

Théorème (Kelfgott, théorème 2.4)

Soit  $q = p^a$ ,  $p$  premier,  $\delta > 0$ .

$A \in \mathbb{F}_q^*$  tq  $c < |A| < p^{1-\delta}$ , alors  
 $\max(|A+A|, |A \cdot A|) \geq |A|^{1+\varepsilon}$ , où  $\varepsilon \in \mathbb{R}$  dépend de  $\delta$ .

Rq: Si  $A \subset \mathbb{F}_q$  est un sous corps,  $|A \cdot A| = |A|$ ,  $|A+A| = |A|$ .

L'idée est que c'est le "seul cas possible" au sens où :

si  $|A+A| \leq K|A|$ ,  $|A \cdot A| \leq k|A|$ , alors  $A$  est proche d'un sous corps de  $\mathbb{F}_q$ .

Théorème (Freiman)  $A \subset \mathbb{F}$ ,  $k \geq 1$ . Alors (i)  $\Leftrightarrow$  (ii) :

(i)  $C_1$

(i)  $|A+A| \leq C_1 k^{C_1} |A|$  et  $|A \cdot A| \leq C_1 k^{C_1} |A|$

$\Leftrightarrow$

(ii) Soit  $|A| \leq C_2 k^{C_2}$

(ii)  $C_2 = C_2(C_1)$

soit il existe un sous corps  $G$  de  $\mathbb{F}$ ,  $x \in \mathbb{F}$ ,  $X \subset \mathbb{F}$ ,

tq  $|G| \leq C_2 k^{C_2} |A|$ ,  $|X| \leq C_2 k^{C_2} |A|$  et

$A \subset \cup G \cup X$ .

Théorème de Freiman  $\Rightarrow$  Thm Kelfgott :

On utilise : si (ii) n'est pas vrai avec  $C_2 \stackrel{!}{=}$  1, alors

(i) n'est pas vrai avec  $C_1 = C_1(C_2) = C_1(1)$ . (Supposant que  $|A|$  assez grand  $\geq c$ )

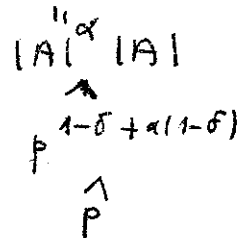
Soit  $1 \leq |A| < p^{1-\delta}$ ,  $A \subset \mathbb{F}^*$ ,  $|\mathbb{F}| = p^a$

Soit  $k = |A|^\alpha$ , où  $0 < \alpha < 1$ , tel que ~~...~~

$0 < 1 - \delta + \alpha(1 - \delta) < 1$ , en particulier  $0 < p^{1 - \delta + \alpha(1 - \delta)} < p$ .

Soit  $C_2 = 1$ . On a  $|A| > C_2 k^{C_2} = k = |A|^\alpha$  et par

ailleurs, il n'existe pas de sous corps  $|G| < C_2 k^{C_2} |A|$



166

Soit  $c_1'$  dans (i)  $\Rightarrow c_2'$  dans (ic).

Soit  $k'$  tq  $k = |A|^d = c_2' k'^{c_2'}$ , càd

$k' = \left(\frac{k}{c_2'}\right)^{1/c_2'} \geq 1$  si  $k = |A|^d \geq c_2'$  donc si  $|A| \geq (c_2')^{1/d}$

Si (ii) pas vrai pour  $c_2 = 1$ , et  $k$ , alors

(ii) pas vrai pour  $c_2 k'^{c_2}$  donc

(i) pas vrai pour  $c_1' k'^{c_1'}$  càd

$$|A+A| \geq c_1' k'^{c_1'} |A|$$

$$\text{ou } |A \cdot A| \geq c_1' k'^{c_1'} |A|$$

$$c_1' \left(\frac{k}{c_2'}\right)^{1/c_2'}$$

cafd.

(2)

donc d'après Freiman :  $|A+A| \geq C_1 k^{C_1} |A|$  ou  
 $|A \cdot A| \geq C_1 k^{C_1} |A| = C_1 |A|^{C_1 + 1}$ , ce qui prouve  
 le théorème d'Helfgott avec  $\varepsilon = C_1 \alpha$ .  $\square$

Le théorème de Freiman repose sur le lemme suivant dû à Tao-Katz  
 et aux théorèmes C, D, en reliant E de l'exposé d'Oliver.

Lemme (Katz-Tao)  $F$  corps,  $A \subset F^* = F \setminus \{0\}$ .

Supposons que pour  $k \geq 1$ ,  $|A+A| \leq k|A|$  et  $|A \cdot A| \leq k|A|$ , alors  
 il existe  $A' \subset A$ ,  $|A'| \geq \frac{|A|}{2k}$  tel que  $|A'A' - A'A'| = O(k^{-O(1)}) |A'|$ .

Rq. On ne peut pas choisir  $A' = A$  (en général). On pourrait penser  
 que  $|A+A| \leq k|A|$  et  $|A \cdot A| \leq k|A| \Rightarrow$  pour tout polynôme  $P$ ,  
 $|P(A)| \leq C k^C |A|$  mais c'est faux

exple :  $G \subset F$  un sous corps,  $A = G \cup \{x\}$ ,  $x \notin G$ .

$|A+A|, |A \cdot A| < 2|A|$ , pourtant  $|A \cdot A - A \cdot A| > |G - xG|$   
 $= 2|G| + 1$

de cardinal  $|G - xG| = |G|^2$ , donc  $|A \cdot A - A \cdot A| \geq (|A| - 1)^2$   $\square$

dém du lemme de Katz-Tao

(3)

les étapes :

$$\textcircled{1} \sum_{a, b \in A} |aA \cap bA| \geq \frac{|A|^3}{k}$$

$$\textcircled{2} \exists b \in A, \sum_{a \in A} |aA \cap bA| \geq \frac{|A|^2}{k}$$

$$\textcircled{3} A' = \left\{ a \in A \mid |aA \cap bA| \geq \frac{|A|^2}{2k} \right\}, \quad b \text{ fixé en } \textcircled{2}$$

$$\bullet |A'| \geq \frac{|A|}{2k}$$

$$\bullet \sum_{a \in A'} |aA \cap bA| \geq \frac{|A|^2}{2k}$$

$$\textcircled{4} \forall a \in A', b \in A \text{ fixé en } \textcircled{2}, d(aA, bA) = O(1 + \log k)$$

où  $d$  = distance de Ruzsa.

$$\textcircled{5} d(a_1 a_2 A, b^2 A) = O(1 + \log k) \quad \forall a_1, a_2 \in A', b \text{ fixé en } \textcircled{2}$$

$$\textcircled{6} d(a_1 a_2 a_3^{-1} A, a_1' a_2' a_3'^{-1} A) = O(1 + \log k) \quad \forall a_i, a_i' \in A'$$

$$\textcircled{7} \text{ Fin de la preuve : D'après } \textcircled{6}, \forall x, y \in A'A'A'^{-1}, d(xA, yB) \leq O(1 + \log k)$$

$$\log \left( \frac{|xA - yB|}{|xA|^{1/2} |kB|^{1/2}} \right)$$

$$\text{donc } \bullet |xA - yB| = O(k^{O(1)}) |A|, \forall x, y \in A'A'A'^{-1}$$

$$\bullet \sum_{x, y \in A'A'A'^{-1}} |xA - yB| = O(k^{O(1)}) |A| |A'A'A'^{-1}|^2$$

$$\bullet \text{Thm D + corollaire E des notes d'Olivier} \Rightarrow |A'A'A'^{-1}| = O(k^{O(1)}) |A|$$

$$\bullet \sum_{x, y \in A'A'A'^{-1}} |xA - yB| = O(k^{O(1)}) |A|^3$$

$$\sum_z \left| \left\{ (x, y) \in A'A'A'^{-1} \mid \exists a, b \in A, z = xa - yb \right\} \right|$$

(4)

• Soit  $z = a_1 a_2 - a_1' a_2' \in A'A - A'A'$ , alors  $z$  peut s'écrire  $z = \underbrace{a_1 a_2 a^{-1}}_x a - \underbrace{a_1' a_2' b^{-1}}_y b = x a - y b$  de  $|A|^2$  façons différentes au moins, donc :

$$|A'A - A'A'| |A|^2 \leq \sum_z |\{ (x, y) \mid \exists a, b \in A, z = x a - y b \}|$$

$$= O(k^{O(1)}) |A|^3$$

d'où  $|A'A - A'A'| \leq O(k^{O(1)}) |A|$   $\square$

Retour sur les étapes

①  $\sum_{\substack{a \in A \\ b \in A}} |a A n b A| = E(A, B) \geq \frac{|A|^3}{k}$

dém :  $\sum_{x \in A \cdot A} \sum_{a \in A} 1_{aA}(x) = \sum_{a \in A} \sum_{x \in A \cdot A} 1_{aA}(x) = |A|^2$

Cauchy-Schwarz  $\Rightarrow |A|^4 = \left( \sum_{x \in A \cdot A} k \left( \sum_{a \in A} 1_{aA}(x) \right) \right)^2 \leq \left( \sum_{x \in A \cdot A} 1 \right) \left( \sum_{x \in A \cdot A} \left( \sum_{a \in A} 1_{aA}(x) \right)^2 \right)$

$$\leq k |A| \sum_{x \in A \cdot A} \left( \sum_{a \in A} 1_{aA}(x) \right) \left( \sum_{b \in A} 1_{bA}(x) \right)$$

$$\Rightarrow \sum_{x \in A \cdot A} \left( \sum_{a \in A} 1_{aA}(x) \right) \left( \sum_{b \in A} 1_{bA}(x) \right) \geq \frac{|A|^3}{k}$$

$$\sum_{\substack{a \in A \\ b \in A}} \left| \sum_{x \in A \cdot A} 1_{aA}(x) 1_{bA}(x) \right|$$

$$\sum_{a, b \in A} |a A n b A| \quad \square$$

② Sinon,  $\forall b \in A, \sum_{a \in A} |a A n b A| < \frac{|A|^2}{k}$ ,

donc  $\sum_{b \in A} \sum_{a \in A} |a A n b A| < |A| \frac{|A|^2}{k} = \frac{|A|^3}{k}$

Dans la suite, on fixe un  $b \in A$ , tel que

$$\sum_{a \in A} |a A n b A| \geq \frac{|A|^2}{k}$$

(5)

(3)  $A' = \{ a \in A \mid |aA \cap bA| \geq \frac{|A|}{2k} \}$ ,  $b$  fixé en (2)

•  $|A'| \geq \frac{|A|}{2k}$ , sinon  $|A'| < \frac{|A|}{2k}$

et  $\sum_{a \in A} |aA \cap bA| = \sum_{a' \in A'} |aA \cap bA| + \sum_{a \in A \setminus A'} |aA \cap bA|$   
 $< \frac{|A|^2}{2k} + |A| \cdot \frac{|A|}{2k} = \frac{|A|^2}{k}$

•  $\sum_{a \in A'} |aA \cap bA| \geq \frac{|A|^2}{2k}$ , sinon  $\sum_{a \in A'} |aA \cap bA| < \frac{|A|^2}{2k}$ , et

$\sum_{a \in A} |aA \cap bA| = \sum_{a \in A'} |aA \cap bA| + \sum_{a \in A \setminus A'} |aA \cap bA|$   
 $< \frac{|A|^2}{2k} + |A| \cdot \frac{|A|}{2k} = \frac{|A|^2}{k} \quad \square$

(4)  $d(aA, bA) = O(1 + \log k)$ ,  $\forall a \in A'$ ,  $b$  fixé en (2).

•  $d(A, A) \leq d(aA, bA) = d(bA, bA) \leq 2d(A, -A)$   
 $\leq 2 \log \left( \frac{|A+A|}{|A|^{1/2} |A|^{1/2}} \right) \leq 2 \log k$

• soit  $b$  fixé en (2) et  $a \in A'$

$d(aA, aA \cap bA) = \log \left( \frac{|aA - (aA \cap bA)|}{|aA|^{1/2} |aA \cap bA|^{1/2}} \right)$   
 $\leq \log \left( \frac{|aA - aA| (2k)}{|A|^{1/2} |A|^{1/2}} \right) = \frac{1}{2} \log(2k) + \log \left( \frac{|A-A|}{|A|} \right)$   
 $= \frac{1}{2} \log(2k) + d(A, A) = \frac{1}{2} \log(2k) + 2 \log k$

d'où  $d(aA, aA \cap bA) = O(1 + \log k) \quad \square$

Remarque  $d(bA, aA \cap bA) = O(1 + \log k)$

(5) Par dilatation :  $d(aA, bA) = O(1 + \log k)$  par inégalité triangulaire.  
Par dilatation :  $d(a, a_2 A, b, b_2 A) = O(1 + \log k)$   
 et  $d(b, b_2 A, b^2 A) = O(\log k)$  d'où par inégalité triangulaire  
 $d(a, a_2 A, b^2 A) = O(1 + \log k) \quad \square$

(6)

⑥ De ⑤,  $d(a_1 a_2 A, b^2 A) = O(1 + \log k)$

donc  $d(a_1 a_2 b^{-1} A, b A) = O(1 + \log k) \quad \forall a_1, a_2 \in A'$

De  $d(a_3 A, b A) = O(1 + \log k) \quad \forall a_3 \in A'$ ,

en posant  $c = a_1 a_2 a_3^{-1} b^{-1}$ ,  $a_i \in A'$ , par dilatation on obtient :

$d(a_1 a_2 b^{-1} A, a_1 a_2 a_3^{-1} A) = O(1 + \log k)$ , d'où par inégalité triangulaire :

$d(a_1 a_2 a_3^{-1} A, b A) = O(1 + \log k)$

et  $d(a_1 a_2 a_3^{-1} A, a_1' a_2' a_3'^{-1} A) = O(1 + \log k) \quad \forall a_i, a_i' \in A' \square$

De même on obtient le lemme suivant, sous les mêmes hypothèses que dans le lemme de Katz-Tao :

~~le lemme~~ : ~~soit  $A, A' \subseteq \mathbb{R}^d$ ,  $A' \subseteq A$ ,  $|A'| \leq \epsilon |A|$ ,  $|A - A'| \leq \epsilon |A|$ ,  $|A^k - A'^k| \leq O(k^{O(1)}) |A|$~~

lem : On montre d'abord que :

$d(a_1 a_2 a_3 a_4^{-1} A^f, a_1' a_2' a_3' a_4'^{-1} A^f) = O(k^{O(1)}) |A^f|$

et on fait comme précédemment  $\square$

(7)

Théorème (Freiman)  $F$  corps,  $A \subset F$ ,  $|A| < \alpha$ ,  $k \geq 1$

$\Downarrow$  (i)  $|A+A| \leq c_1 k^{c_1} |A|$  et  $|A \cdot A| \leq c_1 k^{c_1}$

(ii) soit  $|A| \leq c_2 k^{c_2}$

soit il existe  $G \subset F$  sous corps,  $|G| < c_2 k^{c_2} |A|$ ,  
 $X \subset F$ ,  $|X| < c_2 k^{c_1} |A|$ ,  $x \in F$ ,  $A \subset xG \cup X$

dem: les étapes

$\Downarrow$  •  $k = c_1 k^{c_1}$   $|A+A| \leq k|A|$ ,  $|A \cdot A| \leq k|A|$

•  $|A| \geq c_0 k^{c_0}$  pour  $c_0$  assez grand choisi plus tard

•  $0 \notin A$ ,  $A \subset F^*$

katz-Tao  $\Rightarrow \begin{cases} \exists A' \subset A, & |A'| \geq \frac{|A|}{2k} \\ \text{et } |A'^k - A'^k| = O(k^{o_{m,m,k}^{(1)}}) |A'| \quad \forall k \geq 1 \end{cases}$

①  $|mA'^k - mA'^k| = O(k^{o_{m,m,k}^{(1)}}) |A'| \quad \forall m, m, k \geq 1$

② suppose (dilatation)  $1 \in A'$ ,  $0 \in A'$  (on rajoute 0)  
 $D = (A' - A') \setminus \{0\}$ ,  $G = Q[A'] = \frac{A' - A'}{D}$

si  $|A| \geq c_0 k^{c_0}$  assez grand, alors  $G$  est un sous  
corps de  $F$ , et  $G \supset A'$ .

③ On peut recouvrir  $A$  par  $O(k^{o_{11}^{(1)}})$  translations (~~ou~~  
~~dilatés~~) de  $A' - A'$  et donc de  $G$  et de même  
on peut recouvrir  $A$  par  $O(k^{o_{11}^{(1)}})$  dilatés de  $G$ .

④  $|G| \leq O(k^{o_{11}^{(1)}}) |A'|$ .

8

Conclusion

$$A \subset G \cup x_1 G \cup \dots \cup x_m G, \quad m, m = O(k^{O(1)})$$

$$\text{et } A \subset G \cup (G+y_1) \cup \dots \cup (G+y_m)$$

où  $x_i \notin G, \quad x_i, y_i \in A$

où  $\forall x \notin G, \quad |x \cap G \cap (G+y)| \leq 1$   
 $\forall y$

(en effet,  $xg = h+y$  et  $xg' = h'+y$ )  
 $\Rightarrow x(g-g') = h-h'$

Donc  $X = (x_1 G \cup \dots \cup x_m G) \cap A$  vérifie  $|X| \leq O(k^{O(1)})$

et  $A \subset G \cup X$ .

Comme on avait dit que  $A'$  et  $A$  pouvaient avoir  $1 \in A'$ ,  
on obtient  $A \subset xG \cup X$ .  $\square$

Retour sur les étapes :

① On a vu que  $|A^{1k} - A^{1k}| = O(k^{O(1)} |A'|)$   
 (venant additiver)  
 Par le théorème C des notes d'Oliveri, appliqué à

$A = A^{1k}, \quad B = -A^{1k}$ , comme on a :  $|A+B| \leq O(k^{O(1)} |A'|)$   
 $\leq O(k^{O(1)} |A'|^{1/2})$   
 $|A^{1k} - A^{1k}| \leq O(k^{O(1)} |A'|^{1/2})$

il existe un sous-groupe additif approché HCF,  $|H| \leq O(k^{O(1)} |A'|)$

~~$A \subset X \cup F$~~ ,  $|X| \leq O(k^{O(1)})$ , tq  $A \subset X+H, Y \subset X+H$ .

Ainsi :  $|nA + mB| = |nA^{1k} - mA^{1k}| = O(k^{O(1)} |A'|) \quad \square$

(9)

$$\textcircled{2} \quad A' + GG.A' \subset \frac{G(A')^3 - G(A')^2}{D^2}$$

Par ailleurs,  $|(G(A')^3 - G(A')^2)D^2| \leq O(k^{\alpha''})|A'|$

donc  $\left| \frac{G(A')^3 - G(A')^2}{D^2} \right| \leq O(k^{\alpha''})|A'|$  d'après théorème C

(version multiplicative)

Donc si  $|A'| \geq C_0 k^{\epsilon_0}$ , avec  $C_0$  assez grand,

$$\begin{array}{l} |A' + G.G.A'| < |A'|^2 \\ \text{De même } |A' + (G+G)A'| < |A'|^2 \end{array} \left. \vphantom{\begin{array}{l} |A' + G.G.A'| \\ |A' + (G+G)A'| \end{array}} \right\} \begin{array}{l} \Rightarrow \\ \text{Lemme} \end{array} \quad G \text{ est un corps.}$$

Comme  $G \subset A' + GG.A'$ , on a  $|G| \leq O(k^{\alpha''})|A'|$   
c'est à dire  $\textcircled{4}$ .

$\textcircled{3}$  découle d'un lemme de recouvrement :

lemme:  $U, V \subset \mathbb{Z}$  groupe

Il existe  $X \subset V$ ,  $B \subset U - V + X$

$$\text{en } |X| \leq \frac{|U+V|}{|U|}$$

On l'applique à  $U = A'$ ,  $V = A$ ,

$$\text{et } |U+V| = |A'+A| \leq |A+A| \leq k|A| \leq 2k^2|A'|$$

$$\text{et } \frac{|U+V|}{|U|} \leq 2k^2 \quad \square$$