I. Somme de parties

1a) Par récurrence sur n.

1b) 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 $\{\bullet, |\}$:

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

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.

1c) $\frac{1}{t^N}\binom{N+t-1}{N} = \frac{1}{N!}(1 + \frac{N-1}{t}) \dots (1 + \frac{1}{t})(1 + \frac{0}{t})$ décroît par rapport à t à N fixé, vaut 1 pour $t = 1$ et tend vers $\frac{1}{N!}$ lorsque $t \to \infty$.

2a) Soit $x \in G$. Les ensembles A et $x - B$ ne peuvent être disjoints car la somme de leurs cardinaux dépasse $\operatorname{card} G$; il existe donc $a \in A$ 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.

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

3a) 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 $(a, b) \longmapsto a + b$ induit une surjection de $A \times B$ sur $A + B$ d'où $\operatorname{card}(A + B) \leqslant \operatorname{card}(A \times B) = \operatorname{card}(A) \operatorname{card}(B)$.

3b) 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**.

4a) 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 $A + B$.

4b) Avec les notations précédentes, si $\operatorname{card}(A+B) = p+q-1$ alors $A+B = \{a_1+b_1, \dots, a_1+b_q, a_2+b_q, \dots, a_p+b_q\}$. 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 $b_2 - b_1 = d$.

5a) Le caractère sous-groupe est immédiat. De plus si $a \in H$, on a $H \subset a - A$ donc H est fini et $\operatorname{card}(H) \leqslant \operatorname{card}(A)$.

5b) Si $B \subset H$ alors $A + B = A$ par définition de H. Si $B \subset b + H$ alors $A + B = A + b$. Dans les deux cas on a bien $\operatorname{card}(A + B) = \operatorname{card}(A)$. Réciproquement, si $\operatorname{card}(A + B) = \operatorname{card}(A)$, soit $b \in G$ et $B' = B - b$. On a $A + B' = (A + B) - b$ est un sur-ensemble de A car $0 \in B'$, de même cardinal que A par hypothèse sur B, d'où $A + B' = A$, c'est-à-dire $B' \subset H$. Et donc $B = b + B' \subset b + H$.

6) On a $\operatorname{card}(A - B) \geqslant \max(\operatorname{card}(A), \operatorname{card}(-B)) = \max(\operatorname{card}(A) \operatorname{card}(B)) \geqslant \sqrt{\operatorname{card}(A) \operatorname{card}(B)}$ d'où $d_R(A, B) \geqslant 0$.

Inégalité triangulaire : considérons l'application φ : $\begin{cases} (A - C) \times (B - C) & \longrightarrow & G \\ (x, y) & \longmapsto & x - y. \end{cases}$

Si $z = a - b \in A - B$ alors pour tout $c \in C$ on a $z = \varphi(a - c, b - c)$ donc z a au moins $\operatorname{card}(C)$ antécédants distincts par φ. On en déduit :

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

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

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 $\mathrm{card}(A-B)=\mathrm{card}(A)=\mathrm{card}(B)$. D'après **5**, $-B\subset -b+H$ où $-b$ est un élément quelconque de $-B$ et H le sous-groupe associé à A en **5a**. Ainsi $B\subset b-H=b+H$, puis $\mathrm{card}(B)\leqslant\mathrm{card}(H)\leqslant\mathrm{card}(A)=\mathrm{card}(B)$, donc $B=b+H$. Enfin si $a\in A$, on a $H\subset a-A$ et les deux ensembles ont même cardinal, d'où $A=a+H$. 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 $d_R(A,B)=0$.

II. Valeurs aux entiers de formes quadratiques définies positives

1) Soit M la matrice de $(\vec{v}_1,\ldots,\vec{v}_n)$ dans la base canonique $(\vec{e}_1,\ldots,\vec{e}_n)$ de $\mathbf{R}^n$. La famille $(\vec{v}_1,\ldots,\vec{v}_n)$ est une base entière si et seulement si M est à coefficients entiers et $\vec{e}_1,\ldots,\vec{e}_n$ sont combinaisons linéaires à coefficients entiers de $(\vec{v}_1,\ldots,\vec{v}_n)$, soit si et seulement si $M\in\mathcal{M}_n(\mathbf{Z})$ et il existe $P\in\mathcal{M}_n(\mathbf{Z})$ 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 $M\in\mathcal{M}_n(\mathbf{Z})$ et $\det(M)=\pm1$ alors $P=\det(M)\,{}^t\mathrm{com}(M)\in\mathcal{M}_n(\mathbf{Z})$ et $MP=I_n$ donc $(\vec{v}_1,\ldots,\vec{v}_n)$ est une base entière.

2) Lorsque $s(\vec{v})=1$, $\vec{v}$ est au signe près un des vecteurs de la base canonique et il existe donc une base entière commençant par $\vec{v}$. Supposons la propriété vraie pour tout vecteur $\vec{v}$ à coordonnées premières entre elles tel que $s(\vec{v})<N$ et considérons $\vec{v}=(a_1,\ldots,a_n)\in\mathbf{Z}^n$ à coordonnées premières entre elles avec $s(\vec{v})=N>1$: soit i tel que $|a_i|$ soit minimal parmi les coordonnées non nulles de $\vec{v}$ et $j\neq i$ tel que $a_j\neq0$ (j existe sinon $\vec{v}=a_i\vec{e}_i$ avec $|a_i|=s(\vec{v})>1$ donc les coordonnées de $\vec{v}$ ne sont par premières entre elles). On note $a_j=q|a_i|+r$ la division euclidienne de a_j par $|a_i|$ et on considère le vecteur $\vec{w}=\vec{v}+(r-a_j)\vec{e}_j$ (c'est-à-dire le vecteur obtenu en remplaçant a_j par r dans $\vec{v}$ et en conservant toutes les autres coordonnées). Comme $0\leqslant r<|a_i|\leqslant|a_j|$, on a $s(\vec{w})<s(\vec{v})=N$. De plus le sous-groupe de $\mathbf{Z}$ engendré par les coordonnées de $\vec{v}$ et celui engendré par celles de $\vec{w}$ sont clairements égaux, donc les coordonnées de $\vec{w}$ sont premières entre elles. Par hypothèse de récurrence il existe une base entière commençant par $\vec{w}$, donc une matrice $M\in\mathcal{M}_n(\mathbf{Z})$ de déterminant ±1 dont la première colonne représente le vecteur $\vec{w}$. Soit $P=I_n+\mathrm{sgn}(a_i)qE_{ji}$ la matrice de l'opération élémentaire $L_j\longleftarrow L_j+\mathrm{sgn}(a_i)qL_i$: on a $P\in\mathcal{M}_n(\mathbf{Z})$, $\det(P)=1$ et la première colonne de PM représente $\vec{v}$. Enfin $PM\in\mathcal{M}_n(\mathbf{Z})$ et $\det(PM)=\pm1$ donc PM représente une base entière qui commence par $\vec{v}$.

3) La matrice M de Φ est caractérisée par les relations : ${}^tM=M$ et $\forall\,\vec{x}\in\mathbf{R}^n$, $\Phi(\vec{x})=\mathrm{tr}({}^tXMX)$ où X est la matrice du vecteur $\vec{x}$. Si U est la matrice de l'endomorphisme u on a alors : $\Phi(u(\vec{x}))=\mathrm{tr}({}^t(UX)M(UX))=\mathrm{tr}({}^tX{}^tUMUX)$ et ${}^tUMU$ est symétrique, donc c'est la matrice de $\Phi\circ u$. La relation sur les discriminants s'ensuit.

4a) Φ étant définie positive, $\sqrt{\Phi}$ est une norme sur $\mathbf{R}^n$. En particulier, $A=\{\vec{v}\in\mathbf{Z}^n\setminus\{0\}\ \mathrm{tq}\ \Phi(\vec{v})\leqslant\Phi(\vec{e}_1)\}$ est une partie bornée de $\mathbf{Z}^n$, non vide, donc finie. Ainsi il existe $\vec{v}_1\in A$ tel que $\Phi(\vec{v}_1)$ est minimal. Alors pour $\vec{v}\in\mathbf{Z}^n\setminus\{0\}$, on a $\Phi(\vec{v})\geqslant\Phi(\vec{v}_1)$ si $\vec{v}\in A$ et $\Phi(\vec{v})\geqslant\Phi(\vec{e}_1)\geqslant\Phi(\vec{v}_1)$ si $\vec{v}\notin A$. Ceci prouve que $\Phi(\vec{v}_1)=\min\{\Phi(\vec{v}),\ \vec{v}\in\mathbf{Z}^n\setminus\{0\}\}$ et ce minimum est strictement positif car $\vec{v}_1\neq0$ et Φ est définie positive.

4b) Il suffit de prouver que les coordonnées de $\vec{v}_1$ sont premières entre elles. De fait, si d est le pgcd des coordonnées de $\vec{v}_1$ alors $d>0$ car $\vec{v}_1\neq0$ et $\vec{v}_1/d\in\mathbf{Z}^n\setminus\{0\}$. Donc $\Phi(\vec{v}_1)\leqslant\Phi(\vec{v}_1/d)=\Phi(\vec{v}_1)/d^2$, d'où $d\leqslant1$ et donc $d=1$.

4c) Soit f la forme polaire de Φ. Pour $x_1,\ldots,x_n\in\mathbf{R}$ on a, en notant $\vec{y}=x_2\vec{v}_2+\ldots+x_n\vec{v}_n$:

$$\begin{aligned}\Phi(x_1\vec{v}_1+\ldots+x_n\vec{v}_n)&=x_1^2\Phi(\vec{v}_1)+2x_1f(\vec{v}_1,\vec{y})+\Phi(\vec{y})\\&=m(\Phi)\underbrace{(x_1+f(\vec{v}_1,\vec{y})/m(\Phi))^2}_{L_1(x_1,\ldots,x_n)}+\underbrace{\Phi(\vec{y})-f(\vec{v}_1,\vec{y})^2/m(\Phi)}_{\Phi_1(x_2,\ldots,x_n)}.\end{aligned}$$

4d) On reprend les notations de la question précédente. Soit $(x_2,\ldots,x_n)\in\mathbf{R}^{n-1}$ et $x_1=-f(\vec{v}_1,\vec{y})/m(\Phi)$. Donc $\Phi_1(x_2,\ldots,x_n)=\Phi(x_1\vec{v}_1+\vec{y})\geqslant0$ et $\Phi_1(x_2,\ldots,x_n)=0$ si et seulement si $x_1\vec{v}_1+\vec{y}=0$, soit si et seulement si $\vec{y}=0$, soit encore si et seulement si $x_2=\ldots=x_n=0$. Donc Φ_1 est définie positive.

Considérons à présent les endomorphismes u, v de $\mathbf{R}^n$ définis par $u(x_1,\dots,x_n) = (L(x_1,\dots,x_n), x_2, \dots, x_n)$ et $v(x_1,\dots,x_n) = x_1\vec{v}_1 + \dots + x_n\vec{v}_n$. On a $\det(u) = L(1,0,\dots,0) = 1$ et $\det(v) = \det_{(\vec{e}_1,\dots,\vec{e}_n)}(\vec{v}_1,\dots,\vec{v}_n) = \pm 1$ car $(\vec{v}_1,\dots,\vec{v}_n)$ 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 :

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

4e) Prendre pour x_1 l'entier le plus proche de $-f(\vec{v}_1,\vec{y})/m(\Phi)$.

4f) Soit $(x_2,\dots,x_n) \in \mathbf{Z}^{n-1}\setminus\{0\}$ tel que $\Phi_1(x_2,\dots,x_n) = m(\Phi_1)$ et $x_1 \in \mathbf{Z}$ tel que $|L(x_1,\dots,x_n)| \leqslant \frac{1}{2}$. On a donc $m(\Phi) \leqslant \Phi(x_1\vec{v}_1 + \dots + x_n\vec{v}_n) \leqslant \frac{1}{4}m(\Phi) + m(\Phi_1)$, ce qui donne l'inégalité demandée.

4g) Avec **4d** et **4f** on obtient $\dfrac{m(\Phi)^n}{\operatorname{disc}(\Phi)} = \dfrac{m(\Phi)^{n-1}}{\operatorname{disc}(\Phi_1)} \leqslant (\frac{4}{3})^{n-1}\dfrac{m(\Phi_1)^n}{\operatorname{disc}(\Phi_1)}$, donc la quantité $(\frac{3}{4})^{1+\dots+(n-1)}\dfrac{m(\Phi)^n}{\operatorname{disc}(\Phi)}$ décroît quand la dimension augmente. Pour $n = 1$ elle vaut clairement 1, et l'on en déduit l'inégalité demandée (inégalité de HERMITE).

4h) Pour $n = 1$ c'est évident. Pour $n > 1$ on choisit $\vec{v}_1 \in \mathbf{Z}^n\setminus\{0\}$ tel que $\Phi(\vec{v}_1) = m(\Phi)$ et on complète $(\vec{v}_1)$ en une base entière $(\vec{v}_1,\dots,\vec{v}_n)$. Soit Φ_1 la forme quadratique sur $\mathbf{R}^{n-1}$ définie en **4c**. Par hypothèse de récurrence il existe une base entière $(\vec{u}_2,\dots,\vec{u}_n)$ de $\mathbf{R}^{n-1}$ telle que $\Phi_1(\vec{u}_2)\dots\Phi_1(\vec{u}_n) \leqslant (\frac{4}{3})^{(n-1)(n-2)/2}\operatorname{disc}(\Phi_1)$.

Soit $\vec{u}_i = (x_{i,2},\dots,x_{i,n})$ et $x_{i,1} \in \mathbf{Z}$ tel que $|L_1(x_{i,1},\dots,x_{i,n})| \leqslant \frac{1}{2}$. On pose alors $\vec{w}_i = x_{i,1}\vec{v}_1 + \dots + x_{i,n}\vec{v}_n$ et on vérifie que $(\vec{v}_1,\vec{w}_2,\dots,\vec{w}_n)$ répond au problème :

on a $\Phi(\vec{w}_i) = m(\Phi)L_1^2(x_{i,1},\dots,x_{i,n}) + \Phi_1(\vec{u}_i) \leqslant \frac{1}{4}\Phi(\vec{w}_i) + \Phi_1(\vec{u}_i)$ donc $\Phi(\vec{w}_i) \leqslant \frac{4}{3}\Phi_1(\vec{u}_i)$. Ainsi :

$$\Phi(\vec{v}_1)\Phi(\vec{w}_2)\dots\Phi(\vec{w}_n) \leqslant m(\Phi)(\tfrac{4}{3})^{n-1}\Phi_1(\vec{u}_2)\dots\Phi_1(\vec{u}_n) \leqslant (\tfrac{4}{3})^{n(n-1)/2}\operatorname{disc}(\Phi).$$

Si $\vec{v} \in \mathbf{Z}^n$, il existe des entiers $\alpha_1,\dots,\alpha_n$ tels que $\vec{v} = \alpha_1\vec{v}_1 + \dots + \alpha_n\vec{v}_n$ et il existe des entiers $\beta_2,\dots,\beta_n$ tels que $(\alpha_2,\dots,\alpha_n) = \beta_1\vec{u}_1 + \dots + \beta_n\vec{u}_n$. Alors :

$$\alpha_2\vec{v}_2 + \dots + \alpha_n\vec{v}_n = \beta_2(\vec{w}_2 - x_{2,1}\vec{v}_1) + \dots + \beta_n(\vec{w}_n - x_{n,1}\vec{v}_1).$$

Ceci prouve que $\vec{v}$ est combinaison linéaire à coefficients entiers de $(\vec{v}_1,\vec{w}_2,\dots,\vec{w}_n)$ et donc cette famille est bien une base entière de $\mathbf{R}^n$.

III. Transformation de Fourier et somme d'ensembles

1) Calcul immédiat.

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

2b) $\displaystyle\sum_{x\in\mathbf{Z}/n\mathbf{Z}}\hat{f}(x)\hat{g}(-x) = \sum_{x\in\mathbf{Z}}\sum_{a\in\mathbf{Z}/n\mathbf{Z}}\hat{f}(x)g(a)\omega^{-ax} = \sum_{a\in\mathbf{Z}}\sum_{x\in\mathbf{Z}/n\mathbf{Z}}\hat{f}(x)g(a)\omega^{-ax} = \sum_{a\in\mathbf{Z}/n\mathbf{Z}} Nf(a)g(a).$

2c) $\displaystyle\widehat{f*g}(x) = \sum_{a\in\mathbf{Z}/n\mathbf{Z}}(f*g)(a)\omega^{ax} = \sum_{a\in\mathbf{Z}/n\mathbf{Z}}\sum_{b\in\mathbf{Z}/n\mathbf{Z}} f(b)g(a-b)\omega^{ax} = \sum_{b\in\mathbf{Z}/n\mathbf{Z}}\sum_{a\in\mathbf{Z}/n\mathbf{Z}} f(b)g(a-b)\omega^{ax}$
$\displaystyle= \sum_{b\in\mathbf{Z}/n\mathbf{Z}}\sum_{c\in\mathbf{Z}/n\mathbf{Z}} f(b)g(c)\omega^{(b+c)x} = \Big(\sum_{b\in\mathbf{Z}/n\mathbf{Z}} f(b)\omega^{bx}\Big)\Big(\sum_{c\in\mathbf{Z}/n\mathbf{Z}} g(c)\omega^{cx}\Big) = \hat{f}(x)\hat{g}(x).$

3a) $\displaystyle\sum_{x\in\mathbf{Z}/n\mathbf{Z}}|\hat{f}_A(x)|^2 = \sum_{x\in\mathbf{Z}/n\mathbf{Z}}\Big(\sum_{a\in A}\omega^{ax}\Big)\Big(\sum_{b\in A}\omega^{-bx}\Big) = \sum_{a\in A}\sum_{b\in A}\sum_{x\in\mathbf{Z}/n\mathbf{Z}}\omega^{(a-b)x} = \sum_{a\in a}\sum_{b=a} N = N\operatorname{card}(A).$

$\displaystyle\sum_{x\in\mathbf{Z}/n\mathbf{Z}}|\hat{f}_A(x)|^4 = \sum_{x\in\mathbf{Z}/n\mathbf{Z}}\sum_{a\in A}\sum_{b\in A}\sum_{c\in A}\sum_{d\in A}\omega^{(a+b-c-d)x} = \sum_{a\in A}\sum_{b\in A}\sum_{c\in A}\sum_{d=a+b-c} N$
$= N\operatorname{card}\{(a,b,c,d)\in A^4 \text{ tq } a+b=c+d\}.$

3b) On a de même $\sum_{x\in\mathbf{Z}/n\mathbf{Z}} |\hat{f}(x)|^4\omega^{-tx} = N\,\mathrm{card}\{(a,b,c,d)\in A^4 \text{ tq } a+b-c-d=t\}$.

4a) 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 $x=\sum_{i=1}^{\kappa}(-\varepsilon\varepsilon_i)x_i$.

4b) On a pour $a\in\mathbf{Z}$: $d_N(a \bmod N)=\frac{1}{N}d(a,N\mathbf{Z})$ où d est la distance ordinaire sur $\mathbf{Z}$. 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 $\mathcal{B}(K,r/\kappa)\subset\mathcal{B}(X,r)$.

5a) Dériver deux fois.

5b) La courbe de $y\longmapsto\exp(ty)$ est au dessous de sa corde entre les points tels que $y=-1$ et $y=1$.

5c) $\cosh(t)=\sum_{n=0}^{\infty}\frac{t^{2n}}{(2n)!}\leqslant\sum_{n=0}^{\infty}\frac{t^{2n}}{2^n n!}=\exp(t^2/2)$ car $(2n)!=n!\times(n+1)\dots(2n)\geqslant 2^n n!$.

6a) $\hat{g}(x)=\sum_{a\in A}g(a)\omega^{ax}=\frac{1}{2}\sum_{a\in A}\sum_{j=1}^{\kappa}(c_j\omega^{a(x-x_j)}+\overline{c}_j\omega^{a(x+x_j)})=\frac{1}{2}\sum_{j=1}^{\kappa}\Big(c_j\sum_{a\in A}\omega^{a(x-x_j)}+\overline{c}_j\sum_{a\in A}\omega^{a(x+x_j)}\Big)$.
Si $x\in K$ alors il existe un unique j tel que $x=x_j$ 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 $0=\hat{g}(0)=\sum_{a\in\mathbf{Z}/n\mathbf{Z}}g(a)$.

6b) D'après **2b**, $\sum_{a\in\mathbf{Z}/n\mathbf{Z}}g(a)^2=\sum_{x\in\mathbf{Z}/N\mathbf{Z}}\hat{g}(x)\hat{g}(-x)=\sum_{x\in K\cup(-K)}\hat{g}(x)\hat{g}(-x)=2\sum_{x\in K}\hat{g}(x)\hat{g}(-x)=\frac{N}{2}\sum_{j=1}^{\kappa}|c_j|^2$.

6c) Notons $p=\mathrm{card}(J)$. On a pour $a\in\mathbf{Z}$:

$$\prod_{j\in J}\cos(\tfrac{2\pi}{N}a\tilde{x}_j+\theta_j)=\frac{1}{2^p}\prod_{j\in J}(\omega^{a\tilde{x}_j}e^{i\theta_j}+\omega^{-a\tilde{x}_j}e^{-i\theta_j})=\frac{1}{2^p}\sum_{\varepsilon\in\{-1,1\}^J}\omega^{a\left(\sum_{j\in J}\varepsilon_j x_j\right)}e^{i\left(\sum_{j\in J}\varepsilon_j\theta_j\right)}.$$

Comme $\sum_{j\in J}\varepsilon_j x_j\neq 0$, la somme de ces quantités lorsque a décrit $\{0,\dots,N-1\}$ est nulle d'après **1**.

6d) Pour $a\in\mathbf{Z}$ 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 $\theta_j\in\mathbf{R}$ et $y_j(a)\in[-1,1]$. Alors :

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

D'après la question précédente, seul le cas $J=\varnothing$ fournit une somme interne non nulle. Il vient :

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

7a) D'après **6b**, $\frac{2}{N}\sum_{a\in\mathbf{Z}/N\mathbf{Z}}g(a)^2=\sum_{j=1}^{\kappa}|\hat{f}_A(x_j)|^2=\sum_{j=1}^{\kappa}\hat{f}_A(x_j)\overline{\hat{f}_A(x_j)}=\sum_{j=1}^{\kappa}\hat{f}_A(x_j)\sum_{a\in A}\omega^{-ax_j}=\sum_{a\in A}\sum_{j=1}^{\kappa}\hat{f}_A(x_j)\omega^{-ax_j}$.

Cette somme est réelle, donc égale à la somme des parties réelles : $\frac{2}{N}\sum_{a\in\mathbf{Z}/N\mathbf{Z}} g(a)^2 = \sum_{a\in A} g(a) = \sum_{a\in\mathbf{Z}/N\mathbf{Z}} f(a)g(a)$.

7b) Par convexité de la fonction exponentielle et l'égalité précédente, on a :

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

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

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

Ainsi :

$$\forall\, t\in\mathbf{R},\ \ln(1/\alpha) + \frac{t^2}{N}\sum_{a\in\mathbf{Z}/N\mathbf{Z}} g(a)^2 \geqslant \frac{2t}{N}\sum_{a\in\mathbf{Z}/N\mathbf{Z}} g(a)^2.$$

Le discriminant en t de la différence est donc négatif ou nul, ce qui donne l'inégalité demandée.

7c) Résulte de $N\operatorname{card}(A)^2\ln(1/\alpha) \geqslant \sum_{a\in\mathbf{Z}/N\mathbf{Z}} g(a)^2 = \frac{N}{2}\sum_{j=1}^{\kappa}|\hat{f}_A(x_j)|^2 \geqslant \frac{N}{2}\kappa\rho^2\operatorname{card}(A)^2$.

8a) D'après **3a** et compte tenu de $\operatorname{card}(A)\geqslant\alpha N$, il suffit de prouver que le nombre de quadruplets $(a_1,a_2,a_3,a_4)\in A^4$ 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 :

$$\begin{aligned}
n\operatorname{card}(2A) &= \operatorname{card}(2A)\sum_{t\in 2A}\operatorname{card}\{(a_1,a_2,a_3,a_4)\in A^4 \text{ tq } a_1+a_2=t=a_3+a_4\}\\
&= \operatorname{card}(2A)\sum_{t\in 2A}\operatorname{card}\{(a_1,a_2)\in A^2 \text{ tq } a_1+a_2=t\}\times\operatorname{card}\{(a_3,a_4)\in A^2 \text{ tq } a_3+a_4=t\}\\
&= \operatorname{card}(2A)\sum_{t\in 2A}\operatorname{card}^2\{(a_1,a_2)\in A^2 \text{ tq } a_1+a_2=t\}\\
&= \Big(\sum_{t\in 2A} 1^2\Big)\Big(\sum_{t\in 2A}\operatorname{card}^2\{(a_1,a_2)\in A^2 \text{ tq } a_1+a_2=t\}\Big)\\
&\geqslant \Big(\sum_{t\in 2A}\operatorname{card}\{(a_1,a_2)\in A^2 \text{ tq } a_1+a_2=t\}\Big)^2 = \operatorname{card}(A)^4.
\end{aligned}$$

8b) Pour $x\notin X$ on a $|\hat{f}_A(x)| < \rho\operatorname{card}(A) = \frac{\operatorname{card}(A)}{2\sqrt{\sigma}}$, d'où :

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

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

8c) Soit $a\in\mathbf{Z}$ et $b\in a+N\mathbf{Z}$ 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 :

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

On a vu en **a** que $\sum_{x\in\mathbf{Z}/N\mathbf{Z}}|\hat{f}_A(x)|^4 \geqslant \frac{N\,\mathrm{card}(A)^3}{\sigma}$ et en **b** que $\sum_{x\notin X}|\hat{f}_A(x)|^4 \leqslant \frac{N\,\mathrm{card}(A)^3}{4\sigma}$. Il vient alors :

$$\Big|\sum_{x\in\mathbf{Z}/N\mathbf{Z}}|\hat{f}_A(x)|^4\omega^{-ax}\Big| \geqslant \frac{N\,\mathrm{card}(A)^3}{4\sigma}(4-\tfrac{\pi}{2}-(2-\tfrac{\pi}{8})) \geqslant \frac{N\,\mathrm{card}(A)^3}{4\sigma}(2-\tfrac{3\pi}{8}) > 0.$$

D'après **3b**, ceci implique $a \in 2A-2A$.
Remarque : on peut par les mêmes calculs prouver que $\mathcal{B}(X,r)\subset 2A-2A$ pour tout $r<\frac{1}{3\pi}$.

8d) Soit $(x_1,\dots,x_\kappa)$ une suite indépendante maximale dans X, et $K=\{x_1,\dots,x_\kappa\}$.
Donc $\mathrm{card}(K)=\kappa\leqslant 2\rho^{-2}\ln(1/\alpha)=8\sigma\ln(1/\alpha)$. Et, d'après **4b**, $\mathcal{B}(K,r)\subset\mathcal{B}(K,\frac{1}{16\kappa})\subset\mathcal{B}(X,\frac{1}{16})\subset 2A-2A$.

IV. Progressions arithmétiques

1a) Soit i tel que ξ_i n'est pas divisible par N. Donc ξ_i est premier à N ; soient $a,b_i\in\mathbf{Z}$ 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.

1b) 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 $\mathbf{R}^n$, notée $(\overrightarrow{v}_1,\dots,\overrightarrow{v}_n)$. On a $\overrightarrow{v}_1 = a\overrightarrow{\xi}+N\overrightarrow{b}$ et $\xi_i\overrightarrow{v}_1 = a\xi_i\overrightarrow{\xi}+N\xi_i\overrightarrow{b} = \overrightarrow{\xi}+N(\xi_i\overrightarrow{b}-b_i\overrightarrow{\xi})$, donc les groupes $L=\mathbf{Z}\overrightarrow{\xi}+N\mathbf{Z}^n$ et $L'=\mathbf{Z}\overrightarrow{v}_1+N\mathbf{Z}^n$ sont égaux. En particulier un vecteur $\overrightarrow{x}=t_1\overrightarrow{v}_1+\dots+t_n\overrightarrow{v}_n$ 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.

1c) Soit u l'endomorphisme de $\mathbf{R}^n$ défini par $u(x_1,\dots,x_n)=x_1\overrightarrow{v}_1+Nx_2\overrightarrow{v}_2+\dots+Nx_n\overrightarrow{v}_n$ et Φ la forme quadratique sur $\mathbf{R}^n$ définie par $\Phi(\overrightarrow{x})=\|u(\overrightarrow{x})\|^2$. On a $\mathrm{disc}(\Phi)=\det^2(u)=N^{2n-2}\det^2(\overrightarrow{v}_1,\dots,\overrightarrow{v}_n)=N^{2n-2}$, 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 $\mathbf{R}^n$ 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.

2a) Par définition, $\sum_{i=1}^n\mu_i\overrightarrow{w}_i-p(\mu)\xi\in N\mathbf{Z}^n$. Donc $p(\mu)=p(\mu')\Longrightarrow\sum_{i=1}^n(\mu_i-\mu'_i)\overrightarrow{w}_i\in N\mathbf{Z}^n$. Or, pour $\mu,\mu'\in M$, on a $\Big\|\sum_{i=1}^n(\mu_i-\mu'_i)\overrightarrow{w}_i\Big\|\leqslant 2Nr<N$. On en déduit $p(\mu)=p(\mu')\Longrightarrow\sum_{i=1}^n(\mu_i-\mu'_i)\overrightarrow{w}_i=\overrightarrow{0}\Longrightarrow\mu=\mu'$ car $(\overrightarrow{w}_1,\dots,\overrightarrow{w}_n)$ est libre.

2b) D'après **2a** et **1c**, $\mathrm{card}(P)=\mathrm{card}(M)=\prod_{i=1}^n\Big(1+2\Big\lfloor\frac{Nr}{n\|\overrightarrow{w}_i\|}\Big\rfloor\Big)\geqslant\prod_{i=1}^n\Big(\frac{Nr}{n\|\overrightarrow{w}_i\|}\Big)\geqslant N(\frac{r}{n})^n(\frac{3}{4})^{n(n-1)/4}$.

2c) Comme $\sum_{i=1}^n\mu_i\overrightarrow{w}_i-p(\mu)\overrightarrow{\xi}\in N\mathbf{Z}^n$, on a pour tout j : $d_N(p(\mu)\xi_j)=d_N\Big(\sum_{i=1}^n\mu_i e_j^*(\overrightarrow{w}_i)\Big)\leqslant\frac{1}{N}\Big\|\sum_{i=1}^n\mu_i\overrightarrow{w}_i\Big\|\leqslant r$.

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

4) Cette question est fausse : si l'on prend $A = \mathbf{Z}/N\mathbf{Z}$, 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 $\mathbf{Z}/N\mathbf{Z}$.

Tentative de correction de l'énoncé : avec **III-8**, on a l'existence de $K \subset \mathbf{Z}/N\mathbf{Z}$ 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...

V. Théorème de Freiman-Rusza-Chang

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

1b) Il faut vérifier que la quantité $f(a_1) + \ldots + f(a_m) - f(b_1) - \ldots - f(b_n)$ ne dépend que de $a_1 + \ldots + a_m - b_1 - \ldots - b_n$. Soient $a_1, \ldots, d_n$ des éléments de A. On a :

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

1c) Immédiat.

1d) On note $A = \{x_0 + \sum_{i=1}^{d} n_i x_i,\ 0 \leqslant n_i < N_i\}$. Pour $i \in \{1, \ldots, d\}$ 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 :

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

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

2a) Soient $f : A \longrightarrow B$ et $g : B \longrightarrow A$ 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 :

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

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

2b) Avec $p = 1$ on obtient une bijection entre $mA - nA$ et $mB - nB$ donc ces ensembles ont même cardinal.

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

3b) Si $N = 0$, on considère que $\mathbf{Z}/0\mathbf{Z} = \mathbf{Z}$ et que la relation de congruence modulo N est l'identité sur $\mathbf{Z}$. 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 $\mathbf{Z} \ni t \longmapsto t \bmod N \in \mathbf{Z}/N\mathbf{Z}$, et comme $u \in (\mathbf{Z}/p\mathbf{Z})^*$, 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 $\mathrm{card}(A)/k$.

3c) Si $N \geqslant 1$, les éléments x de $(\mathbf{Z}/p\mathbf{Z})^*$ 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, $u \in (\mathbf{Z}/p\mathbf{Z})^*$ 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 $u \in (\mathbf{Z}/p\mathbf{Z})^*$ tel que :

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

Je dis que pour un tel u, on a :

$$\forall\, a_1, \ldots, b_k \in A(u),\ f_u(a_1) + \ldots . f_u(a_k) = f_u(b_1) + \ldots . f_u(b_k) \iff a_1 + \ldots . a_k = b_1 + \ldots + b_k. \qquad (*)$$

Démonstration :

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

$$\begin{aligned} f_u(a_1) + \ldots . f_u(a_k) = f_u(b_1) + \ldots . f_u(b_k) & \\ \iff f(u(a_1 + \ldots + a_k)) - (j-1)p \equiv f(u(b_1 + \ldots + b_k) + (j-1)p & \pmod N \\ \iff f(u(a_1 + \ldots + a_k)) - f(u(b_1 + \ldots + b_k)) \equiv 0 & \pmod N \end{aligned}$$

Or,

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

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

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

Ainsi $(*)$ est prouvée. On en déduit en prenant $a_2 = a_3 = \ldots = a_n = b_2 = b_3 = \ldots = b_n$ 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 $(*)$.

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

4b) On suppose $k \geqslant 1$ dans cette question. Soit p un nombre premier majorant strictement $kA - kA$ (il en existe) et φ l'application $\mathbf{Z} \ni x \longmapsto x \bmod p \in \mathbf{Z}/p\mathbf{Z}$. Par choix de p et stabilité de de $kA - kA$ par opposé, on a :

$$\forall\, a_1, \ldots, b_k \in A,\ \varphi(a_1) + \ldots + \varphi(a_k) = \varphi(b_1) + \ldots + \varphi(b_k) \iff a_1 + \ldots + a_k = b_1 + \ldots + b_k.$$

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.

4c) On applique **3** à $\varphi(A) \subset \mathbf{Z}/p\mathbf{Z}$: 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 $C \subset \mathbf{Z}/N\mathbf{Z}$ 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.

4d) 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 $C \subset \mathbf{Z}/N\mathbf{Z}$ définie à la question précédente vérifie :

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

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.

5a) 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.

5b) 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 $A \subset P_t - P_t + S_t = (P + S'_0 + \ldots + S'_{t-1}) - (P + S'_0 + \ldots + S'_{t-1}) + S_t = (P - P) + (S'_0 - S'_0) + \ldots + (S'_{t-1} - S'_{t-1}) + S_t$.

5c) 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 :

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

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 $\ln(\tau/\mathrm{card}(A))$:

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

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

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 $\ln(\tau/\operatorname{card}(A))$ est majoré par $O(\sigma^3 \ln^2(\sigma))$.

Fin du corrigé