CHAPTER 4

Expansion in $SL_2(q)$

4.1. Actions of groups

We have so far used basic facts about group theory without bothering explaining them. In beginning this chapter, however, we like to remind a few things, mainly related to actions, that are perhaps slightly more specialized and may not belong to anybody's background. We then prove some preliminary results of Helfgott's regarding actions in the perspective of set-products.

Actions. Let G be a group. An *action* of G on a non-empty set Ω is a map

$$\begin{array}{ccc} G\times\Omega & \to & \Omega \\ (g,x) & \mapsto & g\cdot x \end{array}$$

satisfying the following conditions:

(1) $1\cdot x = x$ for every $x\in\Omega$;

(2) $(g_1g_2)\cdot x = g_1\cdot(g_2\cdot x)$ for every $g_1,g_2\in G$, $x\in\Omega$.

Assume we are given such an action and let $g\in G$. If $x\in\Omega$ and $y=g^{-1}\cdot x$, then

$$g\cdot y = g\cdot(g^{-1}\cdot x) = (gg^{-1})\cdot x = 1\cdot x = x.$$

Next, suppose that, for some $x,y\in\Omega$, $g\cdot x = g\cdot y$; then

$$x = 1\cdot x = (g^{-1}g)\cdot x = g^{-1}\cdot(g\cdot x) = g^{-1}\cdot(g\cdot y) = (g^{-1}g)\cdot y = y.$$

This means that the map $\pi(g):\Omega\to\Omega$ defined by, for every $x\in\Omega$,

$$\pi(g)(x) = g\cdot x$$

is a permutation of Ω, that is $\pi(g)\in Sym(\Omega)$. Moreover, condition (2) implies that setting $g\mapsto\pi(g)$ defines a group homomorphism $\pi : G\to Sym(\Omega)$.

Conversely, if we are given a homomorphism $\pi : G\to Sym(\Omega)$ (this is called a permutation representation of G) then setting $g\cdot x = \pi(g)(x)$, for every $(g,x)\in G\times\Omega$, we obtain an action of G on Ω. Thus, we have two ways, the action map and the permutation representation, to look at the same thing, and we will adopt freely which one seems to be more convenient.

In particular, we say that our action is *faithful* if the kernel $\ker(\pi)$ of the permutation representation is trivial, or, equivalently if the only element $g\in G$ which fixes every $x\in\Omega$ that is $g\cdot x = x$ for every $x\in\Omega$, is the identity.

Given an action $G \times \Omega \to \Omega$, let $x \in \Omega$; if $\emptyset \neq A \subseteq G$ we set

$$A \cdot x = \{a \cdot x \mid a \in A\}.$$

In particular, $G \cdot x$ is called the *G-orbit* (or, simply, the orbit) of x. The *stabilizer* of x is the set

$$G_x = \{g \in G \mid g \cdot x = x\}.$$

It is a basic fact that G_x is a subgroup of G and that, if G is finite,

$$|G_x||G \cdot x| = |G|. \tag{4.1}$$

An action $G \times \Omega \to \Omega$ is *transitive* if for every $x, y \in \Omega$ there is a $g \in G$ such that $g \cdot x = y$ (this is equivalent to saying that Ω is a single G-orbit).

Exercise 33. Let $G \times \Omega \to \Omega$ be an action.

(1) Let $x, y \in \Omega$; prove that if x and y are in the same G-orbit, then G_x and G_y are conjugate.
(2) Let $|\Omega| \geq 3$; prove that the action is 2-transitive if and only if for every $x, y \in \Omega$, with $x \neq y$, one has $G_x \cdot y = \Omega \setminus \{x\}$.

A simple result of Helfgott generalizes the orbit-stabilizer principle (4.1) to non-empty subsets of G.

Proposition 4.1 (Helfgott [**17**]). *Let G be a group acting on a non-empty set Ω; let $x \in \Omega$ and G_x the stabilizer of x in G. Let A be a non-empty finite subset of G; then*

$$|A^{-1}A \cap G_x| \geq \frac{|A|}{|A \cdot x|}.$$

Moreover, for every $B \subseteq G$,

$$|AB^{-1}| \geq |A \cap G_x||B \cdot x|.$$

Proof. Let $\phi : A \to A \cdot x$ be the surjective map defined by $\phi(a) = a \cdot x$ for every $a \in A$. By the pigeon-hole principle there exists $a \cdot x \in A \cdot x$ such that

$$|\phi^{-1}(a \cdot x)| \geq |A|/|A \cdot x|.$$

Let $B = \phi^{-1}(a \cdot x) = \{b \in A \mid b \cdot x = a \cdot x\}$; then $a^{-1}B \subseteq A^{-1}A \cap G_x$, and so

$$|A^{-1}A \cap G_x| \geq |B| \geq \frac{|A|}{|A \cdot x|}.$$

For the second claim, let $B' \subseteq B$ such that $|B'| = |B \cdot x|$, and $b \cdot x \neq b_1 \cdot x$ for every $b, b_1 \in B'$ with $b \neq b_1$. Then the map $\phi : (A \cap G_x) \times B' \to AB^{-1}$, defined by $\phi(a, b) = ab^{-1}$, for all $(a, b) \in (A \cap G_x) \times B'$, is injective; in fact, if $\phi(a, b) = \phi(a_1, b_1)$ then $b^{-1}b_1 = a^{-1}a_1 \in G_x$, hence $b \cdot x = b_1 \cdot x$, ad so $b_1 = b$ and $a_1 = a$. Therefore,

$$|AB^{-1}| \geq |(A \cap G_x) \times B'| = |A \cap G_x||B \cdot x|.$$

■

Conjugation. Let G be any group; then a fundamental action of G on itself is that induced by conjugation. Given $x, g \in G$, the *conjugate* of x by g is

$$x^g := g^{-1}xg.$$

Fixed $g \in G$, it is immediate to check that conjugation by g defines an automorphism σ_g of G, where $\sigma_g(x) = x^g$, for all $x \in G$. Such automorphisms are called *inner automorphisms* of G; moreover the map $G \to Aut(G)$ defined by $g \mapsto \sigma_{g^{-1}}$, for every $g \in G$, is a group homomorphism.
This means that, by setting $g \cdot x = x^{g^{-1}}$, for all $g, x \in G$, we have an action $G \times G \to G$ (which is called, of course, conjugation action).
With respect to this action, the orbit of a $x \in G$ is the *conjugacy class*

$$x^G := \{x^g \mid g \in G\},$$

and the stabilizer of x in G is the *centralizer*

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

If G is finite, then the orbit-stabilizer equality (4.1) says that, for every $x \in G$,

$$|x^G| = [G : C_G(x)].$$

In general, for $H \leq G$ and X a nonempty subset of G, we let

$$C_H(X) = \{h \in H \mid hx = xh \ \forall x \in X\}.$$

It is straightforward to check that $C_H(X)$ is always a subgroup of G. $Z(G) = C_G(G)$ is called the *center* of G and its is a normal subgroup of G.

Conjugation in a group G induces in a natural way also an action of G on the set of all subgroups (or of all subsets) of G. If $X \subseteq G$ and $g \in G$, we let

$$g^{-1} \cdot X = X^g = \{x^g \mid x \in X\}.$$

X^g is just the image of X under the automorphism σ_g, hence $|X^g| = |X|$ and, if H is a subgroup of G, H^g is also subgroup. For $H \leq G$, the stabilizer of H with respect to the conjugation action is called the *normalizer*, $N_G(H)$, of H in G. Thus

$$N_G(H) = \{g \in G \mid H^g = H\},$$

and, if G is finite, the index $[G : N_G(H)]$ in G coincides with the number of distinct conjugates of H. Needles to say, a subgroup $H \leq G$ is normal if $N_G(H) = G$.
Let H, K be subgroups of G; in general, unless G is commutative (and a few other very restricted cases), HK is not a subgroup of G. However, if $K \subseteq N_G(H)$, then HK is a subgroup of G and, in this case, $HK = KH$ (in fact, this latter property is equivalent to $HK \leq G$).

Example 21. To our purposes, a significant example of group-action is that of the 2-dimensional *Special Linear Group* on the projective line.

Let $\mathbb{K}$ be a field, and $G = SL_2(\mathbb{K})$ the group of all invertible 2×2 matrices with entries in $\mathbb{K}$ and determinant 1; that is

$$SL_2(\mathbb{K}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Big| a, b, c, d \in \mathbb{K},\ ad - bc = 1 \right\}.$$

The natural action of $G = SL_2(\mathbb{K})$ on the vector space $V = \mathbb{K}^2$ induces a *sharply 2-transitive* action of G on the *projective line*

$$P(1, \mathbb{K}) = \{\mathbb{K}\mathbf{u} \mid 0 \neq \mathbf{u} \in V\}$$

(the set of all 1-dimensional subspaces of V), by the obvious rule

$$(g, \mathbb{K}\mathbf{u}) \mapsto \mathbb{K}g(\mathbf{u})$$

The kernel K of this action is the set of scalar matrices in G, hence $K = \{\pm I\}$. That the action is sharply 2-transitive means that for every two ordered pairs $(\mathbb{K}\mathbf{u}_1, \mathbb{K}\mathbf{u}_2)$ $(\mathbb{K}\mathbf{u}'_1, \mathbb{K}\mathbf{u}'_2)$, of points in $P(1, \mathbb{K})$, with $\mathbb{K}\mathbf{u}_1 \neq \mathbb{K}\mathbf{u}_2$ and $\mathbb{K}\mathbf{u}'_1 \neq \mathbb{K}\mathbf{u}'_2$, there exists *exactly one* element $gK \in G/K$ such that

$$g(\mathbb{K}\mathbf{u}_1) = \mathbb{K}\mathbf{u}'_1, \quad g(\mathbb{K}\mathbf{u}_2) = \mathbb{K}\mathbf{u}'_2. \tag{4.2}$$

This is the same than asking that $g \in G$ exists for every two ordered pairs of elements in $P(1, \mathbb{K})$ so that (4.2) is satisfied and no element $g \neq \pm I$ fixes more than two distinct elements in $P(1, \mathbb{K})$.

The same action may be understood by viewing $P(1, \mathbb{K})$ as the set obtained by adding to $\mathbb{K}$ an infinite element, thus letting $P(1, \mathbb{K}) = \mathbb{K} \cup \{\infty\}$; then the action is defined by associating to any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ the Moebius transformation

$$x \mapsto \frac{ax + b}{cx + d} \qquad (x \in P(1, \mathbb{K})).$$

Exercise 34. Prove the above statements about the action of $SL_2(\mathbb{K})$ on the projective line.

Actions on left cosets. There is another fundamental class of actions of G that are strictly linked to the group structure: the *actions on left cosets.* For a subgroup H of G we denote by $G\backslash H$ the set of all left cosets xH $(x \in G)$. There is then a natural action of G on $G\backslash H$ defined by left multiplication, that is, for every $g, x \in G$,

$$g \cdot (xH) = gxH. \tag{4.3}$$

These actions, for $H \leq G$, are transitive and for every $x \in G$, $G_{xH} = H^{x^{-1}}$.

By applying Proposition 4.1 in connection with such an action, we have a Lemma on set-products, that shows in particular that approximate subgroups behave well with respect to intersections with subgroups.

LEMMA 4.2 (Helfgott). *Let G be a group, H a subgroup, and A a finite non-empty symmetric subset of G. Then, for every $n \geq 1$,*

$$\frac{|A^{n+1}|}{|A|} \geq \frac{|A^n \cap H|}{|A^2 \cap H|}.$$

PROOF. We look at the left multiplication action of G on $\Omega = G\backslash H$, and we consider just the class $H = 1H \in \Omega$. Since, as mentioned above, the stabilizer in G of the class H is (the subgroup) H, by Proposition 4.1 we have

$$|A^2 \cap H| \geq |A|/|A \cdot H|. \tag{4.4}$$

(observe that $|A \cdot H|$ is the number of distinct left H-cosets that intersect A non trivially). Now, we prove the inequality. This is trivial for $n = 1$; for $n \geq 2$, we apply the second inequality in Proposition 4.1 and (4.4),

$$\frac{|A^{n+1}|}{|A|} = \frac{|A^n A|}{|A|} \geq \frac{|A^n \cap H||A \cdot H|}{|A|} \geq \frac{|A^n \cap H|}{|A^2 \cap H|}$$

and we are done. ■

4.2. Subgroups of $SL_2(\mathbb{K})$

For most of this section, we let $G = SL_2(\mathbb{K})$ (for a generic field $\mathbb{K}$). We first review a number of basic facts about G; some being straightforward, other requiring proofs that are not very difficult, and may be found in many textbooks.

- The identity 2×2 matrix is of course the identical element of G; we will often denote it simply by 1 (if no confusion with the unit element of $\mathbb{K}$ is likely to arise).
- The *center* $Z(G)$ of is composed only by the two scalar matrices:

$$Z(G) = \{1, -1\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

- The following fact, that we state without proof, is one of the important group theoretical features of these groups. Its proof is not particularly difficult and may be found in most introductory texts in group theory.

PROPOSITION 4.3. *If $|\mathbb{K}| \geq 4$ then the only normal subgroups of $G = SL_2(\mathbb{K})$ are the identity subgroup $\{1\}$, the center $Z(G)$, and G.*

- The quotient $PSL_2(\mathbb{K}) = G/Z(G)$ is called the *projective special 2-dimensional linear group* on $\mathbb{K}$; by the preceding Proposition, if $|\mathbb{K}| \geq 4$, $PSL_2(\mathbb{K})$ is a simple group.
- If $\mathbb{K} = \mathbb{F}_q$, the finite field of order q, for q a power of a prime, we write $G = SL_2(q)$. Then, one has

$$|SL_2(q)| = q(q^2 - 1). \tag{4.5}$$

In our approach it will be convenient to consider the algebraic closure $\overline{\mathbb{K}}$ of the field $\mathbb{K}$ (which, with an eye to our target, you may well think to be a finite field) and view naturally at $G = SL_2(\mathbb{K})$ as a subgroup of $\overline{G} = SL_2(\overline{\mathbb{K}})$.
This has, first of all, the advantage that every element g of $\overline{G}$ admits two (possibly equal) eigenvalues a_g, $a_g^{-1} \in \overline{\mathbb{K}}$, and allows to partition the set of elements of $\overline{G}$ in the following way.

Definition 4.4. Let g be an element of $\overline{G}$ and a_g, a_g^{-1} its eigenvalues in $\overline{\mathbb{K}}$; then

1. g is *unipotent* if $a_g = a_g^{-1} = 1$, while we say that g is *negative unipotent* if $a_g = a_g^{-1} = -1$;
2. g is *regular semisimple* if $a_g \neq a_g^{-1}$.

Thus, every element of $\overline{G}$ belongs to one and only one of these classes. A useful fact, that is however peculiar of dealing with matrices of order 2, is that one may distinguish those types just by looking at the trace $tr(g) = a_g + a_g^{-1}$. In fact, for $g \in \overline{G}$, g is unipotent if and only if $tr(g) = 2$, negative unipotent if and only if $tr(g) = -2$, and regular semisimple if and only if $tr(g) \neq \pm 2$.
Another peculiar property of SL_2, which is however very important in keeping the treatment at an elementary level, and may be easily proved by computation, is the fact that *two non-central elements g, h of $\overline{G}$ are conjugate in the group $\overline{G}$ if and only if $tr(g) = tr(h)$.*

Definition 4.5. Important classes of subgroups of $SL_2(\overline{\mathbb{K}})$ are the following

- *Unipotent subgroups*: all conjugates of

$$U(\overline{\mathbb{K}}) = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \Big| b \in \overline{\mathbb{K}} \right\}. \tag{4.6}$$

- *Maximal tori*: all conjugates of

$$T(\overline{\mathbb{K}}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \Big| 0 \neq a \in \overline{\mathbb{K}} \right\}. \tag{4.7}$$

- *Borel subgroups*: all conjugates of

$$B(\overline{\mathbb{K}}) = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \Big| a, b \in \overline{\mathbb{K}}\ a \neq 0 \right\}. \tag{4.8}$$

Then $U = U(\overline{\mathbb{K}})$ is isomorphic to the additive group of the field $\overline{\mathbb{K}}$, while $T = T(\overline{\mathbb{K}})$ is isomorphic to the multiplicative group $\overline{\mathbb{K}}^* = \overline{\mathbb{K}} \setminus \{0\}$, moreover, U is a normal subgroup of $B = B(\overline{\mathbb{K}})$ and $B = UT$.
We also define the *projective unipotent radicals* as all conjugates of $U_* = U_*(\overline{\mathbb{K}})$, which is in turn the set of all unipotent and negative unipotent elements in B; then $U_* = U \times Z(G) = U \cup (-U)$ is a normal subgroup of B; moreover, $U_* \cap H = Z(G)$.

Also, $N_{\overline{G}}(U) = N_{\overline{G}}(U_*) = N_{\overline{G}}(B) = B$; while $|N_{\overline{G}}(T) : T| = 2$ and $N_{\overline{G}}(T)/T$ (the Weyl group of $SL_2(\overline{K})$) is generated by Tw, where

$$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Observe also that the Borel subgroups are the stabilizer of a point in the action of $SL_2(\overline{\mathbb{K}})$ on the projective line $P(1, \overline{\mathbb{K}})$ (example 21), while the maximal tori are the (pointwise) stabilizers of two distinct points. From this fact, a number of immediate informations are easily available; for instance, we see that the intersection of two distinct maximal tori is the centre $Z(G)$, that of two distinct Borel subgroups is a maximal torus, or that every maximal torus is contained in exactly two Borel subgroups.

From this it follows that for every non-central element $u \in U_*$, $C_{\overline{G}}(u) = U_*$, and for every non-central (i.e. regular semisimple) element $g \in T$, $C_{\overline{G}}(g) = T$.

Exercise 35. Let $G = SL_2(\mathbb{K})$, U, H as defined in 4.4, and $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Prove that

$$g^H = \{g^{t^2} \mid t \in \mathbb{K}^*\}.$$

In particular, if q is a power of an odd prime and $\mathbb{K} = \mathbb{F}_q$, then $|g^U| = \frac{q-1}{2}$.

Exercise 36. Let p be a prime and $0 \neq t \in \mathbb{F}_p$. Prove that

$$\left\langle \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \right\rangle = SL_2(p).$$

Deduce that $SL_2(p)$ is generated by two conjugates of $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$.

In the theory of simple groups of Lie type, the following Lemma is a consequence of the fact that groups of type SL_2 have a BN-pair of rank 1 (see [**7**]); it is however easily proved by computation.

Lemma 4.6. *Let $\mathbb{K}$ be a field, $G = SL_2(\mathbb{K})$, $U = U(\mathbb{K})$ and $B = B(\mathbb{K})$. Then, for every $g \in G \setminus B$, G is the disjoint union*

$$G = B \cup UgB;$$

moreover the map $(u, b) \mapsto ugb$ is a bijection from $U \times B$ to $G \setminus B$.

Proof. We have

$$G \setminus B = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \middle| c \neq 0 \right\},$$

and, by computing the product

$$\begin{pmatrix} 1 & -ac^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -c & -d \\ 0 & -c^{-1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Thus $G \setminus B = UwB$, where $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and so $G \setminus B = UgB$ for every $g \in UwB = G \setminus B$.

For the final claim, just observe that, for any $g \in G \setminus B$, the map in the statement is surjective, and if $ugb = u_1gb_1$ for some $u, u_1 \in U$, $b, b_1 \in B$, then

$$g^{-1}u_1^{-1}ug = b_1b^{-1} \in B,$$

forcing $(u_1^{-1}u)^g \in B$. Since $g \notin B = N_G(U)$, this may only happen if $u_1^{-1}u = 1$. Then $b_1 = b$ follows, proving that our map is injective. ■

Corollary 4.7. *Let G, B, U be as in Lemma 4.6, and A a finite non-empty subset of G such that $A \nsubseteq B$. Then*

$$|A^3| \geq |A \cap U||A \cap B|.$$

Proof. By assumption, there is an element $g \in A \setminus B$. Then the claim follows from the last assertion in Lemma 4.6 and the fact that if $u \in A \cap U$ and $b \in A \cap B$ then $ugb \in A^3$. ■

Proposition 4.8. *Let S be a symmetrical subset of $\overline{G} = SL_2(\overline{\mathbb{K}})$. Then one of the following cases occurs*

(i) *S is contained in a Borel subgroup of G;*
(ii) *S^2 contains a regular semisimple element.*

Proof. By possibly conjugating in $\overline{G}$, we may well assume that S contains some non-central element of the standard Borel subgroup $B = B(\overline{\mathbb{K}})$, and at least one element $h \in \overline{G} \setminus B$, which we may also assume to be not regular semisimple. Thus, for some $0 \neq c \in \mathbb{K}$,

$$S \ni h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $tr(h) = \pm 2$. Let $U_* = U_*(\overline{\mathbb{K}})$, $Z = Z(\overline{G})$; since we may well assume that S does not contain any regular semisimple element of B, we have $B \cap A \subseteq U_*$, and so there exists $s \in (S \cap U_*) \setminus Z$; thus, for some $y \neq 0$,

$$s = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad s = \begin{pmatrix} -1 & y \\ 0 & -1 \end{pmatrix}.$$

In the first case, direct computation shows

$$tr(sh) = tr(h) + cy. \tag{4.9}$$

If $char(\mathbb{K}) = 2$, then we are done, as $tr(sh) = cy \neq 0$ and so sh has two distinct eigenvalues and is a regular semisimple element in S^2.

Let $char(\mathbb{K}) \neq 2$. Then, since $cy \neq 0$, it follows from (4.9) that $tr(sh) \in \{2, -2\}$ (that is, sh is not regular semisimple) if and only if

$$tr(sh) = tr(h) + cy = -tr(h). \tag{4.10}$$

Then, we consider the element $s^{-1}h \in S^2$, for which direct computation shows $tr(s^{-1}h) = tr(h) - cy$. Again, either $s^{-1}h$ is a regular semisimple element in S^2, or $tr(h) - cy = tr(s^{-1}h) = -tr(h)$. But this latter possibility is in contrast to (4.10) and $cy \neq 0$.

The case $s = \begin{pmatrix} -1 & y \\ 0 & -1 \end{pmatrix}$ is absolutely similar, hence we have the proof. ■

4.3. The product theorem in SL_2

In this section we prove the following fundamental result, which was first established by Helfgott in his groundbreaking paper [**17**], for $\mathbb{K}$ a field of prime order and a slightly weaker alternative instead of $A^3 = G$, and later extended to any finite field by Dinai [**10**].

Theorem 4.9. *There exists an absolute constant δ such that for every finite field $\mathbb{K}$ and every symmetric generating subset A of $G = SL_2(\mathbb{K})$ containing 1, either $A^3 = G$ or*

$$|A^3| \geq |A|^{1+\delta}.$$

In the case in which $\mathbb{K}$ has prime order, Kowalski [**23**] has proved that one my take $\delta = 1/3024$.

In fact, in order to have a statement more immediately providing the product condition as set in point (2) of Theorem 3.10, we prove the following approximate subgroup version.

Theorem 4.10. *There exists an absolute constant D such that for every finite field $\mathbb{K}$ and every $c \geq 2$, if A is c-approximate subgroup of $G = SL_2(\mathbb{K})$, then one of the following cases occurs:*

(i) $|A| \ll c^{\mathsf{D}}$;
(ii) $|A| \gg c^{-\mathsf{D}}|G|$;
(iii) $\langle A \rangle$ *is a proper subgroup of G.*

Let us see why Theorem 4.9 follows from Theorem 4.10. Let A be a generating symmetric subset of $G = SL_2(q)$ such that $A^3 \neq G$. Then by Gowers' trick (i.e. the Remark after Frobenius Theorem 3.13), $|A| \leq 2|G|^{8/9}$. Let $\delta = \frac{1}{9(1+5\mathsf{D})}$, and suppose, by contradiction, $|A^3| < |A|^{1+\delta}$. Then, by Lemma 1.39, A^2 is a c-approximate subgroup of G, for $c = |A|^{5\delta}$. Hence, assuming Theorem 4.10, we have

$$|A^3| \geq |A^2| \geq |A|^{-5\delta\mathsf{D}}|G| \geq |A|^{-5\delta\mathsf{D}}|A|^{10/9} = |A|^{1-5\delta\mathsf{D}+1/9} = |A|^{1+\delta},$$

which is a contradiction.

Exercise 37. Prove that Helfgott's Theorem 4.9 implies Theorem 4.10.

Proving Theorem 4.10. In the following three lemmas, A is a c-approximate subgroup (for some $c \geq 1$) of the group of $\overline{G} = SL_2(\overline{\mathbb{K}})$. The first of these results (called *non-concentration* property) is one of the bulks of the entire proof.

LEMMA 4.11. *There exist a constant $k \geq 1$ such that for every regular semisimple element x in $\overline{G}$,*

$$|A \cap x^{\overline{G}}| \ll c^k |A|^{\frac{2}{3}}.$$

PROOF. da scrivere. ■

DEFINITION 4.12. We say that a maximal torus T of $SL_2(\overline{\mathbb{K}})$ is *A-involved* if $A^2 \cap T$ contains a regular element.

LEMMA 4.13. *Let T be an A-involved torus. Then*

$$|A^2 \cap T| \gg c^{-(4k+2)} |A|^{\frac{1}{3}}.$$

PROOF. Let $T \leq \overline{G}$ be an A-involved torus, and let $x \in A^2 \cap T$ be a regular semisimple element. Since for every $a \in A$, $x^a = a^{-1}xa \in A^4$, by applying Lemma 4.11 to A^4 (remember from section 1.6 that A^4 is a c^4-approximate subgroup and $|A^4| \leq c^3|A|$), we have

$$|x^A| \leq |A^4 \cap x^{\overline{G}}| \ll c^{4k} |A^4|^{\frac{2}{3}} \leq c^{4k+2} |A|^{\frac{2}{3}}.$$

Now, the centralizer in $\overline{G}$ of x is T, and so, by considering the conjugation action, Lemma 4.1 yields

$$|A^2 \cap T| \geq \frac{|A|}{|x^A|} \gg c^{-(4k+2)} |A|^{\frac{1}{3}}.$$

■

LEMMA 4.14. *Let T be an A-involved torus, then either $|A| \ll c^{12k+18}$ or $T^a = a^{-1}Ta$ is an A-involved torus for every $a \in A$.*

PROOF. Let T be an A-involved torus and suppose that there exists $a \in A$ such that T^a is not A-involved. Then $|A^2 \cap T^a| \leq 2$. Also, by Lemma 4.13,

$$|A^4 \cap T^a| \geq |(A^2 \cap T)^a| = |A^2 \cap T| \gg c^{-k_1} |A|^{\frac{1}{3}},$$

with $k_1 = 4k + 2$, and so, by Lemma 4.2,

$$|A|^{\frac{1}{3}} \ll c^{k_1} |A^4 \cap T^a| \leq c^{k_1} \frac{|A^5|}{|A|} |A^2 \cap T^a| \leq c^{k_1+4} |A^2 \cap T^a| \leq 2c^{k_1+4},$$

whence $|A| \ll c^{12k+18}$. ■

We are now ready for the main result of this section.

PROOF OF THEOREM 4.10. Let q be the power of a prime, $G = SL_2(\mathbb{F}_q) = SL_2(q)$, and $\overline{G} = SL_2(\overline{\mathbb{F}_q})$.
Let $c \geq 2$ and A a c-approximate subgroup of G; suppose further that A generates G, so that case (iii) in the conclusions is ruled out from start.

Let $\mathsf{D} = 12k + 18$, where k is the constant in Lemma 4.11 and assume that we are not in case $|A| \ll c^{\mathsf{D}}$, where the implied constant is that arising in Lemma 4.14. Since A is not contained in a Borel subgroup of $\overline{G}$, there exists, by Proposition 4.8, an A^2-involved torus T of $\overline{G}$. Then, by Lemma 4.14 and the fact that $\langle A\rangle = G$, we immediately have that T^g is an A^2-involved torus for every $g \in G$. Moreover, by Lemma 4.13,

$$|A^4 \cap T^g| \gg c^{-(4k+2)}|A^2|^{\frac{1}{3}}, \tag{4.11}$$

for every $g \in G$.

Now, the number M of distinct G-conjugates of $G \cap T$ (which is properly larger than $Z(G)$) is either $q(q+1)/2$ or $q(q-1)/2$, accordingly to $G \cap T$ being of split type (i.e. diagonalizable in G) or of non-split type; in any case, $\mathsf{M} \gg |G|^{2/3}$.

Since each regular (that is non-central) semisimple element belongs to one and only one maximal torus, from (4.11) we obtain

$$c^2|A^2| \geq |A^4| \gg \mathsf{M}c^{-(4k+2)}|A^2|^{\frac{1}{3}} - 2\mathsf{M} \gg \mathsf{M}c^{-(4k+3)}|A^2|^{\frac{1}{3}},$$

and consequently,

$$c^{8/3}|A|^{2/3} \geq c^2|A^2|^{2/3} \gg \mathsf{M}c^{-(4k+3)} \gg c^{-(4k+3)}|G|^{\frac{2}{3}},$$

and finally

$$|A| \gg c^{-3(2k+3)}|G| \geq c^{-\mathsf{D}}|G|.$$

■

Remark. In a vague sense, this Theorem says that in groups of type SL_2 the interesting approximate subgroups (that is, neither too small or too big) are contained in a proper subgroup. To smooth further things, and make sure that, for groups of type SL_2, this provides axiom (2) in the Bourgain-Gamburd Theorem 3.10, let C_1 and C_2 be the two implicit constants in point (i) and (ii), respectively, of the statement of Theorem 4.10; we may replace the exponent constant D by D', where $\mathsf{D}' > \mathsf{D} + |\log_2 C_i|$, $i = 1, 2$, and deduce from Theorem 4.10 that for a c-approximate subgroup A of $G = SL_2(q)$ either A is contained in a proper subgroup of G, or $|A| <\leq c^{\mathsf{D}'}$, or $|A| > c^{-\mathsf{D}'}|G|$.

For any real number $\delta > 0$, we now put $c(\delta) = \delta/\mathsf{D}'$. Let $G = SL_2(q)$ for some prime power q, and let Q be a c-approximate subgroup of G, with $c = |G|^{c(\delta)}$ and such that

$$|G|^{\delta} \leq |Q| \leq |G|^{1-\delta}.$$

Then, $|Q| \geq |G|^{\delta} = c^{\mathsf{D}'}$ and $|Q| \leq |G|^{1-\delta} \leq c^{-\mathsf{D}'}$; hence by Theorem 4.10 (as restated above), Q is contained in a proper subgroup of G, and this is precisely axiom (2) in the Bourgain-Gamburd Machine.

We emphatize the fact that the function $\delta \mapsto c(\delta)$ depends only on the type SL_2 of the group and not on the size of the ground field.

4.4. Non-concentration in $SL_2(p)$

The first two requirements in the Bourgain-Gamburd machine (Theorem 3.10), queasirandomness and product theorem, are global properties of the considered group, while the third, non-concentration of probability distribution, depends in principle also on the symmetric generating set we are dealing with.
In this section, we establish a property of this kind for groups $SL_2(p)$, where p is a prime. This restriction allows to view our groups as quotients of the integral matrix group $SL_2(\mathbb{Z})$, and look at sets of generators that are, as p changes, homogeneous, in the sense that they are reductions modulo p of a suitable, and fixed, subset of integral matrices.

Another nice aspect we have in restricting to prime fields is the particularly simply description of proper subgroups. This goes back to Dickson.

Proposition 4.15 (Dickson, 1905). *Let $p \geq 5$ be a prime number and H a maximal subgroup of $G = SL_2(p)$. Then one of the following cases occurs:*

1. *H is a Borel subgroup of G;*
2. *H is the normalizer of a split or a non-split maximal torus;*
3. *$H/Z(G)$ is isomorphic to A_4, S_4 or A_5.*

Now, if H is a Borel subgroup of $G = SL_2(p)$, then $|H| = p(p-1)$ and H is the semi-direct product of the unipotent group U, which is isomorphic to the additive group of $\mathbb{F}_p$ by a split maximal torus, which is isomorphic to the multiplicative group $\mathbb{F}_p^*$. If H is as in point (2), then H is a dihedral group of order $2(p-1)$ (if it is the normalizer of a maximal split torus), or a dihedral group of order $2(p+1)$ (if it is the normalizer of a maximal non-split torus). Finally, if H is as in point (3) then $|H| \leq 120$. As an immediate consequence of Proposition 4.15 we have therefore the following useful information.

Corollary 4.16. *Let $p \geq 5$ be a prime number and H a proper subgroup of $SL_2(p)$. Then either $|H| \leq 120$ or H is metabelian, that is*

$$[[a, b], [c, d]] = 1$$

for every $a, b, c, d \in H$.

Given a prime p we denote by π_p the reduction mod p (which is a homomorphism):

$$\pi_p : SL_2(\mathbb{Z}) \to SL_2(p).$$

Exercise 38. Prove that

$$SL_2(\mathbb{Z}) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle.$$

Proposition 4.17. *The following facts hold.*

(1) *Let Γ_2 be the kernel of the reduction π_2, then*

$$\Gamma_2 = \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle \tag{4.12}$$

is a free group of rank 2.

(2) *Let H be a finitely generated subgroup of $SL_2(\mathbb{Z})$; then either H is soluble or has a subgroup of finite index which is a free group of rank $2 \leq k < \infty$.*

Proof. (1) Let H be the subgroup in right term of (4.12); clearly $H \leq \Gamma_2$. Write

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

so that $H = \langle x^2, y^2 \rangle$ and, by exercise 38, $\langle x, y \rangle = SL_2(\mathbb{Z})$. Then, one easily checks that $(x^2)^y, (y^2)^x \in H$, whence H is normal in $SL_2(\mathbb{Z})$. Now, x and y have order 2 modulo H, while

$$(xy)^3 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^3 = \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix} = x^2 y^{-2} x^{-2} y^2 \in H.$$

It follows that $SL_2(\mathbb{Z})/H$ is dihedral of order $6 = |SL_2(\mathbb{Z})/\Gamma_2|$, and so $H = \Gamma_2$.

(2) Let H be a finitely generated subgroup of $SL_2(\mathbb{Z})$, and $K = \Gamma_2 \cap H$. Then $H/K \simeq H\Gamma_2/\Gamma_2$ is isomorphic to a subgroup of $SL_2(2) \simeq S_3$; in particular we have $|H : K| \leq 6$. On the other hand, by Schreier Theorem (see [**8**] 7.7), K is a free group, and it is finitely generated being a finite-index subgroup of a finitely generated group (see [**8**] 6.1). Thus K is free of finite rank; if K is cyclic, H is soluble, and we are done. ■

We recall that every non-trivial subgroup of a free group is free (the Nielsen–Shreirer Theorem we already mentioned in the proof of Proposition 4.17); an easy corollary of this fact is that the centralizer $C_F(g)$, of any non-trivial element g in a free group F, is an infinite cyclic group.

Given a free group F with free generating set X (we then sometime write $F = F(X)$), and $|X| = k$, let $S = X \cup X^{-1}$ and consider the Cayley graph $\Gamma = \Gamma[F; S]$. Then Γ is the infinite regular tree T_{2k}, and for every $w \in F$, the distance in $d_\Gamma(1, w)$ coincides with the smallest length $\ell_S(w)$ of w as a word in the alphabet S. For $m \geq 0$ we write $B_S(m) = \{w \in F \mid \ell_S(w) \leq m\}$, the ball of radius m centered in 1.

We begin with an elementary remark.

Lemma 4.18. *Let $F = F(X)$ be a free group and $S = X \cup X^{-1}$. Then, if U is a cyclic subgroup of F and $m \geq 1$, $|U \cap B_S(m)| \leq 2m + 1$.*

Proof. Exercise. ■

LEMMA 4.19. *Let F, X and S be as in the previous Lemma; let $m \geq 1$ and $\emptyset \neq W \subseteq B_S(m)$. Suppose that*

$$[[x_1, x_2], [x_3, x_4]] = 1$$

for every $x_1, x_2, x_3, x_4 \in W$. Then

$$|W| \leq (4m+1)(8m+1) \leq 48m^2.$$

PROOF. Suppose first that $[x, y] = 1$ for every $x, y \in W$. Then the subgroup generated by W is abelian and therefore it is cyclic; the claim follows at once from Lemma 4.18.
Thus, let $a, b \in W$ be such that $u = [a, b] \neq 1$. Now, by assumption, $[u, [a, x]] = 1$ for every $x \in W$. Then, we have a map $\phi : W \to C_F(u)$ by setting, for every $x \in W$, $\phi(x) = [a, x]$. Observe that, because $a, x \in W \subseteq B_S(m)$, they both have S-length at most m, and so

$$[a, x] = a^{-1}x^{-1}ax \in B_S(4m).$$

Since $C_F(u)$ is cyclic, Lemma 4.18 yields

$$|\phi(W)| \leq 8m + 1. \tag{4.13}$$

Now, let $x, y \in W$ with $\phi(x) = \phi(y)$; then

$$a^x = a[a, x] = a[a, y] = a^y$$

and so $xy^{-1} \in C_F(a)$. But also $xy^{-1} \in WW^{-1} \subseteq B_S(2m)$. Since $C_F(a)$ is cyclic, by applying Lemma 4.18 again, we conclude that, for every $x \in W$, the inverse image $\phi^{-1}([a, x])$ contains at most $4m + 1$ elements. Together with (4.13), this gives the claimed inequality. ■

In the following, we write $G = SL_2(\mathbb{Z})$, and for every prime $p \geq 5$, $G_p = SL_2(p)$. As said, $\pi_p : G \to G_p$ is the projection modulo p.
We also fix a subset X of G, with $2 \leq |X| < \infty$, such that X is a set of free generators of a free group $\langle X \rangle \leq G$, let $S = X \cup X^{-1}$ and let $C = C(S)$ be as defined above. Finally, for every $p \geq 5$, we let $S_p = \pi_p(S)$ (observe that, as well as S in G, S_p is a symmetric subset of G_p).
Now, following an idea of Margulis, we are going to exploit the fact that, up to a certain distance from identity, the Cayley graph $\Gamma[G_p, S_p]$ looks like $\Gamma[\langle X \rangle, S]$ (Lemma 4.21 below), hence like a tree. Thus, the following calssical result of Kesten will be quite useful.

PROPOSITION 4.20 (Kesten [**22**]). *Let X be a free set of generators of the free group F_k of rank $k = |X|$, and $S = X \cup X^{-1}$. Denote by $\tilde{\nu}$ the probability distribution $\tau = |S|^{-1}\mathbf{1}_S$ on F_k. Then, for every $n \geq 1$ and $x \in F_k$,*

$$\tilde{\nu}^{(n)}(x) \leq r^{-n} \quad \textit{where} \quad r = \frac{k}{\sqrt{2k-1}}.$$

Now, consider a sub-multiplicative norm on the space of $n \times n$ matrices (we use in fact only the case $n = 2$); let us say the *maximum absolute row sum* norm

$$||a||_\infty = \max_{1 \leq i \leq n} \Bigl(\sum_{j=1}^{n} |a_{ij}| \Bigr). \tag{4.14}$$

Then, given a finite symmetric subset S of $SL_2(\mathbb{Z})$, we define $C = C(S) > 0$ by letting

$$C^{-1} = \log \bigl(\max_{s \in S} ||s||_\infty \bigr). \tag{4.15}$$

Lemma 4.21. *Let p be a prime, and r a positive integer with $r < C \log(p/2)$.*

1. *The reduction modulo p is injective in $B_S(r)$.*
2. *The subgraph induced by $B_S(r)$ in $\Gamma[G; S]$ is isomorphic to that induced by $B_{S_p}(r)$ in $\Gamma[G_p; S_p]$; in particular, both are trees.*
3. *$g(\Gamma[G_p; S_p]) \geq 2C \log(p/2)$.*

(See section 2.1 for the definition of the girth $g(\Gamma)$ of a graph Γ.)

Proof. (1) This is immediate from the sub-multiplicative property of the norm. In fact, if $s_1, \ldots, s_r \in S$ and $a = (a_{i,j}) = s_1 \cdots s_r$, then

$$\max |a_{i,j}| \leq ||s_1 \cdots s_r||_\infty \leq ||s_1||_\infty \cdots ||s_r||_\infty \leq e^{rC^{-1}} < p/2.$$

From this, it follows that if $a, b \in B_S(r)$, then $\pi_p(a) = \pi_p(b)$ if and only if $a = b$.

(2) Let Δ and Δ_p be, respectively, the subgraph induced by $B_S(r)$ in $\Gamma[G; S]$ and that induced by $B_{S_p}(r)$ in $\Gamma[G_p; S_p]$. Since the reduction π_p is a group homomorphism, we clearly have $\pi_p(B_S(r)) = B_{S_p}(r)$; then point (1) ensures that (the restriction of) π_p is a bijective map from the set of vertices of Δ and that of Δ_p. By the same reason (being a homomorphism), π_p preserves adjacency in both directions.

(3) This is left as an exercise; it follows easily from (2) and the fact (Proposition 2.10) that Cayley graphs are vertex-transitive. ■

Lemma 4.22. *Then there exist $0 < \gamma_1 < 1$, depending only on S, such that for any sufficiently large prime p*

$$\nu_p^{(n)}(x) \leq p^{-\gamma_1} \tag{4.16}$$

for every $x \in G_p$, with $n = \bigl[\frac{C}{16} \log(p/2)\bigr]$.

Proof. Let $p \geq 5$, $n = \bigl[\frac{C}{16} \log(p/2)\bigr]$, and $x \in G_p$. If $x \notin S_p^n$, then $\nu_p^{(n)}(x) = 0$. If $x \in S_p^n$, then $x = \pi_p(w)$ for some $w \in \langle X \rangle = F_k$; more precisely, $w \in B_S(n)$, the ball of radius n in F_k. Since $n \leq C \log(p/2)$, by Lemma 4.21 and Proposition 4.20, we have

$$\nu_p^{(n)}(x) = \tilde{\nu}^{(n)}(w) < r^{-n}. \tag{4.17}$$

where

$$r = \frac{k}{\sqrt{2k-1}} = \frac{|S|}{2\sqrt{|S|-1}}.$$

Now, fix γ_1 so that $0 < 2\gamma_1 \leq \min\left\{1, \frac{C}{16}\log r\right\}$. Then, since $n > \frac{C}{16}\log(p/2) - 1$, we have from (4.20),

$$\nu_p^{(n)}(x) < r^{-n} < r^{1-\frac{C}{16}\log(p/2)} < r\left(\frac{p}{2}\right)^{-\frac{C}{16}\log r} \leq \mathsf{M}p^{-2\gamma_1} \tag{4.18}$$

for some constant M depending only on S (via C and r). Thus, (4.16) holds for every $p \geq M^{\gamma_1^{-1}}$. ■

Lemma 4.23. *Then there exist* $0 < \gamma < 1$, *depending only on* S, *such that for any sufficiently large prime* p *and* $n = \left[\frac{C}{16}\log(p/2)\right]$,

$$\nu_p^{(n)}(H) \leq p^{-\gamma} \tag{4.19}$$

for every proper subgroup H *of* G_p.

Proof. Let H be a proper subgroup of G_p, and n as in the assumptions. Since $\nu_p^{(n)}$ is supported in S_p^n, by Lemma 4.22 we have

$$\nu_p^{(n)}(H) = \sum_{x \in H \cap S_p^n} \nu_p^{(n)}(x) \leq |H \cap S_p^n| p^{-\gamma_1}. \tag{4.20}$$

For $|H| \leq 120$, this does not have effect on the final estimate. Otherwise, by Corollary 4.16, $[[a,b],[c,d]] = 1$ for every $a, b, c, d \in H$.
Now, by Lemma 4.21, the reduction π_p is injective in the ball $B_S(r)$ of $\langle X\rangle = F_k$, for $r = 16n$. Let W be the inverse image in $B_S(r)$ of $H \cap S_p^n$; then, for every $x_1, x_2, x_3, x_4 \in W$, we have $\pi_p[[x_1,x_2],[x_3,x_4]] = 1$. But

$$\ell_S([[x_1,x_2],[x_3,x_4]]) \leq 16\max\{\ell_S(x_i) \mid i = 1,2,3,4\} \leq r,$$

and so $[[x_1,x_2],[x_3,x_4]] = 1$. Therefore, we may apply Lemma 4.19 to W, obtaining

$$|H \cap S_p^n| = |W| \leq 48n^2 \leq \frac{3}{16}C^2\log^2\frac{p}{2} \leq C^2\log^2\frac{p}{2}. \tag{4.21}$$

Then, let $k = [4\gamma_1^{-1}] + 1$, then, by a well known fact

$$\log^2(p/2) \leq k^2(p/2)^{2/k} \leq (k/2^{1/k})^2 p^{\gamma_1/2}.$$

From (4.20) and (4.21) we then have

$$\nu_p^{(n)}(H) \leq |H \cap S_p^n| p^{-\gamma_1} \leq C^2\log^2(p/2)p^{-\gamma_1} \leq \mathsf{M}p^{\gamma_1/2-\gamma_1} = \mathsf{M}p^{-\gamma_1/2},$$

$\gamma = \gamma_1/2$ where M a constant that ultimately depends only on S. For $p \geq \mathsf{M}^{4\gamma_1^{-1}}$, and $\gamma = \gamma_1/4$, we finally have

$$\nu_p^{(n)}(H) \leq p^{-\gamma},$$

for every proper subgroup H of G_p. ■

Observe that this implies, as a by-product, that for sufficiently large primes p, $S_p = \pi_p(S)$ is indeed a set of generators of the whole group $SL_2(p)$.

As said, with Lemma 4.23 we have finished verifying the properties needed to let the Bourgain-Gamburd machine work for the family of groups $SL_2(p)$.

THEOREM 4.24 (Bourgain, Gamburd). *Let X be a finite symmetric subset of $SL_2(\mathbb{Z})$ such that $\langle X \rangle$ is not soluble, and write $S = X \cup X^{-1}$. For any prime p let $\pi_p : SL_2(\mathbb{Z}) \to SL_2(p)$ denote the reduction modulo p. Then there exists a prime p_0 such that the family of Cayley graphs*

$$\Gamma[SL_2(p), \pi_p(S)], \quad p \geq p_0$$

is a family of expanders.

PROOF. We just need to show that, for the given X, the three assumptions in Theorem 3.10 are satisfied, for sufficiently large primes p, with the same parameters $0 < \kappa, \lambda < 1 < \Lambda$ and map $c(\delta)$, for every group $G_p := SL_2(p)$.

Property (3) we have just proved. In fact $|G_p| = p(p^2-1) < p^3$; hence, by letting $\Lambda = C$, with C as in (4.15), and $\lambda = \gamma/3$, with γ as in (4.19), for sufficiently large p, we have, by Lemma 4.23,

$$\nu_p^{(n)}(H) \leq p^{-\gamma} \leq |G_p|^{-\lambda}, \tag{4.22}$$

for every proper subgroup H of G_p.

Property (2) does not depend on X and follows from the product Theorem 4.10, as explained in the remark following the proof of it.

Property (1) is Frobenius Theorem 3.13; denoting by $d(G_p)$ the smallest degree of a non-trivial irreducible $\mathbb{C}$-representation of G_p, given any $0 < \beta < 1/3$ we have

$$d(G_p) \geq |G_p|^{\beta}$$

for p sufficiently large. Thus, parameters λ (in (4.22)) and κ to satisfy condition (1) in Theorem 3.10 may be easily fixed. ■

Diameter bounds.

Bibliography

[1] J. Bourgain, A. Gamburd, Uniform expansion bounds for Cayley graphs of $SL_2(\mathbb{F}_p)$, *Ann. of Math.* **167**, 625–642 (2008).

[2] E. Breuillard, Lectures on approximate groups and Hilbert's 5th problem. *E. Breuillard web page.*

[3] E. Breuillard, A brief introduction to approximate groups. *E. Breuillard web page.*

[4] E. Breuillard, Approximate subgroups and super-strong approximation. *Groups St Andrews 2013.* London Math. Soc. Lecture Notes, **422**, Cambridge Univ. Press, 2015.

[5] E. Breuillard, B. Green, T. Tao, The structure of approximate groups. *Publ. Math. Inst. Hautes Etudes Sci.* **116**, 115–221 (2012).

[6] E. Breuillard, B. Green, T. Tao, Small doubling in groups. *Erdös centennial, Bolyai Soc. Math. Stud.*, **25**, 129–151 (2013).

[7] R. W. Carter. Simple groups of Lie type. Pure and Applied Mathematics **28**, John Wiley & Sons, 1972.

[8] C. C.. Dispense corso Teoria dei Gruppi 2014.

[9] R. Diestel, Graph theory, volume 173 of Graduate Texts in Mathematics vol. 173. Springer-Verlag, 1997 (electronic edition 2000).

[10] O. Dinai, Growth in SL_2 over finite fields. *J. Group Theory*, **14**, 273–297 (2011).

[11] L. van den Dries, Approximate groups [according to Hrushovski and Breuillard, Green, Tao]. *Astrisque* No. 367-368, Exp. No. 1077, 79–113 (2015).

[12] G. A. Freiman, Foundations of a structural theory of set addition, *Translations of Mathematical Monographs* **37**, Amer. Math. Soc., Providence, RI, USA, 1973.

[13] W. T. Gowers, Quasirandom groups, *Comb. Probab. Comp.* **17**, 363–387 (2008).

[14] B. Green, Structure Theory of Set Addition. ICMS Instructional Conf. in Combinatorial Aspects of Mathematical Analysis, Edinburgh 2002.

[15] B. Green, I. Z. Ruzsa, Freiman's theorem in an arbitrary abelian group. *J. London Math. Soc.(2)* **75**, 163–175 (2007).

[16] P. Gruber, C.G. Lekkerkerker, Geometry of Numbers. North Holland, 1987.

[17] H.A. Helfgott, Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$. *Ann. of Math. (2)* **167**, 601–623 (2008).

[18] H.A. Helfgott, Growth in $SL_3(\mathbb{Z}/p\mathbb{Z})$. *J. Europ. Math. Soc.* **13**, 761–851 (2011).

[19] H.A. Helfgott, Growth in groups: ideas and perspectives. *Bull. Amer. Math. Soc.* **52**, 357–413 (2015).

[20] S. Hoory, N. Linial and A. Wigderson, Expander Graphs and their Applications. *Bull. Amer. Math. Soc.* **43**,439–561 (2006).

[21] E. Hrushovski, Stable group theory and approximate subgroups. *J. Amer. Math. Soc.* **25**,189–243 (2012).

[22] H. Kesten, Symmetric random walks on groups. *Trans. Amer. Math. Soc.* **92**, 336–354 (1959).

[23] E. Kowalski, Explicit growth and expansion in SL_2. *Int. Math. Res. Not. IMRN* **24**,5645–5708 (2013).

[24] A.W. Marcus, D.A. Spielman, N. Srivastava, Interlacing families I: bipartite Ramanujan graphs of all degrees. *Ann. of Math.* **182**, 307–325 (2012).

[25] M. B. Nathanson, Additive Number Theory. Inverse problems and the geometry of sumsets. Springer–Verlag, New York, 1996.

[26] N. Nikolov, L. Pyber, Product decomposition of quasirandom groups and a Jordan type theorem. *J. Europ. Math. Soc.* **13**, 1063–1077 (2011).

[27] G. Petridis, New proofs of Plünnecke-type estimates for product sets in groups. *Combinatorica* **32**, 721–733 (2012).

[28] L. Pyber, E. Szabó, Growth in finite simple groups of Lie type. *J. Amer. Math. Soc.* **29**, 95–146 (2016).

[29] O. Reingold, S. Vadhan, A. Wigderson, Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors *Proc. 41-st IEEE Symposium on Foundations of Computer Science*, 3–13 (2000).

[30] I. Z. Ruzsa, Generalized arithmetical progressions and sumsets, *Acta Math. Hungar.* **65**, 379–388 (1994).

[31] I. Z. Ruzsa, Sums of finite sets. In *Number theory* (New York, 1991–1995), 281–293. Springer, New York (1996).

[32] I. Z. Ruzsa, Sumsets and structure. Lecture Notes, 2008.

[33] T. Sanders, On the Bogolyubov–Ruzsa lemma. *Anal. PDE* **5**, 627–655 (2012).

[34] T. Tao, Product set estimates for non-commutative groups, *Combinatorica* **28**, 547–594 (2008).

[35] T. Tao, Expansion in Finite Simple Groups of Lie type. Graduate Studies in Mathematics, vol. 164. Springer, 2015.

[36] T. Tao, V. H. Vu, Additive Combinatorics. Cambridge University Press, 2006.