ENS MPI 2009 MATHS-1 D'APRÈS LE CORRIGÉ DE M. QUERCIA

Partie I. Somme de parties

I.1. **a.** Par récurrence sur n en utilisant la formule de Pascal.

b. On associe à un t-uplet $a = (a_1, \dots, a_t)$ d'entiers naturels la suite finie à valeurs dans un ensemble à deux éléments $\{\bullet, |\}$:

$$\varphi(a) = (\underbrace{\bullet \cdots \bullet}_{a_1 \text{ fois}} | \underbrace{\bullet \cdots \bullet}_{a_2 \text{ fois}} | \dots | \underbrace{\bullet \cdots \bullet}_{a_t \text{ fois}}).$$

Cette association définit clairement une bijection entre les suites finies d'entiers naturels et les suites finies à valeurs dans $\{\bullet, |\}$. Et cette bijection envoie les t-uplets de somme N sur les $(N+t-1)$-uplets comportant N symboles $\bullet$ et $t-1$ symboles $|$. Il y a $\binom{N+t-1}{N}$ tels $(N+t-1)$-uplets, d'où le résultat (cf. sujet d'étude n°3 sur l'algèbre élémentaire).

c. $\dfrac{1}{t^N}\binom{N+t-1}{N} = \frac{1}{N!}(1+\frac{N-1}{t})\dots(1+\frac{1}{t})(1+\frac{0}{t})$ décroît par rapport à t à N fixé, vaut 1 pour $t=1$ et tend vers $\dfrac{1}{N!}$ lorsque $t \to \infty$ d'où $\dfrac{1}{N!}t^N \leqslant \binom{N+t-1}{N} \leqslant t^N$.

I.2. **a.** Soit $x \in G$, $A \cap (x - B) \neq \emptyset$ car la somme de leurs cardinaux dépasse $\operatorname{Card} G$; il existe donc $a \in A \cap (x-B)$ et $b \in B$ tels que $a = x - b$, c'est-à-dire $x = a + b$. Ainsi $G \subset A + B$ et l'inclusion inverse est triviale.

b. $G = \mathbb{Z}/2\mathbb{Z}$, $A = B = \{0 \bmod 2\}$.

I.3. **a.** Si $b \in B$ on a $A + b \subset A + B$ d'où $\operatorname{Card}(A) = \operatorname{Card}(A+b) \leqslant \operatorname{Card}(A+B)$. De même $\operatorname{Card}(B) \leqslant \operatorname{Card}(A+B)$, ce qui donne la première inégalité.
Par ailleurs l'application $(a,b) \mapsto a+b$ induit une surjection de $A \times B$ sur $A+B$ d'où $\operatorname{Card}(A+B) \leqslant \operatorname{Card}(A \times B) = \operatorname{Card}(A)\operatorname{Card}(B)$.

b. La suite $(\operatorname{Card}(kA))$ est croissante d'après la question précédente.
Pour prouver la dernière inégalité on note $t = \operatorname{Card}(A)$, $A = \{x_1, \dots, x_t\}$, et on remarque que tout élément x de nA s'écrit d'au moins une manière sous la forme $x = a_1x_1 + \dots + a_tx_t$ où $a_1, \dots, a_t$ sont des entiers naturels tels que $a_1 + \dots + a_t = n$ (réordonner une décomposition de x). Ainsi $\operatorname{Card}(nA)$ est majoré par le nombre de t-uplets $(a_1, \dots, a_t)$, soit par $\binom{n+t-1}{n}$ d'après **1b**.

I.4. **a.** Si $A = \{a_1, \dots, a_p\}$ et $B = \{b_1, \dots, b_q\}$ avec avec $a_1 < \dots < a_p$ et $b_1 < \dots < b_q$ alors

$$a_1 + b_1 < a_1 + b_2 < \dots < a_1 + b_q < a_2 + b_q < \dots < a_p + b_q,$$

donc on a ainsi mis en évidence $p + q - 1$ éléments distincts dans $A + B$.

b. Avec les notations précédentes, si on a $\operatorname{Card}(A+B) = p+q-1$ alors en posant $C = \{a_1+b_1, \dots, a_1+b_q, a_2+b_q, \dots, a_p+b_q\}$, $C \subset A+B$ et ces deux ensembles ont même cardinal, il sont donc égaux. Les nombres $a_2+b_1, \dots, a_2+b_{q-1}$ forment une suite strictement croissante dans cet ensemble, strictement comprise entre a_1+b_1 et a_2+b_q, d'où $a_2+b_i = a_1+b_{i+1}$ pour $1 \leqslant i < q$. En particulier $b_{i+1} - b_i = a_2 - a_1$ donc les éléments de B forment une suite arithmétique de raison $d = a_2 - a_1$. Par symétrie des rôles, les éléments de A forment une suite arithmétique de raison $b_2 - b_1 = d$.

I.5. **a.** $0 \in H$ est évident. Stabilité : si h_1 et $h_2 \in H$ alors $h_1 + (h_2 + A) = h_1 + A = A$. Symétrique : si $h + A = A$ alors $A = -h + A$.
De plus si $a \in H$, on a $H \subset a - A$ donc H est fini et $\mathrm{Card}(H) \leqslant \mathrm{Card}(A)$.

b. On a $\mathrm{Card}(A+b) = \mathrm{Card}(A) \leqslant \mathrm{Card}(A+B)$. Or $A+B \subset A+b+H = A+H+b = A+b$ d'où $A + B = A + b$ et on a bien $\mathrm{Card}(A + B) = \mathrm{Card}(A)$.
Réciproquement, si $\mathrm{Card}(A + B) = \mathrm{Card}(A)$, soit $b \in G$ et $B' = B - b$. On a $A + B' = (A + B) - b$ contient A car $0 \in B'$ et est de même cardinal que A par hypothèse sur B, d'où $A + B' = A$, c'est-à-dire $B' \subset H$. Et donc $B = b + B' \subset b + H$.

I.6. Positivité :

$$\begin{aligned}\mathrm{Card}(A - B) &\geqslant \max(\mathrm{Card}(A), \mathrm{Card}(-B)) = \max(\mathrm{Card}(A)\,\mathrm{Card}(B)) \\ &\geqslant \sqrt{\mathrm{Card}(A)\,\mathrm{Card}(B)}\end{aligned}$$

d'où $d_R(A, B) \geqslant 0$.

Inégalité triangulaire : soit l'application $\varphi : (x, y) \in (A - B)\times(B - C) \mapsto x - y \in G$. Si $z = a - c \in A - C$ alors pour tout $b \in B$ on a $z = \varphi(a - b, b - c)$ donc z a au moins $\mathrm{Card}(B)$ antécédents distincts par φ. On en déduit :

$$\mathrm{Card}(A-B)\,\mathrm{Card}(B-C) = \sum_{z\in G} \mathrm{Card}(\varphi^{-1}(z)) \geqslant \sum_{z\in A-C} \mathrm{Card}(\varphi^{-1}(z)) \geqslant \mathrm{Card}(B)\,\mathrm{Card}(A-C).$$

En divisant les deux membres extrêmes par $\sqrt{\mathrm{Card}(A)\,\mathrm{Card}(B)}\sqrt{\mathrm{Card}(B)\,\mathrm{Card}(C)}$ puis en prenant les logarithmes, on obtient l'inégalité triangulaire demandée.

I.7. Si $d_R(A, B) = 0$ alors $\mathrm{Card}(A-B) = \max(\mathrm{Card}(A), \mathrm{Card}(B)) = \sqrt{\mathrm{Card}(A)\,\mathrm{Card}(B)}$ d'où $\mathrm{Card}(A) = \mathrm{Card}(B)$ dans un premier temps puis $\mathrm{Card}(A - B) = \mathrm{Card}(A) = \mathrm{Card}(B)$.
D'après **5**, $-B \subset -b + H_A$ où $-b$ est un élément quelconque de $-B$ et H_A le sous-groupe associé à A en **5a**.
Ainsi $B \subset b - H_A = b + H_A$, puis $\mathrm{Card}(B) \leqslant \mathrm{Card}(H_A) \leqslant \mathrm{Card}(A) = \mathrm{Card}(B)$, donc $B = b+H_A$, de même, si $a \in A$, $A = a+H_B$. Enfin, si $g_A \in H_A$ alors $a+g_A \in A = a+H_B$ donc $g_A \in H_B$ i.e. $H_A \subset H_B$ et par symétrie, $H_A = H_B$.
Réciproquement, si $A = a + H$ et $B = b + H$ avec $a, b \in G$ et H un sous-groupe fini de G alors $A - B = (a - b) + H$, d'où $\mathrm{Card}(A) = \mathrm{Card}(B) = \mathrm{Card}(H) = \mathrm{Card}(A - B)$ et $d_R(A, B) = 0$.

Partie II. Valeurs aux entiers de formes quadratiques définies positives

II.1. Soit M la matrice de $(\overrightarrow{v_1}, \ldots, \overrightarrow{v_n})$ dans la base canonique $(\overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ de $\mathbb{R}^n$.
La famille $(\overrightarrow{v_1}, \ldots, \overrightarrow{v_n})$ est une base entière si et seulement si $M \in \mathcal{M}_n(\mathbb{Z})$ et $\overrightarrow{e_1}, \ldots, \overrightarrow{e_n}$ sont combinaisons linéaires à coefficients entiers de $(\overrightarrow{v_1}, \ldots, \overrightarrow{v_n})$,
soit si et seulement si $M \in \mathcal{M}_n\mathbb{Z}$ et il existe $P \in \mathcal{M}_n\mathbb{Z}$ telle que $MP = I_n$.
Dans ce cas, $\det(M)\det(P) = 1$ donc $\det(M) \in \{-1, 1\}$ car les deux facteurs sont entiers.
Réciproquement, si $M \in \mathcal{M}_n(\mathbb{Z})$ et $\det(M) = \pm 1$ alors $P = \det(M)^t\mathrm{com}(M) \in \mathcal{M}_n(\mathbb{Z})$ et $MP = I_n$ donc $(\overrightarrow{v_1}, \ldots, \overrightarrow{v_n})$ est une base entière.

II.2. Lorsque $s(\overrightarrow{v}) = 1$, $\overrightarrow{v}$ est au signe près un des vecteurs de la base canonique et il existe donc une base entière commençant par $\overrightarrow{v}$.
Supposons la propriété vraie pour tout vecteur $\overrightarrow{v}$ à coordonnées premières entre elles tel que $s(\overrightarrow{v}) < N$ et considérons $\overrightarrow{v} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ à coordonnées premières entre elles avec $s(\overrightarrow{v}) = N > 1$:
Soit i_0 tel que $|a_{i_0}|$ soit minimal parmi les coordonnées non nulles de $\overrightarrow{v}$ et $j \neq i_0$ tel que $a_j \neq 0$ (j existe sinon $\overrightarrow{v} = a_{i_0}\overrightarrow{e_{i_0}}$ avec $|a_{i_0}| = s(\overrightarrow{v}) > 1$ donc les coordonnées de $\overrightarrow{v}$ ne sont par premières entre elles).

On note $a_j = q|a_{i_0}| + r$ la division euclidienne de a_j par $|a_{i_0}|$ et on considère le vecteur $\overrightarrow{w} = \overrightarrow{v} + (r - a_j)\overrightarrow{e_j} = \sum_{i \neq j} a_i e_i + (a_j - q|a_{i_0}|)e_j$ (c'est-à-dire le vecteur obtenu en remplaçant a_j par r dans $\overrightarrow{v}$ et en conservant toutes les autres coordonnées).
Comme $0 \leqslant r < |a_{i_0}| \leqslant |a_j|$, on a $s(\overrightarrow{w}) < s(\overrightarrow{v}) = N$. De plus, si $\sum_{i=1}^{n} a_i b_i = 1$ alors

$$\sum_{i \neq i_0, j} a_i b_i + a_{i_0}(1+q)b_{i_0} + b_j(a_j - q|a_{i_0}|) = 1,$$

donc les coordonnées de $\overrightarrow{w}$ sont premières entre elles. Par hypothèse de récurrence il existe une base entière commençant par $\overrightarrow{w}$, donc une matrice $M \in \mathcal{M}_n(\mathbb{Z})$ de déterminant ± 1 dont la première colonne représente le vecteur $\overrightarrow{w}$.
Soit $P = I_n + \mathrm{sgn}(a_{i_0}) q E_{j i_0}$ la matrice de l'opération élémentaire $L_j \leftarrow L_j + \mathrm{sgn}(a_{i_0}) q L_{i_0}$: on a $P \in \mathcal{M}_n(\mathbb{Z})$, $\det(P) = 1$ et la première colonne de PM représente $\overrightarrow{v}$.
Enfin $PM \in \mathcal{M}_n(\mathbb{Z})$ et $\det(PM) = \pm 1$ donc PM représente une base entière qui commence par $\overrightarrow{v}$.

Remarque : Victor nous propose une autre démonstration. Toujours par récurrence mais sur n cette fois-ci. On fait l'hypothèse de récurrence suivante : pour $n \geqslant 1$, $\overrightarrow{v_1} \in \mathbb{Z}^n$ de coordonnées première entre-elles dans leur ensemble, il existe une base entière $(\overrightarrow{v_1}, \ldots, \overrightarrow{v_n})$ et, quitte à multiplier $\overrightarrow{v_1}$ par -1, on peut supposer que la matrice $M_n = (\overrightarrow{v_1} | \ldots | \overrightarrow{v_n})$ admet un déterminant qui vaut 1.

- $n = 1$: immédiat (on peut éventuellement multiplier $\overrightarrow{v_1}$ par -1).
- On suppose la propriété vraie à l'ordre $n-1$, $n \geqslant 2$. Soit $d = a_1 \wedge \ldots \wedge a_{n-1}$, on a par hypothèse $d \wedge a_n = 1$ soit, il existe $(u, v) \in \mathbb{Z}^2$ tel que $ua_n + vd = 1$. alors, avec M'_{n-1} la matrice issue de la récurrence, formée à partir du vecteur $\overrightarrow{v'_1}/d$ où $\overrightarrow{v'_1} = (a_1, \ldots, a_{n-1})$ et en multipliant la première colonne par d, on peut poser
$$M_n = \begin{pmatrix} & & -ua_1/d \\ & M'_{n-1} & \vdots \\ & & -ua_{n-1}/d \\ a_n & 0 \ \ldots \ 0 & v \end{pmatrix}.$$
En effet, en développant par rapport à la dernière ligne, on a $a_n(-1)^{n+1} \det M''_{n-1} + v \det M'_{n-1}$. Or $\det M'_{n-1} = d$ et M''_{n-1} s'obtient à partir de M'_{n-1} en faisant la permutation circulaire c^{-1} où $c = (1, 2, \ldots, n)$ et en multipliant la dernière colonne par $-u/d$. On a ainsi $\det M''_{n-1} = (-1)^{n-1} u/d \det M'_{n-1} = (-1)^{n-1} u$ et, par conséquent $\det M_n = 1$ c.q.f.d.

II.3. Soit A la matrice (symétrique) de Φ, M la matrice de u dans la base canonique et X celle d'un vecteur de $\mathbb{R}^n$ alors $\Phi(x) = {}^tXAX$ et $\Phi \circ u(x) = {}^tX {}^tMAMX$ d'où

$$\mathrm{disc}\,(\Phi_1) = \det {}^tM \det A \det M = \det M^2 \det A = \det(u)^2 \mathrm{disc}\,(\Phi).$$

II.4. **a.** Φ étant définie positive, $\sqrt{\Phi}$ est une norme sur $\mathbb{R}^n$.
En particulier, $A = \{\overrightarrow{v} \in \mathbb{Z}^n \setminus \{0\} \text{ tq } \Phi(\overrightarrow{v}) \leqslant \Phi(\overrightarrow{e_1})\}$ est une partie bornée de $\mathbb{Z}^n$, non vide, donc finie. Ainsi il existe $\overrightarrow{v_1} \in A$ tel que $\Phi(\overrightarrow{v_1})$ est minimal.
Alors pour $\overrightarrow{v} \in \mathbb{Z}^n \setminus \{0\}$, on a $\Phi(\overrightarrow{v}) \geqslant \Phi(\overrightarrow{v_1})$ si $\overrightarrow{v} \in A$ et $\Phi(\overrightarrow{v}) \geqslant \Phi(\overrightarrow{e_1}) \geqslant \Phi(\overrightarrow{v_1})$ si $\overrightarrow{v} \notin A$. Ceci prouve que $\Phi(\overrightarrow{v_1}) = \min\{\Phi(\overrightarrow{v}),\ \overrightarrow{v} \in \mathbb{Z}^n \setminus \{0\}\}$ et ce minimum est strictement positif car $\overrightarrow{v_1} \neq 0$ et Φ est définie positive.

b. Il suffit de prouver que les coordonnées de $\overrightarrow{v_1}$ sont premières entre elles.
De fait, si d est le pgcd des coordonnées de $\overrightarrow{v_1}$ alors $d > 0$ car $\overrightarrow{v_1} \neq 0$ et $\overrightarrow{v_1}/d \in \mathbb{Z}^n \setminus \{0\}$. Donc $\Phi(\overrightarrow{v_1}) \leqslant \Phi(\overrightarrow{v_1}/d) = \Phi(\overrightarrow{v_1})/d^2$, d'où $d \leqslant 1$ et donc $d = 1$.

c. Soit f la forme polaire de Φ.
Pour $x_1,\dots,x_n\in\mathbb{R}$ on a, en notant $\overrightarrow{y}=x_2\overrightarrow{v_2}+\cdots+x_n\overrightarrow{v_n}$:

$$\begin{aligned}\Phi(x_1\overrightarrow{v_1}+\cdots+x_n\overrightarrow{v_n}) &= x_1^2\Phi(\overrightarrow{v_1})+2x_1f(\overrightarrow{v_1},\overrightarrow{y})+\Phi(\overrightarrow{y})\\ &= m(\Phi)\underbrace{(x_1+f(\overrightarrow{v_1},\overrightarrow{y})/m(\Phi))}_{L_1(x_1,\dots,x_n)}{}^2+\underbrace{\Phi(\overrightarrow{y})-f(\overrightarrow{v_1},\overrightarrow{y})^2/m(\Phi)}_{\Phi_1(x_2,\dots,x_n)}.\end{aligned}$$

d. On reprend les notations de la question précédente.
Soit $(x_2,\dots,x_n)\in\mathbb{R}^{n-1}$ et $x_1=-f(\overrightarrow{v_1},\overrightarrow{y})/m(\Phi)$, $\Phi_1(x_2,\dots,x_n)=\Phi(x_1\overrightarrow{v_1}+\overrightarrow{y})\geqslant 0$. $\Phi_1(x_2,\dots,x_n)=0$ si et seulement si $x_1\overrightarrow{v_1}+\overrightarrow{y}=0$, soit si et seulement si $\overrightarrow{y}=0$, soit encore si et seulement si $x_2=\cdots=x_n=0$. Donc Φ_1 est définie positive.

Considérons à présent les endomorphismes u,v de $\mathbb{R}^n$ définis par

$$u(x_1,\dots,x_n)=(L(x_1,\dots,x_n),x_2,\dots,x_n),\ v(x_1,\dots,x_n)=x_1\overrightarrow{v_1}+\cdots+x_n\overrightarrow{v_n}.$$

On a $\det(u)=L(1,0,\dots,0)=1$ et $\det(v)=\det_{(\overrightarrow{e_1},\dots,\overrightarrow{e_n})}(\overrightarrow{v_1},\dots,\overrightarrow{v_n})=\pm1$ car $(\overrightarrow{v_1},\dots,\overrightarrow{v_n})$ est une base entière.
Notons enfin $\Phi_1'(x_1,\dots,x_n)=m(\Phi)x_1^2+\Phi_1(x_2,\dots,x_n)$. Avec **3**, on obtient :

$$\begin{aligned}\operatorname{disc}(\Phi)=\operatorname{disc}(\Phi)\det(v)^2&=\operatorname{disc}(\Phi\circ v)=\operatorname{disc}(\Phi_1'\circ u)\\ &=\operatorname{disc}(\Phi_1')\det(u)^2=\operatorname{disc}(\Phi_1')=m(\Phi)\operatorname{disc}(\Phi_1).\end{aligned}$$

e. Prendre pour x_1 l'entier le plus proche de $-f(\overrightarrow{v_1},\overrightarrow{y})/m(\Phi)$.

f. Soit $(x_2,\dots,x_n)\in\mathbb{Z}^{n-1}\setminus\{0\}$ tel que $\Phi_1(x_2,\dots,x_n)=m(\Phi_1)$ et $x_1\in\mathbb{Z}$ tel que $|L(x_1,\dots,x_n)|\leqslant\frac{1}{2}$.
On a donc $m(\Phi)\leqslant\Phi(x_1\overrightarrow{v_1}+\cdots+x_n\overrightarrow{v_n})\leqslant\frac{1}{4}m(\Phi)+m(\Phi_1)$, ce qui donne l'inégalité demandée.

g. Avec **4d** et **4f** on obtient

$$\frac{m(\Phi)^n}{\operatorname{disc}(\Phi)}=\frac{m(\Phi)^{n-1}}{\operatorname{disc}(\Phi_1)}\leqslant\left(\frac{4}{3}\right)^{n-1}\frac{m(\Phi_1)^n}{\operatorname{disc}(\Phi_1)},$$

donc $(\frac{3}{4})^{1+\cdots+(n-1)}\dfrac{m(\Phi)^n}{\operatorname{disc}(\Phi)}\leqslant(\frac{3}{4})^{1+\cdots+(n-2)}\dfrac{m(\Phi_1)^n}{\operatorname{disc}(\Phi_1)}$ qui est une fonction décroissante de la dimension.
Pour $n=1$ elle vaut clairement 1, et l'on en déduit l'inégalité demandée (inégalité de Hermite).

h. Pour $n=1$ c'est évident.
Pour $n>1$ on choisit $\overrightarrow{v_1}\in\mathbb{Z}^n\setminus\{0\}$ tel que $\Phi(\overrightarrow{v_1})=m(\Phi)$ et on complète $(\overrightarrow{v_1})$ en une base entière $(\overrightarrow{v_1},\dots,\overrightarrow{v_n})$. Soit Φ_1 la forme quadratique sur $\mathbb{R}^{n-1}$ définie en **4c**. Par hypothèse de récurrence il existe une base entière $(\overrightarrow{u_2},\dots,\overrightarrow{u_n})$ de $\mathbb{R}^{n-1}$ telle que $\Phi_1(\overrightarrow{u_2})\dots\Phi_1(\overrightarrow{u_n})\leqslant(\frac{4}{3})^{(n-1)(n-2)/2}\operatorname{disc}(\Phi_1)$.

Soit $\overrightarrow{u_i}=(x_{i,2},\dots,x_{i,n})$ et $x_{i,1}\in\mathbb{Z}$ tel que $|L_1(x_{i,1},\dots,x_{i,n})|\leqslant\frac{1}{2}$. On pose alors $\overrightarrow{w_i}=x_{i,1}\overrightarrow{v_1}+\cdots+x_{i,n}\overrightarrow{v_n}$ et on vérifie que $(\overrightarrow{v_1},\overrightarrow{w_2},\dots,\overrightarrow{w_n})$ répond au problème :
on a $\Phi(\overrightarrow{w_i})=m(\Phi)L_1^2(x_{i,1},\dots,x_{i,n})+\Phi_1(\overrightarrow{u_i})\leqslant\frac{1}{4}\Phi(\overrightarrow{w_i})+\Phi_1(\overrightarrow{u_i})$ donc $\Phi(\overrightarrow{w_i})\leqslant\frac{4}{3}\Phi_1(\overrightarrow{u_i})$.
Ainsi :

$$\Phi(\overrightarrow{v_1})\Phi(\overrightarrow{w_2})\dots\Phi(\overrightarrow{w_n})\leqslant m(\Phi)(\tfrac{4}{3})^{n-1}\Phi_1(\overrightarrow{u_2})\dots\Phi_1(\overrightarrow{u_n})\leqslant(\tfrac{4}{3})^{n(n-1)/2}\operatorname{disc}(\Phi).$$

Si $\overrightarrow{v}\in\mathbb{Z}^n$, il existe des entiers $\alpha_1,\dots,\alpha_n$ tels que $\overrightarrow{v}=\alpha_1\overrightarrow{v_1}+\cdots+\alpha_n\overrightarrow{v_n}$ et il existe des entiers $\beta_2,\dots,\beta_n$ tels que $(\alpha_2,\dots,\alpha_n)=\beta_1\overrightarrow{u_1}+\cdots+\beta_n\overrightarrow{u_n}$. Alors :

$$\alpha_2\overrightarrow{v_2}+\cdots+\alpha_n\overrightarrow{v_n}=\beta_2(\overrightarrow{w_2}-x_{2,1}\overrightarrow{v_1})+\cdots+\beta_n(\overrightarrow{w_n}-x_{n,1}\overrightarrow{v_1}).$$

Ceci prouve que $\overrightarrow{v}$ est combinaison linéaire à coefficients entiers de $(\overrightarrow{v_1},\overrightarrow{w_2},\dots,\overrightarrow{w_n})$ et donc cette famille est bien une base entière de $\mathbb{R}^n$.

Partie III. Transformation de Fourier et somme d'ensembles

III.1. Calcul immédiat.

III.2. **a.** $\sum_{x\in\mathbb{Z}/n\mathbb{Z}} \hat{f}(x)\omega^{-ax} = \sum_{x\in\mathbb{Z}/n\mathbb{Z}}\sum_{b\in\mathbb{Z}/n\mathbb{Z}} f(b)\omega^{(b-a)x} = \sum_{b\in\mathbb{Z}/n\mathbb{Z}}\sum_{x\in\mathbb{Z}/n\mathbb{Z}} f(b)\omega^{(b-a)x}$. La somme interne vaut 0 si $b\neq a$ et $Nf(a)$ si $b=a$ donc la somme double vaut $Nf(a)$.

b.

$$\begin{aligned}\sum_{x\in\mathbb{Z}/n\mathbb{Z}} \hat{f}(x)\hat{g}(-x) &= \sum_{x\in\mathbb{Z}}\sum_{a\in\mathbb{Z}/n\mathbb{Z}} \hat{f}(x)g(a)\omega^{-ax} = \sum_{a\in\mathbb{Z}}\sum_{x\in\mathbb{Z}/n\mathbb{Z}} \hat{f}(x)g(a)\omega^{-ax}\\ &= \sum_{a\in\mathbb{Z}/n\mathbb{Z}} Nf(a)g(a)\end{aligned}$$

c.

$$\begin{aligned}\widehat{f*g}(x) &= \sum_{a\in\mathbb{Z}/n\mathbb{Z}} (f*g)(a)\omega^{ax} = \sum_{a\in\mathbb{Z}/n\mathbb{Z}}\sum_{b\in\mathbb{Z}/n\mathbb{Z}} f(b)g(a-b)\omega^{ax}\\ &= \sum_{b\in\mathbb{Z}/n\mathbb{Z}}\sum_{a\in\mathbb{Z}/n\mathbb{Z}} f(b)g(a-b)\omega^{ax} = \sum_{b\in\mathbb{Z}/n\mathbb{Z}}\sum_{c\in\mathbb{Z}/n\mathbb{Z}} f(b)g(c)\omega^{(b+c)x}\\ &= \Big(\sum_{b\in\mathbb{Z}/n\mathbb{Z}} f(b)\omega^{bx}\Big)\Big(\sum_{c\in\mathbb{Z}/n\mathbb{Z}} g(c)\omega^{cx}\Big) = \hat{f}(x)\hat{g}(x).\end{aligned}$$

III.3. **a.** On peut remarquer que $\overline{\hat{f}(x)} = \hat{\overline{f}}(-x)$ et on utilise le **2.a** (merci Martin) d'où $\sum_{x\in\mathbb{Z}/n\mathbb{Z}} |\hat{f}_A(x)|^2 = \sum_{a\in a}\sum_{b=a} N = N\,\mathrm{Card}(A)$.
Ensuite, un peu de calcul

$$\begin{aligned}\sum_{x\in\mathbb{Z}/n\mathbb{Z}} |\hat{f}_A(x)|^4 &= \sum_{x\in\mathbb{Z}/n\mathbb{Z}}\sum_{a\in A}\sum_{b\in A}\sum_{c\in A}\sum_{d\in A}\omega^{(a+b-c-d)x} = \sum_{a\in A}\sum_{b\in A}\sum_{c\in A}\sum_{d=a+b-c} N\\ &= N\,\mathrm{Card}\{(a,b,c,d)\in A^4 \text{ tq } a+b=c+d\}.\end{aligned}$$

b. On a de même $\sum_{x\in\mathbb{Z}/n\mathbb{Z}} |\hat{f}(x)|^4\omega^{-tx} = N\,\mathrm{Card}\{(a,b,c,d)\in A^4 \text{ tq } a+b-c-d=t\}$ donc il existe $t\in 2A-2A$ ssi cette somme est non nulle.

III.4. **a.** Si $x\in X$ alors $(x_1,\dots,x_\kappa,x)$ n'est pas indépendante au sens de l'énoncé, donc il existe $\varepsilon_1,\dots,\varepsilon_\kappa,\varepsilon\in\{-1,0,1\}$ non tous nuls tels que $\sum_{i=1}^{\kappa}\varepsilon_i x_i + \varepsilon x = 0$. On a $\varepsilon\neq 0$ car $(x_1,\dots,x_\kappa)$ est indépendante, d'où $x = \sum_{i=1}^{\kappa}(-\varepsilon\varepsilon_i)x_i$.

b. On a pour $a\in\mathbb{Z}$: $d_N(a \bmod N) = \frac{1}{N}d(a,N\mathbb{Z})$ où d est la distance ordinaire sur $\mathbb{Z}$. En particulier d_N satisfait à l'inégalité triangulaire.
Soit $x\in\mathcal{B}(K,r/\kappa)$: $d_N(ax)\leqslant r/\kappa$ pour tout $a\in K$, donc $d_N(ax)\leqslant r$ pour tout a de la forme $a=\sum_{i=1}^{\kappa}\varepsilon_i x_i$ avec $\varepsilon_i\in\{-1,0,1\}$, en particulier pour tout $a\in X$. Ceci prouve $\mathcal{B}(K,r/\kappa)\subset\mathcal{B}(X,r)$.

III.5. **a.** Dériver deux fois.

b. La courbe de $y\mapsto\exp(ty)$ est au dessous de sa corde entre les points tels que $y=-1$ et $y=1$ d'où, avec le polynôme d'interpolation de Lagrange

$$\begin{aligned}F(y) &\leqslant \frac{y-1}{-2}F(-1) + \frac{y+1}{2}F(1) = y\frac{F(1)-F(-1)}{2} + \frac{F(1)+F(-1)}{2}\\ &\leqslant y\sinh t + \cosh t.\end{aligned}$$

c. $\cosh(t) = \sum_{n=0}^{\infty} \frac{t^{2n}}{(2n)!} \leqslant \sum_{n=0}^{\infty} \frac{t^{2n}}{2^n n!} = \exp(t^2/2)$ car $(2n)! = n! \times (n+1)\dots(2n) \geqslant 2^n n!$.

III.6. **a.** On utilise le résultat de la question **III.1** :

$$\hat{g}(x) = \sum_{a\in A} g(a)\omega^{ax} = \frac{1}{2}\sum_{a\in A}\sum_{j=1}^{\kappa}(c_j\omega^{a(x-x_j)} + \overline{c}_j\omega^{a(x+x_j)})$$
$$= \frac{1}{2}\sum_{j=1}^{\kappa}\Big(c_j\sum_{a\in A}\omega^{a(x-x_j)} + \overline{c}_j\sum_{a\in A}\omega^{a(x+x_j)}\Big) = \frac{N}{2}\sum_{j=1}^{\kappa}(c_j\delta_{x,x_j} + \overline{c_j}\delta_{x,-x_j})$$

Si $x \in K$ alors il existe un unique j tel que $x = x_j$, $x_j \neq 0$ et on a $x \neq -x_k$ pour tout $k \in \{1,\dots,\kappa\}$ car $(x_1,\dots,x_\kappa)$ est indépendante. On a donc $\hat{g}(x) = \frac{N}{2}c_j$ dans ce cas.
De même si $x \in -K$, $x = -x_j$, alors $\hat{g}(x) = \frac{N}{2}\overline{c_j}$.
Enfin, si $x \notin K \cup (-K)$ alors $\hat{g}(x) = 0$.
C'est en particulier le cas pour $x = 0$ donc $0 = \hat{g}(0) = \sum_{a\in\mathbb{Z}/n\mathbb{Z}} g(a)$.

b. D'après **2b**, **en supposant N impair pour que $x \neq -x$**

$$\sum_{a\in\mathbb{Z}/N\mathbb{Z}} g(a)^2 = \sum_{x\in\mathbb{Z}/N\mathbb{Z}} \hat{g}(x)\hat{g}(-x) = \sum_{x\in K\cup(-K)} \hat{g}(x)\hat{g}(-x)$$
$$= 2\sum_{x\in K}\hat{g}(x)\hat{g}(-x) = \frac{N}{2}\sum_{j=1}^{\kappa}|c_j|^2.$$

c. On prend $c_j = \mathrm{e}^{-i\theta_j}$ et on utilise la question **a** : $c_j\omega^{-ax_j} = \mathrm{e}^{-i(\frac{2\pi}{N}ax_j+\theta_j)}$, la somme considérée est donc nulle.

d. Pour $a \in \mathbb{Z}$ et $j \in \{1,\dots,\kappa\}$, on écrit : $t\Re(c_j\omega^{-ax_j}) = t|c_j|\cos(\frac{2\pi}{N}a\tilde{x}_j + \theta_j) = t|c_j|y_j(a)$ avec $\theta_j \in \mathbb{R}$ et $y_j(a) \in [-1,1]$. Alors, en utilisant la majoration du **5.b** et en développant les produits :

$$\frac{1}{N}\sum_{a=0}^{N-1}\exp(tg(a)) \leqslant \frac{1}{N}\sum_{a=0}^{N-1}\prod_{j=1}^{\kappa}(\cosh(t|c_j|) + y_j(a)\sinh(t|c_j|))$$
$$\leqslant \frac{1}{N}\sum_{a=0}^{N-1}\sum_{J\subset\{1,\dots,\kappa\}}\prod_{j\in J} y_j(a)\sinh(t|c_j|)\prod_{j\notin J}\cosh(t|c_j|)$$
$$\leqslant \sum_{J\subset\{1,\dots,\kappa\}}\frac{1}{N}\sum_{a=0}^{N-1}\prod_{j\in J} y_j(a)\sinh(t|c_j|)\prod_{j\notin J}\cosh(t|c_j|)$$
$$\leqslant \sum_{J\subset\{1,\dots,\kappa\}}\left(\frac{1}{N}\sum_{a=0}^{N-1}\prod_{j\in J} y_j(a)\right)\prod_{j\in J}\sinh(t|c_j|)\prod_{j\notin J}\cosh(t|c_j|).$$

D'après la question précédente, la somme entre parenthèse ci-dessus est non nulle que dans le seul cas où $J = \emptyset$ (encore une facétie de Victor). Il vient, en utilisant la question **5.c** :

$$\frac{1}{N}\sum_{a=0}^{N-1}\exp(tg(a)) \leqslant \prod_{j=1}^{\kappa}\cosh(t|c_j|) \leqslant \prod_{j=1}^{\kappa}\exp\left(\tfrac{1}{2}t^2|c_j|^2\right)$$
$$= \exp\left(\frac{t^2}{2}\sum_{j=1}^{\kappa}|c_j|^2\right) = \exp\left(\frac{t^2}{N}\sum_{a=0}^{N-1}g(a)^2\right)$$

en utilisant pour conclure la question **6.a**.

III.7. **a.** D'après **6b**,

$$\frac{2}{N}\sum_{a\in\mathbb{Z}/N\mathbb{Z}} g(a)^2 = \sum_{j=1}^{\kappa} |\hat{f}_A(x_j)|^2 = \sum_{j=1}^{\kappa} \hat{f}_A(x_j)\overline{\hat{f}_A(x_j)}$$
$$= \sum_{j=1}^{\kappa} \hat{f}_A(x_j)\sum_{a\in A}\omega^{-ax_j} = \sum_{a\in A}\sum_{j=1}^{\kappa}\hat{f}_A(x_j)\omega^{-ax_j}.$$

Cette somme est réelle, donc égale à la somme des parties réelles :

$$\frac{2}{N}\sum_{a\in\mathbb{Z}/N\mathbb{Z}} g(a)^2 = \sum_{a\in A} g(a) = \sum_{a\in\mathbb{Z}/N\mathbb{Z}} f(a)g(a).$$

b. Par convexité de la fonction exponentielle et l'égalité précédente, on a :

$$\frac{1}{\operatorname{Card} A}\sum_{a\in A}\exp(tg(a)) \geqslant \exp\Big(\frac{1}{\operatorname{Card} A}\sum_{a\in A} tg(a)\Big) = \exp\Big(\frac{2t}{N}\sum_{a\in\mathbb{Z}/N\mathbb{Z}} g(a)^2\Big).$$

Mais on a aussi avec **6d** :

$$\frac{1}{\operatorname{Card} A}\sum_{a\in A}\exp(tg(a)) \leqslant \frac{1}{\operatorname{Card} A}\sum_{a\in\mathbb{Z}/N\mathbb{Z}}\exp(tg(a)) \leqslant \frac{N}{\operatorname{Card} A}\exp\Big(\frac{t^2}{N}\sum_{a\in\mathbb{Z}/N\mathbb{Z}} g(a)^2\Big)$$
$$\leqslant \frac{1}{\alpha}\exp\Big(\frac{t^2}{N}\sum_{a\in\mathbb{Z}/N\mathbb{Z}} g(a)^2\Big).$$

Ainsi : $\forall\ t\in\mathbb{R},\ \ln(1/\alpha) + \dfrac{t^2}{N}\sum\limits_{a\in\mathbb{Z}/N\mathbb{Z}} g(a)^2 \geqslant \dfrac{2t}{N}\sum\limits_{a\in\mathbb{Z}/N\mathbb{Z}} g(a)^2$. Comme ceci est vrai pour tout t, le discriminant en t de la différence est donc négatif ou nul, ce qui donne l'inégalité demandée.

c. D'après **6.b**, on a $\sum\limits_{a\in\mathbb{Z}/N\mathbb{Z}} g(a)^2 = \dfrac{N}{2}\sum\limits_{j=1}^{\kappa}|\hat{f}_A(x_j)|^2$ d'où

$$N\operatorname{Card}(A)^2\ln(1/\alpha) \geqslant \sum_{a\in\mathbb{Z}/N\mathbb{Z}} g(a)^2 \ = \frac{N}{2}\sum_{j=1}^{\kappa}|\hat{f}_A(x_j)|^2 \geqslant \frac{N}{2}\kappa\rho^2\operatorname{Card}(A)^2.$$

III.8. **a.** D'après **3a** on sait que $\sum\limits_{x\in\mathbb{Z}/n\mathbb{Z}}|\hat{f}_A(x)|^4 = N\operatorname{Card}\{(a,b,c,d)\in A^4 \text{ tq } a+b=c+d\}$. Vu que $\operatorname{Card}(A)\geqslant\alpha N$, il suffit de prouver que le nombre de quadruplets (a_1,a_2,a_3,a_4) de A^4 tels que $a_1+a_2=a_3+a_4$ est minoré par $\operatorname{Card}(A)^3/\sigma = \operatorname{Card}(A)^4/\operatorname{Card}(2A)$. Soit n ce nombre, on a :

$$n\operatorname{Card}(2A) = \operatorname{Card}(2A)\sum_{t\in 2A}\operatorname{Card}\{(a_1,a_2,a_3,a_4)\in A^4 \mid a_1+a_2=t=a_3+a_4\}$$
$$= \operatorname{Card}(2A)\sum_{t\in 2A}\operatorname{Card}\{(a_1,a_2)\in A^2 | a_1+a_2=t\}\times\operatorname{Card}\{(a_3,a_4)\in A^2 | a_3+a_4=t\}$$
$$= \operatorname{Card}(2A)\sum_{t\in 2A}\operatorname{Card}^2\{(a_1,a_2)\in A^2 \mid a_1+a_2=t\}$$
$$= \Big(\sum_{t\in 2A}1^2\Big)\Big(\sum_{t\in 2A}\operatorname{Card}^2\{(a_1,a_2)\in A^2 \mid a_1+a_2=t\}\Big)$$
$$\geqslant \Big(\sum_{t\in 2A}\operatorname{Card}\{(a_1,a_2)\in A^2 \mid a_1+a_2=t\}\Big)^2 = \operatorname{Card}(A)^4.$$

b. Pour $x \notin X$ on a $|\hat{f}_A(x)| < \rho \operatorname{Card}(A) = \dfrac{\operatorname{Card}(A)}{2\sqrt{\sigma}}$, d'où :

$$\sum_{x\notin X} |\hat{f}_A(x)|^4 \leqslant \frac{\operatorname{Card}(A)^2}{4\sigma} \sum_{x\notin X} |\hat{f}_A(x)|^2 \leqslant \frac{\operatorname{Card}(A)^2}{4\sigma} \sum_{x\in\mathbb{Z}/N\mathbb{Z}} |\hat{f}_A(x)|^2 \leqslant \frac{N \operatorname{Card}(A)^3}{4\sigma}.$$

Si l'on suppose $\operatorname{Card}(A) = \alpha N$ alors on obtient l'inégalité demandée.

Dans le cas général l'inégalité demandée est fausse :

Prenons $N = 5$ et $A = \{0, 1\}$. Alors $\sigma = \frac{3}{2}$ et $\rho = \frac{1}{\sqrt{6}}$.

Par ailleurs, $|\hat{f}_A(0)| = 2$, $|\hat{f}_A(1)| = |\hat{f}_A(4)| = 2\cos(\frac{\pi}{5}) \approx 1.6$ et $|\hat{f}_A(2)| = |\hat{f}_A(3)| = 2\cos(\frac{2\pi}{5}) \approx 0.6$, tandis que $\rho \operatorname{Card}(A) = \sqrt{\frac{2}{3}} \approx 0.8$.

Ainsi $\mathbb{Z}/5\mathbb{Z} \setminus X = \{2, 3\}$ et $\sum\limits_{x\notin X} |\hat{f}_A(x)|^4 > 0$. Cette somme ne peut rester majorée par $\alpha^3 N^4/\sigma = \frac{15}{2}\alpha^3$ sous la seule condition $0 < \alpha \leqslant \operatorname{Card}(A)/N = \frac{2}{5}$.

c. Soit $a \in \mathbb{Z}$ et $b \in a + N\mathbb{Z}$ tel que $d_N(a) = |b/N|$.

On a $|1 - \omega^a| = 2|\sin(\pi b/N)| \leqslant 2\pi|b/N| = 2\pi d_N(a)$.

Soit alors $a \in \mathcal{B}(X, \frac{1}{16})$. Pour $x \in X$ on a $|1 - \omega^{-ax}| \leqslant 2\pi d_N(ax) \leqslant \frac{\pi}{8}$, d'où :

$$\Big|\sum_{x\in X} |\hat{f}_A(x)|^4 - \sum_{x\in X} |\hat{f}_A(x)|^4 \omega^{-ax}\Big| \leqslant \tfrac{\pi}{8} \sum_{x\in X} |\hat{f}_A(x)|^4.$$

On en déduit :

$$\begin{aligned}
\Big|\sum_{x\in\mathbb{Z}/N\mathbb{Z}} |\hat{f}_A(x)|^4 \omega^{-ax}\Big| &\geqslant \Big|\sum_{x\in X} |\hat{f}_A(x)|^4 \omega^{-ax}\Big| - \Big|\sum_{x\notin X} |\hat{f}_A(x)|^4 \omega^{-ax}\Big| \\
&\geqslant (1 - \tfrac{\pi}{8}) \sum_{x\in X} |\hat{f}_A(x)|^4 - \sum_{x\notin X} |\hat{f}_A(x)|^4 \\
&\geqslant (1 - \tfrac{\pi}{8}) \sum_{x\in\mathbb{Z}/N\mathbb{Z}} |\hat{f}_A(x)|^4 - (2 - \tfrac{\pi}{8}) \sum_{x\notin X} |\hat{f}_A(x)|^4.
\end{aligned}$$

On sait que $\sum\limits_{x\in\mathbb{Z}/N\mathbb{Z}} |\hat{f}_A(x)|^4 \geqslant \dfrac{N \operatorname{Card}(A)^3}{\sigma}$ (**a**) et que $\sum\limits_{x\notin X} |\hat{f}_A(x)|^4 \leqslant \dfrac{N \operatorname{Card}(A)^3}{4\sigma}$ (**b**), il vient alors :

$$\begin{aligned}
\Big|\sum_{x\in\mathbb{Z}/N\mathbb{Z}} |\hat{f}_A(x)|^4 \omega^{-ax}\Big| &\geqslant \frac{N \operatorname{Card}(A)^3}{4\sigma}(4 - \tfrac{\pi}{2} - (2 - \tfrac{\pi}{8})) \\
&\geqslant \frac{N \operatorname{Card}(A)^3}{4\sigma}(2 - \tfrac{3\pi}{8}) > 0.
\end{aligned}$$

D'après **3b**, ceci implique $a \in 2A - 2A$.

Remarque : on a par les mêmes calculs que $\mathcal{B}(X, r) \subset 2A - 2A$ pour tout $r < \frac{1}{3\pi}$.

d. Soit $(x_1, \ldots, x_\kappa)$ une suite indépendante maximale dans X, et $K = \{x_1, \ldots, x_\kappa\}$.

Donc $\operatorname{Card}(K) = \kappa \leqslant 2\rho^{-2} \ln(1/\alpha) = 8\sigma \ln(1/\alpha)$.

Et, d'après **4b**, $\mathcal{B}(K, r) \subset \mathcal{B}(K, \frac{1}{16\kappa}) \subset \mathcal{B}(X, \frac{1}{16}) \subset 2A - 2A$.

Partie IV. Progressions arithmétiques

IV.1. **a.** Soit i tel que ξ_i n'est pas divisible par N, comme N est premier, ξ_i est premier à N ; soient $a, b_i \in \mathbb{Z}$ tels que $a\xi_i + Nb_i = 1$. Alors pour tout choix des b_j, $j \neq i$, les nombres $a\xi_1 + Nb_1, \dots, a\xi_n + Nb_n$ sont premiers entre eux dans leur ensemble puisque l'un d'entre eux vaut 1.

b. On choisit $\overrightarrow{v_1} = a\overrightarrow{\xi} + N\overrightarrow{b}$ de sorte que l'une des coordonnées de $\overrightarrow{v_1}$ soit égale à 1 (question précédente), soit $a\xi_i + Nb_i = 1$, puis on complète avec les vecteurs $\overrightarrow{e_j}$, $j \neq i$. On obtient ainsi une base entière de $\mathbb{R}^n$, notée $(\overrightarrow{v_1}, \dots, \overrightarrow{v_n})$. En effet, la matrice de passage de la base canonique $(\overrightarrow{e_1}, \dots, \overrightarrow{e_n})$ dans la base $(\overrightarrow{e_1}, \dots, \overrightarrow{v_1}, \dots, \overrightarrow{e_n})$ (où $\overrightarrow{v_1}$ a pris la place de $\overrightarrow{e_i}$) est à coefficients entiers et a un déterminant 1.
On a $\overrightarrow{v_1} = a\overrightarrow{\xi} + N\overrightarrow{b}$ et $\xi_i\overrightarrow{v_1} = a\xi_i\overrightarrow{\xi} + N\xi_i\overrightarrow{b} = \overrightarrow{\xi} + N(\xi_i\overrightarrow{b} - b_i\overrightarrow{\xi})$ par conséquent $\overrightarrow{\xi} = \xi_i\overrightarrow{v_1} + N(b_i\overrightarrow{\xi} - \xi_i\overrightarrow{b})$.
Les groupes $L = \mathbb{Z}\overrightarrow{\xi} + N\mathbb{Z}^n$ et $L' = \mathbb{Z}\overrightarrow{v_1} + N\mathbb{Z}^n$ sont égaux.
En particulier un vecteur $\overrightarrow{x} = t_1\overrightarrow{v_1} + \cdots + t_n\overrightarrow{v_n}$ appartient à L si et seulement s'il appartient à L', c'est-à-dire si et seulement si t_1 est entier et $t_2, \dots, t_n$ sont des entiers divisibles par N.

c. Soit u l'endomorphisme de $\mathbb{R}^n$ défini par $u(x_1, \dots, x_n) = x_1\overrightarrow{v_1} + Nx_2\overrightarrow{v_2} + \cdots + Nx_n\overrightarrow{v_n}$ et Φ la forme quadratique sur $\mathbb{R}^n$ définie par $\Phi(\overrightarrow{x}) = \|u(\overrightarrow{x})\|^2$.
On a $\operatorname{disc}(\Phi) = \det^2(u) = N^{2n-2}\det^2(\overrightarrow{v_1}, \dots, \overrightarrow{v_n}) = N^{2n-2}$, donc il existe une base entière $(\overrightarrow{x_1}, \dots, \overrightarrow{x_n})$ telle que $\Phi(\overrightarrow{x_1})\dots\Phi(\overrightarrow{x_n}) \leqslant (\frac{4}{3})^{n(n-1)/2}N^{2n-2}$, d'après **II-4h**. Alors la famille définie par $\overrightarrow{w_i} = u(\overrightarrow{x_i})$ convient : c'est une base de $\mathbb{R}^n$ car image par u – linéaire bijectif – de la base $(\overrightarrow{x_1}, \dots, \overrightarrow{x_n})$, et elle est constituée d'éléments de L d'après la question précédente.

IV.2. **a.** Par définition, $\sum_{i=1}^n \mu_i\overrightarrow{w_i} - p(\mu)\overrightarrow{\xi} = \sum_{i=1}^n \mu_i(\overrightarrow{w_i} - x_i\overrightarrow{\xi}) \in N\mathbb{Z}^n$.
Donc $p(\mu) = p(\mu') \Rightarrow \sum_{i=1}^n (\mu_i - \mu'_i)\overrightarrow{w_i} \in N\mathbb{Z}^n$.
Or, pour $\mu, \mu' \in M$, on a

$$\Big\|\sum_{i=1}^n (\mu_i - \mu'_i)\overrightarrow{w_i}\Big\| \leqslant \sum_{i=1}^n \frac{2Nr}{n\|\overrightarrow{w_i}\|}\|\overrightarrow{w_i}\| \leqslant 2Nr < N.$$

On en déduit $p(\mu) = p(\mu') \Rightarrow \sum_{i=1}^n (\mu_i - \mu'_i)\overrightarrow{w_i} = \overrightarrow{0} \Rightarrow \mu = \mu'$ car $(\overrightarrow{w_1}, \dots, \overrightarrow{w_n})$ est libre.

b. D'après **2a** $\mu \in M \mapsto p(\mu) \in P$ est injective donc $\operatorname{Card}(P) = \operatorname{Card}(M)$.
Or $\operatorname{Card}(M) = \prod_{i=1}^n \Big(1 + 2\Big\lfloor \frac{Nr}{n\|\overrightarrow{w_i}\|}\Big\rfloor\Big)$ car le nombre d'entiers μ_i satisfaisant les inégalités $-\frac{Nr}{n\|\overrightarrow{w_i}\|} \leqslant \mu_i \leqslant \frac{Nr}{n\|\overrightarrow{w_i}\|}$ vaut $1 + 2\Big\lfloor \frac{Nr}{n\|\overrightarrow{w_i}\|}\Big\rfloor$.
Par conséquent, vu le **1.c**, $\operatorname{Card} P \geqslant \prod_{i=1}^n \Big(\frac{Nr}{n\|\overrightarrow{w_i}\|}\Big) \geqslant N(\frac{r}{n})^n(\frac{3}{4})^{n(n-1)/4}$.

c. Comme $\sum_{i=1}^n \mu_i\overrightarrow{w_i} - p(\mu)\overrightarrow{\xi} \in N\mathbb{Z}^n$, on a pour tout j :

$$d_N(p(\mu)\xi_j) = d_N\Big(\sum_{i=1}^n \mu_i e_j^*(\overrightarrow{w_i})\Big) \leqslant \frac{1}{N}\Big\|\sum_{i=1}^n \mu_i\overrightarrow{w_i}\Big\| \leqslant r$$

donc $p(\mu) \in \mathcal{B}(X, r)$.

IV.3. Si $X = \{\xi_1, \dots, \xi_n\} \neq \{0\}$, on pose $\overrightarrow{\xi} = (\xi_1, \dots, \xi_n)$ et on applique les résultats précédents (c'est possible car il y a au moins un ξ_j non divisible par N). L'ensemble P défini en **2** est une progression arithmétique au sens de l'énoncé, de raisons $x_1, \dots, x_n$ et l'injectivité de la restriction de p à M montre que c'est une progression arithmétique propre.

Si $X = \{0\}$ alors $\mathcal{B}(X, r) = \mathbb{Z}/N\mathbb{Z}$ est une progression arithmétique propre de dimension 1 et de raison $x_1 = 1$. Et la taille, N, de $\mathbb{Z}/N\mathbb{Z}$ est bien minorée par $(\frac{3}{4})^0(\frac{r}{1})^1 N$.

IV.4. **Cette question est fausse :** si l'on prend $A = \mathbb{Z}/N\mathbb{Z}$, on a $\sigma = 1$ et on peut choisir $\alpha \in]0, 1]$ arbitrairement. Le minorant de l'énoncé est donc non majoré alors qu'il est censé minorer la taille d'une partie incluse dans $\mathbb{Z}/N\mathbb{Z}$.

Tentative de correction de l'énoncé : avec **III-8**, on a l'existence de $K \subset \mathbb{Z}/N\mathbb{Z}$ tel que $\mathcal{B}(K, r) \subset 2A - 2A$ où $\mathrm{Card}(K) = d \leqslant 8\sigma \ln(1/\alpha)$ et $r = 1/(128\sigma \ln(1/\alpha))$. Si l'on suppose $r < \frac{1}{2}$ – ce qui est faux en général, cf. contre-exemple ci-dessus – alors on peut appliquer la question précédente, qui met en évidence une progression arithmétique propre de dimension d et de taille supérieure ou égale à $(\frac{3}{4})^{d(d-1)/4} r^d N/d^d$. Ce minorant, compte-tenu de la valeur de r, est celui demandé au coefficient $1/d^d$ près...

Partie V. Théorème de Freiman-Rusza-Chang

V.1. **a.** Prolonger les listes $(x_1, \dots, x_k)$ et $(y_1, \dots, y_k)$ en ajoutant un même élément $x \in A$, $k - p$ fois à chaque liste.

b. Il faut vérifier que la quantité $f(a_1) + \cdots + f(a_m) - f(b_1) - \cdots - f(b_n)$ ne dépend que de $a_1 + \cdots + a_m - b_1 - \cdots - b_n$. Soient $a_1, \dots, d_n$ des éléments de A. On a :

$$\begin{aligned} a_1 + \cdots + a_m - b_1 - \cdots - b_n &= c_1 + \cdots + c_m - d_1 - \cdots - d_n \\ \Rightarrow a_1 + \cdots + a_m + d_1 + \cdots + d_n &= c_1 + \cdots + c_m + b_1 + \cdots + b_n \\ \Rightarrow f(a_1) + \cdots + f(a_m) + f(d_1) + \cdots + f(d_n) &= f(c_1) + \cdots + f(c_m) + f(b_1) + \cdots + f(b_n) \\ \Rightarrow f(a_1) + \cdots + f(a_m) - f(b_1) - \cdots - f(b_n) &= f(c_1) + \cdots + f(c_m) - f(d_1) - \cdots - f(d_n). \end{aligned}$$

c. Immédiat.

d. On note $A = \{x_0 + \sum_{i=1}^d n_i x_i,\ 0 \leqslant n_i < N_i\}$. Pour $i \in \{1, \dots, d\}$ tel que $N_i > 1$, la quantité $f(x + x_i) - f(x)$ ne dépend pas de $x \in A \cap (A - x_i)$ puisque f est 2-tendue ; soit y_i cette quantité. Pour i tel que $N_i = 1$, on choisit pour y_i un élément arbitraire dans H. Ainsi $f(x + x_i) = f(x) + y_i$ pour tout x tel que $x + x_i$ et x appartiennent à A. On en déduit par récurrence sur les n_i :

$$\forall\ (n_1, \dots, n_d) \in [\![0, N_1[\![\times \cdots \times [\![0, N_d[\![,\ f\Big(x_0 + \sum_{i=1}^d n_i x_i\Big) = f(x_0) + \sum_{i=1}^d n_i y_i.$$

Ainsi $f(A)$ est la progression arithmétique de premier terme $f(x_0)$, de raisons $y_1, \dots, y_d$ et de taille $N_1 \dots N_d = M$.

V.2. **a.** Soient $f : A \to B$ et $g : B \to A$ deux applications k-tendues réciproques et F, G les fonctions associées telles que définies en **1b**. Alors F et G sont p-tendues si $p \leqslant k/(m+n)$ et l'on a par construction :

$$\begin{aligned} G(F(a_1 + \cdots + a_m - b_1 - \cdots - b_n)) &= G(f(a_1) + \cdots + f(a_m) - f(b_1) - \cdots - f(b_n)) \\ &= g(f(a_1)) + \cdots + g(f(a_m)) - g(f(b_1)) - \cdots - g(f(b_n)) \\ &= a_1 + \cdots + a_m - b_1 - \cdots - b_n. \end{aligned}$$

Ceci prouve que $G \circ F = \mathrm{Id}_{mA-nA}$ et l'on a de même $F \circ G = \mathrm{Id}_{mB-nB}$.

b. Avec $p = 1$ on obtient une bijection entre $mA - nA$ et $mB - nB$ donc ces ensembles ont même cardinal.

V.3. **a.** Soient $x_1, \dots, x_k, y_1, \dots, y_k \in f^{-1}(I(j))$ tels que $x_1 + \cdots + x_k = y_1 + \cdots + y_k$. Donc $f(x_1) + \cdots + f(x_k)$ et $f(y_1) + \cdots + f(y_k)$ sont deux éléments de $[(j-1)p,\ jp[\cap \mathbb{N}$ congrus entre eux modulo p ; ils sont égaux.

b. Si $N = 0$, on considère que $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ et que la relation de congruence modulo N est l'identité sur $\mathbb{Z}$. Partitionnons $uA = \{ux,\ x \in A\} = \bigcup_{j=1}^{k} (uA) \cap f^{-1}(I(j))$. La restriction de f_u à chacun de ces sous-ensembles est k-tendue d'après la question précédente et l'addivité de l'application $t \in \mathbb{Z} \mapsto t \bmod N \in \mathbb{Z}/N\mathbb{Z}$, et comme $u \in (\mathbb{Z}/p\mathbb{Z})^*$, on a $\mathrm{Card}(A) = \mathrm{Card}(uA) = \sum_{j=1}^{k} \mathrm{Card}((uA) \cap f^{-1}(I(j)))$. L'un de ces ensembles a donc un cardinal supérieur ou égal à $\mathrm{Card}(A)/k$.

c. Si $N \geqslant 1$, les éléments x de $(\mathbb{Z}/p\mathbb{Z})^*$ tels que $f(x) \equiv 0 \pmod N$ sont les classes de congruence modulo p des entiers jN avec $0 < j < \frac{p}{N}$. Il y a $\lfloor \frac{p-1}{N} \rfloor$ tels x. Pour $z \in (kA - kA) \setminus \{0\}$, les uz, $u \in (\mathbb{Z}/p\mathbb{Z})^*$ sont distincts non nuls, donc il y a au plus $\lfloor \frac{p-1}{N} \rfloor$ valeurs de u telles que $f(uz) \equiv 0 \pmod N$.

Supposons $N \geqslant \mathrm{Card}(kA - kA)$ (et donc $N \geqslant 1$) : il y a au plus $N-1$ éléments non nuls dans $kA - kA$ et $(N-1)\lfloor \frac{p-1}{N} \rfloor < p-1$, donc il existe au moins un élément $u \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que :

$$\forall\ z \in kA - kA,\ f(uz) \equiv 0 \pmod N \Leftrightarrow z = 0.$$

Je dis que pour un tel u, on a :

$$\forall\ a_1, \dots, b_k \in A(u),\ f_u(a_1) + \dots . f_u(a_k) = f_u(b_1) + \dots . f_u(b_k) \Leftrightarrow a_1 + \dots . a_k = b_1 + \cdots + b_k. \quad (*)$$

Démonstration :
soit $j \in \{1, \dots, k\}$ tels que $f(ua_1), \dots, f(ub_k) \in I(j)$. Alors $f(ua_1) + \cdots + f(ua_k) = f(u(a_1 + \cdots + a_k)) + (j-1)p$ car les deux membres sont congrus entre eux modulo p et appartiennent à l'intervalle $[(j-1)p, jp[$. De même, $f(ub_1) + \cdots + f(ub_k) = f(u(b_1 + \cdots + b_k)) + (j-1)p$. Ainsi :

$$\begin{aligned} f_u(a_1) + \dots . f_u(a_k) = f_u(b_1) + \dots . f_u(b_k) & \\ \Leftrightarrow f(u(a_1 + \cdots + a_k)) - (j-1)p \equiv f(u(b_1 + \cdots + b_k) + (j-1)p & \mod N \\ \Leftrightarrow f(u(a_1 + \cdots + a_k)) - f(u(b_1 + \cdots + b_k)) \equiv 0 & \mod N \end{aligned}$$

Or,

$$\underbrace{f(u(a_1 + \cdots + a_k))}_{\alpha} - \underbrace{f(u(b_1 + \cdots + b_k))}_{\beta} = \begin{cases} f(u(a_1 + \cdots + a_k - b_1 - \cdots - b_k)) & \text{si } \alpha \geqslant \beta, \\ -f(u(b_1 + \cdots + b_k - a_1 - \cdots - a_k)) & \text{sinon.} \end{cases}$$

Comme $kA - kA$ et la relation de congruence modulo N sont stables par opposé, on obtient :

$$\begin{aligned} f_u(a_1) + \dots . f_u(a_k) = f_u(b_1) + \dots . f_u(b_k) & \\ \Leftrightarrow u(a_1 + \cdots + a_k - b_1 - \cdots - b_k) = 0 & \\ \Leftrightarrow a_1 + \cdots + a_k = b_1 + \cdots + b_k & \text{ par choix de } u. \end{aligned}$$

Ainsi $(*)$ est prouvée. On en déduit en prenant $a_2 = a_3 = \cdots = a_n = b_2 = b_3 = \cdots = b_n$ que la restriction de f_u à $A(u)$ est injective, donc $f_{u|A(u)}$ induit une bijection de $A(u)$ sur son image. Enfin $f_{u|A(u)}$ et sa réciproque sont k-tendues d'après $(*)$.

V.4. **a.** On sait depuis **I-4a** que $\mathrm{Card}(2A) \geqslant 2\,\mathrm{Card}(A) - 1$, soit $\sigma \geqslant 2 - 1/\mathrm{Card}(A) \geqslant \frac{3}{2}$.

b. On suppose $k \geqslant 1$ dans cette question. Soit p un nombre premier majorant strictement $kA - kA$ (il en existe) et φ l'application $\mathbb{Z} \ni x \mapsto x \bmod p \in \mathbb{Z}/p\mathbb{Z}$. Par choix de p et stabilité de de $kA - kA$ par opposé, on a :

$$\forall\ a_1, \dots, b_k \in A,\ \varphi(a_1) + \cdots + \varphi(a_k) = \varphi(b_1) + \cdots + \varphi(b_k) \Leftrightarrow a_1 + \cdots + a_k = b_1 + \cdots + b_k.$$

Comme on l'a vu en **3c**, ceci implique que φ induit une bijection k-tendue de A sur $\varphi(A)$ dont la réciproque est elle aussi k-tendue.

c. On applique **3** à $\varphi(A) \subset \mathbb{Z}/p\mathbb{Z}$: si $N \geqslant \mathrm{Card}(k\varphi(A) - k\varphi(A))$ alors il existe une partie $B \subset A$ telle que $\varphi(B)$ est k-semblable à une partie $C \subset \mathbb{Z}/N\mathbb{Z}$ et $\mathrm{Card}(\varphi(B)) \geqslant \mathrm{Card}(\varphi(A))/k$. Ceci est vrai en particulier si $N > \sigma^{2k}\,\mathrm{Card}(A)$ car on a :

$$\mathrm{Card}(k\varphi(A) - k\varphi(A)) = \mathrm{Card}(\varphi(kA - kA)) \leqslant \mathrm{Card}(kA - kA) \leqslant \sigma^{2k}\,\mathrm{Card}(A),$$

d'après l'inégalité de Plünnecke admise. Par ailleurs $\mathrm{Card}(\varphi(A)) = \mathrm{Card}(A)$ et $\mathrm{Card}(\varphi(B)) = \mathrm{Card}(B)$ car la restriction de φ à A est injective. Enfin la k-similitude est manifestement une notion transitive, donc B est k-semblable à C.

d. L'existence de N résulte du postulat de Bertrand : *pour tout $n \geqslant 2$, il existe un nombre premier dans l'intervalle $]n, 2n[$*. La partie $C \subset \mathbb{Z}/N\mathbb{Z}$ définie à la question précédente vérifie :

$$\mathrm{Card}(C) = \mathrm{Card}(B) \geqslant \frac{\mathrm{Card}(A)}{8} \geqslant \frac{N}{16\sigma^{16}},$$
$$\frac{\mathrm{Card}(2C)}{\mathrm{Card}(C)} = \frac{\mathrm{Card}(2B)}{\mathrm{Card}(B)} = \sigma' \leqslant \frac{8\,\mathrm{Card}(2A)}{\mathrm{Card}(A)} = 8\sigma.$$

Donc en admettant la question **IV-4** (contestée), $2C - 2C$ contient une progression arithmétique propre de dimension $d \leqslant 64\sigma\ln(16\sigma^{16})$ et de taille supérieure ou égale à $N\frac{(\frac{3}{4})^{d(d-1)/4}}{(128\sigma'\ln(16\sigma^{16}))^d} \geqslant \mathrm{Card}(A)\frac{\sigma^{16}(\frac{3}{4})^{d(d-1)/4}}{(1024\sigma\ln(16\sigma^{16}))^d}$. D'après **1d**, cette progression arithmétique est 2-semblable à une progression arithmétique ayant même dimension et même taille (donc aussi propre), incluse dans $2B - 2B$ et par conséquent incluse dans $2A - 2A$.

Comme $\sigma \geqslant \frac{3}{2}$, on a $16 \leqslant \sigma^7$, d'où $d \leqslant 64\sigma\ln(\sigma^{23}) = 1472\sigma\ln(\sigma)$. Par ailleurs,

$$\begin{aligned}
\ln\Big(\frac{\sigma^{16}(\frac{3}{4})^{d(d-1)/4}}{(1024\sigma\ln(16\sigma^{16}))^d}\Big) &= 16\ln\sigma + d\ln\Big(\frac{(\frac{3}{4})^{(d-1)/4}}{1024\sigma\ln(16\sigma^{16})}\Big)\\
&\geqslant -d\ln(1024\sigma\ln(16\sigma^{16})) - \frac{d(d-1)}{4}\ln(\tfrac{4}{3})\\
&\geqslant -d\ln(1024\sigma\ln(\sigma^{23})) - \frac{d^2}{4}\ln(\tfrac{4}{3})\\
&\geqslant -d\ln(1024\times 23\times\sigma\ln(\sigma)) - \frac{d^2}{4}\ln(\tfrac{4}{3})\\
&\geqslant -d\lambda\sigma\ln(\sigma) - \frac{d^2}{4}\ln(\tfrac{4}{3})\\
&\geqslant -\mu\sigma^2\ln^2(\sigma),
\end{aligned}$$

où λ et μ sont deux constantes que l'on pourrait calculer explicitement. En prenant $c_1 = \max(1472, \mu)$ on obtient le résultat demandé.

Remarque : des calculs similaires peuvent être menés avec la minoration effectivement établie en **IV-4** – la condition $r < \frac{1}{2}$ est satisfaite dans le cas étudié – et conduisent au même résultat avec des constantes différentes.

V.5. **a.** Les relations $\mathrm{Card}(P_t) = c^t \mathrm{Card}(P)$ et $P_t \subset (t+2)A - 2A$ sont évidentes. On en déduit avec l'inégalité de Plünnecke : $2^t\sigma^t \mathrm{Card}(P) \leqslant c^t \mathrm{Card}(P) = \mathrm{Card}(P_t) \leqslant \sigma^{t+4} \mathrm{Card}(A)$, ce qui implique la majoration demandée.

b. Soit $x \in A$. Si $x \notin S_t$ alors il existe $y \in S_t$ tel que $x+P_t$ et $y+P_t$ sont non disjointes ; soit $x+p = y+q$ un élément commun. On a $x = q-p+y \in P_t - P_t + S_t$. On obtient la même conclusion si $x \in S_t$ car $P_t - P_t$ contient 0. Ainsi $A \subset P_t - P_t + S_t = (P + S'_0 + \cdots + S'_{t-1}) - (P + S'_0 + \cdots + S'_{t-1}) + S_t = (P-P) + (S'_0 - S'_0) + \cdots + (S'_{t-1} - S'_{t-1}) + S_t$.

c. Soit $S = \{s_1, \ldots, s_n\}$. On a $S \subset \{0 + \sum_{i=1}^n n_i s_i \text{ tq } 0 \leqslant n_i \leqslant 1\}$, donc $S - S \subset \{0 + \sum_{i=1}^n n_i s_i \text{ tq } -1 \leqslant n_i \leqslant 1\}$. Ce dernier ensemble est une progression arithmétique de dimension $n = \mathrm{Card}(S)$ et de taille 3^n. On en déduit que $S'_0 - S'_0, \ldots, S'_{t-1} - S'_{t-1}$ sont inclus dans des progressions arithmétiques convenables et S_t est lui aussi contenu dans une progression arithmmétique de dimension $\mathrm{Card}(S_t)$ et taille $2^{\mathrm{Card}(S_t)}$. En ce qui concerne $P - P$, écrivons $P = \{x_0 + \sum_{i=1}^d n_i x_i \text{ tq } 0 \leqslant n_i < N_i\}$. Alors $P - P$ est une progression arithmétique de dimension d et de taille $\prod_{i=1}^d (2N_i - 1) \leqslant 2^d \prod_{i=1}^d N_i = 2^d \mathrm{Card}(P)$. D'où finalement A est inclus dans une progression arithmétique dont la dimension δ est la somme des dimensions et la taille τ est le produit des tailles des progressions précédentes.

Majoration de δ :

$$\delta = d + \mathrm{Card}(S'_0) + \cdots + \mathrm{Card}(S'_{t-1}) + \mathrm{Card}(S_t) \leqslant d + (t+1)c \leqslant d + 2tc \leqslant d + 2c\ln(\sigma^4/\beta)/\ln(2).$$

La dernière majoration vient de l'inégalité $2^t \leqslant \sigma^4/\beta$ vue en **a**. On a de plus $c < 2\sigma + 1 \leqslant \frac{8}{3}\sigma$, d'où finalement :

$$\delta \leqslant d + \tfrac{16}{3\ln 2}\sigma \ln(\sigma^4/\beta).$$

Majoration de $\ln(\tau/\mathrm{Card}(A))$:

$$\begin{aligned}\ln(\tau/\mathrm{Card}(A)) &\leqslant d\ln(2) + \ln(\beta) + \ln(3)(\mathrm{Card}(S'_0) + \cdots + \mathrm{Card}(S'_{t-1})) + \ln(2)\,\mathrm{Card}(S_t)\\ &\leqslant d\ln(2) + \ln(\beta) + \ln(3)(t+1)c\\ &\leqslant d\ln(2) + \ln(\beta) + \tfrac{16\ln 3}{3\ln 2}\sigma\ln(\sigma^4/\beta).\end{aligned}$$

On n'obtient pas les majorations demandées, et je ne vois pas comment obtenir ces dernières, mais cela suffira pour la question suivante.

V.6. D'après **4**, on peut trouver P telle que $d \leqslant c_1\sigma\ln(\sigma)$ et $\ln(1/\beta) \leqslant c_1\sigma^2\ln^2(\sigma)$. En reportant ces majorations dans celles obtenues à la question précédente, on obtient :

$$\delta \leqslant c_1\sigma\ln(\sigma) + \tfrac{64}{3\ln 2}\sigma\ln(\sigma) + \tfrac{16}{3\ln 2}c_1\sigma^3\ln^2(\sigma) = O(\sigma^3\ln^2(\sigma))$$

On trouve de même que $\ln(\tau/\mathrm{Card}(A))$ est majoré par $O(\sigma^3\ln^2(\sigma))$.

Fin du corrigé