Jean-Yves DEGOS

Université Bordeaux I
Année 1995-1996

Le théorème des sous-espaces

Mémoire de D.E.A.
effectué sous la direction de
Laurent HABSIEGER

Remerciements

Je souhaite remercier en premier lieu Laurent Habsieger qui a accepté de m'encadrer pour la réalisation de ce travail, et qui a porté à ma connaissance le théorème des sous-espaces, qui se révèle être un beau joyau mathématique.

Je remercie aussi Michel Langevin qui a accepté d'être le rapporteur de ce mémoire, et Boas Erez qui a fait partie du jury de soutenance.

Enfin, je souhaite exprimer ma gratitude à Nicolas Brisebarre, qui a bien voulu relire les dernières épreuves de ce mémoire.

Jean-Yves DEGOS

Sommaire

Introduction

Un des objectifs de l'approximation diophantienne est d'étudier la manière dont on peut approcher les nombres réels par des nombres rationnels. C'est ainsi qu'en 1955, Roth obtint la médaille Fields pour avoir démontré le théorème suivant (cf. [Rot]).

Pour tout nombre algébrique α de degré $d \geq 2$, et tout $\delta > 0$, l'inéquation

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\delta}} \Longleftrightarrow |q||\alpha q - p| < |q|^{-\delta}$$

n'a qu'un nombre fini de solutions $(p, q) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$.

Ce travail, qui s'articule principalement autour du chapitre 6 du livre de W. M. Schmidt intitulé "Diophantine Approximations" (Lecture Notes in Mathematics n° 785), présente une généralisation de ce dernier résultat : le théorème des sous-espaces. Ce résultat s'énonce ainsi :

Soient $L_1, \ldots, L_n$ des formes linéaires sur $\mathbb{R}^n$ à coefficients algébriques, indépendantes sur $\mathbb{R}$ et soit $\delta > 0$. Il existe alors un nombre fini de sous-espaces vectoriels non triviaux de $\mathbb{Q}^n$, disons $T_1, \ldots, T_k$ tels que toute solution $x \in \mathbb{Z}^n \setminus \{0\}$ de l'inéquation

$$|L_1(x) \ldots L_n(x)| < \|x\|_\infty^{-\delta}$$

soit dans la réunion $T_1 \cup \cdots \cup T_k$.

Dans le chapitre 4 de ce mémoire, nous montrons que le théorème des sous-espaces implique le théorème de Roth, et permet même d'en prouver une version plus générale dans les corps de nombres, à savoir

Pour tout entier $k \geq 1$, tout nombre algébrique réel α et tout $\delta > 0$, il existe un nombre fini de nombres algébriques réels β de degré inférieur ou égal à k tels que :

$$|\alpha - \beta| < H(\beta)^{-k-1-\delta}.$$

($H(\beta)$ désignant ici le maximum des valeurs absolues des coefficients d'un polynôme de degré minimal à coefficients entiers premiers entre eux qu'annule β).

Le chapitre 3 traite de la preuve du théorème des sous-espaces proprement dite. En fait, ce dernier résulte du théorème des sous-espaces fort, qui s'énonce ainsi :

Soient $L_1, \dots, L_n$ des formes linéaires sur $\mathbb{R}^n$, indépendantes sur $\mathbb{R}$ à coefficients algébriques réels, et soient $c_1, \dots, c_n$ des nombres réels de somme nulle. Pour $Q > 1$, soit $\Pi(Q)$ le parallélépipède de $\mathbb{R}^n$ défini par

$$\forall i \in \{1, \dots, n\},\ |L_i(x)| \leq Q^{c_i},\ x \in \mathbb{R}^n\,.$$

Notons $\lambda_1(Q), \dots, \lambda_n(Q)$ ses minima successifs. On suppose qu'il existe $\delta > 0$, un entier d compris entre 1 et $n-1$, et une partie $\mathcal{D} \subset]1, +\infty[$ non bornée telle que

$$Q \in \mathcal{D} \Longrightarrow \lambda_d(Q) < \lambda_{d+1}(Q)Q^{-\delta}\,.$$

Alors il existe un sous-espace S de $\mathbb{Q}^n$ de dimension d, et une partie $\mathcal{D}' \subset \mathcal{D}$ telles que pour tout $Q \in \mathcal{D}'$, les d premiers minima successifs soient réalisés par des points $g_1, \dots, g_d$ de S.

En gros, la preuve se déroule ainsi ; on traite d'abord le cas $d = n-1$ en se ramenant, via un lemme de Davenport, à l'hypothèse plus agréable $\lambda_d(Q) < Q^{-\delta}$. Pour traiter ce cas-là, on procède par l'absurde en construisant un polynôme auxiliaire qui possède des propriétés contradictoires relatives à ses zéros. Il est nécessaire pour cela de définir et d'étudier deux notions d'*indice*, notions qui généralisent la notion d'ordre d'une racine. Nous présentons ces outils dans le chapitre 2.

Quant au cas général ($1 \leq d \leq n-1$), il se traite en faisant appel à une construction due à Mahler qui à un parallélépipède $\Pi(Q)$ de $\mathbb{R}^n$ possédant la propriété $\lambda_d(Q) < \lambda_{d+1}(Q)Q^{-\delta}$ permet d'associer un parallélépipède $\Pi^{(l)}(Q)$ de $\mathbb{R}^l$ qui satisfait une hypothèse du type $\lambda_{l-1}(Q) < \lambda_l(Q)Q^{-\delta'}$ pour l et δ' convenables.

Les différents outils permettant cette construction, à savoir l'Algèbre de Grassmann et des résultats de Géométrie des nombres, sont introduits dans le chapitre 1.

Chapitre 1

Géométrie des nombres et Algèbre de Grassmann

Le but de ce chapitre est de rappeler certains résultats relatifs à la Géométrie des nombres et à l'Algèbre de Grassmann, deux notions qui interviennent de façon décisive dans la preuve du théorème des sous-espaces, qui sera étudiée au chapitre 3.

1.1 Géométrie des nombres

1.1.1 Généralités

Dans tout ce qui suit, la lettre K désigne une partie convexe bornée, contenant 0 dans son intérieur, et symétrique par rapport à 0 (i.e. $x \in K \Rightarrow -x \in K$) de l'espace euclidien $\mathbb{R}^n$ usuel ($n \geq 1$). Pour $\lambda \in \mathbb{R}$, $\lambda K = \{\lambda x, x \in K\}$. La convexité de K entraîne que si $0 \leq \lambda \leq \lambda'$, alors $\lambda K \subset \lambda' K$. La Géométrie des nombres, dont le but est d'étudier la présence de points de $\mathbb{Z}^n$ (ou d'un autre réseau) dans des régions de l'espace euclidien, a son origine dans le théorème fondamental suivant.

Théorème 1.1.1 (Premier théorème de Minkowski) *Supposons que l'une des deux conditions soit satisfaite :*
(i) $\mathrm{Vol}\, K > 2^n$,
(ii) $\mathrm{Vol}\, K \geq 2^n$ *et* K *est compact .*
Alors $K \cap \mathbb{Z}^n$ *contient un autre point que 0.*

Preuve : Plaçons-nous sous l'hypothèse (i), et posons $K' = \frac{1}{2}K$, de sorte que $\mathrm{Vol}\, K' > 1$. Il existe alors $(x, y) \in K'^2$ avec $x - y \in \mathbb{Z}^n$. En effet, $\mathbb{Z}^n$ opère sur $\mathbb{R}^n$ par translation et un système de représentants des orbites est $C = [0, 1[^n$, ce qui permet d'écrire

$$\mathrm{Vol}\, K' = \sum_{z \in \mathbb{Z}^n} \mu(K' \cap (z + C)) = \sum_{z \in \mathbb{Z}^n} \mu((K' - z) \cap C)\,,$$

par invariance par translation de la mesure de Lebesgue μ. Il suit que les ensembles $((K'-z)\cap C)_{z\in\mathbb{Z}^n}$ ne sauraient être deux-à-deux disjoints, sinon nous aurions

$$1 = \operatorname{Vol} C \geq \sum_{z\in\mathbb{Z}^n} \mu((K'-z)\cap C) = \operatorname{Vol} K' > 1\,,$$

entraînant une contradiction avec l'hypothèse. Il existe donc bien $(z,z')\in\mathbb{Z}^n\times\mathbb{Z}^n$ distincts, et $(x,y)\in K'^2$ tels que $-z+x=-z'+y$, aussi le couple (x,y) répond-il aux exigences ci-dessus. En posant $a=x-y$, nous obtenons un point de $K\cap(\mathbb{Z}^n\setminus\{0\})$. Plaçons-nous maintenant sous l'hypothèse (ii), et prenons une suite $(\epsilon_k)_{k\in\mathbb{N}}$ de réels strictement positifs tendant vers 0. L'ensemble $K_k=(1+\epsilon_k)K$ satisfait alors (i) pour tout entier k, de sorte qu'il existe $x_k\in\mathbb{Z}^n\setminus\{0\}$ et $y_k\in K_k$ tels que $x_k=y_k(1+\epsilon_k)$. Par compacité de K, la suite $(y_k)_{k\in\mathbb{N}}$ peut être supposée convergente vers $y\in K$. Mais alors $(x_k)_{k\in\mathbb{N}}$ converge aussi vers y. Comme c'est une suite d'entiers non nuls, nous concluons que $y\in K\cap(\mathbb{Z}^n\setminus\{0\})$. ■

La réciproque de ce théorème est bien sûr fausse et c'est là une des difficultés principales de l'approximation diophantienne. Cela dit, rappelons une autre définition due à Minkowski.

Définition 1.1.2 *On appelle* MINIMA SUCCESSIFS *de K les n quantités $\lambda_1(K),\dots,\lambda_n(K)$ définies pour $i=1,\dots,n$ par :*

$$\lambda_i(K) = \inf\{\lambda>0 \mid \dim_{\mathbb{R}}(\operatorname{Vect}(\lambda K\cap\mathbb{Z}^n))\geq i\}\,.$$

Il est facile de voir qu'on a les inégalités :

$$0<\lambda_1(K)\leq\cdots\leq\lambda_n(K)<+\infty\,,$$

mais un fait particulièrement intéressant que nous admettrons est que l'on peut contrôler le produit $\lambda_1(K)\dots\lambda_n(K)$ en fonction uniquement de la dimension n et du volume de K.

Théorème 1.1.3 (SECOND THÉORÈME DE MINKOWSKI) *Si K est compact, l'inégalité suivante a lieu :*

$$\frac{2^n}{n!}\leq\lambda_1(K)\dots\lambda_n(K)\operatorname{Vol} K\leq 2^n\,.$$

Au sous-ensemble K de $\mathbb{R}^n$ on peut attacher certains vecteurs à composantes entières particuliers grâce au lemme suivant.

Lemme 1.1.4 *Il existe des vecteurs $g_1(K),\dots,g_n(K)$ tels que :*
(i) $g_i(K)\in\lambda_i(K)K\cap\mathbb{Z}^n$ pour $i=1,\dots,n$ et
(ii) $g_1(K),\dots,g_n(K)$ sont indépendants sur $\mathbb{R}$.

PREUVE : L'existence de $g_1(K)$ est assurée par le Premier théorème de Minkowski, et celle de $g_2(K),\dots,g_n(K)$ par le fait que pour $i\geq 2$, $\lambda_i(K)K$ doit contenir i vecteurs entiers indépendants, et qu'il contient déjà $g_1(K),\dots,g_{i-1}(K)$. ■

Remarque 1.1.5 *Les $g_1(K), \dots, g_n(K)$ ne sont pas uniques. Dans la suite, $g_1(K), \dots, g_n(K)$ désignera donc* un *choix de tels vecteurs, qu'on notera aussi parfois $g_1, \dots, g_n$ lorsqu'aucune confusion n'est possible.*

Leur introduction est justifiée par la proposition suivante.

Proposition 1.1.6 *Soit K compact et $\lambda_1(K), \dots, \lambda_n(K)$ les minima successifs de K, et $g_1(K)$, $\dots, g_n(K)$ des vecteurs satisfaisant les conditions (i) et (ii) du Lemme 1.1.4. Supposons que $2 \leq j \leq n, \lambda < \lambda_j(K)$ et enfin que $g \in \lambda K \cap \mathbb{Z}^n$. Alors $g \in \mathbb{R}g_1 \oplus \cdots \oplus \mathbb{R}g_{j-1}$.*

PREUVE : Si $\lambda < \lambda_1(K)$, on a $\lambda K \cap \mathbb{Z}^n = 0$ par définition de $\lambda_1(K)$ donc $g = 0$ et le résultat est vrai. Sinon, il existe un entier $l \geq 2$ avec $\lambda_{l-1}(K) \leq \lambda < \lambda_l(K)$; les vecteurs $g_1(K), \dots, g_{l-1}(K)$ et g sont dans λK (observer que $\lambda_i(K)K \subset \lambda K$ pour $i = 1, \dots, l-1$). Comme $g_1(K), \dots, g_{l-1}(K)$ sont indépendants et $\lambda < \lambda_l(K)$, le vecteur g est combinaison linéaire de $g_1(K), \dots, g_{l-1}(K)$ donc de $g_1(K), \dots, g_{j-1}(K)$, ce qu'il fallait démontrer. ■

1.1.2 Parallélépipèdes

Commençons par donner une définition.

Définition 1.1.7 *Un* PARALLÉLÉPIPÈDE *est une partie Π de $\mathbb{R}^n$ défini par*

$$\Pi = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid |L_i(x_1, \dots, x_n)| \leq A_i \text{ pour } i = 1, \dots, n\}$$

où $A_1, \dots, A_n$ sont des réels positifs, et $L_1, \dots, L_n$ des formes linéaires indépendantes sur $\mathbb{R}^n$.

Remarque 1.1.8 *Un tel parallélépipède sera souvent noté $\Pi(L_1, \dots, L_n; A_1, \dots, A_n)$ et sera dit* FERMÉ *; le parallélépipède ouvert correspond au même objet défini avec des inégalités strictes.*

Nous devons savoir calculer le volume d'un parallélépipède (il faut signaler un erreur à ce sujet dans [EdE], p. 42). C'est l'objet du lemme qui suit.

Lemme 1.1.9 *Soit $\Pi(L_1, \dots, L_n; A_1, \dots, A_n)$ un parallélépipède de $\mathbb{R}^n$. Alors :*

$$\operatorname{Vol} \Pi(L_1, \dots, L_n; A_1, \dots, A_n) = \frac{2^n A_1 \times \cdots \times A_n}{|\det(L_1, \dots, L_n)|}.$$

PREUVE : Nous reconnaissons en 2^n le volume de l'ensemble $U \stackrel{def}{=} \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid |x_i| < 1 \text{ pour } i = 1, \dots, n\}$, et nous observons qu'il y a un $\mathcal{C}^1$-difféomorphisme :

$$\begin{array}{rcl} \phi : \overset{\circ}{\Pi} & \longrightarrow & U \\ x & \longmapsto & y = \left(\frac{L_1(x)}{A_1}, \dots, \frac{L_n(x)}{A_n}\right). \end{array}$$

Comme ϕ est linéaire, la matrice jacobienne M_ϕ est constante et égale à :

$$\begin{pmatrix} \dfrac{L_1(e_1)}{A_1} & \cdots & \dfrac{L_n(e_1)}{A_n} \\ \vdots & & \vdots \\ \dfrac{L_1(e_n)}{A_1} & \cdots & \dfrac{L_n(e_n)}{A_n} \end{pmatrix}$$

dont le déterminant vaut $|\det(L_1,\dots,L_n)|/A_1\times\cdots\times A_n$. Le théorème de changement de variable en intégration fournit alors les égalités :

$$\operatorname{Vol} U = \int_U d\mu = \int_{\overset{\circ}{\Pi}} \frac{|\det(L_1,\dots,L_n)|}{A_1\times\cdots\times A_n} d\mu = \operatorname{Vol}\Pi \times \frac{|\det(L_1,\dots,L_n)|}{A_1\times\cdots\times A_n}\,,$$

d'où le résultat (μ désigne bien sûr la mesure de Lebesgue sur $\mathbb{R}^n$). ■

Munis de ces résultats on peut déduire le théorème des formes linéaires de Minkowski et une forme du Théorème 1.1.3 pour les parallélépipèdes fermés.

Théorème 1.1.10 *Soit $L_1,\dots,L_n$ des formes linéaires sur $\mathbb{R}^n$ telles que $\det(L_1,\dots,L_n)=1$, et $A_1,\dots,A_n$ des réels positifs tels que $A_1\dots A_n=1$.*
Alors il existe $(x_1,\dots,x_n)\in\mathbb{Z}^n\setminus\{0\}$ tel que :

$$\begin{cases} |L_i(x_1,\dots,x_n)| & < & A_i \text{ pour } i=1,\dots,n-1\,, \\ |L_n(x_1,\dots,x_n)| & \leq & A_n\,. \end{cases}$$

PREUVE : Quitte à diviser L_i par A_i pour $i=1,\dots,n$, nous pouvons supposer que $A_i=1$ pour $i=1,\dots,n$. Pour $\epsilon>0$, introduisons le parallélépipède ouvert $\Pi_\epsilon=\Pi(L_1,\dots,L_n;1,\dots,1,1+\epsilon)$. C'est une partie convexe, contenant 0 dans son intérieur, symétrique par rapport à 0, et de volume $2^n(1+\epsilon)>2^n$ donc il existe (Théorème 1.1.1) $x_\epsilon\in\Pi_\epsilon\cap(\mathbb{Z}^n\setminus\{0\})$. Prenons maintenant une suite $(\epsilon_k)_{k\in\mathbb{N}}$ qui tend vers 0 ; comme la famille de parallélépipèdes $(\Pi_{\epsilon_k})_{k\in\mathbb{N}}$ est uniformément bornée, on peut supposer que $(x_{\epsilon_k})_{k\in\mathbb{N}}$ converge vers $x\in\mathbb{R}^n$. Mais puisque les x_{ϵ_k} sont des vecteurs entiers cela signifie qu'il existe $k_0\in\mathbb{N}$ tel que pour $k\geq k_0$ nous ayons $x=x_{\epsilon_k}$. Alors $x\in\Pi_{\epsilon_k}\cap(\mathbb{Z}^n\setminus\{0\})$, ce qui prouve le théorème par passage à la limite sur l'inégalité $|L_n(x)|<1+\epsilon_k$ lorsque k tend vers $+\infty$. ■

Théorème 1.1.11 *Soient Π un parallélépipède fermé symétrique par rapport à 0, et $\lambda_1(\Pi),\dots,\lambda_n(\Pi)$ ses minima successifs. Alors :*

$$\frac{2^n}{n!} \leq \lambda_1(\Pi)\dots\lambda_n(\Pi)\operatorname{Vol}\Pi \leq 2^n n!\,.$$

Théorème 1.1.12 (LEMME DE DAVENPORT) *Soient $L_1,\dots,L_n$ des formes linéaires sur $\mathbb{R}^n$, de déterminant 1. Etant donnés Π le parallélépipède $\Pi(L_1,\dots,L_n;1,\dots,1)$, et ses minima successifs notés $\lambda_1,\dots,\lambda_n$, supposons disposer de réels $\rho_1,\dots,\rho_n$ tels que :*

$$\rho_1 > \cdots > \rho_n > 0\,, \tag{1.1}$$

$$\rho_1\lambda_1 \leq \cdots \leq \rho_n\lambda_n\,, \tag{1.2}$$

$$\rho_1\dots\rho_n = 1\,. \tag{1.3}$$

Alors il existe une permutation σ de $\{1,\dots,n\}$ telle que le parallélépipède

$$\Pi' = \Pi(\rho_1 L_{\sigma(1)},\dots,\rho_n L_{\sigma(n)};1,\dots,1)$$

ait des minima successifs $\lambda'_1,\dots,\lambda'_n$ satisfaisant :

$$2^{-n}\lambda_i\rho_i \le \lambda'_i \le 2^{n^2}(n!)^2\lambda_i\rho_i,\ i=1,\dots,n\,. \tag{1.4}$$

De plus si $g_i \overset{not}{=} g_i(\Pi)$ et $S_i \overset{def}{=} \oplus_{k=1}^{i}\mathbb{R}g_k$, alors :

$$\forall x\in\mathbb{Z}^n\setminus S_{i-1},\quad \max\{|\rho_1 L_{\sigma(1)}(x)|,\dots,|\rho_n L_{\sigma(n)}(x)|\}\ge 2^{-n}\lambda_i\rho_i,\quad \textit{pour } i=1,\dots,n\,, \tag{1.5}$$

avec la convention $S_0=\{0\}$.

Preuve : Posons pour $x\in\mathbb{R}^n$, $N(x)=\max\{|L_1(x)|,\dots,|L_n(x)|\}$. Par définition de $g_1,\dots,g_n$ nous avons $N(g_j)=\lambda_j$ pour $j=1,\dots,n$. Nous allons montrer qu'il existe $\sigma\in\mathfrak{S}_n$ (groupe symétrique d'ordre n) tel que pour chaque $j=n,\dots,1$ il existe des réels $\alpha_1^j,\dots,\alpha_{n-j+1}^j$ non tous nuls tels que :

$$\alpha_1^j L_{\sigma(1)}+\cdots+\alpha_{n-j+1}^j L_{\sigma(n-j+1)}\equiv 0 \text{ sur } S_{n-j} \text{ et} \tag{1.6}$$

$$|\alpha_{n-j+1}^j| = \max_{1\le k\le n-j+1}|\alpha_k^j| \tag{1.7}$$

En fait σ est construite grâce à l'algorithme suivant :

1. $j\leftarrow n$ et $\sigma\leftarrow$ Id.
2. Si $j=0$, c'est terminé.
3. Les formes linéaires $L_{\sigma(1)},\dots,L_{\sigma(j)}$ sont indépendantes, donc il existe des réels non tous nuls $b_{\sigma(1)},\dots,b_{\sigma(j)}$ tels que $b_{\sigma(1)}L_{\sigma(1)}+\cdots+b_{\sigma(j)}L_{\sigma(j)}$ vaut 0 sur S_{j-1}, et il existe une permutation τ de $\{\sigma(1),\dots,\sigma(j)\}$ telle que $b_{\tau(\sigma(j))}=\max_{1\le k\le j}|b_{\tau(\sigma(k))}|$. Il suffit alors de poser $\alpha_k^j=b_{\tau(\sigma(k))}$ pour $k=1,\dots,j$, et de remplacer σ par la permutation définie par

$$k\longmapsto\begin{cases}\tau(\sigma(k)) & \text{si } k=1,\dots,j\,,\\ \sigma(k) & \text{sinon}\,.\end{cases}$$

4. $j\leftarrow j-1$ et aller en 2.

Une fois cette construction faite, nous pouvons en déduire que

$$\forall j=1,\dots,n,\forall x\in S_j,\ |L_{\sigma(1)}(x)|+\cdots+|L_{\sigma(j)}(x)|\ge 2^{j-n}(|L_{\sigma(1)}(x)|+\cdots+|L_{\sigma(n)}(x)|) \tag{1.8}$$

En vue de montrer (1.5), considérons un $x \in \mathbb{Z}^n \setminus S_{i-1}$; il existe alors un entier j tel que $i \leq j \leq n$, avec $x \in S_j$ et $x \notin S_{j-1}$. D'après la Proposition 1.1.6 cela entraîne $N(x) > \lambda_j$, mais comme $x \in S_j$, nous avons :

$$\begin{array}{rcl} \max\{|\rho_1 L_{\sigma(1)}(x)|, \dots, |\rho_n L_{\sigma(n)}(x)|\} & \geq & \rho_j \max\{|L_{\sigma(1)}(x)|, \dots, |L_{\sigma(j)}(x)|\} \text{ par (1.1)} \\ & \geq & \frac{2^{j-n}}{j}\rho_j(|L_{\sigma(1)}(x)| + \dots + |L_{\sigma(n)}(x)|) \text{ par (1.8)} \\ & \geq & 2^{-n}\rho_j N(x) \geq 2^{-n}\rho_j\lambda_j \geq 2^{-n}\rho_i\lambda_i \text{ par (1.1)} \end{array}$$

ce qui montre (1.5), et il suit que $\lambda'_i \geq 2^{-n}\rho_i\lambda_i$ pour $i = 1, \dots, n$, ce qui est la première inégalité de (1.4). Pour montrer l'autre inégalité, nous observons que l'hypothèse (1.2) et le Lemme 1.1.9 montrent que $\operatorname{Vol}\Pi = \operatorname{Vol}\Pi' = 2^n$, donc le Théorème 1.1.11 permet d'obtenir les deux inégalités :

$$\frac{1}{n!} \leq \lambda_1 \dots \lambda_n \leq n! \text{ et } \frac{1}{n!} \leq \lambda'_1 \dots \lambda'_n \leq n!\,.$$

Donc pour $i = 1, \dots, n$:

$$\lambda'_i \leq \frac{n!}{\lambda'_1 \dots \hat{\lambda}'_i \dots \lambda'_n} \leq \frac{2^{n(n-1)}n!}{\rho_1\lambda_1 \dots \widehat{\rho_i\lambda_i} \dots \rho_n\lambda_n} < 2^{n^2}(n!)^2\rho_i\lambda_i$$

(la notation $\hat{x}$ signifiant qu'il ne faut pas tenir compte du facteur x dans les produits). ■

Parallélépipèdes réciproques et théorème de Mahler

Si $\Pi(L_1, \dots, L_n; 1, \dots, 1)$ est un parallélépipède au sens de la Définition 1.1.7, et si pour $i = 1, \dots, n$ nous appelons a_i le vecteur des composantes de la forme linéaire L_i sur la base canonique de $(\mathbb{R}^n)^*$, nous obtenons clairement que :

$$\begin{array}{rcl} \Pi(L_1, \dots, L_n; 1, \dots, 1) & = & \{x \in \mathbb{R}^n \mid |a_i.x| \leq 1 \text{ pour } i = 1, \dots, n\}\,, \\ & \overset{not}{=} & \Pi(a_1, \dots, a_n)\,. \end{array}$$

Ceci permet d'introduire une notion naturelle de dualité sur les parallélépipèdes.

Définition 1.1.13 *Les parallélépipèdes $\Pi(a_1, \dots, a_n)$ et $\Pi(a'_1, \dots, a'_n)$ sont dits* DUAUX *(ou réciproques) si $(a_1, \dots, a_n)$ et $(a'_1, \dots, a'_n)$ sont des bases de $\mathbb{R}^n$ duales l'une de l'autre.*

Le théorème de Mahler qui suit répond à la question naturelle suivante : si Π et Π' sont deux parallélépipèdes duaux, que pouvons-nous dire de $\lambda_1(\Pi'), \dots, \lambda_n(\Pi')$ et $g_1(\Pi'), \dots, g_n(\Pi')$ par rapport à $\lambda_1(\Pi), \dots, \lambda_n(\Pi)$ et $g_1(\Pi), \dots, g_n(\Pi)$?

Théorème 1.1.14 *Si $\Pi(a_1, \dots, a_n)$ et $\Pi(a_1^*, \dots, a_n^*)$ sont des parallélépipèdes duaux de minima successifs $\lambda_1, \dots, \lambda_n$ et $\lambda_1^*, \dots, \lambda_n^*$ respectivement. Alors :*

$$\forall i \in \{1, \dots, n\},\ \lambda_i^* \ll \lambda_{n+1-i}^{-1} \ll \lambda_i^*\,, \tag{1.9}$$

où les constantes induites par (1.9) ne dépendent que de n. De plus si $g_i = g_i(\Pi)$ pour $i = 1, \dots, n$ sont comme dans le Lemme 1.1.4, et si $(g_i^*)_{1\leq i\leq n}$ est la base duale $(g_i)_{1\leq i\leq n}$, alors

$$\forall i \in \{1, \dots, n\},\ \forall j \in \{1, \dots, n\},\ |a_i^*.g_j^*| \ll {\lambda_j}^{-1}\,. \tag{1.10}$$

PREUVE : Comme $g_j \in \lambda_j \Pi$, il existe $x_j \in \Pi$ avec $g_j = \lambda_j x_j$ d'où $a_i.g_j = \lambda_i a_i.x_j$ et $\forall i, j,\ |a_i.g_j| \leq \lambda_j$. Posons $E = |\det(g_1, \ldots, g_n)|$; nous avons alors $1 \leq E \leq n!^2$. En effet $g_1, \ldots, g_n$ sont indépendants et entiers donc $E \geq 1$ est clair ; l'autre inégalité vient de :

$$E = \lambda_1 \ldots \lambda_n |\det(x_1, \ldots, x_n)| \leq \lambda_1 \ldots \lambda_n\ n!\ 2^{-n} \operatorname{Vol} \Pi \leq n!^2 .$$

La dernière inégalité résulte du Théorème 1.1.11, tandis que l'avant-dernière résulte de l'observation suivante : comme Π est convexe il contient $\{\sum_{i=1}^n t_i x_i, |t_1| + \ldots + |t_n| \leq 1\}$, ensemble de volume $2^n/n!|\det(x_1, \ldots, x_n)|$. Considérons la matrice $A = (a_l.g_m)_{1 \leq l,m \leq n}$. En écrivant les g_k sur les a_j^* et les g_j^* sur les a_i, on vérifie que :

$$\sum_{i=1}^n a_i.g_k\ a_i^*.g_j^* = g_k.g_j^* = \delta_{kj} .$$

La matrice $B = (a_i^*.g_j^*)_{1 \leq i,j \leq n}$ est alors l'inverse de la matrice ${}^tA$. D'où $a_i^*.g_j^* = A_{ij}/\det A$, A_{ij} étant le cofacteur de a_{ij}. Ceci va nous permettre de déduire l'inégalité (1.10). En effet, en écrivant les a_l et les g_m sur la base canonique de $\mathbb{R}^n$ et en utilisant $\det {}^tMN = \det M \det N$ il vient $|\det A| = DE$. D'où les inégalités, pour $1 \leq i, j \leq n$:

$$\begin{aligned}
|a_i^*.g_j^*| &= \frac{|A_{ij}|}{|\det A|} \\
&\leq \frac{(n-1)!\lambda_1 \ldots \lambda_{j-1}\lambda_{j+1} \ldots \lambda_n}{DE} \text{ (car } |a_i.g_j| \leq \lambda_j) \\
&\leq (n-1)!\lambda_1 \ldots \lambda_n D^{-1} {\lambda_j}^{-1} \text{ (car } E \geq 1) \\
&\ll {\lambda_j}^{-1} \text{ (avec une constante dépendant de n)} .
\end{aligned}$$

En effet $D = 2^n/\operatorname{Vol} \Pi$ et nous savons que $2^{-n}\lambda_1 \ldots \lambda_n \operatorname{Vol}(\Pi) \ll 1$ (Théorème 1.1.11).

Montrons maintenant les inégalités de (1.9) ; il s'agit de trouver une constante $C \geq 1$ telle que $C/\lambda_j \Pi^* \cap \mathbb{Z}^n$ contienne $n + 1 - j$ vecteurs entiers linéairement indépendants. Pour cela il suffit de noter que les vecteurs $Eg_1^*, \ldots, Eg_n^*$ sont indépendants et entiers : si $(\epsilon_k)_{1 \leq k \leq n}$ désigne la base canonique de $\mathbb{R}^n$ et G la matrice de $(g_i)_{1 \leq i \leq n}$ dans cette base, la matrice de $(Eg_i^*)_{1 \leq i \leq n}$ dans cette base est $E\ {}^t(G^{-1}) = \pm \mathrm{com} G$ qui est entière.

Les inégalités (1.10) fournissent une constante $C \geq 1$ (ne dépendant que de n) telle que

$$|a_i^*.Eg_j^*| \leq C/\lambda_j,\ 1 \leq i, j \leq n .$$

Il suit que pour $j = 1, \ldots, n$, les vecteurs $Eg_n^*, \ldots, Eg_j^*$ sont contenus dans $C/\lambda_j \Pi^* \cap \mathbb{Z}^n$ et sont au nombre de $n + 1 - j$, donc $\lambda_{n+1-j}^* \leq C{\lambda_j}^{-1}$, ce qui prouve le premier membre de (1.10) modulo le changement d'indice $j \mapsto n + 1 - j$. Le second membre s'obtient en remarquant que :

$$\operatorname{Vol} \Pi \operatorname{Vol} \Pi^* = \frac{2^n}{|\det(a_1, \ldots, a_n)|} \frac{2^n}{|\det(a_1^*, \ldots, a_n^*)|} = 4^n ,$$

d'où les inégalités :

$$\begin{aligned}
\lambda_1 \ldots \lambda_n \lambda_1^* \ldots \lambda_n^* &= 4^{-n}\ \lambda_1 \ldots \lambda_n \operatorname{Vol} \Pi\ \lambda_1^* \ldots \lambda_n^* \operatorname{Vol} \Pi^* \\
&\geq \tfrac{1}{n!^2} \text{ (Théorème 1.1.11)} ,
\end{aligned}$$

dont nous déduisons finalement :

$$1 \ll \lambda_1 \dots \lambda_n \lambda_1^* \dots \lambda_n^* = \left(\prod_{j \neq i} \lambda_j^* \lambda_{n+1-j} \right) \lambda_i^* \lambda_{n+1-i} \ll \lambda_i^* \lambda_{n+1-i}$$

pour $i = 1, \dots, n$, ce qui achève la preuve du théorème de Mahler. ■

Dans la preuve du théorème des sous-espaces fort, nous aurons besoin à partir d'un parallélépipède Π de $\mathbb{R}^n$ pour lequel λ_{n-1} ne possède pas une certaine propriété de construire un parallélépipède de $\mathbb{R}^N$ (N à déterminer) pour lequel λ_{N-1} possède cette propriété. Cette construction utilise l'Algèbre de Grassmann et les parallélépipèdes composés de Mahler.

1.2 Algèbre de Grassmann et parallélépipèdes composés de Mahler

Dans toute cette section $C(n,p)$ désigne l'ensemble des p-uplets d'entiers $(i_1, \dots, i_p)$ qui satisfont $1 \leq i_1 < \dots < i_p \leq n$, de sorte que $C(n,p)$ contient $l = C_n^p$ éléments. La base canonique de $\mathbb{R}^n$ est notée $(e_1, \dots, e_n)$.

1.2.1 L'Algèbre de Grassmann

Définition 1.2.1 *On note $\mathbb{R}_p^n$ le $\mathbb{R}$-espace vectoriel engendré par les symboles $e_{i_1} \wedge \dots \wedge e_{i_p} = E_\sigma$ où $\sigma = (i_1, \dots, i_p) \in C(n,p)$, et on définit pour un multi-indice $1 \leq j_1, \dots, j_p \leq n$*

$$e_{j_1} \wedge \dots \wedge e_{j_p} = \begin{cases} 0 & \text{si } \exists k \neq k' \text{ avec } j_k = j_{k'}\,, \\ \epsilon(\sigma) e_{i_1} \wedge \dots \wedge e_{i_p} & \text{si } \sigma \text{ envoie } 1 \leq i_1 < \dots < i_p \leq n \text{ sur } (j_1, \dots, j_p)\,. \end{cases}$$

Lemme 1.2.2 *On fait de $\mathbb{R}_p^n$ un espace euclidien de dimension l en posant pour $(\sigma, \tau) \in C(n,p)$:*

$$E_\sigma . E_\tau = \delta_{\sigma\tau} = \begin{cases} 1 & \text{si } \sigma = \tau\,, \\ 0 & \text{sinon}\,. \end{cases}$$

Définition 1.2.3 *On appelle* Algèbre de Grassmann *de $\mathbb{R}^n$, le $\mathbb{R}$-espace vectoriel*

$$G_n = \bigoplus_{p=0}^{n} \mathbb{R}_p^n$$

muni du produit extérieur noté $\wedge$, défini par les formules

$$1 \wedge 1 = 1\,, \tag{1.11}$$

$$1 \wedge (e_{i_1} \wedge \dots \wedge e_{i_p}) = (e_{i_1} \wedge \dots \wedge e_{i_p}) \wedge 1 = e_{i_1} \wedge \dots \wedge e_{i_p}\,,$$

$$(e_{i_1} \wedge \dots \wedge e_{i_p}) \wedge (e_{j_1} \wedge \dots \wedge e_{j_p}) = e_{i_1} \wedge \dots \wedge e_{i_p} \wedge e_{j_1} \wedge \dots \wedge e_{j_p}\,, \tag{1.12}$$

qu'on prolonge par $\mathbb{R}$-linéarité. On obtient ainsi une $\mathbb{R}$-algèbre associative.

Nous poursuivons maintenant par une série de lemmes techniques mais utiles pour calculer dans $(G_n, +, \wedge)$. Nous devons tout d'abord savoir développer un élément de $\mathbb{R}_p^n$ sur la base canonique.

Lemme 1.2.4 *Supposons que $x_i = \sum_{j=1}^n \xi_{ij} e_j$ pour $1 \leq i \leq p$. Nous avons alors l'écriture*

$$x_1 \wedge \cdots \wedge x_p = \sum_{\sigma \in C(n,p)} \xi_\sigma E_\sigma$$

où par définition $\xi_\sigma = \det(\xi_{ij_k})_{1 \leq i,k \leq p}$ si $\sigma = (j_1, \ldots, j_p)$.

PREUVE : Les deux termes de la formule à démontrer sont des fonctions linéaires de $x_i, 1 \leq i \leq p$ de sorte qu'il suffit de la démontrer lorsque $x_i = e_{j_i}, 1 \leq i \leq p$, avec $1 \leq j_1, \ldots, j_p \leq n$. S'il existe deux entiers l et l' pour lesquels $j_l = j_{l'}$, on a $x_{j_1} \wedge \cdots \wedge x_{j_p} = 0$ par définition, et $\xi_\sigma = 0$. Sinon puisque les deux membres se comportent de façon identique quand on permute les x_i, on peut supposer que $1 \leq j_1 < \cdots < j_p \leq n$. Alors d'après la Définition 1.2.1, $e_{j_1} \wedge \cdots \wedge e_{j_p} = E_\sigma$ pour $\sigma = (j_1, \ldots, j_p)$. Il suffit donc de vérifier que $\xi_\tau = 1$ si $\tau = \sigma$ et $\xi_\tau = 0$ sinon, ce qui est clair. ■

Lemme 1.2.5 *Pour $(x_1, \ldots, x_p) \in (\mathbb{R}^n)^p$, nous avons l'équivalence :*

$$x_1 \wedge \cdots \wedge x_p = 0 \Longleftrightarrow x_1, \ldots, x_p \text{ sont linéairement dépendants}.$$

PREUVE : Par le lemme précédent, dont on garde les notations, $x_1 \wedge \cdots \wedge x_p = 0$ signifie que $\xi_\sigma = 0$ pour tout $\sigma \in C(n,p)$, c'est-à-dire que tous les mineurs d'ordre p de la matrice $(\xi_{ij})_{1 \leq i \leq p, 1 \leq j \leq n}$ sont nuls, ce qui équivaut finalement à dire que le système de vecteurs $(x_1, \ldots, x_p)$ est de rang strictement inférieur à p, ce que nous voulions. ■

Lemme 1.2.6 *Soient $(x_1, \ldots, x_p)$ et $(y_1, \ldots, y_p)$ deux p-uplets de vecteurs linéairement indépendants de $\mathbb{R}^n$. Alors*

$$\mathbb{R}x_1 \oplus \cdots \oplus \mathbb{R}x_p = \mathbb{R}y_1 \oplus \cdots \oplus \mathbb{R}y_p \Longleftrightarrow \mathbb{R}y_1 \wedge \cdots \wedge y_p = \mathbb{R}x_1 \wedge \cdots \wedge x_p\,.$$

PREUVE : Si $\mathbb{R}y_1 \oplus \cdots \oplus \mathbb{R}y_p = \mathbb{R}x_1 \oplus \cdots \oplus \mathbb{R}x_p$, nous pouvons écrire $y_j = \sum_{i=1}^p a_{ij} x_i$, $A = (a_{ij})_{1 \leq i,j \leq p}$ étant inversible. Or pour toute permutation $\sigma \in S_p$, nous avons :

$$x_{\sigma(1)} \wedge \cdots \wedge x_{\sigma(p)} = \epsilon(\sigma) x_1 \wedge \cdots \wedge x_p\,,$$

ce qui permet d'obtenir que $y_1 \wedge \cdots \wedge y_p = (\det A) x_1 \wedge \cdots \wedge x_p$, et le second membre de l'équivalence. Réciproquement supposons $y_1 \wedge \cdots \wedge y_p = \lambda x_1 \wedge \cdots \wedge x_p, \lambda \in \mathbb{R}^*$. Alors nous avons $y_1 \wedge \cdots \wedge y_p \wedge x_i = 0$ pour $i = 1, \ldots, p$ donc par le Lemme 1.2.5, $x_i \in \mathbb{R}y_1 \oplus \cdots \oplus \mathbb{R}y_p$, d'où le premier membre de l'équivalence. ■

Lemme 1.2.7 (IDENTITÉ DE LAPLACE) *Soient $(x_1, \ldots, x_p)$ et $(y_1, \ldots, y_p)$ deux p-uplets de vecteurs de $\mathbb{R}^n$. Alors*

$$x_1 \wedge \cdots \wedge x_p . y_1 \wedge \cdots \wedge y_p = \det(x_i . y_j)_{1 \leq i,j \leq p}\,.$$

PREUVE : Le lemme résulte des trois observations suivantes :
– les deux membres sont des fonctions linéaires de $x_1, \dots, x_p, y_1, \dots, y_p$;
– si σ et τ sont deux permutations et $(i_1, \dots, i_p) \in C(n,p), (j_1, \dots, j_p) \in C(n,p)$, alors

1. $e_{\sigma(i_1)} \wedge \cdots \wedge e_{\sigma(i_p)}.e_{\tau(j_1)} \wedge \cdots \wedge e_{\tau(j_p)} = \epsilon(\sigma)\epsilon(\tau) e_{i_1} \wedge \cdots \wedge e_{i_p}.e_{j_1} \wedge \cdots \wedge e_{j_p}$
2. $\det\left(x_{\sigma(i_k)}.y_{\tau(j_l)}\right)_{1\le k,l\le p} = \epsilon(\sigma)\epsilon(\tau) \det\left(x_{i_k}.y_{j_l}\right)_{1\le k,l\le p}$;

– d'après la Définition 1.2.10, $e_{i_1} \wedge \cdots \wedge e_{i_p}.e_{j_1} \wedge \cdots \wedge e_{j_p} = E_\sigma.E_\tau = \delta_{\sigma\tau}$, et

$$\det\left(e_{i_k}.e_{j_l}\right)_{1\le k,l\le p} = \sum_{s\in\mathfrak{S}_p} \prod_{k=1}^{p} e_{i_k}.e_{j_{s(k)}} .$$

Un terme de ce dernier déterminant est non nul lorsque $i_k = j_{s(k)}$ pour tout $k = 1, \dots, p$. Ceci n'a lieu que pour $s = Id$, c'est-à-dire $\sigma = \tau$. ■

Lemme 1.2.8 *Soient* $(x_1, \dots, x_n) \in (\mathbb{R}^n)^n$.
Pour $\tau = (j_1, \dots, j_p) \in C(n,p)$, *posons* $X_\tau = x_{j_1} \wedge \cdots \wedge x_{j_p}$. *Alors*

$$\det\left(X_\tau\right)_{\tau\in C(n,p)} = \left(\det\left(x_1, \dots, x_n\right)\right)^{lp/n} .$$

PREUVE : Si $(x_1, \dots, x_n) = (e_1, \dots, e_n)$, les deux membres de la formule valent 1. Si $x_1, \dots, x_n$ sont dépendants, le membre de droite vaut 0, et il existe $\tau \in C(n,p)$ tel que $X_\tau = 0$, donc les deux membres sont égaux. Reste le cas où $(x_1, \dots, x_n)$ est une base. Dans ce cas c'est l'image de $(e_1, \dots, e_n)$ par une composée d'applications du type :

$$\begin{array}{rccc} D_i(\lambda) & : & (\mathbb{R}^n)^n & \longrightarrow & (\mathbb{R}^n)^n \\ & & (x_1, \dots, x_n) & \longmapsto & (x_1, \dots, \lambda x_i, \dots, x_n) , \end{array}$$

$$\begin{array}{rccc} B_{ij}(\lambda) & : & (\mathbb{R}^n)^n & \longrightarrow & (\mathbb{R}^n)^n \\ & & (x_1, \dots, x_n) & \longmapsto & (x_1, \dots, x_i, \dots, \underbrace{x_j + \lambda x_i}_{j}, \dots, x_n) . \end{array}$$

Sous l'effet de $D_i(\lambda)$, le second membre est multiplié par $\lambda^{lp/n}$, et sous l'effet de $B_{ij}(\lambda)$, il est inchangé. D'autre part, sous l'effet de $D_i(\lambda)$, un vecteur X_τ est inchangé sauf si lorsque $\tau = (j_1, \dots, j_p)$, il existe l compris entre 1 et p tel que $j_l = i$. Le nombre de tels τ étant $C_{n-1}^{p-1} = lp/n$, le premier membre est multiplié par $\lambda^{lp/n}$ tout comme le second. Enfin, sous l'effet de $B_{ij}(\lambda)$, regardons ce que devient $X_\tau = x_{j_1} \wedge \cdots \wedge x_{j_p}$.
– Si $j \notin \{j_1, \dots, j_p\}$, X_τ est inchangé ,
– si $j \in \{j_1, \dots, j_p\}$ et $i \in \{j_1, \dots, j_p\}$, X_τ est encore inchangé ,
– si $j \in \{j_1, \dots, j_p\}$ et $i \notin \{j_1, \dots, j_p\}$, X_τ devient $X_\tau \pm \lambda X_{\tau'}$ pour un $\tau' \in C(n,p)$ convenable, donc globablement le premier membre est inchangé. Nous concluons que la formule est toujours vraie. ■

Le lemme suivant nous donne un moyen simple de déduire des bases duales de $\mathbb{R}_p^n$ à partir de bases duales de $\mathbb{R}^n$.

Lemme 1.2.9 *Soient* $(a_1, \dots, a_n)$ *une base de* $\mathbb{R}^n$ *et* $1 \leq p \leq n$. *Pour* $\sigma = (i_1, \dots, i_p) \in C(n,p)$, *posons* $A_\sigma = a_{i_1} \wedge \cdots \wedge a_{i_p}$. *Alors*
(i) $(A_\sigma)_{\sigma \in C(n,p)}$ *est une base de* $\mathbb{R}^n_p$,
(ii) Si $\det(a_1, \dots, a_n) = 1$ *alors* $\det(A_\sigma)_{\sigma \in C(n,p)} = 1$,
(iii) Si $(a_1^*, \dots, a_n^*)$ *est la base duale de* $(a_1, \dots, a_n)$, *et si pour* $\sigma = (i_1, \dots, i_p) \in C(n,p)$, *nous posons* $A_\sigma^* = a_{i_1}^* \wedge \cdots \wedge a_{i_p}^*$, *alors* $(A_\sigma^*)_{\sigma \in C(n,p)}$ *est la base duale de* $(A_\sigma)_{\sigma \in C(n,p)}$.

PREUVE : Les points (i) et (ii) sont une conséquence immédiate du Lemme 1.2.8. Quant au point (iii), il résulte de l'identité de Laplace (Lemme 1.2.7). ■

Nous avons à ce stade tous les outils nécessaires pour expliciter la construction dont nous parlions en introduisant cette section.

1.2.2 Les parallélépipèdes composés de Mahler

Nous conservons ici toutes les notations du dernier lemme de la section précédente, et de la remarque précédant la Définition 1.1.13.

Définition 1.2.10 *Au parallélépipède* $\Pi(a_1, \dots, a_n)$ *de* $\mathbb{R}^n$ *on associe le p-ième* PARALLÉLÉPIPÈDE COMPOSÉ DE MAHLER $\Pi^{(p)} = \Pi((A_\sigma)_{\sigma \in C(n,p)})$, *à savoir l'ensemble*

$$\{X \in \mathbb{R}^n_p \mid |A_\sigma.X| \leq 1, \text{ pour } \sigma \in C(n,p)\} .$$

Si nous connaissons $\lambda_1(\Pi), \dots, \lambda_n(\Pi)$ et $g_1(\Pi), \dots, g_n(\Pi)$, que pouvons-nous dire des quantités correspondantes pour $\Pi^{(p)}$? La réponse est l'objet du théorème de Mahler qui suit. Toutefois nous avons besoin de quelques notations préalables.

Définition 1.2.11 *Si* $\lambda_1, \dots, \lambda_n$ *sont les minima successifs de* $\Pi = \Pi(a_1, \dots, a_n)$, *nous définissons pour* $\sigma \in C(n,p)$,

$$\lambda_\sigma = \prod_{k=1}^{p} \lambda_{i_k} .$$

En outre nous supposons que $C(n,p)$ *est ordonné de sorte que l'application* $\tau \mapsto \lambda_\tau$ *est croissante. Ses éléments peuvent alors s'écrire* $\lambda_{\tau_i}, 1 \leq i \leq l$ *(rappelons que* $l = C_n^p$*). Si* $g_i = g_i(\Pi)$ *pour* $i = 1, \dots, n$, *nous définissons enfin pour* $\sigma = (i_1, \dots, i_p) \in C(n,p)$,

$$G_\sigma = g_{i_1} \wedge \cdots \wedge g_{i_p} .$$

Remarquons qu'un ordre sur $C(n,p)$ satisfaisant les exigences de la définition ci-dessus n'est pas forcément unique, puisqu'en général l'application $\tau \mapsto \lambda_\tau$ n'est pas injective. Nous pouvons maintenant énoncer le théorème.

Théorème 1.2.12 (MAHLER) *Soit* $\Pi = \Pi(a_1, \dots, a_n)$ *un parallélépipède de minima successifs* $\lambda_1 < \cdots < \lambda_n$ *avec* $g_i = g_i(\Pi)$ *pour* $i = 1, \dots, n$ *(cf. Lemme 1.1.4). Considérons le p-ième*

parallélépipède composé de Mahler $\Pi^{(p)} = \Pi((A_\sigma)_{\sigma\in C(n,p)})$*, et notons* $\nu_1, \dots, \nu_l$ *ses minima successifs. Avec les notations de la Définition 1.2.11, nous avons*

$$\forall(\sigma,\tau) \in C(n,p)\times C(n,p),\ |A_\sigma.G_\tau| \leq p!\lambda_\tau\,, \tag{1.13}$$

et

$$\forall i = 1,\dots,l,\ \lambda_{\tau_i} \ll \nu_i \ll \lambda_{\tau_i}\,, \tag{1.14}$$

où les constantes ne dépendent que de n*.*

PREUVE : L'identité de Laplace nous montre que pour $(\sigma,\tau) \in C(n,p)\times C(n,p)$:

$$\begin{array}{rcl} |A_\sigma.G_\tau| & = & |\det(a_{i_k}.g_{j_l})_{1\leq k,l\leq p}| \\ & \leq & \sum_{s\in\mathfrak{S}_p} |\prod_{k=1}^p a_{i_k}.g_{j_l}| \\ & \leq & \sum_{s\in\mathfrak{S}_p} \lambda_{i_1}\dots\lambda_{i_p} \text{ car } |a_{i_k}.g_{j_l}| \leq \lambda_{j_l} \\ & \leq & p!\lambda_\tau\,. \end{array}$$

Cela prouve l'assertion (1.13). Observons qu'alors les $(G_\tau)_{\tau\in C(n,p)}$ constituent l vecteurs entiers indépendants contenus dans le parallélépipède $p!\lambda_{\tau_i}\Pi^{(p)}$ d'après (1.13). Nous en concluons que $\nu_i \leq p!\lambda_{\tau_i}$ pour $i = 1,\dots,l$.
Puisque d'autre part nous avons $\prod_{i=1}^l \lambda_{\tau_i} = (\lambda_1\dots\lambda_n)^t \ll 1$, où $t = C_{n-1}^{p-1}$, ainsi que $\nu_1\dots\nu_l \gg 1$, nous pouvons en déduire que $\lambda_{\tau_i} \ll \nu_i$ pour $i = 1,\dots,l$. Ceci achève de prouver l'assertion (1.14). ■

Chapitre 2

Lemmes polynomiaux et théorie de l'indice

Nous avons regroupé dans ce chapitre la plupart des outils polynomiaux utilisés dans la preuve du théorème des sous-espaces. Dans la première section, nous donnons des conditions pour qu'un polynôme s'annule sur un produit de sous-espaces vectoriels, puis quelques lemmes et définitions qui seront utiles dans la section suivante, où nous présentons deux notions d'indice (qui généralisent la notion bien connue d'ordre d'une racine). Les deux dernières sections donnent des résultats de majoration, puis de minoration de ces indices.

2.1 Un lemme d'annulation

Commençons par introduire une notation commode.

Définition 2.1.1 *Soit $n \geq 1$ et $s \geq 1$ deux entiers, ainsi que $1 \leq q \leq n-1$. Soient également $(w_1, \ldots, w_q) \in (\mathbb{R}^n)^q$. Le* GRILLAGE *de taille s et de base $(w_1, \ldots, w_q)$ est l'ensemble :*

$$\Gamma(s, w_1, \ldots, w_q) = \left\{ \sum_{i=1}^{q} h_i w_i \mid 1 \leq h_i \leq s \text{ pour } i = 1, \ldots, q \right\}.$$

$\Gamma(s, w_1, \ldots, w_q)$ est un grillage sur un sous-espace vectoriel H de $\mathbb{R}^n$ si de plus $H = \mathbb{R}w_1 \oplus \cdots \oplus \mathbb{R}w_q$.

Nous allons montrer en deux étapes le résultat suivant : un polynôme de degré convenable en m blocs de n variables s'annule sur un produit de m sous-espaces vectoriels de $\mathbb{R}^n$ dès que lui et ses dérivées d'ordre suffisamment grand s'annulent sur un produit de grillages sur ces sous-espaces. Pour cela, nous commençons par traiter le cas d'un seul bloc. Dans la suite, nous identifions polynômes et fonctions polynômes chaque fois que cela est nécessaire.

Lemme 2.1.2 *Soit $P(X_1,\dots,X_n)\in\mathbb{R}[X_1,\dots,X_n]$, r un entier avec $\deg P\le r$, $s\in\mathbb{N}^*$, Γ un grillage de taille s sur un sous-espace vectoriel de dimension $1\le q\le n-1$ et $t\in\mathbb{N}$ tel que $s(t+1)>r$. Supposons que*

$$\frac{\partial^{t_1+\cdots+t_n}}{\partial {X_1}^{t_1}\dots\partial {X_n}^{t_n}}P\equiv 0 \text{ sur } \Gamma \text{ pour } t_1+\cdots+t_n\le t\,.$$

Alors $P\equiv 0$ sur H.

Preuve : Notons $(e_1,\dots,e_n)$ la base canonique de $\mathbb{R}^n$. Nous commençons par nous ramener au cas où $\tilde\Gamma=\Gamma(s,e_1,\dots,e_q)$ et $H=\mathbb{R}e_1\oplus\cdots\oplus\mathbb{R}e_q$.

Soit $\Gamma(s,w_1,\dots,w_q)$ le grillage donné sur H. Comme $\mathbb{R}^n=H\oplus H^\perp$, si $(w_{q+1},\dots,w_n)$ est une base de $H^\perp$, $(w_1,\dots,w_n)$ est une base de $\mathbb{R}^n$. Soit u l'élément de $Gl_n(\mathbb{R})$ tel que $u(w_i)=e_i$ pour $i=1,\dots,n$. Le groupe $Gl_n(\mathbb{R})$ agit sur $\mathbb{R}[X_1,\dots,X_n]$ par :

$$\begin{array}{ccc} Gl_n(\mathbb{R})\times\mathbb{R}[X_1,\dots,X_n] & \longrightarrow & \mathbb{R}[X_1,\dots,X_n] \\ (v,P) & \longmapsto & v*P=P\circ v^{-1}\,, \end{array}$$

et u envoie Γ sur $\tilde\Gamma=\Gamma(s,e_1,\dots,e_q)$ et H sur $(\mathbb{R}e_{q+1}\oplus\cdots\oplus\mathbb{R}e_n)^\perp$. Les deux faits suivants

$$P \text{ s'annule sur } \Gamma \Longleftrightarrow u*P \text{ s'annule sur } u(\Gamma)\,, \tag{2.1}$$

$$u*\frac{\partial^{t_1+\cdots+t_n}}{\partial {X_1}^{t_1}\dots\partial {X_n}^{t_n}}P=\frac{\partial^{t_1+\cdots+t_n}}{\partial {X_1}^{t_1}\dots\partial {X_n}^{t_n}}(u*P)\,, \tag{2.2}$$

montrent que si le lemme est vrai avec $\tilde\Gamma$ et $\mathbb{R}e_1\oplus\cdots\oplus\mathbb{R}e_q$, il est alors vrai pour Γ et H.

Nous supposons donc dans la suite que $\Gamma=\tilde\Gamma$ et $H=\mathbb{R}e_1\oplus\cdots\oplus\mathbb{R}e_q$. Nous devons donc prouver que $Q(X_1,\dots,X_q)=P(X_1,\dots,X_q,0,\dots,0)$, de degré au plus r, est nul si ses dérivées d'ordre au plus t avec $s(t+1)>r$ s'annulent sur les s^q points entiers $(h_1,\dots,h_q),1\le h_i\le s$. Procédons par récurrence sur q. Si $q=1$, le polynôme $Q^{(l)}(X_1)$ s'annulant en $1,\dots,s$ pour $0\le l\le t$, on en déduit que $Q(X_1)$ a au moins $s(t+1)>r$ zéros, compte tenu des multiplicités. Donc $Q(X_1)=0$ puisque Q est de degré au plus r. Supposons maintenant le résultat vrai jusqu'à $q-1$ et montrons-le pour $q\ge 2$. Pour $1\le h\le s$, désignons par e_h le plus grand entier tel que $(X_1-h)^{e_h}$ divise Q. Nous pouvons alors écrire

$$Q(X_1,\dots,X_q)=R(X_1,\dots,X_q)\prod_{h=1}^{s}(X_1-h)^{e_h}\,. \tag{2.3}$$

Il s'agit alors de prouver que $e\overset{def}{=}\min\{e_1,\dots,e_s\}\ge t+1$, et le cas déjà traité d'une variable donnera la conclusion. Supposons donc au contraire que $e\le t$, par exemple $e=e_1$. En dérivant (2.3) e_1 fois par rapport à X_1 et en évaluant en $(1,X_2,\dots,X_q)$, nous trouvons

$$\frac{\partial^{e_1}}{\partial {X_1}^{e_1}}Q(X_1,\dots,X_q)_{|X_1=1}=e!R(1,X_2,\dots,X_q)\prod_{h=2}^{s}(1-h)^{e_h}\,. \tag{2.4}$$

$R(1, X_2, \dots, X_q)$ est proportionnel à $\frac{\partial^{e_1}}{\partial {X_1}^{e_1}} Q(X_1, \dots, X_q)_{|X_1=1}$, de degré total inférieur à $r - se$ à $q-1$ variables, et (2.4) dit que ses dérivées d'ordre au plus $t-e$ s'annulent sur les s^{q-1} points entiers $(h_2, \dots, h_s), 1 \leq h_i \leq s$.

Par hypothèse de récurrence, puisque $s(t-e+1) = s(t+1) - se > r - se$, le polynôme $R(1, X_2, \dots, X_q)$ est nul, donc $(X_1-1)^{e+1}$ divise $Q(X_1, \dots, X_q)$. C'est impossible par définition de $e = e_1$, et ce dernier est donc nul, ce qui montre le lemme. ■

Nous pouvons maintenant traiter le cas de m blocs.

Lemme 2.1.3 *Soit $P \in \mathbb{R}[(X_{h1}, \dots, X_{hn})_{h=1,\dots,m}]$ de degré au plus r_h en les variables $X_{h1}, \dots, X_{hn}$ pour $h = 1, \dots, m$. Soient $\Gamma_1, \dots, \Gamma_m$ des grillages sur des sous-espaces vectoriels $H_1, \dots, H_m$ de $\mathbb{R}^n$ de dimensions respectives $q_1, \dots, q_m$ comprises entre 1 et $n-1$, c'est-à-dire :*

$$\Gamma_h = \Gamma(s_h, w_1^{(h)}, \dots, w_{q_h}^{(h)}) \text{ si } H_h = \mathbb{R}w_1^{(h)} \oplus \dots \oplus \mathbb{R}w_{q_h}^{(h)},\ s_h \in \mathbb{N}^* .$$

Soient $t_1, \dots, t_m$ des entiers avec $s_h(t_h+1) > r_h,\ h = 1, \dots, m$, et posons enfin

$$H = \prod_{h=1}^{m} H_h \text{ et } \Gamma = \prod_{h=1}^{m} \Gamma_h .$$

Supposons que pour

$$\mathcal{I} = (t_{11}, \dots, t_{1n}; \dots; t_{m1}, \dots, t_{mn}) \text{ avec } \sum_{i=1}^{n} t_{hi} \leq t_h,\ h = 1, \dots, m ,$$

nous ayons

$$P^{\mathcal{I}} \stackrel{def}{=} \frac{\partial^{t_{11}+\dots+t_{mn}}}{\partial {X_{11}}^{t_{11}} \dots \partial {X_{mn}}^{t_{mn}}} P \equiv 0 \text{ sur } \Gamma .$$

Alors $P \equiv 0$ sur H.

Preuve : Lorsque $m = 1$, c'est le lemme précédent. Supposons le résultat vrai jusqu'au rang $m-1$ et montrons-le pour $m \geq 2$. Pour $(\underline{x}_1, \dots, \underline{x}_{m-1})$ arbitraire dans $\Gamma_1 \times \dots \times \Gamma_{m-1}$, le Lemme 2.1.2 dit que :

$$Q(X_{m1}, \dots, X_{mn}) = P(\underline{x}_1, \dots, \underline{x}_{m-1}; X_{m1}, \dots, X_{mn})$$

s'annule sur H_m. Pour $\underline{x} \in H_m$, l'hypothèse de récurrence dit que :

$$Q_{\underline{x}}(\underline{X}_1, \dots, \underline{X}_{m-1}) = P(\underline{X}_1, \dots, \underline{X}_{m-1}, \underline{x})$$

s'annule sur $H_1 \times \dots \times H_{m-1}$ donc $P \equiv 0$ sur H ($\underline{X}_h$ désigne bien sûr le bloc de variables $(X_{h1}, \dots, X_{hn})$). ■

Dans les sections suivantes nous travaillerons constamment avec des polynômes en m blocs de n variables. Pour rendre plus concis les énoncés, il est utile d'introduire des notations efficaces.

Définition 2.1.4 *Nous désignerons toujours par $\mathcal{A}$ la $\mathbb{R}$-algèbre des polynômes en les nm variables ($n \geq 1, m \geq 1$)*

$$X_{11}, \dots, X_{1n}; X_{21}, \dots, X_{2n}; \cdots; X_{m1}, \dots, X_{mn}\,.$$

Nous écrirons souvent un élément P de $\mathcal{A}$ sous la forme

$$P(\underline{X}_1, \dots, \underline{X}_m) = \sum a(\underline{I}_1, \dots, \underline{I}_m) {\underline{X}_1}^{\underline{I}_1} \dots {\underline{X}_m}^{\underline{I}_m}$$

où $\underline{I}_k$ est un multi-indice de longueur n, et ${\underline{X}_k}^{\underline{I}_k}$ a le sens habituel.
Pour $P \in \mathcal{A}$, $H(P)$ désigne le maximum des valeurs absolues des coefficients de P. Par $\mathcal{I}$, nous entendrons toujours un multi-indice du type $(i_{11}, \dots, i_{1n}; \cdots; i_{m1}, \dots, i_{mn})$ que nous écrirons parfois $(\underline{I}_1, \dots, \underline{I}_m)$. Avec ces notations, nous posons

$$P^{\mathcal{I}} = \frac{1}{i_{11}! \dots i_{mn}!} \frac{\partial^{i_{11}+\dots+i_{mn}}}{\partial {X_{11}}^{i_{11}} \dots \partial {X_{mn}}^{i_{mn}}} P\,. \tag{2.5}$$

La notation $\underline{r}$ désignera toujours le m-uplets d'entiers strictement positifs $r_1, \dots, r_m$, et, $\mathcal{I}$ et $\underline{r}$ étant donnés,

$$(\mathcal{I}/\underline{r}) = \sum_{h=1}^{m} \frac{i_{h1} + \dots + i_{hn}}{r_h}\,. \tag{2.6}$$

Le lemme suivant nous donne une estimation de $H(P^{\mathcal{I}})$ en fonction de $H(P)$ lorsque P a des coefficients entiers.

Lemme 2.1.5 *Soit $P \in \mathbb{Z}[\underline{X}_1, \dots, \underline{X}_m]$ homogène en $\underline{X}_h$ de degré r_h pour $1 \leq h \leq m$. Alors pour tout $\mathcal{I}$,*
(i) $P^{\mathcal{I}} \in \mathbb{Z}[\underline{X}_1, \dots, \underline{X}_m]$,
(ii) $H(P^{\mathcal{I}}) \leq 2^{r_1+\dots+r_m} H(P)$.

PREUVE : Pour (i), il suffit de vérifier que $\frac{1}{i_{hk}!} \frac{\partial^{i_{hk}}}{\partial {X_{hk}}^{i_{hk}}} P \in \mathbb{Z}[\underline{X}_1, \dots, \underline{X}_m]$ car les dérivations sont linéaires et commutent.
Pour (ii), il suffit, par linéarité, de vérifier le résultat pour les monômes. Or si $\mathcal{J} = (\underline{J}_1, \dots, \underline{J}_m)$,

$$\left({\underline{X}_1}^{\underline{J}_1} \dots {\underline{X}_m}^{\underline{J}_m}\right)^{\mathcal{I}} = \binom{j_{11}}{i_{11}} \dots \binom{j_{mn}}{i_{mn}} {\underline{X}_1}^{(\underline{J}-\underline{I})_1} \dots {\underline{X}_m}^{(\underline{J}-\underline{I})_m}\,,$$

et le produit de coefficients binomiaux se majore par $2^{r_1+\dots+r_m}$ grâce à l'homogénéité de P. ■

Nous aurons besoin d'une notion de hauteur pour les éléments du corps $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ où $\alpha_1, \dots, \alpha_n$ sont des entiers algébriques réels.

Définition 2.1.6 *Soient $\alpha_1, \dots, \alpha_n$ des entiers algébriques réels, $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ et $d = [K : \mathbb{Q}]$. Il existe une base d'entiers $\beta_1, \dots, \beta_d$ de $K/\mathbb{Q}$, et sa table de multiplication $\beta_i\beta_j = \sum_{k=1}^{d} c_{ijk}\beta_k$. Posons $C = \max_{1\le i,j,k\le d} |c_{ijk}|$. Pour $\gamma \in K$, il existe $(x_1, \dots, x_d) \in \mathbb{Q}^d$ tels que $\gamma = x_1\beta_1 + \cdots + x_d\beta_d$. Nous posons alors :*

$$H(\gamma) = Cd^2 \max_{1\le j\le q} |x_j| .$$

La constante Cd^2 a été placée devant le max pour que le lemme suivant soit vrai.

Lemme 2.1.7 *Avec les notations de la Définition 2.1.6, pour $(\gamma, \delta) \in K^2$,*
(i) $H(\gamma + \delta) \le H(\gamma) + H(\delta)$,
(ii) $H(\gamma\ \delta) \le H(\gamma)\ H(\delta)$.

Pour certains $\mathcal{I}$, nous associons maintenant aux polynômes $P^{\mathcal{I}}$ et aux entiers algébriques $\alpha_1, \dots, \alpha_n$, des polynômes $P^*_{\mathcal{I}}$ qui nous serviront dans la section 2.3.

Définition 2.1.8 *Soit $P \in \mathcal{A}$ homogène de degré r_h en $\underline{X}_h$ pour $1 \le h \le m$. Avec les notations de la Définition 2.1.6, nous posons :*

$$\begin{aligned} &P^*_{\mathcal{I}}(X_{12}, \dots, X_{1n}; \cdots; X_{m2}, \dots, X_{mn}) = \\ &P^{\mathcal{I}}(-\alpha_2 X_{12} - \cdots - \alpha_n X_{1n}; \alpha_1 X_{12}, \dots, \alpha_1 X_{1n}; \cdots; \\ &\qquad -\alpha_2 X_{m2} - \cdots - \alpha_n X_{mn}; \alpha_1 X_{m2}, \dots, \alpha_1 X_{mn}) \text{ si} \\ &\mathcal{I} = (i_1, 0, \dots, 0; \cdots; i_m, 0, \dots, 0) . \end{aligned}$$

Ces polynômes possèdent les sympathiques propriétés suivantes.

Lemme 2.1.9 *Avec les notations de la Définition 2.1.8,*
(i) les coefficients de $P^*_{\mathcal{I}}$ sont des formes linéaires en les coefficients de P ;
(ii) les coefficients γ de ces formes linéaires sont des entiers algébriques de K ;
(iii) ces coefficients γ satisfont :

$$H(\gamma) \le (4^n B)^{r_1+\cdots+r_m} \text{ où } B = \max_{1\le i\le n} |\alpha_i| .$$

Preuve : Il s'agit du Lemme 5B de [Sch1], p. 174. Justifions rapidement (i) et (ii). $Q = P^{\mathcal{I}}$ a des coefficients qui sont des mutiples entiers des coefficients de P. Si nous écrivons Q sous la forme indiquée dans la Définition 2.1.4, nous constatons que le passage de Q à $P^*_{\mathcal{I}}$ se fait en remplaçant $\underline{X}_1, \dots, \underline{X}_m$ par $\underline{Y}_1, \dots, \underline{Y}_m$ où les $\underline{Y}_h$ sont linéaires en les composantes de $\underline{X}_h$ pour $h = 1, \dots, m$.
Montrons maintenant (iii). Par homogénéité de P, le nombre de termes de $P^*_{\mathcal{I}}$ est au plus le produit des nombres de n-uplets d'entiers positifs de somme r_h pour $h = 1, \dots, m$, à savoir, d'après le Lemme B de l'Appendice :

$$\binom{r_1 + n - 1}{n - 1} \cdots \binom{r_m + n - 1}{n - 1} \le 2^{n(r_1+\cdots+r_m)} .$$

Une analyse attentive montre que ces termes sont du type

$$\pm c(\mathcal{J})\binom{j_{11}}{i_1}\dots\binom{j_{m1}}{i_m}S_1\dots S_m,\ \text{où}$$

$$S_h=(\alpha_2X_{h2}+\dots+\alpha_nX_{hn})^{j_{h1}-i_h}(\alpha_1X_{h2})^{j_{h2}}\dots(\alpha_1X_{hn})^{j_{hn}},\ \text{pour } h=1,\dots,m\,.$$

La formule du multinôme montre que chaque coefficient de S_h est formé d'un produit de factorielles qui se majore par

$$(n-1)^{j_{h1}-i_h}<n^{r_h}\,,$$

et d'un monôme en $\alpha_1,\dots,\alpha_n$ qui se majore par B^{r_h}. Comme le produit de coefficients binomiaux en facteur de $S_1\dots S_m$ se majore par $2^{r_1+\dots+r_m}$, au total $H(\gamma)$ est borné par

$$2^{n(r_1+\dots+r_m)}2^{r_1+\dots+r_m}\prod_{h=1}^{m}n^{r_h}B^{r_h}=(4^nB)^{r_1+\dots+r_m}\,,$$

ce qu'il fallait démontrer. ■

2.2 Deux notions d'indice

Lorsqu'il a démontré son théorème en 1955 (cf. [Rot]), Roth a introduit la notion d'indice d'un polynôme par rapport à un point, puis Schmidt l'a généralisée en une notion d'indice par rapport à un ensemble de formes linéaires. Nous commencerons par présenter la dernière citée qui est plus agréable à manipuler, puis la première qui demeure tout de même fondamentalement utile comme nous le verrons dans la dernière section de ce chapitre.

2.2.1 L'indice de Schmidt

Définition 2.2.1 *Donnons-nous m formes linéaires*

$$L_h=\alpha_{h1}X_{h1}+\dots+\alpha_{hn}X_{hn},\ 1\le h\le m$$

à coefficients dans $\mathbb{R}$, non identiquement nulles, et $\underline{r}\in\mathbb{N}^m$. Pour c réel positif, désignons par $\mathcal{I}(c)$ l'ideal de $\mathcal{A}$ engendré par les polynômes

$$L_1{}^{i_1}\dots L_m{}^{i_m},\ \text{où}\ \frac{i_1}{r_1}+\dots+\frac{i_m}{r_m}\ge c,$$

de sorte que $\mathcal{I}(0)=\mathcal{A}$, et que l'application $c\mapsto\mathcal{I}(c)$ est décroissante. Nous pouvons donc poser, pour $P\in\mathcal{A}\setminus\{0\}$,

$$\mathrm{Ind}\,(P,L_1,\dots,L_m,r_1,\dots,r_m)=\mathrm{Ind}\,(P,\underline{L},\underline{r})=\max\{c\ge0\mid P\in\mathcal{I}(c)\}\,.$$

Remarque 2.2.2 *La définition a un sens car si $P \in \mathcal{I}(c)$, le degré de P est minoré par c, donc c est majoré. On convient que* $\mathrm{Ind}\,(0, \underline{L}, \underline{r}) = +\infty$.

Il existe une définition équivalente qui est souvent utile. Puisque les formes linéaires sont non identiquement nulles, nous pouvons supposer que

$$L_1, X_{12}, \dots, X_{1n}; \cdots; L_m, X_{m2}, \dots, X_{mn}$$

sont algébriquement libres sur $\mathbb{R}$.

Lemme 2.2.3 *Soit $P \in \mathcal{A} \setminus \{0\}$. Ecrivons (de façon unique)*

$$P = \sum_{\underline{j}} a_{\underline{j}} \underline{L}^{\underline{j}} \ ,$$

où $a_{\underline{j}}$ est un polynôme en les variables $X_{12}, \dots, X_{1n}; \cdots; X_{m2}, \dots, X_{mn}$ nul pour presque tout $\underline{j}$. Alors

$$\mathrm{Ind}\,(P, \underline{L}, \underline{r}) = \min\left\{c \in \mathbb{N} \mid \exists \underline{j} \in \mathbb{N}^m \text{ avec } a_{\underline{j}} \neq 0 \text{ et } \sum_{h=1}^{m} \frac{j_h}{r_h} = c\right\}.$$

PREUVE : Soit $\gamma = \mathrm{Ind}\,(P, \underline{L}, \underline{r})$. Par définition, il est possible d'écrire

$$P = \sum_{\underline{j}} a'_{\underline{j}} \underline{L}^{\underline{j}} \ , \text{ où } \sum_{h=1}^{m} \frac{j_h}{r_h} \geq \gamma\,.$$

Par unicité de la décomposition énoncée dans le lemme précédent, $a_{\underline{j}}$ est nul dans celle-ci pour tout $\underline{j}$ tel que $\sum_{h=1}^{m} \frac{j_h}{r_h} < \gamma$. Donc le minimum du membre de droite est au moins γ. Par ailleurs, soit c_0 réalisant ce minimum, alors $P \in \mathcal{I}(c_0)$, donc $c_0 \leq \gamma$, ce qui prouve le lemme. ■

Une fois ce lemme montré, il n'est pas difficile de voir que l'indice se comporte bien avec la somme et le produit de polynômes.

Lemme 2.2.4 *Soient $(P, Q) \in \mathcal{A} \setminus \{0\} \times \mathcal{A} \setminus \{0\}$. Alors*
(i) $\mathrm{Ind}\,(P+Q, \underline{L}, \underline{r}) \geq \min\{\mathrm{Ind}\,(P, \underline{L}, \underline{r}), \mathrm{Ind}\,(Q, \underline{L}, \underline{r})\}$,
(ii) $\mathrm{Ind}\,(PQ, \underline{L}, \underline{r}) = \mathrm{Ind}\,(P, \underline{L}, \underline{r}) + \mathrm{Ind}\,(Q, \underline{L}, \underline{r})$.

PREUVE : (i) résulte de la décroissance de $c \mapsto \mathcal{I}(c)$ que nous évoquions plus haut.
(ii) s'obtient en écrivant $P = P_1 + P_2$ et $Q = Q_1 + Q_2$ où

$$P_1 = \sum_{\underline{j} \in \mathcal{E}_1} a_{\underline{j}} \underline{L}^{\underline{j}}, \ , Q_1 = \sum_{\underline{j} \in \mathcal{E}_2} b_{\underline{j}} \underline{L}^{\underline{j}}, \ P_2 = P - P_1, \ Q_2 = Q - Q_1 \text{ et}$$

$$\mathcal{E}_1 = \left\{\underline{j} \in \mathbb{N}^m \mid \sum_{h=1}^{m} \frac{j_h}{r_h} = \mathrm{Ind}\,(P, \underline{L}, \underline{r})\right\}, \quad \mathcal{E}_2 = \left\{\underline{j} \in \mathbb{N}^m \mid \sum_{h=1}^{m} \frac{j_h}{r_h} = \mathrm{Ind}\,(Q, \underline{L}, \underline{r})\right\}.$$

En effet, il vient alors $PQ = P_1Q_1 + P_1Q_2 + P_2Q_1 + P_2Q_2$ et le Lemme 2.2.3 montre que P_1Q_1 a pour indice $\mathrm{Ind}\,(P, \underline{L}, \underline{r}) + \mathrm{Ind}\,(Q, \underline{L}, \underline{r})$, alors que les autres termes ont un indice strictement supérieur à $\mathrm{Ind}\,(P, \underline{L}, \underline{r}) + \mathrm{Ind}\,(Q, \underline{L}, \underline{r})$. L'assertion (i) montre donc que $\mathrm{Ind}\,(PQ, \underline{L}, \underline{r}) = \mathrm{Ind}\,(P_1Q_1, \underline{L}, \underline{r}) = \mathrm{Ind}\,(P, \underline{L}, \underline{r}) + \mathrm{Ind}\,(Q, \underline{L}, \underline{r})$. ■

Nous terminons cette section par deux applications utiles de la notion d'indice.

Lemme 2.2.5 *Soient $P \in \mathcal{A} \setminus \{0\}$ et $\mathcal{I}$ un multi-indice (voir Définition 2.1.4). Alors*
(i) $\mathrm{Ind}\,(P^{\mathcal{I}}, \underline{L}, \underline{r}) \geq \mathrm{Ind}\,(P, \underline{L}, \underline{r}) - (\mathcal{I}/\underline{r})$,
(ii) si $(\mathcal{I}/\underline{r}) < \mathrm{Ind}\,(P, \underline{L}, \underline{r})$, $P^{\mathcal{I}}$ est identiquement nul sur le sous-espace de $\mathbb{R}^{mn}$ formé des zéros communs à $L_1, \ldots, L_m$.

Preuve : Nous écrivons

$$P = \sum_{\mathcal{J}} c(\mathcal{J}) {L_1}^{j_{11}} {X_{12}}^{j_{12}} \ldots {X_{1n}}^{j_{1n}} \ldots {L_m}^{j_{m1}} {X_{m2}}^{j_{m2}} \ldots {X_{mn}}^{j_{mn}},\ \sum_{h=1}^{m} \frac{j_{h1}}{r_h} \geq \mathrm{Ind}\,(P, \underline{L}, \underline{r})\,,$$

pour constater que $P^{\mathcal{I}}$ appartient à l'idéal engendré par les polynômes

$$ {L_1}^{j_{11} - i_{11} - \cdots - i_{1n}} \ldots {L_m}^{j_{m1} - i_{m1} - \cdots - i_{mn}},\ \text{avec}$$

$$\frac{j_{11} - i_{11} - \cdots - i_{1n}}{r_1} + \cdots + \frac{j_{m1} - i_{m1} - \cdots - i_{mn}}{r_m} \geq \mathrm{Ind}\,(P, \underline{L}, \underline{r}) - (\mathcal{I}/\underline{r})\,.$$

Cela montre que $\mathrm{Ind}\,(P^{\mathcal{I}}, \underline{L}, \underline{r}) \geq \mathrm{Ind}\,(P, \underline{L}, \underline{r}) - (\mathcal{I}/\underline{r})$ donc (i) est vrai.
Supposons que $(\mathcal{I}/\underline{r}) < \mathrm{Ind}\,(P, \underline{L}, \underline{r})$. Alors $\mathrm{Ind}\,(P^{\mathcal{I}}, \underline{L}, \underline{r}) > 0$ d'après (i), et il résulte alors du Lemme 2.2.3 que chaque terme de $P^{\mathcal{I}}$ est nul ou divisible par l'une des formes $L_1, \ldots, L_m$. Donc $P^{\mathcal{I}}$ est identiquement nul sur l'ensemble des zéros communs à ces formes, comme demandé en (ii). ■

Lemme 2.2.6 *Soit $\mathcal{Z}$ le sous-espace des zéros communs à $L_1, \ldots, L_m$, et $P \in \mathcal{A} \setminus \{0\}$.*
(i) Il existe $\mathcal{I}$ avec $(\mathcal{I}/\underline{r}) = \mathrm{Ind}\,(P, \underline{L}, \underline{r})$ tel que $P^{\mathcal{I}}$ n'est pas identiquement nul sur $\mathcal{Z}$,
(ii) si l'hypothèse précédant le Lemme 2.2.3 est satisfaite, c'est-à-dire $\alpha_{h1} \neq 0$ pour $h = 1, \ldots, m$, il existe un tel $\mathcal{I}$ du type

$$\mathcal{I} = (i_1, 0, \ldots, 0; \cdots; i_m, 0, \ldots, 0)\,.$$

Preuve : Nous montrons simultanément (i) et (ii) en supposant directement que $\alpha_{h1} \neq 0$ pour $h = 1, \ldots, m$, et en écrivant

$$P = \sum_{\underline{j'}} a_{\underline{j'}} \underline{L}^{\underline{j'}}.$$

Choisissons $\underline{j} = (j_1, \ldots, j_m)$ tel que $\frac{j_1}{r_1} + \cdots + \frac{j_m}{r_m} = \mathrm{Ind}\,(P, \underline{L}, \underline{r})$ et $a_{\underline{j}} \neq 0$, ce qui est toujours possible d'après le Lemme 2.2.3. Si nous posons maintenant

$$\mathcal{I} = (j_1, 0, \ldots, 0; \cdots; j_m, 0, \ldots, 0)\,,$$

alors $P^{\mathcal{I}}$ n'est pas identiquement nul sur $\mathcal{Z}$, car $a_{\underline{j'}}$ ne comporte pas la variable X_{h1} pour $h = 1, \ldots, m$ donc

$$P^{\mathcal{I}} = \sum_{\underline{j'}} a_{\underline{j'}} (\underline{L}^{\underline{j'}})^{\mathcal{I}} .$$

Or $a_{\underline{j}} \neq 0$ par choix de $\underline{j}$, et $(\underline{L}^{\underline{j}})^{\mathcal{I}}$ est une constante non nulle. ■

2.2.2 L'indice de Roth

Il s'agit simplement ici de donner la définition et un lemme qui montre le lien avec l'indice de Schmidt.

Définition 2.2.7 *Pour $P(X_1, \ldots, X_m) \in \mathbb{Z}[X_1, \ldots, X_m]$ et $I = (i_1, \ldots, i_m) \in \mathbb{N}^m$, nous posons à nouveau*

$$P^I = \frac{1}{i_1! \ldots i_m!} \frac{\partial^{i_1 + \cdots + i_m}}{\partial {X_1}^{i_1} \ldots \partial {X_m}^{i_m}} P$$

L'indice de Roth de P en $\underline{\alpha} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{R}^m$ par rapport à $\underline{r}$ est

$$i(P, \underline{\alpha}, \underline{r}) = \inf \left\{ \frac{i_1}{r_1} + \cdots + \frac{i_m}{r_m} \mid I = (i_1, \ldots, i_m) \text{ et } P_I(\underline{\alpha}) \neq 0 \right\}$$

Remarquons que si $m = 1$, $P \in \mathbb{R}[X_1]$, $r_1 = 1$, $\alpha_1 \in \mathbb{R}$ alors $i(P, \alpha_1, r_1)$ n'est autre que l'ordre de α_1 comme racine de P. Le lemme qui suit montre le lien entre l'indice de Roth et l'indice de Schmidt.

Lemme 2.2.8 *Soit $P(X_1, \ldots, X_m)$ un polynôme de degré au plus r_h en X_h pour $1 \leq h \leq m$, et $(\alpha_1, \ldots, \alpha_m) \in \mathbb{R}^m$. Alors*

$$i(P, \underline{\alpha}, \underline{r}) = \mathrm{Ind}\,(\hat{P}, \underline{L}, \underline{r}) ,$$

où $L_h = X_{h1} - \alpha_h X_{h2}$ pour $h = 1, \ldots, m$ et $\hat{P}$ est le polynôme obtenu à partir de P en remplaçant formellement ${X_h}^{i_h}$ par ${X_{h1}}^{i_h} {X_{h2}}^{r_h - i_h}$ pour $0 \leq i_h \leq r_h$ et $1 \leq h \leq m$.

Preuve : En écrivant la formule de Taylor au point $(\alpha_1, \ldots, \alpha_m)$, soit :

$$P(X_1, \ldots, X_m) = \sum_{\underline{j}} c(j_1, \ldots, j_m)(X_1 - \alpha_1)^{j_1} \ldots (X_m - \alpha_m)^{j_m} ,$$

nous nous apercevons que

$$i(P, \underline{\alpha}, \underline{r}) = \min \left\{ \frac{j_1}{r_1} + \cdots + \frac{j_m}{r_m} \mid c(j_1, \ldots, j_m) \neq 0 \right\}$$

car $c(j_1, \ldots, j_m) = P^{(j_1, \cdots, j_m)}(\alpha_1, \ldots, \alpha_m)$. Or, avec la formule du binôme, nous obtenons

$$\hat{P}(X_{11}, X_{12}; \cdots; X_{m1}, X_{m2}) = \sum_{\underline{j}} c(j_1, \ldots, j_m) {X_{12}}^{r_1 - j_1} \ldots {X_{m2}}^{r_m - j_m} {L_1}^{j_1} \ldots {L_m}^{j_m} .$$

Cette dernière inégalité et le Lemme 2.2.3 nous montrent que

$$\mathrm{Ind}\,(\hat{P}, \underline{L}, \underline{r}) = \min\left\{\frac{j_1}{r_1} + \cdots + \frac{j_m}{r_m} \mid c(j_1, \ldots, j_m) \neq 0\right\}.$$

Donc

$$i(P, \underline{\alpha}, \underline{r}) = \mathrm{Ind}\,(\hat{P}, \underline{L}, \underline{r}),$$

comme annoncé. ■

2.3 Minoration de l'indice de Schmidt

Cette section comporte deux théorèmes classiquement appelés théorème de l'indice et théorème polynomial. Le premier, étant données des formes linéaires à coefficients algébri- ques, assure, sous certaines conditions, l'existence d'un polynôme P d'indice pas trop petit, et le second nous donne des renseignements sur la taille des $P^{\mathcal{I}}$ correspondants.

Nous commençons par une définition.

Définition 2.3.1 *Etant donnés $P \in \mathcal{A}\setminus\{0\}$, et une forme linéaire $L = \alpha_1 X_1 + \cdots + \alpha_n X_n$, $\alpha_i \in \mathbb{R}$ pour $i = 1, \ldots, n$ non tous nuls,* $\mathrm{Ind}\,(P, L, \underline{r})$ *désigne l'indice* $\mathrm{Ind}\,(P, \underline{L}, \underline{r})$ *où $L_1, \ldots, L_m$ sont les formes linéaires suivantes associées à L*

$$L_h = \alpha_1 X_{h1} + \cdots + \alpha_n X_{hn}, \text{ pour } h = 1, \ldots, m.$$

Théorème 2.3.2 *Soient n et t deux entiers supérieurs à 1, et $(\alpha_{ij})_{1\leq i\leq t, 1\leq j\leq n}$ une famille d'entiers algébriques réels telle que les formes linéaires*

$$L^{(i)} = \alpha_{i1} X_1 + \cdots + \alpha_{in} X_n, \text{ pour } i = 1, \ldots, t.$$

soient non identiquement nulles. Nous posons

$$K_i = \mathbb{Q}(\alpha_{i1}, \ldots, \alpha_{in}), \quad \Delta_i = [K_i : \mathbb{Q}], \text{ et } \Delta = \max\{\Delta_1, \ldots, \Delta_t\}.$$

Nous nous donnons

$$\epsilon > 0, \quad m > 4e^{-2}\log(2t\Delta) \text{ entier}, \quad \underline{r} \text{ comme d'habitude.}$$

Alors il existe $P \in \mathcal{A} \setminus \{0\}$ à coefficients entiers satisfaisant les conditions suivantes.
(i) P est homogène de degré r_h en $\underline{X}_h$ pour $1 \leq h \leq m$,
(ii) Pour $i = 1, \ldots, t$, $\mathrm{Ind}\,(P, L^{(i)}, \underline{r}) \geq \left(\frac{1}{n} - \epsilon\right) m$,
(iii) $H(P) \leq D^{r_1+\cdots+r_m}$ où D ne dépend que de $(\alpha_{ij})_{1\leq i\leq t, 1\leq j\leq n}$.

PREUVE : Nous devons construire un polynôme à coefficients entiers dont les valeurs absolues sont bornées par une certaine constante. Nous allons donc chercher à appliquer le lemme de Siegel (Lemme A de l'Appendice). Il nous faut pour cela estimer le nombre M d'équations liant les coefficients cherchés qui seront les inconnues, au nombre de N, et montrer que $N > M$. Si nous montrons ensuite que la borne donnée par le Lemme A est inférieure à une quantité du type de celle demandée dans le point (iii), le théorème sera montré.

Remarquons tout d'abord que nous voulons P homogène de degré r_h en $\underline{X}_h$ à coefficients dans $\mathbb{Z}$, donc P est à chercher sous la forme

$$P = \sum_{\substack{(j_{h1},\dots,j_{hn})\in\mathbb{N}^n \\ j_{h1}+\dots+j_{hn}=r_h \\ 1\le h\le n}} c(j_{11},\dots,j_{mn}) {X_{11}}^{j_{11}} \dots {X_{mn}}^{j_{mn}} \text{ avec } c(j_{11},\dots,j_{mn}) \in \mathbb{Z}\,.$$

Nous déterminons maintenant le nombre d'équations que doivent satisfaire les coefficients, en analysant le sens des conditions (ii). Ainsi, moyennant l'hypothèse (non restrictive) que $\alpha_{11} \neq 0$, le Lemme 2.2.6 montre que (ii) est satisfaite pour $i = 1$ dès que pour

$$\mathcal{I} = (i_1, 0, \dots, 0; \dots; i_m, 0, \dots, 0), \quad \sum_{h=1}^{m} \frac{i_h}{r_h} < \left(\frac{1}{n} - \epsilon\right) m \text{ et } 0 \le i_h \le r_h,\ 1 \le h \le m\,,$$

$P^{\mathcal{I}}$ est identiquement nul sur le sous-espace de $\mathbb{R}^{mn}$ formé par l'intersection des zéros des polynômes $L_1^{(1)}, \dots, L_m^{(1)}$ définis dans la Définition 2.3.1. En nous reportant à la Définition 2.1.8, nous constatons que cela signifie que $P^*_{\mathcal{I}}$ est identiquement nul. Mais, P étant homogène de degré r_h en $\underline{X}_h$ pour $h = 1, \dots, m$, une étude attentive montre que $P^{\mathcal{I}}$ est homogène de degré $r_h - i_h$ en $\underline{X}_h$, donc que $P^*_{\mathcal{I}}$ est homogène de degré $r_h - i_h$ en $X_{h2}, \dots, X_{hn}$ pour $h = 1, \dots, m$. D'après les lemmes B et C de l'Appendice dont nous utilisons les notations, $P^*_{\mathcal{I}}$ a donc au plus

$$f_1(i_1) \dots f_m(i_m)$$

coefficients. Mais d'après le Lemme 2.1.9, chaque coefficient de $P^*_{\mathcal{I}}$ est une forme linéaire en les coefficients de P, dont les coefficients sont des entiers algébriques du corps K_1 satisfaisant

$$H(\gamma) \le (4^n B_1)^{r_1+\dots+r_m}, \text{ où } B_1 = \max_{1\le k\le n} |\alpha_{1k}|\,,$$

chacun des γ étant lui-même la donnée de Δ_1 éléments de $\mathbb{Z}$ de valeurs absolues inférieures à $(4^n B_1)^{r_1+\dots+r_m}$. Ainsi pour que (ii) soit satisfaite pour $i = 1$, les coefficients ont à satisfaire au plus $\Delta_1 \mathcal{M}^-$ (cf. Lemme C de l'Appendice) équations linéaires homogènes à coefficients entiers bornés par $(4^n B_1)^{r_1+\dots+r_m}$. Toujours d'après le Lemme C,

$$\begin{aligned}
\Delta_1 \mathcal{M}^- &\le \binom{r_1+n-1}{n-1} \dots \binom{r_m+n-1}{n-1} e^{-\epsilon^2 m/4} \\
&\le \Delta_1 \binom{r_1+n-1}{n-1} \dots \binom{r_m+n-1}{n-1} \frac{1}{2t\Delta} \text{ par choix de } m \\
&\le \frac{N}{2t} \text{ si } N = \binom{r_1+n-1}{n-1} \dots \binom{r_m+n-1}{n-1},
\end{aligned}$$

N étant aussi égal à $\binom{r_1-i_1+n-2}{n-2}\dots\binom{r_m-i_m+n-2}{n-2}$, qui est le nombre de coefficients de $P^*_{\mathcal{I}}$. Le nombre M d'équations à satisfaire par ces N inconnues est au plus

$$t \times \frac{N}{2t} \leq \frac{N}{2}\,,$$

donc $N > M$ et le Lemme A de l'Appendice s'applique, et fournit un polynôme $P \neq 0$ satisfaisant (i), (ii) et dont les coefficients sont bornés par

$$(NA)^{M/(N-M)} \leq NA = \binom{r_1+n-1}{n-1}\dots\binom{r_m+n-1}{n-1}A \leq 2^{n(r_1+\cdots+r_m)}A$$

sachant qu'une borne pour les coefficients des M équations est

$$A = (4^n \max_{1\leq i\leq t} B_i)^{r_1+\cdots+r_m}\,.$$

Ainsi nous pouvons conclure que

$$H(P) \leq 2^{n(r_1+\cdots+r_m)}A = D^{r_1+\cdots+r_m} \text{ où nous posons } D = 8^n \max_{1\leq i\leq t} B_i\,.$$

Cela montre que P ainsi construit satisfait aussi (iii) puisque les B_i ne dépendent que de $(\alpha_{ij})_{1\leq i\leq t, 1\leq j\leq n}$. ■

Théorème 2.3.3 *Nous reprenons toutes les hypothèses du Théorème 2.3.2, mais nous supposons de plus que*

$$n = t \text{ et } \det(L^{(1)},\dots,L^{(n)}) \neq 0\,.$$

Soit P le polynôme fourni dans ces conditions par le Théorème 2.3.2. Alors pour tout $\mathcal{I}$ nous pouvons écrire

$$P^{\mathcal{I}} = \sum_{\mathcal{J}} d^{\mathcal{I}}(j_{11},\dots,j_{mn}) L_1^{(1)^{j_{11}}}\dots L_1^{(n)^{j_{1n}}}\dots L_m^{(1)^{j_{m1}}}\dots L_m^{(n)^{j_{mn}}}\,. \tag{2.7}$$

De plus, nous avons les résultats suivants :
(i) Il existe une constante E ne dépendant que de $(\alpha_{ij})_{1\leq i,j\leq n}$ telle que

$$\forall \mathcal{I},\ \forall \mathcal{J}\ |d^{\mathcal{I}}(j_{11},\dots,j_{mn})| \leq E^{r_1+\cdots+r_m}\,,$$

(ii) Si $(\mathcal{I}/\underline{r}) \leq 2\epsilon m$, $d^{\mathcal{I}}(j_{11},\dots,j_{mn}) = 0$ dans (2.7) sauf si

$$\left|\left(\sum_{h=1}^{m}\frac{j_{hk}}{r_h}\right) - \frac{m}{n}\right| \leq 3mn\epsilon \text{ pour } 1\leq k\leq n\,.$$

PREUVE : L'hypothèse $\det(L^{(1)},\dots,L^{(m)}) \neq 0$ permet de montrer que les éléments $(L_h^{(k)})_{1\leq h\leq m, 1\leq k\leq n}$ sont algébriquement libres, sinon $(X_{hk})_{1\leq h\leq m,1\leq k\leq n}$ ne le seraient pas. Si nous développons $P^{\mathcal{I}}$ sur cette dernière famille, nous obtenons que $c(j_{11},\dots,j_{mn})$ sont bornés par $(2D)^{r_1+\cdots+r_m}$ grâce aux conditions (i) et (ii) du Théorème 2.3.2 et au Lemme 2.1.5. Lorsque nous passons de cette écriture, à l'écriture (2.7), il faut tenir compte d'une "matrice de passage" des (X_{hk}) aux $(L_h^{(k)})$. Si nous désignons par G le maximum de 1 et des valeurs absolues des coefficients de cette matrice, nous constatons après quelques calculs que chaque terme

$$c^{\mathcal{I}}(j_{11},\dots,j_{mn}){X_{11}}^{j_{11}}\dots{X_{mn}}^{j_{mn}}$$

a, comme polynôme en les $(L_h^{(k)})$, des coefficients bornés par $(2DnG)^{r_1+\cdots+r_m}$. Mais d'après le Lemme B de l'Appendice, il y a au plus

$$\binom{r_1+n-1}{r_1}\dots\binom{r_m+n-1}{r_m} \leq 2^{n(r_1+\cdots+r_m)}$$

tels termes dans l'écriture (2.7), donc

$$|d^{\mathcal{I}}(j_{11},\dots,j_{mn})| \leq (2^n 2DnG)^{r_1+\cdots+r_m} \stackrel{def}{=} E^{r_1+\cdots+r_m}\,.$$

Cela prouve (i).
Vérifions maintenant le (ii). Le théorème de l'indice (Théorème 2.3.2) nous dit que :

$$\mathrm{Ind}\,(P, L^{(k)}, \underline{r}) \geq \left(\frac{1}{n}-\epsilon\right) m \text{ pour } 1\leq k\leq n\,,$$

et le Lemme 2.2.5 assure que

$$\mathrm{Ind}\,(P^{\mathcal{I}}, \underline{L}^{(k)}, \underline{r}) \geq \mathrm{Ind}\,(P, \underline{L}^{(k)}, \underline{r}) - (\mathcal{I}/\underline{r}) \geq \left(\frac{1}{n}-\epsilon\right)m - 2\epsilon m = \left(\frac{1}{n}-3\epsilon\right)m\,.$$

Donc la définition de l'indice montre que si $d^{\mathcal{I}}(j_{11},\dots,j_{mn}) \neq 0$, alors c'est que $\sum_{h=1}^m \frac{j_{hk}}{r_h} \geq \left(\frac{1}{n}-3\epsilon\right)m$, ce qui conduit à l'une des deux inégalités induites par (ii). Pour obtenir l'autre, il suffit d'observer que P est homogène de degré r_h en $\underline{X}_h$, donc $P^{\mathcal{I}}$ est homogène de degré au plus r_h en $\underline{X}_h$ pour $h=1,\dots,m$, ce qui implique :

$$\sum_{k=1}^n \frac{j_{hk}}{r_h} \leq 1 \text{ pour } h=1,\dots,m\,,$$

d'où

$$\sum_{k=1}^n\sum_{h=1}^m \frac{j_{hk}}{r_h} = \sum_{h=1}^m\sum_{k=1}^n \frac{j_{hk}}{r_h} \leq m \text{ soit } \sum_{k=1}^n\left(\left(\sum_{h=1}^m \frac{j_{hk}}{r_h}\right) - \frac{m}{n}\right) \leq 0\,.$$

Cette dernière inégalité, jointe à la partie de (ii) que nous avons déjà prouvée, montre que

$$\left(\sum_{h=1}^m \frac{j_{hk}}{r_h}\right) - \frac{m}{n} \leq 3m\epsilon(n-1) \leq 3m\epsilon n\,.$$

C'est précisément l'autre inégalité que nous voulions, donc (ii) est prouvé. ■

2.4 Majoration de l'indice de Schmidt

Dans cette section, nous donnons des conditions suffisantes sous lesquelles un polynôme P de $\mathcal{A}$ non nul a un indice de Schmidt petit. L'idée consiste à majorer l'indice de Schmidt par l'indice de Roth d'un polynôme $\tilde{P}$ convenablement construit, puis d'invoquer le lemme de Roth classique, que nous énonçons ci-après.

Lemme 2.4.1 (Lemme de Roth) *Soient* $0 < \epsilon < \frac{1}{12}$, $\omega = 24.2^{-m}\left(\frac{\epsilon}{12}\right)^{2^{m-1}}$, $\underline{r} \in \mathbb{N}^m$ *tels que*

$$\omega r_h \geq r_{h+1}, \text{ pour } 1 \leq h \leq m\,. \tag{2.8}$$

Soient aussi $0 < \gamma \leq 1$ *et* $p_1/q_1, \ldots, p_m/q_m$ *des rationnels écrits sous forme irréductible, avec dénominateur positif satisfaisant*

$$q_h{}^{r_h} \geq q_1{}^{\gamma r_1},\ 1 \leq h \leq m\,, \tag{2.9}$$

$$q_h{}^{\omega\gamma} \geq 2^{3m},\ 1 \leq h \leq m\,. \tag{2.10}$$

Si $P(X_1, \ldots, X_m) \in \mathbb{Z}[X_1, \ldots, X_m] \setminus \{0\}$ *est de degré au plus* r_h *en* X_h *pour* $1 \leq h \leq m$ *et*

$$H(P) \geq q_1{}^{\omega\gamma r_1}\,. \tag{2.11}$$

Alors :

$$i\left(P, \left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right), \underline{r}\right) \leq \epsilon\,.$$

Preuve : Elle se trouve par exemple dans [Rot], dans le chapitre 5 de [Sch1], ou encore dans [Hab] (Théorème 8 du chapitre 2). ■

Remarque 2.4.2 *La constante* ω *intervenant dans le Lemme 2.4.1 est petite ; en uti- lisant des méthodes faisant appel à la géométrie algébrique décrites dans [EdE], J.-H. Evertse est parvenu à l'augmenter sensiblement (cf. [Eve]) et a montré :*

Lemme *Soit* $P(X_1, \ldots, X_m)$ *de degré en* X_h *inférieur à* r_h *tel que*

$$r_h \geq \omega_1(m, \epsilon) r_{h+1},\ \text{où } \omega_1(m, \epsilon) = \frac{2m^3}{\epsilon}\,.$$

Soient $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}$ *des points de* $\mathbb{Q}$ *avec* $(p_i, q_i) = 1$ *et* $q_i > 0$ *pour* $i = 1, \ldots, m$, *tels que*

$$q_h{}^{r_h} \geq (5^{r_1+\cdots+r_m} H(P))^{\omega_2(m,\epsilon)} \text{ où } \omega_2(m, \epsilon) = \left(\frac{3m^3}{\epsilon}\right)^m\,.$$

Alors

$$i\left(P, \left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right), \underline{r}\right) \leq \epsilon\,.$$

Cette remarque étant faite, voici le théorème annoncé ci-dessus.

Théorème 2.4.3 *Soient* $0 < \epsilon < \frac{1}{12}$, $m \geq 1$ *un entier, et*

$$\omega = 24.2^{-m}\left(\frac{\epsilon}{12}\right)^{2^{m-1}} \leq 1\,.$$

Soient $r_1, \ldots, r_m$ *des entiers strictement positifs tels que*

$$r_h\omega \geq r_{h+1},\ \textit{pour}\ h = 1, \ldots, m\,. \tag{2.12}$$

Soit $n \geq 2$ *un entier et supposons disposer de polynômes linéaires non nuls en* n *variables,* $M_1, \ldots, M_m$, *à coefficients premiers entre eux. Supposons que* $0 < \Gamma \leq q$ *(où* $q \stackrel{def}{=} n-1$*), et que*

$$H(M_h)^{r_h} \geq H(M_1)^{r_1\Gamma},\ \textit{pour}\ h = 1, \ldots, m\,, \tag{2.13}$$

$$H(M_h)^{\omega\Gamma} \geq 2^{3mq^2},\ \textit{pour}\ h = 1, \ldots, m\,. \tag{2.14}$$

Soit enfin $P \in \mathcal{A} \setminus \{0\}$, *à coefficients entiers, homogène en* $\underline{X}_h$ *de degré* r_h *pour* $h = 1, \ldots, m$ *satisfaisant de plus*

$$H(P)^{q^2} \geq H(M_1)^{\omega r_1\Gamma},\ \textit{pour}\ h = 1, \ldots, m\,. \tag{2.15}$$

Alors

$$\mathrm{Ind}\,(P, \underline{M}, \underline{r}) \leq \epsilon\,.$$

Preuve : Désignons par $A = (a_{hk})_{\substack{1\leq h\leq m\\ 1\leq k\leq n}}$ la matrice des coefficients de $M_1, \ldots, M_m$, c'est-à-dire que

$$M_h = a_{h1}X_{h1} + \cdots + a_{hn}X_{hn},\ \text{pour}\ h = 1, \ldots, m\,.$$

Nous pouvons supposer sans perte de généralité que $H(M_h) = |a_{h1}|$ pour $h = 1, \ldots, m$, et d'après le Lemme D de l'Appendice, nous pouvons aussi supposer que

$$(a_{h1}, a_{h2}) \leq |a_{h1}|^{(q-1)/q} \text{ pour } h = 1, \ldots, m\,. \tag{2.16}$$

Si nous désignons par η l'indice de P par rapport à $\underline{M}$ et $\underline{r}$, nous savons que P appartient à l'idéal de $\mathcal{A}$ engendré par les polynômes :

$$M_1{}^{i_1} \ldots M_m{}^{i_m},\ \text{pour lesquels}\ \sum_{h=1}^{m}\frac{i_h}{r_h} \geq \eta\,.$$

Nous construisons maintenant le polynôme $\tilde{P}$ que nous évoquions au début de cette section. Nous passons par un intermédiaire $\hat{P}$. Si $n = 2$, nous posons $\hat{P} = P$, sinon nous obtenons $\hat{P}$ grâce l'algorithme suivant.

1. [**Initialisation**]
   $\hat{P} \leftarrow P$

2. [**Boucle sur les variables**]
   Pour $i = 1, \dots, m$ faire
      Pour $j = 3, \dots, n$ faire
      $\alpha_{ij} \leftarrow v_{X_{ij}}(\hat{P})$
      $\hat{P} \leftarrow \hat{P}/{X_{ij}}^{\alpha_{ij}}$
      $\hat{P} \leftarrow \hat{P}(\underline{X}_1; \dots; X_{i1}, \dots, X_{i(j-1)}, 0, X_{i(j+1)}, \dots, X_{in}; \dots; \underline{X}_m)$

Il est clair que cet algorithme fournit pour résultat un polynôme
(i) à coefficients entiers ;
(ii) en les $2m$ variables $X_{11}, X_{12}, \dots, X_{m1}, X_{m2}$;
(iii) non nul ;
(iv) homogène de degré au plus r_h en X_{h1}, X_{h2} pour $h = 1, \dots, m$;
(v) satisfaisant $H(\hat{P}) \leq H(P)$;
(vi) appartenant à l'idéal de $\mathbb{R}[X_{11}, X_{12}, \dots, X_{m1}, X_{m2}]$ engendré par les polynômes

$$(a_{11}X_{11} + a_{12}X_{12})^{i_1} \dots (a_{m1}X_{m1} + a_{m2}X_{m2})^{i_m} \text{ pour lesquels } \sum_{h=1}^{m} \frac{i_h}{r_h} \geq \eta\,.$$

$\hat{P}$ étant construit, nous posons $\tilde{P}(X_1, \dots, X_m) = \hat{P}(X_1, 1; \dots; X_m, 1)$ qui est par conséquent un polynôme non nul, satisfaisant $H(\tilde{P}) \leq H(P)$, et appartenant à l'idéal de $\mathbb{R}[X_1, \dots, X_m]$ engendré par les polynômes

$$\left(X_1 + \frac{a_{12}}{a_{11}}\right)^{i_1} \dots \left(X_m + \frac{a_{m2}}{a_{m1}}\right)^{i_m} \text{ où } \sum_{h=1}^{m} \frac{i_h}{r_h} \geq \eta\,.$$

Il en résulte que nous avons $i(P, \left(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}\right), \underline{r}) \geq \eta = \mathrm{Ind}\,(P, \underline{M}, \underline{r})$ si nous posons

$$q_h = \frac{|a_{h1}|}{(a_{h1}, a_{h2})} \text{ et } p_h = \frac{-|a_{h1}|a_{h2}}{(a_{h1}, a_{h2})a_{h1}} \text{ pour } h = 1, \dots, m\,.$$

Il reste pour conclure, à vérifier que $\tilde{P}$ satisfait les hypothèses du lemme de Roth (2.4.1). La condition (2.8) est satisfaite puisque c'est la condition (2.12) du théorème. Les conditions (2.9), (2.10) et (2.11) vont résulter quant à elles des hypothèses (2.13), (2.14) et (2.15) du théorème : en effet, posons $\gamma = \Gamma/q$, de sorte que $0 < \gamma \leq 1$. Nous observons d'après (2.16), que pour $h = 1, \dots, m$,

$$H(M_h)^{1/q} = |a_{h1}|^{1/q} = |a_{h1}|^{(1-q)/q+q/q} = \frac{|a_{h1}|}{|a_{h1}|^{(1-q)/q}} \leq \frac{|a_{h1}|}{(a_{h1}, a_{h2})} = q_h \leq H(M_h)\,.$$

Donc, d'après (2.13),

$$q_h{}^{r_h} \geq H(M_h)^{r_h/q} \geq H(M_1)^{\Gamma r_1/q} = H(M_1)^{\gamma r_1} \geq q_1{}^{r_1\gamma}\,,$$

qui est exactement (2.9). De même, (2.14) nous donne

$$q_h{}^{\omega\gamma} = q_h{}^{\omega\Gamma/q} \geq H(M_h)^{\omega\Gamma/q^2} \geq 2^{3m}\,,$$

qui est exactement (2.10). Et finalement, grâce à (2.15), nous obtenons

$$H(\tilde{P}) \leq H(P) \leq H(M_1)^{\omega r_1\gamma/q} \leq q_1{}^{\omega r_1\gamma}\,,$$

qui est exactement (2.11) pour le polynôme $\tilde{P}$. Donc le Lemme de Roth s'applique bien et assure que

$$\mathrm{Ind}\,(P, \underline{M}, \underline{r}) \leq \mathrm{Ind}\left(\tilde{P}, \left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right), \underline{r}\right) \leq \epsilon\,. \quad \blacksquare$$

Cette section termine la description des outils utilisés dans la preuve du théorème des sous-espaces, qui est l'objet du chapitre suivant.

Chapitre 3

Preuves des théorèmes des sous-espaces et des sous-espaces fort

Ce chapitre est consacré à la démonstration du théorème des sous-espaces et du théorème des sous-espaces fort. Avant d'énoncer ces deux théorèmes, mettons en place quelques notations.

Définition 3.0.1 *$L_1, \dots, L_n$ désignent des formes linéaires indépendantes sur $\mathbb{R}^n$ à coefficients algébriques réels, que nous pouvons donc écrire*

$$L_i(x) = L_i(x_1, \dots, x_n) = \sum_{j=1}^{n} a_i^{(j)} x_j = a_i.x,\ a_i^{(j)} \in \overline{\mathbb{Q}} \cap \mathbb{R}\,.$$

$(a_1^*, \dots, a_n^*)$ désigne la base duale de $(a_1, \dots, a_n)$, et $\underline{c} = (c_1, \dots, c_n)$ est un vecteur de nombres réels tels que

$$c_1 + \cdots + c_n = 0\,, \tag{3.1}$$

avec, en plus, lorsqu'il n'est pas précisé que seule (3.1) est satisfaite,

$$\forall i \in \{1, \dots, n\},\ |c_i| \leq 1\,, \tag{3.2}$$

Pour $Q > 0$, $\Pi(Q)$ désigne le parallélépipède $\Pi(L_1, \dots, L_n; Q^{c_1}, \dots, Q^{c_n})$ (voir Définition 1.2.1) ; ses minima successifs sont notés $\lambda_1(Q), \dots, \lambda_n(Q)$, et $g_1(Q), \dots, g_n(Q)$ désignent des vecteurs entiers indépendants de $\Pi(Q)\lambda_i(Q) \cap \mathbb{Z}^n$, $i = 1, \dots, n$. La notation $M(Q)$ désigne l'unique forme linéaire à coefficients entiers premiers entre eux dont la première composante est positive, qui s'annule sur $g_1(Q), \dots, g_{n-1}(Q)$. Si Q est de la forme Q_h ($h \in \mathbb{N}$), M_h désigne le polynôme linéaire en le bloc de variables $\underline{X}_h$, à coefficients entiers premiers entre eux dont le premier est positif, qui s'annule sur $g_1(Q_h), \dots, g_{n-1}(Q_h)$. Enfin pour $\delta > 0$ nous posons

$$\Sigma(\underline{c}, \delta) = \{i \in \{1, \dots, n\} \mid c_i + \delta/2 \geq 0\}\,.$$

C'est un ensemble non vide à cause des hypothèses sur $\underline{c}$.

Nous pouvons maintenant énoncer les deux théorèmes.

Théorème 3.0.2 (DES SOUS-ESPACES FORT) *Soit $\underline{c}$ satisfaisant (3.1). Supposons qu'il existe un entier $1 \leq d \leq n-1$ et une partie $\mathcal{D} \subset]1, +\infty[$ non bornée telle que la famille de parallélépipèdes $\Pi(Q)_{Q\in\mathcal{D}}$ possède la propriété :*

$$\forall Q \in \mathcal{D},\ \lambda_d(Q) < \lambda_{d+1}(Q)Q^{-\delta}\,.$$

Il existe alors une partie $\mathcal{D}' \subset \mathcal{D}$ non bornée, et un sous-espace vectoriel S de $\mathbb{Q}^n$ de dimension d, telle que la famille de parallélépipèdes $\Pi(Q)_{Q\in\mathcal{D}'}$ satisfasse

$$\forall Q \in \mathcal{D}',\ \mathbb{Q}g_1(Q) \oplus \cdots \oplus \mathbb{Q}g_d(Q) = S\,.$$

Théorème 3.0.3 (DES SOUS-ESPACES) *Supposons que $L_1, \ldots, L_n$ soient à coefficients algébriques. Alors si $\underline{c}$ satisfait (3.1), il existe un nombre fini de sous-espaces non triviaux de $\mathbb{Q}^n$, à savoir $T_1, \ldots, T_k$, tels que l'inéquation*

$$|L_1(x)\ldots L_n(x)| < \|x\|_\infty^{-\delta},\ x \in \mathbb{Z}^n \setminus \{0\} \tag{3.3}$$

ait ses solutions dans $T_1 \cup \cdots \cup T_k$.

3.1 Preuve du théorème des sous-espaces fort dans le cas $d = n-1$

Reprenons les notations du Théorème 3.0.2. Nous constatons qu'il s'agit de prouver que $g_n^*(Q)$ est constant sur $\mathcal{D}'$ sous l'hypothèse $\lambda_{n-1}(Q) < \lambda_n(Q)Q^{-\delta}, Q \in \mathcal{D}$. En utilisant le lemme de Davenport (Théorème 1.1.12), il est possible de se ramener à l'hypothèse $\lambda_{n-1}(Q) < Q^{-\delta}, Q \in \mathcal{D}$ (nous le faisons dans le Lemme 3.1.6) qui est plus facile à manipuler car elle signifie que $\Pi(Q)Q^{-\delta}$ contient $g_1(Q), \ldots, g_{n-1}(Q)$. Pour montrer que $g_n^*(Q)$ est constant sur $\mathcal{D}'$ (Lemme 3.1.5), nous extrayons de $\mathcal{D}$ une partie $\mathcal{D}_1 \subset \mathcal{D}$ non bornée sur laquelle $g_n^*(Q)$ vaut en fait un certain $h \in \Pi^*(Q)$. L'existence de ce vecteur h est assurée par le Théorème 3.1.4, où nous montrerons que sous l'hypothèse $\lambda_{n-1}(Q) < Q^{-\delta}$, nous avons le fait suivant :

$$\forall i \in \Sigma(\underline{c}, \delta), a_i^*.g_n^*(Q) = 0\,,$$

pour Q assez grand. La preuve de ce résultat s'effectue par l'absurde, en supposant non borné l'ensemble des $Q > 1$ tels que $\lambda_{n-1}(Q) < Q^{-\delta}$ et l'énoncé contraire à celui ci-dessus. Nous sommes alors capables de trouver
– un réel $\epsilon > 0$,
– des entiers $m, r_1, \ldots, r_m$,
– des réels $Q_1, \ldots, Q_m$,
tels que les données $L_1, \ldots, L_n, r_1, \ldots, r_m, \epsilon, m$ satisfassent les hypothèses du théorème polynomial (Théorème 2.3.3). Cela permet d'exhiber un polynôme $P \in \mathcal{A} \setminus \{0\}$ dont nous saurons montrer grâce aux outils développés dans le chapitre 2 que son indice par rapport à $(\underline{M}, \underline{r})$ (cf.

Définition 3.0.1) est au moins $m\epsilon$ (Théorème 3.1.2). Par ailleurs l'hypothèse de départ nous permet d'obtenir des informations sur la taille de $g_n^*(Q_h)$ donc sur $H(M_h)$ (Lemme 3.1.3) qui impliquent que les hypothèses du Thèorème 2.4.3 sont également satisfaites, donc $\mathrm{Ind}\,(P, \underline{M}, \underline{r}) \leq \epsilon$, ce qui est absurde et montre le Théorème 3.1.4.

Une fois la stratégie mise en place, il n'y a plus qu'à la mettre à exécution.

Commençons tout d'abord par formaliser une remarque que nous avons déjà implicitement utilisée ci-dessus, et qui est omniprésente dans beaucoup des raisonnements qui sui- vront.

Remarque 3.1.1 *Les notations étant celles de la Définition 3.0.1, nous pouvons écrire pour tout* $Q > 0$

$$g_n^*(Q) = \frac{M(Q)}{F(Q)},\ F(Q) \in \mathbb{Z},\ 1 \leq |F(Q)| \leq n!^2\,.$$

En effet, $g_n^*(Q)$ et $M(Q)$ sont $\mathbb{Q}$-proportionnels puisque tous deux s'annulent sur le sous-espace $\mathbb{Q}g_1(Q) \oplus \cdots \oplus \mathbb{Q}g_{n-1}(Q)$. Si $E(Q) = \det(g_1(Q), \ldots, g_n(Q))$, il existe d'après le Théorème 1.1.14, un entier $t(Q) \in \mathbb{Z}$ avec $|E(Q)|g_n^*(Q) = t(Q)M(Q)$, de sorte que $t(Q)$ divise $F(Q)$. Si nous posons $F(Q) = \pm E(Q)\ t(Q)$, nous avons la relation énoncée.
Il suit que toute information sur la taille de $g_n^*(Q)$ en fonction de Q se traduit en une information sur la taille de $M(Q)$, et que de toute famille non bornée de réels $Q > 1$, nous pouvons extraire une famille pour laquelle $F(Q)$ ne dépende pas de Q appartenant à cette famille.

Théorème 3.1.2 *Soient* $\epsilon > 0, 0 < \delta < 1$ *tels que* $16n^2\epsilon < \delta$, $L^{(i)} = L_i$ $(i = 1, \ldots, n)$ *des formes linéaires* $m, \underline{r}$ *satisfaisant les hypothèses du Théorème 2.3.3. Continuons à noter* E *la constante et* P *le polynôme mentionnés dans ce même théorème. Supposons que* $Q_1, \ldots, Q_m$ *soient des réels satisfaisant*

$$Q_h^\epsilon > 2^n E \text{ et } Q_h^\epsilon > n(1+\epsilon^{-1}) \text{ pour } 1 \leq h \leq m\,, \tag{3.4}$$

$$r_1 \log Q_1 \leq r_h \log Q_h \leq (1+\epsilon) r_1 \log Q_1 \text{ pour } 1 \leq h \leq m\,, \tag{3.5}$$

$$\lambda_{n-1}(Q_h) < Q_h^{-\delta} \text{ pour } 1 \leq h \leq m\,. \tag{3.6}$$

Alors $\mathrm{Ind}\,(P, \underline{M}, \underline{r}) \geq m\epsilon$.

Preuve : Ecrivons $g_{ht} = g_t(Q_h)$ pour $h = 1, \ldots, m$ et $t = 1, \ldots, q \overset{def}{=} n-1$. La formule (3.6) s'écrit alors

$$|L_k(g_{ht})| \leq {Q_h}^{c_k - \delta} \text{ pour } 1 \leq k \leq n,\ 1 \leq h \leq m,\ 1 \leq t \leq q\,. \tag{3.7}$$

Le Lemme 2.2.6 nous dit que pour avoir la conclusion du présent théorème, il suffit de prouver que $P^{\mathcal{J}}$ est nul sur le sous-espace de l'intersection des zéros de $M_1, \ldots, M_m$ dès que $(\mathcal{J}/\underline{r}) < \epsilon m$. Or cette intersection est le produit de m sous-espaces vectoriels de dimension q, à savoir

$$\mathbb{R}g_1(Q_h) \oplus \cdots \oplus \mathbb{R}g_q(Q_h) \text{ pour } 1 \leq h \leq m\,,$$

sur lesquels nous disposons des grillages

$$\Gamma_h = \Gamma(s_h, g_{h1}, \dots, g_{hq}), s_h = [\epsilon^{-1}] + 1,\ 1 \leq h \leq m\,.$$

Nous appliquons alors le Lemme 2.1.3 qui nous dit qu'il suffit de prouver que

$$(P^{\mathcal{J}})^{\mathcal{I}}(\gamma_1, \dots, \gamma_m) = 0 \text{ pour } \left\{ \begin{array}{l} (\gamma_1, \dots, \gamma_m) \in \Gamma_1 \times \cdots \times \Gamma_m \text{ et} \\ \mathcal{I} = (t_{11}, \dots, t_{1n}; \cdots; t_{m1}, \dots, t_{mn}) \text{ tel que} \\ t_{h1} + \cdots + t_{hn} \leq t_h \stackrel{def}{=} [r_h\epsilon] \text{ pour } h = 1, \dots, m\,, \end{array} \right.$$

car $s_h(t_h + 1) = ([\epsilon^{-1}] + 1)([r_h\epsilon] + 1) > \epsilon^{-1} r_h \epsilon = r_h$. En fait, il suffit même de prouver

$$(\mathcal{J}/\underline{r}) < 2\epsilon m \Longrightarrow \forall (\gamma_1, \dots, \gamma_m) \in \Gamma_1 \times \cdots \times \Gamma_m,\ P^{\mathcal{J}}(\gamma_1, \dots, \gamma_m) = 0$$

puisque

$$\begin{array}{rcl} (\mathcal{I} + \mathcal{J}/\underline{r}) & = & (\mathcal{I}/\underline{r}) + (\mathcal{J}/\underline{r}) \\ & < & \epsilon m + \dfrac{[r_1\epsilon]}{r_1} + \cdots + \dfrac{[r_m\epsilon]}{r_m} = 2\epsilon m\,. \end{array}$$

Or nous avons alors l'écriture

(3.8)
$$P^{\mathcal{J}}(\gamma_1, \dots, \gamma_m) = \sum_{\underline{j}} d^{\mathcal{J}}(j_{11}, \dots, j_{mn}) L_1(\gamma_1)^{j_{11}} \dots L_n(\gamma_1)^{j_{1n}} \dots L_1(\gamma_m)^{j_{m1}} \dots L_n(\gamma_m)^{j_{mn}}\,.$$

En écrivant γ_h sur la base du grillage Γ_h, nous obtenons les inégalités suivantes pour $1 \leq h \leq m$ et $1 \leq k \leq n$:

$$\begin{array}{rcl} |L_k(\gamma_h)| & \leq & \left(1 + \dfrac{1}{\epsilon}\right) {Q_h}^{c_k - \delta} \dots \left(1 + \dfrac{1}{\epsilon}\right) {Q_h}^{c_k - \delta} \text{ d'après (3.7)} \\ & < & {Q_h}^{c_k - \delta + \epsilon} \text{ d'après (3.4)} \\ & \leq & {Q_h}^{c_k - 15n^2\epsilon} \text{ puisque } 16n^2\epsilon < \delta\,. \end{array}$$

En faisant le produit sur h de ces inégalités, nous obtenons

$$\begin{array}{rcl} |L_k(\gamma_1)^{j_{1k}} \dots L_k(\gamma_1)^{j_{1k}}| & \leq & \exp\left(\displaystyle\sum_{h=1}^{m} (c_k - 15n^2\epsilon) j_{hk} \log Q_h\right) \\ & \leq & \exp\left((c_k - 15n^2\epsilon) \displaystyle\sum_{h=1}^{m} j_{hk} \log Q_h\right) \end{array} \tag{3.9}$$

car c_k ne dépend pas de h. Maintenant, le point (ii) du Théorème 2.3.3 nous dit que $d^{\mathcal{J}}(j_{11}, \dots, j_{mn}) = 0$, sauf peut-être si

$$\left| \sum_{h=1}^{m} \frac{j_{hk}}{r_h} - \frac{m}{n} \right| \leq 3mn\epsilon\,.$$

Comme le membre de gauche de (3.8) est entier, montrer qu'il est nul, c'est montrer qu'il est strictement inférieur à 1. Or

$$\sum_{h=1}^{m} j_{hk} \log Q_h \geq r_1 \log Q_1 \sum_{h=1}^{m} \frac{j_{hk}}{r_h} \geq r_1 \log Q_1 \left(\frac{1}{n} - 3n\epsilon \right) m \text{ d'après (3.5)},$$

et

$$\begin{aligned} \sum_{h=1}^{m} j_{hk} \log Q_h &\leq (1+\epsilon) r_1 \log Q_1 \sum_{h=1}^{m} \frac{j_{hk}}{r_h} \\ &\leq r_1 \log Q_1 (1+\epsilon) \left(\frac{1}{n} + 3n\epsilon \right) m \\ &\leq r_1 \log Q_1 \left(\frac{1}{n} + 7n\epsilon \right) m \text{ d'après (3.5)}, \end{aligned}$$

conduisent à

$$\left| \sum_{h=1}^{m} j_{hk} \log Q_h - r_1 \log Q_1 \frac{m}{n} \right| \leq r_1 \log Q_1 7mn\epsilon, \text{ d'après (3.5)}.$$

Nous disposons également de $|c_k - 15n^2\epsilon| \leq 2$ (d'après la Définition 3.0.1, et le fait que $16n^2\epsilon < \delta < 1$). En ajoutant et retranchant $r_1 \log Q_1 m/n$ à l'argument de exp dans (3.9) et en utilisant les deux majorations que nous venons d'établir, nous trouvons pour le membre de gauche de (3.9) une borne du type

$$Q_1{}^{r_1 \frac{m}{n}(c_k - 15n^2\epsilon)} \exp(\alpha\beta), \ \alpha \leq 2, \ \beta \leq r_1 \log Q_1 .7nm\epsilon,$$

qui peut encore être majorée par

$$Q_1{}^{r_1 \frac{m}{n}(c_k - 15n^2\epsilon) + 2r_1 .7mn\epsilon} = Q_1{}^{r_1 \frac{m}{n}(c_k - nm\epsilon)}.$$

En faisant le produit sur k de ces bornes, et en tenant compte de la borne $E^{r_1+\cdots+r_m}$ pour $d^{\mathcal{J}}(j_{11}, \ldots, j_{mn})$ donnée par le Théorème 2.3.3, nous constatons que chaque terme de (3.8) est majoré par

$$\begin{aligned} E^{r_1+\cdots+r_m} Q_1{}^{r_1 \frac{m}{n}(c_1+\cdots+c_n) - r_1 n^2 m\epsilon} &= E^{r_1+\cdots+r_m} Q_1{}^{-r_1 n^2 m\epsilon} \ (\text{car } c_1 + \cdots + c_n = 0) \\ &\leq E^{r_1+\cdots+r_m} \left(Q_1{}^{-r_1\epsilon} \ldots Q_m{}^{-r_m\epsilon} \right)^{\frac{n^2}{1+\epsilon}} \text{ d'après (3.5)} \\ &\leq E^{r_1+\cdots+r_m} Q_1{}^{-r_1\epsilon} \ldots Q_m{}^{-r_m\epsilon}. \end{aligned}$$

Sachant que le nombre de ces termes est majoré par $2^{n(r_1+\cdots+r_m)}$ (Lemme B de l'Appendice), le membre de gauche de (3.8) se trouve borné par

$$\prod_{h=1}^{m} (2^n E Q_h{}^{\epsilon})^{r_h} < 1 \text{ d'après (3.4)},$$

ce qu'il fallait démontrer. ■

Nous réglons maintenant la question de la taille de $g_n^*(Q)$ (ou de $M(Q)$).

Lemme 3.1.3 *Supposons que la famille de parallélépipèdes $\Pi(Q)_{Q>1}$ satisfasse*

$$\forall Q > 1, \lambda_{n-1}(Q) < Q^{-\delta}\,, \tag{3.10}$$

$$\forall Q > 1, \exists i(Q) \in \Sigma(\underline{c}, \delta) \mid a_{i(Q)}^* . g_n^*(Q) \neq 0\,. \tag{3.11}$$

Alors il existe six constantes strictement positives $C_1, \ldots, C_6$ ne dépendant que des formes linéaires $L_1, \ldots, L_n$, δ et $\underline{c}$ telles que

$$\forall Q \geq C_3,\ Q^{C_1} \leq H(g_n^*(Q)) \leq Q^{C_2}\,, \tag{3.12}$$

$$\forall Q \geq C_6,\ Q^{C_4} \leq H(M(Q)) \leq Q^{C_5} \text{ avec } C_4 \leq C_5(n-1)\,. \tag{3.13}$$

Preuve : Nous allons faire usage de théorème de Mahler sur les parallélépipèdes réciproques (Théorème 1.1.14) pour obtenir la borne supérieure. La borne inférieure viendra pour sa part d'un argument de type Liouville. Posons

$$a_i'(Q) = Q^{-c_i} a_i \text{ d'où } a'^*_i(Q) = Q^{c_i} a_i^* \text{ pour } i = 1, \ldots, n\,.$$

Par le théorème de Mahler appliqué aux parallélépipèdes duaux $\Pi(a_1'(Q), \ldots, a_n'(Q)) = \Pi(Q)$ et $\Pi^*(a'^*_1(Q), \ldots, a'^*_n(Q)) = \Pi^*(Q)$, nous trouvons une constante $K_1 > 0$ telle que

$$\forall (i,j) \in \{1, \ldots, n\}^2,\ |a'^*{}_i(Q) . g_j^*(Q)| \leq K_1 \lambda_j(Q)^{-1}\,,$$

d'où

$$\forall i \in \{1, \ldots, n\},\ |a_i^* . g_n^*(Q)| \leq K_1 \lambda_n(Q)^{-1} Q^{-c_i} \leq K_2 Q^{-\delta(n-1)-c_i}\,, \tag{3.14}$$

car en posant $K_2 = K_1 n!/|\det(L_1, \ldots, L_n)|$, le Théorème 1.1.11, le Lemme 1.1.9, et (3.10) nous montrent que

$$\lambda_n(Q)^{-1} \leq \lambda_1(Q) \ldots \lambda_{n-1}(Q) \frac{n!}{2^n} \operatorname{Vol} \Pi(Q) \leq Q^{-\delta(n-1)} \frac{n!}{\det(L_1, \ldots, L_n)}\,.$$

En écrivant la base canonique sur les a_i^*, nous obtenons que $H(g_n^*(Q)) \leq K_3 Q^{1-\delta(n-1)}$, donc pour

$$C_2 > 0 \text{ et } Q > K_3^{-C_2+\delta n},\ H(g_n^*(Q)) \leq Q^{C_2}\,,$$

et nous avons alors la deuxième inégalité. Ecrivons (3.14) pour $i \in \Sigma$. Il vient alors

$$\forall i \in \Sigma,\ |a_i^* . g_n^*(Q)| \leq K_2 Q^{-\delta(n-1)+\delta/2} \leq Q^{-\delta/2} K_2\,. \tag{3.15}$$

Utilisons maintenant la propriété (3.11), en appelant $\Delta^*_{i(Q)}$ le degré du corps de nombres $K^*_{i(Q)}$ engendré par les composantes de $a^*_{i(Q)}$. La Remarque 3.1.1 montre que $g^*_n(Q)$ a des coordonnées dans $\mathbb{Q}$, avec un dénominateur au plus égal à $n!^2$.
Comme $a^*_{i(Q)}.g^*_n(Q)n!^2 \det(L_1,\dots,L_n)$ est un entier algébrique non nul, sa norme est au moins 1, mais si σ est l'un des plongements de K^*_i dans $\mathbb{C}$, l'égalité

$$|\sigma(a^*_{i(Q)}.g^*_n(Q))| = \left|\sum_{k=1}^{n} \sigma(a^*_{i(Q),k}).\sigma(g^*_{n,k}(Q))\right| = \left|\sum_{k=1}^{n} \sigma(a^*_{i(Q),k}).g^*_{n,k}(Q)\right|$$

montre qu'il existe une constante K_4 telle que

$$|\sigma(a^*_{i(Q)}.g^*_n(Q))| \geq K_4 H(g^*_n(Q))^{1-\Delta^*_{i(Q)}} \geq H(g^*_n(Q))^{1-\Delta^*}, \text{ où } \Delta^* = \max_{1\leq i\leq n}\{\Delta^*_i\}. \tag{3.16}$$

En confrontant (3.15) et (3.16) nous obtenons $\Delta^* > 1$ et

$$H(g^*_n(Q)) \geq K_4 {K_2}^{-1} Q^{\delta/(2(\Delta^*-1))}.$$

En posant alors $C_1 = \delta/(3(\Delta^*-1))$ nous en déduisons que

$$Q > ({K_4}^{-1}K_2)^{6(\Delta^*-1)/\delta} \Longrightarrow H(g^*_n(Q)) \geq Q^{C_1}.$$

Il suffit donc de prendre

$$C_3 > \max\left\{({K_4}^{-1}K_2)^{6(\Delta^*-1)/\delta}, {K_3}^{-C_2+\delta n}\right\}$$

pour obtenir l'assertion (3.12), car les constantes K_1 à K_4 ne dépendent que de $L_1,\dots,L_n$ et $c_1,\dots,c_n$. L'assertion (3.13) résulte pour sa part de (3.12), de la Remarque 3.1.1 et du fait que la constante C_2 peut être choisie arbitrairement grande, comme le montre la preuve de (3.12). ■

Théorème 3.1.4 *Supposons que la famille de parallélépipèdes $\Pi(Q)_{Q>1}$ satisfasse*

$$\forall Q > 1,\ \lambda_{n-1}(Q) < Q^{-\delta}. \tag{3.17}$$

Alors il existe $Q_1 > 0$ ne dépendant que de $\delta, \underline{L}, \underline{c}$ telle que

$$\forall Q > Q_1,\ \forall i \in \Sigma(\underline{c},\delta),\ a^*_i.g^*_n(Q) = 0. \tag{3.18}$$

Preuve : Nous procédons comme annoncé dans l'introduction de cette section. Appelons

$$\mathcal{P} = \{Q \in]1,+\infty[\mid \lambda_{n-1}(Q) < Q^{-\delta}, \text{ et } \exists i \text{ tel que } a^*_i.g^*_n(Q) \neq 0\},$$

et supposons que $\mathcal{P}$ soit non bornée. Nous nous ramenons d'abord au cas où $L_1,\dots,L_n$ ont des coefficients *entiers* algébriques réels. Appelons pour cela d le plus petit commun multiple des coefficients dominants des polynômes minimaux des composantes de a^*_i ($i =$

$1, \dots, n$). Les formes linéaires $L'_i = dL_i$ $(i = 1, \dots, n)$ répondent à cette exigence. Si $\Pi'(Q) \stackrel{def}{=} \Pi(L'_1, \dots, L'_n; Q^{c_1}, \dots, Q^{c_n})$, l'application $x \mapsto d^{-1}x$ est une bijection de $\Pi(Q)$ sur $\Pi'(Q)$, et il suit que $a'_i = da_i, g'_i(Q) = dg_i(Q), \lambda'_i(Q) = d\lambda_i(Q)$ pour $i = 1, \dots, n$. Donc si le théorème est vrai pour $\Pi'(Q)_{Q>1}$ il est vrai pour $\Pi(Q)_{Q>1}$. Nous posons maintenant $q = n - 1$ et faisons un certain nombre de choix en vue d'appliquer les théorèmes 2.3.3 et 3.1.2. Choisissons d'abord $0 < \delta_1 < \delta$ tel que $\delta_1 < \delta$ et ϵ tel que $16n^2\epsilon < \delta_1$, puis Δ, m, ω comme dans les hypothèses des théorèmes 2.3.2, 2.3.3 et 2.4.3 en prenant $L^{(i)} = L_i$ pour $i = 1, \dots, n$. La partie $\mathcal{P}$ étant non bornée, il est possible de trouver $Q_1 \in \mathcal{P}$ tel que

$$Q_1 > C_6,\ {Q_1}^{\omega {C_4}^2/C_5} \geq 2^{3mq^2},\ {Q_1}^{\omega {C_4}^2/C_5} \geq D^{mq^2},\ {Q_1}^{\epsilon} > \max\{2^n E, n(1+\epsilon^{-1})\},$$

(où les constantes D, E, C_4, C_5, C_6 sont celles qui ont été introduites dans le Théorème 2.3.3 et le Lemme 3.1.3), puis $Q_2, \dots, Q_m$ satisfaisant

$$\omega \log Q_{h+1} \geq 2 \log Q_h,\ h = 1, \dots, m-1.$$

Puisque $Q_m > \cdots > Q_1$, il en résulte que l'hypothèse (3.4) du Théorème 3.1.2 : ${Q_h}^{\epsilon} > 2^n E$ pour $h = 1, \dots, m$ est satisfaite, de même que

$${Q_h}^{\omega {C_4}^2/C_5} \geq 2^{3mq^2},\ h = 1, \dots, m,$$

qui nous permettra de vérifier l'hypothèse (2.14) du Théorème 2.4.3. Ayant choisi les nombres réels $Q_1, \dots, Q_m$ de cette manière, nous choisissons $r_1, \dots, r_m$ de façon à pouvoir satisfaire les hypothèses (3.5) du Théorème 3.1.2. Pour cela, nous prenons successivement

$$r_1 \geq \frac{\log Q_m}{\epsilon \log Q_1} \text{ entier et } r_h = \left[\frac{r_1 \log Q_1}{\log Q_h}\right] + 1,\ h = 2, \dots, m.$$

Nous avons alors bien

$$r_1 \log Q_1 \leq r_h \log Q_h \leq (1+\epsilon) r_1 \log Q_1 \text{ puisque } \log Q_m > \log Q_h,\ h = 1, \dots, m,$$

ce qui est (3.5). Appliquons le Théorème 2.3.3 à $\epsilon, m, L^{(i)} = L_i, i = 1, \dots, m$ et $\underline{r}$. Nous trouvons un polynôme $P \in \mathcal{A} \backslash \{0\}$ satisfaisant les conclusions de ce théorème. Mais par le choix judicieux de $Q_1, \dots, Q_m, r_1, \dots, r_m$, les hypothèses du Théorème 3.1.2 sont aussi satisfaites. Ainsi

$$\mathrm{Ind}\,(P, M_1, \dots, M_m, r_1, \dots, r_m) \geq m\epsilon.$$

En vue d'obtenir une contradiction, nous vérifions maintenant les conditions d'applications du Théorème 2.4.3. De (3.5) et du choix de Q_{h+1} en fonction de Q_h, nous déduisons

$$\omega r_h \geq \frac{r_h}{1+\epsilon} \frac{\omega \log Q_{h+1}}{\log Q_h} \geq \frac{2}{1+\epsilon} \geq r_{h+1},\ h = 1, \dots, m-1,$$

car $\epsilon < 16n^2\epsilon < \delta_1 < 1$, et (2.12) est donc satisfaite. Pour vérifier (2.13) nous notons que pour $h = 1, \dots, m$, $Q_h \in \mathcal{P}$ et $Q_h > C_6$ donc

$${Q_h}^{C_4} \leq H(M_h) \leq {Q_h}^{C_5}.$$

Mais nous avons judicieusement choisi $C_4/C_5 \leq n-1$. En posant $\Gamma = C_4/C_5$, nous aurons donc $0 < \Gamma \leq q$ (où nous posons $q = n-1$) et

$$H(M_h)^{r_h} \geq {Q_h}^{C_4 r_h} \geq {Q_1}^{C_4 r_1} \geq H(M_1)^{r_1 C_4/C_5} = H(M_1)^{r_1 \Gamma}\,,$$

ce qu'il fallait ; il faut noter que la dernière inégalité provient de la chaîne d'implication

$$H(M_1) \leq {Q_1}^{C_5} \Rightarrow H(M_1)^{r_1 C_4} \leq {Q_1}^{r_1 C_4 C_5} \Rightarrow {Q_1}^{C_4 r_1} \geq H(M_1)^{r_1 C_4/C_5}\,.$$

Nous avons également

$$H(M_h)^{\omega\Gamma} \geq {Q_h}^{\omega\Gamma C_4} = {Q_h}^{\omega {C_4}^2/C_5} \geq 2^{3mq^2},\ h = 1, \ldots, m\,,$$

ce qui est exactement (2.14). Enfin nous devons vérifier l'hypothèse relative à la hauteur de P (i.e. (2.15)). Or

$$\begin{aligned}
H(P)^{q^2} &\leq D^{q^2(r_1+\cdots+r_m)} \text{ (Théorème 2.3.3))} \\
&\leq D^{q^2 m r_1} \text{ (car } r_1+\cdots+r_m \leq r_1(1+\omega+\cdots+\omega^{m-1}) \text{ et } \omega \leq 1) \\
&\leq \left({Q_1}^{\omega {C_4}^2/C_5}\right)^{r_1} \\
&\leq H(M_1)^{\omega r_1 C_4/C_5} \text{ (car } {Q_1}^{C_4} \leq H(M_1)) \\
&= H(M_1)^{\omega r_1 \Gamma}
\end{aligned}$$

Ainsi toutes les hypothèses du Théorème 2.3.3 sont-elles bien satisfaites, ce qui nous permet de conclure que

$$\mathrm{Ind}\,(P, M_1, \ldots, M_m, r_1, \ldots, r_m) \leq \epsilon\,.$$

Mais ceci est en contradiction avec un résultat antérieur. Nous en déduisons que la partie $\mathcal{P}$ est bornée. Le théorème est donc vrai. ■

Voici maintenant l'un des lemmes les plus esthétiques de cette preuve.

Lemme 3.1.5 *Supposons $\mathcal{D} \subset]1, +\infty[$ non bornée telle que la famille de parallélépipèdes $\Pi(Q)_{Q\in\mathcal{D}}$ satisfasse*

$$\forall Q \in \mathcal{D},\ \lambda_{n-1}(Q) < Q^{-\delta}\,.$$

Alors il existe $\mathcal{D}' \subset \mathcal{D}$ non bornée et $h \in \mathbb{R}^n$ tels que

$$\forall Q \in \mathcal{D}',\ g_n^*(Q) = h\,.$$

Plus généralement, pour $Q \in \mathcal{D}$, soit donné $(A_1(Q), \ldots, A_n(Q)) \in \mathbb{R}^n$ satisfaisant

$$A_i(Q) > 0 \text{ pour } i = 1, \ldots, m\,, \tag{3.19}$$

$$A_1(Q) \ldots A_n(Q) = 1\,, \tag{3.20}$$

(3.21) $$\max\{A_1(Q),\dots,A_n(Q),A_1(Q)^{-1},\dots,A_n(Q)^{-1}\}\le Q$$

et soit $\tilde\Pi(Q)=\Pi(L_1,\dots,L_n;A_1(Q),\dots,A_n(Q))$. *Si la famille* $\tilde\Pi(Q)_{Q\in\mathcal{D}}$ *satisfait*

$$\forall Q\in\mathcal{D},\ \tilde\lambda_{n-1}(Q)<Q^{-\delta}\,.$$

Alors il existe $\mathcal{D}'\subset\mathcal{D}$ *non bornée et* $\tilde h\in\mathbb{R}^n$ *tels que*

$$\forall Q\in\mathcal{D}',\ \tilde g_n^*(Q)=\tilde h\,.$$

Preuve : Commençons par la première assertion. D'après le Théorème 3.1.4, il existe $\overline{Q}\in\mathcal{D}$ tel que pour $Q\ge\overline{Q}$ et $Q\in\mathcal{D}$, nous ayons

$$a_i^*.g_n^*(Q)=0 \text{ pour } i\in\Sigma(\underline{c},\delta)\,.$$

Posons $\overline{g}_n^*(Q)=g_n^*(\overline{Q})$. En multipliant $\overline{g}_n^*(Q)$ par un rationnel non nul convenable, nous obtenons $\overline{h}\in\mathbb{Z}^n$ (désormais fixé) à composantes entières premières entre elles, tel que

$$a_i^*.\overline{h}=0 \text{ pour } i\in\Sigma(\underline{c},\delta)\,.$$

Nous allons extraire de $\mathcal{D}$ une partie $\mathcal{D}'$ sur laquelle g_n^* est constamment égal à un multiple rationnel de $\overline{h}$: nous montrerons que pour Q assez grand dans $\mathcal{D}$, nous avons à la fois

$$\overline{h}\in\Pi^*(Q)=\Pi(Q^{c_1}a_1^*(Q),\dots,Q^{c_n}a_n^*(Q)) \text{ (dual de } \Pi(Q))\,,$$

$$\lambda_2^*(Q)>1\,,$$

$$M(Q)=F(Q)g_n^*(Q)\in\Pi^*(Q),\ F(Q)\in\mathbb{Z},\ 1\le|F(Q)|\le n!^2 \text{(cf. Remarque 3.1.1)}\,.$$

Donc $M(Q)$ et $\overline{h}$ sont égaux ou opposés, et comme $\mathcal{D}$ est non bornée, $F(Q)$ prend une valeur une infinité de fois.

Pour cela, posons $C=\max_{1\le i\le n}|a_i^*.\overline{h}|$. Les deux faits suivants
– pour $i\notin\Sigma(\underline{c},\delta)$, $c_i+\delta/2\ge0$ donc $|a_i^*.\overline{h}|\le CQ^{-\delta/2}Q^{-c_i}$,
– pour $i\in\Sigma(\underline{c},\delta)$, $|a_i^*.\overline{h}|=0\le Q^{-c_i}$,
montrent que pour $Q\ge Q_0=\max\{Q^{2/\delta},\overline{Q}\}$, $\overline{h}\in\Pi^*(Q)$. Mais nous avons de plus $\lambda_{n-1}(Q)<Q^{-\delta}$, et le théorème des parallélépipèdes duaux de Mahler (Théorème 1.1.14) nous dit donc que

$$\lambda_2^*(Q)\gg\frac{1}{\lambda_{n+1-2}(Q)}=\frac{1}{\lambda_{n-1}(Q)}>Q^{\delta}\,.$$

Ainsi il existe $Q_1>0$ pour lequel $Q\ge Q_1\Rightarrow\lambda_2^*(Q)>1$ (nous voyons ici pourquoi l'hypothèse $\lambda_{n-1}(Q)<Q^{-\delta}$ est si agréable). Par définition de $\lambda_2^*(Q)$, nous avons

$$Q\in\mathcal{D}\text{ et }Q\ge\max\{Q_0,Q_1\}\Rightarrow\Pi^*(Q)\cap\mathbb{R}^n\subset\mathbb{R}\overline{h}\,.$$

D'après la Remarque 3.1.1, nous pouvons écrire $g_n^*(Q)=M(Q)/F(Q)$ avec les conventions de cette remarque. Les mêmes arguments que ceux utilisés dans le Lemme 3.1.3 montrent qu'il existe $C'>0$ tel que :

$$|a_i^*.g_n^*(Q)|\le C'Q^{-\delta(n-1)}Q^{-c_i},\ \text{pour } i=1,\dots,n\,.$$

Il suit de cela que

$$|a_i^*.M(Q)| = |a_i^*.F(Q)g_n^*(Q)| \leq C'n!^2 Q^{-\delta(n-1)}Q^{-c_i}, \text{ pour } i = 1, \dots, n\,.$$

Ainsi pour $Q \geq Q_2 = (C'n!^2)^{1/(\delta(n-1))}$, $M(Q) \in \Pi^*(Q)$, et nous avons donc établi

$$Q \in \mathcal{D} \text{ et } Q \geq \max\{Q_0, Q_1, Q_2\} \Longrightarrow \begin{cases} \overline{h} \in \Pi^*(Q)\,, \\ \Pi^*(Q) \cap \mathbb{Z}^n \subset \mathbb{R}\overline{h}\,, \\ F(Q)g_n^*(Q) = M(Q) \in \Pi^*(Q)\,. \end{cases}$$

Définissons maintenant $\mathcal{D}_0 = \{Q \in \mathcal{D}, Q \geq \max\{Q_0, Q_1, Q_2\}\}$. C'est une partie de $\mathcal{D}$ non bornée. De plus pour $Q \in \mathcal{D}_0, M(Q) = \pm\overline{h}$ car ce sont deux vecteurs de $\Pi^*(Q) \cap \mathbb{Z}^n$, qui sont $\mathbb{Q}$-proportionnels et à composantes premières entre elles. Il suffit pour conclure d'extraire de $\mathcal{D}_0$ une partie $\mathcal{D}_1$ dénombrable discrète (donc non bornée), et de remarquer que $Q \mapsto F(Q)$ est à valeurs dans l'ensemble fini $\{-n!^2, \dots, n!^2\} \setminus \{0\}$, ce qui assure l'existence de $\mathcal{D}' \subset \mathcal{D}_1$ infinie (donc non bornée car $\mathcal{D}_1$ est discrète) sur laquelle cette fonction vaut, disons, a. Alors

$$\forall Q \in \mathcal{D}',\ g_n^*(Q) = \frac{\pm\overline{h}}{a}\,,$$

et en posant $h = \pm a^{-1}\overline{h}$, nous avons montré la première partie du lemme.

Passons à la généralisation. Il est naturel de poser $c_i(Q) = \log A_i(Q)/\log Q$ pour $i = 1, \dots, n$, ce qui est possible d'après (3.19), après quoi nous avons

$$\begin{cases} c_1(Q) + \cdots + c_n(Q) = 0 & \text{d'après (3.20)}\,, \\ |c_i(Q)| \leq 1 \text{ pour } i = 1, \dots, n & \text{d'après (3.21)}\,. \end{cases}$$

La difficulté par rapport à la précédente partie vient de ce que les c_i dépendent de Q, et nous ne pouvons donc pas utiliser directement le Théorème 3.1.4 (à cause de la remarque faite au cours de la preuve du Théorème 3.1.2). Toutefois nous observons que

$$K = \{(c_1, \dots, c_n) \in \mathbb{R}^n \mid c_1 + \cdots + c_n = 0 \text{ et } |c_i| \leq 1 \text{ pour } i = 1, \dots, n\}$$

est un compact de $\mathbb{R}^n$. Nous pouvons donc trouver un élément $\underline{\gamma} = (\gamma_1, \dots, \gamma_n)$ de K, et une partie $\mathcal{D}_1$ de $\mathcal{D}$ non bornée telle que :

$$\forall Q \in \mathcal{D}_1,\ \forall i = 1, \dots, n,\ |c_i(Q) - \gamma_i| < \frac{\delta}{8}\left(< \frac{\delta}{2}\right)\,.$$

Si nous appelons $\Pi^{\#}(Q) = \Pi(L_1, \dots, L_n; Q^{\gamma_1}, \dots, Q^{\gamma_n})$, nous obtenons alors que pour $Q \in \mathcal{D}_1$, $\lambda_{n-1}^{\#}(Q) < Q^{-\delta/2}$. D'après la première partie du lemme, il existe alors $\mathcal{D}_2 \subset \mathcal{D}_1$ non bornée, telle que $g_n^{\#*}(Q)$ soit indépendant de $Q \in \mathcal{D}_2$. Plus précisément, en remplaçant $\Sigma(\underline{c}, \delta)$ par $\Sigma(\underline{\gamma}, \delta/2)$, et en reprenant la preuve déjà faite, nous obtiendrons

$$g_n^{\#*}(Q) = \frac{m}{F} \text{ avec } \begin{cases} F \in [-n!^2, n!^2] \cap (\mathbb{Z} \setminus \{0\})\,, \\ m \in \Pi^{\#*}(Q) \text{ pour } Q \in \mathcal{D}_2\,, \\ m \in \mathbb{Z}^n \text{ à composantes premières entre elles.} \end{cases}$$

Si nous exhibons $\mathcal{D}_3 \subset \mathcal{D}_2$ non bornée telle que $m \in \tilde{\Pi}^*(Q)$ pour $Q \in \mathcal{D}_3$, nous aurons terminé car cela nous fournira l'équivalent du $\overline{h}$ précédent. Or si i est tel que
– $a_i^*.m = 0$, clairement $|a_i^*.m| \leq Q^{-c_i(Q)}$,
– $a_i^*.m \neq 0$, le Théorème 3.1.4 utilisé avec $\underline{\gamma}$ au lieu de $\underline{c}$ et $\Sigma(\underline{\gamma}, \delta/2)$ au lieu de $\Sigma(\underline{c}, \delta)$ montre que $\gamma_i + \delta/4 < 0$. Donc pour $Q \in \mathcal{D}_2$,

$$\gamma_i(Q) - \frac{\delta}{8} < c_i(Q) < \gamma_i(Q) + \frac{\delta}{8} < -\frac{\delta}{4} + \frac{\delta}{8} = -\frac{\delta}{8}\,,$$

et pour $Q \in \mathcal{D}_2$ assez grand $|a_i^*.m| \leq Q^{-c_i(Q)}$. Ainsi nous pouvons trouver $\mathcal{D}_3$ répondant aux exigences formulées ci-dessus.

Maintenant, comme dans la première partie, en extrayant de $\mathcal{D}_3$ une partie $\mathcal{D}_4$ non bornée pour laquelle nous ayons $\tilde{\lambda}_2^*(Q) > 1$ pour $Q \in \mathcal{D}_4$ puis une partie $\mathcal{D}_5 \subset \mathcal{D}_4$ non bornée telle que pour $Q \in \mathcal{D}_5$, on ait $\tilde{F}(Q)\tilde{g}_n^*(Q) = \tilde{M}(Q) \in \tilde{\Pi}^*(Q) \cap \mathbb{Z}^n$, nous constatons que les vecteurs m et $\tilde{M}(Q)$ sont alors égaux pour $Q \in \mathcal{D}_5$ et nous pouvons extraire de $\mathcal{D}_5$ une partie $\mathcal{D}'$ sur laquelle

$$\tilde{g}_n^*(Q) = \frac{m}{a'},\ a' \in [-n!^2, n^2] \cap \mathbb{Z} \setminus \{0\}\,,$$

et poser $\tilde{h} = {a'}^{-1} m$ pour avoir la conclusion. ■

Nous pouvons alors enfin achever la preuve du théorème des sous-espaces fort dans le cas $d = n - 1$.

Lemme 3.1.6 *Supposons $\mathcal{D} \subset]1, +\infty[$ non bornée telle que la famille de parallélépipèdes $\Pi(Q)_{Q\in\mathcal{D}}$ satisfasse*

$$\forall Q \in \mathcal{D},\ \lambda_{n-1}(Q) < \lambda_n(Q) Q^{-\delta}\,. \tag{3.22}$$

Alors il existe $\mathcal{D}' \subset \mathcal{D}$ non bornée et $h \in \mathbb{R}^n$, tels que la famille de parallélépipèdes $\Pi(Q)_{Q\in\mathcal{D}'}$ satisfasse

$$\forall Q \in \mathcal{D}',\ g_n^*(Q) = h\,.$$

Preuve : Nous allons utiliser le lemme de Davenport (Théorème 1.1.12) pour associer aux $\Pi(Q)$ des parallélépipèdes $\Pi'(Q)$ qui satisferont les hypothèses de la deuxième partie du Lemme 3.1.5, donc g'^*_n sera constant sur une certaine partie non bornée de $\mathcal{D}$, mais le lemme de Davenport nous dira aussi que g_n^* et g'^*_n sont proportionnels, de sorte que le même type d'arguments que dans le Lemme 3.1.5 fonctionnera encore.

Pour $Q \in \mathcal{D}$, définissons

$$\begin{aligned} \rho_0(Q) &= \left(\lambda_1(Q) \dots \lambda_{n-2}(Q)\lambda_{n-1}(Q)^2\right)^{1/n}\,, \\ \rho_i(Q) &= \rho_0(Q)/\lambda_i(Q),\ i = 1, \dots, n-1\,, \\ \rho_n(Q) &= \rho_0(Q)/\lambda_{n-1}(Q)\,. \end{aligned} \tag{3.23}$$

Les hypothèses (1.1), (1.1) et (1.2) du lemme de Davenport sont alors satisfaites par les nombres réels $\rho_1(Q), \dots, \rho_n(Q)$. Il existe donc une permutation $\sigma(Q)$ de $\{1, \dots, n\}$ telle que le parallélépipède

$$\Pi'(Q) \stackrel{def}{=} \Pi(\rho_1(Q)Q^{-c_{\sigma(Q)(1)}}L_{\sigma(Q)(1)}, \dots, \rho_n(Q)Q^{-c_{\sigma(Q)(n)}}L_{\sigma(Q)(n)}; 1, \dots, 1)$$

ait des minima successifs $\lambda'_1(Q), \dots, \lambda'_n(Q)$ satisfaisant

$$2^{-n}\lambda_i(Q)\rho_i(Q) \leq \lambda'_i(Q) \leq 2^{n^2}n!^2\lambda_i(Q)\rho_i(Q), \text{ pour } i = 1, \dots, n\,. \tag{3.24}$$

Comme le groupe symétrique d'ordre n est fini et $\mathcal{D}$ est non bornée, nous pouvons supposer quitte à diminuer $\mathcal{D}$ que $\sigma(Q) = \sigma$, indépendante de Q. Nous avons alors

$$\begin{aligned}\Pi'(Q) &= \Pi(\rho_1(Q)Q^{-c_{\sigma(1)}}L_{\sigma(1)}, \dots, \rho_n(Q)Q^{-c_{\sigma(n)}}L_{\sigma(n)}; 1, \dots, 1)\\ &= \Pi(L_{\sigma(1)}, \dots, L_{\sigma(n)}; \rho_1(Q)^{-1}Q^{c_{\sigma(1)}}, \dots, \rho_n(Q)^{-1}Q^{c_{\sigma(n)}})\\ &= \Pi(L'_1, \dots, L'_n; A'_1(Q), \dots, A'_n(Q))\,,\end{aligned}$$

en posant $L'_i = L_{\sigma_i}$ et $A'_i(Q) = \rho_i(Q)^{-1}Q^{c_{\sigma(i)}}$ pour $i = 1, \dots, n$. Il nous reste à montrer que les hypothèses de la seconde partie du Lemme 3.1.5 sont satisfaites. La somme des c_i étant nulle et le produit des $\rho_i(Q)$ valant l'unité, nous avons clairement $A'_1(Q)\dots A'_n(Q) = 1$. De même $A'_i(Q) > 0$ pour $i = 1, \dots, n$ est évidente. Nous avons alors à estimer

$$\lambda'_{n-1}(Q) \text{ et } \max\{A'_1(Q), \dots, A'_n(Q), A'_1(Q)^{-1}, \dots, A'_n(Q)^{-1}\}\,. \tag{3.25}$$

D'après (3.24), nous avons

$$\begin{aligned}\lambda'_{n-1}(Q) &\ll \lambda_{n-1}(Q)\rho_{n-1}(Q)\\ &= \rho_0(Q) \text{ d'après (3.23)}\\ &= (\lambda_1(Q)\dots\lambda_n(Q))^{1/n}\left(\frac{\lambda_{n-1}(Q)}{\lambda_n(Q)}\right)^{1/n} \text{ d'après (3.23)}\\ &\ll \left(\frac{\lambda_{n-1}(Q)}{\lambda_n(Q)}\right)^{1/n} \text{ d'après le Théorème 1.1.11}\\ &\ll Q^{-\delta/n} \text{ d'après (3.22)}\end{aligned}$$

Pour estimer le maximum de (3.25), nous avons besoin d'établir d'abord

$$\lambda_1(Q) \gg Q^{-1} \text{ et } \lambda_n(Q) \ll Q\,. \tag{3.26}$$

Pour cela, notons que si $y \in \lambda\Pi(Q) \cap \mathbb{Z}^n$, $y \neq 0$, alors $\max_{1\leq i\leq n}|Q^{-c_i}L_i(y)| \leq \lambda$. Mais pour tout vecteur $y \in \mathbb{Z}^n \setminus \{0\}$, nous avons

$$\max_{1\leq i\leq n}|Q^{-c_i}L_i(y)| \geq Q^{-1}\max_{1\leq i\leq n}|L_i(y)| \gg Q^{-1}\|y\|_\infty \geq Q^{-1}\,,$$

en observant que $-1 \leq c_i \leq 1$ et que $y \mapsto \|y\|_\infty$ et $y \mapsto \max_{1\leq i\leq n}|L_i(y)|$ sont deux normes équivalentes sur $\mathbb{R}^n$. Cela prouve que $\lambda_1(Q) \gg Q^{-1}$. D'autre part si $(e_1, \dots, e_n)$ est la base

canonique de $\mathbb{R}^n$, nous avons $|L_i(e_j)| \leq Q^{c_i+1}$ pour $1 \leq i,j \leq n$. Cela assure que $\lambda_n(Q) \ll Q$ (noter qu'il existe $C > 0$ telle que $CQ\Pi(Q) \cap \mathbb{Z}^n$ contienne $e_1, \ldots, e_n$). Donc les deux assertions de (3.26) sont valables. Nous en déduisons d'après (3.22)

$$\rho_1(Q) = \lambda_1(Q)^{-1}\rho_0(Q) \ll \lambda_1(Q)^{-1}\left(\frac{\lambda_{n-1}(Q)}{\lambda_n(Q)}\right)^{1/n} \leq \lambda_1(Q)^{-1} \ll Q\,, \tag{3.27}$$

et

$$\rho_n(Q) = \lambda_{n-1}(Q)^{-1}\rho_0(Q) \gg \lambda_{n-1}(Q)^{-1}\left(\frac{\lambda_{n-1}(Q)}{\lambda_n(Q)}\right)^{1/n} \geq \lambda_n(Q)^{-1} \gg Q^{-1}\,. \tag{3.28}$$

L'avant dernière égalité vient de ce que $x^{1/n-1} \geq 1$ pour $0 < x < 1$, et de ce que d'après le Théorème 1.1.11,

$$\rho_0(Q) = (\lambda_1(Q)\ldots\lambda_n(Q))^{1/n} \gg \left(\frac{\lambda_{n-1}(Q)}{\lambda_n(Q)}\right)^{1/n}\,.$$

En regroupant (3.27), (3.28) et (1.1) du lemme de Davenport, nous obtenons :

$$Q^{-1} \ll \rho_n(Q) \leq \cdots \leq \rho_1(Q) \ll Q \text{ d'où } Q^{-2} \ll A'_i(Q) \ll Q^2 \text{ pour } i = 1, \ldots, n\,.$$

Il existe donc $\mathcal{D}_1 \subset \mathcal{D}$ non borné tel que pour $Q \in \mathcal{D}_1$

$$\begin{array}{l}
\lambda'_{n-1}(Q) < (Q^3)^{-\delta_2},\ \text{avec } \delta_2 = \delta/(4n)\,,\\
\max\{A'_1(Q), \ldots, A'_n(Q), {A'}_1(Q)^{-1}, \ldots, {A'}_n(Q)^{-1}\} \leq Q^3\,,\\
A'_1(Q)\ldots A'_n(Q) = 1\,,\\
A'_i(Q) > 0 \text{ pour } i = 1, \ldots, n\,.
\end{array}$$

Nous avons bien les hypothèses du Lemme 3.1.5 modulo la présence de Q^3 au lieu de Q. Mais il suffit de faire intervenir

$$\mathcal{P}_1 = \{Q' > 1 \mid \exists Q \in \mathcal{D}_1 \text{ et } Q' = Q^3\} \text{ et } A''_i(Q') = A'_i(Q) \text{ pour } i = 1, \ldots, n \text{ si } Q' = Q^3\,,$$

pour pouvoir appliquer la deuxième partie du Lemme 3.1.5 à la famille de parallélépipèdes $\Pi''(Q')_{Q' \in \mathcal{P}_1}$ où

$$\Pi''(Q') = \Pi(L'_1, \ldots, L'_n; A''_1(Q'), \ldots, A''_n(Q'))$$

avec δ_2 à la place de δ. Si $g''_1(Q'), \ldots, g''_n(Q')$ sont comme dans le Lemme 1.1.4 pour le parallélépipède $\Pi''(Q')$, et si $({g''}^*_1(Q'), \ldots, {g''}^*_n(Q'))$ est la base duale de $(g''_1(Q'), \ldots, g''_n(Q'))$, le Lemme 3.1.5 dit qu'il existe $\mathcal{P}_2 \subset \mathcal{P}_1$ non bornée telle que

$$\forall Q' \in \mathcal{P}_2,\ {g''}^*_n(Q') = h'',\ h'' \in \mathbb{R}^n\,.$$

Notons $T(Q) = \mathbb{R}g_1(Q) \oplus \cdots \oplus \mathbb{R}g_{n-1}(Q)$. D'après l'inégalité (1.5) du lemme de Davenport,

$$\begin{array}{rcl}
\forall g \in \mathbb{Z}^n \setminus T(Q),\ \max|L'_i(g)A'_i(Q)| & = & \max|\rho_i(Q)Q^{-c_{\sigma_i}}L_{\sigma(i)}(g)|\\
& \gg & \lambda_n(Q)\rho_n(Q) \gg \lambda'_n(Q) \gg 1 \text{ d'après (3.24)}\,.
\end{array}$$

Donc $g'_1(Q), \dots, g'_{n-1}(Q)$ doivent appartenir à $T(Q)$, sinon il existerait une constante $C > 0$ indépendante de Q telle que

$$g'_i(Q) \notin C\Pi'(Q) \text{ d'où } C < \lambda'_i(Q) \leq \lambda'_{n-1}(Q) < Q^{-3\delta/4n}\,,$$

ce qui est impossible. Ainsi

$$\begin{array}{rl} & \forall Q \in \mathcal{D}_1,\ \mathbb{R}g'_1(Q) \oplus \cdots \oplus \mathbb{R}g'_{n-1}(Q) = \mathbb{R}g_1(Q) \oplus \cdots \oplus \mathbb{R}g_{n-1}(Q) \\ \iff & \forall Q \in \mathcal{D}_1,\ \mathbb{R}g'^*_n(Q) = \mathbb{R}g^*_n(Q)\,. \end{array}$$

Si nous écrivons maintenant avec les notations de la Remarque 3.1.1

$$g^*_n(Q) = \frac{M(Q)}{F(Q)} \text{ et } g'^*_n(Q) = \frac{M'(Q)}{F'(Q)}\,,$$

nous avons $M(Q) = M'(Q)$ pour $Q \in \mathcal{D}_1$. Or, posons maintenant

$$\mathcal{D}_2 \stackrel{def}{=} \{Q \in \mathcal{D}_1 \mid Q^3 \in \mathcal{P}_1\}\,,$$

qui est non borné et contenu dans $\mathcal{D}_1$. Pour $Q \in \mathcal{D}_2$, $g'^*_n(Q) = g''^*_n(Q^3) = h'' = M(Q)/F'(Q)$. Comme $F(Q)$ et $F'(Q)$ ne prennent qu'un nombre fini de valeurs sur $\mathcal{D}_2$, il en est de même de $M(Q) = F'(Q)h''$ et de $g^*_n(Q) = M(Q)/F(Q)$. Nous pouvons donc trouver une partie $\mathcal{D}' \subset \mathcal{D}_2 \subset \mathcal{D}_1 \subset \mathcal{D}$ non bornée telle g^*_n est constant sur $\mathcal{D}'$. Ceci achève la preuve du lemme, et donc du théorème des sous-espaces fort dans le cas $d = n - 1$, car en fait nous pouvons supposer que (3.1) *et* (3.2) sont satisfaites. ■

Passons alors au cas général.

3.2 Preuve du théorème des sous-espaces fort dans le cas général

Compte tenu de ce qui a déjà éte fait jusqu'ici, le passage du cas $d = n - 1$ au cas quelconque est essentiellement formel mais astucieux. L'idée consiste à écrire $p = n - d$, et à montrer que le p-ième composé de Mahler du parallélépipède $\Pi(Q)$, $Q \in \mathcal{D}$, qui est un parallélépipède de $\mathbb{R}^n_p \simeq \mathbb{R}^l$ où $l = \binom{n}{p}$, a ses l minima successifs $\nu_1(Q), \dots, \nu_l(Q)$ qui satisfont les hypothèses du Lemme 3.1.6. Si donc $V_i(Q) \in \nu_i(Q)\Pi^{(p)}(Q)$ sont entiers et indépendants, $V^*_l(Q)$ sera constant pour $Q \in \mathcal{D}$ assez grand, et en utilisant les propriétés de la section 1.2, il ne sera plus difficile de conclure. Précisons maintenant tout cela.

Nous gardons bien sûr les notations du Théorème 3.0.2 et de la Définition 3.0.1. Cela dit, nous pouvons supposer que les formes $L_1, \dots, L_n$ sont de déterminant 1 ; si elles ne l'étaient pas, nous poserions $\Delta = |\det(L_1, \dots, L_n)|^{1/n}$ (qui est un nombre algébrique réel), et nous remplacerions L_i par $\pm L_i/\Delta$ pour $i = 1, \dots, n$, qui sont encore des formes linéaires indépendantes sur $\mathbb{R}^n$. Ce faisant nous changerions $\Pi(Q)$ en $\Pi^\Delta(Q)$ défini par

$$\Pi^\Delta(Q) = \Pi(L_1/\Delta, \dots, L_n/\Delta; Q^{c_1}, \dots, Q^{c_n})$$

image de $\Pi(Q)$ par l'homothétie de rapport Δ, et $\Pi^{\Delta}(Q)$ remplit par conséquent la condition $\lambda_{n-1}^{\Delta}(Q) < \lambda_n^{\Delta}(Q)Q^{-\delta}$ (avec des notations évidentes).

De plus nous pouvons aussi supposer

$$|c_i| \leq 1/n \text{ pour } i = 1, \dots, n\,. \tag{3.29}$$

En effet, si nous remplaçons c_i par ρc_i pour $i = 1, \dots, n$, où $\rho > 0$, nous transformons $\Pi(Q)$ en $\Pi_\rho(Q) = \Pi(Q^\rho)$ et $Q \mapsto Q^\rho$ est une bijection de $]1, +\infty[$.

Nous considérons maintenant la famille de parallélépipèdes $\Pi(Q)_{Q\in\mathcal{D}}$ avec les hypothèses supplémentaires ci-dessus. Nous posons $p = n-d$, et allons construire $\Pi^{(p)}(Q)$ comme annoncé. Pour $\sigma = (i_1, \dots, i_p) \in C(n,p)$, posons

$$c_\sigma = \sum_{k=1}^{p} c_{i_k}\,. \tag{3.30}$$

L'hypothèse (3.29) sert bien entendu à pouvoir dire à ce stade que $|c_\sigma| \leq 1$ pour tout $\sigma \in C(n,p)$. D'autre part, $C(n,p)$ est un système de représentants de

$$A(n,p) = \{(i_1, \dots, i_p) \in \{1, \dots, n\}^p \mid k \neq k' \Rightarrow i_k \neq i_{k'}\}$$

modulo la relation d'équivalence définie sur $C(n,p)$ par

$$\sigma = (i_1, \dots, i_p)\ \mathcal{R}\ \tau = (j_1, \dots, j_p) \Leftrightarrow \exists s \in \mathfrak{S}_p \mid j_l = i_{s(l)} \text{ pour } 1 \leq l \leq n\,.$$

Nous en déduisons par conséquent que

$$\sum_{\sigma\in C(n,p)} c_\sigma = 0\,.$$

Appliquons alors la théorie des parallélépipèdes composés de Mahler (Théorème 1.2.12) qui à $\Pi(Q) = \Pi(Q^{-c_1}a_1, \dots, Q^{-c_n}a_n)$ permet d'associer $\Pi^{(p)}(Q) = \Pi\big((A_\sigma)_{\sigma\in C(n,p)}\big)$. Pour un ordre sur $C(n,p)$ qui rend $\tau \mapsto \lambda_\tau$ croissante (cf. Définition 1.2.11), le dernier élément est $(d+1, \dots, n)$ et l'avant-dernier est $(d, d+2, \dots, n)$. D'après le théorème de Mahler,

$$\nu_i(Q) \ll \lambda_{\tau_i}(Q) \ll \nu_i(Q), \text{ pour } i = 1, \dots, l\,.$$

En particulier,

$$\nu_l(Q) \ll \lambda_{d+1}(Q)\dots\lambda_n(Q) \ll \nu_l(Q) \text{ et } \nu_{l-1}(Q) \ll \lambda_d(Q)\lambda_{d+2}(Q)\dots\lambda_n(Q) \ll \nu_{l-1}(Q)\,.$$

Grâce à l'hypothèse $\lambda_d(Q) < \lambda_{d+1}(Q)Q^{-\delta}$ nous avons heureusement

$$\nu_{l-1}(Q) \ll \nu_l(Q)Q^{-\delta} \text{ d'où } \forall Q \in \mathcal{D}_1,\ \nu_{l-1}(Q) < \nu_l(Q)Q^{-\delta/2}\,, \tag{3.31}$$

où $\mathcal{D}_1$ est une partie non bornée de $\mathcal{D}$. Nous pouvons donc utiliser le Lemme 3.1.6 avec $\Pi^{(p)}(Q)$ et $\delta/2$ en lieu et place de $\Pi(Q)$ et δ. La conclusion obtenue est que si pour $i = 1, \dots, l$, nous

notons $V_i(Q) \in \nu_i(Q)\Pi^{(p)}(Q)$ des vecteurs entiers indépendants de $\mathbb{R}^n_p$, et si $(V_i^*(Q))_{1\leq i\leq l}$ la base duale pour le produit scalaire de $\mathbb{R}^n_p$, il existe une partie $\mathcal{D}_2 \subset \mathcal{D}_1$ non bornée et $H \in \mathbb{R}^n_p$, avec

$$V_l^*(Q) = H \text{ pour } Q \in \mathcal{D}_2\,.$$

Mais d'après le théorème de Mahler, pour $\tau \in C(n,p), \tau \neq (d+1,\dots,n)$ et $\sigma \in C(n,p)$:

$$|A_\sigma.G_\tau(Q)| \ll \nu_{l-1}(Q)Q^{c_\sigma}\,.$$

En effet, avec les notations de la section 1.2.2, nous avons $G_\tau = \lambda_\tau X_\tau$, et d'après l'identité de Laplace, nous obtenons

$$\begin{aligned} |A_\sigma.X_\tau| &\leq p!Q^{c_\sigma}\,,\\ |A_\sigma.G_\tau(Q)| &\leq p!\lambda_\tau(Q)Q^{c_\sigma}\,,\\ |A_\sigma.G_\tau(Q)| &\ll \nu_{l-1}(Q)Q^{c_\sigma}\,. \end{aligned}$$

Cette dernière propriété nous permet d'affirmer que

$$\bigoplus_{\tau\neq\tau_l} \mathbb{R}G_\tau(Q) = \bigoplus_{i=1}^{l-1} \mathbb{R}V_i(Q) \text{ pour } Q \in \mathcal{D}_3\,,$$

où $\mathcal{D}_3$ est une partie non bornée de $\mathcal{D}_2$. Il suit que $(G_{\tau_l}(Q))^*$ et $V_l^*(Q)$ sont $\mathbb{R}$-proportionnels (et même $\mathbb{Q}$-proportionnels) — il convient de remarquer que d'après le Lemme 1.2.6, nous jouissons de $(G_{\tau_l}(Q))^* = (G^*(Q))_{\tau_l}$. Nous avons donc établi

$$\exists\lambda \in \mathbb{Q}^* \text{ tel que } G^*(Q)_{\tau_l} = g_{d+1}^*(Q) \wedge \cdots \wedge g_n^*(Q) = \lambda H \text{ pour } Q \in \mathcal{D}_3\,.$$

Il existe donc d'après le Lemme1.2.6 un sous-espace de S^* de $\mathbb{R}^n$ de dimension $p = n-d$, tel que pour tout $Q \in \mathcal{D}_3, g_i^*(Q) \in S^*$ pour $i = d+1,\dots,n$. Si S désigne l'orthogonal de S^*, nous avons finalement bien

$$\forall Q \in \mathcal{D}',\ S = \mathbb{Q}g_1(Q) \oplus \cdots \oplus \mathbb{Q}g_d(Q)\,,$$

comme demandé dans le Théorème 3.0.2 qui est donc complètement démontré.

3.3 Preuve du théorème des sous-espaces

La preuve du Théorème 3.0.3, dont nous reprenons les notations, se déroule en cinq étapes. Soit $\delta > 0$.

1. Nous commençons par nous ramener au cas où les formes $L_1,\dots,L_n$ sont à coefficients algébriques *réels*.

2. Nous remarquons que tout ensemble borné $\mathcal{B}$ de solutions de (3.3) est contenu dans une réunion finie de sous-espaces non triviaux de $\mathbb{Q}^n$, et qu'il suffit de considérer les solutions x de (3.3) qui n'annulent pas le produit $L_1(x)\dots L_n(x)$.

3. En utilisant des faits de théorie algébrique des nombres, nous trouvons $A > 0$ tel que toute solution x de (3.3) assez grande satisfasse

$$\|x\|_\infty^{-A} \leq |L_i(x)| \leq \|x\|_\infty^2,\ i = 1, \ldots, n\,.$$

4. Nous montrons qu'il existe $\delta' > 0$ et un nombre fini de n-uplets $(c_1, \ldots, c_n)$ satisfaisant (3.1) tels que toute solution x de (3.3) assez grande satisfasse

$$|L_i(x)| \leq \|x\|_\infty^{c_i - \delta'},\ i = 1, \ldots, n\,.$$

5. Nous montrons par un raisonnement par l'absurde utilisant le théorème des sous-espaces fort qu'il existe un nombre fini de sous-espaces $T_1, \ldots, T_k$ non triviaux de $\mathbb{Q}^n$, tels que le système

$$\forall i \in \{1, \ldots, n\},\ |L_i(x)| \leq \|x\|_\infty^{c_i - \delta'},\ x \in \mathbb{Z}^n \setminus \{0\} \tag{3.32}$$

ait ses solutions dans $T_1 \cup \cdots \cup T_k$.

Détaillons maintenant chacun de ces points.

1. Pour chacune des formes linéaires L_j, nous écrivons $L_j = \mathcal{R}e\ L_j + i\mathcal{I}m\ L_j$ comme somme de ses parties réelles et imaginaires, toutes deux à coefficients réels. Puisque $L_1, \ldots, L_n$ sont indépendantes, et donc $L_2, \ldots, L_n$ aussi, soit $\mathcal{R}e\ L_1, L_2, \ldots, L_n$, soit $\mathcal{I}m\ L_1, L_2, \ldots, L_n$ sont indépendantes. En répétant ce procédé avec $L_2, \ldots, L_n$, nous obtenons de nouvelles formes $L'_1, \ldots, L'_n$ indépendantes sur $\mathbb{R}^n$, à coefficients réels, telles que

$$\forall j \in \{1, \ldots, n\},\ L'_j = \mathcal{R}e\ L_j \text{ ou } L'_j = \mathcal{I}m\ L_j \text{ d'où } |L'_j(x)| \leq |L_j(x)|\,.$$

Ainsi, si x est solution de (3.3) avec $L_1, \ldots, L_n$, il est solution de (3.3) avec $L'_1, \ldots, L'_n$, et nous pouvons bien supposer que $L_1, \ldots, L_n$ sont à coefficients algébriques *réels*.

2. Ce fait est clair, car un ensemble borné de solutions de (3.3) est fini puisque $\mathbb{Z}^n$ est discret. Alors :

$$\mathcal{B} \subset \bigcup_{x \in \mathcal{B}} \mathbb{Q}x\,.$$

D'autre part une solution x de (3.3) qui annule le produit $L_1(x) \ldots L_n(x)$ se trouve dans la réunion des noyaux des formes linéaires $L_1, \ldots, L_n$, qui sont indépendantes. Ces noyaux sont nuls ou non triviaux et deux-à-deux distincts.

3. D'une part, nous disposons d'une application linéaire

$$\begin{array}{rccc} \phi & : & \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ & & x & \longmapsto & (L_1(x), \ldots, L_n(x))\,. \end{array}$$

En considérant la norme fonctionnelle $\|\phi\| = \sup_{\|x\|_\infty \leq 1} \|\phi(x)\|_\infty$ sur $\mathrm{End}_{\mathbb{R}}(\mathbb{R}^n)$, nous avons alors

$$\|x\|_\infty \geq \|\phi\| \text{ et } 1 \leq j \leq n \Rightarrow |L_j(x)| \leq \|\phi(x)\|_\infty \leq \|\phi\|\|x\|_\infty \leq \|x\|_\infty^2 .$$

D'autre part, soit $j \in \{1, \ldots, n\}$. La forme L_j est à coefficients algébriques ; soit K_j le corps engendré sur $\mathbb{Q}$ engendré par ses composantes et d_j son degré. Il existe $\alpha_j \in K_j$, *entier* non nul tel que $\alpha_j L_j$ soit à coefficients dans l'anneau des entiers de K_j. Envisageons deux cas séparément.

Cas 1 : $d_j = 1$.
Alors α_j est un entier (relatif) non nul, donc pour toute solution x de (3.3) n'annulant pas $L_j(x)$, $L_j(x)$ est un entier non nul donc supérieur ou égal à 1, donc $|L_j(x)| \geq 1/|\alpha_j|$.

Cas 2 : $d_j > 1$.
Appelons $\sigma_1, \ldots, \sigma_{d_j}$ les plongements de K_j dans $\mathbb{C}$. Pour x solution de (3.3) n'annulant pas $L_j(x)$, $L_j(x)$ est un entier de K_j non nul, donc

$$|N_{K_j/\mathbb{Q}}(L_j(x))| \geq |N_{K_j/\mathbb{Q}}(\alpha_j)|^{-d_j} .$$

D'autre part

$$|N_{K_j/\mathbb{Q}}(L_j(x))| = \prod_{k=1}^{d_j} |\sigma_k(L_j(x))| \leq |L_j(x)|\ C_j\ \|x\|_\infty^{d_j - 1}$$

où C_j est une constante qui ne dépend que des formes linéaires conjuguées de L_j.

En combinant ces deux faits, nous obtenons

$$|L_j(x)| \geq {C_j}^{-1} |N_{K_j/\mathbb{Q}}(\alpha_j)|^{-d_j} \|x\|_\infty^{-(d_j-1)} \geq \|x\|_\infty^{-d_j} \text{ dès que } \|x\|_\infty \geq C_j |N_{K_j/\mathbb{Q}}(\alpha_j)| .$$

Ainsi pour $\|x\|_\infty \geq C \stackrel{def}{=} \max_{1 \leq j \leq n} C_j |N_{K_j/\mathbb{Q}}(\alpha_j)|$ et $d = \min\{d_j \mid d_j > 1\}$, nous aurons

$$|L_j(x)| \geq \|x\|_\infty^{-d} \text{ pour } j = 1, \ldots, n .$$

Cela prouve le point 3 en posant $A = d$.

4. L'ensemble $[-A, 2]$ est un compact de $\mathbb{R}^n$. Il peut être recouvert par un nombre fini d'intervalles de la forme $]c', c''[$ où $0 < c'' - c' < \delta/(2n)$. Nous avons donc un nombre fini de $2n$-uplets $(c'_1, \ldots, c'_n, c''_1, \ldots, c''_n)$ dépendant de x avec

$$0 < c''_i - c'_i < \frac{\delta}{2n} \text{ et } \|x\|_\infty^{c'_i} \leq |L_i(x)| \leq \|x\|_\infty^{c''_i} \text{ pour } 1 \leq i \leq n .$$

Comme $|L_1(x) \ldots L_n(x)| < \|x\|_\infty^{-\delta}$, nous avons aussi la condition $c'_1 + \cdots + c'_n < -\delta$, d'où $c''_1 + \cdots + c''_n < -\delta/2$. Posons alors

$$c_i = c''_i - \frac{1}{n} \sum_{i=1}^{n} c''_i .$$

Il vient $c_1 + \cdots + c_n = 0$, $c_i'' < c_i - \delta/(2n)$ et $|L_i(x)| \leq \|x\|_\infty^{c_i - \delta/(2n)}$ pour $i = 1, \ldots, n$. Nous avons alors prouvé le point 4 avec $\delta' = \delta/(2n)$.

5. Si le point 5 est faux, il existe une suite $(x_m)_{m\in\mathbb{N}}$ de solutions de (3.32) telle que $\|x_m\|_\infty$ tende vers $+\infty$ lorsque m tend vers $+\infty$, et que n termes quelconques de la suite soient indépendants sur $\mathbb{Q}$ (on construit cette suite par récurrence en utilisant que pour toute réunion finie de sous-espaces non triviaux de $\mathbb{Q}^n$, on peut trouver une solution qui n'est pas dans cette réunion). Nous allons extraire une partie $\mathcal{D}$ non bornée de $\mathcal{D}_0 = \{\|x_m\|_\infty,\ m \in \mathbb{N}\}$, telle que la famille de parallélépipèdes $\Pi(Q)_{Q\in\mathcal{D}}$ satisfasse les hypothèses du théorème des sous-espaces fort, ce qui permettra de trouver au moins n points dépendants dans la suite, et fournira une contradiction. Pour cela, notons d'une part que pour $Q \in \mathcal{D}_0$, il existe $m \in \mathbb{N}$ tel que $x_m \in Q^{-\delta'}\Pi(Q) \cap \mathbb{Z}^n$ non nul, donc $\lambda_1(Q) \leq Q^{-\delta'}$. Observons d'autre part que d'après le Théorème 1.1.11 nous avons

$$\lambda_n(Q) = \frac{\lambda_1(Q)\ldots\lambda_n(Q)}{\lambda_1(Q)\ldots\lambda_{n-1}(Q)} \gg Q^{\delta'(n-1)} \gg 1\,,$$

et il existe donc une partie $\mathcal{D}_1 \subset \mathcal{D}_0$ non bornée telle que

$$Q \in \mathcal{D}_1 \Longrightarrow \lambda_n(Q) > 1 \text{ et } \lambda_1(Q) \leq Q^{-\delta'}\,.$$

D'après la Proposition 1.1.6, pour $Q_m = \|x_m\|_\infty \in \mathcal{D}_1$, puisque $x_m \in \Pi(Q_m)$ et $\lambda_n(Q_m) > 1$,

$$x_m \in S_{n-1}(Q_m) = \mathbb{R}g_1(Q_m) \oplus \cdots \oplus \mathbb{R}g_{n-1}(Q_m)\,.$$

Si nous appelons k_m le plus petit entier k tel que

$$x_m \in S_k(Q_m) = \mathbb{R}g_1(Q_m) \oplus \cdots \oplus \mathbb{R}g_k(Q_m)\,,$$

nous avons $\lambda_{k_m}(Q_m) \leq (Q_m)^{-\delta'}$ (sinon d'après la proposition déjà citée ci-dessus, puisque $x_m \in {Q_m}^{-\delta'}\Pi(Q_m) \cap \mathbb{Z}^n$, nous aurions $x_m \in S_{k_m-1}(Q_m)$, contredisant la minimalité de k_m). Il existe alors un entier $d_m \leq n-1$ tel que

$$\lambda_{d_m}(Q_m) < \lambda_{d_m+1}(Q_m){Q_m}^{-\delta'/n} \text{ et } k_m \leq d_m,\ m \text{ assez grand.}$$

L'application $m \mapsto d_m$ va d'un ensemble infini dans un ensemble fini, et nous pouvons donc trouver $\phi : \mathbb{N} \to \mathbb{N}$ strictement croissante et un entier m_0 tels que

$$\forall m \geq m_0,\ \lambda_d(Q_{\phi(m)}) < \lambda_{d+1}(Q_{\phi(m)})(Q_{\phi(m)})^{-\delta'/n}\,.$$

Nous appliquons donc le théorème des sous-espaces fort avec la famille $\Pi(Q)_{Q\in\mathcal{D}}$ et $\delta = \delta'/n$ où

$$\mathcal{D} = \{Q_{\phi(m)} = \|x_{\phi(m)}\|_\infty,\ m \geq m_0\}\,.$$

La conclusion est qu'il existe $\mathcal{D}' \subset \mathcal{D}$ non borné tel que pour $Q \in \mathcal{D}'$

$$S = \mathbb{Q}g_1(Q) \oplus \cdots \oplus \mathbb{Q}g_d(Q)$$

ne dépende pas de $Q \in \mathcal{D}'$. Nous déduisons alors facilement une sous-suite de $(x_{\phi(m)})_{m\geq m_0}$ formée de points de S : contradiction ! Le théorème des sous-espaces (3.0.3) est donc complètement démontré.

Chapitre 4

Applications

Le but de ce chapitre est d'utiliser le théorème des sous-espaces pour en déduire le théorème de Roth, ainsi qu'une version de ce dernier dans les corps de nombres.

4.1 Caractérisation des systèmes de Roth

Nous commençons par donner une définition.

Définition 4.1.1 *Soient $L_1, \dots, L_u$ des formes linéaires sur $\mathbb{R}^n, n \geq u$, à coefficients dans $\overline{\mathbb{Q}} \cap \mathbb{R}$. On dit qu'elles forment un* SYSTÈME DE ROTH *sur $\mathbb{R}^n$ si pour tout $\delta > 0$, le système de u inéquations :*

$$|L_j(x)| < \|x\|_\infty^{-(n-u)/u-\delta}, \ j = 1, \dots, u \tag{4.1}$$

n'a qu'un nombre fini de solutions.

Définition 4.1.2 *Soient $L_1, \dots, L_n$ des formes linéaires sur $\mathbb{R}^n, n \geq u$, à coefficients dans $\overline{\mathbb{Q}}$, et $c_1 \leq \cdots \leq c_n$ des nombres réels tels que $c_1 + \cdots + c_n = 0$. On dit que*

$$(L_1, \dots, L_n; c_1, \dots, c_n)$$

est un SYSTÈME DE ROTH GÉNÉRALISÉ *si pour tout $\delta > 0$ il existe*

$$Q_1(\delta, L_1, \dots, L_n; c_1, \dots, c_n)$$

tel que le système d'inéquations :

$$|L_j(x)| \leq Q^{c_j - \delta}, \ j = 1, \dots, n \tag{4.2}$$

n'admet pas de solution $x \in \mathbb{Z}^n \setminus \{0\}$ pour $Q > Q_1$.

Voici comment nous allons atteindre le théorème de Roth : nous montrons qu'à un système de Roth correspond un système de Roth généralisé. Grâce au théorème des sous-espaces, nous sommes capables de caractériser très simplement les systèmes de Roth généralisés ; cela nous permet de trouver une caractérisation des systèmes de Roth, et il nous suffit alors de vérifier que si α est un nombre algébrique de degré $d \geq 2$, la forme linéaire $L(x_1, x_2) = \alpha x_1 - x_2$ définit un système de Roth sur $\mathbb{R}^2$.

Commençons par démontrer le lemme suivant.

Lemme 4.1.3 *Soient $L_1, \ldots, L_u$ des formes linéaires sur $\mathbb{R}^n$ de rang $r \leq u$. Alors le système :*

$$|L_j(x)| \ll \|x\|_\infty^{-(n-r)/r},\ 1 \leq j \leq u$$

a une infinité de solutions $x \in \mathbb{Z}^n \setminus \{0\}$.

PREUVE : Cas 1 : On suppose que $r = u$.

Posons $v = n - u$. Quitte à permuter les variables, on peut supposer que les formes linéaires $e_1^*, \ldots, e_v^*, L_1, \ldots, L_u$ sont indépendantes. Nous allons constuire une constante $C_1 > 0$ ne dépendant que des formes linéaires $L_1, \ldots, L_u$ telle que :

$$\forall Q > 0, \exists x \in \mathbb{Z}^n \setminus \{0\} \text{ tel que } |x_i| \leq C_1 Q^u, 1 \leq i \leq v, \text{ et } |L_j(x)| \leq Q^{-v}, 1 \leq j \leq u\,.$$

Pour cela, nous observons que la matrice de $e_1^*, \ldots, e_v^*, L_1, \ldots, L_u$ dans la base $(e_1^*, \ldots, e_n^*)$ est de la forme :

$$\begin{array}{c} \\ v \\ u \end{array} \begin{array}{c} \begin{array}{cc} v & u \end{array} \\ \begin{pmatrix} I_v & A \\ 0 & B \end{pmatrix} \end{array}$$

où I_v est bien sûr la matrice identité d'ordre v, et $\det B \neq 0$ car $e_1^*, \ldots, e_v^*, L_1, \ldots, L_u$ sont indépendantes. Posons maintenant :

$$\left\{ \begin{array}{rcll} L_i' & = & |\det B|^{-1/v} e_i^* & 1 \leq i \leq v\,, \\ L_i' & = & L_{i-v} & v+1 \leq i \leq n\,. \end{array} \right.$$

de sorte que la matrice des $L_1', \ldots, L_n'$ dans les $e_1^*, \ldots, e_n^*$ est de déterminant ± 1.

Soit $Q > 0$. Comme $(Q^u)^v (Q^{-v})^u = 1$, le théorème des formes linéaires de Minkowski (cf. Théorème 1.1.10) nous montre que le système :

$$\left\{ \begin{array}{rcll} L_i'(x) & \leq & Q^u & 1 \leq i \leq v\,, \\ L_j'(x) & \leq & Q^{-v} & v+1 \leq j \leq n\,, \end{array} \right.$$

a une solution $x_Q \in \mathbb{Z}^n \setminus \{0\}$. Ainsi, il suffit de prendre $C_1 = |\det B|^{1/v}$, et il nous reste à montrer que $\{x_Q, Q > 0\}$ est infini. Si c'était faux, nous pourrions poser $m = \min_{Q>0, 1 \leq j \leq u} |L_j(x_Q)| > 0$, et nous aurions alors $Q^v \leq 1/m$ pour tout $Q > 0$, ce qui est impossible.

Donc, nous pouvons trouver une constante $C_2 > 0$ telle que

$$\forall Q > 0, |L_j(x_Q)| \leq C_2 \|x_Q\|_\infty^{-v/u}\ 1 \leq j \leq u\,.$$

Ce qu'il fallait démontrer.

Cas 2 : On suppose que $r < u$.

Supposons que $L_1, \dots, L_r$ soient les r formes indépendantes. Par le cas 1, nous avons une constante $C_1 > 0$ (différente de celle du cas 1) telle que :

$$|L_j(x)| \leq C_1 \|x\|_\infty^{-(n-r)/r},\ 1 \leq j \leq r$$

possède une infinité de solutions $x \in \mathbb{Z}^n \setminus \{0\}$.

Pour $k \geq 1$, nous écrivons $L_{j+k} = \alpha_{k,1} L_1 + \cdots + \alpha_{k,r} L_r$, et nous posons

$$A = \max_{1 \leq i \leq r, 1 \leq k \leq u-r} |\alpha_{k,i}|,\ \text{puis } C_2 = \max\{C_1, C_1 A r\},$$

de sorte que pour toute solution du système précedent, nous avons :

$$|L_j(x)| \leq C_2 \|x\|_\infty^{-(n-r)/r},\ 1 \leq j \leq u\,.$$

Ainsi le lemme est-il prouvé. ■

Nous introduisons maintenant une quantité importante qui va nous permettre de caractériser les systèmes de Roth généralisés.

Définition 4.1.4 *Soient $L_1, \dots, L_n$ des formes linéaires sur $\mathbb{R}^n$, et $c_1, \dots, c_n$ des nombres réels satisfaisant*

$$\begin{cases} c_1 \leq \cdots \leq c_n\,, \\ c_1 + \cdots + c_n = 0\,. \end{cases}$$

et S un sous-espace de $\mathbb{R}^n$ dimension d. Soit r le rang sur $\mathbb{Q}$ des restrictions $L_{1|S}, \dots, L_{n|S}$. On pose

$$c(S) = \begin{cases} +\infty & \text{si } r < d\,, \\ c_{t_1} + \cdots + c_{t_d} & \text{si } r = d\,. \end{cases}$$

où la suite $t_1, \dots, t_d$ est définie de la façon suivante :

$$\begin{cases} t_1 = \min\{1 \leq i \leq n \mid \operatorname{rang}(L_{i|S}) = 1\}\,, \\ t_i = \min\{i - 1 < j \leq n \mid \operatorname{rang}(L_{t_1|S}, \dots, L_{t_{i-1}|S}, L_{j|S}) = i\}, \quad i = 2, \dots, d\,. \end{cases}$$

Nous pouvons maintenant énoncer le théorème.

Théorème 4.1.5 *Soient $L_1, \dots, L_n$ des formes linéaires sur $\mathbb{R}^n$, à coefficients dans $\overline{\mathbb{Q}} \cap \mathbb{R}$ et $c_1, \dots, c_n$ des nombres réels satisfaisant*

$$\begin{cases} c_1 \leq \cdots \leq c_n\,, \\ c_1 + \cdots + c_n = 0\,. \end{cases}$$

Alors $(L_1, \dots, L_n; c_1, \dots, c_n)$ est un système de Roth généralisé, si et seulement si pour tout sous-espace S de dimension $d \geq 1$ de $\mathbb{Q}^n$, nous avons $c(S) \leq 0$.

PREUVE : a) Supposons que $(L_1, \dots, L_n; c_1, \dots, c_n)$ soit un système de Roth généralisé. Si $c(S) = +\infty$ pour un certain sous-espace vectoriel S de $\mathbb{Q}^n$ de dimension $d \geq 1$, alors $r \stackrel{def}{=} \text{rang}\,(L_{1|S}, \dots, L_{n|S}) < d$ et nous allons montrer dans ce cas que :

$$\forall \epsilon > 0, \exists x_\epsilon \in S \cap (\mathbb{Z}^n \setminus \{0\}) \text{ tel que } |L_j(x_\epsilon)| < \epsilon, 1 \leq j \leq n\,.$$

Soit $(a_1, \dots, a_d)$ une $\mathbb{Q}$-base de S, où $a_1, \dots, a_d$ ont des coordonnées entières premières entre elles. Pour $1 \leq j \leq n$, on considère la forme linéaire :

$$\begin{array}{rccc} L'_j : & \mathbb{Q}^d & \longrightarrow & \mathbb{R} \\ & (x_1, \dots, x_d) & \longmapsto & L_{j|S}\left(\sum_{i=1}^d a_i x_i\right)\,. \end{array}$$

Alors $\text{rang}\,(L'_1, \dots, L'_n) = \text{rang}\,(L_{1|S}, \dots, L_{n|S})$. Il existe une constante $C > 0$ telle que le système

$$\forall j = 1, \dots, n,\ |L'_j(x)| \leq C\|x\|_\infty^{-(d-r)/r}$$

a une infinité de solutions $x \in \mathbb{Z}^d \setminus \{0\}$. Lorsque x parcourt l'ensemble de ces solutions, $\|x\|_\infty$ ne peut être borné. Or puisque $d > r$, $\lim_{t\to+\infty} Ct^{-(d-r)/r} = 0$. Il y a donc une solution $x \in \mathbb{Z}^d \setminus \{0\}$ telle que $C\|x\|_\infty^{-(d-r)/r} < \epsilon$. Donc $x_\epsilon \stackrel{def}{=} \sum_{i=1}^d a_i x_i$ répond bien à nos exigences.

Si $Q > 0$ et $\delta > 0$ sont donnés, en prenant $\epsilon < \min\{Q^{c_j-\delta}, 1 \leq j \leq n\}$, on obtient d'après ce qui précède, une solution $x_\epsilon \in S \cap (\mathbb{Z}^n \setminus \{0\})$ qui satisfait :

$$\forall j = 1, \dots, n,\ |L_j(x_\epsilon)| < Q^{c_j-\delta}\,,$$

ce qui contredit le fait que $(L_1, \dots, L_n; c_1, \dots, c_n)$ est un système de Roth généralisé.

Si maintenant $0 < c(S) < +\infty$, on a $\text{rang}\,(L_{1|S}, \dots, L_{n|S}) = d$. Posons $\delta = c(S)/(2d)$, de sorte que nous avons $\prod_{i=1}^d Q^{c_{t_i}-2\delta} = 1$, où $t_1, \dots, t_d$ sont choisis comme indiqué dans la Définition 4.1.4. Comme $L_{t_1|S}, \dots, L_{t_d|S}$ sont indépendantes, le théorème des formes linéaires de Minkowski montre que le système :

$$|L_{t_i}(x)| \leq DQ^{c_{t_i}-2\delta},\ i = 1, \dots, d$$

a une solution $x \in S \cap (\mathbb{Z}^d \setminus \{0\})$ pour tout $Q > 0$ où D est bien sûr la valeur absolue du déterminant de $L_{t_1|S}, \dots, L_{t_d|S}$. On en déduit que pour cette solution, on a :

$$|L_j(x)| \leq D_1 Q^{c_j-2\delta},\ j = 1, \dots, n\,.$$

En effet, $x \in S \cap (\mathbb{Z}^d \setminus \{0\})$ donc si j est l'un des $t_1, \dots, t_d$, il suffit de choisir $D_1 \geq D$ pour que le résultat soit vrai. Si $j < t_1$, L_j est nulle sur S, donc le résultat est valable pour $D_1 > 0$. Sinon, avec la convention $t_{d+1} = \infty$, il existe un $i \in \{1, \dots, d\}$ avec $t_i < j < t_{i+1}$, et nous pouvons écrire $L_{j|S}$ comme combinaison linéaire de $L_{t_1|S}, \dots, L_{t_i|S}$. Si nous désignons par K le maximum des valeurs absolues des coefficients intervenant dans toutes ces combinaisons linéaires lorsque $j \in \cup_{1\leq i\leq d}]t_i, t_{i+1}[$, il est facile de constater que :

$$|L_{j|S}(x)| \leq KdQ^{c_{t_i}-2\delta} \leq D_1 Q^{c_j-2\delta}$$

dès que $D_1 \geq DdK$. Il convient d'observer que nous avons utilisé de façon décisive le fait que la suite $(c_1, \ldots, c_n)$ est croissante!

En prenant donc $D_1 \geq \max\{D, dDK\}$, nous avons bien le résultat annoncé. Mais alors, pour $Q > {D_1}^{-\delta}$, le système :

$$|L_j(x)| < Q^{c_j - \delta},\ j = 1, \ldots, n$$

a une solution $x \in \mathbb{Z}^n \setminus \{0\}$, ce qui contredit une fois de plus que $(L_1, \ldots, L_n; c_1, \ldots, c_n)$ est un système de Roth généralisé. Ainsi pour tout sous-espace S de $\mathbb{Q}^n$ de dimension $d \geq 1$, on a bien $c(S) \leq 0$.

b) Supposons maintenant que pour tout sous-espace S de $\mathbb{Q}^n$ de dimension $d \geq 1$, nous avons $c(S) \leq 0$, et montrons que $(L_1, \ldots, L_n; c_1, \ldots, c_n)$ est forcément un système de Roth généralisé. Si c'était faux, il existerait $\delta > 0$ tel que le système (4.2) ait une solution $x \in \mathbb{Z}^n \setminus \{0\}$ pour Q arbitrairement grand. Il existe alors — à cause de la décroissance des dimensions — un sous-espace de $\mathbb{Q}^n$ de solutions, qui est de plus minimal, c'est-à-dire qu'on a les propriétés suivantes :

1. le système (4.2) a des solutions $x \in S \cap (\mathbb{Z}^n \setminus \{0\})$ pour Q arbitrairement grand ;
2. si $S' \subset S$ est un sous-espace de $\mathbb{Q}^n$ avec $S' \neq S$, alors il est $Q_0(S')$ tel que pour $Q > Q_0(S')$, (4.2) n'a pas de solutions $x \in S' \cap (\mathbb{Z}^n \setminus \{0\})$.

Posons alors $d = \dim S$. Comme $c(S) \leq 0$, la Définition 4.1.4 montre que

$$\operatorname{rang}(L_{1|S}, \ldots, L_{n|S}) = d\,.$$

Soient $t_1, \ldots, t_d$ comme dans cette même définition ; nous affirmons qu'il existe $Q_1 > 0$ et $\rho > 0$ tels que pour $Q > Q_1$, on ait $\|x\|_\infty < Q^\rho$ pour toute solution $x \in S \cap (\mathbb{Z}^n \setminus \{0\})$ de (4.2). Il suffit en effet de choisir $\alpha > 0$ tel que $\rho \overset{def}{=} \alpha + c_n - \delta > 0$. Posons, pour $i = 1, \ldots, d$, $\phi_i = L_{t_i|S}$, et soit $(a_1, \ldots, a_d)$ une $\mathbb{Q}$-base de S où a_i est à composantes entières premières entre elles ; on a alors un isomorphisme naturel :

$$\begin{array}{rccl} T: & S_{\mathbb{R}} & \longrightarrow & \mathbb{R}^d \\ & x & \longmapsto & (\phi_1(x), \ldots, \phi_d(x))\,, \end{array}$$

où $S_{\mathbb{R}} = \mathbb{R}a_1 \oplus \cdots \oplus \mathbb{R}a_d$, sur lequel on dispose de la norme $N_1\left(\sum_{i=1}^d \lambda_i a_i\right) = \max_{1 \leq i \leq d} |\lambda_i|$. Ces préparatifs étant faits, soit $y = T(x)$, où $x \in S \cap (\mathbb{Z}^n \setminus \{0\})$ satisfait (4.2). Comme $x = T^{-1}(y)$, on en déduit les inégalités suivantes :

$$N_1(x) \leq \|T^{-1}\| \|y\|_\infty \leq Q^{c_n - \delta} \|T^{-1}\|\,.$$

Par équivalence des normes sur $S_{\mathbb{R}}$, il existe une constante $C(S,d) > 0$ telle que $\forall x \in S_{\mathbb{R}}$, $\|x\|_\infty \leq C(S,d) N_1(x)$. Par conséquent, si nous posons $Q_1 = \left(C(S,d)\|T^{-1}\|\right)^{1/\alpha}$, pour $Q > Q_1$, nous aurons bien $\|x\|_\infty < Q^\rho$.

Il suit que pour $Q > Q_1$ et $x \in S \cap (\mathbb{Z}^n \setminus \{0\})$ une solution de (4.2) :

$$|L_{t1}(x) \dots L_{td}(x)| \leq Q^{c(S)-d\delta} \leq Q^{-\delta} \leq \|x\|_\infty^{-\delta/\rho}, \tag{4.3}$$

et, d'autre part pour $\|x\|_\infty \geq \|T\|$:

$$\|y\|_\infty \leq \|T\|\|x\|_\infty \leq \|x\|_\infty^2. \tag{4.4}$$

Nous appliquons alors le théorème des sous-espaces aux d formes linéaires indépendantes sur $\mathbb{R}^d$ que sont :

$$\tilde{L_i}(y) = L_i(T^{-1}(y)),\ i = 1, \dots, d,$$

sachant que (4.3) et (4.4) montrent que lorsque $x \in S \cap (\mathbb{Z}^n \setminus \{0\})$ satisfait (4.2) avec Q et $\|x\|_\infty$ assez grands, on a :

$$|\tilde{L}_1(y) \dots \tilde{L}_d(y)| < \|y\|_\infty^{-\delta/2\rho}.$$

Nous en concluons que les solutions $x \in \mathbb{Z}^d \setminus \{0\}$ de cette dernière équation sont contenues dans un nombre fini de sous-espaces non triviaux de $\mathbb{Q}^d$, disons $V_1, \dots, V_t$. L'un des sous-espaces $T^{-1}(V_1), \dots, T^{-1}(V_t)$ contient donc des solutions $x \in \mathbb{Z}^n \setminus \{0\}$ de (4.2) pour Q arbitrairement grand, et c'est une contradiction avec la minimalité de S. Il faut donc conclure que $(L_1, \dots, L_n; c_1, \dots, c_n)$ est bien un système de Roth généralisé. ■

Voici un petit lemme qui montre le lien entre systèmes de Roth et systèmes de Roth généralisés.

Lemme 4.1.6 *Soient $L_1, \dots, L_u$ des formes linéaires sur $\mathbb{R}^n$ à coefficients dans $\overline{\mathbb{Q}} \cap \mathbb{R}$ et $v = n - u$. On suppose que* $\operatorname{rang}(L_1, \dots, L_u, e_1^*, \dots, e_v^*) = n$, *et que pour tout $\delta > 0$ il existe $Q_2(\delta, L_1, \dots, L_u)$ tel que pour $Q > Q_2$ le système :*

$$\begin{cases} |L_j(x)| \leq Q^{-v-\delta} & (1 \leq j \leq u) \\ |x_i| \leq Q^{u-\delta} & (1 \leq i \leq v) \end{cases} \tag{4.5}$$

n'a aucune solution $x \in \mathbb{Z}^n \setminus \{0\}$.
Alors $L_1, \dots, L_u$ est un système de Roth.

Preuve : Nous raisonnons par l'absurde ; supposons qu'il existe $\delta > 0$ tel que (4.1) possède une infinité de solutions $x \in \mathbb{Z}^n \setminus \{0\}$. Il est clair que nous pouvons supposer que $u - \delta > 0$. Nous choisissons alors un réel ρ satisfaisant

$$0 < \rho < u - \delta \text{ et } \rho < \frac{v + \delta u}{u(v + \delta)}.$$

Pour toute solution x de (4.1), posons $Q_x = \|x\|_\infty^{1/\rho}$. Il n'est alors pas difficile de constater que le choix de ρ fait que x est une solution de (4.5) lorsque Q_x remplace Q. Cela fournit une contradiction avec l'hypothèse du lemme car Q_x est arbitrairement grand. ■

Nous sommes alors capables de caractériser les systèmes de Roth comme annoncé au début de ce chapitre.

Théorème 4.1.7 *Soient $L_1, \dots, L_u$ des formes linéaires sur $\mathbb{R}^n$ à coefficients dans $\overline{\mathbb{Q}} \cap \mathbb{R}$ et $v = n - u$. Alors $(L_1, \dots, L_u)$ est un système de Roth si et seulement si pour tout sous-espace S de $\mathbb{Q}^n$ de dimension $d \geq 1$, on a*

$$\text{rang}\,(L_{1|S}, \dots, L_{u|S}) \geq du/n\,. \tag{4.6}$$

PREUVE : a) Supposons que $L_1, \dots, L_u$ soit un système de Roth et soit S un sous-espace de $\mathbb{Q}^n$ de dimension $d \geq 1$. Posons $r = \text{rang}\,(L_{1|S}, \dots, L_{u|S})$; il s'agit de voir que $r \geq du/n$. Choisissons une fois de plus une $\mathbb{Q}$-base de S $(a_1, \dots, a_d)$, où les a_i sont primitifs. Pour $1 \leq i \leq u$, définissons une forme linéaire ϕ_i par $\phi_i(x_1, \dots, x_d) = x_1 L_1(a_1) + \cdots + x_d L_d(a_d)$.

Par le Lemme 4.1.3, le système :

$$|\phi_j(x)| \ll \|x\|_\infty^{-(d-r)/r},\ 1 \leq j \leq u \tag{4.7}$$

a une infinité de solutions $x \in \mathbb{Z}^d \setminus \{0\}$. Appelons donc C la constante induite par (4.7), et considérons l'application :

$$\begin{array}{rccc} \psi : & \mathbb{Z}^d & \longrightarrow & S \cap \mathbb{Z}^n \\ & x = (x_1, \dots, x_d) & \longmapsto & a_1 x_1 + \cdots + a_d x_d\,. \end{array}$$

Comme $a_1, \dots, a_d$ sont indépendants dans $\mathbb{Q}^n$, ψ est injective. Nous allons donc montrer que si

$$|\phi_j(x)| \leq C\|x\|_\infty^{-(d-r)/r},\ 1 \leq j \leq u \text{ et } r < du/n, \tag{4.8}$$

alors

$$|\phi_j(\psi(x))| \leq \|\psi(x)\|_\infty^{-(n-u)/u-\delta},\ 1 \leq j \leq u, \tag{4.9}$$

pour un δ que nous déterminerons, ce qui fournira une contradiction avec l'hypothèse de départ et imposera $r \geq du/n$.

Si $C' \overset{def}{=} \|a_1\|_\infty + \cdots + \|a_d\|_\infty$, on a $\|\psi(x)\| \leq C'\|x\|_\infty$.
On a l'équivalence :

$$C\|x\|_\infty^{-(d-r)/r} < \|\psi(x)\|_\infty^{-(n-u)/u-\delta} \Longleftrightarrow \|\psi(x)\|_\infty^{(n-u)/u+\delta} < C^{-1}\|x\|_\infty^{(d-r)/r}\,.$$

Puisque $\|\psi(x)\|_\infty^{(n-u)/u+\delta} \leq C'^{(n-u)/u+\delta}\|x\|_\infty^{(n-u)/u+\delta}$, il suffit de faire en sorte que

$$C'^{(n-u)/u+\delta}\|x\|_\infty^{(n-u)/u+\delta} < C^{-1}\|x\|_\infty^{(d-r)/r}\,,$$

soit encore

$$\|x\|_\infty^{(d-r)/r-(n-u)/u-\delta} > C'^{(n-u)/u+\delta}C\,.$$

Or $(d-r)/r - (n-u)/u - \delta = d/r - n/u - \delta$, et on a $d/r > n/u$ sous l'hypothèse $r < du/n$. D'après tout ce qui précède, il suffit de poser

$$\delta = \frac{1}{2}\left(\frac{d}{r} - \frac{n}{u}\right) \text{ et } C'' = C'^{(n-u)/u+\delta}C$$

pour obtenir que si $x \in \mathbb{Z}^d \setminus \{0\}$ est une solution de (4.8), telle que $\|x\|_\infty > C''^{1/\delta}$ (il y a une infinité de telles solutions) alors $\psi(x) \in S \cap (\mathbb{Z}^n \setminus \{0\})$ est une solution de (4.9).

b) Supposons la propriété (4.6) vraie pour tout sous-espace S de dimension $d \geq 1$. En particulier, $L_1, \ldots, L_u$ sont donc indépendantes (faire $d = n!$), et quitte à renommer les variables, on peut supposer que $e_1^*, \ldots, e_v^*, L_1, \ldots, L_u$ sont indépendantes. Nous allons montrer que $(L_1, \ldots, L_u; c_1 = -v, \ldots, c_u = -v, c_{u+1} = u, \ldots, c_n = u)$ est un système de Roth généralisé, ce qui suffira pour montrer que $(L_1, \ldots, L_u)$ est un système de Roth, d'après le Lemme 4.1.6.

Comme $\operatorname{rang}(L_1, \ldots, L_u, e_1^*, \ldots, e_v^*) = n$, si S est un sous-espace de $\mathbb{Q}^n$ de dimension $d \geq 1$, on a $\operatorname{rang}(L_{1|S}, \ldots, L_{u|S}, e_{1|S}^*, \ldots, e_{v|S}^*) = d$.

Soit $r = \operatorname{rang}(L_{1|S}, \ldots, L_{u|S})$, et $t_1, \ldots, t_d$ les entiers de la Définition 4.1.4. Alors $t_r \leq u < t_{r+1}$, et il suit que :

$$\begin{aligned} c(S) &= c_{t_1} + \cdots + c_{t_r} + c_{t_{r+1}} + \cdots + c_{t_n} \\ &= r(-v) + (d-r)u \text{ (noter à nouveau la croissance des } c_i) \\ &= ud - nr \\ &\leq 0 \text{ d'après la propriété (4.6).} \end{aligned}$$

Par le Théorème 4.1.5, nous avons bien un système de Roth généralisé, donc la preuve est achevée. ■

Corollaire 4.1.8 (Théorème de Roth) *Soit α un nombre algébrique de degré $d \geq 2$. Alors pour tout $\epsilon > 0$, l'inéquation :*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}} \tag{4.10}$$

n'a qu'un nombre fini de solutions $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$.

Preuve : La forme linéaire $L(x_1, x_2) = s\alpha x_1 - s x_2$ est un système de Roth sur $\mathbb{R}^2$ quel que soit le rationnel non nul s. En effet soit S un sous-espace de $\mathbb{Q}^2$ de dimension $d \geq 1$, et $(x_1, x_2) \in S \setminus \{0\}$. Alors $L(x_1, x_2) \neq 0$ car $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 2$. Il suit que $r = \operatorname{rang} L_{|S} \geq 1$. Mais ici $u = 1$ et $n = 2$ assurent que du/n vaut 1 ou $1/2$ donc $r \geq du/n$. Le Théorème 4.1.7 montre donc que L constitue un système de Roth sur $\mathbb{R}^2$. Un choix convenable du rationnel s nous permet d'aboutir au résultat souhaité ; explicitement, posons $C = 1 + |\alpha|$ et choisissons s tel que $0 < s < C^{-(\delta+1)}$. Si (p, q) est solution de (4.10), nous avons $\|(q, p)\|_\infty \leq C|q|$. Ainsi : $|r\alpha q - pr| < (Cq)^{-(\delta+1)} < \|(q, p)\|_\infty^{-(\delta+1)}$. Or cette dernière inéquation n'a qu'un nombre fini de solutions. ■

4.2 Le théorème de Roth dans les corps de nombres

On entend ici utiliser le théorème des sous-espaces pour démontrer un résultat d'approximation d'un nombre algébrique donné par d'autres nombres algébriques de degré borné.

Nous commençons par donner une définition.

Définition 4.2.1 *Soit α un nombre algébrique de degré $d \geq 1$. On pose :*

$$H(\alpha) = \max_{0 \leq i \leq d} |a_i| \,,$$

où $P(X) = \sum_{i=0}^{d} a_i x^i$ est un polynôme de $\mathbb{Z}[X]$ de degré d à coefficients premiers entre eux, tel que $P(X)$ est irréductible sur $\mathbb{Q}[X]$ et $Q(\alpha) = 0$.

Remarque 4.2.2 *Un tel polynôme étant unique à multiplication près par ± 1, la définition ci-dessus a un sens ; on notera désormais $\pi_\alpha(X)$ un tel polynôme.*

Nous énonçons maintenant le principal résultat de ce chapitre.

Théorème 4.2.3 *Soit α un nombre algébrique réel, $k \geq 1$ et $\delta > 0$. Il existe alors un nombre fini de nombres algébriques β, de degré inférieur ou égal à k avec :*

$$|\alpha - \beta| < H(\beta)^{-k-1-\delta} \,.$$

Nous avons besoin de quelques résultats intermédiaires pour démontrer ce théorème.

Théorème 4.2.4 *Soient $1, \alpha_1, \ldots, \alpha_v$ des nombres algébriques réels linéairement indépendants sur $\mathbb{Q}$, et $\delta > 0$. Alors l'inéquation :*

$$|q_1 \ldots q_v|^{1+\delta} \|\alpha_1 q_1 + \cdots + \alpha_v q_v\| < 1 \tag{4.11}$$

n'a qu'un nombre fini de solutions $(q_1, \ldots, q_v) \in (\mathbb{Z} \setminus \{0\})^v$.

Preuve : Nous allons utiliser le théorème des sous-espaces pour raisonner par récurrence sur v, à partir du cas $v = 1$. Considérons alors :

$$|q_1|^{1+\delta} \|\alpha_1 q_1\| < 1, q_1 \in \mathbb{Z} \setminus \{0\} \,. \tag{4.12}$$

Choisissons p tel que $\|\alpha_1 q_1\| = |\alpha_1 q_1 - p|$; on a alors $|q_1(\alpha_1 q_1 - p)| < |q_1|^{-\delta}$, et on remarque aussi que $|p| \leq 1 + |\alpha_1||q_1| \leq (1 + |\alpha_1|)|q_1|$, donc $\|(q_1, p)\|_\infty \leq (1 + |\alpha_1|)|q_1|$. Si r est un rationnel tel que $0 < r < (1 + |\alpha_1|)^{-\delta}$, on a donc :

$$|L_1(q_1, p) L_2(q_1, p)| < \|(q_1, p)\|_\infty{}^{-\delta} \,, \tag{4.13}$$

où :

$$\begin{aligned} L_1(q_1, p) &= r q_1 \,, \\ L_2(q_1, p) &= \alpha_1 q_1 - p \,. \end{aligned}$$

D'après le théorème des sous-espaces, les solutions de (4.13) se trouvent dans un nombre fini de sous-espaces de $\mathbb{Q}^2$ de dimension 1, de la forme $\mathbb{Q}(r_i, s_i)$, où r_i et s_i sont premiers entre eux. Donc, pour une solution (q_1, p) de (4.12), il existe i tel que $(q_1, p) = \lambda(r_i, s_i)$, λ ne pouvant prendre qu'un nombre fini de valeurs. Cela montre le Théorème 4.2.4 dans le cas $v = 1$.

Supposons maintenant le résultat vrai jusqu'au rang $v-1$ et montrons-le au rang v. Définissons $C = 1 + \sum_{i=1}^{v} |\alpha_i|$, et choisissons un rationnel r avec $0 < r < C^{-\delta}$, puis en vue d'appliquer le théorème des sous-espaces, posons :

$$\begin{aligned} L_1(x_1, \ldots, x_{v+1}) &= rx_1\,, \\ L_i(x_1, \ldots, x_{v+1}) &= x_i, \text{ pour } 1 < i < v+1\,, \\ L_{v+1}(x_1, \ldots, x_{v+1}) &= \textstyle\sum_{i=1}^{v} \alpha_i q_i - x_{v+1}\,. \end{aligned}$$

Soient $q_1, \ldots, q_v$ des entiers non nuls tels que (4.11) soit vraie. On choisit p tel que $\|\alpha_1 q_1 + \cdots + \alpha_v q_v\| = |\alpha_1 q_1 + \cdots + \alpha_v q_v - p|$. Nous constatons que si $x = (q_1, \ldots, q_v, p)$, la propriété (4.11) implique :

$$|L_1(x) \ldots L_{v+1}(x)| < \|x\|_\infty^{-\delta}\,. \tag{4.14}$$

En effet, par choix de C nous avons

$$|p| \leq \left|\sum_{i=1}^{v} \alpha_i q_i - p\right| + \left|\sum_{i=1}^{v} \alpha_i q_i\right| \leq C|q_1 \ldots q_v|\,,$$

donc $\|x\|_\infty \leq C|q_1 \ldots q_v|$ et par conséquent, par choix de r :

$$\begin{aligned} |L_1(x) \ldots L_{v+1}(x)| &= r|q_1 \ldots q_v|\,|\textstyle\sum_{i=1}^{v} \alpha_i q_i - p| \\ &\leq C^{-\delta}|q_1 \ldots q_v|\,|\textstyle\sum_{i=1}^{v} \alpha_i q_i - p| \\ &< C^{-\delta}|q_1 \ldots q_v|^{-\delta} \\ &\leq \|x\|_\infty^{-\delta}\,. \end{aligned}$$

Convenons d'écrire $q = (q_1, \ldots, q_v)$. Il nous suffit maintenant de prouver que (4.14) a un nombre fini de solutions pour $\|q\|_\infty \geq C_0$, où C_0 est une constante arbitraire. Or :

$$\begin{aligned} |L_1(x) \ldots L_{v+1}(x)| &= r|q_1 \ldots q_v|\,|\textstyle\sum_{i=1}^{v} \alpha_i q_i - p| \\ &\leq C^{-\delta}|q_1 \ldots q_v|\,|\textstyle\sum_{i=1}^{v} \alpha_i q_i - p| \\ &< C^{-\delta}|q_1 \ldots q_v|^{-\delta} \\ &\leq \|x\|_\infty^{-\delta}\,. \end{aligned}$$

Par le théorème des sous-espaces, il existe un nombre fini de sous-espaces de $\mathbb{Q}^{v+1}$, $T_1, \ldots, T_k$ tels que $x \in T_1 \cup \cdots \cup T_k$. Soit T l'un de ces sous-espaces. Comme $1 \leq \dim T \leq v$, il existe des entiers $c_1, \ldots, c_{v+1}$ non tous nuls, tels que $x \in T \Rightarrow c_1 q_1 + \cdots c_v q_v + c_{v+1} p = 0$. Nous allons nous servir de cette propriété pour supprimer une variable ; il y a deux cas à considérer.

Cas 1 : $c_{v+1} \neq 0$ et $\forall i \in \{1, \ldots, v\}, c_i = 0$.

On a alors $c_{v+1} p = 0$ donc $p = 0$ et si l'on pose $\alpha'_i = \alpha_i/\alpha_v$, on a :

$$\|\alpha_1 q_1 + \cdots + \alpha_v q_v\| = \left|\sum_{i=1}^{v} \alpha_i q_i\right| = |\alpha_v|\|\alpha'_1 q_1 + \cdots + \alpha'_{v-1} q_{v-1}\|\,.$$

On montre alors qu'il existe une constante $C_1 > 0$ telle que

$$\|q\|_\infty \geq C_1 \Rightarrow |q_1 \dots q_{v-1}|^{1+\delta/2} \|\alpha'_1 q_1 + \cdots + \alpha'_{v-1} q_{v-1}\| < 1\,.$$

Pour cela il suffit d'observer qu'on a la succession d'inégalités :

$$\begin{aligned}
|q_1 \dots q_v|^{1+\delta} \|\alpha'_1 q_1 + \cdots + \alpha'_{v-1} q_{v-1}\| &< \frac{1}{|\alpha_v|} \\
|q_1 \dots q_{v-1}|^{1+\delta} \|\alpha'_1 q_1 + \cdots + \alpha'_{v-1} q_{v-1}\| &< \frac{1}{|\alpha_v| |q_v|^{1+\delta}} \\
|q_1 \dots q_{v-1}|^{1+\delta/2} \|\alpha'_1 q_1 + \cdots + \alpha'_{v-1} q_{v-1}\| &< \frac{1}{|\alpha_v| |q_1 \dots q_v|^{\delta/2}} \\
&\leq \frac{1}{|\alpha_v| \|q\|_\infty^{\delta/2}} \quad < \quad 1
\end{aligned}$$

dès que $\|q\|_\infty > |\alpha_v|^{-2/\delta}$. On prend donc $C_1 > |\alpha_v|^{-2/\delta}$.

Cas 2 : $\exists j \in \{1, \dots, v\}$ tel que $c_j \neq 0$.

Quitte à renommer les variables, on peut supposer que $j = v$ et $c_v > 0$. On pose cette fois :

$$\alpha'_i = \frac{c_v \alpha_i - c_i \alpha_v}{c_v + c_{v+1} \alpha_v}, \text{ pour } i = 1, \dots, v-1\,.$$

On a :

$$c_v \|\alpha_1 q_1 + \cdots + \alpha_v q_v\| = |c_v + c_{v+1} \alpha_v| |\alpha'_1 q_1 + \cdots + \alpha'_{v-1} q_{v-1} - p|\,. \tag{4.15}$$

Pour raisonner par récurrence, on exhibe une constante $C_2 > 0$ telle que l'on ait $\|q\|_\infty \geq C_2 \Rightarrow |q_1 \dots q_{v-1}|^{1+\delta/2} \|\alpha'_1 q_1 + \cdots + \alpha'_{v-1} q_{v-1}\| < 1$. L'égalité (4.15) montre que $\|\alpha'_1 q_1 + \cdots + \alpha'_{v-1} q_{v-1}\| \leq K \|\alpha_1 q_1 + \cdots + \alpha_v q_v\|$, où on pose $K = |c_v + c_{v+1} \alpha_v| / c_v$. On en déduit les inégalités successives :

$$\begin{aligned}
|q_1 \dots q_{v-1}|^{1+\delta/2} \|\alpha'_1 q_1 + \cdots + \alpha'_{v-1} q_{v-1}\| &\leq \frac{K}{|q_1 \dots q_{v-1}|^{\delta/2} |q_v|^{1+\delta}} \\
&\leq \frac{K}{|q_1 \dots q_v|^{\delta/2}} \quad \leq \quad \frac{K}{\|q\|_\infty^{\delta/2}}\,.
\end{aligned}$$

Il suffit ainsi de prendre $C_2 > K^{2/\delta}$.

L'hypothèse de récurrence dit alors qu'il existe un nombre fini de solutions à l'inéquation

$$|q_1 \dots q_{v-1}|^{1+\delta/2} \|\alpha'_1 q_1 + \cdots + \alpha'_{v-1} q_{v-1}\| < 1\,,$$

car $1, \alpha'_1, \dots, \alpha'_{v-1}$ sont linéairement indépendants sur $\mathbb{Q}$. Mais alors le nombre de valeurs de q_v telles que $(q_1, \dots, q_v)$ satisfasse (4.11) est fini. Le Théorème 4.2.4 est donc prouvé. ■

Corollaire 4.2.5 *Soient $1, \alpha_1, \dots, \alpha_v$ des nombres algébriques réels linéairement indépendants sur $\mathbb{Q}$, et $\delta > 0$. Alors l'ensemble*

$$\mathcal{E} = \{(q_1, \dots, q_v, p) \in \mathbb{Z}^{v+1} \mid \|q\|_\infty > 0 \text{ et } |\alpha_1 q_1 + \cdots + \alpha_v q_v - p| < \|q\|_\infty^{-v-\delta}\}$$

est fini.

PREUVE : Pour $\emptyset \neq J \subset \{1, \dots, v\}$, définissons :

$$S_J = \{(q_1, \dots, q_v, p) \in \mathbb{Z}^{v+1} \mid (q_i \neq 0 \Leftrightarrow i \in J) \text{ et } |\alpha_1 q_1 + \cdots + \alpha_v q_v - p| < \|q\|_\infty^{-v-\delta}\}.$$

Par le Théorème 4.2.4, S_J est fini pour tout $\emptyset \neq J \subset \{1, \dots, v\}$ car on a :

$$|q_1 \dots q_v|^{1+\delta/2} \|\alpha_1 q_1 + \cdots + \alpha_v q_v\| \leq \|q\|_\infty^{v(1+\delta/v)} |\alpha_1 q_1 + \cdots + \alpha_v q_v - p|$$

pour $(q_1, \dots, q_v, p) \in S_J$. Pour conclure, on note que $\mathcal{E} = \cup_{\emptyset \neq J \subset \{1,\dots,v\}} S_J$, réunion d'au plus 2^v ensembles finis. ■

Nous donnons maintenant le Corollaire 4.2.5 sous une forme plus proche de nos préoccupations de cette section.

Corollaire 4.2.6 *Soit α un nombre réel qui n'est pas algébrique de degré inférieur ou égal à k. Alors pour tout $\delta > 0$,*

$$\{P \in \mathbb{Z}[X] \mid \deg P \leq k \text{ et } 0 < |P(\alpha)| < H(P)^{-k-\delta}\}$$

est fini.

PREUVE : En effet recherchons P sous la forme $P(X) = \sum_{i=0}^{k} a_i X^i$. On applique le Corollaire 4.2.5 à $\alpha_i := \alpha^i, i = 0, \dots, k$ qui sont linéairement indépendants sur $\mathbb{Q}$ par hypothèse, et $k = v$. ■

Nous rappelons deux définitions dues à Mahler et Koksma respectivement.

Définition 4.2.7 *Soit $\alpha \in \mathbb{R}, \omega \in \mathbb{R}$ et $k \geq 1$. On pose :*

$$\mathcal{A}_k(\alpha, \omega) = \{P \in \mathbb{Z}[X] \mid \deg P \leq k \text{ et } 0 < |P(\alpha)| < H(P)^{-\omega}\}, \text{ et}$$

$$\omega_k(\alpha) = \sup\{\omega \in \mathbb{R} \mid \mathcal{A}_k(\alpha, \omega) \text{ est infini.}\}.$$

Définition 4.2.8 *Soit $\alpha \in \mathbb{R}, \omega \in \mathbb{R}$ et $k \geq 1$. On pose :*

$$\mathcal{A}_k^*(\alpha, \omega^*) = \{\beta \in \overline{\mathbb{Q}} \cap \mathbb{R} \mid \deg \beta \leq k \text{ et } |\alpha - \beta| < H(\beta)^{-\omega^*-1}\}, \text{ et}$$

$$\omega_k^*(\alpha) = \sup\{\omega^* \in \mathbb{R} \mid \mathcal{A}_k^*(\alpha, \omega^*) \text{ est infini.}\}.$$

Nous démontrons maintenant quelques propriétés élémentaires de ces deux quantités afin d'atteindre le Théorème 4.2.3.

Lemme 4.2.9 *Soit $\alpha \in \mathbb{R}$*
(i) $\forall k \geq 1, \omega_k(\alpha) \leq \omega_{k+1}(\alpha)$,
(ii) Si α n'est pas algébrique de degré inférieur ou égal à k alors $\omega_k(\alpha) \leq k$,
(iii) Si α est algébrique de degré d alors $\forall k \geq 1, \omega_k(\alpha) \leq d - 1$,
(iv) $\forall k \geq 1, \omega_k^*(\alpha) \leq \omega_{k+1}^*(\alpha)$,
(v) $\forall k \geq 1, \omega_k(\alpha) \geq \omega_k^*(\alpha)$.

PREUVE : (i) Il suffit d'observer que : $\forall \omega \in \mathbb{R}, \mathcal{A}_k(\alpha,\omega) \subset \mathcal{A}_{k+1}(\alpha,\omega)$.
(ii) C'est une simple traduction du Corollaire 4.2.6.
(iii) Il suffit d'utiliser une inégalité de type Liouville. Explicitement, il existe une cons- tante $C(k,\alpha) > 0$ telle que si $P \in \mathbb{Z}[X], P(\alpha) \neq 0$, et $\deg P \leq k$, on ait $|P(\alpha)| \geq C(k,\alpha) H(P)^{-(d-1)}$. Si $P \in \mathcal{A}_k(\alpha,\omega)$, on a forcément :

$$H(P)^{\omega-(d-1)} \leq 1/C(k,\alpha)\,.$$

Ainsi : $\mathcal{A}_k(\alpha,\omega)$ infini $\Rightarrow \omega \leq d-1$. Donc $\omega_k(\alpha) \leq d-1$.
(iv) Il suffit d'observer que : $\forall \omega^* \in \mathbb{R}, \mathcal{A}_k^*(\alpha,\omega^*) \subset \mathcal{A}_{k+1}^*(\alpha,\omega^*)$.
(v) Nous allons construire une injection de $\mathcal{A}_k^*(\alpha,\omega^*)$ dans $\mathcal{A}_k(\alpha,\omega^*)$, ce qui montrera le résultat voulu, en prenant la borne supérieure sur $\omega^* \in \mathbb{R}$. Soit $\beta \in \mathcal{A}_k^*(\alpha,\omega^*)$ supposé infini, avec $\beta \neq \alpha$. Si α est algébrique de degré inférieur à k, nous supposerons de plus que β est différent des conjugués de α, de sorte que nous aurons toujours $\pi_\beta(\alpha) \neq 0$.

Soit d le degré de β. Nous observons que $H(\beta) = H(\pi_\beta(X))$ et que $\pi_\beta(\alpha) = (\alpha-\beta)Q_\beta(\alpha)$, où $Q_\beta(X) \in \mathbb{Q}(\beta)[X]$. Nous allons estimer la taille des coefficients du polynôme Q_β ; écrivons pour cela :

$$\pi_\beta(X) = \sum_{i=0}^{d} a_i X^i \text{ et } Q_\beta(X) = \sum_{i=0}^{d-1} q_i X^i\,.$$

Un calcul élémentaire montre que :

$$-\beta q_0 = a_0 \tag{4.16}$$

$$a_i = q_{i-1} - q_i\beta,\ i = 1,\ldots,d-1 \tag{4.17}$$

$$q_{d-1} = a_d \tag{4.18}$$

Comme π_β est irréductible, $q_0 \neq 0$ et (4.16) nous donne $\beta = -a_0/q_0$. En joignant cette égalité à (4.17) et (4.18), on montre par récurrence sur les indices les deux propriétés suivantes :

$$\forall i \in \{0,\ldots,d-1\}, |q_i| \leq \textstyle\sum_{i=0}^{d-1} \frac{H(\pi_\beta)}{|\beta|^i}\,,$$

$$\forall i \in \{0,\ldots,d-1\}, |q_i| \leq \textstyle\sum_{i=0}^{d-1} H(\pi_\beta)|\beta|^i\,.$$

Il résute de ces deux faits que : $|\pi_\beta(\alpha)| \leq |\alpha-\beta| C(k,\alpha) H(\pi_\beta)$ où $C(k,\alpha) = k\sum_{i=0}^{d-1}|\alpha|^i$.

Cela prouve que pour $\epsilon > 0$ et $H(\pi_\beta)$ assez grand (rappelons que $\mathcal{A}_k^*(\alpha,\omega^*)$ est infini), nous avons :

$$0 < |\pi_\beta(\alpha)| < H(\pi_\beta)^{-\omega^*+\epsilon}\,.$$

Ainsi $\mathcal{A}_k(\alpha,\omega^*-\epsilon)$ est infini, donc $\omega^*-\epsilon \leq \omega_k(\alpha)$, et comme ceci est vrai pour tout $\epsilon > 0$, on en déduit : $\omega_k^*(\alpha) \leq \omega_k(\alpha)$. ■

Nous sommes maintenant en mesure de montrer le Théorème 4.2.3.

Soit d le degré de α. Nous observons que :

a) Si $k < d$, α n'est pas algébrique de degré inférieur ou égal à k donc $\omega_k(\alpha) \leq k$ d'après le cas (ii) du Lemme 4.2.9.
b) Si $k \geq d$, l'assertion (iii) du Lemme 4.2.9 montre que $\omega_k(\alpha) \leq d - 1 \leq k - 1 \leq k$.

Dans les deux cas $\forall k \geq 1, \omega_k(\alpha) \leq k$, donc d'après l'assertion (v) du Lemme 4.2.9, $\forall k \geq 1, \omega_k^*(\alpha) \leq k$. En particulier $\forall \delta > 0, \omega_k^*(\alpha) < k + \delta$, ce qui est exactement le contenu du Théorème 4.2.3.

Appendice : quelques lemmes techniques

Nous avons regroupé dans cet appendice, certains lemmes techniques qui ont été utilisés dans les chapitres 2 et 3 qui ne rentraient pas de façon naturelle dans les chapitres 1 et 2.

Lemme A (Lemme de Siegel) *Soient M formes linéaires à coefficients dans $\mathbb{Z}$*

$$L_j(z_1, \dots, z_N) = \sum_{k=1}^{N} a_{jk} z_k, \quad j = 1, \dots, M, \quad N > M\,.$$

Supposons que $\max_{\substack{1\le j\le M\\ 1\le k\le N}} |a_{jk}| \le A$, *où* $A \in \mathbb{N}^*$. *Alors il existe* $z \in \mathbb{Z}^N \setminus \{0\}$ *tel que*

$$\forall j = 1, \dots, M,\ L_j(z) = 0 \text{ et } \|z\|_\infty \le (NA)^{(M/(N-M))}\,.$$

Preuve : Voir exemple [Sch1] p. 123, [Sch2] p. 1, ou encore le Lemme 6 du Chapitre 2 de [Hab]. ■

Lemme B *Soient r et n deux entiers supérieurs à 1, alors le nombre d'éléments de $\mathbb{N}^n$ dont la somme des composantes est r vaut*

$$c(n,r) = \binom{r+n-1}{n-1} = \frac{(n-1+r)!}{(n-1)!\ r!}\,.$$

Preuve : C'est un résultat classique utilisant les séries formelles. On part de l'identité

$$\frac{1}{1-X_1} \cdots \frac{1}{1-X_n} = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} {X_1}^{i_1} \dots {X_n}^{i_n}\,,$$

qui montre que

$$c(n,r) = \frac{f_n^{(r)}(0)}{r!} \text{ où } f_n(X) = \frac{1}{(1-X)^n}\,. \quad ■$$

Lemme C *Soient $(r_1, \dots, r_m)$ des entiers positifs, $0 < \epsilon < 1$ et $n \ge 2$. Le nombre de nm-uplets d'entiers positifs avec*

(i)
$$\sum_{k=1}^{n} i_{hk} = r_h,\ 1 \le h \le m\,,$$

(*ii*)
$$\left|\left(\sum_{h=1}^{m}\frac{i_{h1}}{r_h}\right)-\frac{m}{n}\right|\geq \epsilon m\,,$$

est au plus égal à

$$\binom{r_1+n-1}{r_1}\dots\binom{r_m+n-1}{r_m}.2.e^{-\epsilon^2 m/4}\,.$$

Plus précisément, si $\mathcal{M}^+$ désigne l'ensemble des mn-uplets vérifiant (i) tels que

$$\left(\sum_{h=1}^{m}\frac{i_{h1}}{r_h}\right)-\frac{m}{n}\geq \epsilon m\,,$$

et si $\mathcal{M}^-$ désigne l'ensemble des mn-uplets satisfaisant (i) tels que

$$\left(\sum_{h=1}^{m}\frac{i_{h1}}{r_h}\right)-\frac{m}{n}\leq -\epsilon m\,,$$

alors

$$\max\{\mathcal{M}^+,\mathcal{M}^-\}\leq\binom{r_1+n-1}{r_1}\dots\binom{r_m+n-1}{r_m}.2.e^{-\epsilon^2 m/4}\,.$$

En fait si pour $j=1,\dots,m$, on a $0\leq c_j\leq r_j$ et si $f_j(c_j)$ désigne le nombre de $(n-1)$-uplets d'entiers positifs $(i_{j2},\dots,i_{jn})$ avec $i_{j2}+\dots+i_{jn}=r_j-c_j$, alors

$$\mathcal{M}^{\pm}=\sum_{(c_1,\dots,c_m)\in\mathcal{E}^{\pm}} f_1(c_1)\dots f_m(c_m)$$

où

$$\mathcal{E}^+=\{(c_1,\dots,c_m)\in\mathbb{N}^m, 0\leq c_j\leq r_j \text{ pour } j=1,\dots,m \text{ et } \left(\textstyle\sum_{h=1}^{m}\frac{c_h}{r_h}\right)-\frac{m}{n}\geq\epsilon m\}$$
$$\mathcal{E}^-=\{(c_1,\dots,c_m)\in\mathbb{N}^m, 0\leq c_j\leq r_j \text{ pour } j=1,\dots,m \text{ et } \left(\textstyle\sum_{h=1}^{m}\frac{c_h}{r_h}\right)-\frac{m}{n}\leq-\epsilon m\}$$

PREUVE : C'est le Lemme 4C de [Sch1] p. 124-125. ■

Lemme D *Soit $n\geq 2$ un entier, $a_1,\dots,a_n$ des entiers premiers entre eux et $a_1\neq 0$. Il existe alors $j\in\{2,\dots,n\}$ tel que*

$$(a_1,a_j)\leq |a_1|^{(n-2)/(n-1)}\,.$$

PREUVE : On pose $d_j=(a_1,a_j)$, de sorte que $d_2\dots d_n$ divise ${m_1}^{n-2}$ donc a fortiori $d_2\dots d_n\leq |m_1|^{n-2}$. En raisonnant par l'absurde on en déduit l'inégalité demandée. ■

Bibliographie

[Dav] Davenport H. – Minkowski's inequality for the successive minima associated with a convex body, Quart. J. Math. Oxford **10** 119-121 (1939).

[EdE] Edixhoven B., Evertse J.-H. – Diophantine approximation and Abelian varieties, Lecture Notes in Mathematics n° 1566, Springer-Verlag, New-York, Berlin, Heidelberg (1993).

[Eve] Evertse J.-H. – The subspace theorem, Lundis Arithmétiques de l'I.H.P., deuxième exposé du 26 Février 1996.

[Hab] Habsieger L. – Introduction à l'approximation diophantienne, Cours de D.E.A., Université Bordeaux I, (1993-94).

[Rot] Roth K. F. – Rational approximations to algebraic numbers, Mathematika **2** 1-20 (1955).

[Sam] Samuel P. – Théorie algébriques des nombres, Hermann, Paris (1967).

[Sch1] Schmidt W. M. – Diophantine approximations, Lecture Notes in Mathematics n°785, Springer-Verlag, New-York, Berlin, Heidelberg (1991).

[Sch2] Schmidt W. M. – Diophantine approximation and Diophantine equations, Lecture Notes in Mathematics n°1467, Springer-Verlag, New-York, Berlin, Heidelberg (1991).