Journées mathématiques X-UPS

Année 1995

Aspects géométriques et combinatoires de la convexité

Michel BRION

Polytopes convexes entiers

Journées mathématiques X-UPS (1995), p. 23-49.
https://doi.org/10.5802/xups.1995-02

Les Éditions de l'École polytechnique
Route de Saclay
F-91128 PALAISEAU CEDEX
https://www.editions.polytechnique.fr

Centre de mathématiques Laurent Schwartz
CMLS, École polytechnique, CNRS,
Institut polytechnique de Paris
F-91128 PALAISEAU CEDEX
https://portail.polytechnique.edu/cmls/

Publication membre du
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org

Journées mathématiques X-UPS
1995, p. 23–49 doi: 10.5802/xups.1995-02

POLYTOPES CONVEXES ENTIERS

par

Michel Brion

Table des matières

Introduction

On présente quelques résultats sur les polytopes convexes entiers, c'est-à-dire les sous-ensembles d'un espace vectoriel $\mathbb{R}^d$ qui sont l'enveloppe convexe d'un nombre fini de points de $\mathbb{Z}^d$. C'est un sujet élémentaire, mais qui ne s'est développé que depuis les années soixante ; en particulier, les travaux pionniers d'E. Ehrhart, professeur de lycée à Strasbourg, y ont joué un rôle important. Ehrhart a étudié le nombre de points entiers dans un polytope convexe entier, et dans ses multiples rationnels. On redémontre une partie de ses résultats

Publication originelle dans Journées X-UPS 1995. Aspects géométriques et combinatoires de la convexité. Prépublication du Centre de mathématique de l'École polytechnique, 1995.

dans la première partie de ce texte (1.1 et 1.2) ; quelques compléments sont donnés sans démonstration en 1.3 et 1.4. La deuxième partie est consacrée à une généralisation récente (1991) de la formule sommatoire d'Euler-MacLaurin ; on y calcule la somme des valeurs d'une fonction polynomiale aux points entiers d'un polytope convexe entier. Dans la troisième partie, on expose un théorème de Betke et Kneser (1985) qui décrit toutes les « mesures finiment additives » sur les polytopes convexes entiers, qui sont invariantes par automorphismes affines entiers. Enfin, dans la quatrième partie, on fait le point sur des travaux plus récents, concernant les mesures finiment additives et invariantes par translations.

Le présent texte n'est ni détaillé (en compléter les démonstrations peut être une bonne source d'exercices), ni exhaustif. En particulier, on fait l'impasse sur les relations entre polytopes convexes entiers et géométrie algébrique ou symplectique, bien que ces relations jouent un rôle essentiel dans beaucoup de travaux récents. Pour ces liens, on renvoie entre autres à [27], [4] et [1].

1. Le polynôme d'Ehrhart d'un polytope convexe entier

1.1. On considère l'espace vectoriel réel $\mathbb{R}^d$ de dimension d, et le réseau $\mathbb{Z}^d$ dans $\mathbb{R}^d$. Un *polytope convexe* P dans $\mathbb{R}^d$ est l'enveloppe convexe d'un nombre fini de points de $\mathbb{R}^d$. On appelle *dimension* de P, et on note $\dim(P)$, la dimension de l'espace affine engendré par P. On appelle *intérieur relatif* de P, et on désigne par P^0, l'intérieur de P dans l'espace affine qu'il engendre. L'enveloppe convexe dans $\mathbb{R}^d$ d'un nombre fini de points de $\mathbb{Z}^d$ est appelée *polytope convexe entier*.

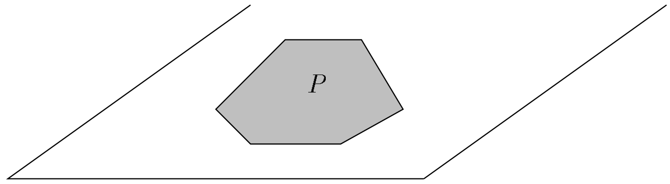

FIGURE 1.

On cherche à compter les points entiers dans P et P^0, c'est-à-dire à dénombrer les ensembles (finis) $P \cap \mathbb{Z}^d$ et $P^0 \cap \mathbb{Z}^d$. Des propriétés remarquables des nombres de points entiers dans les multiples nP et nP^0, considérés comme fonctions de l'entier positif n, ont été découvertes par E. Ehrhart ; voir [10], [9], [11]. Voici une partie de ses résultats.

Théorème. *Il existe un unique polynôme* $i_P(t)$*, de degré* $\dim(P)$*, à coefficients rationnels, tel que*

$$i_P(n) = \operatorname{card}(nP \cap \mathbb{Z}^d)$$

pour tout entier $n \geqslant 1$*. De plus, on a :* $i_P(0) = 1$ *et*

$$i_P(-n) = (-1)^{\dim(P)} \operatorname{card}(nP^0 \cap \mathbb{Z}^d)$$

pour tout entier $n \geqslant 1$ *(« loi de réciprocité »).*

1.2. Démonstration. Considérons d'abord le cas où P est un simplexe de sommets $s_0, \ldots, s_d$, c'est-à-dire : P est l'enveloppe convexe des points affinement indépendants $s_0, \ldots, s_d$. Définissons un sous-ensemble C de $\mathbb{R}^d \times \mathbb{R}$ par

$$C = \{(v, t) \mid v \in tP,\ t \geqslant 0\}.$$

Alors C est le cône convexe fermé dont les arêtes sont engendrées par les vecteurs (linéairement indépendants) $(s_0, 1), \ldots, (s_d, 1)$. De plus, pour tout $v \in \mathbb{R}^d$, on a : $v \in nP \cap \mathbb{Z}^d \Leftrightarrow (v, n) \in (\mathbb{Z}^d \times \mathbb{Z}) \cap C$. Notons Π le sous-ensemble de $\mathbb{Z}^d \times \mathbb{Z}$ formé des points qui peuvent s'écrire $\sum_{i=0}^d t_i(s_i, 1)$ avec des $t_i \in [0, 1[$. Alors les couples (m, n) tels que $m \in nP \cap \mathbb{Z}^d$ sont ceux qui peuvent s'écrire

$$(m, n) = (m_0, n_0) + \sum_{i=0}^{d} x_i(s_i, 1)$$

où $(m_0, n_0) \in \Pi$ et où les x_i sont des entiers non négatifs ; une telle décomposition est unique. Par conséquent, le nombre de points de $nP \cap \mathbb{Z}^d$ est le coefficient de z^n dans la série formelle

$$F_P(z) = \sum_{(m_0,n_0)\in\Pi} z^{n_0} \sum_{x_0,\ldots,x_d \geqslant 0} z^{x_0+\cdots+x_d}.$$

Observons que $0 \leqslant n_0 \leqslant d$ pour tout $(m_0, n_0) \in \Pi$ et que $n_0 = 0$ implique $m_0 = 0$. Par suite, il existe des entiers $\delta_0, \dots, \delta_d$ tels que

$$F_P(z) = (\delta_0 + \delta_1 z + \cdots + \delta_d z^d) \cdot (1 - z)^{-d-1}.$$

De plus, $\delta_0 = 1$. En développant la série, on en déduit que

$$\mathrm{card}(nP \cap \mathbb{Z}^d) = \delta_0 \binom{n+d}{d} + \delta_1 \binom{n+d-1}{d} + \cdots + \delta_d \binom{n}{d}$$

où $\binom{t}{d}$ désigne le polynôme $t(t-1)\cdots(t-d+1)/d!$. Ainsi, la fonction $n \mapsto \mathrm{card}(nP \cap \mathbb{Z}^d)$ est polynomiale, et la valeur en 0 de cette fonction est 1. Notons Π' le sous-ensemble de $\mathbb{Z}^d \times \mathbb{Z}$ formé des points qui peuvent s'écrire $\sum_{i=0}^d t_i(s_i, 1)$ avec des $t_i \in]0,1]$. On montre comme ci-dessus que

$$\sum_{n=1}^{\infty} \mathrm{card}(nP^0 \cap \mathbb{Z}^d)\, z^n = \sum_{(m_0,n_0)\in\Pi'} z^{n_0}(1-z)^{-d-1}.$$

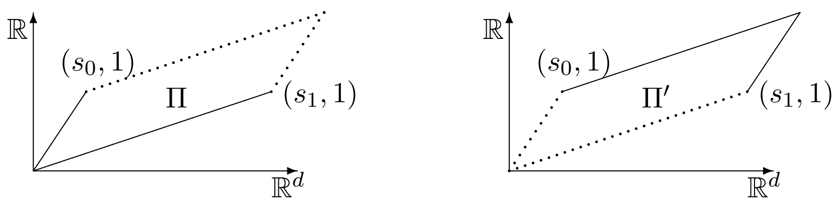

Figure 2.

Observons que Π et Π' sont échangés par la symétrie centrale qui envoie (m, n) sur $(s_0 + \cdots + s_d - m, d + 1 - n)$, d'où

$$\sum_{n=1}^{\infty} \mathrm{card}(nP^0 \cap \mathbb{Z}^d) = \sum_{(m,n)\in\Pi} z^{d+1-n}(1-z)^{-d-1}$$
$$= \sum_{i=0}^{d} \delta_i z^{d+1-i}(1-z)^{-d-1}$$

et finalement

$$\mathrm{card}(nP^0 \cap \mathbb{Z}^d) = \delta_0 \binom{n-1}{d} + \delta_1 \binom{n}{d} + \cdots + \delta_d \binom{n+d-1}{d}.$$

D'autre part, on a

$$\binom{-t}{d} = (-1)^d \binom{t+d-1}{d}$$

et ceci entraîne la loi de réciprocité pour les simplexes entiers. Considérons maintenant le cas d'un polytope entier P quelconque. Alors P peut être subdivisé par des simplexes entiers, c'est-à-dire qu'il existe une famille finie de simplexes entiers $(S_j)_{j\in J}$, telle que :

(i) si F est une face de S_j, alors $F = S_k$ pour un $k \in J$;

(ii) si $j, k \in J$, alors $S_j \cap S_k$ est une face (éventuellement vide) de S_j et de S_k ;

(iii) P est réunion disjointe des intérieurs relatifs des S_j.

On en déduit que

$$\operatorname{card}(nP \cap \mathbb{Z}^d) = \sum_{j\in J} \operatorname{card}(nS_j^\circ \cap \mathbb{Z}^d).$$

La première partie de la preuve entraîne que $\operatorname{card}(nP\cap\mathbb{Z}^d)$ est fonction polynomiale de n ; le polynôme correspondant est

$$i_P(t) = \sum_{j\in J} (-1)^{\dim(S_j)}\, i_{S_j}(-t)$$

d'après la loi de réciprocité pour les simplexes entiers. La valeur en 0 de ce polynôme est donc $\sum_{j\in J}(-1)^{\dim(S_j)} = 1$ (caractéristique d'Euler-Poincaré de P). De plus, on a :

$$(-1)^{\dim(P)}\, i_P(-t) = \sum_{j\in J} (-1)^{\operatorname{codim}(S_j)}\, i_{S_j}(t)$$

où on pose $\operatorname{codim}(S_j) = \dim(P) - \dim(S_j)$. Mais pour tout entier $n \geqslant 0$, on a :

$$\begin{aligned}\sum_{j\in J} (-1)^{\operatorname{codim}(S_j)}\, i_{S_j}(n) &= \sum_{j\in J} (-1)^{\operatorname{codim}(S_j)} \operatorname{card}(nS_j \cap \mathbb{Z}^d)\\ &= \operatorname{card}(nP^\circ \cap \mathbb{Z}^d)\end{aligned}$$

d'après l'identité d'Euler. Ceci démontre la loi de réciprocité pour P.

1.3. Les coefficients du polynôme d'Ehrhart. Avec les notations de 1.1, écrivons

$$i_P(t) = a_0(P) + a_1(P)\,t + \cdots + a_d(P)\,t^d$$

(on suppose pour simplifier que P engendre $\mathbb{R}^d$, c'est-à-dire que $\dim(P) = d$). Notons $\mathrm{vol}_d(P)$ le volume de P, normalisé de façon que les mailles du réseau $\mathbb{Z}^d$ soient de volume 1. De même, toute k-face de P a un volume bien défini $\mathrm{vol}_k(F)$; en effet, puisque l'espace affine engendré par F est rationnel, son intersection avec $\mathbb{Z}^d$ y induit un réseau, et celui-ci permet de normaliser le volume.

Proposition. *Avec les notations précédentes, on a :* $a_d(P) = \mathrm{vol}_d(P)$ *et*

$$a_{d-1}(P) = \frac{1}{2}\sum_{F\subset P} \mathrm{vol}_{d-1}(F)$$

où la somme porte sur les $(d-1)$*-faces de* P.

Démonstration. Pour n entier positif, on a :

$$i_P(n) = \mathrm{card}(nP \cap \mathbb{Z}^d) = \mathrm{card}(P \cap \tfrac{1}{n}\mathbb{Z}^d) = \sum_{m\in P\cap\frac{1}{n}\mathbb{Z}^d} 1.$$

Par suite, $n^{-d} i_P(n)$ est une somme de Riemann pour l'intégrale $\int_P dx = \mathrm{vol}_d(P)$, d'où $a_d(P) = \lim_{n\to\infty} n^{-d} i_P(n) = \mathrm{vol}_d(P)$. La seconde équation se déduit de la loi de réciprocité ; en effet, celle-ci implique

$$i_{P^\circ}(n) = a_d(P)n^d - a_{d-1}(P)n^{d-1} + \cdots$$

et ainsi

$$\lim_{n\to\infty} n^{-d+1}(i_P(n) - i_{P^\circ}(n)) = 2a_{d-1}(P).$$

D'autre part, $P \setminus P^\circ$ est réunion des $(d-1)$-faces de P, et leurs intérieurs relatifs sont deux à deux disjoints. D'où

$$\lim_{n\to\infty} n^{-d+1}(i_P(n) - i_{P^\circ}(n)) = \sum_{F\subset P} \mathrm{vol}_{d-1}(F)$$

par l'argument précédent. □

En particulier, lorsque $d = 2$, on retrouve la *formule de Pick* (voir [22]) : le nombre de points entiers dans un polygone convexe entier P est égal à l'aire de P, plus la moitié du nombre de points entiers sur le bord de P, plus 1. Cette formule est d'ailleurs valable pour les polygones entiers simplement connexes ; pour la démontrer directement, on subdivise le polygone en triangles entiers, qui ne contiennent pas d'autres points entiers que leurs sommets. On montre ensuite que pour un tel triangle ABC, les vecteurs $\vec{AB}$ et $\vec{AC}$ forment une base du réseau ; en particulier, l'aire du triangle est 1/2. En dimension 3, tout se complique. En effet, dans $\mathbb{R}^3$ muni du réseau $\mathbb{Z}^3$, considérons le tétraèdre $T(p,q)$ de sommets $(0,0,0)$, $(1,0,0)$, $(0,1,0)$, $(1,p,q)$ où p et q sont des entiers premiers entre eux tels que $0 \leqslant p < q$. Alors $T(p,q)$ ne contient pas d'autres points entiers que ses sommets ; mais $T(p,q)$ n'est pas engendré par une base de $\mathbb{Z}^3$, car il est de volume $q/6$. Tout tétraèdre entier, ne contenant pas d'autres points entiers que ses sommets, est l'image d'un $T(p,q)$ par un automorphisme affine entier ; ce résultat non trivial est dû à White, voir [28].

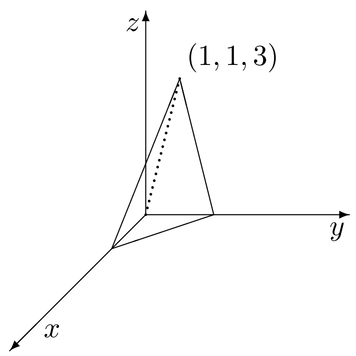

Figure 3. : $T(1,3)$

Pour un polytope convexe entier P de dimension 3, on a :

$$i_P(t) = 1 + a_1(P)\,t + \frac{1}{2}\sum_{F\subset P} \mathrm{vol}_2(F)\,t^2 + \mathrm{vol}_3(P)\,t^3$$

et le seul terme inconnu est $a_1(P)$. Contrairement au cas de la dimension 2, on ne peut exprimer ce terme en fonction des volumes des arêtes de P. En effet les faces de $T(p,q)$ sont de volume 1/2, et ses arêtes sont de volume 1. D'où

$$a_1(T(p,q)) = \mathrm{card}(T(p,q)\cap\mathbb{Z}^3) - 1 - a_2(T(p,q)) - a_3(T(p,q)) = 2 - \frac{q}{6}$$

et notre assertion. Plus généralement, en dimension d, on ne peut exprimer aucun des coefficients $a_1(P), \ldots, a_{d-2}(P)$ en fonction des termes $\sum_{F \subset P} \mathrm{vol}_k(F)$ (somme sur les faces de dimension k) ; voir [K]. Par contre, $a_k(P)$ est combinaison linéaire des volumes des k-faces de P, avec des coefficients qui ne dépendent que de la géométrie locale de P en ces faces. Plus précisément, pour toute face F, considérons le cône P_F engendré par les points $-f + p$ où $p \in P$ et $f \in F$ (voir figure 4). Alors P_F est un cône convexe polyédral rationnel (c'est-à-dire : P_F est engendré par un nombre fini de demi-droites entières). De plus, le plus grand sous-espace linéaire contenu dans P_F est la direction de la face F.

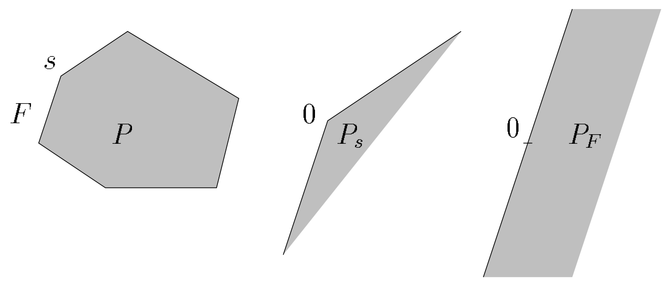

FIGURE 4.

Théorème. *On peut associer à tout cône convexe polyédral rationnel σ, un nombre rationnel $\mu(\sigma)$ tel que*

$$a_k(P) = \sum_{F \subset P} \mu(P_F)\,\mathrm{vol}_k(F)$$

où la somme porte sur les k-faces de P.

Ceci résulte de [20] ; voir aussi [4]. Par exemple, pour les faces de dimension $d-1$, on peut prendre $\mu(P_F) = 1/2$ d'après le calcul de $a_{d-1}(P)$, et c'est le seul choix possible. Pour les faces de dimension plus petite, il n'y a pas de choix unique de μ.

1.4. Le nombre de points entiers dans un tétraèdre. On va donner la valeur du coefficient $a_1(P)$ lorsque P est un tétraèdre entier dans $\mathbb{R}^3$; le résultat final est dû à J. Pommersheim (voir [23]) et il fait intervenir des expressions arithmétiques appelées « sommes de Dedekind » (voir [26]). Soit A une arête de P ; soient F_1 et F_2 les faces de P qui contiennent A. Notons $\overline{\mathbb{R}^3}$ le quotient de $\mathbb{R}^3$ par la droite affine engendrée par A, et $\overline{\mathbb{Z}^3}$ l'image de $\mathbb{Z}^3$ dans $\overline{\mathbb{R}^3}$. On peut trouver une base (e_1, e_2) du groupe abélien libre $\overline{\mathbb{R}^3}$ telle que e_1 et $\overline{F_1}$ engendrent la même demi-droite. Alors la demi-droite engendrée par $\overline{F_2}$ est engendrée par $pe_1 + qe_2$ où p, q sont des entiers premiers entre eux. De plus, on peut supposer que $1 \leqslant p < q$. Définissons la *somme de Dedekind* associée à (p, q) par

$$s(p,q) = \sum_{i=1}^{q-1} ((i/q))((pi/q))$$

où $((x)) = x - [x] - 1/2$ si x n'est pas entier, et $((x)) = 0$ sinon. Enfin, posons $m_A = q$ et $d_A = -s(p,q) + 1/4$.

Théorème. *Avec les notations précédentes, on a :*

$$a_1(P) = \sum_A \left(\frac{1}{36 m_A} \left(\frac{\mathrm{vol}_2(F_{A,1})}{\mathrm{vol}_2(F_{A,2})} + \frac{\mathrm{vol}_2(F_{A,2})}{\mathrm{vol}_2(F_{A,1})} \right) + d_A \right) \mathrm{vol}_1(A).$$

En particulier, lorsque $P \subset \mathbb{R}^3$ a pour sommets $(0,0,0)$, $(a,0,0)$, $(0,b,0)$, $(0,0,c)$ où a, b, c sont des entiers positifs, on trouve :

$$a_1(P) = \frac{1}{12}\left(\frac{ab}{c} + \frac{bc}{a} + \frac{ac}{b} + \frac{d^2}{abc}\right) + \frac{a+b+c+A+B+C}{4} - As\left(\frac{bc}{d}, \frac{aA}{d}\right) - Bs\left(\frac{ac}{d}, \frac{bB}{d}\right) - Cs\left(\frac{ab}{d}, \frac{cC}{d}\right)$$

où $A = \mathrm{pgcd}(b,c)$, $B = \mathrm{pgcd}(a,c)$, $C = \mathrm{pgcd}(a,b)$ et $d = ABC$. Dans le cas où a, b, c sont premiers entre eux deux à deux, on retrouve une formule due à Mordell, et redécouverte par Ehrhart ; voir [18], [8]. D'autre part, Kantor et Khovanskii ont redémontré les résultats de Pommersheim, dans le cadre de leur généralisation de la formule sommatoire d'Euler et MacLaurin (voir [14] et 2.3 ci-dessous). Enfin, Cappell et Shaneson ont annoncé une formule qui dénombre les points entiers dans un simplexe entier de dimension quelconque, voir [6].

2. Une généralisation de la formule sommatoire d'Euler et MacLaurin

On expose un résultat de Pukhlikov, Kantor et Khovanskii (voir [13] et [24]) qui généralise aux polytopes convexes entiers la classique *formule sommatoire d'Euler et MacLaurin* :

$$\sum_{m=a}^{b} f(m) = \int_a^b f(x)dx + \frac{f(a)+f(b)}{2} + \sum_{n=1}^{\infty}(-1)^{n-1}\frac{B_n}{(2n)!}(f^{(2n-1)}(b) - f^{(2n-1)}(a))$$

pour tout intervalle entier $[a,b]$, et pour toute fonction $f : [a,b] \to \mathbb{C}$ suffisamment régulière. Ici les B_n sont les *nombres de Bernoulli*, définis par la série génératrice

$$\frac{z}{1-\exp(-z)} = 1 + \frac{1}{2}z + \sum_{n=1}^{\infty}(-1)^{n-1}\frac{B_n}{(2n)!}z^{2n}.$$

On peut reformuler ce résultat en introduisant l'*opérateur différentiel de Todd* :

$$\mathrm{Td}(\partial/\partial h) = \frac{\partial/\partial h}{1-\exp(-\partial/\partial h)} = 1 + \frac{1}{2}\frac{\partial}{\partial h} + \sum_{n=1}^{\infty}(-1)^{n-1}\frac{B_n}{(2n)!}\frac{\partial^{2n}}{\partial h^{2n}}.$$

C'est une série formelle en l'opérateur de dérivation partielle $\partial/\partial h$. Observons que

$$\mathrm{Td}(\partial/\partial h)\int_a^{b+h} f(x)\,dx\Big|_{h=0} = \int_a^b f(x)dx + \frac{1}{2}f(b) + \sum_{n=1}^{\infty}(-1)^{n-1}\frac{B_n}{(2n)!}f^{(2n-1)}(b).$$

On a donc :

$$\sum_{m=a}^{b} f(m) = \mathrm{Td}(\partial/\partial h_1)\,\mathrm{Td}(\partial/\partial h_2)\int_{a-h_1}^{b+h_2} f(x)\,dx\Big|_{h_1=h_2=0}.$$

C'est cette version de la formule sommatoire d'Euler et MacLaurin qu'on va généraliser aux polytopes convexes entiers, en établissant au passage d'autres formules sommatoires.

2.1. On conserve les notations de 1.1, et on note

$$A = \mathbb{Z}[x_1, x_1^{-1}, \ldots, x_d, x_d^{-1}]$$

l'anneau des polynômes de Laurent en d variables, à coefficients entiers. Cet anneau est intègre ; on note K son corps des fractions. Le monôme de Laurent $x_1^{m_1} \cdots x_d^{m_d}$ sera souvent noté x^m, avec $m \in \mathbb{Z}^d$. On note M l'ensemble des « séries formelles » $\sum_{m \in \mathbb{Z}^d} a_m \, x^m$ où les a_m sont des entiers relatifs. L'ensemble M est un groupe abélien, et même un A-module : on peut multiplier une série formelle par un polynôme, mais le produit de deux séries formelles n'est pas défini en général. Une série formelle $f \in M$ est dite *sommable* s'il existe $Q \in A$ non nul, tel que la série formelle $Qf := P$ est dans A. La *somme* de f est alors $P/Q \in K$. On vérifie que la somme de f est uniquement définie, si elle existe. Par exemple, pour $m \in \mathbb{Z}^d \setminus \{0\}$ fixé, la série $\sum_{n=0}^{\infty} x^{nm}$ est sommable, et sa somme est $(1 - x^m)^{-1}$; tandis que la série $\sum_{n=-\infty}^{\infty} x^{nm}$ est sommable, de somme nulle. Revenons aux polytopes convexes entiers. Soit P un tel polytope. Pour s sommet de P, rappelons que P_s désigne le cône engendré par les $-s + p$ avec $p \in P$. C'est un cône convexe polyédral rationnel.

Théorème

(i) *Pour tout cône convexe polyédral rationnel σ, la série formelle*

$$\varphi(\sigma) := \sum_{x \in \sigma \cap \mathbb{Z}^d} x^m$$

est sommable ; notons $\Phi(\sigma)$ sa somme. De plus, $\Phi(\sigma) = 0$ si σ contient une droite.

(ii) *Pour tout polytope convexe entier P, on a dans K :*

$$\sum_{m \in P \cap \mathbb{Z}^d} x^m = \sum_s x^s \Phi(P_s)$$

(somme sur l'ensemble des sommets de P).

Démonstration

(1) On se ramène par subdivision au cas où le cône σ est engendré par d arêtes dont les directions sont linéairement indépendantes. Soient $m_1, \ldots, m_d$ les points à coordonnées entières, premières entre elles, sur ces arêtes. Soit Π le sous-ensemble de $\mathbb{Z}^d$ formé des points qui peuvent s'écrire $\sum_{i=1}^d t_i m_i$ avec des $t_i \in [0, 1[$. On vérifie, comme dans la preuve du théorème 1.1, que

$$\varphi(\sigma) \prod_{i=1}^{d} (1 - x^{m_i}) = \sum_{m \in \Pi \cap \mathbb{Z}^d} x^m.$$

Ainsi, $\varphi(\sigma)$ est sommable. Si de plus σ contient une droite, alors σ est invariant par une translation de vecteur entier $m \neq 0$, d'où $(1 - x^m)\varphi(\sigma) = 0$.

(2) Pour toute face F de P, on dispose du cône convexe P_F engendré par les $-f + p$ avec $f \in F$ et $p \in P$. Notons $\widetilde{P}_F$ le cône $f + P_F$ où f est un point arbitraire de F^0. Alors $\widetilde{P}_F$ ne dépend pas du choix de f, et on a $\varphi(\widetilde{P}_F) = x^f \varphi(P_F)$. Montrons qu'on a dans M :

$$(*) \qquad \sum_{m \in P \cap \mathbb{Z}^d} x^m = \sum_F (-1)^{\dim(F)} \Big(\sum_{m \in \widetilde{P}_F \cap \mathbb{Z}^d} x^m \Big).$$

L'énoncé en résulte, en sommant les séries et en observant que la somme de $\sum_{x \in \widetilde{P}_F \cap \mathbb{Z}^d} x^m$ est nulle si P_F contient une droite, c'est-à-dire si F n'est pas un sommet.

Soit $m \in \mathbb{Z}^d$. Vérifions que x^m apparaît avec le même coefficient dans les deux membres de $(*)$. Si $m \in P$ alors $m \in \widetilde{P}_F$ pour toute face F. De plus $1 = \sum_F (-1)^{\dim(F)}$ (identité d'Euler). D'autre part, si $m \notin P$, notons Q l'enveloppe convexe de P et de m ; notons R l'adhérence de $Q \setminus P$. Alors les faces F de P telles que $m \notin \widetilde{P}_F$ sont exactement les faces de R qui ne contiennent pas m. Mais puisque R est étoilé par rapport à m, on a : $\sum_G (-1)^{\dim(G)} = 1$ (somme sur toutes les faces G de R), et aussi $\sum_H (-1)^{\dim(H)} = 0$ (somme sur les faces H de R qui contiennent m). D'où $\sum_{m \notin \widetilde{P}_F} (-1)^{\dim(F)} = 1$ et $\sum_{m \in \widetilde{P}_F} (-1)^{\dim(F)} = 0$, ce qui termine la vérification de $(*)$. $\square$

2.2. On considère maintenant un polytope convexe entier P de dimension d, tel que tous les cônes P_s (où s décrit l'ensemble des sommets de P) ont exactement d arêtes. Un tel polytope P est appelé *simple*. Pour chaque sommet s, on note $m_1(s), \ldots, m_d(s)$ les points à coordonnées entières, premières entre elles, sur les arêtes de P_s. On pose $\Pi_s := \sum_{i=1}^d [0, 1[m_i(s)$.

Théorème. *Soit L une forme linéaire sur $\mathbb{R}^d$, à valeurs complexes, telle que $L(m_i(s)) \neq 0$ pour tout i et tout sommet s de P. Alors :*

$$(i) \qquad \sum_{m \in P \cap \mathbb{Z}^d} \exp L(m) = \sum_s \frac{\sum_{m \in \Pi_s \cap \mathbb{Z}^d} \exp L(s+m)}{\prod_{i=1}^d (1 - \exp L(m_i(s)))}$$

et de plus :

$$(ii) \qquad \int_P \exp L(x) dx = (-1)^d \sum_s \exp L(s) \frac{|\det(m_1(s), \ldots, m_d(s))|}{\prod_{i=1}^d L(m_i(s))}$$

Démonstration. D'après la preuve du théorème 2.1, on a :

$$\sum_{m \in P \cap \mathbb{Z}^d} x^m = \sum_s \frac{\sum_{m \in \Pi_s \cap \mathbb{Z}^d} x^{s+m}}{\prod_{i=1}^d (1 - x^{m_i(s)})}$$

Pour en déduire (i), on voudrait substituer $\exp L(m)$ à x^m. A cet effet, définissons un homomorphisme de groupes $\varepsilon : A \to \mathbb{C}$ par $\varepsilon(x^m) = \exp L(m)$. Alors ε est un homomorphisme d'anneaux. De plus, ε s'étend au sous-anneau de K formé des fractions ayant pour dénominateur un produit de termes $1 - x^{m_i(s)}$; en effet, on a $\varepsilon(1 - x^{m_i(s)}) = 1 - \exp L(m_i(s))$ et ce nombre n'est pas nul. L'identité (i) en résulte. Pour (ii), observons que le polytope P est entier par rapport au réseau $\frac{1}{n}\mathbb{Z}^d$ où n est un entier positif arbitraire. Appliquant (i) à ce réseau et divisant par n^d, on obtient

$$\frac{1}{n^d} \sum_{m \in P \cap \frac{1}{n}\mathbb{Z}^d} \exp L(m) = \sum_s \exp L(s) \frac{\sum_{m \in \Pi_s \cap \mathbb{Z}^d} \exp L(m/n)}{\prod_{i=1}^d n(1 - \exp L(m_i(s)/n))}$$

On en déduit (ii) par passage à la limite, en observant que

$$\mathrm{card}(\Pi_s \cap \mathbb{Z}^d) = |\det(m_1(s), \ldots, m_d(s))|. \qquad \square$$

Remarquons que l'équation (ii) est valable pour tout polytope convexe simple P, à sommets non nécessairement entiers ; un bon exercice consiste à démontrer directement cette identité. On renvoie à [3] pour une généralisation du théorème 2.2 aux polytopes convexes entiers non nécessairement simples.

2.3. On conserve les notations de 2.2, et on note $F_1, \dots, F_N$ les faces de codimension 1 de P. Chaque F_i a pour équation $f_i = 0$ où f_i est une forme affine sur $\mathbb{R}^d$, définie à un multiple près. On normalise f_i en imposant que ses coefficients soient entiers, premiers entre eux, et que $f_i(x) \geqslant 0$ pour tout $x \in P$. Pour $h = (h_1, \dots, h_N) \in \mathbb{R}^N$, on note $P(h)$ le polytope convexe défini par les inéquations $f_i(x) + h_i \geqslant 0$. Ainsi $P(h)$ est obtenu par déplacement des faces de P. On définit l'*opérateur différentiel de Todd* en N variables, par

$$\mathrm{Td}(\partial/\partial h_1, \dots, \partial/\partial h_N) = \prod_{i=1}^{N} \frac{\partial/\partial h_i}{1 - \exp(-\partial/\partial h_i)}.$$

C'est une série formelle en les opérateurs de dérivation partielle $\partial/\partial h_i$. En particulier, pour toute fonction polynomiale $f(h_1, \dots, h_N)$, l'expression

$$\mathrm{Td}(\partial/\partial h_1, \dots, \partial/\partial h_n) f(h_1, \dots, h_N) = \mathrm{Td}(\partial/\partial h) f(h)$$

a un sens.

Théorème. *Soit P un polytope convexe entier de dimension d. On suppose que chaque cône P_s (s sommet de P) est engendré par une base du réseau $\mathbb{Z}^d$; en particulier, P est simple. Alors pour toute fonction polynomiale f de degré au plus n sur $\mathbb{R}^d$, la fonction*

$$h \longrightarrow \int_{P(h)} f(x)\, dx$$

est polynomiale de degré au plus $n + d$ au voisinage de l'origine, et on a :

$$(*) \qquad \mathrm{Td}(\partial/\partial h) \int_{P(h)} f(x)\, dx \Big|_{h=0} = \sum_{m \in P \cap \mathbb{Z}^d} f(m).$$

En particulier, on a : $\mathrm{Td}(\partial/\partial h)\, \mathrm{vol}(P(h))|_{h=0} = \mathrm{card}(P \cap \mathbb{Z}^d)$. Le membre de gauche de $(*)$ dépend doublement du réseau $\mathbb{Z}^d$: par la normalisation de l'élément de volume, et par les normalisations des inéquations des faces, qui servent à définir $P(h)$.

Démonstration. On utilise les notations de 2.2. On vérifie d'abord que toute fonction polynomiale homogène de degré n est combinaison linéaire à coefficients constants de fonctions de la forme $x \to L(x)^n$ où L est une forme linéaire sur $\mathbb{R}^d$, telle que $L(m_i(s)) \neq 0$ pour tous s et i. On peut donc supposer que $f(x) = L(x)^n$; alors $\int_{P(h)} f(x)\,dx$ est le terme homogène de degré n dans le développement en série de $n! \int_{P(h)} \exp L(x)\,dx$ comme fonction de L. Appliquons l'identité (ii) du théorème 2.2 au polytope convexe $P(h)$ pour h assez petit. Les sommets de $P(h)$ sont alors

$$s(h) = s - \sum_{i=1}^{d} h_{j(s,i)} m_i(s)$$

où $j(s,i)$ est l'indice de la face F_j de P qui contient s, mais qui ne contient pas l'arête de P issue de s et de direction $m_i(s)$. De plus, chaque cône $P(h)_{s(h)}$ s'identifie à P_s.

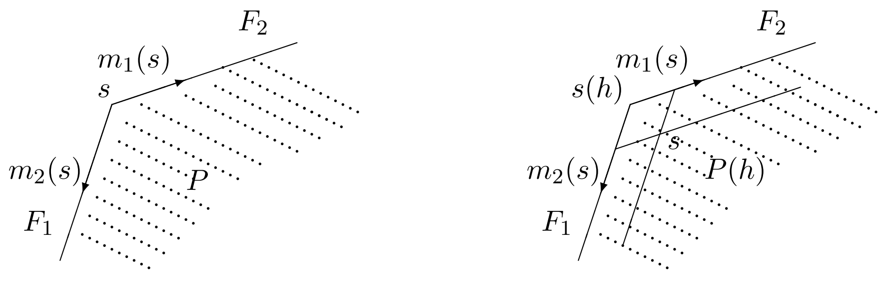

FIGURE 5.

On a donc

$$\int_{P(h)} \exp L(x)\,dx = (-1)^d \sum_s \frac{\exp(L(s) - \sum_{i=1}^d h_{j(s,i)} L(m_i(s)))}{\prod_{i=1}^d L(m_i(s))}.$$

En développant en série par rapport à L, on en déduit la première assertion du théorème. De plus, pour vérifier $(*)$, il suffit de montrer que

$$(-1)^d \sum_s \mathrm{Td}(\partial/\partial h) \frac{\exp(L(s) - \sum_{i=1}^d h_{j(i,s)} L(m_i(s)))}{\prod_{i=1}^d L(m_i(s))}\Big|_{h=0}$$
$$= \sum_{m \in P \cap \mathbb{Z}^d} \exp L(m)$$

Mais d'après le théorème 2.2 (i), le second membre est égal à

$$\sum_s \frac{\exp L(s)}{\prod_{i=1}^d (1 - \exp L(m_i(s)))}$$

Enfin, observons qu'on a pour tout $t \in \mathbb{C}$:

$$\mathrm{Td}(\partial/\partial h) \exp(th)|_{h=0} = \frac{t}{1 - \exp(-t)}.$$

En effet, la dérivation par rapport à h multiplie $\exp(th)$ par t. On en déduit que

$$\mathrm{Td}(\partial/\partial h) \exp\Big(L(s) - \sum_{i=1}^d h_{j(s,i)} L(m_i(s))\Big)\Big|_{h=0}$$
$$= \exp L(s) \cdot \prod_{i=1}^d \frac{-L(m_i(s))}{1 - \exp L(m_i(s))}.$$

Ceci permet de terminer la vérification de $(*)$. □

On trouvera dans [13] et [24], des énoncés analogues, pour les fonctions produit d'un polynôme par l'exponentielle d'une forme linéaire. Lorsqu'on essaie de généraliser le théorème dans une autre direction, en affaiblissant les hypothèses sur les cônes P_s, la situation est beaucoup moins claire ; on renvoie à [14] pour des résultats partiels, qui permettent cependant de retrouver la formule de Pommersheim énoncée en 1.4.

3. Polynôme d'Ehrhart et mesures invariantes des polytopes entiers

On expose un résultat de Betke et Kneser qui caractérise le polynôme d'Ehrhart, voir [2].

3.1. On conserve les notations de 1.1, et on note $\mathcal{P}(\mathbb{Z}^d)$ l'ensemble des polytopes convexes entiers. Une *mesure (finiment additive)* sur $\mathcal{P}(\mathbb{Z}^d)$, à valeurs dans un groupe abélien Γ, est une application

$$\mu : \mathcal{P}(\mathbb{Z}^d) \longrightarrow \Gamma$$

qui vérifie le « principe d'inclusion et d'exclusion » : chaque fois que $P \in \mathcal{P}(\mathbb{Z}^d)$ est réunion de $P_1, \ldots, P_n \in \mathcal{P}(\mathbb{Z}^d)$, on a

$$\mu(P) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} (-1)^k \mu(P_{i_1} \cap \cdots \cap P_{i_k})$$

Par exemple, le volume est une mesure à valeurs dans $(1/d!)\mathbb{Z}$. L'application qui à P associe son polynôme d'Ehrhart i_P est aussi une mesure : en effet le principe d'inclusion et d'exclusion est vérifié pour tous les $i_P(n) = \operatorname{card}(nP \cap \mathbb{Z}^d)$ où $n \in \mathbb{N}$, et donc pour $i_P(t)$. Notons $\operatorname{Aut}(\mathbb{Z}^d)$ le groupe des transformations affines bijectives de $\mathbb{R}^d$ qui préservent $\mathbb{Z}^d$; ce groupe opère dans l'ensemble $\mathcal{P}(\mathbb{Z}^d)$. Observons que P et $g(P)$ ont le même nombre de points entiers, pour tout $g \in \operatorname{Aut}(\mathbb{Z}^d)$; d'où $i_{g(P)}(t) = i_P(t)$. Ainsi, *le polynôme d'Ehrhart est une mesure invariante par* $\operatorname{Aut}(\mathbb{Z}^d)$. Réciproquement, on a le

Théorème. *Soit $\mu : \mathcal{P}(\mathbb{Z}^d) \to \Gamma$ une mesure invariante par $\operatorname{Aut}(\mathbb{Z}^d)$. Alors μ est fonction linéaire des valeurs du polynôme d'Ehrahrt en $0, 1, \ldots, d$, c'est-à-dire : il existe $\gamma_0, \ldots, \gamma_d \in \Gamma$ tels que*

$$\mu(P) = \sum_{k=0}^{d} \gamma_k \, i_P(k).$$

Dans cet énoncé, on peut remplacer les valeurs en $0, 1, \ldots, d$ par les valeurs en $n, n+1, \ldots, n+d$ où n est un entier arbitraire. En effet, le polynôme d'Ehrhart appartient à l'ensemble des fonctions polynomiales de degré au plus d, qui prennent des valeurs entières en tous les entiers ; notons E_d cet ensemble. Pour $0 \leqslant k \leqslant d$, la fonction

$$\binom{t}{k} = \frac{t(t-1)\cdots(t-k+1)}{k!}$$

est dans E_d, et ces fonctions forment une base du groupe abélien E_d (exercice). Il en est de même des fonctions $\binom{t+n}{k}$ pour $0 \leqslant k \leqslant d$:

ainsi, les valeurs en $n, n+1, \ldots, n+d$ de tout $f \in E_d$ sont combinaisons linéaires entières des valeurs en $0, 1, \ldots, d$.

3.2. Démonstration. On commence par construire un groupe abélien $\mathcal{B}K(\mathbb{Z}^d)$ et une application

$$\begin{aligned} \mathcal{P}(\mathbb{Z}^d) &\longrightarrow \mathcal{B}K(\mathbb{Z}^d) \\ P &\longmapsto [P] \end{aligned}$$

qui vérifient la propriété universelle suivante : pour toute mesure μ, à valeurs dans Γ et invariante par $\mathrm{Aut}(\mathbb{Z}^d)$, il existe un unique homomorphisme de groupes $\widetilde{\mu} : \mathcal{B}K(\mathbb{Z}^d) \to \Gamma$ tel que $\widetilde{\mu}([P]) = [P]$ pour tout $P \in \mathcal{P}(\mathbb{Z}^d)$. Autrement dit, l'application de $\mathcal{P}(\mathbb{Z}^d)$ vers $\mathcal{B}K(\mathbb{Z}^d)$ est la mesure invariante par $\mathrm{Aut}(\mathbb{Z}^d)$ et universelle. A cet effet, on définit $\mathcal{B}K(\mathbb{Z}^d)$ comme le groupe abélien qui a pour générateurs les éléments de $\mathcal{P}(\mathbb{Z}^d)$, et pour relations :

$$P - \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} P_{i_1} \cap \cdots \cap P_{i_k}$$

pour tout P qui est réunion de $P_1, \ldots, P_n$, et

$$P - g(P)$$

pour tous $P \in \mathcal{P}(\mathbb{Z}^d)$ et $g \in \mathrm{Aut}(\mathbb{Z}^d)$. On note $[P]$ l'image du générateur P dans $\mathcal{B}K(\mathbb{Z}^d)$; il est clair que l'application ainsi définie est la mesure universelle. Pour $0 \leqslant k \leqslant d$, appelons *$k$-simplexe standard* tout simplexe entier de dimension k et de volume k-dimensionnel $(1/k!)$. Les k-simplexes standard sont les images par $\mathrm{Aut}(\mathbb{Z}^d)$ du simplexe S_k dont les sommets sont l'origine et les k premiers vecteurs d'une base de $\mathbb{Z}^d$. Le polynôme d'Ehrhart d'un tel k-simplexe est :

$$\binom{t+k}{k} = \frac{(t+1)(t+2)\cdots(t+k)}{k!}.$$

En dimension au moins trois, il existe des polytopes convexes entiers qui n'admettent aucune subdivision par des simplexes standard (par exemple, les tétraèdres $T(p,q)$ définis en 1.3). Cependant, on peut trouver de telles subdivisions si on s'autorise à faire des différences de polytopes. Plus précisément, on va montrer le résultat suivant.

Proposition. *Le groupe $\mathcal{B}K(\mathbb{Z}^d)$ est engendré par les k-simplexes standard.*

Le théorème en résulte ; en effet, soit P un polytope convexe entier. La proposition implique l'existence d'entiers $x_0(P),\ldots,x_d(P)$ tels qu'on ait dans $\mathcal{B}K(\mathbb{Z}^d)$:

$$[P]=\sum_{k=0}^{d} x_k(P)[\Delta_k].$$

Il en résulte d'une part que

$$\mu(P)=\sum_{k=0}^{d} x_k(P)\mu(\Delta_k)$$

et d'autre part que

$$i_P(t)=\sum_{k=0}^{d} x_k(P)\binom{t+k}{k}.$$

Cette dernière équation permet d'exprimer les $x_k(P)$ comme combinaisons linéaires entières de $i_P(0),\ldots,i_P(d)$. Pour démontrer la proposition, observons que le groupe $\mathcal{B}K(\mathbb{Z}^d)$ est engendré par les images des simplexes entiers ; en effet, tout polytope convexe entier P admet une subdivision par des simplexes entiers $(S_j)_{j\in J}$ comme en 1.2 ; alors on a dans $\mathcal{B}K(\mathbb{Z}^d)$:

$$[P]=\sum_{j\in J}(-1)^{\operatorname{codim}(S_j)}\,[S_j].$$

De plus, par récurrence sur la dimension, on peut supposer que l'image dans $\mathcal{B}K(\mathbb{Z}^d)$ de tout simplexe entier de dimension $\leqslant d-1$ est dans le sous-groupe engendré par les $[\Delta_k]$, $0\leqslant k\leqslant d-1$. Soit S un simplexe entier de dimension d de sommets $x_0,\ldots,x_d$; alors $d!\operatorname{vol}(S):=V(S)$ est un entier positif. Si $V(S)=1$, alors S est standard, et c'est terminé. On va montrer par récurrence sur $V(S)$ que $[S]-V(S)[\Delta_d]$ appartient au sous-groupe engendré par les $[\Delta_k]$, $0\leqslant k\leqslant d-1$. Notons $F_0,\ldots,F_d$ les $(d-1)$-faces de S. Soit $p\in\mathbb{Z}^d$; soient $F_{i_1},\ldots,F_{i_l}$ les faces dont l'hyperplan sépare strictement p et S ; soient $F_{j_1},\ldots,F_{j_m}$ les autres faces. Alors le polyèdre convexe $\operatorname{conv}(p,S)$ engendré par p et S admet deux subdivisions en simplexes entiers : l'une par S et les $\operatorname{conv}(p,F_{i_\alpha})$, et l'autre par les $\operatorname{conv}(p,F_{j_\beta})$.

Pour terminer la démonstration, il suffit donc de trouver $p\in\mathbb{Z}^d$ tel que

$$V(\operatorname{conv}(p,F_i))<V(S)$$

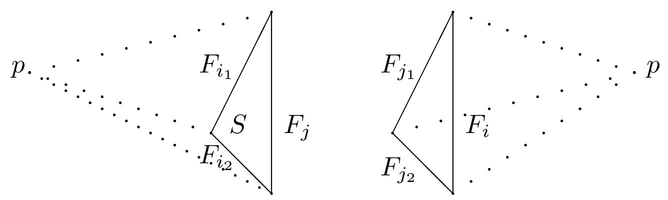

FIGURE 6.

pour $0 \leqslant i \leqslant d$; autrement dit, que p est plus proche de chaque F_i que le sommet de S qui n'est pas dans F_i. On va expliciter un tel point p. On peut supposer que les seuls points entiers de S sont ses sommets ; alors les vecteurs $x_1 - x_0, \dots, x_d - x_0$ sont indivisibles dans $\mathbb{Z}^d$. Soit s le plus grand entier tel que $(x_1-x_0, \dots, x_s-x_0)$ peut être complété en une base de $\mathbb{Z}^d$. Quitte à remplacer S par $g(S)$ pour un $g \in \mathrm{Aut}(\mathbb{Z}^d)$, on peut supposer que $x_0 = 0$, $x_1 = e_1, \dots, x_s = e_s$. Alors $x_{s+1} = a_1e_1 + \cdots + a_de_d$ avec $\mathrm{pgcd}(a_{s+1}, \dots, a_d) > 1$ par maximalité de s. On peut supposer que $a_{s+2} = \cdots = a_d = 0$, puis que

$$0 \leqslant a_1 \leqslant a_2 \leqslant \cdots \leqslant a_{s-1} < a_s$$

et $a_s > 1$. Soit r le plus grand entier tel que

$$r < 1 + a_s^{-1}(a_1 + \cdots + a_{s-1} - 1),$$

alors $r < s$. Soit p le point de coordonnées 0 ($s-r-1$ fois), 1 ($r+1$ fois), 0 ($d - s$ fois). Vérifions que p convient. Pour $0 \leqslant i \leqslant d$, notons F_i la $(d-1)$-face de S qui ne contient pas le sommet x_i. Notons f_i l'unique forme affine sur $\mathbb{R}^d$ qui vaut 0 sur F_i et 1 en x_i. Les valeurs des f_i sont :

$$\begin{aligned}
f_0 &= x_1 + \cdots + x_{s-1} + a_s^{-1}(1 - a_1 - \cdots - a_{s-1})x_s \\
&\qquad\qquad\qquad\qquad + g_0(x_{s+1}, \dots, x_d) - 1, \\
f_i &= x_i - a_ia_s^{-1}x_s + g_i(x_{s+1}, \dots, x_d) \quad (1 \leqslant i \leqslant s-1), \\
f_s &= a_s^{-1}x_s + g_s(x_{s+1}, \dots, x_d), \\
f_j &= g_j(x_{s+1}, \dots, x_d) \quad (s+1 \leqslant j \leqslant d).
\end{aligned}$$

Il faut vérifier que $|f_i(p)| < 1$ pour $0 \leqslant i \leqslant d$. Observons d'abord que$p$ est dans l'hyperplan engendré par F_i, pour tout $i \geqslant s+1$. D'autre part, on a :

$$f_0(p) = r + a_s^{-1}(1 - a_1 - \cdots - a_{s-1})$$

d'où $0 \leqslant f_0(p) < 1$. On a aussi : $f_s(p) = a_s^{-1} \in [0,1[$ et pour $1 \leqslant i \leqslant s-r-1$, on a : $f_i(p) = -a_s^{-1} a_i \in]-1,0]$. Enfin, pour $s-r \leqslant i \leqslant s-1$, on a : $f_i(p) = 1 - a_s^{-1} a_i$, d'où $f_i(p) \in [0,1]$. Si de plus $f_i(p) = 1$, alors $a_i = 0$, d'où $a_1 = \cdots = a_{i-1} = 0$ et

$$r < 1 + a_s^{-1}(a_{i+1} + \cdots + a_{s-1} - 1) < 1 + (s - 1 - i)$$

et $i < s - r$, contradiction.

Remarque. La démonstration ci-dessus redonne l'existence du polynôme d'Ehrhart, en n'utilisant que son calcul (facile) pour les simplexes standard.

4. L'anneau des polytopes entiers

On expose une partie des résultats de McMullen, Morelli, Kantor, Pukhlikov et Khovanskii sur l'anneau des polytopes et son analogue entier, ainsi que leurs applications aux mesures (ou valuations) invariantes par translations. Des constructions universelles analogues à celle du groupe $\mathcal{B}K(\mathbb{Z}^d)$ de 3.2, joueront un grand rôle dans cette dernière partie.

4.1. Mesures et valuations sur les polytopes. On note $\mathcal{P}(\mathbb{R}^d)$ l'ensemble des polytopes convexes de $\mathbb{R}^d$. Comme en 3.1, on a la notion de *mesure* (finiment additive) sur $\mathcal{P}(\mathbb{R}^d)$, à valeurs dans un groupe abélien Γ. Une notion apparemment plus faible est celle de *valuation* : il s'agit d'une application $\mu : \mathcal{P}(\mathbb{R}^d) \to \Gamma$ telle que

$$\mu(P \cup Q) = \mu(P) + \mu(Q) - \mu(P \cap Q)$$

pour tous P et Q dans $\mathcal{P}(\mathbb{R}^d)$ tels que $P \cup Q$ est aussi dans $\mathcal{P}(\mathbb{R}^d)$. En fait, ces deux notions coïncident, comme le montre le résultat suivant.

Proposition. *Soit* $\mu : \mathcal{P}(\mathbb{R}^d) \to \Gamma$ *une application qui vérifie*

$$\mu(P) = \mu(P \cap H^+) + \mu(P \cap H^-) - \mu(P \cap H)$$

pour tout $P \in \mathcal{P}(\mathbb{R}^d)$ et pour tout hyperplan H de $\mathbb{R}^d$, délimitant deux demi-espaces fermés H^+ et H^-. Alors μ est une mesure.

Démonstration. Notons $\mathcal{E}(\mathbb{R}^d)$ le groupe abélien ayant pour générateurs les éléments de $\mathcal{P}(\mathbb{R}^d)$ et pour relations

$$[P] - [P \cap H^+] - [P \cap H^-] + [P \cap H]$$

où P et H sont comme ci-dessus, et où $[P]$ désigne l'image de P dans $\mathcal{E}(\mathbb{Z}^d)$. D'autre part, associons à tout polytope convexe P sa fonction caractéristique $\mathbf{1}_P : \mathbb{R}^d \to \{0,1\}$; notons $L(\mathbb{R}^d)$ le sous-groupe du groupe additif des applications de $\mathbb{R}^d$ dans $\mathbb{Z}$, engendré par les fonctions caractéristiques des polytopes convexes. La relation évidente

$$\mathbf{1}_P = \mathbf{1}_{P\cap H^+} + \mathbf{1}_{P\cap H^-} - \mathbf{1}_{P\cap H}$$

permet de définir l'homomorphisme de groupes

$$\varphi : \mathcal{E}(\mathbb{R}^d) \longrightarrow L(\mathbb{R}^d),\ [P] \longrightarrow \mathbf{1}_P.$$

L'énoncé de la proposition équivaut à l'injectivité de φ. Pour la vérifier, considérons $x = \sum[P_i] - \sum[Q_j] \in \mathcal{E}(\mathbb{R}^d)$ tel que $\varphi(x) = 0$. Écrivons les P_i et les Q_j comme intersections finies de demi-espaces ; d'où une famille (finie) d'hyperplans (H_α). Le complémentaire de la réunion de ces hyperplans n'a qu'un nombre fini de composantes connexes, et chacune de ces composantes n'a qu'un nombre fini de faces bornées ; soit (R_β) la famille finie des adhérences de ces faces. Les relations

$$[P] = [P \cap H_\alpha^+] + [P \cap H_\alpha^-] - [P \cap H_\alpha]$$

permettent d'écrire les P_i et Q_j comme combinaisons entières des R_β. Par suite, on a $x = \sum_\beta a_\beta[R_\beta]$ avec des a_β entiers. Choisissons un R_γ dont la dimension est maximale parmi les dimensions des R_β figurant dans x. En évaluant $\varphi(x)$ en un point de l'intérieur relatif de R_β, on obtient $a_\beta = 0$. On conclut par une récurrence immédiate. $\square$

4.2. L'anneau des polytopes (voir [15], [16]**).** Il existe une mesure (ou valuation) universelle sur $\mathcal{P}(\mathbb{R}^d)$, donnée par la construction suivante. Notons $\widetilde{\Pi}(\mathbb{R}^d)$ le groupe abélien ayant pour générateurs les éléments de $\mathcal{P}(\mathbb{R}^d)$, et pour relations

$$[P \cup Q] - [P] - [Q] + [P \cap Q]$$

chaque fois que P, Q et $P \cup Q$ sont dans $\mathcal{P}(\mathbb{R}^d)$. Alors *l'application canonique*

$$\mathcal{P}(\mathbb{R}^d) \longrightarrow \widetilde{\Pi}(\mathbb{R}^d),\ P \longrightarrow [P]$$

est la valuation universelle. On s'intéresse plus particulièrement aux valuations invariantes par un groupe de transformations affines, le plus simple étant le groupe des translations. En désignant par $\Pi(\mathbb{R}^d)$ le quotient de $\widetilde{\Pi}(\mathbb{R}^d)$ par les relations

$$[v + P] - [P] \quad (v \in \mathbb{R}^d,\ P \in \mathcal{P}(\mathbb{R}^d)),$$

l'application canonique de $\mathcal{P}(\mathbb{R}^d)$ dans $\Pi(\mathbb{R}^d)$ est la valuation invariante par translations, universelle. Rappelons que la *somme de Minkowski* de deux polytopes convexes P et Q est définie par

$$P + Q = \{p + q \mid p \in P, q \in Q\};$$

c'est un polytope convexe. Du lemme ci-dessous résulte que la formule

$$[P][Q] = [P + Q]$$

définit une structure d'anneau sur $\widetilde{\Pi}(\mathbb{R}^d)$ et $\Pi(\mathbb{R}^d)$. Ce dernier est appelé *l'anneau des polytopes.*

Lemme. *Soient P, Q, $R \in \mathcal{P}(\mathbb{R}^d)$. Alors*

$$(P \cup Q) + R = (P + R) \cup (Q + R).$$

Si de plus $P \cup Q \in \mathcal{P}(\mathbb{R}^d)$, alors

$$(P \cap Q) + R = (P + R) \cap (Q + R).$$

Démonstration. La première assertion est évidente, ainsi que l'inclusion de $(P \cap Q) + R$ dans $(P + R) \cap (Q + R)$. Pour l'inclusion opposée, soient $p \in P$, $q \in Q$ et $r_1, r_2 \in R$ tels que $p + r_1 = q + r_2 := x$. Puisque $P \cup Q$ est convexe, le segment $[p, q]$ rencontre $P \cap Q$. Soit $t \in [0, 1]$ tel que $tp + (1 - t)q \in P \cap Q$. Alors $x = tp + (1 - t)q + tr_1 + (1 - t)r_2$ est dans $(P \cap Q) + R$.

Pour tout entier $k \geqslant 0$, notons $F_k\mathbb{Z}\mathcal{P}(\mathbb{R}^d)$ le sous-groupe de $\mathbb{Z}\mathcal{P}(\mathbb{R}^d)$ engendré par les polytopes de dimension au plus k. On définit ainsi des filtrations croissantes des anneaux $\widetilde{\Pi}(\mathbb{R}^d)$ et $\Pi(\mathbb{R}^d)$. La proposition 4.1 entraîne que le groupe $\Pi(\mathbb{R}^d)/F_{d-1}\Pi(\mathbb{R}^d)$ a pour générateurs les polytopes de dimension d, et pour relations : $[P \cup Q] - [P] - [Q]$ avec P, Q polytopes de dimension d, tels que $P \cup Q$ est convexe et que $P \cap Q$ est contenu dans un hyperplan. Ce groupe joue un rôle essentiel dans les problèmes de décomposition des polyèdres, voir [7]. L'application deg : $\mathbb{Z}\mathcal{P} \to \mathbb{Z}$ définie par $\deg(\sum n_P P) = \sum n_P$ est nulle sur les relations de $\widetilde{\Pi}(\mathbb{R}^d)$ et $\Pi(\mathbb{R}^d)$. On peut donc définir des degrés sur $\widetilde{\Pi}(\mathbb{R}^d)$ et $\Pi(\mathbb{R}^d)$; ce sont des homomorphismes d'anneaux. Pour tout $P \in \mathcal{P}(\mathbb{R}^d)$, on pose

$$[P]^* = \sum_{F \subset P} (-1)^{\dim(F)}[F]$$

c'est-à-dire : $[P]^* = (-1)^{\dim(P)}[P^0]$ grâce à l'identité (équivalente à la relation d'Euler) :

$$\mathbf{1}_{P^0} = \sum_{F \subset P} (-1)^{\operatorname{codim}(F)} \mathbf{1}_F.$$

On vérifie que * est un automorphisme involutif de $\widetilde{\Pi}(\mathbb{R}^d)$ et de $\Pi(\mathbb{R}^d)$. Pour $\lambda \in \mathbb{R}$ non nul, on définit l'homothétie de rapport λ, notée $\lambda\cdot$, par :

$$\lambda \cdot [P] = \begin{cases} [\lambda P] & \text{si } \lambda > 0, \\ [-\lambda P]^* & \text{si } \lambda < 0. \end{cases}$$

On obtient ainsi un automorphisme de $\widetilde{\Pi}(\mathbb{R}^d)$ et de $\Pi(\mathbb{R}^d)$; on pose : $0 \cdot P = \deg(P)$. □

On doit à MacMullen des résultats très profonds sur la structure de l'anneau $\Pi(\mathbb{R}^d)$. On va énoncer une version abstraite d'une partie de ces résultats ; des corollaires plus concrets seront donnés ensuite.

Théorème. *Il existe une unique décomposition*

$$\Pi(\mathbb{R}^d) = \bigoplus_{k=0}^{d} \Pi_k$$

du groupe abélien $\Pi(\mathbb{R}^d)$ *telle que :*

(i) $\Pi_0 = \mathbb{Z}$ *et* $\Pi_{\geqslant 1} = \Pi_1 \oplus \cdots \oplus \Pi_d$ *est le noyau de* deg.

(ii) *Pour* $1 \leqslant k \leqslant d$*, le sous-groupe* Π_k *a une structure d'espace vectoriel réel, telle que pour tout* $\lambda \in \mathbb{R}$ *et pour tout* $x \in \Pi_k$*, on a :* $\lambda \cdot x = \lambda^k x$*.*

(iii) *L'espace vectoriel réel* Π_d *est de dimension* 1*.*

En fait, un isomorphisme de Π_d sur $\mathbb{R}$ est donné par le volume. Ceci équivaut à un résultat classique de Hadwiger : *toute mesure sur* $\mathcal{P}(\mathbb{R}^d)$*, invariante par translations, et homogène de degré d, est un multiple constant du volume* (voir [12]). Observons d'autre part que l'énoncé (ii), joint au fait que l'homothétie de rapport λ est un automorphisme de $\Pi(\mathbb{R}^d)$, entraîne que $\Pi_k \, \Pi_\ell \subset \Pi_{k+\ell}$ pour tous $k, \ell \in [1, d]$. Autrement dit, $\Pi_{\geqslant 1}$ *est une* $\mathbb{R}$*-algèbre graduée.* Les démonstrations de McMullen sont élémentaires mais astucieuses ; on renvoie à [5] pour une approche plus algébrique, et une généralisation du théorème de Hadwiger.

4.3. L'anneau des polytopes entiers (voir [19]**,** [21]**,** [25]**).** Comme en 4.1, on définit $\widetilde{\Pi}(\mathbb{Z}^d)$ et son quotient $\Pi(\mathbb{Z}^d)$ par le sous-groupe engendré par les $[m + P] - [P]$ où $m \in \mathbb{Z}^d$ et $P \in \mathcal{P}(\mathbb{Z}^d)$. Les groupes abéliens $\widetilde{\Pi}(\mathbb{Z}^d)$ et $\Pi(\mathbb{Z}^d)$ ont une structure d'anneau, muni d'une involution $*$. On note $L(\mathbb{Z}^d)$ le sous-groupe de $L(\mathbb{R}^d)$ engendré par les fonctions caractéristiques des éléments de $\mathcal{P}(\mathbb{Z}^d)$. L'application naturelle de $\widetilde{\Pi}(\mathbb{Z}^d)$ vers $L(\mathbb{Z}^d)$ est un isomorphisme. *Autrement dit, les notions de mesure et de valuation coïncident pour les polytopes convexes entiers.* Ce résultat, bien plus difficile que son analogue non entier (proposition 4.1) est démontré par Morelli, voir [19]. Comme ci-dessus, l'homothétie de rapport n définit un endomorphisme $n\cdot$ de $\widetilde{\Pi}(\mathbb{Z}^d)$ et de $\Pi(\mathbb{Z}^d)$, pour tout entier $n \neq 0$. Les résultats de MacMullen s'étendent alors, pourvu que l'on remplace $\Pi(\mathbb{Z}^d)$ par son produit tensoriel avec $\mathbb{Q}$; de plus, l'application naturelle de $\Pi(\mathbb{Z}^d)$ dans $\Pi(\mathbb{R}^d)$ est injective, voir [19]. Voici un corollaire plus concret de ces résultats. Soit μ une valuation sur les polytopes convexes entiers, et invariante par translations par $\mathbb{Z}^d$; soit $P \in \mathcal{P}(\mathbb{Z}^d)$. Alors *l'application* $\mu_P : \mathbb{Z} \to \Gamma$ *définie par*

$$\mu_P(n) = \begin{cases} \mu(nP) & si\ n \geqslant 0, \\ (-1)^{\dim(P)} \mu(-nP^0) & si\ n < 0 \end{cases}$$

est polynomiale de degré au plus d (voir [17]). En effet, une valuation invariante par translations, et à valeurs dans Γ, n'est autre qu'un homomorphisme du groupe $\Pi(\mathbb{Z}^d)$ vers Γ, et de plus $\mu_P(n) = \mu(n \cdot [P])$. Un exemple de telle valuation est donné par : $\mu(P) = \mathrm{card}(P \cap \mathbb{Z}^d)$; on retrouve ainsi les résultats d'Ehrhart.

Références

[1] M. Audin – *The topology of torus actions on symplectic manifolds*, Progress in Math., vol. 93, Birkhäuser Verlag, Basel, 1991.

[2] U. Betke & M. Kneser – « Zerlegungen und Bewertungen von Gitterpolytopen », *J. reine angew. Math.* **358** (1985), p. 202–208.

[3] M. Brion – « Polyèdres et réseaux », *Enseign. Math.* **38** (1992), p. 71–88.

[4] ______, « Points entiers dans les polytopes convexes », in *Séminaire Bourbaki, Vol. 1993/94*, Astérisque, vol. 227, Société Mathématique de France, Paris, 1995, Exp. no. 780, p. 145–169.

[5] ______, « Piecewise polynomial functions, convex polytopes and enumerative geometry », in *Parameter spaces (Warsaw, 1994)*, Banach Center Publ., vol. 36, Polish Acad. Sci. Inst. Math., Warsaw, 1996, p. 25–44.

[6] S. E. Cappell & J. L. Shaneson – « Genera of algebraic varieties and counting of lattice points », *Bull. Amer. Math. Soc.* **30** (1994), p. 62–69.

[7] P. Cartier – « Décomposition des polyèdres : le point sur le troisième problème de Hilbert », in *Séminaire Bourbaki, Vol. 1984/85*, Astérisque, vol. 133-134, Société Mathématique de France, Paris, 1986, Exp. no. 646, p. 261–288.

[8] E. Ehrhart – « Nombre de points entiers d'un tétraèdre », *C. R. Acad. Sci. Paris Sér. I Math.* **258** (1964), p. 3945–3948.

[9] ______, « Démonstration de la loi de réciprocité pour le polyèdre convexe entier », *C. R. Acad. Sci. Paris Sér. I Math.* **265** (1967), p. 5–7.

[10] ______, « Sur un problème de géométrie diophantienne linéaire I. Polyèdres et réseaux », *J. reine angew. Math.* **226** (1967), p. 1–29.

[11] ______, *Polynômes arithmétiques et méthode des polyèdres en combinatoire*, International Series of Numerical Mathematics, vol. 35, Birkhäuser Verlag, Basel-Stuttgart, 1977.

[12] H. Hadwiger – *Vorlesungen über Inhalt, Oberfläche und Isoperimetrie*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1957.

[13] J.-M. Kantor & A. V. Khovanskii – « Integral points in convex polyhedra, combinatorial Riemann-Roch theorem and generalized Euler-MacLaurin formula », prépublication de l'I.H.E.S., 1992.

[14] ______, « Une application du théorème de Riemann-Roch combinatoire au polynôme d'Ehrhart des polytopes entiers de $\mathbb{R}^d$ », *C. R. Acad. Sci. Paris Sér. I Math.* **317** (1993), p. 501–507.

[15] P. McMullen – « The polytope algebra », *Adv. in Math.* **78** (1989), p. 76–130.

[16] ______, « Valuations and dissections », in *Handbook of convex geometry*, vol. B, North-Holland, 1993, p. 933–988.

[17] P. McMullen & R. Schneider – « Valuations on convex bodies », in *Convexity and its applications*, Birkhäuser, Basel, 1983, p. 170–247.

[18] L. J. Mordell – « Lattice points in a tetrahedron and generalized Dedekind sums », *J. Indian Math. Soc.* **15** (1951), p. 41–46.

[19] R. Morelli – « A theory of polyhedra », *Adv. in Math.* **97** (1993), p. 1–73.

[20] ———, « The Todd class of a toric variety », *Adv. in Math.* **100** (1993), p. 182–231.
[21] ———, « Translation scissors congruence », *Adv. in Math.* **100** (1993), p. 1–27.
[22] G. Pick – « Geometrisches zur Zahlenlehre », *Naturwiss. Z. Logos, Prag.* (1899), p. 311–319.
[23] J. E. Pommersheim – « Toric varieties, lattice points and Dedekind sums », *Math. Ann.* **295** (1993), p. 1–24.
[24] A. V. Pukhlikov & A. G. Khovanskii – « A Riemann-Roch theorem for integrals and sums of quasipolynomials over virtual polytopes », *St. Petersburg Math. J.* **4** (1993), p. 789–812.
[25] ———, « Finitely additive measures of virtual polytopes », *St. Petersburg Math. J.* **4** (1993), p. 337–356.
[26] H. Rademacher & E. Grosswald – *Dedekind sums*, Carus Math. Monogr., vol. 16, Mathematical Association of America, Washington, 1972.
[27] B. Teissier – « Variétés toriques et polytopes », in *Séminaire Bourbaki*, Lect. Notes in Math., vol. 901, Springer, 1980, p. 71–84.
[28] G. K. White – « Lattice polyhedra », *Canad. J. Math.* **16** (1964), p. 389–396.

Michel Brion, Laboratoire de Mathématiques,UMR 128 du CNRS, Ecole Normale Supérieure de Lyon
46 allée d'Italie, 69364 Lyon cedex 07
E-mail : `Michel.Brion@univ-grenoble-alpes.fr`
Url : `https://www-fourier.ujf-grenoble.fr/~mbrion/`