

TRAVAUX DE HELFGOTT SUR LA GÉNÉRATION DE $SL_2(\mathbb{F}_p)$.

NALINI ANANTHARAMAN

1. RÉSULTATS.

Theorem 1.1 (Main theorem). *Il existe C tel que, pour tout p premier, pour tout A système générateur de $G = SL_2(\mathbb{F}_p)$, le diamètre du graphe de Cayley $\Gamma(G, A)$ soit inférieur à $C(\log p)^C$.*

Proposition 1.2 (Key proposition). *(a) Pour tout $\delta > 0$, il existe $c, \epsilon > 0$ tel que, pour tout p , pour tout A système générateur de $SL_2(\mathbb{F}_p)$,*

$$|A| < p^{3-\delta} \Rightarrow |A.A.A| > c|A|^{1+\epsilon}.$$

(b) Pour tout $\delta > 0$, il existe un entier k tel que, pour tout p , pour tout A système générateur de $SL_2(\mathbb{F}_p)$ tel que $|A| > p^\delta$, tout élément de $SL_2(\mathbb{F}_p)$ peut s'exprimer comme produit d'au plus k éléments de A .

Helfgott démontre aussi :

Corollary 1 (Corollaire 6.3). Soit A un sous-ensemble de $SL_2(\mathbb{Z})$ engendrant un groupe libre (plutôt : il n'existe pas de relation entre les éléments de A). [On peut même supposer que A engendre un sous-groupe non élémentaire]

Il existe $C = C(A)$ tel que, pour tout p tel que \bar{A} engendre $SL_2(\mathbb{F}_p)$, on ait

$$\text{diam } \Gamma(SL_2(\mathbb{F}_p), \bar{A}) \leq C \log p.$$

Corollary 2. On considère \mathcal{C}_p , l'ensemble des paires (g, h) génératrices de $SL_2(\mathbb{F}_p)$, muni de la probabilité uniforme \mathbb{P}_p . Il existe $C > 0$ tel que

$$\mathbb{P}_p\{\text{diam } \Gamma(SL_2(\mathbb{F}_p), (g, h)) > C \log p\} \xrightarrow{p \rightarrow +\infty} 0.$$

2. UNE NOTATION.

$$A^r = \{x^r, x \in A\},$$

$$A_r = \{x_1.x_2.\dots.x_r, x_i \in A \cup A^{-1} \cup \{1\}\}.$$

Notons que $A_r \subset A_{r+1}$, et $A_{p+q} = A_p.A_q$, $A_{pq} = [A_p]_q$.

3. PRÉREQUIS POUR CET EXPOSÉ.

On admet ici les résultats suivants, qui ont déjà été démontrés lors d'exposés antérieurs :

Theorem 3.1 (Bourgain–Katz–Tao, Konyagin, Freiman). *Pour tout $\delta > 0$, il existe $C, \epsilon > 0$ tel que, pour tout premier p , pour tout $q = p^\alpha$, pour tout $A \subset \mathbb{F}_q^*$,*

$$C < |A| < p^{1-\delta} \Rightarrow \max(|A.A|, |A + A|) > |A|^{1+\epsilon}.$$

On rappelle aussi

Theorem 3.2. *Soit G un groupe commutatif et $d(A, B) = \log \frac{|AB^{-1}|}{\sqrt{|A|}\sqrt{|B|}}$ la "distance" de Ruzsa entre sous-ensembles finis de G . On a*

$$d(A, B^{-1}) \leq 4d(A, B).$$

C'est une conséquence directe du théorème C des notes d'Olivier.

On utilise enfin un résultat technique dû à Gowers ("version quantitative du théorème de Balog–Szemerédi") :

Theorem 3.3. *Il existe $c, C > 0$ tel que, pour tout groupe abélien G , pour tout A sous-ensemble fini de G , pour tout $K > 0$, s'il existe $S \subset A \times A$ tel que $|S| \geq |A|^2/K$ et $\{a + b, (a, b) \in S\} \leq K|A|$, alors il existe $A' \subset A$ tel que $|A'| \geq cK^{-C}|A|$ et*

$$|A' + A'| \leq CK^C|A|.$$

Preuve. C'est une conséquence du théorème A démontré par Olivier. En effet, la partie (ii) \Rightarrow (iii) dit qu'il existe $A', B' \subset A$ avec $|A'|, |B'| \geq cK^{-C}|A|$ et $|A' + B'| \leq CK^C|A|$. Par le principe des tiroirs, il doit exister $z \in A' + B'$ tel que $a + b = z$ a au moins $(CK^{-C})^2(cK^C)^{-1} = C^{-1}c^2K^{-3C}|A|$ couples $(a, b) \in A' \times B'$.

On définit $V = A' \subset (z - B')$, de sorte que $|V| \geq C^{-1}c^2K^{-3C}|A|$. On a $V - V \subset A' + B' - z$, donc $|V - V| \leq CK^C|A|$, puis en utilisant $d(V, -V) \leq 4d(V, V)$ on en déduit $|V + V| \leq C^8c^{-8}K^{16C}|A|$.

4. PLAN DE LA PREUVE.

4.1. Simplification préliminaire.

Lemma 4.1 (Lemme 2.2). *Soit $n > 2$ un entier. Soit A un sous-ensemble fini d'un groupe G . Supposons que*

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

Alors

$$|A.A.A| > c'|A|^{1+\epsilon'}$$

où $c' > 0, \epsilon' > 0$ ne dépendent que de c, ϵ, n (pas de G ni de A).

C'est le théorème D démontré par Olivier.

Donc, il nous suffira de trouver un n tel que A_n croisse suffisamment.

4.2. Comme conséquence des estimées somme-produit on déduit la Proposition suivante. **C'est le seul endroit où les résultats admis de la Section 3 sont utilisés, tout le reste est "self-contained".**

Proposition 4.2. [Proposition 3.3] Soit $q = p^\alpha$. Soit $\delta > 0$ et $a_1, a_2 \in \mathbb{F}_q^*$ donnés. Alors, pour tout $A \in \mathbb{F}_q^*$ tel que $C < |A| < p^{1-\delta}$, on a

$$|\{a_1(xy + x^{-1}y^{-1}) + a_2(x^{-1}y + xy^{-1}) : x, y \in A_{20}\}| > |A|^{1+\epsilon}$$

où $C > 0$, $\epsilon > 0$ ne dépendent que de δ (et pas de p^α).

Interprétation : La trace d'un produit de la forme

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

(a, b, c, d tous non nuls) est $ad(xy + x^{-1}y^{-1}) - bc(x^{-1}y + xy^{-1})$. On va se servir de la Proposition 4.2 pour montrer que $|Tr(A_k)|$ est grand pour k grand, puis on aura besoin de savoir comparer $|Tr(A_k)|$ et $|A_{k'}|$.

Les nombres x, y seront des valeurs propres d'un sous-ensemble de A , formé de matrices simultanément diagonalisables, et seront dans un corps isomorphe à \mathbb{F}_{p^2} . Autrement dit, la Proposition 4.2 sera appliquée dans le cas $p^\alpha = p^2$.

Remark 4.3. Sans utiliser [BKT] on a déjà la Proposition suivante [4.10] : Il existe C, c, k tels que, pour tout corps K de cardinal $|K| > C$, pour tout A sous-ensemble fini de $SL_2(K)$ qui n'est pas contenu dans un sous-groupe propre de $SL_2(K)$, on ait

$$(4.1) \quad |Tr(A_k)| \geq c|A|^{1/3}.$$

Helgott sait aussi montrer [Prop 4.8] qu'il existe k tel que

$$(4.2) \quad |A_k| \geq C \frac{|Tr(A)|^3 |A|^3}{|A_6|^3}$$

dès que $|A|$, $|Tr(A)|$ et $\frac{|Tr(A)||A|}{|A_6|}$ sont chacun assez grands, mettons ≥ 1000 (et A pas contenu dans un sous-groupe propre). Donc, sans utiliser la Proposition 4.2 [BKT], on sait déjà que

$$|A_{k^2}| \geq C \frac{|A|^3}{|A_{6k}|^3} |A|.$$

Pour pouvoir conclure il faudrait pouvoir améliorer ce résultat en quelque chose du genre

$$|A_k| \geq C \frac{|A|^\beta}{|A_{k'}|^\beta} |A|^{1+\epsilon}.$$

Autrement dit on veut essentiellement améliorer la puissance de $|A|$ dans (4.1), et c'est à ça que sert la Proposition 4.2.

Pour pouvoir utiliser la Proposition 4.2 qui dit que $|Tr(A_k)|$ croît plus vite que prévu, il faut trouver à la fois :

- un gros sous-ensemble de A formé de matrices simultanément diagonalisables;

– une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dont toutes les entrées sont non nulles (dans la base qui diagonalise les matrices précédentes !).

4.3. Où l'on cherche un sous-ensemble de A formé de matrices simultanément diagonalisables.

Proposition 4.4 (Corollaire 4.3). *Soit K un corps, soit A un sous-ensemble fini de $SL_2(K)$ non contenu dans un sous-groupe propre. Supposons que $|Tr(A)| \geq 2$, $|A| \geq 4$. Alors il y a un sous-ensemble $V \subset A_4$, formé de matrices simultanément diagonalisables, et de cardinal*

$$\frac{(\frac{1}{2}|Tr(A)| - 2)(\frac{1}{4}|A| - 1)}{|A_6|}.$$

4.4. Où l'on cherche une matrice de A dont les entrées sont toutes non nulles.

Helgott démontre le Lemme suivant, dans un cadre très général :

Lemma 4.5 (Escaping from subvarieties). *Soit G un groupe agissant linéairement sur un espace vectoriel V , défini sur un corps K . Soit $W = W_1 \cup \dots \cup W_n$ une union de sous-espaces vectoriels stricts de V .*

Soit A un sous-ensemble de G , et soit \mathcal{O} une orbite de $\langle A \rangle$ dans V . Alors il existe $\eta > 0$ et $m \in \mathbb{N}$, de dépendant que de n et de $d = \dim V$ tels que, pour tout $x \in \mathcal{O}$, il existe au moins $\max(1, \eta|A|)$ éléments $g \in A_m$ tels que $gx \notin W$.

Corollary 3. Soit K un corps tel que $|K| > 3$, soit A un sous-ensemble fini de $SL_2(K)$ non contenu dans un sous-groupe propre. Soit \bar{K} une extension de K . Alors pour tout base (v_1, v_2) de \bar{K}^2 , il existe $g \in A_k$ tel que $gv_i \neq \lambda v_j$ pour tout $\lambda \in \bar{K}$, $i, j \in \{1, 2\}$. L'entier k est indépendant de K et de A .

Preuve. On fait agir $G = SL(2, K)$ par multiplication à gauche sur $V = M_2(\bar{K})$. L'ensemble W est l'ensemble des matrices h telles que $hv_i \neq \lambda v_j$ pour un $\lambda \in \bar{K}$, $i, j \in \{1, 2\}$. On part de $x = I \in W$, on considère $\mathcal{O} = SL(2, K)$ l'orbite de l'identité.

Il faut vérifier que \mathcal{O} n'est pas inclus dans W . On va le faire en comptant le nombre d'éléments de ces deux ensembles. On a $|\mathcal{O}| = |K|(|K|^2 - 1)$.

Par ailleurs $\mathcal{O} \cap W = G_{1,1} \cup G_{1,2} \cup G_{2,1} \cup G_{2,2}$. Soit $g \in G_{i,j}$, et soit $v \in K^2$ (par exemple l'un des vecteurs de la base canonique) linéairement indépendant de v_i . La matrice g est entièrement déterminée par gv_i et gv , et en fait uniquement par gv à cause du déterminant. On en déduit que $|G_{i,j}| \leq |K|^2 - 1$.

Dès que $4(|K|^2 - 1) - 1 < |K|(|K|^2 - 1)$ on peut conclure que \mathcal{O} n'est pas inclus dans W .

Corollary 4. Soit K un corps, soit A un sous-ensemble fini de $SL_2(K)$ non contenu dans un sous-groupe propre. Il existe $k, c > 0$ indépendants de K et de A tels que, pour tous vecteurs non-nuls $v_1, v_2 \in \bar{K}^2$,

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

où l'on a noté H_v les matrices de $M_2(\bar{K})$ qui ont v comme vecteur propre.

Preuve. Là encore il faut vérifier que $SL(2, K)$ n'est pas inclus dans $W = H_{v_1} \cup H_{v_2}$. Mais il n'est pas possible que les trois matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ soient dans W .

Ce deuxième corollaire interviendra uniquement dans la preuve de (4.1).

4.5. Fin de la preuve de (a). – On peut toujours supposer p et $|A|$ assez grand.

– Je n'écris pas les constantes multiplicatives qui apparaissent dans toutes les inégalités.

L'inégalité (4.1) donne k_0 tel que $|Tr(A_{k_0})| \geq |A|^{1/3}$.

La Proposition 4.4 nous donne un sous-ensemble de A_{4k_0} , simultanément diagonalisable, de cardinal

$$\frac{|A|^{1/3}|A_{k_0}|}{|A_{6k_0}|}.$$

On appelle $V \subset \mathbb{F}_{p^2}$ l'ensemble des valeurs propres associées. On a $|V| \leq |A|^{1/3} \leq p^{1-\delta/3}$. Par ailleurs on peut toujours supposer $|A_{6k_0}| < |A|^{7/6}$ et donc $|V| \geq |A|^{1/6}$.

Dans la base qui diagonalise les matrices précédentes (sur \mathbb{F}_{p^2}), il existe $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in A_{k_1}$ telle que $abcd \neq 0$. La Proposition 4.2 et les remarques qui suivent sont alors utilisées pour montrer que

$$(4.3) \quad |Tr(A_{160k_0+2k_1})| \geq |V|^{1+\epsilon}.$$

On peut toujours supposer que

$$(4.4) \quad \frac{|Tr(A_{160k_0+2k_1})||A_{160k_0+2k_1}|}{|A_{6(160k_0+2k_1)}|} \geq 1000.$$

En effet, si ce n'est pas le cas, alors on a, ou bien $|A_{6(160k_0+2k_1)}| \geq |A|^{1+\epsilon/16}$ et on a terminé, ou bien $|Tr(A_{160k_0+2k_1})| \leq 1000|A|^{\epsilon/16}$, mais ce dernier cas est incompatible avec (4.3) si ϵ a été pris assez petit.

Une fois supposé (4.4), on peut alors utiliser (4.2) pour écrire

$$\begin{aligned} |A_{k_2(160k_0+2k_1)}| &\geq \frac{|Tr(A_{160k_0+2k_1})|^3 |A_{160k_0+2k_1}|^3}{|A_{6(160k_0+2k_1)}|^3} \geq \frac{|A_{160k_0+2k_1}|^3}{|A_{6(160k_0+2k_1)}|^3} |V|^{3(1+\epsilon)} \\ &\geq \frac{|A_{160k_0+2k_1}|^3}{|A_{6(160k_0+2k_1)}|^3} \frac{|A_{k_0}|^3}{|A_{6k_0}|^3} |A|^{1+\epsilon} \geq \frac{|A|^6}{|A_{6(160k_0+2k_1)}|^6} |A|^{1+\epsilon} \end{aligned}$$

(à la fin on a juste utilisé $|A_k| \leq |A_{k+1}|$). C'est fini : soit $|A_{k_2(160k_0+2k_1)}|$, soit $|A_{6(160k_0+2k_1)}|$ est supérieur à $|A|^{1+\epsilon/7}$.

4.6. Preuve de (b). [D'après Nikolov et Pyber]

Soit A tel que $|A| > p^\delta$. D'après (a), tant que $|A^{3^k}| < p^{3-\delta}$, on a $|A^{3^k}| > (c|A|)^{(1+\epsilon)^k}$. Donc, dès que $(cp^\delta)^{(1+\epsilon)^k} > p^{3-\delta}$ on doit aussi avoir $|A^{3^k}| > p^{3-\delta}$. Par conséquent, il existe K ne dépendant que de δ , et pas de p ni de A , tel que

$$|A| > p^\delta \implies |A^K| > p^{3-\delta}.$$

On conclut grâce à la proposition suivante due à Gowers, et à son corollaire :

Proposition 4.6. *Soit G un groupe de cardinal n , et tel que toute représentation irréductible de G soit de dimension k . Si A, B, C sont trois sous-ensembles de G tels que $|A||B||C| \geq \frac{n^3}{k}$, alors il existe $(a, b, c) \in A \times B \times C$ tel que $ab = c$.*

Corollary 5 (Nikolov et Pyber). *Soit G un groupe de cardinal n , et tel que toute représentation irréductible de G soit de dimension k . Si A, B, C sont trois sous-ensembles de G tels que $|A||B||C| \geq \frac{n^3}{k}$, alors $A.B.C = G$.*

Dans notre cas $n \sim p^3$ et $k \sim p$.

Preuve du corollaire. Soit $g \in G$, on veut trouver a, b, c tels que $abc = g$. Pour cela il suffit d'appliquer la proposition précédente aux ensembles A, B et $C^{-1}g$.

Preuve de la proposition. [Nikolov et Pyber].

Soit $V = \mathbb{C}G$ l'algèbre du groupe G , c'est un espace vectoriel complexe de dimension $n = |G|$. On le munit de son produit scalaire "standard" (qui fait de la base $(g)_{g \in G}$ une BON). C'est aussi un G -module à gauche.

Soit X la matrice $G \times G$ d'entrées $x_{g,h} = 0$ si $h^{-1}g \notin B$, $x_{g,h} = 1$ sinon. Pour $u \in G \subset V$ on a $Xu = \sum_{b \in B} ub$, donc X est un endomorphisme de G -module (c'est-à-dire $X(gv) = gXv$).

On considère la matrice symétrique positive $Y = {}^tXX$. Elle a pour plus grande valeur propre $\lambda_1^2 = |B|^2$, associée au vecteur $e = \sum_{g \in G} g$. Soit $I = e^\perp$, ce sous-espace est Y -invariant, G -invariant (et G ne fixe aucun vecteur de I). Par hypothèse, toute valeur propre λ^2 de Y sur I est de multiplicité $\geq k$. Donc

$$n|B| = \text{tr}Y \geq k\lambda^2,$$

autrement dit $\lambda^2 \leq n|B|/k$. Par conséquent,

$$(4.5) \quad \|Xv\|^2 \leq \frac{n|B|}{k} \|v\|^2$$

pour tout $v \in I$.

Supposons, par contraposition, que $ab = c$ n'ait aucune solution $(a, b, c) \in A \times B \times C$. On introduit $v = n \sum_{g \in A} g$ et on décompose $v = v_1 + v_2$, $v_1 = |A|e$ et $v_2 \in I$, $\|v_2\|^2 = n^2|A| - n|A|^2 < n^2|A|$. On a $Xv \in \sum_{g \notin C} \mathbb{C}g$. Par ailleurs

$$Xv = |A||B|e + Xv_2$$

et par conséquent Xv_2 a comme coordonnée $-|A||B|$ sur tous les vecteurs de base $g \in C$. Donc $\|Xv_2\|^2 \geq |C||A|^2|B|^2$. Par (4.5),

$$|C||A|^2|B|^2 \leq \frac{n|B|}{k} \|v_2\|^2 < \frac{n|B|}{k} n^2|A|$$

et donc $|A||B||C| < \frac{n^3}{k}$.

5. PREUVES.

5.1. Élément(s) non simultanément diagonalisables.

Lemma 5.1 (Escaping from subvarieties). *Soit G un groupe agissant linéairement sur un espace vectoriel V , défini sur un corps K . Soit $W = W_1 \cup \dots \cup W_n$ une union de sous espaces vectoriels stricts de V .*

Soit A un sous-ensemble de G , et soit \mathcal{O} une orbite de $\langle A \rangle$ dans V . Alors il existe $\eta > 0$ et $m \in \mathbb{N}$, de dépendant que de n et de $d = \dim V$ tels que, pour tout $x \in \mathcal{O}$, il existe au moins $\max(1, \eta|A|)$ éléments $g \in A_m$ tels que $gx \notin W$.

Preuve. (i) On montre d'abord qu'il existe $g_1, \dots, g_l \in A_r$ tels que, pour tout $x \in \mathcal{O}$, au moins l'un des $g_i x$ n'est pas dans W .

On procède par récurrence sur ($s = \max \dim W_k$, $N =$ number of W_i of maximal dimension). Si $s = 0$ c'est évident. À chaque pas de la récurrence, soit s diminuera strictement (dans ce cas N sera au plus élevé au carré), soit s sera constant et N diminuera strictement. Dans ce cas, le nombre de pas est borné par une fonction de (s, n) : le nombre de prédecesseurs de (s, n^{2^s}) pour l'ordre lexicographique sur $\mathbb{N} \times \{0, \dots, n^{2^s}\}$.

Appelons \tilde{W} l'union des W_i de dimension s . Si $\mathcal{O} \cap \tilde{W} = \emptyset$, alors on ignore \tilde{W} et on applique l'hypothèse de récurrence à $W \setminus \tilde{W}$. Si $\mathcal{O} \cap \tilde{W} \neq \emptyset$, il existe nécessairement $x_0 \in \mathcal{O} \cap \tilde{W}$ et $g \in A \cup A^{-1}$ tel que $gx_0 \notin \tilde{W}$. Donc $W' = gW \cap W$ est une union de n^2 sous-espaces de dimension $\leq s$, et a strictement moins de sous-espaces de dimension s que W . Par hypothèse de récurrence, il existe $g'_1, \dots, g'_{l'}$ tels que, pour tout $x \in \mathcal{O}$, il existe g'_i tel que $g'_i x \notin W' = gW \cap W$. Et l', r' sont bornés en fonction de (s, n^2) . Pour avoir le résultat pour W , on pose alors $l = 2l'$, $g_1 = g'_1, \dots, g_{l'} = g'_{l'}$, $g_{l'+1} = g^{-1}g'_1, \dots, g_{2l} = g^{-1}g'_{l'}$. Chaque g_i est dans A_r , $r = r' + 1$. Cela termine le (i)

(ii) Pour montrer le lemme il reste à montrer que $gx \notin W$ pour *beaucoup* de g .

Pour tout $x \in \mathcal{O}$ et $g \in A$, il y a au moins un $g_i \in A_r$ ($1 \leq i \leq l$) tel que $g_i g x \notin W$. Par le lemme des tiroirs, il doit exister un g_i pour lequel au moins $\frac{|A|}{l}$ éléments distincts $g \in A$ donnent $g_i g x \notin W$. Or $g_i g \in A_{r+1}$, et on obtient le résultat avec $\eta = l^{-1}$.

5.2. Éléments simultanément diagonalisables.

Proposition 5.2 (4.1). *Soit G un groupe et A un sous-ensemble fini non vide. Soit Λ_A l'ensemble des classes de conjugaison de G rencontrant A . Pour $g \in G$, on note $C_G(g)$ le centralisateur de g .*

Alors il existe $g \in A$ tel que

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

Preuve. Soit g fixé quelconque. On considère l'application $A \rightarrow G$ (à valeurs dans $\{hgh^{-1}, h \in A\}$), $h \mapsto hgh^{-1}$. Deux éléments h_1, h_2 ont la même image ssi $h_2^{-1}h_1 \in C_G(g) \cap A^{-1}A$. Donc

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

Soit $\Gamma \subset A$ un ensemble de représentants de Λ_A .

$$|A.A.A^{-1}| \geq |\{hgh^{-1}, h \in A, g \in \Gamma\}| \geq \sum_{g \in \Gamma} \frac{|A|}{|C_G(g) \cap A^{-1}A|}.$$

Cela implique qu'il existe $g \in \Gamma$ tel que

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

Lemma 5.3 (Lemma 4.2). *Soit K un corps. Soit A un sous-ensemble fini générateur de $SL_2(K)$. Alors A_2 a au moins $\frac{1}{4}|A| - 1$ éléments de trace différente de ± 2 .*

Preuve. On fixe g , un élément de A de trace ± 2 , autre que $\pm I$. Un tel g est semblable à $\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

On note $B \subset A$ les matrices de A de trace ± 2 et qui ont un vecteur propre commun avec g . Deux cas sont possibles :

(a) si $|B| \leq \frac{1}{4}|A| + 3$. Soit $h \in A \setminus B$, $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans la base qui triangule g .

On a $c \neq 0$ par hypothèse, et $Tr(gh) = \pm(Tr(h) + c)$, $Tr(g^{-1}h) = \pm(Tr(h) - c)$. On voit donc que l'une des trois traces $\{Tr(h), Tr(gh), Tr(g^{-1}h)\}$ est différente de ± 2 . Donc $A \cup (A.A) \cup (A^{-1}.A)$ a au moins $\frac{1}{3}|A \setminus B| \geq \frac{1}{4}|A| - 1$ éléments de trace différente de ± 2 .

(b) si $|B| > \frac{1}{4}|A| + 3$. Soit $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in A$ qui n'a pas de vecteur propre en commun avec g (c'est-à-dire $c \neq 0$). Il y a au plus deux éléments g' de B tels que $Tr(g'h) = 2$. En effet si

$$g' = \pm \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$$

on trouve $\pm(a + d + \alpha c) = 2$ donc au plus deux possibilités pour α . De même, il y a au plus deux éléments g' de B tels que $Tr(g'h) = -2$.

Là aussi on conclut que $A.A$ a au moins $|B| - 4 > \frac{1}{4}|A| - 1$ éléments de trace différente de ± 2 .

Corollary 6. Soit K un corps. Soit A un sous-ensemble fini non vide de $SL(2, K)$, non contenu dans un sous-groupe propre. Supposons $|A| \geq 4$, $|TrA| \geq 2$. Alors dans A_4 il y a au moins $\frac{(|TrA|-2)(\frac{1}{4}|A|-4)}{|A_6|}$ matrices simultanément diagonalisables .

Preuve. On appelle B l'ensemble des éléments de A_2 , de trace autre que ± 2 (c'est-à-dire diagonalisables dans \bar{K} et non égaux à $\pm I$). On a $|B| \geq \frac{1}{4}|A| - 4$.

Il existe $g \in B$ tel que

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

Les éléments de $C_G(g) \cap B^{-1}B \subset A_4$ commutent tous avec g . Donc ils sont tous simultanément diagonalisables sur \bar{K} (et en fait dans une extension de degré 2 de K , $\sim \mathbb{F}_{p^2}$ dans le cas $K = \mathbb{F}_p$).

5.3. Croissance "sans surprise" des traces. Le but de cette section est de démontrer les deux propositions suivantes, qui en gros comparent $|A|$ et $|\text{Tr}A|^3$:

Proposition 5.4. *Soit K un corps. Soit A un sous-ensemble fini de $SL_2(K)$ non contenu dans un sous-groupe propre. Si $|\text{Tr}A| \geq 2$, $|A| \geq 4$ et $|K| > 3$ alors*

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

où k ne dépend pas de K ni de A .

Proposition 5.5. *Soit K un corps, $|K| > 3$. Soit A un sous-ensemble fini de $SL_2(K)$ non contenu dans un sous-groupe propre. Alors il existe k, c indépendants de K et de A tels que*

$$|\text{Tr}A_k| \geq c|A|^{1/3}.$$

Preuve de 5.4.

Lemma 5.6. *Soit $V \subset SL_2(K)$ simultanément diagonalisable, de vecteurs propres v_1, v_2 . Soit $g \in SL_2(K)$ tel que $gv_i \neq v_j$ pour tout $\lambda \in \bar{K}$, i, j . Alors*

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

En effet, plaçons-nous dans la base (v_1, v_2) . On écrit $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $abcd \neq 0$. On calcule

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

On a $h_{12}h_{21} = -(r - r^{-1})^2abcd$. Donc (g est fixé) $|\{h_{12}h_{21}, h \in gVg^{-1}\}| \geq \frac{1}{4}|V|$. Soit $U = \{h \in gVg^{-1}, h_{12}h_{21} \neq 0, h_{11} \neq 0 \text{ or } h_{22} \neq 0\}$. Alors $|\{h_{12}h_{21}, h \in U\}| \geq \frac{1}{4}|V| - 5$.

Soit $h \in U$ fixé. On calcule

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

Le produit des deux entrées antidiagonales est $h_{12}h_{21}$, non nul et indépendant de s et t . Connaissant h et $f_h(s, t)$ on peut récupérer s^2, t^2, st , donc au plus deux valeurs de (s, t) sont possibles. Cela finit la preuve.

Pour prouver la proposition, on utilise le Corollaire 6 qui nous donne $V \subset A_4$, simultanément diagonalisable, $|V| \geq \frac{(|\text{Tr}A|-2)(\frac{1}{4}|A|-4)}{|A_6|}$. Par le Corollaire 3, il existe dans A_k une matrice g dont toutes les entrées sont non nulles (dans la base qui diagonalise V). On sait qu'alors $|VgVg^{-1}V| \geq \frac{1}{2} \left(\frac{1}{4}|V| - 5 \right) |V|^2$.

Preuve de la Proposition 5.5. On commence d'abord par un

Lemma 5.7. *Soit $A \subset SL_2(K)$ tel que $g_{12}g_{21} \neq 0$ pour tout $g \in A$ (dans une base fixée de \bar{K}^2). Alors*

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

Pour le démontrer, notons $D = \{(g_1, g_2), g \in A\}$. Soit $g, g' \in A$, on calcule

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

Donc il y a au plus 2 éléments g' qui ont les mêmes entrées diagonales que g et tels que $\mathrm{Tr}(gg'^{-1})$ prenne une valeur donnée. Autrement dit, une fois g fixé,

$$|\{\mathrm{Tr}(gg'^{-1})\}| \geq \frac{1}{2} |\{g' \in A, g'_{11} = g_{11}, g'_{22} = g_{22}\}|.$$

Il suffit de choisir g tel que ce dernier ensemble soit de cardinal maximal.

On peut maintenant démontrer 5.5 ! On peut toujours supposer que A a un élément h de trace autre que ± 2 (sinon, soient g_1, g_2 deux éléments de A de trace ± 2 et qui ne commutent pas, alors g_1g_2 ou $g_1^{-1}g_2$ a trace $\neq \pm 2$).

On se place désormais dans une base (v_1, v_2) qui diagonalise h , et on appelle r, r^{-1} les valeurs propres de h . Le Corollaire 4 nous dit que $|X| \geq c|A|$, où X est l'ensemble des matrices de A_{k_0} qui ne sont pas triangulaires. Le Lemme précédent dit que

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

Étant donné $t \in K$ on note $D_t = \{(g_{11}, g_{22}), g \in X, g_{11} + g_{22} = t\}$. Soit t tel que $|D_t|$ est maximal. Pour $(a, b) \in D_t$, on a $ra + r^{-1}d = (r - r^{-1})a + r^{-1}t$, donc pour $(a, b), (a', b') \in D_t$, les quantités $ra + r^{-1}d, ra' + r^{-1}d'$ sont distinctes. Ainsi,

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

En prenant le produit des deux inégalités précédentes on obtient

$$|\mathrm{Tr}A_{2k_0}| |\mathrm{Tr}A_{2k_0}| |\mathrm{Tr}X| \geq \frac{|X|}{2} \geq \frac{c|A|}{2}.$$

C'est fini.

5.4. "Estimée somme-produit \Rightarrow croissance surprenante des traces". On rappelle l'identité

$$\mathrm{Tr} \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = ad(xy + x^{-1}y^{-1}) - bc(x^{-1}y + xy^{-1}).$$

Les matrices $\begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix}$ vont décrire un ensemble de matrices dans $|A_*|$, simultanément diagonalisables (de cardinal en gros $|A|^{1/3}$), et la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est fixée dans $|A_*|$, d'entrées toutes non nulles dans la base qui diagonalise les matrices précédentes. Toutes ces matrices sont à coefficients dans \mathbb{F}_{p^2} .

Proposition 5.8. *Pour tout $\delta > 0$, il existe $C, \epsilon > 0$ tels que, pour tout $q = p^\alpha$, pour tous $a_1, a_2 \in \mathbb{F}_q^*$, pour tout $B \subset \mathbb{F}_q^*$ de cardinal $C < |B| < p^{1-\delta}$, on ait*

$$|\{a_1(xy + x^{-1}y^{-1}) + a_2(x^{-1}y + xy^{-1}), x, y \in B_{20}\}| \geq |B|^{1+\epsilon}.$$

On démontre d'abord

Lemma 5.9. *Pour tout $\delta > 0$, il existe $C, \epsilon > 0$ tels que, pour tout $q = p^\alpha$, pour tout $B \subset \mathbb{F}_q^*$ de cardinal $C < |B| < p^{1-\delta}$, on ait*

$$|\{(x + x^{-1})(y + y^{-1}), x, y \in B_2\}| \geq |B|^{1+\epsilon}.$$

Preuve. Notons $w(x) = x + x^{-1}$. Supposons qu'on ait $|\{(x + x^{-1})(y + y^{-1}), x, y \in B_2\}| < |B|^{1+\epsilon}$. Alors $|B| \leq |B_2| \leq 2|B|^{1+\epsilon}$.

On remarque que $w(x)w(y) = w(xy) + w(xy^{-1})$ et aussi que $S = \{(w(xy), w(xy^{-1})), x, y \in B\}$ est de cardinal au moins $|B|^2/16$. D'après le Thm 3.3, il existe $B' \subset B_2$ tel que $|B'| > c'|B|^{1-C'\epsilon}$, et tel que $|w(B') + w(B')| < C'|B_2|^{1+C'\epsilon} \leq C'|B|^{1+C'\epsilon}$.

Par ailleurs, on a $|w(B').w(B')| \leq |w(B_2).w(B_2)| \leq |B|^{1+\epsilon}$, par hypothèse. Mais, si ϵ est assez petit et C assez grand (en fonction de δ), l'estimée somme-produit dit que c'est impossible.

Lemma 5.10. *Soient A et B des sous-ensembles d'un groupe G . Alors A peut être recouvert par au plus $|AB|/|B|$ "classes à gauche" aB_2 , avec $a \in A$.*

Preuve. Soient $\{a_1, \dots, a_k\}$ un sous-ensemble maximal de A tel que les a_jB soient disjoints. On a $k|B| \leq |AB|$. Soit $x \in A$, alors il existe j tel que $a_jB \cap xB$ soit non vide. Donc $x \in a_jB_2$.

Preuve de la prop. 5.8. Par le lemme précédent, on peut recouvrir B_4 par au plus $|B_4.B^2|/|B^2|$ ensembles $b_j(B^2)_2$, $b_j \in B_4$. Si 2 éléments $x, y \in B_2$ sont tels que $xy \in b_j(B^2)_2$, on a $xy^{-1} = xy.y^{-2} \in b_j(B^2)_2(B_2)^{-2} \subset b_j(B^2)_4$.

Par la proposition 5.9 et le lemme des tiroirs, il existe au moins un j tel que

$$(5.1) \quad |\{(r + r^{-1}) + (s + s^{-1}), r, s \in b_j(B^2)_4\}| > \frac{|B|^{1+\epsilon}}{|B_4.B^2|/|B^2|}.$$

On a $|B_4.B^2|/|B^2| \leq 2|B_6|/|B|$, on a soit $2|B_6| > |B|^{1+\epsilon/4}$ ou

$$\frac{|B|^{1+\epsilon}}{|B_4.B^2|/|B^2|} > |B|^{1+3\epsilon/4}.$$

Dans le premier cas, il suffit de laisser varier $x \in A_6$ et $y = x$ pour conclure. Supposons donc $2|B_6| \leq |B|^{1+\epsilon/4}$.

Soit $C = b_j(B^2)_4 \subset B_{12}$. On a $|C| \leq |B_4| \leq |B|^{1+\epsilon/4}$. L'inégalité (5.1) implique que

$$d_+(w(C), -w(C)) \geq \frac{\epsilon}{2} \log |B|$$

et donc

$$d_+(w(C), w(C)) \geq \frac{\epsilon}{8} \log |B|$$

Puis par inégalité triangulaire et homogénéité,

$$d_+(a_1w(C), -a_2w(C)) \geq \frac{1}{2} \geq d_+(w(C), w(C)) \geq \frac{\epsilon}{1} 6 \log |B|.$$

De manière équivalente

$$(5.2) \quad |\{a_1(r + r^{-1}) + a_2(s + s^{-1}), r, s \in C\}| > \frac{|C|}{2} |B|^{\epsilon/12} \geq \frac{1}{4} |B|^{1+\epsilon/12}.$$

Pour conclure, on écrit, pour $r, s \in C$, $r/s \in (B^2)_4(B^{-2})_4 \subset B_8^2$. Donc $r/s = y^2$, $y \in B_8$. D'efinissons $x = r/y \in B_{20}$. Alors $r = xy$ et $s = xy^{-1}$, et $\{a_1(r + r^{-1}) + a_2(s + s^{-1}), r, s \in C\} \subset \{a_1(xy + x^{-1}y^{-1}) + a_2(x^{-1}y + xy^{-1}), x, y \in B_{20}\}$.