maximality of Y_2. We get $|Y_2| \leqslant K^4|Y_1|$. Reversing the roles of Y_1 and Y_2, we are done. □

4. Multiplicative energy and the Balog-Szemeredi-Gowers lemma

There are several ways in which one may want to relax the axioms for a group and thus come up with a notion of an "approximate group". One way is the small tripling condition, and we saw in Proposition 2.2 above that this condition is essentially equivalent (up to symmetrizing and taking the product set) to the approximate group notion defined in 1.1. Another possible way is to count the number of coincidences of the form $a_1 a_2 = a_3 a_4$ occurring among elements $a_1, a_2, a_3, a_4 \in A$. This leads to the notion of *multiplicative energy* of a finite set A. The main result of this section, the Balog-Szemeredi-Gowers lemma (in short BSG lemma), says that here again, this leads to a roughly equivalent notion of approximate group.

Let A, B be two finite subsets of an ambient group G and let 1_A (resp. 1_B) be the indicator function of A (resp. B).

Definition 4.1 (Multiplicative energy). *The multiplicative energy of the pair (A, B) is the quantity*

$$E(A, B) = \|1_A * 1_B\|_2^2 = |\{(a, b, a', b') \in A \times B \times A \times B; ab = a'b'\}|$$

To see that the last equality, simply expand

$$\|1_A * 1_B\|_2^2 = \sum_x \Big(\sum_{a \in A, b \in B} 1\Big)^2 = |\{(a,b,a',b') \in A \times B \times A \times B; ab = a'b'\}|.$$

Note that $E(gA, Bh) = E(A,B)$ for every $g, h \in G$. If $A = B$, then we talk about the multiplicative energy $E(A,A)$ of a single set A. In particular, $E(A,A)/|A|^4$ is the probability that 4 elements of A chosen at random uniformly and independently satisfy $a_1a_2 = a_3a_4$. If A were a finite subgroup of G, then this probability would be exactly $\frac{1}{|A|}$ and we would have $E(A,A) = |A|^3$. Asking for $E(A,A)/|A|^3$ to be not too small (say $\geq \frac{1}{K}$) is therefore another tentative way to approximate the notion of a finite subgroup. In the next two statements, we will compare this to the small tripling and approximate group conditions.

In fact, the multiplicative energy can never be larger than $|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}$ and a simple application of the Cauchy-Schwarz inequality shows that the multiplicative energy is large whenever the doubling constant is small. This is the content of the following lemma.

Lemma 4.2 (small doubling implies large multiplicative energy)**.** *Given two finite subsets A, B of G and $K \geqslant 1$ one has*

(i) *$E(A,B) \leqslant |A|^{\frac{3}{2}}|B|^{\frac{3}{2}}$, and*

(ii) *If $|AB| \leqslant K|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$, then $E(A,B) \geqslant \frac{|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}}{K}$*

Proof. We have $\|1_A * 1_B\|_2 \leqslant \|1_A\|_1\|1_B\|_2 = |A||B|^{\frac{1}{2}}$. Interchanging A and B and multiplying the two inequalities, we obtain (i).

To prove (ii), set $r(x) = |\{(a,b) \in A \times B; x = ab\}|$ and observe that $E(A,B) = \sum_{x \in AB} r(x)^2$, while $\sum_{x \in AB} r(x) = |A \times B|$. Applying Cauchy-Schwarz we get

$$|A \times B|^2 \leqslant |AB| E(A,B)$$

and the result follows. □

The converse of (ii) does not hold as such. If A is a set of doubling at most K, then adding to A any set of comparable size may very well ruin completely the small doubling condition (for example $A = \{1, ..., n\} \subset \mathbb{Z}$ has doubling at most 2, but $A \cup \{2, 2^2, ..., 2^n\}$ has doubling $\geqslant n$). However this operation will not alter too much the inequality $E(A,A) \geqslant |A|/K$. Indeed if $A \subset A'$ and $|A'| \leqslant M|A|$, then $E(A',A') \geqslant E(A,A) \geqslant |A'|/MK$. In that sense the large multiplicative energy condition is a much more robust one than small doubling.

A consequence of the Balog-Szemeredi-Gowers lemma below will be a partial converse to Lemma 4.2(ii), namely if $E(A,B)$ is large, then some non trivial proportion of A and B will satisfy the doubling condition.

We will state the BSG lemma first in its graph theoretic form and then describe its consequences for the multiplicative energy. The BSG lemma is one of the most important results from combinatorics that will be used in these lectures. Much can be done without it (for example the *Ruzsa calculus* that we have been using so far), but much can be done with it as well.

Lemma 4.3 (Balog-Szemeredi-Gowers lemma, graph theoretic form)**.** *There is a universal constant $C > 0$ such that the following holds. Suppose A, B are two finite subsets of an ambient group G with $|A| = |B| = N$ and suppose that $\mathcal{G}$ is a bipartite* *graph whose left vertices are elements of A and right vertices are elements of B. Suppose that the number of edges satisfies*

$$|\mathcal{G}| \geqslant N^2/K,$$

but that

$$|A \cdot_{\mathcal{G}} B| \leqslant KN,$$

where $A \cdot_{\mathcal{G}} B$ denotes the set of products ab with $a \in A$, $b \in B$ and (a, b) is an edge of $\mathcal{G}$. Then there are subsets $A' \subset A$ and $B' \subset B$ with $|A'| \geqslant N/CK^C$ and $|B'| \geqslant N/CK^C$ such that

$$|A'B'| \leqslant CK^C N.$$

In fact the following (obviously) stronger statement holds: for every $a' \in A'$ and $b' \in B'$, there are at least N^5/CK^C representations of $a'b'$ in the form

$$a'b' = a_1b_1(a_2b_2)^{-1}(a_3b_3),$$

where $a_1, a_2, a_3 \in A$, $b_1, b_2, b_3 \in B$ and each $(a_i, b_i) \in \mathcal{G}$.

Proof. We will not give the full proof of the Balog-Szemeredi-Gowers lemma here, rather we will show how to derive it from the following purely graph theoretical statement.

Lemma 4.4 (Existence of many paths of length 3, Lemma 6.20 in [31]). *Let $\mathcal{G}$ be a bipartite graph, and suppose that the number of left vertices equals the number of right vertices equals N and that the number of edges satisfies $|\mathcal{G}| \geqslant N^2/K$. Then there are subsets A' (resp. B') of left (resp. right) vertices of size $\geqslant N/CK^c$ such that for any $a' \in A'$ and $b' \in B'$, there are at least N^2/CK^c paths of length 3 in $\mathcal{G}$ between a' and b'. Here $C, c > 0$ are absolute constants (in fact one can take $c = 4$, $C = 2^{12}$).*

The BSG Lemma is a simple application of the above "paths of length three lemma". To see it, we first need to trim our bipartite graph $\mathcal{G}$ a little bit by removing the edges (a, b) such that $r(ab) := |\{(x, y) \in \mathcal{G}; xy = ab\}| \leqslant N/2K^2$. The number of removed edges is

$$\sum_{x \in A \cdot_{\mathcal{G}} B, r(x) \leqslant N/2K^2} r(x) \leqslant |A \cdot_{\mathcal{G}} B| \cdot N/2K^2 \leqslant N^2/2K \leqslant |\mathcal{G}|/2.$$

So we can apply Lemma 4.4 to the resulting bipartite graph $\mathcal{G}'$ and conclude that there are subsets A' and B' of size $\geqslant N/CK^c$ such that for any $a' \in A'$ and $b' \in B'$, there are at least N^2/CK^c paths of length 3 in $\mathcal{G}'$ between a' and b'. This means we can find at least N^2/CK^c pairs $(a, b) \in A \times B$ such that $(a', b), (a, b)$ and (a, b') belong to $\mathcal{G}'$. By definition of $\mathcal{G}'$, for each one of these three pairs, we can find at least $N/2K^2$ pairs $(x, y) \in \mathcal{G}$ with the same product. Since $a'b' = a'b(ab)^{-1}ab'$, this makes at least $N^5/4CK^{c+2}$ 6-tuples $(a_1, a_2, a_3, b_1, b_2, b_3) \in A^3 \times B^3$ such that $a'b' = (a_1b_1)(a_2b_2)^{-1}(a_3b_3)$ with each $(a_i, b_i) \in \mathcal{G}$. □

Corollary 4.5 (Balog-Szemeredi-Gowers lemma, multiplicative energy form). *If A, B are two finite subsets of an ambient group G such that $E(A, B) \geqslant |A|^{\frac{3}{2}}|B|^{\frac{3}{2}}/K$. Then the following holds*

(i) $|A| \leqslant K^2|B|$ *and* $|B| \leqslant K^2|A|$,

(ii) *There are subsets* $A' \subset A$ *and* $B' \subset B$ *such that* $|A'| \geqslant |A|/CK^C$ *and* $|B'| \geqslant |B|/CK^C$ *such that*
$$|A'B'| \leqslant CK^C|A|,$$

Note that, as we saw in Lemma 4.2, conversely (i) and (ii) imply a lower bound on the multiplicative energy $E(A,B) \geqslant |A|^{\frac{3}{2}}|B|^{\frac{3}{2}}/C'K^{C'}$ for some other constant C'.

Proof of Corollary 4.5. To see (i), note that $E(A,B) = \|1_A * 1_B\|_2^2 \leqslant \|1_A\|_1^2\|1_B\|_2^2 \leqslant |A|^2|B|$. From the assumption $E(A,B) \leqslant |A|^{\frac{3}{2}}|B|^{\frac{3}{2}}/K$, it follows that $|B| \leqslant K^2|A|$, and vice-versa exchanging the roles of A and B. In particular $|A|^{\frac{1}{2}}|B|^{\frac{1}{2}} \geqslant \max\{|A|,|B|\}/K$.

In order to prove (ii) we will apply Lemma 4.3 and build a bipartite graph $\mathcal{G}$ as follows. The set of left and right vertices will be the disjoint union $A \sqcup B$ with $N := |A| + |B|$ elements and we will connect a left vertex a to a right vertex b if $a \in A$, $b \in B$ and ab admits at least $|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}/2K$ representations $a'b'$, with $a' \in A$ and $b' \in B$. Note that if $r(x)$ is the number of representations of $x \in AB$ as $x = a'b'$, with $a' \in A$ and $b' \in B$, then
$$E(A,B) = \sum_{(a,b)\in A\times B} r(ab).$$

It follows immediately that
$$\frac{|\mathcal{G}| \cdot \max\{|A|,|B|\}}{|A||B|} \geqslant \frac{1}{|A||B|}\sum_{(a,b)\in\mathcal{G}} r(ab) \geqslant \frac{|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}}{2K},$$

hence
$$|\mathcal{G}| \geqslant \frac{|A||B|}{2K^2} \geqslant \frac{N^2}{4K^4}.$$

On the other hand, by construction $|A \cdot_{\mathcal{G}} B|\frac{|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}}{2K} \leqslant |A \times B|$, and hence
$$|A \cdot_{\mathcal{G}} B| \leqslant 2KN.$$

We may then apply Lemma 4.3 and conclude that there exist subsets $A' \subset A$ and $B' \subset B$ with $|A'| \geqslant |A|/CK^C$ and $|B'| \geqslant |B|/CK^C$ such that $|A'B'| \leqslant CK^CN$. This proves (ii). □

A useful observation in connection with multiplicative energy is that, although $E(A,B) \neq E(B,A)$ for arbitrary finite sets A, B, we nevertheless have $E(A,A^{-1}) = E(A^{-1},A)$ for every finite subset A. This allows to obtain the following important fact.

Lemma 4.6. *Let* A *be a finite subset of an ambient group* G*, such that* $|A^{-1}A| \leqslant K|A|$*. Then there is a subset* $A_0 \subset A$ *such that* $|A_0| \geqslant |A|/CK^C$ *and*
$$\max\{|A_0^{-1}A_0|, |A_0A_0^{-1}|\} \leqslant CK^C|A_0|.$$
Moreover we can choose A_0 *so that both* $A_0A_0^{-1}$ *and* $A_0^{-1}A_0$ *are* CK^C*-approximate subgroups.*

Observe that a small doubling assumption $|AA| \leqslant K|A|$ (such as in Proposition 2.4(i)) always implies $|A^{-1}A| \leqslant K^2|A|$ and $|AA^{-1}| \leqslant K^2|A|$, since $d(A,A)$ and $d(A^{-1},A^{-1})$ are both $\leqslant 2d(A,A^{-1})$ by the Ruzsa triangle inequality. However the converse does not hold (e.g. take A to be a coset xH of a subgroup H such that $xHx^{-1} \cap H = \{1\}$).

Proof. By Lemma 4.2 $E(A^{-1}, A) \geqslant |A|^3/K$. But since $E(A, A^{-1}) = E(A^{-1}, A)$, we also have $E(A, A^{-1}) \geqslant |A|^3/K$, from where it follows by Corollary 4.5 that there exists a subset $A_0 \subset A$ satisfying the desired inequality.

Then by applying Petridis's lemma (Lemma 3.3) twice to $|A_0^{-1}A_0| \leqslant CK^C|A_0|$ first and then to $|A_0A_0^{-1}| \leqslant CK^C|A_0|$, we may assume (after changing A_0 into some large subset) that $|A_0^{-1}A_0X| \leqslant CK^C|A_0X|$ and $|A_0A_0^{-1}X| \leqslant CK^C|A_0^{-1}X|$ for every finite set X. It follows immediately that $|(A_0^{-1}A_0)^2A_0^{-1}| \leqslant CK^C|A_0|$ and $|(A_0A_0^{-1})^2A_0| \leqslant CK^C|A_0|$ and thus that $A_0A_0^{-1}$ and $A_0^{-1}A_0$ are CK^C-approximate subgroups, by Ruzsa covering. □

We can now prove Proposition 2.5 from Section 2, the statement of which we now recall.

Corollary 4.7 (Control by an approximate group, Proposition 2.5)**.** *Assume that A and B are two subsets of an ambient group such that $|AB| \leqslant K \min\{|A|, |B|\}$. Then there is a CK^C-approximate subgroup H of G, with size $\leqslant CK^C \min\{|A|, |B|\}$, such that $H \subset (A^{-1}A)^2 \cap (BB^{-1})^2$ for which $A \subset XH$ and $B \subset HY$ for some subsets X and Y of size at most CK^C.*

Proof. By the Ruzsa triangle inequality, we see that $|AA^{-1}| \leqslant K^2|A|$ and $|B^{-1}B| \leqslant K^2|B|$. We can then apply Lemma 4.6 and conclude that there are large subsets $A_0 \subset A$ and $B_0 \subset B$ such that $H_a := A_0^{-1}A_0$ and $H_b := B_0B_0^{-1}$ are CK^C-approximate groups of size $\leqslant CK^C \min\{|A|, |B|\}$. Now, since $|AA_0^{-1}| \leqslant CK^C|A_0|$, by Ruzsa covering $A \subset X_aH_a$, where $X_a \subset A$ has size $\leqslant CK^C$, and similarly since $|A_0B| \leqslant CK^C|A_0|$, we get $B \subset H_aY_a$ for some $Y_a \subset B$ of size $\leqslant CK^C$. Similarly $A \subset X_bH_b$ and $B \subset H_bY_b$. Let $H = H_a^2 \cap H_b^2$. Note that, as in Proposition 3.5(ii) $H_aY_a \cap H_bY_b \subset HY$ for some set Y of size $\leqslant |Y_a||Y_b| \leqslant CK^C$. Similarly $X_aH_a \cap X_bH_b \subset XH$. We are done. □

Part 2. The sum product phenomenon

In this chapter, we begin our investigation of the structure of approximate groups by two landmarks of additive combinatorics: the sum-product phenomenon and the Freiman-Ruzsa theorem. Both results provide some structural information on a set submitted to a small sumset condition. Such results are sometimes called *inverse theorems*, and we already saw two examples of these in Propositions 2.6 and 2.7 which gave a description of sets of very small doubling.

5. Approximate rings and fields

It is natural to ask for the approximate variants of other algebraic structures, such as rings and fields to begin with. As we shall see, unlike mere approximate groups, the structure of approximate fields is fairly well understood. Approximate rings are more delicate as one needs to take zero divisors into account (see [30] for a detailed treatment of approximate rings). In what follows, we restrict our attention to approximate fields (except in Lemma 5.5).

Definition 5.1 (Approximate field)**.** *Let F be a field and $K \geqslant 1$ a constant. A finite subset A of F is said to be a K-approximate subfield of F if $A = -A$ and $A^\times = (A^\times)^{-1}$, A contains 0 and 1, and if there is a subset X in F with $|X| \leqslant K$, such that $AA + A$ is contained in $AX \cap (A + X)$.*

From this definition, one can very quickly show that an approximate field is almost stable under all algebraic operations. This is the content of the following lemma. Given $d \in \mathbb{N}$, and a finite subset A is F, let $Alg_d(A)$ be the set of elements in F that can be written as a sum of at most d terms each of which is a product of at most d elements from $\pm A \cup \pm A^{-1}$, or as ratios of any two such elements. Namely,

$$Alg_d(A) = \frac{B^d \pm \ldots \pm B^d}{B^d \pm \ldots \pm B^d},$$

where $B := A \cup A^{-1} \cup \{1\}$.

Lemma 5.2. *Let $K \geqslant 1$ and let $A \subset F$ be a K-approximate subfield. Then there is a subset Y_d of size at most $K^{O_d(1)}$, such that* $\mathrm{Alg}_d(A) \subset AY_d \cap (A + Y_d)$*.*

Proof. This is a rather straightforward exercise using repeated applications of the Ruzsa covering lemma. Let us briefly sketch the steps. Abusing notation let us denote by X_n a subset of F of size $K^{O_n(1)}$ which may change from line to line as the argument flows. First one shows by induction on n that $A^{n+1} + A^n \subset AX^{2n-1}$ writing $A^{n+1} + A^n \subset (A + A)(A^n + A^{n-1}) \subset AXAX^{2n-3}$. Then one deduces from this (using the Ruzsa covering lemma and induction) that $A^n \subset A + X_n$ for some X_n of size $K^{O_n(1)}$. Adding, one gets $\sum_{i=1,\ldots,n} A^i \subset A + X_n$ (where we have abused notation). Multiplying by A on the left and applying the Ruzsa covering once again we get $\sum_{i=1,\ldots,n} A^i \subset AX_n$. Taking inverses and mutiplying we get $Alg_n(A) \subset AX_n$. Finally using $A + Alg_n(A) \subset Alg_{n+1}(A)$ and Ruzsa covering, we obtain $Alg_n(A) \subset A + X_n$ and we are done. □

We are now ready to describe the structure of approximate fields. In fact it is not so surprising: an approximate field generates a subfield that is itself not much larger. Equivalently we could phrase this saying that there are no interesting approximate fields. We have:

Theorem 5.3 (Classification of approximate fields)**.** *Let A be a K-approximate subfield of F. Let F_A be the subfield generated by A. Then either $|A| \leqslant K^C$ or $|F_A| \leqslant K^C|A|$.*

Proof. We claim that unless $|A| \leqslant K^C$, $Alg_2(A)$ is a genuine subfield of F, and hence coincides with F_A. By Lemma 5.2, this will clearly conclude the proof of the theorem. To prove the claim, we make the following key observation: if $x \notin Alg_2(A)$, then $|A + xA| = |A|^2$. Indeed the map $A \times A \to A + xA$ is injective unless $x \in \frac{A-A}{A-A}$. On the other hand we verify easily that $A + (Alg_2(A) \cdot Alg_2(A))A \subset Alg_8(A)$ and $A + (Alg_2(A) + Alg_2(A))A \subset Alg_{16}(A)$. But, according to lemma 5.2, both subsets are of size $K^{O(1)}|A|$, which is $< |A|^2$ unless $|A| \leqslant K^{O(1)}$. Hence $Alg_2(A)$ is stable under multiplication and addition : it is a finite subring of F, hence a finite subfield. We are done. □

It is useful to have a simple criterion for when a subset of a field can give rise to an approximate subfield. We show:

Proposition 5.4 (Sufficient conditions to get an approximate field)**.** *Let A be a finite subset of a field such that $|A| \geqslant 2$, $|A+A| \leqslant K|A|$, and $|AA+A| \leqslant K|A|$, then $\frac{A-A}{A-A}$ is a CK^C-approximate subfield of size $\leqslant CK^C|A|$.*

The proof will follow easily from the following analogue of the small tripling implies small n-pling lemma proved earlier in the context of groups (Proposition 2.2).

Lemma 5.5. *Let A be a finite subset of a ring R such that $|A+A| \leqslant K|A|$, and $|AA+A| \leqslant K|A|$. Then for every $M, m \geqslant 1$, we have $|M(\pm A^m)| \leqslant O_{M,m}(1)K^{O_{M,m}(1)}|A|$.*

Proof. Note that $A-A$ is a K^5-approximate group (by the Plunnecke-Ruzsa estimates Prop. 2.3). Now we claim that for every element $x \in M(\pm A^m)$ we have $xA \subset A - A + X_{x,M,m}$, where $X_{x,M,m}$ is a subset of R of size $K^{O_{M,m}(1)}$. This easily follows by induction on M and m. Indeed if x, y satisfy $xA \subset A - A + X$ and $yA \subset A - A + Y$, then $(x+y)A \subset A - A + A - A + X + Y \subset A - A + Z$ with $|Z| \leqslant K^5|X||Y|$. The same holds for $x-y$. Similarly, to deal with xy, note that since $|AA+A| \leqslant K|A|$ we have $AA \subset A - A + Z$ for some Z of size $\leqslant K$, by Ruzsa covering. Hence $xyA \subset x(A-A+Y) \subset AA - AA + xY \subset 2(A-A) + Z - Z + xY \subset A - A + Z'$ for some Z' of size $\leqslant K^C|Y|$. This proves the claim.

Now let us show by induction on m that $A^m \subset A - A + X_m$ for some subset X_m of size $\leqslant O_m(1)K^{O_m(1)}$. For $m = 2$, this follows by Ruzsa covering from the assumption $|AA+A| \leqslant K|A|$. Suppose we know it for $m \geqslant 2$, then X_m can be of course chosen to lie inside $A^m + A - A$. By the claim we just proved, it follows that every $x \in X_m$ satisfies $xA \subset A - A + X_{x,3,m}$ for some $X_{x,3,m}$ of size at most $K^{O_m(1)}$. In particular $X_mA \subset A - A + \cup_{x \in X_m} X_{x,3,m} \subset A - A + Y_m$ where Y_m has size at most $O_m(1)K^{O_m(1)}$. Hence $A^{m+1} \subset AA - AA + X_mA \subset 3(A-A) + Z - Z + Y_m \subset A - A + X_{m+1}$ with again $|X_{m+1}| \leqslant O_m(1)K^{O_m(1)}$.

So we have now established that for every $m \geqslant 2$ one has $A^m \subset A - A + X_m$ for some X_m of size $\leqslant O_m(1)K^{O_m(1)}$. Using Proposition 2.2 additively, we can right away conclude that $M(\pm A^m) \subset A - A + X_{M,m}$ for every $M \geqslant 1$ and some $X_{M,m}$ of size $\leqslant O_{M,m}(1)K^{O_{M,m}(1)}$ and this implies the desired bound. □

Proof of Proposition 5.4 Let $Q = \frac{A-A}{A-A}$. Since $|A| \geqslant 2$, there is $x \in (A-A) \setminus \{0\}$. We observe that in order to show that Q is an approximate subfield, it is enough to check that $|\frac{A}{x} + QQ + Q|$ and $|(A-A)(QQ+Q)|$ are both of size $\leqslant CK^C|A|$. Indeed, by additive Ruzsa covering we would get $QQ + Q \subset \frac{A}{x} - \frac{A}{x} + X \subset Q + X$ for some X of size $\leqslant CK^C$, while by multiplicative Ruzsa covering we would get $QQ + Q \subset QY$ for some Y of size $\leqslant CK^C$, and hence Q is a CK^C-approximate subfield.

But as one readily checks, both expressions $(A-A)(QQ+Q)$ and $\frac{A}{x} + QQ + Q$ are contained in $\frac{12(\pm A^3)}{4(\pm A^3)}$. Now, recall that the Ruzsa triangle inequality implies that $|BB^{-1}|/|B| \leqslant (|BB|/|B|)^2$ for any set B in the multiplicative group of $R \setminus \{0\}$. Applying this to $B = 12(\pm A^3)$, we will be done if we can bound $BB \subset 144(\pm A^6)$. But we know from Lemma 5.5 that this is of size $CK^C|A|$. We are now done. □

6. The sum-product theorem

One of the corner stones of modern arithmetic combinatorics is the *sum-product phenomenon* of Bourgain-Katz-Tao [6]. This result lead to many ground breaking applications in particular to exponential sums in number theory (see [5]), to non-commutative sieve theory (see [4]) and to expander graphs and spectral gap phenomena ([2], [3]).

Theorem 6.1 (sum-product phenomenon over $\mathbb{F}_p$). *For every $\delta > 0$, there is $\epsilon > 0$ such that if p is a prime and A is a finite subset of $\mathbb{F}_p$, then either $|A| \geqslant p^{1-\delta}$, or*

$$\min\{|AA|, |A+A|\} \geqslant |A|^{1+\epsilon}.$$

An analogous result holds over $\mathbb{C}$ and in fact over an arbitrary field, where it takes the following form:

Theorem 6.2 (sum-product over an arbitrary field). *There is an absolute constant $C > 0$ such that the following holds. Let F be a field and A a finite subset of F such that $max\{|AA|, |A+A|\} \leqslant K|A|$. Then either $|A| \leqslant CK^C$, or there is a finite subfield $G \subset F$ with $|G| \leqslant CK^C|A|$ and there is $x \in F$ such that $A \subset xG \cup X$ for some finite subset $X \subset F$ of cardinal at most CK^C.*

Note that the conclusion is sharp in the sense that any set $A \subset xG \cup X$ with $|X| \leqslant K^{O(1)}$ with $|G| \leqslant O(K^{O(1)})|A|$ satisfies $max\{|AA|, |A+A|\} \leqslant O(K^{O(1)})|A|$. Also note that Theorem 6.2 easily implies Theorem 6.1 because $\mathbb{F}_p$ has no non trivial subfields.

We will derive Theorem 6.2 from the classification of approximate fields obtained in the previous paragraph, i.e. Theorem 5.3. In order to do so, we would need to show that the small doubling assumption for both multiplication and addition implies a bound on $Alg_d(A)$ (see §5 for the definition of Alg_d). This is akin to the passage from small doubling to small n-pling for approximate groups (i.e. Proposition 2.2). Unfortunately, very much like in the approximate group situation, such a bound is not true in this generality (indeed take for A the union of a finite subfield G and a few other points in $F \setminus G$: this will have small multiplicative and additive doubling, but $AA + A$ will contain $xG + G$, which is of size $|G|^2$). However, it becomes true for some proportion of A. This is the content of the Katz-Tao lemma, which we now prove.

Lemma 6.3 (Katz-Tao lemma [6], [30]). *Suppose A is a finite subset of a field F such that $max\{|AA|, |A+A|\} \leqslant K|A|$. Then there is a subset $A' \in A$ with $|A'| \geqslant |A|/CK^C$ such that $|A'+A'| \leqslant CK^C|A'|$ and $|A'A' - A'A'| \leqslant CK^C|A'|$.*

Proof. First observe that by Plunnecke-Ruzsa (Prop. 2.3), $A - A$ is a K^5-approximate group of size $\leqslant K^2|A|$. We now proceed to find a large A' in A with $|A'A' - A'A'| \leqslant CK^C|A'|$. By Proposition 2.2, we know that $|nA| \leqslant K^{O_n(1)}|A|$ for every $n \in \mathbb{N}$. We now claim that there is some $b \in A$ such that $|A'| \geqslant |A|/CK^C$, where $A' := \{a \in A, d(aA, bA) \leqslant C \log K + \log C\}$ and $d(\cdot,\cdot)$ is the additive Ruzsa distance.

Before proving the claim, let us see how to finish the proof of Lemma 6.3. For all $a \in A'$, we have $|aA - bA| \leqslant CK^C|A|$, hence by Ruzsa covering $aA \subset b(A-A) + X$ for some X of size $\leqslant CK^C$. It follows that for all $a_1, ..., a_4 \in A'$, we have $(a_1a_2 - a_3a_4)A \subset b(A - A + A - A) + X - X \subset b(A-A) + Y$ for some Y of size $\leqslant CK^C$. Hence, by the pigeonhole principle, for every $c \in A'A' - A'A'$ there is $y \in Y$ and at least $|A|/CK^C$ elements $a \in A$ such that $ca \in b(A-A)+y$. Taking the difference of two such elements, this makes at least $|A|/CK^C$ elements $u \in A-A$ such that $cu \in b(A-A+A-A)$. Hence every $c \in A'A'-A'A'$ has at least $|A|/CK^C$ representations of the form $c = v/u$, where $v \in b(A-A+A-A)$ and $u \in A-A$. Since both $|A-A+A-A|$ and $|A-A|$ are $\leqslant CK^C|A|$, we immediately get the desired bound $|A'A'-A'A'| \leqslant CK^C|A|$.

We now prove the claim. It is enough to find b such that $|aA \cap bA| \geqslant |A|/CK^C$ for more than $|A|/CK^C$ elements $a \in A$, because then by the Ruzsa triangle inequality $d(aA, bA) \leqslant d(aA, aA \cap bA) + d(aA \cap bA, bA)$ and both terms are $\leqslant C\log K + \log C$ because $|A-A| \leqslant CK^C|A|$ (as follows from small doubling by an application of the Ruzsa inequality). Suppose by way of contradiction that for every $b \in A$, there are fewer than $|A|/2K$ elements $a \in A$ such that $|aA \cap bA| \geqslant |A|/2K$. Then

$$\sum_{a,b} |aA \cap bA| \leqslant |A|(|A| - |A|/2K)|A|/2K + |A|^3/2K < |A|^3/K.$$

But on the other hand we have the identities

$$\sum_{a,b} |aA \cap bA| = \sum_{a,b} \sum_{x \in AA} 1_{aA}(x) 1_{bA}(x) = \sum_{x \in AA} \big(\sum_{a \in A} 1_{aA}(x)\big)^2 = \sum_{x \in AA} |\{(a,b) \in A \times A; ab = x\}|^2$$

while

$$\sum_{x \in AA} |\{(a,b) \in A \times A; ab = x\}| = |A \times A| = |A|^2.$$

From these two identities, applying Cauchy-Schwarz we derive

$$\sum_{a,b} |aA \cap bA| \geqslant |A|^4/|AA| \geqslant |A|^3/K.$$

We are done □

Proof of Theorem 6.2. Applying the Katz-Tao lemma, we obtain $A' \subset A$ such that $|A'A' - A'A'| \leqslant CK^C|A| \leqslant CK^C|A'|$ and $|A'| \geqslant |A|/CK^C$. By changing A into $a^{-1}A$ for some $a \in A'$ if necessary, we may assume that $-1 \in A'$. Without loss of generality, we may also add $\{0\}$ to A' (and to A) if necessary. Then $|A'A' + A'| \leqslant |A'A' - A'A'| \leqslant CK^C|A|$. On the other hand $|A' + A'| \leqslant CK^C|A'|$. Therefore we are in a position to apply Proposition 5.4 to A', and we conclude that $\frac{A'-A'}{A'-A'}$ is a CK^C-approximate subfield G of size $\leqslant CK^C|A'|$ and which contains A', because $0, -1 \in A'$.

We know by Theorem 5.3 that the field $F_{A'}$ generated by A' has size at most $CK^C|A|$. On the other hand $|A + A'| \leqslant CK^C|A'|$, so applying the (additive) Ruzsa covering lemma (Lemma 3.2) we get $A \subset F_{A'} + X$ for some set X of size CK^C and similarly with the multiplicative Ruzsa covering lemma, we get $A \subset F_{A'}Y$ for some Y of size CK^C. Hence A lies in the union of at most CK^C sets of the form $F_{A'}y \cap (F_{A'} + x)$. But, as the reader will easily check, each such set is either equal to $F_{A'}$ or of size at most 1. Thus $A \subset F_{A'} \cup Z$ for some Z of size CK^C. We are done. □

Proof of Theorem 6.1. Set $K = |A|^\varepsilon$ and apply Theorem 6.2. There is a subfield G such that $A \subset xG \cup X$ where $|G| \leqslant CK^C|A| \leqslant C|A|^{1+C\varepsilon} \leqslant Cp^{(1-\delta)(1+C\varepsilon)}$. Now if ε is small enough, then $Cp^{(1-\delta)(1+C\varepsilon)} < p$, for all $p \geqslant 2$. But on the other hand $\mathbb{F}_p$ has no proper subfields, so $G = \mathbb{F}_p$, a contradiction. □

Theorem 6.1 says nothing when $|A| > p^{1-\delta}$. In fact one can still say something, namely that the entire field $\mathbb{F}_p$ will be covered by a few sums and products of A. We have:

Lemma 6.4. *Let A be a finite subset of $\mathbb{F}_p$ such that $|A| \geqslant p^{\frac{5}{6}}$, then $A^2+A^2+A^2 = \mathbb{F}_p$.*

Together with the classification of approximate fields given in the previous section, we will see that this easily implies the following result, which can also often serve as a substitute for Theorem 6.1.

Theorem 6.5. *There is $\varepsilon > 0$ such that for any prime p and any finite subset A of $\mathbb{F}_p$, one has*

$$|A^2 + A^2 + A^2| \geqslant \min\{|\mathbb{F}_p|, |A|^{1+\varepsilon}\}.$$

Lemma 6.4 on the other hand follows by a standard Fourier argument and is a simple consequence of the following two observations:

Observation 1. Given $z \in \mathbb{F}_p$, the number of solutions in 6 variables $x_1, ..., x_6 \in A$ of the equation $z = x_1x_2 + x_3x_4 + x_5x_6$ can be expressed in Fourier analytic terms as follows

$$p|\{(x_1, ..., x_6) \in A\times ...\times A; z = x_1x_2+x_3x_4+x_5x_6\}| = \sum_{x_1,...,x_6\in A, \xi\in\mathbb{F}_p} e^{\frac{2i\pi}{p}\xi(z-x_1x_2+x_3x_4+x_5x_6)},$$

Observation 2. If X, Y are subsets of $\mathbb{F}_p$, then for any $\xi \in \mathbb{F}_p^*$,

$$|\sum_{x\in X, y\in Y} e^{\frac{2i\pi}{p}\xi xy}| \leqslant \sqrt{p|X||Y|}.$$

Proof. This is a simple application of Cauchy-Schwarz and the Parseval identity. We write for every $y \in Y$,

$$\sum_{x\in X} e^{\frac{2i\pi}{p}\xi xy} = \widehat{1_X}(\xi y),$$

then by Cauchy-Schwarz

$$|\sum_{y\in Y} \widehat{1_X}(\xi y)| \leqslant \sqrt{|Y|}\sqrt{\sum_{y\in Y} |\widehat{1_X}(\xi y)|^2} \leqslant \sqrt{|Y|}\sqrt{\sum_{r\in\mathbb{F}_p} |\widehat{1_X}(r)|^2},$$

where we have used that $\xi \neq 0$. Applying Parseval to the right hand side, we immediately get the desired inequality. □

With these two observations, we can give a quick proof of Lemma 6.4.
Proof of Lemma 6.4 Splitting the sum in Observation 2 according to whether $\xi = 0$ or not, we see that it is enough to prove that

$$|\sum_{\xi\in\mathbb{F}_p^*} e^{\frac{2i\pi}{p}\xi z}\big(\sum_{x,y\in A} e^{\frac{2i\pi}{p}\xi xy}\big)^3| < |A|^6.$$

By Observation 1, the left hand side satisfies

$$|\sum_{\xi\in\mathbb{F}_p^*} e^{\frac{2i\pi}{p}\xi z}\big(\sum_{x,y\in A} e^{\frac{2i\pi}{p}\xi xy}\big)^3| \leqslant (p-1)p^{3/2}|A|^3,$$

and this is $< |A|^6$ because we assumed $|A| \geqslant p^{\frac{5}{6}}$. □

We refer the reader to [31, Lemma 4.10] for an improvement from $\frac{5}{6}$ to $\frac{3}{4}$ of the power of p needed in Lemma 6.4, which follows from a slightly more clever, albeit very similar, argument.

Proof of Theorem 6.5 Without loss of generality, we may assume that $1 \in A$ by changing A into A/a for some $a \in A \setminus \{0\}$. Let $K = |A|^{\varepsilon}$, and suppose that $|3A^2| \leqslant K|A|$. Then $|A + A|, |AA + A| \leqslant K|A|$, and we may apply Proposition 5.4 to conclude that $\frac{A-A}{A-A}$ is a CK^C-approximate field of size $\leqslant CK^C|A|$. By the classification of approximate fields, this means that the field generated by this approximate subfield is also of size $\leqslant CK^C|A| \leqslant C|A|^{1+C\varepsilon}$. However $\mathbb{F}_p$ has no subfields, so this means that $C|A|^{1+C\varepsilon} \geqslant p$ and $|A| \geqslant (p/C)^{1/(1+C\varepsilon)}$. This is $\geqslant p^{5/6}$ as soon as p is large enough. Applying Lemma 6.4, we then get $3A^2 = \mathbb{F}_p$ and we are done. □

Note that this proof did not need the Katz-Tao lemma.

Part 3. Fourier techniques

Harmonic analysis and the Fourier transform are very useful tools to understand the structure of abelian approximate groups: this leads to the Freiman-Ruzsa theorem discussed below. When the group is non abelian, then it will come to no surprise that representation theory and harmonic analysis alone is not sufficient to understand the structure of non abelian approximate groups. However we will see that some important information on approximate subgroups can be deduced by looking at finite dimensional representations of the ambient group.

7. The Freiman-Ruzsa theorem

The Freiman-Ruzsa theorem uncovers the structure of sets of small doubling in $G = \mathbb{Z}$, or more generally, when G is an arbitrary abelian group (Green-Ruzsa theorem). As often when dealing with abelian groups, Fourier analytic tools can be put to use and they turn out to be quite powerful.

A basic example of approximate group was given shortly after Definition 1.1, namely that of (symmetric) generalized arithmetic progressions. Let $B = \prod_{i=1}^{d}[-L_i, L_i]$ in $\mathbb{Z}^d$ with $L_i \in \mathbb{N}$. A (symmetric) generalized arithmetic progression of dimension d in a group G is by definition any homomorphic image of such a box B. These are easily seen to be 2^d-approximate subgroups of G.

The Freiman-Ruzsa theorem states that in some sense these are the only examples of approximate subgroups of $\mathbb{Z}$. We have

Theorem 7.1 (Freiman-Ruzsa theorem). *Let A be a K-approximate subgroup of $G = \mathbb{Z}$. Then*[3] *A^4 contains a symmetric generalized arithmetic progression P of rank at most $O(K^{O(1)})$ and of size at least $exp(-O(K^{O(1)}))|A|$. Moreover, A is contained in a symmetric generalized arithmetic progression P of rank at most $O(K^{O(1)})$ and of size at most $exp(O(K^{O(1)}))|A|$.*

The theorem was originally proved by Freiman (in a slightly different form) and Ruzsa later came up with a much simplified proof, which we will give in this section. Building on this proof Green and Ruzsa extended the result to all abelian groups. In that case, one needs to take into account finite subgroups of G, since they are

[3] In this section, we will use both the additive $A + A$ and multiplicative AA notation alike.

clearly another kind of approximate groups. It is thus convenient to introduce the following terminology:

Definition 7.2. *A* coset progression *is a finite subset P_c of an ambient group G which is a union of cosets of a subgroup H of G such that P_c normalizes H and P_c/H is a symmetric generalized arithmetic progression in the quotient group $\langle P_c\rangle/H$.*

The rank of a coset progression is defined to be the rank of the generalized arithmetic progression used to define it. The result takes the following form:

Theorem 7.3 (Green-Ruzsa theorem)**.** *Let A be a K-approximate subgroup of an abelian group G. Then A^4 contains a coset progression of size $\geqslant |A|/exp(-O(K^{O(1)}))$ and rank $O(K^{O(1)})$. Moreover, A is contained of size $\leqslant exp(O(K^{O(1)}))|A|$ and rank $O(K^{O(1)})$.*

In these lectures, we will prove Theorem 7.1 in full and reduce the proof of Theorem 7.3 to the proof of the existence of a *good model* for an approximate group in an arbitrary abelian group, a result of Green and Ruzsa ([19]).

The argument can be split into 4 steps. First one shows that (a positive proportion of) A is *freiman isomorphic* to a subset of an other abelian group of size $\leqslant C|A|$, where C can be bounded in terms of K only. Since the statement of the theorem is invariant under Freiman 2-isomorphism (see Proposition 1.5), passing to this *good model* does not reduce the generality. Then one shows (Bogolyubov argument) that the set A^4 contains a large Bohr set $B(\xi_1, ..., \xi_d, \alpha) := \{x \in \mathbb{Z}/p\mathbb{Z}; |\xi(x) - 1| < \alpha \text{ for all } i\}$, where the $\xi : \mathbb{Z}/p\mathbb{Z} \to S^1 = \{z \in \mathbb{C}; |z| = 1\}$ are suitable characters of G and α and d are bounded in terms of K only. It turns out that the structure of Bohr sets can be rather easily described using some simple geometry of numbers : they contain and are contained in coset progressions whose rank is controlled in terms of α and d, hence K only. This finishes the first part of both theorems. To obtain the containment inside a coset progression, one applies a covering argument (Chang covering) similar but more refined than the Ruzsa covering lemma.

We now pass to the proof of the above theorems. The Fourier transform on a finite abelian group G exchanges functions on G and functions on the dual group $\widehat{G}$ of characters of G, i.e. homomorphisms from G to $S^1 := \{z \in \mathbb{C}; |z| = 1\}$. Recall that $|\widehat{G}| = |G|$ (see [27]).

If for $f : G \to \widehat{G}$, we define

$$\widehat{f}(\xi) = \sum_{x \in G} f(x)\xi(x),$$

then the Parseval identity reads

$$\frac{1}{|\widehat{G}|} \sum_{\xi \in \widehat{G}} |\widehat{f}(\xi)|^2 = \sum_{x \in G} |f(x)|^2,$$

and the Fourier inverse formula reads

$$f(x) = \frac{1}{|G|} \sum_{\xi \in \widehat{G}} \widehat{f}(x)\xi(-x).$$

The Fourier transform also establishes a correspondence between subgroups of G and subgroups of $\widehat{G}$. Indeed to any subgroup H of G one can associate $H^{\perp} :=$

$\{\xi \in \widehat{G}; \xi(H) = 1\}$, and conversely to every subgroup $F \leqslant \widehat{G}$, one associates $F^{\perp} = \bigcap_{\xi \in F} \ker \xi$. It is a basic result of the theory of characters of finite abelian groups (see e.g. [27]) that $F^{\perp\perp} = F$ and $H^{\perp\perp} = H$.

Note that the transform $H \to H^{\perp}$ is inclusion-reversing. In particular if H is a large subgroup of G then $H^{\perp}$ will be a small subgroup of $\widehat{G}$. In fact $H^{\perp} \simeq \widehat{G/H}$ and $|H||H^{\perp}| = |G|$.

This correspondence works very well between subgroups and one would like to have a similar correspondence between approximate subgroups. However defining $A^{\perp}$ as above by $\{\xi \in \widehat{G}, \xi(A) = 1\}$ does not work, because this is always a genuine subgroup of $\widehat{G}$, and we know that in many abelian groups, there are many more approximate subgroups than subgroups.

One way to remedy this is to consider the *spectrum* of the set A, namely

$$S_{\alpha}(A) := \{\xi \in \widehat{G}; |\widehat{1_A}(\xi)| > \alpha|A|\},$$

where $\alpha \in [0,1]$.

Another way is to consider a smaller set, called Bohr set, and defined as follows:

$$B_{\alpha}(A) := \{\xi \in \widehat{G}; \Re\xi(x) > \alpha \text{ for all } x \in A\}.$$

This is indeed a smaller set since $\widehat{1_A}(\xi) = \sum_{x \in A} \Re\xi(x)$.

The following statement can be seen as some approximate analogue of the identity $H^{\perp\perp} = H$ for genuine subgroups of G.

Proposition 7.4 (Bogolyubov argument)**.** *Let A be a K-approximate subgroup of a finite abelian group G, then $B_{1/2K}(S_{1/2K}(A)) \subset A^4$.*

Proof. Let $\alpha, \delta > 0$ to be determined later. We want to prove that if $x \in B_{\delta}(S_{\alpha}(A))$, then $1_A * 1_A * 1_A * 1_A(x) > 0$. To achieve this, we write the Fourier inverse formula:

$$1_A * 1_A * 1_A * 1_A(x) = \frac{1}{|G|} \sum_{\xi \in \widehat{G}} \widehat{1_A}(\xi)^4 \Re\xi(-x)$$

$$= \frac{1}{|G|} \sum_{|\widehat{1_A}(\xi)| > \alpha|A|} \widehat{1_A}(\xi)^4 \Re\xi(x) + \frac{1}{|G|} \sum_{|\widehat{1_A}(\xi)| \leqslant \alpha|A|} \widehat{1_A}(\xi)^4 \Re\xi(x).$$

$$\geqslant \frac{\delta}{|G|} \sum_{|\widehat{1_A}(\xi)| > \alpha|A|} \widehat{1_A}(\xi)^4 - \frac{1}{|G|} \sum_{|\widehat{1_A}(\xi)| \leqslant \alpha|A|} \widehat{1_A}(\xi)^4$$

$$\geqslant \frac{\delta}{|G|} \sum_{\xi \in \widehat{G}} \widehat{1_A}(\xi)^4 - \frac{1+\delta}{|G|} \sum_{|\widehat{1_A}(\xi)| \leqslant \alpha|A|} \widehat{1_A}(\xi)^4.$$

On the other hand $\frac{1}{|G|} \sum_{\xi \in \widehat{G}} \widehat{1_A}(\xi)^4 = \frac{1}{|G|} \sum_{\xi \in \widehat{G}} \widehat{1_A * 1_A}(\xi)^2 = \sum_{x \in G} (1_A * 1_A)(x)^2 = E(A,A)$ is the multiplicative energy of A, while we may bound the other term by

$$\frac{1+\delta}{|G|} \sum_{|\widehat{1_A}(\xi)| \leqslant \alpha|A|} \widehat{1_A}(\xi)^4 \leqslant \frac{1+\delta}{|G|} \alpha^2 |A|^2 \sum_{\xi \in \widehat{G}} \widehat{1_A}(\xi)^2 = (1+\delta)\alpha^2|A|^3,$$

where we applied Parseval in the last inequality.

In other words, we have obtained:

$$1_A * 1_A * 1_A * 1_A(x) \geqslant \delta E(A,A) - (1+\delta)\alpha^2|A|^3.$$

But $E(A,A) \geqslant |A|^3/K$, since A is a K-approximate group and $|AA| \leqslant K|A|$ (see Lemma 4.2). Hence

$$1_A * 1_A * 1_A * 1_A(x) \geqslant |A|^3(\delta/K - (1+\delta)\alpha^2).$$

This is > 0 for instance for $\delta = \alpha = 1/2K$. We are done. □

In case of good modelling, i.e. when A is a positive proportion of the group G, then there are only a bounded number of elements in the spectrum $S_\alpha(A)$. This observation will be key for finding a large generalized progression in the Bohr set obtained in the last proposition.

Lemma 7.5 (Few elements in large spectrum). *Suppose A is a subset of G such that $|A| \geqslant |G|/L$ and let $\alpha \in [0,1]$. Then $|S_\alpha(A)| \leqslant L/\alpha^2$.*

Proof. This follows easily from the Parseval formula. Write $\frac{1}{|G|}\sum_{\xi\in\widehat{G}} |\widehat{1_A}(\xi)|^2 = \sum_{x\in A} |1_A(x)|^2 = |A|$. Hence $|A| \geqslant \frac{1}{|G|}|S_\alpha(A)|\alpha^2|A|^2$, i.e. $|S_\alpha(A)| \leqslant |G|/(\alpha^2|A|) \leqslant L/\alpha^2$. □

We now need to understand the structure of Bohr sets and relate it to generalized arithmetic progressions.

Proposition 7.6 (Structure of Bohr sets). *Let $\alpha \in (0,1)$. Any Bohr set $B_\alpha(X) := \{x \in G, \Re\xi(x) > \alpha \text{ for all } \xi \in X\}$ contains a coset progression of rank $\leqslant |X|$ and size $\geqslant |G|\big(\frac{\sigma}{d^{3/2}}\big)^d$, where $\sigma = \arccos(\alpha)/2\pi \in (0,\frac{1}{2})$.*

Proof. This result is a rather simple application of Minkowski's second theorem on successive minimas of lattices in Euclidean space (see e.g. [?]). Let $X = \{\xi_1, ..., \xi_d\}$ and write $\xi = exp(2i\pi\sigma_i)$, where $\sigma_i : G \to \mathbb{R}/\mathbb{Z}$ is a homomorphism. Since the homomorphism $\pi_X : G \to \mathbb{R}^d/\mathbb{Z}^d, g \mapsto (\sigma_1(g), ..., \sigma_d(g))$ has finite image, its the inverse image in $\mathbb{R}^d$, i.e. the subgroup $\Delta := \pi_X(G) + \mathbb{Z}^d$ is a lattice (i.e. discrete subgroup of full rank) in $\mathbb{R}^d$. Note here that $vol(\mathbb{R}^d/\Delta) = 1/|\pi_X(G)|$.

Let $||v||$ be the Euclidean norm on $\mathbb{R}^d$ and $||v||_\infty$ the ℓ^∞-norm. Let $v_1, ..., v_d$ be a sequence of successive minimas in Δ, i.e. $||v_1|| = \inf\{||x||, x \in \Delta \setminus \{0\}\}$, $||v_2|| = \inf\{||x||, x \in \Delta \setminus \mathbb{R}v_1\}$, ..., $||v_d|| = \inf\{||x||, x \in \Delta \setminus \{\mathbb{R}v_1 + ... + \mathbb{R}v_{d-1}\}\}$. Then Minkowski's second theorem asserts that, although $\mathbb{Z}v_1 + ... + \mathbb{Z}v_d$ may not be all of Δ, it makes a subgroup of index at most $2^d/\gamma_d$, where $\gamma_d = vol(\{x, ||x|| \leqslant 1\})$, and in fact we even have $||v_1|| \cdot ... \cdot ||v_d|| \leqslant vol(\mathbb{R}^d/\Delta)2^d/\gamma_d$.

Let $\sigma = \arccos(\alpha)/2\pi \in (0,\frac{1}{2})$ so that $B_\alpha(X) = \{g \in G; |\sigma_i(g)| < \sigma \text{ for all } i = 1, ..., d\} = \{g \in G; ||\pi_X(g)||_\infty < \sigma\}$, where we have abused notations and wrote $\pi_X(g)$ for the unique representative of $\pi(g)$ in $\mathbb{R}^d$ with coordinates in $[-\frac{1}{2},\frac{1}{2})$.

For each $i = 1, ..., d$, let $L_i = \max\{n \in \mathbb{N}; ||nv_i||_\infty < \frac{\sigma}{d}\}$. It follows that $2L_i + 1 \geqslant \frac{\sigma}{d||v_i||_\infty} \geqslant \frac{\sigma}{d||v_i||}$.

Now let $P_c := \{g \in G, \pi_X(g) \in \sum_1^d[-L_i, L_i]v_i\}$. Then P_c is a coset progression (it is union of cosets of $\ker \pi_X$) and has size $\frac{|G|}{|\pi_X(G)|}\prod_1^d(2L_i+1)$. Moreover $P_c \subset B_\alpha(X)$.

By the above bound obtained from Minkowski's theorem, we have $\prod_1^d(2L_i+1) \geqslant \frac{\sigma^d}{\prod||v_i||} \geqslant |\pi_X(G)|\frac{\gamma_d}{2^d}\sigma^d$. An easy lower bound on γ_d is gotten by observing that the Euclidean ball of radius 1 contains the ℓ^∞ ball of radius $d^{-\frac{1}{2}}$, hence $\gamma_d \geqslant 2^d d^{-\frac{d}{2}}$. Finally we get $|P_c| \geqslant |G|\frac{\sigma^d}{d^{3d/2}}$ as desired.

□

Lemma 7.7 (Chang covering Lemma). *Let G be an abelian group, let $L \geqslant K$ and let A be a K-approximate subgroup of G and B a finite subset of G such that $|A+B| \leqslant L|B|$. Then $A \subset P+B-B$, where P is a symmetric generalized progression with rank $\leqslant 2K(\log_2 L+1)$ and side lengths $\leqslant 1$.*

Recall that the side lengths of a symmetric generalized progression P of rank d are the integers L_i's such that $P = \sum_1^d [-L_i, L_i]x_i$. Observe that an application of the Ruzsa covering lemma would only give $A \subset X+B-B$, for some set X of size $\leqslant L$. The Chang covering lemma thus assets that, under the assumption that A is a K-approximate group, we have can improve L into $\log L$, that is X can be taken to be a progression of rank $\leqslant 2K(\log_2 L+1)$.

Proof. Let $X_1 \subset A$ be a subset of A such that the $x+B$, $x \in X$ are disjoint and such that X_1 is maximal among subsets of size $\leqslant 2K$ in A. We let $B_1 = B + X_1$, and then build $X_2 \subset A$ such that the $x+B_1$, $x \in X_2$ are disjoint and such that X_2 is maximal among subsets of size $\leqslant 2K$ in A. We keep going this way and build $X_k \subset A$ and $B_k = B_{k-1} + X_k$. Let n be the first integer such that $|X_{n+1}| < 2K$.

Observe that by construction $|B_n| = |B_{n-1}||X_n| = ... = |B||X_1|...|X_n| = |B|(2K)^n$. However $B_n = B + X_1 + ... + X_n \subset B + nA$, and thus $|B_n| \leqslant |B+nA|$. However by the Ruzsa triangle inequality, $d(B, -nA) \leqslant d(B,-A) + d(-A,-nA)$, so $|B+nA||A| \leqslant |A+B||nA-A| \leqslant L|B|K^n|A|$. It follows that $(2K)^n|B| = |B_n| \leqslant |B_nA| \leqslant LK^n|B|$. Consequently $2^n \leqslant L$, i.e. $n \leqslant \log_2 L$.

By definition of X_{n+1}, for any $a \in A$, there is $x \in X_{n+1}$ such that $a + B_n$ intersects $x + B_n$ non trivially. This means $A \subset X_{n+1} + B_n - B_n \subset P + B - B$, where P is the symmetric generalized arithmetic progression $\sum_{x \in \cup_{i=1}^{n+1} X_i} [-1,1]x$. Its rank is clearly $\leqslant \sum_1^{n+1} |X_i| \leqslant (n+1)2K \leqslant 2K(\log_2 L + 1)$. We are done. □

We now pass to the conclusion of the proof of the Freiman-Ruzsa and Green-Ruzsa theorems. The last remaining step is to find a good model for A. This is provided by:

Proposition 7.8 (Passing to a good model). *Let $A \subset \mathbb{Z}$ be a K-approximate subgroup and let $k \geqslant 2$. Let p be a prime $\geqslant K^{4k}|A|$. Then there exists a symmetric subset Δ of A^2 with size $|\Delta| \geqslant |A|/8k$ and a Freiman k-isomorphism $\phi : \Delta \to \mathbb{Z}/p\mathbb{Z}$.*

Proof. The idea consists in "reshuffling" the set A by applying a suitable automorphism of $\mathbb{Z}/\ell\mathbb{Z}$, after viewing A as a subset of $\mathbb{Z}/\ell\mathbb{Z}$ for some sufficiently large prime ℓ, and then reduce modulo p.

Let ℓ be a very large prime, which we will fix so that no element in A^{2k} is a multiple of ℓ. Then reduction modulo ℓ is a Freiman k-isomorphism on A and abusing notation we will consider A as lying in $\mathbb{Z}/\ell\mathbb{Z}$. Let now $\psi : \mathbb{Z}/\ell\mathbb{Z} \to [-\frac{\ell-1}{2}, \frac{\ell-1}{2}] \subset \mathbb{Z}$ be the map assigning the remainder of the Euclidean division mod ℓ. Viewed as a map from $\mathbb{Z}/\ell\mathbb{Z}$ to $\mathbb{Z}$, this is not a homomorphism, but for every $k \geqslant 1$ it induces a Freiman k-isomorphism on the set $\psi^{-1}[-\frac{\ell-1}{4k}, \frac{\ell-1}{4k}]$. Let $\overline{\psi} : \mathbb{Z}/\ell\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ be the composition of ψ with the reduction modulo p. If $B \subset \mathbb{Z}/\ell\mathbb{Z}$ is a symmetric subset containing $\{0\}$, then we observe that $\overline{\psi}$ induces a Freiman k-isomorphism on B whenever $\psi(B) \subset [-\frac{\ell-1}{4k}, \frac{\ell-1}{4k}]$ and $\psi(B^{2k}) \cap p\mathbb{Z} = \{0\}$.

We now claim that if $p > |A^{4k}|$, then there exists $\alpha \in \mathbb{Z}/\ell\mathbb{Z}^*$ such that $\psi((\alpha A)^{4k}) \cap p\mathbb{Z} = \{0\}$. Indeed for every $x \in A^{4k} \setminus \{0\}$, the elements αx when α varies in $\mathbb{Z}/\ell\mathbb{Z}^*$

cover all of $\mathbb{Z}/\ell\mathbb{Z}^*$. On the other hand there are at most $\frac{\ell-1}{p}$ non zero multiples of p in $[-\frac{\ell-1}{2}, \frac{\ell-1}{2}]$ and thus at most $\frac{\ell-1}{p}$ elements $\alpha \in \mathbb{Z}/\ell\mathbb{Z}^*$ can possibly send αx on a multiple of p under the map ψ. Hence at most $|A^{4k}|\frac{\ell-1}{p}$ elements $\alpha \in \mathbb{Z}/\ell\mathbb{Z}^*$ could possibly have $\psi((\alpha A)^{4k}) \cap p\mathbb{Z} \neq \{0\}$. Since $p > |A^{4k}|$, the claim is proved.

By the pigeonhole principle, at least one of the $8k$ intervals of length $\ell/8k$ in $[-\frac{\ell-1}{2}, \frac{\ell-1}{2}]$ contains $\geqslant |A|/8k$ elements from $\psi(\alpha A)$. If I_k is this interval, set $\alpha\Delta = \alpha A \cap \psi^{-1}(I_k) - \alpha A \cap \psi^{-1}(I_k)$. Then $\Delta \subset A^2$, $|\Delta| \geqslant |A|/8k$, $\psi(\alpha\Delta) \subset [-\frac{\ell-1}{4k}, \frac{\ell-1}{4k}]$ and $\psi((\alpha\Delta)^{2k}) \cap p\mathbb{Z} = \{0\}$. Hence the composition ϕ of the automorphism α with $\overline{\psi}$ induces the desired Freiman k-isomorphism on Δ into $\mathbb{Z}/p\mathbb{Z}$. □

We can now conclude.

Proof of Theorem 7.1 Since the notions of a K-approximate group and that of a coset progression of rank d are both invariant under Freiman 2-homomorphism, we may assume applying Proposition 7.8 that $|G| \leqslant K^{O(1)}|A|$. It then follows from Lemma 7.5 that $|S_{1/2K}(A)| \leqslant d := K^{O(1)}$, and thus Propositions 7.4 and 7.6 say that A^4 contains a coset progression P_c of rank $O(K^{O(1)})$ and size at least $|G|/O(exp(K^{O(1)}))$. Finally Chang's covering lemma, Lemma 7.7, applied to $B = P_c$, implies that A is contained in a contained in a coset progression of rank $O(K^{O(1)})$ and size at most $O(exp(K^{O(1)}))|G|$. □

In the general abelian case, a substitute for the last proposition was proved by Green and Ruzsa.

Proposition 7.9 (Green-Ruzsa model theorem [19])**.** *Let A be a K-approximate subgroup of an abelian group G. Let $k \geqslant 2$ be an integer. Then there is a group G', with $|G'| \leqslant (10kK)^{10K^2}|A|$, such that A is Freiman s-isomorphic to a subset of G'.*

Although the bound here is worse than in Proposition 7.8, it can be combined with a Chang covering argument to yield a proof of Theorem 7.3. We will not prove this result here and rather refer the reader to the original paper.

8. Quasirandomness

One way to define a notion of quasirandomness for subsets of a finite group G, is to look at non trivial irreducible finite dimensional unitary representations π of G and consider the norm of the averaging operator $\frac{1}{|A|}\sum_{a\in A}\pi(a)$. If $A = G$, then this norm is 0 if whenever π is non trivial: this corresponds to saying that non trivial irreducible representations have no G-invariant vectors.

Definition 8.1 (Quasirandom set)**.** *We will say that a finite subset A of a finite group G is ε-quasirandom if $||\frac{1}{|A|}\sum_{a\in A}\pi(a)|| \leqslant \varepsilon|G|/|A|$ for every non trivial irreducible unitary representation of G.*

This terminology is justified by the following fact.

Proposition 8.2. *Let A be a random subset of a finite group G. Then for every $\varepsilon > 0$, the probability that A is ε-quasirandom tends to 1 as $|G|$ tends to infinity.*

Quasirandom sets tend to behave like random sets, in particular with respect to sumsets. The following is an illustration of this phenomenon (compare with Exercise 1.3).

Proposition 8.3. *Let $n \geqslant 3$. Suppose A is an ε-quasirandom subset of a finite group G such that $\varepsilon < (|A|/|G|)^{\frac{n-1}{n-2}}$. Then $A^n = G$.*

For the proof of the above two propositions, we will need to review some basic facts about non-abelian Fourier analysis on finite groups, which subsume our previous discussion of similar facts in the abelian setting in the last section. We let the unfamiliar reader check by himself the facts below and we refer him to [27] or any textbook on basic representation theory of finite groups.

If G is a finite group $\widehat{G}$ denotes the set of irreducible unitary representations of G. Since G is not assumed abelian, $\widehat{G}$ has no group structure, it is merely a finite set. The regular representation $\ell^2(G)$, defined by its action on functions $\rho(g)f : x \mapsto f(g^{-1}x)$, decomposes as a direct sum of subrepresentations

$$\ell^2(G) = \oplus_{\pi \in \widehat{G}} d_\pi V_\pi,$$

where V_π is a G-invariant subspace on which the G-action is isomorphic to the irreducible representation $\pi \in \widehat{G}$, and $d_\pi = \dim(V_\pi)$ is the dimension of this irreducible subrepresentation. Note that V_π appears with multiplicity equal to d_π in $\ell^2(G)$, and $d_\pi V_\pi$ is the *isotypic* component of $\ell^2(G)$ corresponding to π, i.e. the sum of the subrepresentations isomorphic to π.

Now the Fourier transform on G associates to every function f on G an irreducible representation $\pi \in \widehat{G}$, the linear operator $\widehat{f}(\pi) = \pi(f) : V_\pi \to V_\pi$ defined by

$$\widehat{f}(\pi) = \pi(f) = \sum_{g \in G} f(g)\pi(g).$$

The space $End(V_\pi)$ of endomorphisms of V_π, when endowed with the Hilbert-Schmidt scalar product $\langle A, B\rangle_{HS} := tr_{V_\pi}(AB^*)$, becomes isometric to the isotypic component of $\ell^2(G)$ corresponding to π via the map $A \mapsto (g \mapsto \langle A, \pi(g^{-1})\rangle_{HS})$.

The Fourier inversion formula now reads:

$$f(g) = \frac{1}{|G|} \sum_{\pi \in \widehat{G}} d_\pi tr_{V_\pi}(\widehat{f}(\pi)\pi(g^{-1})).$$

and the Parseval identity reads:

$$\sum_{g \in G} |f(g)|^2 = \frac{1}{|G|} \sum_{\pi \in \widehat{G}} d_\pi ||\widehat{f}(\pi)||_{HS}^2.$$

We also note that $\langle \pi(g)A, \pi(g)B\rangle_{HS} = \langle A, B\rangle_{HS}$, and that if $||A||_{op}$ denotes the operator norm of $A \in End(V_\pi)$ associated to the original Euclidean norm on V_π (coming from ℓ^2), then $||AB||_{HS} \leqslant ||A||_{op}||B||_{HS}$ and $||A||_{op} \leqslant ||A||_{HS}$ for every $A, B \in End(V_\pi)$.

Proof of Proposition 8.3 Let us convolve 1_A with itself n times. It is enough to show that $1_A * ... * 1_A(g) > 0$ for all $g \in G$. By the Fourier inversion formula, we have

$$1_A * ... * 1_A(g) = \frac{1}{|G|} \sum_{\pi \in \widehat{G}} d_\pi tr(\widehat{1_A}(\pi)^n \pi(g^{-1})) = \frac{|A|^n}{|G|} - \frac{1}{|G|} \sum_{\pi \neq 1} d_\pi \cdot \langle \widehat{1_A}(\pi)^{n-1}, (\pi(g)\widehat{1_A}(\pi))^*)\rangle_{HS},$$

while the right hand side can be bounded below by

$$\frac{|A|^n}{|G|} - \frac{1}{|G|} \sum_{\pi \neq 1} d_\pi \cdot ||\widehat{1_A}(\pi)^{n-1}||_{HS} ||\widehat{1_A}(\pi))||_{HS} \geqslant \frac{|A|^n}{|G|} - \frac{1}{|G|} \sum_{\pi \neq 1} d_\pi \cdot ||\widehat{1_A}(\pi)||_{op}^{n-2} ||\widehat{1_A}(\pi))||_{HS}^2.$$

Then applying the Parseval identity we get the lower bound

$$\frac{|A|^n}{|G|} - ||\widehat{1_A}(\pi)||_{op}^{n-2}|A| \geqslant \frac{|A|^n}{|G|} - (\varepsilon|G|)^{n-2}|A| \geqslant |G|^{n-2}|A|\big[(\frac{|A|}{|G|})^{n-1} - \varepsilon^{n-2}\big] > 0$$

□

Proof of Proposition 8.2 This follows from classical concentration of measure type bounds such as the Chernoff of Hoeffding inequalities. For instance, if E is say a Banach space and $X_1, ..., X_n$ are independent random variables taking values in the unit ball, and $S = X_1 + ... + X_n$, then it is known (see e.g. [22]) that $\mathcal{P}(||S|| \geqslant \mathbb{E}(||S||) + r) \leqslant \exp(-\frac{r^2}{8n})$ for every $r > 0$.

In our case the indicator function of a random subset A of G is $1_A = \sum_{g\in G} \varepsilon_g 1_{\{g\}}$, where the ε_g are Bernoulli random variables taking value 0 with probability $\frac{1}{2}$ and 1 with probability $\frac{1}{2}$. For $\pi \in \widehat{G}$, we have $\pi(1_A) = \sum_{g\in G} \varepsilon_g \pi(g)$, thus the random variables $\varepsilon_g\pi(g)$ are independent, take value in the unit ball of $End(V_\pi)$ endowed with the operator norm and satisfy $\mathbb{E}(\sum_g \varepsilon_g\pi(g)) = 0$ whenever $\pi \neq 1$. On the other hand $\mathbb{E}(||\pi(1_A)||) \leqslant \mathbb{E}(||\pi(1_A)||_{HS}) \leqslant \mathbb{E}(||\pi(1_A)||_{HS}^2)^{1/2}$. But one computes easily $\mathbb{E}(||\pi(1_A)||_{HS}^2) = \mathbb{E}(tr(\pi(1_A)\pi(1_A)^*)) = \sum_{g,h} \varepsilon_g\varepsilon_h tr(\pi(gh^{-1})) = \frac{1}{2}d_\pi|G|$.

On the other hand $\sum_{\pi\in\widehat{G}} d_\pi^2 = |G|$, so $d_\pi \leqslant \sqrt{|G|}$ and

$$\mathcal{P}(||\pi(1_A)|| > 2C\frac{\log^{1/2}|G|}{|G|^{1/4}}|G|) \leqslant \mathcal{P}(||\pi(1_A)|| > 2C\sqrt{d_\pi|G|\log|G|})$$

$$\leqslant \mathcal{P}\left(||\pi(1_A)|| > \mathbb{E}(||\pi(1_A)||) + C\sqrt{d_\pi|G|\log|G|}\right) \leqslant \exp(-\frac{C^2}{8}d_\pi \log|G|) \leqslant |G|^{-C^2/8},$$

where we applied the concentration of measure bound in the last line. In particular

$$\mathcal{P}\left(\max_{\pi\neq 1} ||\pi(1_A)|| > 2C\frac{\log^{1/2}|G|}{|G|^{1/4}}|G|\right) \leqslant |G|^{-(C^2-8)/8} \qquad (8.3.1)$$

□

In [15], Tim Gowers introduced a notion of quasirandomness for finite groups.

Definition 8.4 (Quasirandom group)**.** *A finite group G is said to be ε-quasirandom if every subset of G is ε-quasirandom in the sense of Definition 8.1.*

The following gives a handy characterization of quasirandom groups:

Proposition 8.5. *Let G be a finite group. Let $m(G) := \min_{\pi\in\widehat{G}} d_\pi$ be the smallest dimension of an irreducible representation of G. If $m(G) \geqslant \varepsilon^{-2}$, then G is ε-quasirandom. Conversely, if G is ε-quasirandom, then $m(G) \geqslant \left(\varepsilon^{-1}/(4\sqrt{2})\right)^{2/3}$.*

Proof. From the Parseval identity we have

$$|A| = ||1_A||_2^2 = \frac{1}{|G|}\sum_{\pi\in\widehat{G}} d_\pi \cdot ||\widehat{1_A}(\pi)||_{HS}^2 \geqslant \frac{1}{|G|}m(G)\max_{\pi\in\widehat{G}} ||\pi(1_A))||_{op}^2,$$

and hence $\max_{\pi\in\widehat{G}} ||\pi(1_A))||_{op} \leqslant \sqrt{\frac{|A||G|}{m(G)}} \leqslant \varepsilon|G|$ since $|A| \leqslant |G|$ and $m(G) \geqslant \varepsilon^{-2}$. Therefore G is ε-quasirandom.

Conversely, note that if π is a non trivial unitary representation of G with $\dim\pi = m = m(G)$, then, given a fixed unit vector v, the vectors $\pi(g)v$, $g \in G$ are unit vectors. Therefore for each of them, there is an index i, $1 \leqslant i \leqslant m = m(G)$ such that $|\langle \pi(g)v, e_i\rangle|^2 \geqslant 1/m$, in particular either the real part, its opposite, or the imaginary part, or its opposite is $\geqslant 1/\sqrt{2m}$. This makes $4m$ possibilities for $\pi(g)v$. By the pigeonhole principle, there must be some i and some subset $A \subset G$ of size $\geqslant |G|/4m$ such that, say $\Re\langle \pi(g)v, e_i\rangle \geq 1/\sqrt{2m}$ for all $g \in A$. This implies that $||\pi(1_A)||_{op} \geqslant |G|/(4m\sqrt{2m})$. If G is ε-quasirandom, this forces $m(G) \geqslant \left(\varepsilon^{-1}/(4\sqrt{2})\right)^{2/3}$. We are done. □

Corollary 8.6. *For any $n \geqslant 3$ and any subset A in G, we have: $|A| \geqslant |G|/m(G)^{1-\frac{2}{n}}$ implies $A^n = G$.*

Proof. This follows immediately from the combination of Propositions 8.3 and 8.5. □

Exercise 8.7. *Let G be a finite group and X,Y,Z finite subsets of G such that $|X||Y||Z| > \frac{|G|^3}{m(G)}$, where $m(G)$ is the smallest degree of a non trivial complex linear representation of G. Then there exists $x \in X$, $y \in Y$ and $z \in Z$ such that $z = xy$. Show that this implies $XYZ = G$.* *Hint: mimic the proof of Proposition 8.3*

Exercise 8.8. *Assuming that G is ε-quasirandom, improve the bound* (8.3.1) *obtained in the proof of Proposition 8.2.*

Every non abelian finite simple group is ε-quasirandom with $\varepsilon \to 0$ as $|G| \to \infty$. This follows directly from Jordan's theorem, according to which every finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ has a normal abelian subgroup of index bounded by a function of n only. From the classical bounds on Jordan's theorem due to Bieberbach and Frobenius (see e.g. [**?**]) one gets that $m(G) \gg (\log |G|)^{1/3}$. In fact, as Gowers shows in [15], the argument in the proof of Jordan's theorem gives $m(G) \geqslant \sqrt{\log |G|}/2$. Using the recent sharp bounds of Collins [**?**] on Jordan's theorem, one gets $m(G) \gg \log |G|/\log\log |G|$, which is sharp for the family of alternating groups $G = A_n$.

However, much better bounds are known for finite simple groups of Lie type. Landazuri and Seitz [20] showed that $m(G) \gg_d |G|^{r/d}$ for every finite simple group of Lie type with rank r and dimension d. Henceforth:

Theorem 8.9 (Landazuri-Seitz [20])**.** *If $G = \mathbf{G}(\mathbb{F}_q)$, where $\mathbf{G}$ is a simple algebraic group of dimension d defined over a finite field $\mathbb{F}_q$, then every projective complex linear representation of G has dimension $\gg_d q^r$, where r is the absolute rank of $\mathbf{G}$. In particular $m(G) \gg_d q^r$.*

We recall that algebraic groups are subgroups of GL_d defined by algebraic equations in the matrix entries and that simple algebraic groups are algebraic groups with no proper normal algebraic subgroups of positive dimension. The rank of a simple algebraic group is the dimension of its maximal tori (i.e. maximal diagonalizable algebraic subgroups).

We recall further that simple groups of Lie type are closely related to the groups of the form $\mathbf{G}(\mathbb{F}_q)$ considered above. In fact[4], they are obtained from $\mathbf{G}(\mathbb{F}_q)$ by taking the derived subgroup and passing to the quotient modulo the center. Hence Theorem 8.9 implies that $m(G) \gg_d q^r$ for every finite simple group of Lie type G.

[4] apart for the Suzuki and Ree family of finite simple groups, but these also verify the Landazuri-Seitz theorem, see [20]

In these notes we will just prove the following special case (a result dating back to Frobenius).

Proposition 8.10. *Let $\mathbb{F}_q$ be the finite field with q elements (q a prime power) and $G = \mathrm{PSL}_2(\mathbb{F}_q)$. Then $m(G) \geqslant \frac{q-1}{2}$.*

Proof. The main idea is that finite simple groups of Lie type have large unipotent subgroups, with even larger normalizers, while no such thing happens in $\mathrm{GL}_n(\mathbb{C})$. Let U be the subgroup of unipotent upper triangular matrices in G, and let $N(U)$ its normalizer. It is easy to see that $N(U)$ is the set of upper triangular matrices, that $U \simeq \mathbb{F}_q$ and that under this identification the conjugation action of $N(U)/U$ on U is multiplication by a square, i.e. $N(U)/U \simeq (\mathbb{F}_q^*)^2$. In particular every orbit of a non trivial element in U has cardinality precisely $\frac{q-1}{2}$.

Since G is simple, any non trivial linear representation of G over $\mathbb{C}$ is faithful and we may assume that $G \leqslant \mathrm{GL}_n(\mathbb{C})$. Now U is an abelian finite subgroup. Hence it is diagonalizable and we may write $\mathbb{C}^n = \oplus_\chi V_\chi$, where V_χ is the eigenspace (weight space) of U on $\mathbb{C}^n$ associated to the character $\chi : U \to \mathbb{C}^*$. Now $N(U)$ permutes the V_χ's and $gV_\chi = V_{g.\chi}$, where $g.\chi(\cdot) = \chi(g^{-1} \cdot g)$. Since $G \leqslant \mathrm{GL}_n(\mathbb{C})$, there must be at least one non trivial character χ occurring in this decomposition. By the observation in the previous paragraph, there must be at least $\frac{q-1}{2}$ different V_χ's that are permuted by $N(U)$. Hence $n \geqslant \frac{q-1}{2} \dim V_\chi \geqslant \frac{q-1}{2}$. We are done. □

Part 4. Approximate subgroups of linear groups and applications

In this chapter, we will present some recent results on the structure of approximate subgroup of linear groups. Given a field k, which we will assume algebraically closed without loss of generality, we will study approximate subgroups of $\mathrm{GL}_d(k)$, where d is fixed. We will also describe some applications to spectral properties of Cayley graphs of finite linear groups.

9. Approximate subgroups of simple algebraic groups

Our goal in this section will be to establish a structure theorem for approximate subgroups of simple algebraic groups (Theorem 9.1 below) over arbitrary fields. The first results of this kind were obtained by Elekes and Kirany [9] for SL_2 over the reals, then by Helfgott for SL_2 and SL_3 over a finite field of prime order [10, 11], and Dinai [8] over arbitrary finite fields. The general case presented here follows the recent works of Breuillard-Green-Tao [7] and Pyber-Szabo [24].

In order to formulate the result, it will be convenient to define a notion of complexity of algebraic varieties. There are several roughly equivalent ways to do so. Informally we will say that a closed subvariety of the affine space $\mathbb{A}^n$ has complexity at most $M \geqslant 1$ if $n \leqslant M$ and if it is the zero set of polynomials of degree at most M.

Theorem 9.1 (Structure of approximate subgroups of simple algebraic groups)**.** *Let $\mathbf{G}$ be a simple algebraic group over an algebraically closed field k. There is a constant $C = C(\dim \mathbf{G}) > 0$, independent of k, such that the following holds. Let $A \subset \mathbf{G}(k)$ be a K-approximate subgroup of $\mathbf{G}(k)$. Then one of the following holds*

(i) A is contained in a proper algebraic subgroup $\mathbf{H}(k)$ of complexity at most C,

(ii) $|A| \leqslant CK^C$,

(iii) $|\langle A\rangle| \leqslant CK^C|A|$.

The event (i) does not happen if, for example A generates a Zariski-dense subgroup of $\mathbf{G}$. Then event (ii) can of course happen, as any symmetric set containing 1 and of cardinality at most K is a K-approximate group. The third possibility, i.e. $|\langle A\rangle| \leqslant CK^C|A|$ implies that A generates a finite subgroup of $\mathbf{G}$ and that it is in fact a large proportion of that finite subgroup. The theorem can be paraphrased as saying that there are no dense approximate subgroups of simple algebraic groups: there are either stuck in a proper algebraic subgroup, or they are very close to genuine subgroups.

As a consequence, we derive the following result, which can be seen as an analogue of the sum-product theorem for simple algebraic groups.

Corollary 9.2 ([24], [7] Product theorem for simple algebraic groups)**.** *Let* $\mathbf{G}$ *be a center-free simple algebraic group over an algebraically closed field* k*. There are constants* $\varepsilon = \varepsilon(\dim \mathbf{G}) > 0, C = C(\dim \mathbf{G}) > 0$*, independent of* k*, such that the following holds. Any finite subset* A *of* $\mathbf{G}(k)$ *with* $1 \in A$ *is either contained in a proper algebraic subgroup* $\mathbf{H}(k) \leqslant \mathbf{G}(k)$ *of complexity at most* C*, or satisfies*

$$|AAA| \geqslant \min\{|A|^{1+\varepsilon}, |\langle A\rangle|\}.$$

We first derive the corollary and then pass to the proof of Theorem 9.1. The proof of the corollary depends on a deep structural result on finite subgroups of algebraic groups, which give now state.

This result was initially obtained by Weisfeiler using the classification of finite simple groups, but a beautiful and completely different classification-free proof was later found by Larsen and Pink [21].

Theorem 9.3 (Structure of finite subgroups of simple algebraic groups, [21])**.** *There is an absolute constant* $C = C(d) > 0$ *such that the following holds. Let* k *be an algebraically closed field and* $\mathbf{G}$ *a center-free simple algebraic group with* $\dim \mathbf{G} \leqslant d$*. Let* Γ *be a finite subgroup of* $\mathbf{G}(k)$*. Then either* Γ *is contained in a proper algebraic subgroup* $\mathbf{H}(k) \leqslant \mathbf{G}(k)$ *of complexity at most* C*, or char(k)=* $p > 1$ *and there is finite subfield* $\mathbb{F}_q$ *of* k *such that*

$$[\mathbf{G}(q), \mathbf{G}(q)] \subset \Gamma \subset \mathbf{G}(q),$$

where[5] $\mathbf{G}(q) = \mathbf{G}(\mathbb{F}_q)$*. Moreover* $[\mathbf{G}(q) : [\mathbf{G}(q), \mathbf{G}(q)]] \leqslant C$*.*

We recall (see [1], [28]), that simple algebraic groups over an algebraic closed field have a model defined over $\mathbb{Z}$. This allows to speak of the $\mathbb{F}_q$-points of $\mathbf{G}$ for any finite field $\mathbb{F}_q$.

Combining Theorem 9.3 with the Landazuri-Seitz theorem on the quasirandomness of simple groups of Lie type (Theorem 8.9) and Proposition 8.5, we conclude that either Γ is contained in a proper algebraic subgroup of bounded complexity, or Γ is $|\Gamma|^{-\eta}$-quasirandom in the sense of Definition 8.4 for some $\eta = \eta(d) > 0$.

We are now ready to deduce Corollary 9.2 from Theorem 9.1.

Proof of Corollary 9.2. Suppose $|AAA| \leqslant |A|^{1+\varepsilon}$. Setting $K = |A|^{\varepsilon}$, we see that A has tripling at most K, and therefore, applying Proposition 2.2, we get that

[5] If $p = 2$ and $\mathbf{G}$ is of type B_2 or F_4, or if $p = 3$ and $\mathbf{G}$ is of type G_2, then $\mathbf{G}(q)$ can have a slightly different definition (giving rise to the Suzuki and Ree groups) and be the set of fixed points of the composite of the Frobenius map $x \mapsto x^q$ and a certain non-standard isogeny arising in those cases only.

$B := (A \cup A^{-1} \cup \{1\})^2$ is a cK^c-approximate group, where $c > 0$ is an absolute constant. We may thus apply Theorem 9.1 and conclude that either B (hence A) is contained in a proper algebraic subgroup $\mathbf{H}(k) \leqslant \mathbf{G}(k)$ of complexity at most C, or $|A| \leqslant CK^C$, or $|\langle A\rangle| \leqslant CK^C|A|$. If we are in the case when $|A| \leqslant CK^C$, then $|A| \leqslant C|A|^{C\varepsilon}$. But choosing $\varepsilon \leqslant 1/2C$, this forces $|A| \leqslant C^2$. Hence if ε is small enough (depending on C only), then $|AAA| = |A|$, and thus $A = xH$ by Proposition 2.6, where H is a finite subgroup of size at most C^2. Since $1 \in A$, $A = H$ and hence we are back in the case when $|\langle A\rangle| \leqslant CK^C|A|$.

So we may assume that $|\langle A\rangle| \leqslant CK^C|A|$ and apply Theorem 9.3 to $\Gamma = \langle A\rangle$. By the remark following Theorem 9.3, we conclude that $\langle A\rangle$ is $|\langle A\rangle|^{-\eta}$-quasirandom for some $\eta = \eta(d) > 0$. Since $|A|/|\langle A\rangle| \geqslant 1/CK^C \geqslant 1/C|A|^{C\varepsilon} \geqslant 1/|\langle A\rangle|^{-\eta}$ for $\varepsilon > 0$ small enough, we get $A^3 = \langle A\rangle$ by Proposition 8.3. We are done. □

Exercise 9.4. *Recall that finite normal subgroups of center-free simple algebraic groups are trivial. Show that Corollary 9.2 continues to hold without the assumption $1 \in A$. Recall that the center of a simple algebraic group of dimension $\leqslant d$ is a finite group of order bounded in terms of d only. Show further that the assumption center-free can be removed as well.*

10. Notes

Apart from the original articles, many surveys and notes already exist in the literature on the above material. See for example Green's notes [16], [18], [17]. A basic reference is the book by Tao and Vu ([31]). Tao's weblog is also a very useful place to look for information on the topics of these lectures. These references as well as notes from a course taught at Princeton in 2006 by Elon Lindenstrauss have helped us a lot in writing the present notes.

- Sections 1 to 3. The definition of an approximate group is due to Tao (see [29]) and the Ruzsa lemmas (covering and inequality) described in Sections 2 and 3 can be found in this non-commutative setting in [29] or in Tao-Vu [31]. The new proof of the Plunnecke-Ruzsa estimates in the abelian case and the control of sets of small doubling by approximate groups given in these notes follow Petridis' recent paper [**?**]. The doubling $< \frac{3}{2}$ result dates back to Freiman and can be found on Tao's blog. The inheritance to subgroups lemma is implicit in [29] as is the closely related lemma about group actions.

- Sections 5 and 6. The sum-product theorem is due to Bourgain-Katz-Tao over $\mathbb{F}_p$. The statement for a general field can be found in Tao-Vu. See these references for a history of the sum-product phenomenon, which dates back to Erdos and Szemeredi. Although implicit in the proofs of the sum-product theorem, approximate fields have not been defined in the literature prior to these notes. Our approach however follows quite closely the original proof of Bourgain-Katz-Tao (in particular Lemma 5.5). The proof that approximate fields are controlled by genuine fields is close in spirit to [5], see also Tao-Vu [31]. The proof of the Katz-Tao lemma given in Lemma 6.3 is from [30]. Alternatively one can make use of the Balog-Szemeredi-Gowers theorem as in [6].

- Section 4. Good accounts on multiplicative energy and the Balog-Szemeredi-Gowers theorem can be found in Tao-Vu [31] and Green's notes [17]. Balog-Szemeredi proved Lemma 4.4 with worse bounds and Gowers gave a proof with polynomial bounds as stated in that lemma. Polynomial bounds are crucial for many applications. The non-commutative version of the Balog-Szemeredi-Gowers theorem and its corollaries (in particular Corollary 4.7) is due to Tao in [29].

- Section 8. The definition of quasirandomness for groups and results of this section are due to Gowers [15]. The short proof we give of Theorem 8.3 is inspired from a similar treatment of the abelian case in [31][Lemma 4.13].

References

[1] A. Borel, *Linear algebraic groups*, Springer.

[2] J. Bourgain and A. Gamburd, *Uniform expansion bounds for Cayley graphs of $SL_(\mathbb{F}_p)$*, Ann. Math. 167 (2008), 625–642.

[3] J. Bourgain and A. Gamburd, *On the spectral gap for finitely-generated subgroups of* SU(2), Invent. Math. 171 (2008), no. 1, 83121.

[4] J. Bourgain, A. Gamburd and P. Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math.

[5] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. (2) 73 (2006), no. 2, 380–398.

[6] J. Bourgain, N. H. Katz and T. C. Tao, *A sum-product estimate in nite elds and applications*, GAFA 14 (2004), no 1, 27-57.

[7] E. Breuillard, B. Green, T. Tao, *Approximate subgroups of linear groups*, to appear in G.A.F.A.

[8] O. Dinai, *Expansion properties of finite simple groups*, preprint, arXiv:1001.5069.

[9] Gy. Elekes and Z. Király, *On the combinatorics of projective mappings,* J. Algebraic Combin. **14** (2001), no. 3, 183–197.

[10] H. A. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. (2) **167** (2008), no. 2, 601–623.

[11] H. A. Helfgott, *Growth in* $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$, J. Eur. Math. Soc.

[12] G. Freiman, *Foundations of a structural theory of set addition*, Translations of Mathematical Monographs, Vol 37. AMS 1973.

[13] G. Freiman, *Groups and the inverse problems of additive number theory*, Kalinin Gos. Univ. Moskow 175–183 (1973)

[14] G. Freiman, *On finite subsets of nonabelian groups with small doubling*, preprint 2010.

[15] W. T. Gowers, *Quasirandom groups*, Combin. Probab. Comput. **17** (2008), no. 3, 363–387.

[16] B. J. Green, *Structure Theory of Set Addition*, Notes by B. J. Green, ICMS Instructional Conference in Combinatorial Aspects of Mathematical Analysis, Edinburgh 2002. Available from the B. Green's webpage.

[17] B. J. Green, *Additive Combinatorics*, Cambridge lecture notes 2009. Available from the B. Green's webpage.

[18] B. J. Green, *Approximate groups and their applications*, AMS Current Events Bulletin, 2010.

[19] B. J. Green and I. Z. Ruzsa, *Freiman's theorem in an arbitrary abelian group*, J. Lond. Math. Soc. (2) 75 (2007), no. 1, 163–175.

[20] V. Landazuri and G. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443.

[21] M. Larsen and R. Pink, *Finite subgroups of algebraic groups*, preprint (1995).

[22] M. Ledoux, *Concentration of measure.*

[23] G. Petridis, *New Proofs of Plunnecke-type Estimates for Product Sets in Groups,* preprint 2011, arXiv:1101.3507v2

[24] L. Pyber and E. Szabo *Growth in finite simple groups of Lie type*, preprint 2010.

[25] T. Sanders, *A Freiman-type theorem for locally compact abelian groups*, Ann. Inst. Fourier (Grenoble) 59 (2009), no. 4, 1321-1335.

[26] T. Sanders, *On the Bogolyubov-Ruzsa lemma*, preprint arXiv:1011.0107 .

[27] J. P. Serre, *Representations of finite groups*, springer.

[28] R. Steinberg, *Lectures on Chevalley groups*, Yale University notes.

[29] T. C Tao, *Product set estimates in noncommutative groups*, Combinatorica **28** (2008), 547–594.

[30] T. C Tao, *The sum-product phenomenom in arbitrary rings*, Contrib. Discrete Math. 4 (2009), no. 2, 5982.

[31] T. C. Tao and V. H. Vu, *Additive Combinatorics*, CUP 2006.

[32] T. C. Tao weblog.

Laboratoire de Mathématiques, Bâtiment 425, Université Paris Sud 11, 91405 Orsay, FRANCE

E-mail address: `emmanuel.breuillard@math.u-psud.fr`