ANNALES DE L'INSTITUT FOURIER

ROLAND BACHER
P. DE LA HARPE
BORIS VENKOV

Séries de croissance et polynômes d'Ehrhart associés aux réseaux de racines

Annales de l'institut Fourier, tome 49, n° 3 (1999), p. 727-762
<http://www.numdam.org/item?id=AIF_1999__49_3_727_0>

Ann. Inst. Fourier, Grenoble
49, 3 (1999), 727–762

SÉRIES DE CROISSANCE ET POLYNÔMES D'EHRHART ASSOCIÉS AUX RÉSEAUX DE RACINES

par R. BACHER, P. DE LA HARPE & B. VENKOV

1. Introduction.

Pour un groupe Γ de type fini et un système fini S de générateurs de Γ, on définit la *fonction longueur* $\ell_S : \Gamma \to \mathbb{N}$, associant à $\gamma \in \Gamma$ la longueur minimum d'un mot en les lettres de $S \cup S^{-1}$ représentant γ. La *série de croissance* correspondante est la série formelle

$$\Sigma(z) = \Sigma(\Gamma, S; z) = \sum_{\gamma \in \Gamma} z^{\ell_S(\gamma)} = \sum_{k=0}^{\infty} \sigma(k) z^k \in \mathbb{Z}[[z]]$$

où $\sigma(k)$ est le cardinal de $\{\gamma \in \Gamma | \ell_S(\gamma) = k\}$. Si Γ est abélien libre de rang m, on sait que $\Sigma(z)$ est une fonction rationnelle, et plus précisément que $(1-z)^m \Sigma(z)$ est un polynôme. (Billington [Bil] a observé que c'est une conséquence de la rationalité des séries de Hilbert-Poincaré des algèbres graduées commutatives de type fini [KoM], chap. 3, th. 11.9; on trouve d'autres arguments dans [Kla] et [Ben].) L'objet de ce travail est de calculer explicitement $\Sigma(\Gamma, R; z)$ lorsque Γ est le groupe abélien libre engendré par

Les auteurs ont bénéficié d'un soutien du "Fonds National Suisse de la Recherche Scientifique".
Mots-clés : Croissance des groupes – Séries de croissance – Réseau de racine – Polynôme d'Ehrhart.
Classification math. : 05C25 – 11H06 – 20F32 – 52B20.

un système de racines R de l'une des quatre familles

$$\begin{aligned}
A_n &= \left\{(x_1, \dots, x_{n+1}) \in \mathbb{Z}^{n+1} | \sum_{i=1}^{n+1} x_i = 0\right\} \\
&\qquad\qquad \supset R(A_n) = \{\pm(e_i - e_j) | 1 \le i < j \le n+1\} \\
B_n &= \mathbb{Z}^n \supset R(B_n) = \{\pm e_i | 1 \le i \le n\} \cup R(D_n) \\
C_n &= \left\{(x_1, \dots, x_n) \in \mathbb{Z}^n | \sum_{i=1}^{n} x_i \equiv 0 \,(\mathrm{mod}\, 2)\right\} \\
&\qquad\qquad \supset R(C_n) = \{\pm 2e_i | 1 \le i \le n\} \cup R(D_n) \\
D_n &= \left\{(x_1, \dots, x_n) \in \mathbb{Z}^n | \sum_{i=1}^{n} x_i \equiv 0 \,(\mathrm{mod}\, 2)\right\} \\
&\qquad\qquad \supset R(D_n) = \{\pm e_i \pm e_j | 1 \le i < j \le n\}
\end{aligned}$$

où $\{e_1, \dots, e_m\}$ désigne la base canonique de $\mathbb{Z}^m$. (Selon l'usage, on considère la série des D_n pour $n \ge 2$, et les autres séries pour $n \ge 1$.)

Ce travail a été résumé dans [BHV].

THÉORÈME 1. — *Les séries de croissance des paires* (Γ, R) *ci-dessus sont les suivantes :*

$$\begin{aligned}
\Sigma(A_n, R; z) &= (1-z)^{-n} \sum_{i=0}^{n} \binom{n}{i}^2 z^i \\
\Sigma(B_n, R; z) &= (1-z)^{-n} \left(\sum_{i=0}^{n} \binom{2n+1}{2i} z^i - 2nz(1+z)^{n-1}\right) \\
\Sigma(C_n, R; z) &= (1-z)^{-n} \sum_{i=0}^{n} \binom{2n}{2i} z^i \\
\Sigma(D_n, R; z) &= (1-z)^{-n} \left(\sum_{i=0}^{n} \binom{2n}{2i} z^i - 2nz(1+z)^{n-2}\right).
\end{aligned}$$

À titre d'exercice préliminaire, le lecteur pourra vérifier ces formules pour les deux cas $A_1 = B_1 = C_1$ et A_2, ainsi que les égalités pour $B_2 = C_2$, $D_2 = A_1 \times A_1$ et $D_3 = A_3$ (voir les "cas particuliers" qui suivent le théorème 3 du chapitre 3). Laurent Bartholdi nous a signalé que la série pour A_n s'écrit aussi

$$\Sigma(A_n, R; z) \;=\; P_n\left(\frac{1+z}{1-z}\right)$$

où P_n désigne le n-ième polynôme de Legendre [(1)] (voir [PoS], vol. II, part. VI, N° 85). Par ailleurs, Thierry Vust nous a signalé qu'on a

$$\Sigma(A_n, R; z) = \frac{1}{(1-z)^{n+1}} F(n+1, n+1, 1; z)$$

où $F(a, b, c; z)$ est la notation usuelle pour une série hypergéométrique (ce qui indique sans doute qu'il existe une variante "hypergéométrique", pour la preuve de la proposition 2 ci-dessous).

Remarques. — (1) On peut observer que chacune de ces séries est de la forme $(1-z)^{-n}P(z)$ où P est un polynôme dont tous les coefficients sont *positifs* (voir la fin du chapitre 2, ainsi que l'exercice IV.28.a de [Sta], pages 271 et 288). Ceci n'est pas vrai pour des systèmes de générateurs arbitraires, puisqu'on a par exemple

$$(1-z)\Sigma(\mathbb{Z}, \{\pm 2, \pm 3\}; z) = 1 + 3z + 4z^2 - 2z^3.$$

(2) On peut aussi observer que les séries du théorème 1 pour les cas A_n, C_n et D_n satisfont l'identité $\Sigma(1/z) = (-1)^n \Sigma(z)$; voir ci-dessous le corollaire de la proposition 3. Ce n'est pas le cas pour pour B_n, puisqu'on a par exemple

$$\begin{aligned}(1-z)^3\Sigma(B_3, R; z) &= \left(\binom{7}{0} + \binom{7}{2}z + \binom{7}{4}z^2 + \binom{7}{6}z^3 - 6z(1+z^2)\right) \\ &= 1 + 15z + 23z^2 + z^3.\end{aligned}$$

La première étape de la preuve du théorème consiste à expliciter les fonctions longueur en termes des normes usuelles définies par

$$\|(x_1, \ldots, x_m)\|_1 = \sum_{i=1}^{m} |x_i| \quad \text{et} \quad \|(x_1, \ldots, x_m)\|_\infty = \max_{i=1}^{m} |x_i|$$

pour tout $x = (x_1, \ldots, x_m)$ dans $\mathbb{Z}^m$ (ou dans $\mathbb{R}^m$). On désigne par $\lceil q \rceil$ la partie entière *supérieure* d'un nombre réel q (de sorte que $\lceil q \rceil - 1 < q \le \lceil q \rceil$).

PROPOSITION 1. — *Les fonctions longueur des paires (Γ, R) considérées au théorème 1 sont données par*

$$\ell_R(x) = \begin{cases} N(x) & \text{pour tout } x \in \Gamma \text{ dans les cas } A_n, C_n, D_n, \\ \lceil N(x) \rceil & \text{pour tout } x \in \Gamma \text{ dans les cas } B_n \end{cases}$$

où $N : \Gamma \otimes_{\mathbb{Z}} \mathbb{R} \longrightarrow \mathbb{R}_+$ est la norme définie par

$$N(x) = \begin{cases} \frac{1}{2}\|x\|_1 & \text{dans les cas } A_n \text{ et } C_n, \\ \max\left\{\frac{1}{2}\|x\|_1, \ \|x\|_\infty\right\} & \text{dans les cas } B_n \text{ et } D_n. \end{cases}$$

(1) Cette remarque, également due à H. Wilf, est consignée dans [CS3].

Il faut prendre note de la particularité des cas B_n pour $n \geq 3$. Pour tout vecteur x dans l'un des réseaux A_n, C_n ou D_n, la norme $\|x\|_1$ est toujours paire, et par suite $\ell_R(x) = N(x)$. En revanche, pour $x \in B_n$ tel que $\sum_{i=1}^{n} x_i$ est impair et $\frac{1}{2}\|x\|_1 \geq \|x\|_\infty$, on a $\ell_R(x) = N(x) + \frac{1}{2}$. Il en résulte que la fonction ℓ_R *n'est pas homogène* pour B_3 ; par exemple, pour $x = e_1 + e_2 + e_3 \in B_3$, on a $\ell_R(x) = 2$ et $\ell_R(2x) = 3$.

Les formules du théorème 1 s'interprètent aussi en termes de polynômes d'Ehrhart ([Ehr], [Br1], [Br2], [Sta]). Voir le chapitre 3 ci-dessous.

Aux chapitres 4 et 5, nous traitons les cas exceptionnels dont nous savons venir à bout "à la main", c'est-à-dire les cas G_2 et F_4. Nous ne faisons qu'énoncer quelques résultats pour E_8, E_7 et E_6, obtenus par des calculs sur machine, et que nous ne souhaitons pas commenter davantage dans le présent travail. Le cas d'un réseau de racines quelconque résulte bien évidemment des cas irréductibles ainsi énumérés.

Les formules du théorème pour A_n et C_n apparaissent (sans preuve détaillée) dans une très courte note de Panyushev [Pa1]; voir aussi [Pa2], dont nous n'avons appris l'existence qu'après notre rédaction. C'est de même après avoir achevé ce travail que nous avons pris connaissance de [CS3] et [BaG].

Dans [CS3], Conway et Sloane prouvent les formules des théorèmes 1 et 4 pour A_n, E_6, E_7 et E_8 (voir leurs formules (3.7), (3.20), (3.35) et (3.42) respectivement), et ils conjecturent la formule pour D_n (d'autres réseaux apparaissent, mais les autres cas du présent travail n'apparaissent pas) ; voir aussi leur théorème 3.2 pour le cas D_n de l'énoncé de notre proposition 1. La terminologie de Conway et Sloane est par ailleurs différente de la nôtre; en particulier, les coefficients des séries du théorème 1 sont les "suites de coordination" des "graphes de contact" correspondants.

Dans [BaG], Baake et Grimm écrivent toutes les formules de nos théorèmes 1 et 4, en offrant les cas de B_n et D_n comme conjectures et en démontrant les autres.

2. Preuves de la proposition 1 et du théorème 1.

Preuve de la proposition 1. — (A) Soit $x \in A_n$. Posons $k = N(x) = \frac{1}{2}\|x\|_1$ et $l = \ell_R(x)$.

Comme on peut écrire $x = \alpha_1 + \ldots + \alpha_l$ avec $\alpha_1, \ldots \alpha_l \in R$, on a

$$k \leq \frac{1}{2}\left(\|\alpha_1\|_1 + \ldots + \|\alpha_l\|_1\right) = l$$

par sous-additivité de la norme N.

Pour l'égalité opposée, on remarque d'abord qu'on a évidemment $k = l$ si $x = 0$ et si $x \in R$ (c'est-à-dire si $k \leq 1$), puis on suppose que $k \geq 2$ et on procède par récurrence sur k. Comme on peut choisir $\alpha \in R$ tel que $\frac{1}{2}\|x - \alpha\|_1 = k - 1$, on obtient

$$l \leq \ell_R(x - \alpha) + \ell_R(\alpha) = (k-1) + 1 = k$$

par hypothèse de récurrence, et la preuve de ce cas est achevée.

(C) L'argument est en tout point semblable à celui de (A).

(D) Soit $x \in D_n$; posons $k = N(x) = \max\left\{\frac{1}{2}\|x\|_1, \|x\|_\infty\right\}$ et $l = l_R(x)$. Comme pour (A), on remarque que $k \leq l$ résulte de l'inégalité du triangle, et on continue en procédant par récurrence sur k. On suppose désormais $k \geq 2$, et on distingue trois cas.

Si $\frac{1}{2}\|x\|_1 > \|x\|_\infty$, on achève comme pour (A).

Si $\frac{1}{2}\|x\|_1 \leq \|x\|_\infty$ et s'il existe deux indices distincts $i, j \in \{1, \ldots, n\}$ tels que $\|x\|_\infty = |x_i| = |x_j|$, alors x est un multiple entier d'une des racines de la forme $\pm e_i \pm e_j$ et l'égalité $l = k$ est évidente.

Enfin, si $\frac{1}{2}\|x\|_1 \leq \|x\|_\infty$ et s'il existe un unique indice $i \in \{1, \ldots, n\}$ tel que $\|x\|_\infty = |x_i|$, alors on peut choisir $\alpha = \pm e_i \pm e_* \in R$ tel que $\max\left\{\frac{1}{2}\|x - \alpha\|_1, \|x - \alpha\|_\infty\right\} = k - 1$, et on obtient à nouveau $l \leq \ell_R(x - \alpha) + \ell_R(\alpha) = k$.

(B) Soit $x \in B_n$. Posons

$$l = \ell_R(x) \quad \text{et} \quad k = \lceil N(x) \rceil = \max\left\{\left\lceil \frac{1}{2}\|x\|_1 \right\rceil, \|x\|_\infty\right\}.$$

Premier cas : $\sum_{i=1}^{n} x_i \equiv 0 \,(\mathrm{mod}\, 2)$. Comme $R(D_n) \subset R(B_n)$, on a $l \leq \ell_{R(D_n)}(x) = k$ par le cas (D). Pour l'inégalité opposée, écrivons $x = \alpha_1 + \ldots + \alpha_l$ avec $\alpha_1, \ldots, \alpha_l \in R$. Comme $\|\alpha\|_1 \in \{1, 2\}$ et $\|\alpha\|_\infty = 1$ pour tout $\alpha \in R$, l'inégalité triangulaire implique bien que $k = N(x) \leq N(\alpha_1) + \ldots + N(\alpha_l) = l$.

Deuxième cas : $\sum_{i=1}^{n} x_i \equiv 1 \,(\mathrm{mod}\, 2)$. Pour tout $\epsilon \in \{1, -1\}$ et pour tout $i \in \{1, \ldots, n\}$, on a $\max\left\{\left\lceil \frac{1}{2} \|x + \epsilon e_i\|_1 \right\rceil, \|x + \epsilon e_i\|_\infty\right\} \geq k - 1$, de sorte que $\ell_R(x + \epsilon e_i) \geq k - 1$ par le premier cas. Comme toute somme de l racines égale à x comporte au moins une racine de la forme ϵe_i, il en résulte que $l = \ell_R(x) \geq k$.

Pour montrer l'inégalité opposée, et quitte à permuter et changer de signes les coordonnées de x (ce qui ne change ni k ni l), on peut supposer que $x_1 = \|x\|_\infty$. On a évidemment $\|x - e_1\|_1 < \|x\|_1$; par ailleurs, si $\|x - e_1\|_\infty = \|x\|_\infty$, alors il existe $j, k \in \{2, \ldots, n\}$ tels que $|x_j| = x_1$, $j \neq k$, et $|x_k| \neq 0$, de sorte que $\frac{1}{2} \|x\|_1 > \|x\|_\infty$. Il en résulte que $\max\left\{\left\lceil \frac{1}{2} \|x - e_1\|_1 \right\rceil, \|x - e_1\|_\infty\right\} = k - 1$. En utilisant de nouveau le premier cas, on a donc aussi $\ell_R(x - e_1) = k - 1$, et par suite $l = \ell_R(x) \leq k$.

Ceci achève la preuve de la proposition 1. □

Preuve des cas C, D et B du théorème 1. — Cas de (C_n). Rappelons qu'on a

$$\sum_{x \in \mathbb{Z}} z^{\frac{1}{2}|x|} = 1 + 2z^{1/2} + 2z + 2z^{3/2} + 2z^2 + \ldots = \frac{1 + \sqrt{z}}{1 - \sqrt{z}}.$$

Par un résultat de multiplicativité approprié pour les produits directs, on a donc aussi

$$\sum_{x \in \mathbb{Z}^n} z^{\frac{1}{2}\|x\|_1} = \left(\frac{1 + \sqrt{z}}{1 - \sqrt{z}}\right)^n.$$

On définit une fonction f et une suite numérique $(\sigma_k)_{k \geq 0}$ par

$$f(\sqrt{z}) = \left(\frac{1 + \sqrt{z}}{1 - \sqrt{z}}\right)^n = \sum_{k=0}^{\infty} \sigma_k z^{k/2}.$$

Comme C_n est le sous-groupe de $\mathbb{Z}^n$ des vecteurs x pour lesquels

$\|x\|_1 \equiv 0 \pmod 2$, on a

$$\Sigma(C_n, R; z) = \sum_{x \in C_n} z^{\frac{1}{2}\|x\|_1} = \sum_{k=0}^{\infty} \sigma_{2k} z^k = \frac{1}{2}\Big(f(\sqrt{z}) + f(-\sqrt{z})\Big)$$
$$= \frac{1}{2}\frac{(1+\sqrt{z})^{2n} + (1-\sqrt{z})^{2n}}{(1-z)^n} = (1-z)^{-n}\sum_{i=0}^{n}\binom{2n}{2i} z^i$$

comme affirmé au théorème 1.

Cas de (D_n). Vu le résultat pour le cas précédent, il suffit de calculer la série

$$\mathrm{Cor}_D(z) = \sum_{x \in D_n \text{ et } \|x\|_\infty > \frac{1}{2}\|x\|_1} \left(z^{\frac{1}{2}\|x\|_1} - z^{\|x\|_\infty}\right)$$

(où "Cor" vaut pour "terme de correction"). Pour $x \in D_n$ tel que $\|x\|_\infty > \frac{1}{2}\|x\|_1$, il existe un *unique* indice $i \in \{1, \ldots, n\}$ tel que $\|x\|_\infty = |x_i|$; par suite

$$\mathrm{Cor}_D(z) = 2n \sum_{x \in D_n \text{ et } x_1 > \frac{1}{2}\|x\|_1} \left(z^{\frac{1}{2}\|x\|_1} - z^{x_1}\right)$$

(le facteur 2 vient du remplacement d'une somme sur les x tels que $|x_1| > \frac{1}{2}\|x\|_1$ par la somme indiquée, avec x_1 positif). Pour x apparaissant dans cette dernière somme, écrivons $y = x - x_1 e_1$, de sorte que $x = (\|y\|_1 + 2s)\, e_1 + y$ pour un entier $s \geq 1$ convenable; on a donc

$$\mathrm{Cor}_D(z) = 2n \sum_{y \in \mathbb{Z}^{n-1}} \sum_{s=1}^{\infty} \left(z^{\|y\|_1 + s} - z^{\|y\|_1 + 2s}\right)$$
$$= 2n \left(\sum_{y \in \mathbb{Z}^{n-1}} z^{\|y\|_1}\right)\left(\frac{z}{1-z} - \frac{z^2}{1-z^2}\right)$$
$$= 2n \left(\frac{1+z}{1-z}\right)^{n-1} \frac{z}{1-z^2}$$
$$= \frac{2nz(1+z)^{n-2}}{(1-z)^n}$$

et la formule du théorème 1 pour D_n en résulte.

Cas de (B_n). La série de croissance est la somme de deux termes. Le premier est la contribution des vecteurs x tels que $\sum_{i=1}^{n} x_i$ est pair, et la proposition 1 montre que c'est la série de croissance de D_n. Le second est la contribution des vecteurs tels que $\sum_{i=1}^{n} x_i$ est impair, et s'écrit lui-même comme une différence

$$\sum_{x\in\mathbb{Z}^n, \|x\|_1\equiv 1 \ (\mathrm{mod}\ 2)} z^{\frac{1}{2}\|x\|_1+\frac{1}{2}} - \mathrm{Cor}_B(z).$$

En termes de la fonction f introduite pour le cas de (C_n), on a

$$\begin{aligned}\sum_{x\in\mathbb{Z}^n, \|x\|_1\equiv 1 \ (\mathrm{mod}\ 2)} z^{\frac{1}{2}\|x\|_1+\frac{1}{2}} &= \sqrt{z}\,\frac{1}{2}\Big(f(\sqrt{z}) - f(-\sqrt{z})\Big) \\ &= (1-z)^{-n} \sum_{i=1}^{n} \binom{2n}{2i-1} z^i.\end{aligned}$$

Quant à la "correction", elle s'écrit

$$\begin{aligned}\mathrm{Cor}_B(z) &= \sum_{\substack{x\in\mathbb{Z}^n, \|x\|_1\equiv 1 \ (\mathrm{mod}\ 2) \\ \|x\|_\infty > \frac{1}{2}\|x\|_1+\frac{1}{2}}} \left(z^{\frac{1}{2}\|x\|_1+\frac{1}{2}} - z^{\|x\|_\infty}\right) \\ &= 2n \sum_{\substack{x\in\mathbb{Z}^n, \|x\|_1\equiv 1 \ (\mathrm{mod}\ 2) \\ x_1 > \frac{1}{2}\|x\|_1+\frac{1}{2}}} \left(z^{\frac{1}{2}\|x\|_1+\frac{1}{2}} - z^{x_1}\right).\end{aligned}$$

Pour x apparaissant dans cette dernière somme, écrivons à nouveau $y = x - x_1 e_1$, de sorte que $x = (\|y\|_1 + 2s + 1)\,e_1 + y$ pour un entier $s \geq 0$ convenable; on a donc

$$\begin{aligned}\mathrm{Cor}_B(z) &= 2n \sum_{y\in\mathbb{Z}^{n-1}} \sum_{s=0}^{\infty} \left(z^{\|y\|_1+s+1} - z^{\|y\|_1+2s+1}\right) \\ &= 2n \left(\frac{1+z}{1-z}\right)^{n-1} \left(\frac{z}{1-z} - \frac{z}{1-z^2}\right) \\ &= 2nz^2 \frac{(1+z)^{n-2}}{(1-z)^n}.\end{aligned}$$

En regroupant les termes, on obtient pour la série de croissance

$$(1-z)^{-n}\Big\{\sum_{i=0}^{n}\binom{2n}{2i} z^i - 2nz(1+z)^{n-2} + \sum_{i=0}^{n}\binom{2n}{2i-1} z^i \\ -2nz^2(1+z)^{n-2}\Big\}$$

c'est-à-dire

$$\Sigma(B_n, R; z) = (1-z)^{-n}\Big\{\sum_{i=0}^{n}\binom{2n+1}{2i} z^i - 2nz(1+z)^{n-1}\Big\}.$$

Ceci achève la preuve du théorème 1 pour le cas B_n. □

Remarque. — Il existe aussi une famille

$$BC_n = \mathbb{Z}^n \supset R(BC_n) = \{e_i \mid 1 \leq i \leq n\} \cup \{\pm e_i \pm e_j \mid 1 \leq i \leq j \leq n\}$$

de systèmes de racines irréductibles *non réduits* ($n \geq 2$). On laisse au lecteur le soin de vérifier que, pour tout $n \geq 2$, la fonction longueur de la paire $(\mathbb{Z}^n, R)$ correspondante est donnée par

$$\ell_R(x) = \lceil \frac{1}{2} \|x\|_1 \rceil = \begin{cases} \frac{1}{2} \|x\|_1 & \text{si} \quad \sum_{i=0}^{n} x_i \equiv 0 \pmod 2) \\ \frac{1}{2} \|x\|_1 + \frac{1}{2} & \text{si} \quad \sum_{i=0}^{n} x_i \equiv 1 \pmod 2). \end{cases}$$

Pour la série de croissance, on obtient, avec $f(\sqrt{z}) = \sum_{x \in \mathbb{Z}^n} z^{\frac{1}{2}\|x\|_1}$ comme dans la preuve du théorème 1 pour C_n,

$$\begin{aligned} \Sigma(BC_n, R; z) &= \frac{1}{2}\Big(f(\sqrt{z}) + f(-\sqrt{z})\Big) + \sqrt{z}\frac{1}{2}\Big(f(\sqrt{z}) - f(-\sqrt{z})\Big) \\ &= (1-z)^{-n} \sum_{i=0}^{n} \binom{2n+1}{2i} z^i. \end{aligned}$$

Nous remercions T. Vust de nous avoir suggéré cette remarque.

Preuve du cas A du théorème 1. — Nous rassemblons dans l'énoncé suivant quelques propriétés élémentaires des coefficients binomiaux. Rappelons qu'on pose

$$\binom{x}{k} = \frac{x(x-1)\dots(x-k+1)}{k!}$$

pour tous $x \in \mathbb{C}$ (ou, selon le contexte, pour x l'indéterminée) et $k \in \mathbb{N}$, avec $\binom{x}{0} = 1$.

LEMME 1. — (i) *Pour tout entier $k \geq 0$, la notation $\binom{x}{k}$ désigne un polynôme de degré k en x à coefficient dominant $\frac{1}{k!}$.*

(ii) *On a* $\binom{n}{k} = \binom{n}{n-k}$ *pour tous* $n, k \in \mathbb{N}$, $0 \leq k \leq n$.

(iii) *On a* $\binom{-x}{k} = (-1)^k \binom{x+k-1}{k}$ *pour tous* $x \in \mathbb{C}$ *et* $k \in \mathbb{N}$; *en particulier* $\binom{-1}{k} = (-1)^k$ *pour tout* $k \in \mathbb{N}$.

(iv) *On a* $\sum_{l=0}^{k} \binom{x}{l}\binom{y}{k-l} = \binom{x+y}{k}$ *pour tous* $x, y \in \mathbb{C}$ *et* $k \in \mathbb{N}$.

Preuve. — Facile et standard. $\square$

Les étapes suivantes consistent à montrer au lemme 2 une première formule pour $\Sigma(A_n, R; z)$, puis à transformer cette formule à l'aide de l'identité binomiale établie à la proposition 2.

LEMME 2. — *La série de croissance de la paire $(A_n, R(A_n))$ est donnée par*

$$\Sigma(A_n, R; z) = 1 + \sum_{k=1}^{\infty} \sum_{s=1}^{n} \binom{n+1}{s} \binom{k-1}{s-1} \binom{n+k-s}{k} z^k.$$

Preuve. — À chaque $x = (x_1, \ldots, x_{n+1}) \in A_n$ on peut associer le nombre s [respectivement t] de ses coordonnées > 0 [resp. < 0] et la somme k de ses coordonnées strictement positives. Pour $k \geq 1$, le nombre σ_k des vecteurs $x \in A_n$ tels que $\frac{1}{2} \|x\|_1 = k$ est donné par

$$\sigma_k = \sum_{s,t=1}^{n} \binom{n+1}{s} \binom{n+1-s}{t} N(s,k) N(t,k)$$

où $N(s,k) = 0$ si $k < s$ et

$$N(s,k) = \sharp\Big\{(x_1, \ldots, x_s) \in \mathbb{Z}^s \big| x_1 > 0, \ldots, x_s > 0, \sum_{j=1}^{s} x_j = k\Big\}$$

si $k \geq s$. (Le nombre σ_k est a priori une somme sur les paires (s,t) telles que $s + t \leq n+1$, mais il faut noter que $\binom{n+1-s}{t} = 0$ si $s + t > n+1$.) En associant à chaque suite $(x_1, \ldots, x_s)$ comme ci-dessus les $s-1$ nombres $\sum_{j=1}^{r} x_j$ $(r = 1, \ldots, s-1)$, qui sont distincts et dans $\{1, \ldots, k-1\}$, on vérifie qu'on a

$$N(s,k) = \binom{k-1}{s-1}$$

(voir par exemple le §1.2 dans [Sta]). Par suite

$$\sigma_k = \sum_{s,t=1}^{n} \binom{n+1}{s} \binom{n+1-s}{t} \binom{k-1}{s-1} \binom{k-1}{t-1}.$$

On a enfin

$$\sum_{t=1}^{n+1-s} \binom{n+1-s}{t} \binom{k-1}{t-1} = \sum_{t=1}^{n+1-s} \binom{n+1-s}{n+1-s-t} \binom{k-1}{t-1}$$

$$= \sum_{u=0}^{n-s} \binom{n+1-s}{n-s-u} \binom{k-1}{u} = \binom{n+k-s}{n-s} = \binom{n+k-s}{k}$$

en utilisant les relations (ii) et (iv) du lemme 1, de sorte que

$$\sigma_k = \sum_{s=1}^{n} \binom{n+1}{s} \binom{k-1}{s-1} \binom{n+k-s}{k}$$

pour tout $k \geq 1$. □

PROPOSITION 2. — *On a*

$$\sum_{s=1}^{n} \binom{n+1}{s} \binom{k-1}{s-1} \binom{n+k-s}{k} = \sum_{l=0}^{n} \binom{n}{l}^2 \binom{n-1+k-l}{n-1}$$

pour toute paire d'entiers $n \geq 1, k \geq 1$.

Preuve. — Pour tous $n \geq 1$ et $k \in \mathbb{Z}$, on pose

$$a(n,k) = \sum_{s=1}^{n} \binom{n+1}{s} \binom{k-1}{s-1} \binom{n+k-s}{k}$$

et

$$b(n,k) = \sum_{l=0}^{n} \binom{n}{l}^2 \binom{n-1+k-l}{n-1}.$$

Il s'agit de montrer que $a(n,k) = b(n,k)$.

Premier pas : symétrie en k. On a

$$\begin{aligned}
a(n,-k) &= \sum_{t=1}^{n} \binom{n+1}{t} \binom{-k-1}{t-1} \binom{n-k-t}{n-t} \\
&\overset{s=n+1-t}{=} \sum_{s=1}^{n} \binom{n+1}{n+1-s} \binom{-k-1}{n-s} \binom{s-1-k}{s-1} \\
&\overset{\text{lemme 1}}{=} \sum_{s=1}^{n} \binom{n+1}{s} (-1)^{n-s} \binom{k+1+n-s-1}{n-s} \\
&\qquad\qquad (-1)^{s-1} \binom{-s+1+k+s-1-1}{s-1} \\
&= (-1)^{n-1} \sum_{s=1}^{n} \binom{n+1}{s} \binom{n+k-s}{n-s} \binom{k-1}{s-1} \\
&= (-1)^{n-1} a(n,k)
\end{aligned}$$

ainsi que

$$\begin{aligned}
b(n,-k) &= \sum_{m=0}^{n} \binom{n}{n-m}^2 \binom{n-1-k-m}{n-1} \\
&\overset{l=n-m}{=} \sum_{l=0}^{n} \binom{n}{l}^2 \binom{l-1-k}{n-1} \\
&\overset{\text{lemme 1}}{=} (-1)^{n-1} \sum_{l=0}^{n} \binom{n}{l}^2 \binom{-l+1+k+n-1-1}{n-1} \\
&= (-1)^{n-1} b(n,k).
\end{aligned}$$

Deuxième pas : dépendance polynomiale en k. Vues comme fonctions de k, les expressions $a(n,k)$ et $b(n,k)$ sont des polynômes de degré $n-1$. Elles ont même terme constant car

$$a(n,0) = -\sum_{s=1}^{n} \binom{n+1}{s} (-1)^s = 1 + (-1)^{n+1}$$

(conséquence de la formule du binôme pour $(1-1)^{n+1} = 0$) et

$$\begin{aligned}
b(n,0) &= \sum_{l=1}^{n} \binom{n}{l}^2 \binom{n-1-l}{n-1} \\
&= \binom{n}{0}^2 \binom{n-1}{n-1} + \binom{n}{n}^2 \binom{-1}{n-1} = 1 + (-1)^{n-1}
\end{aligned}$$

(car $\binom{k}{n-1} = 0$ si $0 \leq k \leq n-2$).

Troisième pas: dépendance polynomiale en n. Définissons pour tout $k \geq 1$ un polynôme en x par

$$a(x,k) = \sum_{s=1}^{k} \binom{x+1}{s} \binom{k-1}{s-1} \binom{x+k-s}{k}.$$

C'est un polynôme de degré $2k$, de coefficient dominant $(k!)^{-2}$ et de terme constant $a(0,k) = 0$.

La borne supérieure de l'indice de sommation dans la formule ci-dessus définissant $a(x,k)$, qui est k, est *différente* de la borne supérieure n définissant au début de la preuve le nombre $a(n,k)$. Toutefois, pour les valeurs entières $x = n \geq 1$ de la variable, on peut écrire la somme ci-dessus de $s = 1$ à $s = n$; en effet, si $n > k$, on a $\binom{k-1}{s-1} = 0$ pour $k < s \leq n$, alors que, si $n < k$, on a $\binom{n+k-s}{k} = 0$ pour $n < s \leq k$. Il en résulte que, si $x = n \geq 1$, la formule ci-dessus redonne bien les nombres $a(n,k)$ définis au début de la preuve.

On définit aussi

$$b(x,k) = \sum_{l=0}^{k} \binom{x}{l}^2 \binom{x+k-1-l}{k-l}.$$

C'est également un polynôme de degré $2k$, de coefficient dominant $(k!)^{-2}$, de terme constant $b(0,k) = 0$, et qui interpole les nombres $b(n,k)$ définis au début de la preuve.

Quatrième pas : récurrence sur n. Soit $n \geq 1$. Montrons qu'on a

$$(*) \qquad a(n,k) = b(n,k) \quad \text{pour tout} \quad k \in \mathbb{Z}.$$

C'est évident pour $n = 1$, car les deux membres de $(*)$ sont des polynômes en k de degré 0 qui sont égaux à l'origine (deuxième pas). On procède alors par récurrence sur n, en choisissant un entier $m \geq 1$ et en supposant l'égalité $(*)$ vraie pour $n \in \{1, 2, \ldots, 2m-1\}$.

Soit $j \in \{1, \ldots, m\}$. Les polynômes $a(x,j)$ et $b(x,j)$ en la variable x ont même degré, $2j$, même coefficient dominant, $(j!)^{-2}$, et même terme constant, 0 (troisième pas). De plus, ils prennent les mêmes valeurs pour $x \in \{1, \ldots, 2m-1\}$, par hypothèse de récurrence. Ces polynômes sont donc égaux, de sorte qu'on a en particulier

$$a(2m,j) = b(2m,j) \quad \text{et} \quad a(2m+1,j) = b(2m+1,j)$$

pour tout $j \in \{1, \ldots, m\}$.

Les polynômes $a(2m,y)$ et $b(2m,y)$ en la variable y ont même degré, $2m-1$, même terme constant (deuxième pas), ils prennent les mêmes valeurs pour $y \in \{1, \ldots, m\}$ (argument ci-dessus) ainsi que pour $y \in \{-1, \ldots, -m\}$ (premier pas). Ces polynômes sont donc égaux, ce qui montre $(*)$ pour $n = 2m$.

On montre de même que $a(2m+1,y) = b(2m+1,y)$, d'où $(*)$ pour $n = 2m+1$. □

On peut montrer que la proposition 2 résulte aussi d'identités connues entre fonctions hypergéométriques.

Rappelons encore l'énoncé suivant, bien connu (voir par exemple [Sta], page 209).

LEMME 3. — *Si, étant donné des entiers $d, m \geq 0$ et des nombres complexes $p_0, p_1, \ldots, p_m$, on définit une suite $(a_k)_{k \geq 0}$ par*

$$(1-z)^{-(d+1)} \sum_{l=0}^{m} p_l z^l = \sum_{k=0}^{\infty} a_k z^k$$

alors on a

$$a_k = \sum_{l=0}^{m} p_l \binom{d+k-l}{d}$$

pour tout $k \geq m-d$.

Preuve. — Pour tout $l \in \{0,1,\ldots,m\}$, on a

$$\frac{1}{(1-z)^{d+1}} = \sum_{j=0}^{\infty} \binom{d+j}{d} z^j$$

et donc aussi

$$\frac{z^l}{(1-z)^{d+1}} = \sum_{k=l}^{\infty} \binom{d+k-l}{d} z^k.$$

D'autre part, pour $k \in \{0,1,\ldots,l-1\}$, on a $\binom{d+k-l}{d} = 0$. Par suite

$$\frac{z^l}{(1-z)^{d+1}} = \sum_{k=0}^{\infty} \binom{d+k-l}{d} z^k$$

et le lemme en résulte. □

Avec la proposition 2 et le lemme 3, la preuve du cas (A) du théorème 1 est achevée.

Vérifions enfin un cas de la remarque 1 du chapitre 1 (après le théorème 1). Pour $i \in \{1,2,\ldots,n-2\}$, on a

$$\begin{aligned}\binom{2n+1}{2i} &= \sum_{k=0}^{2i} \binom{n}{k}\binom{n+1}{2i-k} > \binom{n}{i-1}\binom{n+1}{i+1} + \binom{n}{i+1}\binom{n+1}{i-1} \\ &\geq \binom{n-1}{i-1}(n+1) + n\binom{n-1}{i-1} \geq 2n\binom{n-1}{i-1}\end{aligned}$$

et le coefficient de z^i dans $(1-z)^n\Sigma(B_n, R; z)$ est strictement positif. Nous laissons les autres vérifications au lecteur.

3. Polynômes d'Ehrhart.

Soit Γ un réseau dans un espace vectoriel réel V de dimension finie; autrement dit, si V est de dimension n, soit Γ un sous-groupe discret du groupe additif de V isomorphe à $\mathbb{Z}^n$. Un *polytope convexe K de dimension d* est l'enveloppe convexe d'un nombre fini de points de V qui engendrent un sous-espace affine $< K >$ de dimension d. L'*intérieur relatif* de K, noté $\overset{\circ}{K}$, est l'intérieur de K dans $< K >$. Le *bord relatif,* noté ∂K, est le complément de $\overset{\circ}{K}$ dans K; il est réunion de faces de codimension 1 appelées *facettes.* On convient ici que K est un *polytope convexe entier* si K est l'enveloppe convexe d'une partie finie du réseau Γ.

Le *volume réticulaire* d'un polytope convexe entier K est le rapport $\mathrm{Vol}_{\mathrm{ret}}(K)$ entre le volume de K et celui d'un domaine fondamental de $\Gamma \cap < K >$ dans $< K >$. De même le *volume réticulaire du bord de K* est la somme $\mathrm{Vol}_{\mathrm{ret}}(\partial K)$ des volume réticulaires des facettes de K (chacune étant un polytope convexe dans un sous-espace affine convenable A de V de dimension $d-1$, polytope entier relativement au réseau affine $\Gamma \cap A$).

Notons que, si V est muni d'un produit scalaire pour lequel Γ est de discriminant $\mathrm{disc}(\Gamma)$ et si la dimension de K coïncide avec celle de V, alors le volume usuel de K est donné par la formule $\mathrm{Vol}(K) = \sqrt{\mathrm{disc}(\Gamma)}\ \mathrm{Vol}_{\mathrm{ret}}(K)$ (voir par exemple la section 1.1 de [Ebe]). Il n'y a pas de relation également simple entre le volume réticulaire de ∂K et son $(d-1)$-volume riemannien relativement à un produit scalaire de V.

Si K est un polytope convexe entier comme ci-dessus, on désigne pour tout entier $k \geq 1$ par

$$\begin{array}{lll} E_K(k) & \text{le cardinal de} & kK \cap \Gamma \\ E_K^{\circ}(k) & \text{le cardinal de} & k\overset{\circ}{K} \cap \Gamma \\ E_K^{\partial}(k) & \text{le cardinal de} & \partial(kK) \cap \Gamma \end{array}$$

(où kK désigne l'image de K par l'homothétie de rapport k). On pose aussi

$$E_K(0) = 1, \quad E_K^{\circ}(0) = 0, \quad E_K^{\partial}(0) = 1.$$

On définit les *séries d'Ehrhart* $\mathcal{E}_K(z)$, $\mathcal{E}_K^{\circ}(z)$ et $\mathcal{E}_K^{\partial}(z)$, ainsi que $P_k(z)$ et $P_K^{\circ}(z)$, par

$$\mathcal{E}_K(z) = \sum_{k=0}^{\infty} E_K(k) z^k = \frac{P_K(z)}{(1-z)^{d+1}}$$

$$\mathcal{E}_K^{\circ}(z) = \sum_{k=0}^{\infty} E_K^{\circ}(k) z^k = \frac{P_K^{\circ}(z)}{(1-z)^{d+1}}$$

$$\mathcal{E}_K^{\partial}(z) = \sum_{k=0}^{\infty} E_K^{\partial}(k)\ z^k = \mathcal{E}_K(z) - \mathcal{E}_K^{\circ}(z).$$

Ce sont des séries dans $\mathbb{Z}[[z]]$; la notation anticipe le fait que $P_K(z)$ et $P_K^{\circ}(z)$ sont des *polynômes.*

Le polytope convexe entier K est dit *laminateur* si, pour tout $x \in \Gamma$, il existe un unique entier $k \geq 0$ tel que $x \in \partial(kK)$, c'est-à-dire si $E_K^\circ(k) = E_K(k-1)$ pour tout $k \geq 1$, c'est-à-dire encore si $\mathcal{E}_K^\circ(z) = z\mathcal{E}_K(z)$. (Cette définition se trouve dans l'article de Panyushev [Pa1].)

Le théorème qui suit rassemble les premiers résultats de la théorie du polynôme d'Ehrhart.

THÉORÈME 2 (Ehrhart). — *Soit K un polytope convexe entier de dimension d, comme ci-dessus.*

(i) *La fonction $k \mapsto E_K(k)$ est polynomiale de degré d en k, et $E_K(0) = 1$. Autrement dit, $P_K(z)$ est un polynôme de degré au plus d tel que $P_K(1) \neq 0$, et $P_K(0) = 1$.*

(ii) *On a $E_K(-k) = (-1)^d E_K^\circ(k)$ pour tout $k \geq 1$, c'est-à-dire*

$$z^{d+1} P_K\left(\frac{1}{z}\right) = P_K^\circ(z) \quad \text{et} \quad \mathcal{E}_K\left(\frac{1}{z}\right) = (-1)^{d+1}\mathcal{E}_K^\circ(z).$$

(iii) *On a aussi $E_K^\partial(-k) = (-1)^{d+1} E_K^\partial(k)$ pour tout $k \geq 1$, c'est-à-dire*

$$\mathcal{E}_K^\partial\left(\frac{1}{z}\right) = (-1)^d \mathcal{E}_K^\partial(z).$$

(iv) *Le polytope K est laminateur si et seulement si P_K est palindromique, c'est-à-dire si et seulement si*

$$P_K\left(\frac{1}{z}\right) = z^d \, P_K(z).$$

(v) *Le coefficient dominant du polynôme $E_K(k)$ est* $\mathrm{Vol}_{\mathrm{ret}}(K)$.

(vi) *Le double du coefficient de k^{d-1} du polynôme $E_K(k)$ est* $\mathrm{Vol}_{\mathrm{ret}}\,(\partial K)$.

Sur la preuve. — Pour ces assertions, voir notamment [Ehr], [Br1], [Br2] et [Sta]. Pour la seconde partie de (i), voir plus précisément le corollaire 4.3.1 de [Sta].

Dans l'assertion (ii), si on admet la relation $E_K(-k) = (-1)^d E_K^\circ(k)$, on obtient la relation entre $P_K\left(\frac{1}{z}\right)$ et $P_K^\circ(z)$ via le lemme 3, puis la relation entre $\mathcal{E}_K\left(\frac{1}{z}\right)$ et $\mathcal{E}_K^\circ(z)$ en résulte immédiatement. L'assertion (iii) est conséquence immédiate de l'assertion (ii), et l'assertion (iv) des définitions. □

Les relations (v) et (vi), qui s'écrivent $E_K(k) = \mathrm{Vol}_{\mathrm{ret}}(K)k^d + \frac{1}{2}\mathrm{Vol}_{\mathrm{ret}}(\partial K)k^{d-1} + \sum_{j=2}^{d} c_j k^{d-j}$ se traduisent en termes du polynôme $P_K(z)$ et de sa dérivée $P'_K(z)$ par

$$\mathrm{Vol}_{\mathrm{ret}}(K) = \frac{1}{d!}P_K(1)$$

$$\frac{1}{2}\mathrm{Vol}_{\mathrm{ret}}(\partial K) = \frac{1}{(d-1)!}\Big\{(d+1)P_K(1) - 2P'_K(1)\Big\}.$$

Cela résulte d'expressions classiques pour $\sum_{k=0}^{\infty} k^d x^k$, qu'on trouve par exemple à la table 337 de [GKP].

Dans ce chapitre, on s'intéresse au cas particulier où $K = \mathrm{Conv}(R)$ est l'enveloppe convexe d'un des systèmes de racines du chapitre 1.

PROPOSITION 3. — *Soit R un des systèmes de racines du chapitre 1, engendrant un réseau Γ, soit $\Sigma(z) = \Sigma(\Gamma, R; z)$ la série de croissance correspondante, soit K l'enveloppe convexe de R et soit N la norme définie à la proposition 1. Alors*

(i) $$K = \{x \in \Gamma \otimes_{\mathbb{Z}} \mathbb{R} | N(x) \leq 1\}$$

et

(ii) $$\Sigma(z) = 1 + \sum_{k=1}^{\infty}\Big(E_K(k) - E_K(k-1)\Big)z^k.$$

Remarques. — (a) L'égalité (ii) se reformule aussi en

$$\frac{\Sigma(\Gamma, R; z)}{1-z} = \sum_{k=0}^{\infty} \sharp\left\{x \in \Gamma \middle| \ell_R(x) \leq k\right\} z^k = \mathcal{E}_K(z) = \sum_{k=0}^{\infty} E_K(k) z^k.$$

(b) Si le polytope K de la proposition 3 est laminateur, on a de plus

$$\mathcal{E}_K(z) = \frac{\mathcal{E}_K^{\partial}(z)}{1-z} = \frac{\Sigma(z)}{1-z}.$$

Preuve. — (i) Posons $L = \{x \in \Gamma \otimes_{\mathbb{Z}} \mathbb{R} | N(x) \leq 1\}$. Dans chacun des cas (A) à (D), il est évident que $K \subset L$; il s'agit donc de vérifier que $L \subset K$.

(A) La proposition étant évidente pour A_1, on procède par récurrence sur n, en supposant $n \geq 2$ et la proposition vraie pour A_{n-1}. Soit $x = (x_1, \ldots, x_{n+1}) \in \mathbb{R}^{n+1}$ tel que $\sum_{i=1}^{n+1} x_i = 0$ et tel que $N(x) = \frac{1}{2}\|x\|_1 \leq 1$.

Si l'une au moins des coordonnées x_i est nulle, l'hypothèse de récurrence implique que x est dans l'enveloppe convexe d'un sous-ensemble strict de R, et a fortiori dans $K = \mathrm{Conv}(R)$.

Si les coordonnées de x sont toutes non nulles, on peut supposer que

$$\begin{aligned}&0 < x_{n+1} = \min\{|x_1|, \ldots, |x_{n+1}|\}\\ &x_n < 0\\ &\text{et donc } |x_n| \geq x_{n+1}\end{aligned}$$

car les permutations des coordonnées et la transformation $x \mapsto -x$ ne changent ni K ni L d'une part, et $\sum_{i=1}^{n+1} x_i = 0$ d'autre part. Posons alors

$$y = \frac{x - x_{n+1}(e_{n+1} - e_n)}{1 - x_{n+1}} \quad \text{et} \quad z = e_{n+1} - e_n.$$

Vu que

$$\|x - x_{n+1}(e_{n+1} - e_n)\|_1 = \Big(\sum_{i=1}^{n} |x_i|\Big) - |x_{n+1}| = \|x\|_1 - 2x_{n+1} \leq 2 - 2x_{n+1}$$

on a $\dfrac{1}{2}\|y\|_1 \leq 1$. Comme de plus $y_{n+1} = 0$, l'hypothèse de récurrence implique que y est dans l'enveloppe convexe du système de racines de A_{n-1} ; a fortiori $y \in K = \mathrm{Conv}(R(A_n))$. Comme $z \in R(A_n)$, la combinaison convexe $x = (1 - x_{n+1})y + x_{n+1}z$ est bien dans K.

(C & D) Les arguments sont analogues, et nous en laissons le détail au lecteur.

(B) D'une part, on a $\mathrm{Conv}(R(B_n)) = \mathrm{Conv}(R(D_n))$; d'autre part la norme N est la même pour les cas B_n et D_n. Par suite, la preuve du cas (D) couvre aussi le cas (B).

(ii) On a

$$\begin{aligned}\Sigma(z) &= 1 + \sum_{k=1}^{\infty} \sharp\{\, x \in \Gamma | \ell_R(x) = k\} z^k && \text{par définition de } \Sigma\\ &= 1 + \sum_{k=1}^{\infty} \sharp\left\{x \in \Gamma \middle| k - \tfrac{1}{2} \leq N(x) \leq k\right\} z^k && \text{par la proposition 1}\\ &= 1 + \sum_{k=1}^{\infty} \sharp\left\{x \in \Gamma \middle| x \in kK \text{ et } x \notin (k-1)K\right\} z^k && \text{par (i)}\\ &= 1 + \sum_{k=1}^{\infty} \Big(E_K(k) - E_K(k-1)\Big) z^k && \text{par définition de } E_K.\end{aligned}$$

□

COROLLAIRE. — *Soit R un système de racines engendrant un réseau Γ, soit $\Sigma = \Sigma(\Gamma, R; z)$ la série de croissance correspondante, et soit K l'enveloppe convexe de R.*

Si R est de l'un des types A_n, C_n $(n \geq 1)$, ou D_n $(n \geq 2)$, alors K est laminateur et

$$\Sigma\left(\frac{1}{z}\right) = (-1)^n \Sigma(z).$$

Si R est de type B_n avec $n \geq 3$, alors K n'est pas laminateur.

Preuve. — Dans les cas A_n, C_n et D_n, la norme N de la proposition 1 prend des valeurs entières en tous les points du réseau engendré par R. C'est donc une conséquence immédiate de la proposition 3 que K soit laminateur.

L'égalité $\Sigma\left(\frac{1}{z}\right) = (-1)^n \Sigma(z)$ est donc une ré-écriture de celle du théorème 2.iv.

Dans le cas de B_n avec $n \geq 3$, pour voir directement que K n'est pas laminateur, considérons par exemple le vecteur $x = (1,1,1,0,\dots,0)$ (avec $n-3$ zéros) du réseau engendré par R. Alors

$$x = \frac{1}{2}(0,1,1,0,\dots,0) + \frac{1}{2}(1,0,1,0,\dots,0) + \frac{1}{2}(1,1,0,0,\dots,0) \in \partial\Big(\frac{3}{2}K\Big)$$

et

$$x \notin \bigcup_{k=0}^{\infty} \partial(kK),$$

de sorte que K n'est pas laminateur ; on peut aussi vérifier que $\Sigma\left(\frac{1}{z}\right) \neq (-1)^n \Sigma(z)$, avec la formule du théorème 1. □

Si on veut bien voir les fonctions $\Sigma(z)$ comme des variantes des séries thêta pour les réseaux considérés, la relation du théorème 2.iv et du corollaire ci-dessus pour les cas A_n, C_n et D_n rappelle l'égalité $\vartheta_\Gamma\left(-\frac{1}{\tau}\right) = \tau^{n/2}\vartheta_\Gamma(\tau)$ montrant que la série thêta d'un réseau Γ entier unimodulaire pair de rang n est une forme modulaire de poids $n/2$, et résultant de la formule sommatoire de Poisson (voir par exemple [Ser], n° 6.5, formule (100)).

THÉORÈME 3. — *Les polynômes d'Ehrhart des enveloppes convexes* *des systèmes de racines des séries A, B, C, et D sont les suivants :*

Cas de A_n : $E_K(k) = \sum_{i=0}^{n} \binom{n}{i}^2 \binom{k-i+n}{n}$.

Cas de B_n : $E_K(k) = \binom{k+n}{n} + \sum_{i=1}^{n} \left\{ \binom{2n+1}{2i} - 2n\binom{n-1}{i-1} \right\} \binom{k-i+n}{n}$.

Cas de C_n : $E_K(k) = \sum_{i=0}^{n} \binom{2n}{2i} \binom{k-i+n}{n}$.

Cas de D_n : $E_K(k) = \binom{k+n}{n} + \sum_{i=1}^{n} \left\{ \binom{2n}{2i} - 2n\binom{n-2}{i-1} \right\} \binom{k-i+n}{n}$.

Preuve. — Pour le cas de A_n, le théorème 1 et la proposition 3 montrent qu'on a

$$\sum_{k=0}^{\infty} E_K(k) z^k = \frac{1}{1-z} \left\{ 1 + \sum_{k=1}^{\infty} \left(E_K(k) - E_K(k-1) \right) z^k \right\}$$
$$= \frac{1}{(1-z)^{n+1}} \sum_{i=1}^{n} \binom{n}{i}^2 z^i$$

et la formule du théorème 3 résulte alors du lemme 3.

Les autres cas sont analogues. □

Cas particuliers "classiques". — (i) Pour B_2, on a

$$E_{B_2}(k) = (2k+1)^2$$

qui est le nombre de points à coordonnées entières dans le carré de $\mathbb{R}^2$ de sommets $(\pm k, \pm k)$.

Pour C_2, on a bien sûr également

$$E_{C_2}(k) = (2k+1)^2,$$

mais on interprète cette fois ceci comme le nombre des points du réseau pair

$$\{(a,b) \in \mathbb{Z}^2 | a+b \text{ pair}\}$$

dans le carré de $\mathbb{R}^2$ de sommets $(\pm 2k, 0), (0, \pm 2k)$.

(ii) Pour D_2, la formule

$$E_{D_2}(k) = 2k^2 + 2k + 1$$

donne le nombre de points du réseau pair qui sont dans le carré de sommets $(\pm k, \pm k)$, c'est-à-dire le k-ième "nombre carré centré" de Conway et Guy [CoG], page 42.

(iii) Pour A_2, la formule

$$E_{A_2}(k) = \sum_{i=0}^{2} \binom{2}{i}^2 \binom{k-i+2}{2} = 3k^2 + 3k + 1$$

donne le nombre des "nombres hex" de Martin Gardner, comptant le nombre de points entiers dans un hexagone convenable [CoG], page 41.

(iv) Pour C_3, on trouve

$$E_{C_3}(k) = \frac{1}{3}\big(16k^3 + 24k^2 + 14k + 3\big) = \frac{1}{3}(2k+1)\big(2(2k+1)^2 + 1\big)$$

qui est le nombre de points du réseau "cubique faces centrées"

$$\{(a,b,c) \in \mathbb{Z}^3 | a+b+c \text{ pair}\}$$

dans l'octaèdre $k\,\mathrm{Conv}(R(C_3))$ de $\mathbb{R}^3$ de sommets $(\pm 2k, 0, 0)$, $(0, \pm 2k, 0)$, $(0, 0, \pm 2k)$. En d'autres termes

$$E_{C_3}(k) = \mathrm{Oct}_{2k+1}$$

est le $(2k+1)$-ième "nombre octaédral" de Conway et Guy [CoG], page 50.

(v) Pour B_3, on trouve

$$E_{B_3}(k) = \frac{1}{3}\Big(20k^3 + 24k^2 + 10k + 3\Big)$$

qui est le nombre de points de $\mathbb{Z}^3$ dans le cuboctaèdre $k\,\mathrm{Conv}(R(B_3)) = k\,\mathrm{Conv}(R(D_3))$ obtenu par troncature du cube de sommets $(\pm k, \pm k, \pm k)$; il y a par exemple une image de ce cuboctaèdre dans [HiC], Fig. 178.

À titre de vérification, et si

$$\mathrm{Tet}_k = \frac{1}{6}k(k+1)(k+2)$$

désigne le k-ième nombre tétraédral $\sum_{j=1}^{k} \frac{j(j+1)}{2}$ (voir [CoG], page 44), on note qu'on a bien

$$E_{B_3}(k) + 8\,\mathrm{Tet}_k = (2k+1)^3$$

car le recollement de l'octaèdre $k\,\mathrm{Conv}(R(B_3))$ et de 8 tétraèdres convenables redonne bien le cube de sommets $(\pm k, \pm k, \pm k)$.

(vi) pour D_3, on trouve

$$E_{D_3}(k) = \frac{1}{3}\big(10k^3 + 15k^2 + 11k + 3\big)$$

qui est le nombre de points du réseau cubique faces centrées dans le même cuboctaèdre.

On peut bien sûr vérifier sur les formules du théorème 3 que

$$E_{A_3}(k) = E_{D_3}(k)$$

pour tout $k \geq 0$.

Voici une conséquence du théorème 3. (Rappel : $\mathrm{Vol}(K) = \sqrt{\mathrm{disc}(\Gamma)}\ \mathrm{Vol}_{\mathrm{ret}}(K)$, et $\mathrm{disc}(\Gamma)$ vaut respectivement $n+1, 1, 4, 4$ si le réseau Γ est A_n, B_n, C_n, D_n.)

PROPOSITION 4. — *Si K désigne l'enveloppe convexe du système de racines R, le volume euclidien de K et le volume réticulaire de ∂K sont donnés par les formules suivantes :*

Cas de A_n :
$$\mathrm{Vol}(K) = \frac{\sqrt{n+1}(2n)!}{(n!)^3} = \frac{\sqrt{n+1}}{n!}\binom{2n}{n}$$
$$\mathrm{Vol}_{\mathrm{ret}}(\partial K) = \frac{1}{(n-1)!}\binom{2n}{n}.$$

Cas de B_n :
$$\mathrm{Vol}(K) = \frac{2^n\,(2^n-n)}{n!}$$
$$\mathrm{Vol}_{\mathrm{ret}}(\partial K) = \frac{2^{2n-1}}{(n-1)!}.$$

Cas de C_n :
$$\mathrm{Vol}(K) = \frac{4^n}{n!}$$
$$\mathrm{Vol}_{\mathrm{ret}}(\partial K) = \frac{2^{2n-1}}{(n-1)!}.$$

Cas de D_n :
$$\mathrm{Vol}(K) = \frac{2^n\,(2^n-n)}{n!}$$
$$\mathrm{Vol}_{\mathrm{ret}}(\partial K) = \frac{2^{n-1}}{(n-1)!}(2^n-n).$$

En particulier on a

$$\frac{\mathrm{Vol}_{\mathrm{ret}}(\partial K)}{\mathrm{Vol}_{\mathrm{ret}}(K)} = n$$

dans les cas A_n, C_n et D_n, ainsi que

$$\frac{\mathrm{Vol}_{\mathrm{ret}}(\partial K(B_n))}{\mathrm{Vol}_{\mathrm{ret}}(K(B_n))} < n\ (n \geq 3) \quad \text{et} \quad \lim_{n\to\infty} \frac{1}{n}\,\frac{\mathrm{Vol}_{\mathrm{ret}}(\partial K(B_n))}{\mathrm{Vol}_{\mathrm{ret}}(K(B_n))} = \frac{1}{2}.$$

Preuve. — Vu les assertions (v) et (vi) du théorème 2, il suffit essentiellement d'écrire convenablement les coefficients de k^n et k^{n-1} dans les polynômes en k donnés par le théorème 3.

Cas de A_n. On a

$$\mathrm{Vol}_{\mathrm{ret}}(K) = \sum_{i=0}^{n} \binom{n}{i}^2 \frac{1}{n!} = \frac{1}{n!} \sum_{i=0}^{n} \binom{n}{i} \binom{n}{n-i} = \frac{1}{n!} \binom{2n}{n}.$$

Comme le réseau A_n est de discriminant $n+1$, on obtient la formule de l'énoncé pour $\mathrm{Vol}(K)$.

Le coefficient de k^{n-1} dans $\binom{k-i+n}{n}$ vaut

$$\frac{1}{n!} \sum_{j=-i+1}^{-i+n} j = \frac{1}{n!} \sum_{j=1}^{n} (-i+j) = \frac{1}{n!} \left(-ni + \frac{n(n+1)}{2} \right) = \frac{n+1-2i}{2(n-1)!}.$$

Par suite

$$\begin{aligned} \mathrm{Vol}_{\mathrm{ret}}(\partial K) &= 2 \sum_{i=0}^{n} \binom{n}{i}^2 \frac{n+1-2i}{2(n-1)!} \\ &= \frac{1}{(n-1)!} \sum_{i=0}^{n} \binom{n}{n-i}^2 (n-i) - \frac{1}{(n-1)!} \sum_{i=0}^{n} \binom{n}{i}^2 i \\ &\quad + \frac{1}{(n-1)!} \sum_{i=0}^{n} \binom{n}{i}^2. \end{aligned}$$

Les deux premières sommes de la dernière expression étant égales, il reste

$$\mathrm{Vol}_{\mathrm{ret}}(\partial K) = \frac{1}{(n-1)!} \frac{2n}{n}.$$

Cas de C_n. On a

$$\mathrm{Vol}_{\mathrm{ret}}(K) = \sum_{i=0}^{n} \binom{2n}{2i} \frac{1}{n!} = \frac{2^{2n-1}}{n!}$$

et la formule pour $\mathrm{Vol}(K)$ résulte de ce que le réseau C_n est de discriminant 4.

En reprenant une partie du calcul ci-dessus pour le cas de A_n, on a ici

$$\mathrm{Vol}_{\mathrm{ret}}(\partial K) = 2 \sum_{i=0}^{n} \binom{2n}{2i} \frac{n+1-2i}{2(n-1)!}.$$

Or

$$\sum_{i=0}^{n} \binom{2n}{2i} (n-2i) = \sum_{i=0}^{n} \binom{2n}{2i} (n-i) - \sum_{i=0}^{n} \binom{2n}{2n-2i} i = 0.$$

Donc

$$\mathrm{Vol}_{\mathrm{ret}}(\partial K) = \frac{1}{(n-1)!} \sum_{i=0}^{n} \binom{2n}{2i} = \frac{2^{2n-1}}{(n-1)!}.$$

Cas de D_n. On a

$$\begin{aligned}\mathrm{Vol}_{\mathrm{ret}}(K) &= \frac{1}{n!} + \sum_{i=1}^{n}\left\{\binom{2n}{2i} - 2n\binom{n-2}{i-1}\right\}\frac{1}{n!}\\ &= \frac{1}{n!}\left\{\sum_{i=0}^{n}\binom{2n}{2i} - 2n\sum_{i=0}^{n-1}\binom{n-2}{i}\right\}\\ &= \frac{1}{n!}\left\{2^{2n-1} - 2n2^{n-2}\right\} = \frac{2^{n-1}}{n!}\{2^n - n\}\end{aligned}$$

et $\mathrm{Vol}(K) = 2\,\mathrm{Vol}_{\mathrm{ret}}(K)$ puisque D_n est de discriminant 4.

En utilisant le calcul fait pour C_n, on a

$$\begin{aligned}\mathrm{Vol}_{\mathrm{ret}}(\partial K) &= 2\sum_{i=0}^{n}\binom{2n}{2i}\frac{n+1-2i}{2(n-1)!} - 4n\sum_{i=1}^{n-1}\binom{n-2}{i-1}\frac{n+1-2i}{2(n-1)!}\\ &= \frac{2^{2n-1}}{(n-1)!} - \frac{2n}{(n-1)!}\sum_{i=0}^{n-2}\binom{n-2}{i}(n-1-2i).\end{aligned}$$

Or

$$\sum_{i=0}^{n-2}\binom{n-2}{i}(n-2-2i) = \sum_{i=0}^{n-2}\binom{n-2}{i}(n-2-i) - \sum_{i=0}^{n-2}\binom{n-2}{n-2-i}i = 0.$$

Donc

$$\begin{aligned}\mathrm{Vol}_{\mathrm{ret}}(\partial K) &= \frac{2^{2n-1}}{(n-1)!} - \frac{2n}{(n-1)!}\sum_{i=0}^{n-2}\binom{n-2}{i}\\ &= \frac{2^{2n-1}}{(n-1)!} - \frac{2n}{(n-1)!}2^{n-2} = \frac{2^{n-1}}{(n-1)!}(2^n - n).\end{aligned}$$

Cas de B_n. Comme $\mathrm{Conv}(R(B_n)) = \mathrm{Conv}(R(D_n))$, la formule pour $\mathrm{Vol}(K)$ doit évidemment être la même dans les cas B_n et D_n. Vérifions-le. Pour $K = \mathrm{Conv}(R(B_n))$, on a

$$\begin{aligned}\mathrm{Vol}_{\mathrm{ret}}(K) &= \frac{1}{n!} + \sum_{i=1}^{n}\left\{\binom{2n+1}{2i} - 2n\binom{n-1}{i-1}\right\}\frac{1}{n!}\\ &= \frac{1}{n!}\left\{\sum_{i=0}^{n}\binom{2n+1}{2i} - 2n\sum_{i=0}^{n-1}\binom{n-1}{i}\right\}\\ &= \frac{1}{n!}\left\{\frac{1}{2}2^{2n+1} - 2n2^{n-1}\right\} = \frac{2^n}{n!}\{2^n - n\}\end{aligned}$$

qui est aussi la valeur de $\mathrm{Vol}(K)$, car le réseau $\mathbb{Z}^n$ engendré par $R(B_n)$ est de discriminant 1.

Le double du coefficient de k^{n-1} dans le polynôme d'Ehrhart de $\mathrm{Conv}(R(B_n))$ donné au théorème 3 s'écrit

$$\begin{aligned}\mathrm{Vol}_{\mathrm{ret}}(\partial K) = \frac{2}{2(n-1)!}\Bigg\{\sum_{i=0}^{n}\binom{2n+1}{2i}(n+1-2i)\\ -2n\sum_{i=1}^{n}\binom{n-1}{i-1}(n+1-2i)\Bigg\}.\end{aligned}$$

On calcule d'abord

$$\begin{aligned}\sum_{i=1}^{n}\binom{n-1}{i-1}(n+1-2i) &= \sum_{i=0}^{n-1}\binom{n-1}{i}(n-1-2i)\\ &= \sum_{i=0}^{n-1}\binom{n-1}{n-1-i}(n-1-i) - \sum_{i=0}^{n-1}\binom{n-1}{i}i\\ &= 0.\end{aligned}$$

Comme $\sum_{i=0}^{n}\binom{2n}{2i}(n-2i) = 0$ (voir le cas C_n), on obtient ensuite

$$\begin{aligned}\sum_{i=0}^{n}\binom{2n+1}{2i}(n-2i) &= \sum_{i=0}^{n}\binom{2n}{2i}(n-2i) + \sum_{i=1}^{n}\binom{2n}{2i-1}(n-2i)\\ &= \sum_{i=1}^{n}\binom{2n}{2i-1}(n-i) - \sum_{i=1}^{n}\binom{2n}{2i-1}i\\ &= \sum_{i=1}^{n}\binom{2n}{2(n+1-i)-1}((n+1-i)-1)\\ &\quad - \sum_{i=1}^{n}\binom{2n}{2i-1}i\\ &= \sum_{j=1}^{n}\binom{2n}{2j-1}j - \sum_{i=1}^{n}\binom{2n}{2n+1-2i}\\ &\quad - \sum_{i=1}^{n}\binom{2n}{2i-1}i\\ &= -2^{2n-1}.\end{aligned}$$

On a donc enfin

$$\begin{aligned}\mathrm{Vol}_{\mathrm{ret}}(\partial K) &= \frac{1}{(n-1)!}\left\{\sum_{i=0}^{n}\binom{2n+1}{2i}(n-2i) + \sum_{i=0}^{n}\binom{2n+1}{2i}\right\}\\ &= \frac{1}{(n-1)!}\{-2^{2n-1}+2^{2n}\}\\ &= \frac{2^{2n-1}}{(n-1)!}\end{aligned}$$

et la preuve est achevée. □

Remarques. — (1) La formule pour le volume de $\mathrm{Conv}\big(R(C_n)\big)$ s'obtient bien plus facilement comme suit : le convexe est réunion de 2^n tétraèdres de la forme

$$\mathrm{Conv}(0, 2\epsilon_1 e_1, \ldots, 2\epsilon_n e_n)$$

avec $\epsilon_i \in \{1, -1\}$, chacun de volume $\dfrac{2^n}{n!}$.

(2) En passant de B_n à D_n, on est passé à un sous-réseau d'indice 2. Pour certaines facettes, les restrictions des deux réseaux à l'hyperplan correspondant sont identiques. Pour d'autres facettes, les restrictions du réseau D_n sont d'indice 2 dans celles du réseau B_n. On peut voir que la proportion des facettes de ce second type tend vers 100 % quand n tend vers l'infini. C'est la raison pour laquelle le rapport

$$\frac{\mathrm{Vol}_{\mathrm{ret}}(\partial K(B_n))}{\mathrm{Vol}_{\mathrm{ret}}(\partial K(D_n))} = \frac{2^n}{2^n - n}$$

est toujours compris entre 2 (pour $n = 2$) et 1, et que sa limite quand $n \to \infty$ vaut 1. C'est aussi la raison de la dernière égalité dans l'énoncé de la proposition 4.

4. Polynômes d'Ehrhart pour les cas exceptionnels.

Cas de G_2. Le polygone $\mathrm{Conv}(R(G_2))$ est un hexagone dans le réseau $G_2 \approx \mathbb{Z}^2$. Un dessin montre immédiatement qu'on a

$$E_K(0) = 1, \quad E_K(1) = 13, \quad E_K(2) = 43$$

de sorte qu'on peut écrire

$$E_K(k) = 1 + 3k + 9k^2$$

(on arrive d'ailleurs au même résultat en observant que $\mathrm{Vol}_{\mathrm{ret}}(K) = 9$ et $\mathrm{Vol}_{\mathrm{ret}}(\partial K) = 6$). Par suite

$$\mathcal{E}_K(z) = \frac{1 + 10z + 7z^2}{(1-z)^3}$$

(voir le théorème 2).

Cas de F_4. Le système de racines s'écrit

$$R = \{\pm e_i\}_{1\leq i\leq 4} \cup \{\pm e_i \pm e_j\}_{1\leq i<j\leq 4} \cup \left\{\frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4)\right\}$$

et ces 48 racines engendrent le réseau

$$\mathbb{Z}^4 + \mathbb{Z}\frac{e_1 + e_2 + e_3 + e_4}{2}.$$

L'enveloppe convexe de ce système, qui est la même que celle de $R(D_4)$, a pour sommets les racines $\{\pm e_i \pm e_j\}_{1\leq i<j\leq 4}$, c'est-à-dire les milieux des côtés de l'hyperoctaèdre de sommets $\{\pm 2e_i\}_{1\leq i\leq 4}$. On reconnaît là le polytope régulier de symbole de Schläfli $\{3,4,3\}$; voir [Cox], N° 8.7.

LEMME 4. — *On désigne par K l'enveloppe convexe de $R(F_4)$ et par N la norme définie sur $\mathbb{R}^4$ par* $N(x) = \max\left\{\frac{1}{2}\|x\|_1, \|x\|_\infty\right\}$.

(i) *K est la boule unité de N.*

(ii) *Si, pour tout nombre réel $\lambda \geq 0$, on note $\sigma(\lambda)$ le nombre de points du réseau F_4 dans $\lambda\partial K$, alors les paires $(\lambda, \sigma(\lambda))$ avec $\lambda \leq 2$ et $\sigma(\lambda) \neq 0$ sont données par le tableau suivant :*

$$\begin{array}{llcr}
\lambda & = 0 & \sigma(\lambda) = & 1 \\
 & = 1 & = & 48 \\
 & = \dfrac{3}{2} & = & 96 \\
 & = 2 & = & 288.
\end{array}$$

Preuve. — L'assertion (i) résulte de la proposition 3 puisque

$$\mathrm{Conv}(R(F_4)) = \mathrm{Conv}(R(D_4)).$$

Pour l'assertion (ii), il s'agit de compter les vecteurs x du réseau F_4 pour lesquels $N(x) \leq 2$.

Comptons d'abord les vecteurs $x = (x_1, x_2, x_3, x_4)$ de $\mathbb{Z}^4$, en convenant que le *type* d'un tel vecteur est le réarrangement décroissant de $(|x_1|, |x_2|, |x_3|, |x_4|)$. On a

$$\begin{aligned}
2\binom{4}{1} &= \ \ 8 \text{ vecteurs de type } (1,0,0,0) \text{ et de } N\text{−norme } 1\\
2^2\binom{4}{2} &= 24 \text{ vecteurs de type } (1,1,0,0) \text{ et de } N\text{−norme } 1\\
2^3\binom{4}{3} &= 32 \text{ vecteurs de type } (1,1,1,0) \text{ et de } N\text{−norme } \frac{3}{2}\\
2^4 &= 16 \text{ vecteurs de type } (1,1,1,1) \text{ et de } N\text{−norme } 2\\
2\binom{4}{1} &= \ \ 8 \text{ vecteurs de type } (2,0,0,0) \text{ et de } N\text{−norme } 2\\
2^2\binom{4}{1}\binom{3}{1} &= 48 \text{ vecteurs de type } (2,1,0,0) \text{ et de } N\text{−norme } 2\\
2^3\binom{4}{1}\binom{3}{2} &= 96 \text{ vecteurs de type } (2,1,1,0) \text{ et de } N\text{−norme } 2\\
2^2\binom{4}{2} &= 24 \text{ vecteurs de type } (2,2,0,0) \text{ et de } N\text{−norme } 2
\end{aligned}$$

et tous les autres vecteurs de $\mathbb{Z}^4$ sont de N-norme strictement supérieure à 2.

Comptons ensuite les vecteurs $x = \frac{1}{2}(a_1, a_2, a_3, a_4)$ du réseau F_4 pour lesquels a_1, a_2, a_3, a_4 sont des entiers *impairs*. On a

$$\begin{aligned}
2^4 &= 16 \quad \text{vecteurs de type } \frac{1}{2}(1,1,1,1) \quad \text{et de } N\text{−norme } 1\\
2^4\binom{4}{1} &= 64 \quad \text{vecteurs de type } \frac{1}{2}(3,1,1,1) \quad \text{et de } N\text{−norme } \frac{3}{2}\\
2^4\binom{4}{2} &= 96 \quad \text{vecteurs de type } \frac{1}{2}(3,3,1,1) \quad \text{et de} N\text{−norme } 2
\end{aligned}$$

et tous les autres vecteurs de $\mathbb{Z}^4 + \frac{1}{2}(1,1,1,1)$ sont de N-norme strictement supérieurs à 2.

Doù l'assertion (ii) par comptabilité. □

Du lemme 4 résultent les évaluations suivantes du polynôme d'Ehrhart de $K = \mathrm{Conv}(R(F_4))$:

$$E_K(0) = 1 \qquad E_K(-1) = 1$$
$$E_K(1) = 1 + 48 = 49 \qquad E_K(-2) = 49 + 96 = 145$$
$$E_K(2) = 145 + 288 = 433.$$

Comme $E_K(z)$ est un polynôme de degré 4, on en déduit les expressions

$$E_K(k) \ = \ 1 + 8k + 8k^2 + 16k^3 + 16k^4$$

et

$$\mathcal{E}_K(z) = \frac{1 + 44z + 198z^2 + 140z^3 + z^4}{(1-z)^5}.$$

Autre cas : E_8, E_7 et E_6. Bien que le cas de E_8 puisse se traiter en principe comme celui de F_4, il nécessite une étude préalable du polytope $\mathrm{Conv}(R(E_8))$, enveloppe convexe des racines du système correspondant. (Dans plusieurs travaux de Coxeter et dans [CS1], les polytopes $\mathrm{Conv}(R(E_l))$ pour $l = 6, 7$ et 8 sont respectivement notés 1_{22}, 2_{31} et 4_{21}.)

Ensuite, pour mener à terme le calcul du polynône E_{K_8} (puis ceux de E_{K_6} et E_{K_7}), nous nous sommes assurés la collaboration d'une machine. Vu le changement de ton que cela impliquerait, nous nous bornons ici à reproduire les résultats, comme suit.

THÉORÈME 4. — *On a*

$$\begin{aligned}
\mathcal{E}_{K(G_2)}(z) &= \frac{1 + 10z + 7z^2}{(1-z)^3},\\
\mathcal{E}_{K(F_4)}(z) &= \frac{1 + 44z + 198z^2 + 140z^3 + z^4}{(1-z)^5},\\
\mathcal{E}_{K(E_6)}(z) &= \frac{1 + 66z + 645z^2 + 1384z^3 + 645z^4 + 66z^5 + z^6}{(1-z)^7},\\
\mathcal{E}_{K(E_7)}(z) &= \frac{1+119z+2037z^2+8211z^3 + 8787z^4 + 2037z^5 + 119z^6 + z^7}{(1-z)^8},\\
\mathcal{E}_{K(E_8)}(z) &= \frac{1 + 232z + 7228z^2 + 55\,384z^3 + 133\,510z^4}{(1-z)^9}\\
&\qquad + \frac{107\,224z^5 + 24\,508z^6 + 232z^7 + z^8}{(1-z)^9}.
\end{aligned}$$

On note que $\mathrm{Conv}(R(E_6))$ est laminateur alors que $\mathrm{Conv}(R(E_7))$, $\mathrm{Conv}(R(E_8))$, $\mathrm{Conv}(R(F_4))$ et $\mathrm{Conv}(R(G_2))$ ne sont pas laminateurs.

5. Séries de croissance pour les cas exceptionnels.

Cas de G_2. Le réseau engendré par le système de racines de type G_2 est le même que celui de A_2, à savoir

$$\Gamma = \left\{(x_1, x_2, x_3) \in \mathbb{Z}^3 | x_1 + x_2 + x_3 = 0\right\}.$$

Les racines s'écrivent

$$R = \left\{\pm(e_i - e_j)\right\}_{1 \le i < j \le 3} \cup \left\{\pm(2e_i - e_j - e_k)\right\}_{\curvearrowright}$$

(où $\curvearrowright$ indique que (i,j,k) est une permutation circulaire de $(1,2,3)$). On définit une norme N sur $\mathbb{R}^3$ en posant

$$N(x_1,x_2,x_3) = \frac{1}{3}\max\{|x_1|+|x_2|, |x_2|+|x_3|, |x_3|+|x_1|\} \ ;$$

rappelons que $\lceil t \rceil$ désigne la partie entière *supérieure* d'un nombre réel t (de sorte que $\lceil t \rceil - 1 < t \leq \lceil t \rceil$). L'analogue pour G_2 des propositions 1 et 3 se présente comme suit.

PROPOSITION 5. — *Soient R, Γ et N comme ci-dessus, soit $\ell_R : \Gamma \to \mathbb{N}$ la fonction longueur définie par R et soit $\Sigma(\Gamma, R; z)$ la série de croissance définie au chapitre 1. Soit K l'enveloppe convexe de R dans $\mathbb{R}^3$ et soit E_K son polynôme d'Ehrhart. On a*

(i) $\ell_R(x) = \lceil N(x) \rceil$ *pour tout* $x \in \Gamma$,

(ii) $K = \{x \in \mathbb{R}^3 | N(x) \leq 1$ *et* $x_1 + x_2 + x_3 = 0\}$,

(iii) $\Sigma(\Gamma, R; z) = 1 + \sum_{k=1}^{\infty} \big(E_K(k) - E_K(k-1)\big) z^k$.

Preuve. — (i) Soit $x \in \Gamma$. Posons $k = \lceil N(x) \rceil$ et $l = \ell_R(x)$. Comme $N(r) \in \{\frac{2}{3}, 1\}$, et en particulier $N(r) \leq 1$, pour tout $r \in R$, il résulte de l'inégalité du triangle que $N(x) \leq l$; par suite $k \leq l$.

Montrons que $l \leq k$. Cette inégalité étant évidemment vraie si $k \leq 1$, on suppose désormais que $k \geq 2$ et on procède par récurrence sur k. Quitte à permuter les coordonnées de x et à changer (simultanément) leurs signes, ce qui ne change ni k ni l, on peut supposer que $x_1 \geq |x_2| \geq |x_3|$; on observe alors que $x_2 < 0$ et $x_3 \leq 0$ (parce que $x_1 + x_2 + x_3 = 0$), et aussi que $x_1 > 1$ (parce que $N(x) > 1$).

Premier cas : $x_3 < 0$. On pose $y = x - (2,-1,-1)$. On a $N(y) = N(x) - 1$, donc aussi $\lceil N(y) \rceil = k - 1$. L'hypothèse de récurrence implique que $\ell_R(y) \leq k-1$, et par suite que $l \leq k$.

Second cas : $x_3 = 0$. Si $x_1 = 2$, alors $x = 2(1,-1,0)$ de sorte que $N(x) = \frac{4}{3}$, $k = 2$ et $l = 2$. Si $x_1 \geq 3$ on pose $y = x - (2,-1,-1) - (1,-2,1)$ de sorte que $N(y) = N(x) - 2$, et on achève comme dans le premier cas.

(ii) et (iii). L'égalité de (ii) s'observe par contemplation du dessin usuel, et l'argument pour (iii) est le même que pour la preuve de la proposition 3. $\square$

Cas de F_4. On considère maintenant le système de racines R de type

F_4 et le réseau Γ qu'il engendre dans $\mathbb{R}^4$, comme au chapitre précédent, ainsi que la fonction longueur associée $\ell_R : \Gamma \to \mathbb{N}$, la norme N définie sur $\mathbb{R}^4$ par $N(x) = \max\left\{\frac{1}{2}\|x\|_1, \|x\|_\infty\right\}$, et l'enveloppe convexe K de R dans $\mathbb{R}^4$. (On note que Γ contient le réseau engendré par $R(B_4)$.)

PROPOSITION 6. — *Les conclusions (i) et (iii) de la proposition 5 sont aussi vraies pour R, Γ, ℓ_R, N et K comme ci-dessus, et on a*

(ii) $$K = \left\{x \in \mathbb{R}^4 | N(x) \leq 1\right\}.$$

Preuve. — (i) Soit $x \in \Gamma$; posons $k = \lceil N(x) \rceil$ et $l = \ell_R(x)$. Montrons par exemple que $l \leq k$; on suppose que $k \geq 2$ et on procède par récurrence sur k.

Premier cas : x_1, x_2, x_3 et x_4 sont dans $\mathbb{Z}$. Alors x est dans le réseau de B_4. Comme $R(F_4) \supset R(B_4)$, on a $l = \ell_{R(F_4)}(x) \leq \ell_{R(B_4)}(x) = k$, en vertu de la proposition 1.

Second cas : x_1, x_2, x_3 et x_4 sont dans $\frac{1}{2} + \mathbb{Z}$. Alors il existe $\delta_1, \delta_2, \delta_3, \delta_4 \in \{\pm 1\}$ et $r = \frac{1}{2}(\delta_1 e_1 + \delta_2 e_2 + \delta_3 e_3 + \delta_4 e_4) \in R$ tels que, si on pose $y = x - r$, on ait $\frac{1}{2}\|y\|_1 = \frac{1}{2}\|x\|_1 - 1$ et $\|y\|_\infty = \|x\|_\infty - \frac{1}{2}$.

On note que $\frac{1}{2}\|x\|_1$ est entier et que $\|x\|_\infty$ est dans $\frac{1}{2} + \mathbb{Z}$. On a donc deux sous-cas. Ou bien $\frac{1}{2}\|x\|_1 > \|x\|_\infty$, et alors $k = N(x)$ donc $N(y) = \frac{1}{2}\|y\|_1 = k - 1$. Ou bien $\frac{1}{2}\|x\|_1 < \|x\|_\infty$, et alors $N(y) = \|y\|_\infty = N(x) - \frac{1}{2} = k - 1$. Ainsi, dans les *deux* sous-cas, il en résulte que $\lceil N(y) \rceil = k - 1$.

La preuve de l'inégalité $l \leq k$ s'achève comme à la proposition 5.

(ii) Si $L = \{x \in \mathbb{R}^4 | N(x) \leq 1\}$, l'inclusion $R \subset L$ implique évidemment $K \subset L$. Par ailleurs, on a d'une part $K \supset K_{B_4}$ parce que $R(F_4) \supset R(B_4)$, et d'autre part $K_{B_4} = L$ par la proposition 3. Donc $K = L$.

(iii) Voir l'argument de la proposition 3. □

Généralités sur la comparaison entre séries de croissance et séries d'Ehrhart. Voici un énoncé dont l'égalité (ii) de la proposition 3 est essentiellement un cas particulier.

PROPOSITION 7. — *Soit* Γ *un sous-groupe discret de* $\mathbb{R}^n$ *engendré par un système fini* S *de générateurs tel que* $-S = S$. *Pour tout entier* $k \geq 0$, *on note* $B_S(k)$ *la boule de rayon* k *centrée en* 0 *dans* Γ, *relativement à la longueur des mots* $\ell_S : \Gamma \longrightarrow \mathbb{N}$.

Soit K *l'enveloppe convexe de* S *dans* $\mathbb{R}^n$, *et soit* $N : \mathbb{R}^n \longrightarrow \mathbb{R}_{\geq 0}$ *la norme de boule unité* K, *définie par* $N(x) = \inf\{\lambda > 0 | x \in \lambda K\}$ *pour tout* $x \in \mathbb{R}^n$.

(i) *On a* $B_S(k) \subset kK \cap \Gamma$ *pour tout* $k \geq 0$ *et* $\ell_S(x) \geq \lceil N(x) \rceil$ *pour tout* $x \in \Gamma$.

(ii) *Les égalités suivantes sont équivalentes :*

$(ii)_1$	$\lvert B_S(k)\rvert$	$= \lvert kK \cap \Gamma\rvert$	*pour tout*	$k \geq 1$,
$(ii)_2$	$B_S(k)$	$= kK \cap \Gamma$	*pour tout*	$k \geq 1$,
$(ii)_3$	$\ell_S(x)$	$= \lceil N(x) \rceil$	*pour tout*	$x \in \Gamma$.

Preuve. — Les affirmations de (i) résultent des définitions (pour les détails, voir la preuve du lemme 5).

L'équivalence $(ii)_1 \Leftrightarrow (ii)_2$ résulte de (i) et de la finitude de $kK \cap \Gamma$ (pour tout $k \geq 1$).

On observe que $B_S(k)$ est strictement contenu dans $kK \cap \Gamma$ si et seulement s'il existe $x \in kK \cap \Gamma$ avec $\ell_S(x) > \lceil N(x) \rceil$, ce qui implique que $(ii)_2 \Leftrightarrow (ii)_3$. □

L'intérêt de la condition $(ii)_1$ est qu'il suffit souvent de n'en vérifier qu'une partie *finie*.

LEMME 5. — *Soit* $S \subset \mathbb{Z}^n$ *un sous-ensemble fini qui engendre* $\mathbb{Z}^n$ *comme semi-groupe; on désigne par* $\ell_S : \mathbb{Z}^n \longrightarrow \mathbb{N}$ *la fonction de longueur associée, par* $B_S(k) = \{x \in \mathbb{Z}^n | \ell_S(x) \leq k\}$ *la* ℓ_S*-boule de rayon* k *(pour tout* $k \geq 0$*), par* K *le polytope entier enveloppe convexe de* S, *et par* E_K *son polynôme d'Ehrhart.*

(i) *On a* $B_S(k) \subset kK \cap \mathbb{Z}^n$ *pour tout* $k \geq 0$.

(ii) *Si* $|B_S(k)| = E_K(k)$ *pour tout* $k \in \{0, 1, \ldots, n\}$, *alors*

$$B_S(k) = kK \cap \mathbb{Z}^n, \quad \textit{et a fortiori} \quad |B_S(k)| = E_K(k)$$

pour tout $k \in \mathbb{N}$.

Preuve. — (i) Le cas $k = 0$ est évident. Soient $k \geq 1$ et $x \in B_S(k)$.

Il existe $s_1, \ldots, s_k \in S$ tels que $x = \sum_{j=1}^{k} s_j$. Si $y = \frac{1}{k} \sum_{j=1}^{k} s_j$, on a $y \in K$ (par convexité de K) et $x = ky \in kK \cap \mathbb{Z}^n$.

(ii) Notons que l'assertion (i) et l'hypothèse de (ii) impliquent qu'on a $B_S(k) = kK \cap \mathbb{Z}^n$ pour $k \leq n$. On procède ensuite par récurrence sur k, en considérant un entier $k_0 \geq n$ et en supposant l'assertion (ii) vraie pour $k \leq k_0$. Soit $x \in (k_0 + 1)K \cap \mathbb{Z}^n$. On choisit une triangulation du bord de K, par des simplexes $F_1, \ldots, F_r$ à sommets dans S, numérotés de telle sorte que x est dans le cône défini par l'origine et F_1. Notons $t_1, \ldots, t_n$ les sommets de F_1 ; il existe donc des nombres réels positifs $\lambda_1, \ldots, \lambda_n$ tels que

$$x = \sum_{j=1}^{n} \lambda_j t_j \quad \text{et} \quad \sum_{j=1}^{n} \lambda_j \leq k_0 + 1.$$

Si $\sum_{j=1}^{n} \lambda_j \leq k_0$, alors $x \in k_0 K \cap \mathbb{Z}^n$ et $x \in B_S(k_0)$ par hypothèse de récurrence, et a fortiori $x \in B_S(k_0 + 1)$. Sinon, comme $k_0 \geq n$, on peut trouver $j \in \{1, \ldots, n\}$ tel que $\lambda_j \geq 1$, donc tel que $x - t_j \in k_0 K$; on a $\ell_S(x - t_j) \leq k_0$ par hypothèse de récurrence, donc $\ell_S(x) \leq k_0 + 1$, c'est-à-dire $x \in B_S(k_0 + 1)$. □

Remarquons que, avec les notations du lemme, l'inclusion $B_S(k) \subset kK \cap \mathbb{Z}^n$ peut être stricte, même si le système de générateurs S est égal à $-S$ et si $S = K \cap \mathbb{Z}^n$. On trouve un exemple où K est un octaèdre de $\mathbb{R}^3$ à la fin du chapitre 1 de [BHV].

En utilisant la proposition 7, le lemme 5, et des calculs sur machine assez simples à programmer, on montre que les calculs du polynômes d'Ehrhart et de la série de croissance sont encore essentiellement équivalents dans les cas plus compliqués de E_8, E_7 et E_6. Autrement dit, les assertions (iii) des propositions 5 et 6 s'étendent comme suit.

COROLLAIRE. — *Soit R un système de racines exceptionnel, Γ le groupe abélien libre engendré par R, et K l'enveloppe convexe de R. Alors la fonction de croissance $\Sigma(\Gamma, R; z)$ et la série d'Ehrhart $\mathcal{E}_K(z)$ apparaissant au théorème 4 satisfont la relation*

$$\frac{\Sigma(\Gamma, R, z)}{1 - z} = \mathcal{E}_K(z).$$

6. Questions.

(1) Soit $S \subset \mathbb{Z}^n$ un système de générateurs et $K = \mathrm{Conv}(S)$ son enveloppe convexe dans $\mathbb{R}^n$. Quand a-t-on

$$\frac{\Sigma(\mathbb{Z}^n, S; z)}{1-z} = \mathcal{E}_K(z)$$

comme aux propositions 3, 5 et 6? Si S n'est pas symétrique (*i.e.*, si $-S \neq S$), il faut comprendre que S engendre $\mathbb{Z}^n$ *comme semi-groupe*, et définir $\Sigma(\mathbb{Z}^n, S; z)$ à l'avenant.

(2) Que peut-on dire de l'ensemble des polytopes entiers convexes K de $\mathbb{R}^n$, tels que l'intérieur $\overset{\circ}{K}$ contient 0, et qui sont laminateurs?

Par exemple, modulo l'action du groupe affine $\mathbb{Z}^n \rtimes GL(n, \mathbb{Z})$, il semble que le nombre de ces polytopes soit fini.

(3) Plus généralement, pour tout réseau Γ engendré par ses vecteurs de longueur minimale, il serait intéressant de connaître les propriétés de la série de croissance correspondante. Quitte à formuler une question provocante, on peut demander quelle est cette série pour le réseau de Leech!

(3') Il est sans doute préférable de formuler la question précédente pour les "vecteurs relevants" dans un réseau (voir le § 1.2 du chapitre 2 de [CS2]), dont on sait qu'ils engendrent le réseau.

Pour les types A_n, D_n, et E_n, les vecteurs relevants sont les racines (voir le § 3.G du chapitre 21 de [CS2]).

Est-ce que la série de croissance relative aux vecteurs relevants est toujours la série associée au polynôme d'Ehrhart du polytope convenable?

Nous remercions Michel Brion pour plusieurs indications bibliographiques et Thierry Vust pour son intérêt constant.

BIBLIOGRAPHIE

[BaG] M. BAAKE et U. GRIMM, Coordination sequences for root lattices and related graphs, Zeitschrift für Kristallographie, 212 (1997), 253–256.

[BHV] R. BACHER, P. de la HARPE et B. VENKOV, Séries de croissance et séries d'Ehrhart associées aux réseaux de racines, C. R. Acad. Sci. Paris, 325 Sér. I (1997), 1137–1142.

[Ben] M. BENSON, Growth series of finite extensions of $\mathbb{Z}^n$ are rational, Inventiones Math., 73 (1983), 251–269.

[Bil] N. BILLINGTON, Growth of groups and graded algebras : erratum, Communications in Algebra, 13(3) (1985), 753–755.

[Bou] N. BOURBAKI, Groupes et algèbres de Lie (chapitres 4, 5 et 6), Hermann, 1968.

[Br1] M. BRION, Points entiers dans les polytopes convexes, Séminaire Bourbaki, mars 1994, Astérisque 227, Soc. Math. France (1995), 145–169.

[Br2] M. BRION, Polytopes convexes entiers, Gazette des mathématiciens, 67 (janvier 1996), 21–42.

[CoG] J.H. CONWAY et R.K. GUY, The book of numbers, Springer, 1996.

[CS1] J.H. CONWAY et N.J.A. SLOANE, The cell structure of certain lattices, in "Miscellanea Mathematics", édité par P. Hilton, F. Hirzebruch et R. Remmert, Springer (1991), 72–107.

[CS2] J.H. CONWAY et N.J.A. SLOANE, Sphere packings, lattices and groups (second edition), Springer, 1993.

[CS3] J.H. CONWAY et N.J.A. SLOANE, Low-dimensional lattices. VII Coordination sequences, Proc. R. Soc. Lond., Ser. A, 453 (1997), 2369–2389.

[Cox] H.S.M. COXETER, The polytopes with regular-prismatic vertex figures, Phil. Trans. Royal Soc. of London, Ser. A, 229 (1930), 329–425.

[Ebe] W. EBELING, Lattices and codes (a course partially based on lectures by F. Hirzebruch), Vieweg, 1994.

[Ehr] EHRHART, Sur un problème de géométrie diophantienne linéaire, J. reine angew. Math., 226 (1967), 1–29.

[GKP] R.L. GRAHAM, D.E. KNUTH et O. PATASHNIK, Concrete mathematics, Addison-Wesley, 1991.

[HiC] D. HILBERT and S. COHN-VOSSEN, Geometry and the imagination, Chelsea Publishing Company, 1952 and 1983.

[Kla] D.A. KLARNER, Mathematical crystal growth II, Discrete Applied Math., 3 (1981), 113–117.

[KoM] A.I. KOSTRIKIN and Yu. I. MANIN, Linear algebra and geometry, Gordon and Breach, 1989.

[Pa1] D.I. PANYUSHEV, Multiplicities of weights of some representations and convex polytopes, Functional Analysis and its Applications, 28-4 (1994), 293–295.

[Pa2] D.I. PANYUSHEV, Cones of highest weight vectors, weight polytopes, and Lusztig's q-analog, Transformation Groups, 2 (1997), 91–115.

[PoS] G. PÓLYA and G. SZEGÖ, Problems and theorems in analysis, volume I and II, Springer, 1972 and 1976.

[Ser] J-P. SERRE, Cours d'arithmétique, P.U.F., 1970.

[Sta] R.P. STANLEY, Enumerative combinatorics, Volume I, Wadsworth and Brooks, 1986.

R BACHER,
Université Joseph Fourier
B.P. 74
38402 St-Martin-d'Hères Cedex (France).
Roland.Bacher@ujf-grenoble.fr

P. de la HARPE,
Université de Genève
Section de Mathématiques
C.P. 240
CH-1211 Genève 24 (Suisse).
Pierre.delaHarpe@math.unige.ch

B. VENKOV,
St. Petersbourg's Department
of the Steklov Mathematical Institute
Fontanka 27
St. Petersbourg (Russie).