Combinatoire additive

1 Généralités

G groupe ambiant.

On étudie les liens entre la structure de groupe et le cardinal de certaines sous-parties. Typiquement on considère A et B deux parties finies de G, et on s'intéresse à l'ensemble produit

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

De même, pour $n \in \mathbb{N}^*$, on note

$$A^n = \{a_1 a_2 \dots a_n \ ; \ a_i \in A\}$$

Exercice 1. Si $|A^2| = |A|$, montrer qu'il existe un sous-groupe fini H et $a \in N(H)$ tel que $A = aH$.

Solution. Soit $a \in A$ quelconque. Montrons que $a^{-1}A$ est un groupe fini. Notons que $aA = A^2 = Aa$ car tous ces ensembles ont le même cardinal, et A^2 contient les deux autres. Donc $H = a^{-1}A = Aa^{-1}$. $HH = a^{-1}AAa^{-1} = a^{-1}aAa^{-1} = Aa^{-1} = H$.

Exercice 2. Supposons maintenant $|A^2| < \frac{3}{2}|A|$. On veut voir qu'il existe un sous-groupe fini H et $a \in N(H)$ tels que $A \subset aH$, $|H| < \frac{3}{2}|A|$.

1. Vérifier que ces conditions donnent bien $|A^2| < \frac{3}{2}|A|$.
2. Soit $H = A^{-1}A$. Montrer que tout $x \in H$ s'écrit de $k > |A|/2$ façons différentes $x = d_1 c_1^{-1} = \dots = d_k c_k^{-1}$.
3. Montrer que H est un sous-groupe fini normalisé par A.
4. Montrer que si $a \in A$ et $B = a^{-1}A$, alors $a^{-1}BaB = H$, et conclure.

Solution. 1. En effet, $A^2 \subset a^2 H$ donc $|A^2| = |H| < \frac{3}{2}|A|$.

2. Écrivons $x = a^{-1}b$. Notons que $|aA \cap bA| = 2|A| - |aA \cup bA| \geq 2|A| - |A^2| > \frac{|A|}{2}$. Donc $|A \cap xA| = k > \frac{|A|}{2}$. Écrivons $A \cap xA = \{d_1, \dots, d_k\}$. Pour chaque i, il existe c_i tel que $d_i = xc_i$, i.e. $x = d_i c_i^{-1}$.

3. Si $x, y \in H$, on écrit $x = d_1 c_1^{-1} = \cdots = d_k c_k^{-1}$ et de même $y = a_1 b_1^{-1} = \cdots = a_k b_k^{-1}$. Comme $k > |A|/2$, il existe i, j tels que $a_i = c_j$, et alors $xy = d_i b_j^{-1} \in AA^{-1}$. Mais le point 2. montre aussi que $H = A^{-1}A = AA^{-1}$. Donc H est stable par multiplication, et comme H est fini, c'est un sous-groupe. Si $a \in A$, $aHa^{-1} \subset AA^{-1}AA^{-1} = HH = H$.

4. Soit a quelconque dans A, on a bien sûr $B = a^{-1}A \subset H$. Pour tout $h \in H$, $a^{-1}Ba$ et hB^{-1} sont des parties de H, non disjointes, pour des raisons de cardinal. Donc il existe b, b' tels que $a^{-1}ba = h(b')^{-1}$ i.e. $h = a^{-1}bab' \in a^{-1}BaB$. Par conséquent, $AA = aBaB = a^2(a^{-1}BaB) = a^2 H$.

La suite du cours a pour but de comprendre les parties telles que $|A^2| \leq K|A|$, pour un certain $K \geq 1$. Si $K > \frac{3}{2}$, il n'y a pas de caractérisation simple comme ci-dessus.

Définition 1 (Distance de Ruzsa)**.**

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

Exercice 3. 1. $d(A, B) \geq 0$;

2. $d(A, B) = d(B, A)$;

3. $d(A, B) = 0$ si et seulement si $A = aH$ et $B = bH$ pour un certain sous-groupe fini H.

Solution. Si $d(A, B) = 0$ alors $|AB^{-1}| = \sqrt{|A||B|}$ donc $|A| = |B| = |AB^{-1}| = |BA^{-1}|$. Soit $a \in A$ et $b \in B$. Notons que $AB^{-1} = aB^{-1} = Ab^{-1}$. Donc l'ensemble $H = a^{-1}A$ vérifie $H = B^{-1}b$. Par conséquent $HH = a^{-1}AB^{-1}b = a^{-1}aB^{-1}b = B^{-1}b = H$.

Lemme 2 (Inégalité triangulaire)**.** *Pour toutes parties finies A, B, C,*

$$d(A, C) \leq d(A, B) + d(B, C).$$

Proof. Cela signifie
$$|AC^{-1}||B| \leq |AB^{-1}||BC^{-1}|.$$
Pour voir cela, on choisit pour chaque $x \in AC^{-1}$ une écriture $x = a_x c_x^{-1}$, et on considère l'application $AC^{-1} \times B \to AB^{-1} \times BC^{-1}$ définie par $(x, b) \mapsto (a_x b^{-1}, bc_x^{-1})$. Cette application est injective, ce qui montre l'inégalité souhaitée. □

Proposition 3. *Soit $A \subset G$ et $K \geq 2$, tel que $|A^3| \leq K|A|$. Alors, pour tout $n \geq 3$, $|A^n| \leq K^{2n-5}|A|$. Plus généralement, si $\varepsilon_i \in \{-1, 1\}$, $|A^{\varepsilon_1} \dots A^{\varepsilon_n}| \leq K^{5n}|A|$.*

Proof. En effet, par l'inégalité triangulaire,
$$d(A^{n-1}, A^{-2}) \leq d(A^{n-1}, A^{-1}) + d(A^{-1}, A) + d(A, A^{-2})$$
Donc $|A^{n+1}| \leq |A^n| \frac{|A^2|}{|A|} \frac{|A^3|}{|A|} \leq K^2|A^n|$, et par récurrence, cela démontre la première assertion.

Pour la deuxième partie, notons $A_n = A^{\varepsilon_1} \dots A^{\varepsilon_n}$, et écrivons
$$d(A_{n-1}, A^{-\varepsilon_n} A^{-\varepsilon_{n-1}}) \leq d(A_{n-1}, A^{-\varepsilon_n}) + d(A^{-\varepsilon_n}, A) + d(A, A^{-\varepsilon_n} A^{-\varepsilon_{n-1}}).$$
Cela donne
$$|A_{n+1}| \leq |A_n| \frac{|AA^{\varepsilon_{n-1}}|}{|A|} \frac{|AA^{\varepsilon_{n-1}} A^{\varepsilon_n}|}{|A|}$$
Donc il suffit de contrôler les deux quotients de droite. Par exemple, comme $d(A, A) \leq d(A, A^{-1}) + d(A^{-1}, A)$, on trouve $|AA^{-1}| \leq \frac{|AA|^2}{|A|} \leq K^2|A|$. Et de même (à vérifier en exercice) $|AA^{\varepsilon_{n-1}} A^{\varepsilon_n}| \leq K^3|A|$. □

Exercice 4. Montrer que la proposition n'est pas valable si l'on suppose seulement $|A^2| \leq K|A|$.

Solution. Dans $F_2 = \langle a, b \rangle$, on prend $A = \{1, a, \dots, a^n\} \cup \{b\}$. Alors $A^2 = \{1, a, \dots, a^{2n}\} \cup \{ba^i, i \leq n\} \cup \{a^i b, i \leq n\}$ donc $|A^2| \leq 5n \leq 5|A|$. Mais $A^3 \supset \{a^i b a^j \ ; \ i, j \leq n\}$ donc $|A^3| \geq n^2 \geq n|A|$.

Définition 4 (Sous-groupe approximatif)**.** Pour $K \geq 1$, un ensemble $A \subset G$ est un *sous-groupe K-approximatif* s'il vérifie

1. $1 \in A$ et $A = A^{-1}$;

2. $A^2 \subset AX$ où $X \subset G$ vérifie $|X| \leq K$.

Exercice 5. Vérifier que si H est un sous-groupe K-approximatif, alors pour tout n, $|H^n| \leq K^n|H|$.

Solution. Par récurrence, $H^n \subset HX^n$ et donc $|H^n| \leq |H||X|^n \leq K^n|H|$.

Lemme 5 (Lemme de recouvrement de Ruzsa)**.** *Si $|AB| \leq K|A|$ alors il existe $X \subset B$ tel que $|X| \leq K$ et $B \subset A^{-1}AX$.*

Proof. Soit $b_1, \ldots, b_k$ une famille maximale d'éléments de B telle que les parties $Ab_1, \ldots, Ab_k$ soient disjointes. Comme toutes ces parties sont incluses dans AB et $|AB| \leq K|A|$, on doit avoir $k \leq K$. De plus, si $b \in B$, il existe i tel que Ab rencontre Ab_i, par maximalité, et donc $b \in A^{-1}Ab_i$. Cela montre que $B \subset A^{-1}AX$, où $X = \{b_1, \ldots, b_i\}$. □

Proposition 6 (Caractérisation des ensembles à petit triplement)**.** *Soit $A \subset G$ et $K \geq 2$. Les assertions suivantes sont équivalentes.*

1. $|A^3| \leq K^{O(1)}|A|$*;*
2. *Il existe un sous-groupe $K^{O(1)}$-approximatif tel que $A \subset H$ et $|H| \leq K^{O(1)}|A|$.*

Proof. Il est clair que 2 imlique 1: si $A \subset H$ avec $|H| \leq K|A|$ et H K-approximatif, alors $|A^3| \leq |H^3| \leq K^2|H| \leq K^3|A|$.

Pour la réciproque, supposons $|A^3| \leq K|A|$, et montrons que $H = (A \cup A^{-1} \cup \{1\})^2$ est un sous-groupe $K^{O(1)}$-approximatif. Comme $H \ni 1$ et $H = H^{-1}$, il suffit de voir que $H \subset HX$ pour un certain X tel que $|X| \leq K^{O(1)}$. Notons $A_1 = A \cup A^{-1} \cup \{1\}$. Alors A_1^5 est inclus dans la réunion des $A^{\varepsilon_1}A^{\varepsilon_2}A^{\varepsilon_3}A^{\varepsilon_4}A^{\varepsilon_5}$, avec $\varepsilon_i \in \{-1, 0, 1\}$, donc, d'après la proposition sur les ensembles à petit triplement, $|A_1^5| \leq K^{O(1)}|A|$. Par le lemme de recouvrement appliqué à $B = H^2 = A_1^4$ et $A = A_1$, cela implique $H^2 \subset A_1^{-1}A_1X = HX$ pour un certain X tel que $|X| \leq K^{O(1)}$. □

Proposition 7 (Caractérisation des ensembles à petit doublement)**.** *Pour $A, B \subset G$ et $K \geq 2$, les assertions suivantes sont équivalentes.*

1. $|AB| \leq K^{O(1)}|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$*;*
2. *Il existe un sous-groupe $K^{O(1)}$-approximatif H et $X, Y \subset G$ telles que $|X|, |Y| \leq K^{O(1)}$ et $A \subset XH$ et $B \subset HY$.*

Remarque. Il est facile de voir que 2 implique 1: $AB \subset XHHY$ donc $|AB| \leq K^{O(1)}|HH| \leq K^{O(1)}|H|$. L'autre implication est sensiblement plus difficile à démontrer.

Définition 8 (Énergie multiplicative)**.** Étant donnés $A, B \subset G$, on définit

$$E(A,B) = |\{(a,b,a',b') \in A \times B \times A \times B \mid ab = a'b'\}|.$$

Proposition 9. *1.* $E(A,B) = \|1_A * 1_B\|_2^2$*;*

2. $\forall g, h, \quad E(gA, Bh) = E(A,B)$*;*

3. $E(A, A^{-1}) = E(A^{-1}, A)$*;*

4. $|A||B| \leq E(A,B) \leq |A|^{3/2}|B|^{3/2}$*;*

5. Si $|AB| \leq K|A|^{1/2}|B|^{1/2}$*, alors* $E(A,B) \geq \frac{1}{K}|A|^{3/2}|B|^{3/2}$*;*

6. Si $E(A,B) \geq \frac{1}{K}|A|^{3/2}|B|^{3/2}$ *alors il existe* $S \subset A \times B$ *tel que* $|S| \geq \frac{1}{2K}|A||B|$ *et* $|A \cdot_S B| \leq 2K|A|^{1/2}|B|^{1/2}$*, où*

$$A \cdot_S B = \{ab \ ; \ (a,b) \in S\}.$$

Proof. La vérification des quatres premières propriétés est laissée en exercice.

5. Montrons que si $\phi : X \to Z$ et $E_\phi = |\{(x,y) \in X \times X \mid \phi(x) = \phi(y)\}|$, alors

$$E_\phi |\phi(X)| \geq |X|^2.$$

Il suffit d'appliquer l'inégalité de Cauchy-Schwarz, en notant $\phi(X) = \{z_1, \ldots, z_k\}$ et $n_i = |\{|x \mid \phi(x) = z_i\}$. Alors $E_\phi = \sum n_i^2$, $|\phi(X)| = k$ et $|X| = \sum n_i$. En prenant $X = A \times B$ et $\phi : (a,b) \mapsto ab$, on obtient l'inégalité souhaitée.

6. On pose

$$S = \{(a,b) \mid ab \text{ a au moins } \frac{1}{2K}|A|^{1/2}|B|^{1/2} \text{ représentations sous la forme } a'b'\}.$$

Il est clair que $|A \cdot_S B| \leq 2K|A|^{1/2}|B|^{1/2}$. De plus,

$$\frac{|A|^{3/2}|B|^{3/2}}{K} \leq E(A,B) \leq |S||A|^{1/2}|B|^{1/2} + \frac{1}{2K}|A|^{1/2}|B|^{1/2}|A||B|$$

donc $|S| \geq \frac{|A||B|}{2K}$. □

Exercice 6. Montrer que $E(B,A) \neq E(A,B)$ en général.

Solution. Dans $F_2 = \langle a, b\rangle$, on choisit $A = \{1, a, \dots, a^n\}$ et $B = Ab$. Alors $AB = \{a^i b \ ; \ i \leq 2n\}$ donc $|AB| \leq 2n+1$ et $E(A,B) \gg n^3$. Tandis que $a^k b a^l = a^{k'} b a^{l'}$ implique $k = k'$ et $l = l'$ donc $E(B,A) \ll n^2$.

Lemme 10 (Balog-Szemerédi-Gowers, énergie multiplicative)**.** *Soit $K \geq 2$, $A, B \subset G$ tels que $E(A,B) \geq \frac{1}{K}|A|^{3/2}|B|^{3/2}$. Alors, il existe $A' \subset A$ et $B' \subset B$ tels que*

1. *$|A'| \geq K^{O(1)}|A|$ et $|B'| \geq K^{O(1)}|B|$;*
2. *$|A'B'| \leq K^{O(1)}|A|^{1/2}|B|^{1/2}$*

Lemme 11 (Balog-Szemerédi-Gowers, théorie des graphes)**.** *Soit $A \sqcup B$ un graphe biparti tel que $|A|, |B| \leq n$ contenant au moins $\frac{n^2}{K}$ arêtes. Alors, il existe $A' \subset A$ et $B' \subset B$ tels que*

1. *$|A'| \geq K^{O(1)}|A|$ et $|B'| \geq K^{O(1)}|B|$;*
2. *Pour tout $(a,b) \in A' \times B'$, il existe au moins $K^{-O(1)}n^2$ chemins de longueur 3 entre a et b.*

Notation: pour $x \in A \sqcup B$, on note $V(x)$ l'ensemble des voisins de x. Pour $X \subset A$ (ou $X \subset B$) on note $V(X) = \cap_{x \in X} V(x)$ l'ensemble des voisins communs à tous les points de X.

Exercice 7. Montrer que sous les hypothèses du lemme, il n'existe pas nécessairement A' et B' satisfaisant la première condition et tels que $\forall (a,b) \in A' \times B'$, $a \leftrightarrow b$. (Et vérifier que si on avait cette propriété, alors on aurait bien le point 2 ci-dessus.)

Solution. Si A', B' sont de cardinal $K^{-O(1)}n$ et totalement connectés, et si $(a,b) \in A' \times B'$, tout chemin $a - b' - a' - b$ avec $a' \in A'$ et $b' \in B'$ connecte a et b, donc on trouve bien $K^{-O(1)}n^2$ chemins de longueur 3.

Graphe aléatoire $A \sqcup B$ biparti où chaque arête est retenue avec probabilité $1/2$. Si $A' \subset A$ et $b \in B$, alors

$$\mathbb{P}(b \in V(A')) = 2^{-|A'|}$$

Donc

$$\mathbb{E}[|V(A')|] \leq 2^{-|A'|}|B|.$$

La probabilité d'avoir $|V(A')| \geq n/K$, avec K fixé est infime si $|A'| \geq n/K$. (Cela ne répond pas tout à fait à la question, et il faudrait compléter la démonstration.)

Démonstration du lemme de BSG. On restreint le graphe à $A \sqcup B_0$, où

$$B_0 = \{b \in B \mid |V(b)| \geq \frac{n}{2K}\}.$$

Le nombre d'arêtes dans $A \sqcup B_0$ est supérieur à $n^2/(2K)$. Soit x un point aléatoire choisi uniformément dans A.

$$\mathbb{E}[|V(x)|] = \frac{1}{|A|}|\{arêtes\}| \geq \frac{n}{2K}.$$

Un couple (b, b') d'éléments de B_0 est dit *mal connecté* si

$$|V(b, b')| \leq \frac{n}{128K^3}.$$

Soit

$$N(x) = |\{(b, b') \in V(x) \times V(x) \text{ mal connecté}\}|$$

Remarquons que si (b, b') est un couple d'éléments de $V(x)$ mal connecté, on a $x \in V(b, b')$. Mais $|V(b, b')| \leq \frac{n}{128K^3}$ donc $\mathbb{P}(x \in V(b, b')) \leq \frac{1}{128K^3}$ et par conséquent

$$\mathbb{E}[N(x)] \leq \frac{n^2}{128K^3}.$$

Soit $Z(x) \subset V(x)$ l'ensemble des éléments b mal connectés à au moins $\frac{n}{32K^2}$ éléments $b' \in V(x)$. Comme $N(x) \geq \frac{n}{32K^2}|Z(x)|$, on a

$$E[|Z(x)|] \leq \frac{n}{4K}.$$

Donc on peut choisir x tel que l'ensemble $B' = V(x) \setminus Z(x)$ vérifie $|B'| \geq \frac{n}{4K}$. On pose ensuite

$$A' = \{a \in A \mid |V(a) \cap B'| \geq \frac{n}{16K^2}\}.$$

Soit R le nombre d'arêtes partant de B'. On a

$$\frac{n^2}{8K^2} \leq |B'|\frac{n}{2K} \leq R \leq |A'|n + n\frac{n}{16K^2}$$

donc $|A'| \geq \frac{n}{16K^2}$.

Soit $(a,b) \in A' \times B'$ on a $|V(a) \cap B'| \geq \frac{n}{16K^2}$ donc (b,b') est bien connecté pour au moins $\frac{n}{32K^2}$ éléments $b' \in V(a) \cap B'$. Pour chaque $b' \in V(a) \cap B'$, bien connecté à b, il y a $\frac{n}{128K^3}$ chemins $b' - a' - b$, $a' \in A$. Donc au total, cela fait $\frac{n}{128K^3}\frac{n}{16K^2} = \frac{n^2}{K^{O(1)}}$ chemins $a - b' - a' - b$ de longueur 3 entre a et b. □

Démonstration de BSG, énergie multiplicative. Soit A, B tels que $E(A,B) \geq K^{-1}|A|^{3/2}|B|^{3/2}$, on veut construire A' et B' riches dans A et B tels que $|A'B'| \leq K^{-O(1)}|A|^{1/2}|B|^{1/2}$.

D'après le point 6 de la proposition 9, il existe $S \subset A \times B$ tel que $|S| \geq K^{-O(1)}|A||B|$, et $|A \cdot_S B| \leq K|A|^{1/2}|B|^{1/2}$. Posons $n = \max(|A|,|B|)$. On vérifie sans peine que le nombre d'arêtes du graphe $A \sqcup B$ défini par la partie S est minoré par $K^{-O(1)}n^2$.

Soient A' et B' les parties données par le lemme de théorie des graphes. Notons que $A'B' \subset (A \cdot_S B)(A \cdot_S B)^{-1}(A \cdot_S B)$. En effet, si $(a,b) \in A' \times B'$, on a $a - b' - a' - b$ et alors

$$ab = ab'(a'b')^{-1}a'b.$$

Et même tout produit ab dans $A'B'$ admet $K^{-O(1)}n^2$ représentations de cette forme. Donc

$$|A'B'| \leq K^{O(1)}n^{-2}|A \cdot_S B|^3 \leq K^{O(1)}n = K^{O(1)}|A|^{1/2}|B|^{1/2}.$$

□

À partir du lemme de Balog-Szemerédi-Gowers, on peut montrer la caractérisation des parties A,B telles que $|AB| \leq K|A|^{1/2}|B|^{1/2}$ en termes de sous-groupes approximatifs (cf. notes).

2 Somme-produit

Dans le cas commutatif, il suffit de contrôler A^2 pour contrôler toutes les puissances A^n. Dans la suite, on note G additivement, et en particulier

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

et pour $k \in \mathbb{N}^*$,

$$kA = \{a_1 + \cdots + a_k \ ; \ a_i \in A\}.$$

Théorème 12 (Inégalité de Plünnecke)**.** *Soit $(G,+)$ un groupe abélien, et $A \subset G$ telle que $|A+A| \leq K|A|$. Alors, pour tous entiers naturels k, l,*

$$|kA - lA| \leq K^{k+l}|A|.$$

La démonstration utilise le lemme suivant.

Lemme 13 (Petridis)**.** *Soit A, B deux parties de $(G,+)$. Soit $B_0 \subset B$ tel que le rapport $\frac{|A+B_0|}{|B_0|}$ soit minimal. Alors, pour toute partie $X \subset G$,*

$$|A + B_0 + X| \leq K_0|B_0 + X|$$

où $K_0 = \frac{|A+B_0|}{|B_0|}$.

Proof. On procède par récurrence sur $|X|$. Si $|X| = 1$,

$$|A + B_0 + X| = |A + B_0| = K_0|B_0| = K_0|B_0 + X|.$$

Supposons le résultat connu pour $|X| = n \geq 1$ et soit X tel que $|X| = n+1$. Écrivons $X = X' \cup \{x\}$, pour x quelconque dans X et $X' = X \setminus \{x\}$. Alors

$$\begin{aligned} |A + B_0 + X| &= |A + B_0 + X'| + |A + B_0 + x| - |(A + B_0 + X') \cap (A + B_0 + x)| \\ &\leq K_0|B_0 + X'| + K_0|B_0 + x| - |(A + B_0 + X') \cap (A + B_0 + x)| \\ &\leq K_0|B_0 + X'| + K_0|B_0 + x| - |(A + Z + x)| \end{aligned}$$

où $Z = \{z \in B_0 \mid A+z+x \subset A+B_0+X'\}$. Notons que $Z \supset B_0 \cap (B_0+X'-x)$ et donc $|Z| \geq |(B_0 + x) \cap (B_0 + X')|$. De plus, $Z \subset B$ donc par définition de K_0, $|A + Z| \geq K_0|Z|$. Cela donne ce qu'on veut:

$$\begin{aligned} |A + B_0 + X| &\leq K_0|B_0 + X'| + K_0|B_0 + x| - |(A + Z)| \\ &\leq K_0(|B_0 + X'| + |B_0 + x| - |Z|) \\ &\leq K_0(|B_0 + X'| + |B_0 + x| - |(B_0 + x) \cap (B_0 + X')|) \\ &= K_0|B_0 + X|. \end{aligned}$$

□

Exercice 8. Montrer que le lemme de Petridis implique l'inégalité de Plünnecke.

Solution. On applique le lemme de Petridis avec $A = B$, cela donne une partie $A_0 \subset A$ telle que pour tout X,

$$|A + A_0 + X| \leq K|A_0 + X|.$$

En particulier, pour $X = (k-1)A$,

$$|A_0 + kA| = |A + A_0 + (k-1)A| \leq K|A_0 + (k-1)A|$$

donc par récurrence, $|A_0 + kA| \leq K^k|A_0|$. De même, $|A_0 + lA| \leq K^l|A_0|$. On applique alors l'inégalité de Ruzsa: $d(kA, lA) \leq d(kA, -A_0) + d(-A_0, lA)$, cela donne

$$|kA - lA| \leq \frac{|kA + A_0||lA + A_0|}{|A_0|} \leq K^{k+l}|A_0| \leq K^{k+l}|A|.$$

Théorème 14 (Somme-produit dans $\mathbb{F}_p$)**.** *Il existe $\tau > 0$ tel que pour tout p premier et tout $A \subset \mathbb{F}_p$,*

$$|A + A| + |AA| \geq |A| \min(|A|, \frac{p}{|A|})^\tau.$$

En d'autres termes, pour tout $\varepsilon > 0$, si $|A| < p^{1-\varepsilon}$, alors soit $|A + A| \geq |A|^{1+\tau}$ soit $|AA| \geq |A|^{1+\tau}$.