POLYTOPES ET POINTS ENTIERS

Sommaire

Introduction 2
1. Les simplexes 3
2. Polytopes et points entiers 4
3. Polygones entiers 7
4. Le polynôme d'Ehrhart 9
5. Points entiers dans des convexes compacts assez symétriques 12
6. Énoncé du théorème de Hensley sur les points entiers dans les polytopes entiers

Résumé. Un polytope est l'enveloppe convexe d'un ensemble fini de points de l'espace. Il est dit entier si ces points peuvent être choisis à coordonnées entières. Le thème général de cet article est le comptage du nombre de points à coordonnées entières dans un polytope entier et la finitude du nombre de types de polytopes entiers pour lesquels ce nombre est fixé non nul. Les techniques utilisées sont complètement élémentaires. Outre leur intérêt propre, ces problèmes ont un lien très étroit avec des problèmes de géométrie.

Introduction

Dans tout ce texte, un *polytope* est l'enveloppe convexe[1] d'un sous-ensemble fini de l'espace euclidien $\mathbf{R}^n$. C'est donc un compact (fermé et borné). Sa *dimension* est celle de l'espace affine qu'il engendre.

On appelle *intérieur relatif* d'un polytope P son intérieur dans l'espace affine qu'il engendre. On le note P'.

Un point de P est un *sommet* s'il n'est intérieur à aucun segment entièrement contenu dans P.

Soit Σ un sous-ensemble de $\mathbf{R}^n$. Le *théorème de Carathéodory* énonce que *tout point de l'enveloppe convexe* $\mathrm{Conv}(\Sigma)$ *est dans l'enveloppe convexe d'un sous-ensemble de* Σ *de points affinement indépendants.*

Proposition 1. *Les sommets d'un polytope P sont en nombre fini et leur enveloppe convexe est P.*

Démonstration. Soit Σ un ensemble (fini) de cardinal minimal dont P soit l'enveloppe convexe. Nous allons montrer que Σ est exactement l'ensemble des sommets de P.

Soit s un sommet de P. Par le théorème de Carathéodory, on peut écrire $s = \lambda_1 s_1 + \cdots + \lambda_m s_m$, avec $s_1, \ldots, s_m$ points de Σ affinement indépendants, $\lambda_i > 0$ et $\lambda_1 + \cdots + \lambda_m = 1$. Si $m > 1$, le point s est dans l'intérieur du segment joignant

$$(1 - \lambda_3 - \cdots - \lambda_m)s_1 + \lambda_3 s_3 + \cdots + \lambda_m s_m$$

à

$$(1 - \lambda_3 - \cdots - \lambda_m)s_2 + \lambda_3 s_3 + \cdots + \lambda_m s_m$$

ce qui est absurde. On a donc $m = 1$, c'est-à-dire $s \in \Sigma$.

Inversement, pour tout point s de Σ, notons $Q \subsetneq P$ l'enveloppe convexe de $\Sigma - \{s\}$. Notons x le point de Q le plus proche de s et H l'hyperplan affine passant par x et orthogonal au segment xs. Son équation est $\varphi(y) = \langle y - x, s - x\rangle = 0$ et φ est négative sur Q, strictement positive en s. On en déduit que φ atteint son maximum sur P en le seul point s, qui est par conséquent un sommet de P. □

Plus généralement, on appelle *face* d'un polytope P tout sous-ensemble de P défini comme $P \cap H$, où H est un hyperplan affine tel que P soit entièrement contenu dans un des deux demi-espaces qu'il définit. En particulier $\varnothing$ est une face de P. Il est aussi pratique de décréter que P est une face de P. Ces deux faces sont dites impropres.

[1] L'*enveloppe convexe* d'un sous-ensemble S de $\mathbf{R}^n$ est l'intersection des sous-ensembles convexes de $\mathbf{R}^n$ qui contiennent S: c'est le plus petit sous-ensemble convexe de $\mathbf{R}^n$ qui contient S. C'est aussi l'ensemble des barycentres à coefficients positifs de points de S.

On montre que P n'a qu'un nombre fini de faces, et que chaque face est elle-même un polytope, enveloppe convexe des sommets de P qu'elle contient. Une *facette* est une face de dimension $\dim(P) - 1$. Enfin, un polytope est réunion disjointe des intérieurs relatifs de ses faces.

1. Les simplexes

On appelle *r-simplexe* l'enveloppe convexe de $r+1$ points affinement indépendants dans $\mathbf{R}^n$. Les r-simplexes sont donc exactement les polytopes de dimension r avec $r+1$ sommets.

On appelle *r-simplexe ouvert* l'intérieur relatif d'un simplexe. En particulier, un point est un simplexe et un simplexe ouvert.

Proposition 2. *Tout polytope P est réunion disjointe de simplexes ouverts dont les sommets sont des sommets de P.*

Démonstration. Soit s un sommet de P, soient $F_1, \dots, F_r$ les faces (propres) de P ne contenant pas s et soient $F_1', \dots, F_r'$ leurs intérieurs relatifs. Les ensembles $\{s\}, \mathrm{Conv}(\{s\} \cup F_1') - \{s\}, \dots, \mathrm{Conv}(\{s\} \cup F_r') - \{s\}$ forment une partition de P.

En raisonnant par récurrence sur la dimension de P, on sait décomposer chaque F_i en réunion disjointe de simplexes ouverts dont les sommets sont des sommets de F_i, donc de P. En excluant les simplexes contenus dans $F_i - F_i'$, on obtient une décomposition de chaque F_i' en réunion disjointe de simplexes ouverts, donc aussi une telle décomposition de chaque $\mathrm{Conv}(\{s\} \cup F_i') - \{s\}$. □

Le volume euclidien d'un n-simplexe de sommets $s_0, \dots, s_n$ dans $\mathbf{R}^n$ est

$$\frac{1}{n!} \det(\overrightarrow{s_0 s_1}, \dots, \overrightarrow{s_0 s_n}) \tag{1}$$

Soit K un convexe compact dans $\mathbf{R}^n$. La fonction qui à $n+1$ points de K associe le volume du simplexe (peut-être dégénéré) engendré est donc continue. Elle atteint donc son maximum et on peut parler d'un simplexe de volume maximal contenu dans K.

Un polytope P contient un simplexe de volume maximal dont les sommets sont des sommets de P. En effet, soit s un sommet d'un simplexe S de volume maximal contenu dans P. Considérons l'hyperplan affine H engendré par les autres sommets de S. Le point s est un point de P à distance maximale de H. L'intersection avec P de l'hyperplan affine parallèle à H et passant par s est par définition une face de P donc contient un sommet de P. On peut donc changer s en un sommet de P (sans changer les autres sommets de S). On procède ainsi pour chaque sommet de S.

Proposition 3. *Soit K un convexe compact dans $\mathbf{R}^n$ et soit S un simplexe de volume maximal contenu dans K, de centre de gravité g_0. On a*

$$K \subset -nS + (n+1)g_0$$

Démonstration. On peut supposer $g_0 = 0$. Soient $s_0, \dots, s_n$ les sommets de S. Pour chaque i, on note H_i l'hyperplan affine passant par les sommets de S autres que s_i. Le convexe K est tout entier contenu dans la région R_i composée des points de $\mathbf{R}^n$ situés à distance moindre que $d(s_i, H_i)$ de H_i. Nous allons montrer que $\bigcap_{i=0}^n R_i$ est contenu dans $-nS$. En coordonnées barycentriques, on a

$$R_i = \Big\{ \sum_{j=0}^n \alpha_j s_j \;\Big|\; \sum_{j=0}^n \alpha_j = 1,\ |\alpha_i| \le 1 \Big\}$$

puisque la distance d'un point $\sum_{j=0}^n \alpha_j s_j$ à H_i est $|\alpha_i| d(s_i, H_i)$. Posons $\beta_j = \frac{1-\alpha_j}{n}$. On a $\sum_{j=0}^n \beta_j = 1$ et $\beta_i \ge 0$ et comme $\sum_{j=0}^n s_j = 0$,

$$R_i \subset \Big\{ -n \sum_{j=0}^n \beta_j s_j \;\Big|\; \sum_{j=0}^n \beta_j = 1,\ \beta_i \ge 0 \Big\}$$

de sorte que l'on a $\bigcap_{i=0}^n R_i \subset -nS$. □

2. Polytopes et points entiers

On appelle *point entier* dans $\mathbf{R}^n$ un point dont toutes les coordonnées sont entières, c'est-à-dire un point de $\mathbf{Z}^n$. On appelle *polytope entier* un polytope dont tous les sommets sont entiers. C'est un très vieux problème que d'estimer ou de relier le nombre de points entiers d'un tel polytope, le nombre de points entiers dans son intérieur relatif P' et le volume de P.

Il est utile d'introduire le concept de *base* de $\mathbf{Z}^n$. La définition est la même que pour un espace vectoriel.

Définition 1. *Une famille $(x_1, \dots, x_n)$ de vecteurs de $\mathbf{Z}^n$ en est une* base *si tout vecteur de $\mathbf{Z}^n$ peut s'écrire comme combinaison linéaire de $x_1, \dots, x_n$ à coefficients entiers.*

Attention, n vecteurs de $\mathbf{Z}^n$ peuvent être libres dans l'espace vectoriel $\mathbf{R}^n$ sans former une base de $\mathbf{Z}^n$. On a les caractérisations suivantes.

Proposition 4. *Soient $x_1, \dots, x_n$ des vecteurs de $\mathbf{Z}^n$ qui forment une base de l'espace vectoriel $\mathbf{R}^n$. Les conditions suivantes sont équivalentes :*

(i) *la famille $(x_1, \dots, x_n)$ est une base de $\mathbf{Z}^n$;*
(ii) *le déterminant de $(x_1, \dots, x_n)$ dans la base canonique est ± 1 ;*

(iii) *le parallélépipède construit sur les vecteurs $x_1, \dots, x_n$ ne contient aucun point entier autre que les 2^n points $\varepsilon_1 x_1 + \cdots + \varepsilon_n x_n$, $\varepsilon_i \in \{0, 1\}$.*

Démonstration. Soient A la matrice (entière) dont les colonnes sont les coordonnées des vecteurs $(x_1, \dots, x_n)$ dans la base canonique et B son inverse, c'est-à-dire la matrice dont les colonnes sont les coordonnées des vecteurs de la base canonique dans la base $(x_1, \dots, x_n)$ de l'espace vectoriel $\mathbf{R}^n$.

Si (i) est vérifié, la matrice B est à coefficients entiers et $AB = I_n$. En prenant les déterminants (entiers), on obtient (ii). Inversement, si le déterminant de A est ± 1, la formule donnant les coefficients de l'inverse A^{-1} à partir des cofacteurs (entiers) de A montre que B est aussi à coefficients entiers. On en déduit (i). Donc (i) et (ii) sont équivalents.

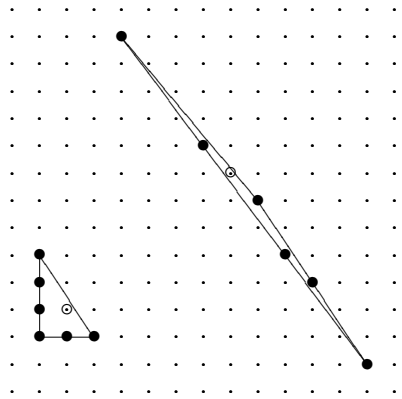
Supposons (iii) vérifié. Tout vecteur de $\mathbf{Z}^n$ peut s'écrire $\lambda_1 x_1 + \cdots + \lambda_n x_n$, avec $\lambda_1, \dots, \lambda_n \in \mathbf{R}$. Le point entier

$$(\lambda_1 - [\lambda_1])x_1 + \cdots + (\lambda_n - [\lambda_n])x_n$$

est dans le parallélépipède construit sur les vecteurs $x_1, \dots, x_n$, donc $\lambda_i - [\lambda_i] = 0$ pour tout i et (i) est vérifié. Inversement, si (i) est vérifié, tout point entier dans le parallélépipède construit sur les vecteurs $x_1, \dots, x_n$ est combinaison linéaire de ceux-ci à coefficients entiers, qui valent donc nécessairement 0 ou 1. Donc (i) et (iii) sont équivalents. □

Lorsque l'on étudie les polytopes entiers, il faut tenir compte des transformations de l'espace euclidien $\mathbf{R}^n$ préservant le réseau $\mathbf{Z}^n$ (et donc les notions de point entier et de polytope entier) : ces transformations sont les translations par un vecteur à coordonnées entières et les transformations linéaires $x \mapsto Ax$, où A est une matrice de $\mathrm{GL}_n(\mathbf{Z})$ c'est-à-dire, par la proposition 4, une matrice $n \times n$ à coefficients entiers et de déterminant ± 1. Une telle transformation préserve donc aussi le volume euclidien. Deux polytopes qui diffèrent par une telle transformation seront dits *équivalents.*

Attention, des polytopes équivalents peuvent sembler très différents, mais de notre point de vue, leurs propriétés sont les mêmes : même volume, même nombre de points entiers, même nombre de points entiers intérieurs. Les triangles suivants sont équivalents



Ils sont chacun d'aire 3 et contiennent chacun 7 points entiers dont un seul intérieur.

L'inégalité suivante majore le nombre de points entiers en fonction du volume. C'est très important de notre point de vue : il nous « suffira » de majorer le volume d'un polytope entier ayant un nombre de points entiers intérieurs fixé.

Théorème 1 (Blichfeldt)**.** *Soit K un compact convexe de l'espace euclidien $\mathbf{R}^n$ tel que $K \cap \mathbf{Z}^n$ ne soit pas inclus dans un hyperplan. On a*

$$\mathrm{Card}(K \cap \mathbf{Z}^n) \leq n + n! \,\mathrm{vol}(K)$$

Démonstration. Quitte à remplacer K par l'enveloppe convexe de ses points entiers, on voit qu'il suffit de traiter le cas d'un polytope entier P de dimension n.

On procède par récurrence sur la quantité $\mathrm{Card}(P \cap \mathbf{Z}^n)$, qui est au moins égale à $n + 1$. Si $\mathrm{Card}(P \cap \mathbf{Z}^n) = n + 1$, le polytope P est un simplexe entier, donc de volume au moins égal à $\frac{1}{n!}$ par la formule (1).

Si P n'est pas un simplexe, il existe un sommet s de P tel que le polytope (entier) Q enveloppe convexe des autres sommets de P soit de dimension n. Le polytope Q est intersection de demi-espaces définis par ses facettes. Comme $s \notin Q$, il existe une de ces facettes, $F = Q \cap H$, telle que s et Q soient de part et d'autre de H. Soit R le polytope $\mathrm{Conv}(\{s\} \cup F)$. Les polytopes Q et R sont chacun de dimension n, ont strictement moins de points entiers que P et ont au moins n sommets (entiers) en commun (ceux de F). De plus, $P = Q \cup R$ et $F = Q \cap R$. On en déduit, à l'aide de l'hypothèse de récurrence,

$$\begin{aligned} \mathrm{Card}(P \cap \mathbf{Z}^n) &\leq \mathrm{Card}(Q \cap \mathbf{Z}^n) + \mathrm{Card}(R \cap \mathbf{Z}^n) - n \\ &\leq n + n! \,\mathrm{vol}(Q) + n! \,\mathrm{vol}(R) \\ &= n + n! \,\mathrm{vol}(P) \end{aligned}$$

d'où le théorème. □

Il n'y a bien sûr pas de majoration générale dans l'autre sens, puisqu'il existe des convexes compacts arbitrairement grands sans point entier. En revanche, pour certains polytopes, on peut obtenir une telle majoration. Ce sera l'objet du § 5.

3. Polygones entiers

Examinons tout d'abord le cas beaucoup plus simple des polygones (convexes), c'est-à-dire des polytopes de dimension 2. On souhaite estimer le nombre de points entiers sur le bord d'un polygone entier en fonction du nombre de points entiers à l'intérieur. Le premier résultat dans cette direction est le célèbre théorème de Pick.

Théorème 2 (Pick, 1900)**.** *Si $P \subset \mathbf{R}^2$ est un polygone convexe entier,*

$$\mathrm{vol}(P) = \mathrm{Card}(P \cap \mathbf{Z}^2) - \frac{1}{2}\,\mathrm{Card}(\partial P \cap \mathbf{Z}^2) - 1 \tag{2}$$

Démonstration. Considérons d'abord un triangle entier T dont les seuls points entiers sont les sommets. Les seuls points entiers du parallélogramme obtenu par symétrie de T par rapport au milieu d'un de ses côtés en sont les quatre sommets. Par la proposition 4, l'aire de T est donc $1/2$ et la formule (2) est vérifiée dans ce cas.

On traite maintenant le cas d'un triangle entier quelconque, en procédant par récurrence sur le nombre de points entiers qu'il contient. Si T est un triangle entier avec au moins 4 points entiers, on choisit un point entier x dans T qui ne soit pas un sommet. En le joignant aux 3 sommets, on décompose T en la réunion de 2 ou 3 triangles, selon que x est sur le bord de T ou non, triangles pour lesquels la formule (2) est connue. Dans le premier cas, si T_1 et T_2 sont ces triangles et s le sommet de T opposé à x, on a ainsi

$$\begin{aligned}
\mathrm{vol}(T) &= \mathrm{vol}(T_1) + \mathrm{vol}(T_2)\\
&= \mathrm{Card}(T_1 \cap \mathbf{Z}^2) + \mathrm{Card}(T_2 \cap \mathbf{Z}^2)\\
&\qquad - \frac{1}{2}\,\mathrm{Card}(\partial T_1 \cap \mathbf{Z}^2) - \frac{1}{2}\,\mathrm{Card}(\partial T_2 \cap \mathbf{Z}^2) - 2\\
&= \mathrm{Card}(T \cap \mathbf{Z}^2) + \mathrm{Card}([sx] \cap \mathbf{Z}^2)\\
&\qquad - \frac{1}{2}\big(\mathrm{Card}(\partial T \cap \mathbf{Z}^2) + 2\,\mathrm{Card}(]sx[\cap \mathbf{Z}^2) + 2\big) - 2\\
&= \mathrm{Card}(T \cap \mathbf{Z}^2) - \frac{1}{2}\,\mathrm{Card}(\partial T \cap \mathbf{Z}^2) - 1
\end{aligned}$$

On procède de façon analogue si l'on a 3 triangles.

Enfin, on peut traiter le cas des polygones entiers généraux par récurrence sur le nombre de sommets. Si s est un sommet d'un polygone entier P, on écrit P comme la réunion du triangle de sommets s et les sommets de P voisins de s, et du polygone $\mathrm{Conv}(P - \{s\})$, qui a un sommet de moins que P. On utilise ensuite le même raisonnement que celui employé ci-dessus. □

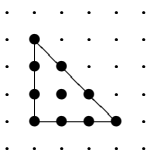
Si les seuls points entiers d'un polygone entier P sont sur son bord, on déduit de la formule de Pick l'égalité $\mathrm{Card}(P \cap \mathbf{Z}^2) = 2\,\mathrm{vol}(P) + 2$ et cette quantité n'est pas bornée comme le montre l'exemple du triangle de sommets $(0,0)$, $(0,1)$ et $(d,0)$ (d entier positif quelconque).

La situation est complètement différente pour les polygones entiers ayant au moins un point entier intérieur, comme le montre le résultat suivant.

Théorème 3 (Scott, 1976)**.** *Soit P un polygone dont le nombre k de points entiers intérieurs n'est pas nul. On a*

$$\mathrm{Card}(P \cap \mathbf{Z}^2) \leq 3k + 6$$

sauf si P est équivalent au triangle



avec un point entier intérieur et 10 points entiers.

On déduit de la formule de Pick la majoration

$$\mathrm{vol}(P) \leq 2k + 2$$

sauf dans le cas exceptionnel ci-dessus.

Démonstration. Il s'agit de montrer que la quantité

$$\delta = \mathrm{Card}(P \cap \mathbf{Z}^2) - 3\,\mathrm{Card}(\overset{\circ}{P} \cap \mathbf{Z}^2) = 2(\mathrm{Card}(\partial P \cap \mathbf{Z}^2) - \mathrm{vol}(P) - 1)$$

est majorée par 6, sauf dans le cas du triangle ci-dessus.

On peut supposer que P est contenu entre les droites horizontales d'équation $y = 0$ et $y = h \geq 2$, rencontre la droite $y = 0$ le long du segment (entier) $S_0 = [0, a]$ et la droite $y = h$ le long d'un segment (entier) S_h de longueur $b \geq a$.

On a

$$\mathrm{Card}(\partial P \cap \mathbf{Z}^2) \leq a + b + 2h \quad , \quad \mathrm{vol}(P) \geq \frac{1}{2}h(a+b)$$

donc

$$\delta \leq 2(a + b + 2h) - h(a+b) - 2 = 6 - (a + b - 4)(h - 2)$$

On a $h \geq 2$ car P contient un point intérieur entier.

Si $h = 2$, on a terminé. Si $h = 3$ aussi, sauf si $a + b \leq 3$. Si $a + b \leq 2$, on a $\mathrm{Card}(\partial P \cap \mathbf{Z}^2) \leq 8$ et $\delta = \mathrm{Card}(\partial P \cap \mathbf{Z}^2) - 2\,\mathrm{Card}(\overset{\circ}{P} \cap \mathbf{Z}^2) \leq 6$ puisque P contient (au moins) un point intérieur entier. Si $a+b = 3$, on a $\mathrm{Card}(\partial P \cap \mathbf{Z}^2) \leq 9$ et $\delta \leq 7$, avec égalité si et seulement si

$$\mathrm{Card}(\partial P \cap \mathbf{Z}^2) = 9\ ,\quad \mathrm{Card}(\overset{\circ}{P} \cap \mathbf{Z}^2) = 1\ ,\quad \mathrm{vol}(P) = \frac{9}{2} = \frac{1}{2}h(a+b)$$

Cette dernière égalité montre que P est un trapèze de bases S_0 et S_h. Si $a = 1$ (et $b = 2$), il y a au plus 7 points entiers sur le bord. Donc $a = 0$ et P est un triangle, équivalent au triangle ci-dessus.

Supposons donc $h \geq 4$ et $a + b \leq 3$. On peut aussi supposer que la plus grande différence h' entre abcisses de points de P est $\geq h$ (sinon, on échange les coordonnées). Appliquons une équivalence $A : (x, y) \mapsto (x + my, y)$, avec $m \in \mathbf{Z}$, de façon que le segment entier $A(S_h) - (0, h)$, porté par l'axe des x, soit le plus proche possible de S_0. La distance d entre ces deux segments entiers est alors $\leq \frac{1}{2}(h-a-b)$. Si par hasard, h' est devenu $< h$, on échange les coordonnées et on recommence le processus (qui doit s'arrêter, puisqu'à chaque pas, l'entier $h+h'$ décroît strictement).

On minore alors le volume de P par celui d'un quadrilatère pour obtenir

$$\mathrm{vol}(P) \geq \frac{1}{2}h(h' - d) \geq \frac{1}{2}h(h - d) \geq \frac{1}{4}h(h + a + b)$$

de sorte que

$$\begin{aligned}\delta &\leq 2(a+b+2h) - \frac{1}{2}h(h+a+b) - 2\\ &= \frac{1}{2}h(8-h) - \frac{1}{2}(a+b)(h-4) - 2\\ &\leq 6\end{aligned}$$

Ceci termine la démonstration. □

4. Le polynôme d'Ehrhart

Ce paragraphe est de nature un peu différente et n'est pas nécessaire pour la suite. Il est consacré à un très joli résultat qui généralise la formule de Pick en toute dimension et ne peut être passé sous silence.

Théorème 4 (Ehrhart, 1967)**.** *Soit P un polytope entier dans $\mathbf{R}^n$. La fonction*

$$\begin{array}{rccc}\varphi_P & : & \mathbf{N} & \longrightarrow & \mathbf{N}^* \\ & & m & \longmapsto & \mathrm{Card}(mP \cap \mathbf{Z}^n)\end{array}$$

est polynomiale, de degré la dimension r de P et de coefficient dominant le volume r-dimensionnel de P. On a d'autre part, pour tout entier $m > 0$,

$$\mathrm{Card}(mP' \cap \mathbf{Z}^n) = (-1)^r \varphi_P(-m)$$

Un polytope entier P dans $\mathbf{R}$ est un intervalle $[p, q]$. Il contient $q - p + 1$ points entiers, et

$$\begin{aligned}\varphi_P(m) &= mq - mp + 1\\ \varphi_{P'}(m) &= mq - mp - 1 = -\varphi_P(-m)\end{aligned}$$

On a de même $\varphi_{]p,q]}(m) = mq - mp = m\varphi_{]p,q]}(1)$. On a la même formule pour un segment entier semi-ouvert dans le plan. Lorsque P est de dimension 2, on en déduit $\varphi_{\partial P}(m) = m\varphi_{\partial P}(1)$ d'où, en utilisant la formule de Pick,

$$\begin{aligned}\varphi_P(m) &= m^2\,\mathrm{vol}(P) + \frac{m}{2}\,\mathrm{Card}(\partial P \cap \mathbf{Z}^n) + 1\\ \varphi_{P'}(m) &= \varphi_P(m) - \mathrm{Card}(\partial(mP) \cap \mathbf{Z}^n)\\ &= m^2\,\mathrm{vol}(P) - \frac{m}{2}\,\mathrm{Card}(\partial P \cap \mathbf{Z}^n) + 1\\ &= \varphi_P(-m)\end{aligned}$$

Inversement, on peut déduire la formule de Pick du théorème.

Démonstration du théorème 4. Grâce à la proposition 2, il suffit pour montrer la première moitié du théorème de traiter le cas d'un r-simplexe entier S, de sommets $0, s_1, \ldots, s_r$. L'ensemble mS est la réunion disjointe de ses sous-ensembles

$$S_{m,j} = \left\{\lambda_1 s_1 + \cdots + \lambda_r s_r \;\middle|\; \lambda_i \geq 0\ ,\ \sum_{i=1}^r \lambda_i \leq m\ ,\ \sum_{i=1}^r [\lambda_i] = m - j\right\}$$

pour $j \in \{0, \ldots, m\}$. Le nombre de points entiers dans $S_{m,j}$ est le nombre de solutions entières positives de l'équation $\sum_{i=1}^r x_i = m - j$, c'est-à-dire $\mathbf{C}^{r-1}_{m-j+r-1}$, fois le nombre a_j de points entiers de

$$\left\{\mu_1 s_1 + \cdots + \mu_r s_r \;\middle|\; \mu_i \in [0, 1[\ ,\ \sum_{i=1}^r \mu_i \leq j\right\}$$

Comme $a_j = a_r$ pour tout $j \geq r$, on en déduit

$$\begin{aligned}
\mathrm{Card}(mS \cap \mathbf{Z}^n) &= \sum_{j=0}^{m} a_j \, \mathbf{C}^{r-1}_{m-j+r-1} \\
&= \sum_{j=0}^{r-1} a_j \, \mathbf{C}^{r-1}_{m-j+r-1} + a_r \sum_{j=r}^{m} \mathbf{C}^{r-1}_{m-j+r-1} \\
&= \sum_{j=0}^{r-1} (a_j - a_r) \, \mathbf{C}^{r-1}_{m-j+r-1} + a_r \sum_{j=0}^{m} \mathbf{C}^{r-1}_{m-j+r-1} \\
&= \sum_{j=0}^{r-1} (a_j - a_r) \, \mathbf{C}^{r-1}_{m-j+r-1} + a_r \, \mathbf{C}^{r}_{m+r}
\end{aligned}$$

C'est donc bien un polynôme en m de degré r et de coefficient dominant $\frac{1}{r!}a_r$.

Pour tout convexe compact K dans $\mathbf{R}^n$, on a d'autre part

$$\frac{\mathrm{Card}(mK \cap \mathbf{Z}^n)}{m^n} = \mathrm{vol}\, \mathscr{C}_{\frac{1}{m}} \, \mathrm{Card}\Big(K \cap \frac{1}{m}\mathbf{Z}^n\Big)$$

où $\mathscr{C}_{\frac{1}{m}}$ est un cube de côté $\frac{1}{m}$. Lorsque m tend vers $+\infty$, cette quantité est supérieure au volume de la réunion des cubes de côté $\frac{1}{m}$ et de sommets dans $\frac{1}{m}\mathbf{Z}^n$ qui sont contenus dans K, et inférieure au volume de la réunion de ces cubes dont un sommet est dans K. On en déduit facilement que la limite est le volume (n-dimensionnel) de K.

Montrons maintenant la seconde partie du théorème, dite formule de réciprocité. Lorsque P est un r-simplexe, on vérifie directement, de façon analogue à ci-dessus, la formule $\varphi_{P'}(m) = (-1)^r \varphi_P(-m)$. Si P n'est pas un simplexe, on l'écrit comme dans la démonstration du théorème 1 comme $Q \cup R$, où Q et R sont des polytopes avec strictement moins de points entiers que P qui se rencontrent le long d'une facette commune F. On a alors

$$\begin{aligned}
\varphi_P(m) &= \varphi_Q(m) + \varphi_R(m) - \varphi_F(m) \\
\varphi_{P'}(m) &= \varphi_{Q'}(m) + \varphi_{R'}(m) + \varphi_{F'}(m)
\end{aligned}$$

En faisant une récurrence sur le nombre des points entiers du polytope, on obtient

$$\begin{aligned}
\varphi_{P'}(m) &= \varphi_{Q'}(m) + \varphi_{R'}(m) + \varphi_{F'}(m) \\
&= (-1)^r \varphi_Q(-m) + (-1)^r \varphi_R(-m) + (-1)^{r-1} \varphi_F(-m) \\
&= (-1)^r \varphi_P(-m)
\end{aligned}$$

Ceci termine la démonstration. □

5. Points entiers dans des convexes compacts assez symétriques

Compter des points entiers dans des polytopes est à l'origine une question liée à « l'approximation diophantienne » (on désigne par cette expression les techniques fines permettant entre autres d'approcher un nombre irrationnel par une suite de nombres rationnels). Cette théorie ancienne progressa tout particulièrement grâce à Minkowski à la fin du dix-neuvième siècle. Elle permet de montrer l'existence de points entiers dans des compacts convexes *symétriques* de volume assez grand et, plus généralement, de montrer l'existence de points entiers intérieurs dans des compacts convexes de volume assez grand, en fonction d'un *coefficient de symétrie* que nous définissons plus bas.

Comme on l'a déjà remarqué, un compact convexe de grand volume peut ne contenir aucun point entier. En revanche, un translaté convenable contiendra obligatoirement de nombreux tels points. C'est l'objet du résultat suivant, élémentaire mais crucial.

Théorème 5 (Blichfeldt, 1914)**.** *Soient K un compact de l'espace euclidien $\mathbf{R}^n$ et k un entier positif. Si $\mathrm{vol}(K) \geq k$, il existe des points distincts $v_0, \ldots, v_k$ de K tels que $v_i - v_j \in \mathbf{Z}^n$ pour tous i et j.*

Démonstration. Posons

$$\mathscr{C} = [0,1[^{\,n} \subset \mathbf{R}^n$$

Lorsque u décrit $\mathbf{Z}^n$, les $u + \mathscr{C}$ forment une partition de $\mathbf{R}^n$. Si on pose $K_u = \{x \in \mathscr{C} \mid u + x \in K\}$, on a donc $\mathrm{vol}(K) = \sum_{u \in \mathbf{Z}^n} \mathrm{vol}(K_u)$.

Supposons d'abord $\mathrm{vol}(K) > k$. On a

$$k < \mathrm{vol}(K) = \sum_{u \in \mathbf{Z}^n} \int_{\mathbf{R}^n} 1_{K_u} d\mu = \int_{\mathscr{C}} \sum_{u \in \mathbf{Z}^n} 1_{K_u} d\mu$$

Comme le volume de $\mathscr{C}$ est 1, il existe un point x de $\mathscr{C}$ vérifiant $\sum_{u \in \mathbf{Z}^n} 1_{K_u}(x) > k$, c'est-à-dire appartenant à au moins $k+1$ ensembles K_u. Autrement dit, il existe $u_0, \ldots, u_k$ distincts dans $\mathbf{Z}^n$ tels que $v_j = x + u_j \in K$, d'où le résultat dans ce cas.

Le cas $\mathrm{vol}(K) = k$ se traite en remplaçant K par λK, $\lambda > 1$. Il existe des points distincts $v_0(\lambda), \ldots, v_k(\lambda)$ de K tels que $v_i(\lambda) - v_j(\lambda) \in \mathbf{Z}^n$ pour tous i et j. Comme K est compact, on peut supposer que les limites $v_i = \lim_{\lambda \to 1} v_i(\lambda)$ existent et cela prouve le théorème. □

Le résultat suivant semble dû à Minkowski pour $k = 1$ (1891), et à Blichfeldt en général.

Corollaire 1. *Soit K un compact convexe de l'espace euclidien $\mathbf{R}^n$ symétrique par rapport à 0 et soit k un entier positif. Si $\mathrm{vol}(K) \geq k2^n$, il existe k paires disjointes $\pm u_j$ de points non nuls appartenant à $K \cap \mathbf{Z}^n$.*

Pour tout réel x, notons $[x]_<$ le plus grand entier strictement inférieur à x. Le corollaire peut aussi s'exprimer ainsi: si K est un compact convexe symétrique par rapport à un point entier, on peut minorer de façon effective le nombre de points entiers intérieurs à K en fonction de son volume:

$$\mathrm{Card}(\overset{\circ}{K} \cap \mathbf{Z}^n) \geq 2 \left[\frac{\mathrm{vol}(K)}{2^n} \right]_< + 1$$

(il suffit d'appliquer l'énoncé à λK, avec $k = \left[\frac{\mathrm{vol}(K)}{2^n} \right]_<$, où $\lambda \in]0,1[$ est tel que $\mathrm{vol}(\lambda K) \geq k 2^n$).